Control of Multi-Module Nuclear Reactor Stations

by

Matthew Jay Schor

B.S. Nuclear Engineering, University of Virginia
(1985)

SUBMITTED TO THE DEPARTMENT OF
NUCLEAR ENGINEERING
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

MASTER OF SCIENCE
IN NUCLEAR ENGINEERING

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 1986

Signature of Author Signature redacted
Department of Nuclear Engineering
December 11, 1985

Certified by Signature redacted
Michael J. Driscoll
Thesis Supervisor

Certified by Signature redacted
David D. Lanning
Thesis Supervisor

Accepted by Signature redacted
Allan F. Henry
Chairman, Departmental Committee on Graduate Studies

Control of Multi-Module Nuclear Reactor Stations

by

Matthew Jay Schor

Submitted to the Department of Nuclear Engineering
on December 11, 1985 in partial fulfillment of the requirements
for the Degree of Master of Science in Nuclear Engineering

Abstract

Technological and regulatory issues associated with the control of multi-module nuclear reactor stations have been examined. Applicable technologies from other related industries have been investigated, and their impact on a power plant control system design are discussed.

The new technologies which promise to have the most effect on a multi-module control system are: fault tolerant processors, sensor fault tolerance techniques, artificial intelligence in the form of real time 'expert systems', and fiber optic communications. A control system incorporating these features would be highly automated, extremely reliable, and require a minimum number of operators.

A candidate configuration employing the above components is presented for discussion purposes, and aspects requiring further clarification are identified.

Thesis Supervisors: Dr. David D. Lanning
Title: Professor of Nuclear Engineering

Dr. Michael J. Driscoll
Title: Professor of Nuclear Engineering

Acknowledgements

This work was supported under a research contract with the General Electric Corporation as part of their Department of Energy sponsored efforts on advanced reactor development. Work performed in the fall of 1985 was supported by the Department of Energy through a fellowship in Nuclear Engineering.

The author would like to thank Professor Michael Driscoll and Professor David Lanning for their guidance and helpful insight throughout the entire research effort.

The author also gratefully acknowledges Dr. John Hopps, of the Charles Stark Draper Laboratories, for the information on the Advanced Information Processing System. The author would also like to thank Bruce Bodnar of Northeast Utilities for his generosity in taking his own time to explain, in detail, the state of control technology at Millstone Unit 3. Also, the engineers and managers at Lisp Machine Incorporated were extremely helpful in their description of PICON, and real time artificial intelligence systems. Finally, W. R. Daniel of the General Electric Company is thanked for his input.

The control system described in this report is presented for discussion purposes only, and is not necessarily the best design or the only possible one for a multi-module nuclear power plant. In particular, it should not be construed as critical of specific features under development by General Electric for their PRISM reactor.

Table of Contents

Table of Contents (continued)

Chapter 4 Conceptual Features of a Multi-Module Control System (continued)

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Foreword

The current emphasis on small, inherently safe, modular nuclear power plant designs which rely upon passive means for decay heat removal has led to the consideration of digital computers for active control of the entire power plant.

The relatively low thermal power of individual modules necessitates coupling several units to a single turbine / generator for the economic operation of the plant. Up to five modules (reactor plus steam generator) will feed a single turbine, and there may be as many as three or four of these combined units operating at one site. Thus up to twenty modules (100 MWe per module) may be at a single site.

This multitude of modules makes the use of digital computers for plant control almost mandatory. If conventional control methods were employed, there could be a total of 80,000 control signals and operating parameters to be monitored and processed. If each module were to have its own complete control room with the usual complement of operators, the cost of both constructing and operating the plant would make multi-modular power plants prohibitively expensive. New process control and data processing techniques must be intelligently applied in order for the dis-economies of scale to be offset for this smaller design.

1.2 Background

Direct digital control of nuclear power plants has not been practiced in the past in the United States. Only recently have U.S. researchers begun to apply digital control to nuclear reactor control, and this has been done only on small research reactors. The application of digital computers to power plant control will only occur if the reliability of computer-based systems is increased and if regulatory agencies revise their current position on such use.

The reliability and availability of computers can be increased through a variety of fault tolerant techniques developed for the industrial use of computers. Additionally, the 'reliability' of the control software is being increased through advanced programming methods that allow the power plant design engineer to 'program' the computer without the need to learn the programming language or having a computer programmer do the job. This eliminates the previously error prone step of having the design engineer communicate the description of the power plant to the programmer. These methods, which promise to increase the reliability of the digital computer, will enable the computer to become fully qualified for nuclear power plant control.

1.3 Organization of this Report

Non-nuclear industries are under a different set of constraints than the nuclear industry, and are thus able to apply the latest in control technologies to their specific needs. A survey of a variety of industries ranging from aircraft to chemical plants was performed in order to identify which industries are most closely related to nuclear power plant control. The most closely related industries with the furthest advanced control techniques were chosen, and descriptions of their control systems appear in Chapter 2.

In Chapter 3 new technology that can be combined with the control technologies described in Chapter 2, is reviewed. Fault tolerant processors, fiber optic networking, and data analysis techniques are described. Additionally, a few examples of new display technologies which promise to improve the man-machine interface are reviewed, and a few relevant human factors considerations are discussed.

In Chapter 4 all these technologies are brought together in a description of a possible multi-module digital control system. Various questions are identified which need to be answered before advanced work can proceed on development of such a control system, as discussed in Chapter 5 in the summary and recommendation sections.

Chapter 2

Control Technology: State of the Art and Practice

2.1 Introduction

In order to identify control technologies relevant to multi-modular nuclear power plants, a survey of the state-of-the-art of control technologies in other industries was performed. Applications that received in depth studies were ones that had characteristics most resembling those of a nuclear power plant from a control viewpoint, namely large investment, accident severity, complexity, multi-modularity, number of control signals, operating conditions, and response time domain (e.g. milliseconds vs. hours). Table 2.1 lists applications that were initially considered, and rates each category (qualitatively) on a scale of one to four, where four correlates best with a nuclear power plant.

Table 2.1
Relevance of Control Applications to a Nuclear Power Plant

Application	Investment	Accident Severity	Complexity	Multi-Modularity	# of Control Signals	Operating Conditions	Time Domain
Multi-Engine Aircraft	2	2	2	2	1	1	1
Space Shuttle	3	1	3	2	2	1	1
U.S.S. Enterprise	2	2	4	4	3	4	4
Fly-by-Wire Aircraft	2	1	2	1	2	1	1
Fossil Power Plants	2	3	2	3	2	3	3
Chemical Plants	4	4	3	3	4	3	3
Space Nuclear Power	2	1	2	1	1	4	4

Multi-engine aircraft are only superficially multi-modular in the sense of multi-modular nuclear power plants because the engine is basically either off or on. Some comparison might be made relative to power control wherein the aircraft engine is controlled by local controllers and the pilot merely sets the required power. There are some other aspects of aircraft technology that are applicable, particularly in the area of sensor fault identification, as is demonstrated by a microwave landing system developed for a Boeing 737.

The Space Shuttle is almost completely digital computer controlled, but it is in a totally different time domain than a nuclear power plant. That is, many decisions need to be made so quickly that they can only be done by a computer. However, like multi-engine aircraft, there are also relevant sensor fault techniques used.

Digital Fly-by-Wire supersonic aircraft such as the X-29 or F-16 also must be controlled by a computer because they are unstable and adjustments must continuously be made to the control surfaces in order for the aircraft to fly stably. Again the time domain of these aircraft is much shorter than nuclear power plant control, and thus less applicable. Also, detailed technical information is classified.

The aircraft carrier U.S.S. Enterprise is perhaps the most related to a multi-modular nuclear power plant since it has eight reactors on board (with two reactors per propeller shaft[1]) and four control rooms. However, since it was the first nuclear powered aircraft carrier (launched in 1960) the degree of digital computer control is probably not high, and, like the F-16, technical information is classified.

[1] R. G. Hewlett, F. Duncan, Nuclear Navy, University of Chicago Press, Chicago, 1974. Page 280.

Fossil-fired power plants, especially gas turbines, are multi-modular, but they interconnect only at the switchyard. In addition, the degree of computer control is not high enough to warrant further study.

By far the most applicable case discovered was found in the chemical process industry. A computer system has been developed that combines artificial intelligence capabilities with fast data collection to create an expert system process control advisor. It is being applied to oil refinery control, and is likely to be the most advanced application of artificial intelligence relevant to multi-modular nuclear power plants.

To put these technologies in perspective, a nuclear power plant nearing completion was investigated with respect to its process computer and data transmission techniques. Finally, the Japanese and Canadian experience with automatic control was investigated, since these countries are not under the same regulatory constraints and have applied automatic control to a much greater extent.

2.2.1 Regulatory Constraints

The nuclear regulatory environment is a conservative one. This conservatism requires that any system needed for the safe shutdown of the plant (safety related), or is associated with a safety related system, must go through an exhaustive quality control test. Traditionally this has meant that only proven technology could be employed in safety systems. As a result, utilities have shied away from using sophisticated digital computers because it is next to impossible to fully test their software. An extension of this philosophy led to a policy of not allowing a digital computer to actively control a nuclear reactor core. However, this situation is slowly changing as is illustrated by experiments on the Massachusetts Institute of Technology's research reactor. A computer with sensor fault tolerance controlled the position of the reactor's regulating control rod.[2] And, in the safety area, a digital computer on Arkansas Unit 1 continuously calculates various reactor core safety limits, and when one of them is exceeded the reactor scrams.[3] Despite these advances, the regulatory climate remains conservative and currently excludes, with few exceptions, the use of digital computers in either an active safety or operational role.

---

[2] A. Ray, M. Desai, J. Deyst, "Fault Detection and Isolation in a Nuclear Reactor," Journal of Energy, Vol. 7, No. 1, (January - February 1983). Page 79.

[3] This system was built by Combustion Engineering.

2.2.2 United States Practice - Millstone Unit 3*

The Millstone 3 Nuclear Power Plant was selected in order to investigate, in the shortest amount of time, the state of control technologies at current power plants. Millstone 3 was chosen because the plant is scheduled to come online in May of 1986, it is nearby, and because of the researcher's familiarity with the plant. The plant is an 1150 MWe Westinghouse PWR, to be operated by Northeast Utilities. The plant process computer is of particular interest since it is considered by some to be the most advanced at an existing nuclear power plant.

The Millstone 3 process computer is a ModComp Classic-32 computer (ModComps are used for ground control of the Space Shuttle) with two identical central processing units (hosts), and two satellite computers associated with each host for preprocessing of data. The system has 4000 digital inputs and 2000 analog inputs, almost all of which are hardwired into the satellites. The system is purely a display device and serves no control functions. Its most sophisticated function is as part of the Safety Parameter Display System (SPDS). SPDS is similar to expert systems in terms of inference ability in that it measures various plant conditions to determine if certain accident scenarios are occurring. For example if there is a leak in the primary coolant system it will account for all sources and sinks (letdown, makeup, coolant pump seal leakage), calculate the difference, check to see if the containment sump level is rising at a corresponding rate, and if all conditions exist it will signal a primary leak. However, SPDS is less sophisticated than expert systems since it is programmed in FORTRAN and thus needs the services of a skilled programmer

* The information presented in this section resulted from an interview with Bruce Bodnar, Computer Operations Dept., Northeast Utilities in July, 1985.

for development and modification. Nevertheless, SPDS does offer simple sensor fault detection (analytic and sensor redundancy) with a more advanced information display system than that of simple annunciators and meters.

The process computer was designed to be dual redundant with respect to hardware and software. Each host is capable of processing six application programs concurrently in addition to the scan and alarm programs. If one host fails the programs 'fail over' to the other host. The two satellites that preprocess the data are similarly configured in that each has the capability to process all of the data. The satellites are fed by data multiplexors which gather data from termination cabinets outside of the computer room. The multiplexors are not redundant and thus are susceptible to single mode failure.

In addition to the protection afforded by this dual redundancy some parts of the process computer are, in a sense, distributed. The radiation monitor subsystem is controlled by dual redundant PDP-11's and the flux mapping subsystem is microprocessor (Intel 8085) controlled. These subsystems are serially linked (RS-232) to the process computer. The most advanced data link at the plant is to the Inadequate Core Cooling system.

The Inadequate Core Cooling (ICC) system consists of several systems such as the subcooled margin monitor and the reactor water level system (Combustion Engineering heated junction thermocouple). The data from the ICC is multiplexed over a fiber optic line to the process computer.

The process computer also is replacing some of the control board in the sense that not all of the data that is fed to the computer appears on the control board. For instance if there is a fire in a certain part of the plant, the 'Fire Area

A' annunciator lights on the control board and the operator has to query the computer for more detailed information.

It is important to recognize how the utility views the process computer from the regulatory viewpoint. Northeast Utilities considers the process computer to be 'quality related'. That is, it is useful for the economic operation of the plant. If the process computer with its associated hardware and software were to be classified as safety related, Northeast Utilities feels it would be impossible to apply conventional quality control procedures to the computer.

Overall, the degree of technology at Millstone is very advanced in a few subsystems, i.e. the plant computer is state of the art, but it is not allowed to control any device. Any critical control functions are served by proven technology such as PID loops; a circumstance which can be attributed to a variety of reasons ranging from the conservatism of the plant's owner/operator to the perceived difficulties of shepherding such a complicated system through the regulatory process.

2.2.3 Foreign Practice - Canada & Japan

Foreign nations have proceeded further with automatic digital control for nuclear power plants than the United States because of their different regulatory climate. Canada and Japan are prime examples since both have made extensive progress to date. Canada has used digital computers for control since the CANDU (CANadian Deuterium Uranium) reactor was first developed in 1966.[5]

The CANDU computer control system is used for numerous purposes including the vital functions of: alarm annunciation, data display, reactor power control, primary heat transport system pressure control, steam drum pressure control, and steam generator level control. Allocating these functions to the computer resulted in a 40% reduction in the numbers of meters and recorders in the control room.[6]

The computer uses alarm conditioning to suppress alarms, except the primary alarm, which result from an event such as a power loss. In addition, alarm reports are sorted in order of priority. These techniques reduce operator confusion.

The control system is supervised and run by two independent identical minicomputers used in a redundant fashion; and each computer has been found in practice to have an availability of over 99%. While neither is capable of running all applications individually, they are able to run all vital functions for normal plant operation should one fail. If this occurs the computer that was in a 'hot standby' mode takes over control of the plant. These computers are

---

[5] E. M. Hinchley, et. al. "The CANDU Man-Machine Interface and Simulator Training," Chalk River Nuclear Laboratories, Ontario. AECL-7768, (Sept. 1982). Page 2.

[6] Ibid 5, Page 4

independent of the safety system, and all safety systems are controlled by hard-wired logic systems, not digital computers. This situation may change since a computer based system called the "Intelligent Safety System" is being developed at the Chalk River National Laboratories.[7]

The Intelligent Safety System (ISS) is being developed because existing shutdown systems, which contain 87 sensors, are difficult to test, and because plant operators would benefit by a computer display of the shutdown system status. The ISS design is based on a supervisory computer (such as a ModComp CLASSIC-32) and three safety computers (DEC PDP-11/55's) for numerical processing of the data. The safety computers contain algorithms for sensor fault tolerance and an algorithm which estimates the maximum fuel channel power via a diffusion theory reactor physics calculation. This fuel channel power is then compared to the maximum allowed for the fuel design, and if the margin is too small the reactor trips. The software for the safety computers is written in RATFOR (RATional FORtran). Software for the supervisory computer has not been developed yet (July, 1984).[8] This system is notable for its distributed architecture, which is directly applicable to multi-modular control system design.

The possible future of control systems for the CANDU was described in a 1978 report entitled: "Distributed Computer Control Systems in Future Nuclear Power Plants"[9] This report specifies that the transmission medium for distributed control systems will be based on cable television (CATV), possibly followed by fiber optics. It is interesting to note that it only took 7 years for fiber

---

[7] J. A. Hall, et. al. "The Intelligent Safety System: Could it Introduce Complex Computing into CANDU Shutdown Systems?,"Chalk River Nuclear Laboratories, Ontario. AECL-8561, (July 1984).

[8] Ibid 5, Page 4.

[9] G. Yan, J.V.R. L'Archèveque, L.M. Watkins, "Distributed Computer Control Systems in Future Nuclear Power Plants," Chalk River Nuclear Laboratories, Ontario. AECL-6365, Sept. 1978.

optics to totally bypass the use of CATV, as is illustrated by the use of fiber optics at Millstone Unit 3.

Progress in nuclear power plant control technology is also occurring in Japan. The Japanese, have automated their plants, but not to the extent that Canada has. Nevertheless it appears that the Japanese intend to extend the concept further through the use of expert systems. Three plant automation programs in progress which were reviewed are: 1) Backfitting of current boiling water reactors (BWRs) with automation, 2) Development of automation for the Advanced Boiling Water Reactor (ABWR), and 3) Development of expert system techniques to support both these programs.

The goals of the Japanese automation programs are threefold. The first is to improve monitoring of the plant status through the use of video displays (11 CRTs* in the control room). The second is to prevent error through the use of color coding of instruments and alarms and through the automatic transfer of CRT displays when a plant trip occurs. The third is to reduce operator workload through plant automation.

The goals of BWR automation are to control: the reactor water level during start up, plant trip, and full power; the primary system pressure during start up and shutdown; the turbine start up and generator synchronization with the electrical grid. Automating these systems will result in the reduction of required personnel to two for start up and shut down, one for continuous operation, and two in the event of a plant trip.

One objective of the ABWR automation, in addition to the previous goals, is to reduce operational cost through a shortened restart period after full load

* Cathode Ray Tubes.

rejection (90% output within five hours of the trip). To achieve automation a microprocessor based digital controller will be used for plant subsystems with a supervisory process computer for the entire plant. One notable specification is the availability for many revisions of the plant function diagram after the installation of the system. This is one capability that PICON (a process control expert system described in section 2.3.1) meets well.

The specifications of the knowledge based expert system for BWR control includes a LISP processor coupled with a FORTRAN processor which handles data communication with the various plant subsystems. Data transfer between the two processors is accomplished by sharing the memory where the data is stored. LISP handles this memory management.[11] (In PICON, the memory management is handled by the Unix processor freeing up the LISP machine for inference processing).

A knowledge based control system was developed and simulated for control rod withdrawal. The system was able to select the optimum rule in an average time of 0.3 seconds.[12] It used 50 rules, which were written in LISP. Since the rules are written in LISP, the engineer is required to have knowledge of both LISP and the plant being described.

Current BWRs in Japan use automatic control for plant start up. The computer controls the plant from 100% steam conditions and zero power to full power. The computer only regulates the recirculation rate in the core, not the control rods. Additionally the computer controls the turbine start-up, acceleration, initial load holding, and increase to rated power. Reliability is

---

[11] Takashi Kiguchi, et. al. "A Knowledge Based System for Plant Diagnosis," Energy Research Laboratory, Hitachi, Japan. (June 1985).

[12] Mitsuo Kinahita, et. al. "An Event-driven Control Method for Automatic Operation and Control of Nuclear Power Plant," Energy Research Laboratory, Hitachi, Japan. (June 1985).

accomplished by requiring operator verification of plant status before the computer takes the next step in the start up. Like other control systems the safety system controls are independent of the plant operational controls. As of June 1985, Toshiba corporation is testing automatic shutdown, and is developing a system incorporating control rod maneuvering, as part of an overall plan to fully automate BWR operations.[13] The completion and subsequent operation of these automatic control systems will be beneficial to the U.S. nuclear community.

Overall, the Canadian and Japanese experiences to date with computer based automatic control demonstrates the safe, reliable operation of a nuclear power plant by a digital computer while simultaneously reducing the operator workload. This reduction of operator workload will be instrumental to the implementation of multi-modular control systems.

[13] Seishiro Kawakami, et. al. "Operating Experience in Using Computerized Plant Automatic Start-Up Control System," Toshiba Corporation, Japan. (April, 1985).

2.3.1 Chemical Process Industry - Artificial Intelligence

Outside of the fossil-fired section of the electric utility industry the petrochemical field is the most closely related to the nuclear power field from a process control viewpoint. A large modern oil refinery has a replacement value capital cost on the order of one billion dollars (corresponding to a refining capacity of five million tons of crude oil annually[14]). Total U.S. refinery capacity in 1979 was equivalent to 245 large refineries.[15] The control system for a modern refinery is also complex, as is illustrated by the fact that 5000 variables are used by a typical control system.[16] Adding to the control complexity is the fact that pressures can be as high as 2500 pounds per square inch in hydrocracking units, and temperatures can reach 720°C (1328°F) for fluidized catalytic cracking.[17] Total product flow rates are on the order of 5 million pounds per hour, however internal circulation in some processing units can be several times the product flow. For comparison, a nominal 1000 MWe nuclear power plant currently costs on the order of 2.5 billion dollars.[18] The number of control variables is also high; 6000 control variables are monitored at the Millstone Unit 3 Nuclear Plant. Operating conditions are also similar: PWR coolant operating pressures and temperatures are 2200 pounds per square inch and 330°C (626°F) respectively. Feedwater/steam flow rates are on the order of 12 million pounds per hour.[19] In terms of complexity, multi-modularity (number of components in series and parallel), number of process control signals, investment, and operating conditions an oil refinery is roughly comparable to a

---

14 , The Petroleum Handbook, 6th ed. Elsevier Science Publishers, New York, 1983. Page 235.

15 S. P. Parker, McGraw Hill Encyclopedia of Energy, McGraw Hill, New York, 1981.

16 M. Kramer, Massachusetts Institute of Technology, personal communication, July, 1986.

17 D. M. Considine, (ed), Energy Technology Handbook, McGraw Hill Book Co., New York, 1977. Page 244.

18 F. J. Rahn, et. al. A Guide to Nuclear Power Technology, Electric Power Research Institute, Palo Alto, Ca. 1984. Page 833

19 Ibid 18, Page 266

multi-modular nuclear power plant from a control point of view. Futhermore, improper control of oil refineries and their associated petrochemical plants can involve significant financial and safety risks: a comprehensive compilation of major "catastrophes" lists some half-dozen incidents involving this industry.[20] Since the oil industry has greater freedom in the deployment of its sizable financial resources, and is not as constrained by prescriptive federal regulations with respect to its process equipment design and operation, advances in process control have proceeded, and should continue to proceed, at a more rapid pace at refineries and other chemical plants than at nuclear power plants. A pioneering example of particular interest here is the use of artificial intelligence in chemical process control.

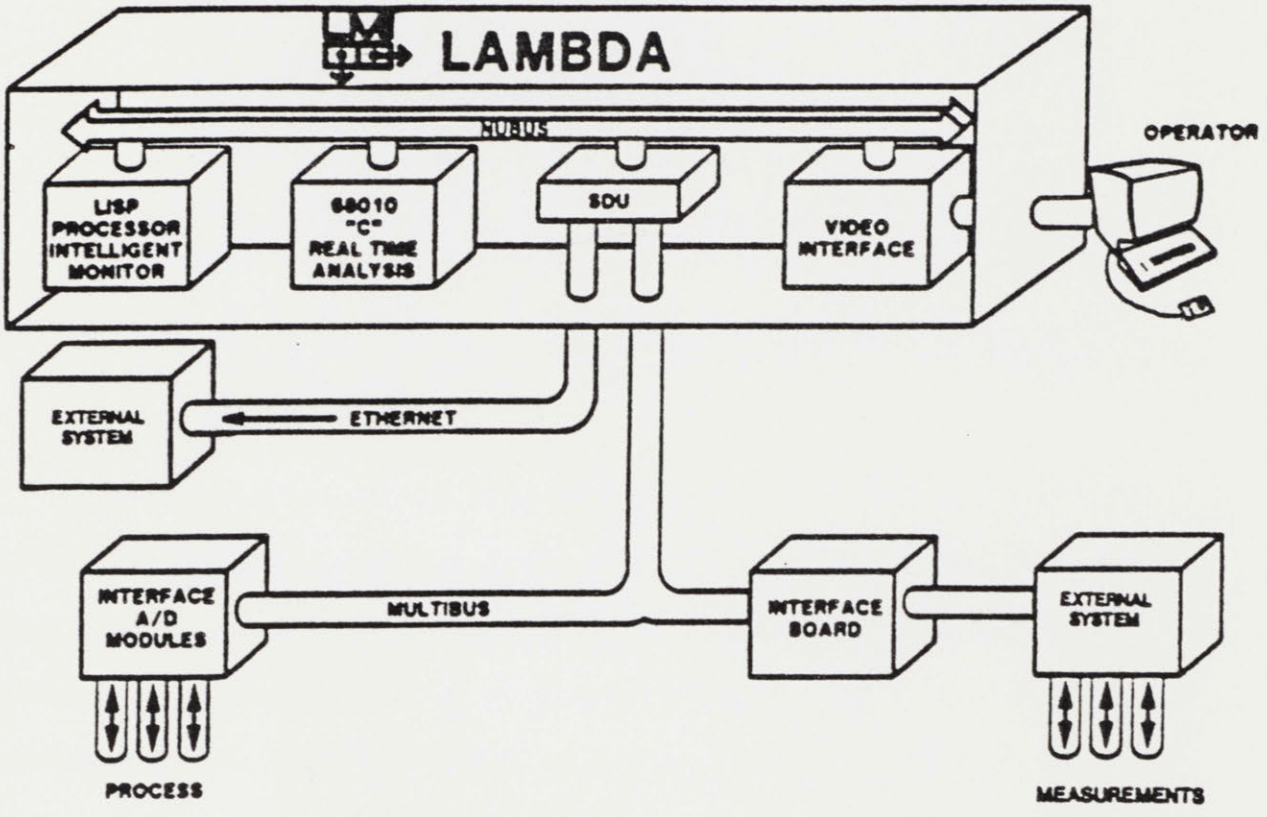
Chemical process control engineers are currently applying artificial intelligence to control in the form of real time expert systems. The system investigated here was PICON, developed by Lisp Machine Incorporated[21] (LMI), claimed by its developers to be the only real time expert system commercially available. Based on our review, this application represents the farthest that process control technology has proceeded in non-nuclear industrial applications.

PICON combines artificial intelligence with a plant process computer to enhance an operator's understanding of problems within the plant. PICON is intended for process control, although currently it is purely an operational aid for the plant operators. Hierarchically the device sits on top of an existing process control system (Fig. 2.1), and this control system is used as an input device for PICON. PICON consists of a LISP processor for making inferences about the

---

[20] F. Gibney, R. Pope, (editors), Catastrophe! When Man Loses Control, Bantam/Britannica Books, New York, 1979.

[21] Lisp Machine Incorporated, 6033 Century Boulevard, Los Angeles, Ca. 90045 (213) 642-1116



Courtesy Lisp Machine Inc.

Figure 2.1 PICON Architecture

state of the plant, and a Motorola 68010 processor (in a UNIX/C environment) for collecting and preprocessing data. The key advances that PICON represents are:

- It allows a description of the plant and its operating constraints (knowledge base) to be 'programmed' into the computer without the need to employ a skilled programmer.
- It is a real-time expert system.
- It can recognize accident scenarios as they unfold and recommend operator action while giving reasons for its recommendations.
- Its knowledge base can be easily updated and modified as the operators of the plant gain experience, thus enabling the system to learn with time.

Expert systems are fundamentally different than other computers in that there is a distinct difference between the knowledge in the program (knowledge base) and the program (inference engine) that acts upon that knowledge. In conventional programs, such as the Safety Parameter Display System (backfitted to current Light Water Reactors), the knowledge is buried in the code (typically FORTRAN) and it takes an extensive effort to develop the code, and even a more dedicated effort to modify it. PICON's 'programming' is accomplished by the engineer drawing a schematic on the screen, and then entering rules that describe the plant operators knowledge.

To draw the plant schematic the engineer chooses an icon from a menu and places it on the screen. Then attributes are described for this device (Fig. 2.2). The required attributes are a tag name, and for sensors, the engineering unit, and a currency interval. The currency interval is how long a value is valid. If the currency interval is too long the value may not accurately represent the variable at all times, and if it is too short the real time part (RTIME) of PICON will become overloaded.

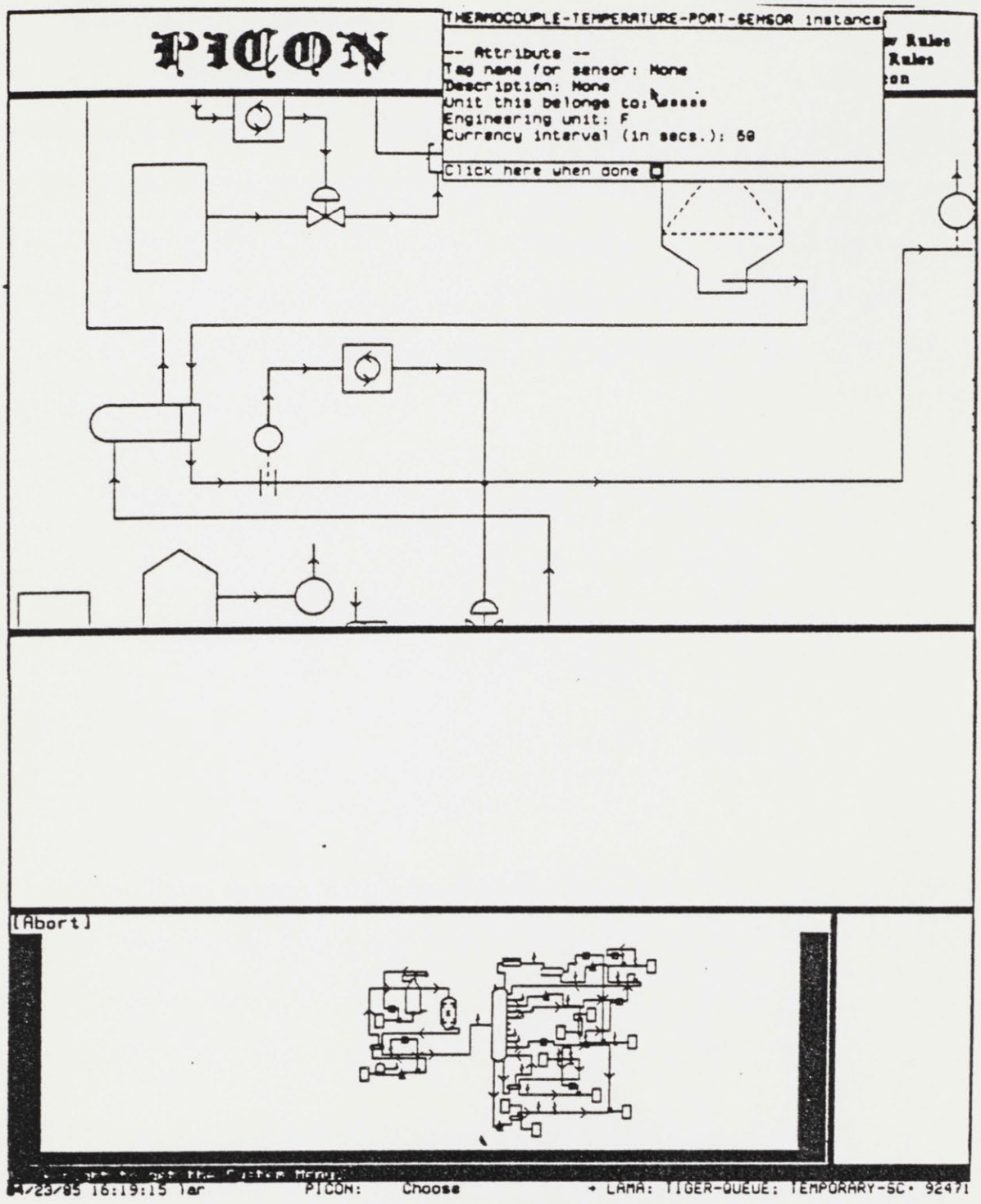


Figure 2.2 Establishing Attributes for Icons

Courtesy Lisp Machine Inc

Once the schematic is complete (see Fig. 2.3 for a catalytic cracker schematic) the engineer enters the rules (Fig. 2.4). If the rules are carefully designed only the most important messages will be sent to the operator. This is accomplished by creating primary and secondary rules. Primary rules are tested periodically and when one of them tests true it sends the operator a message and activates secondary rules which further diagnose the problem. For example the rule listed below activates secondary rules when the focus or suspect commands are used.

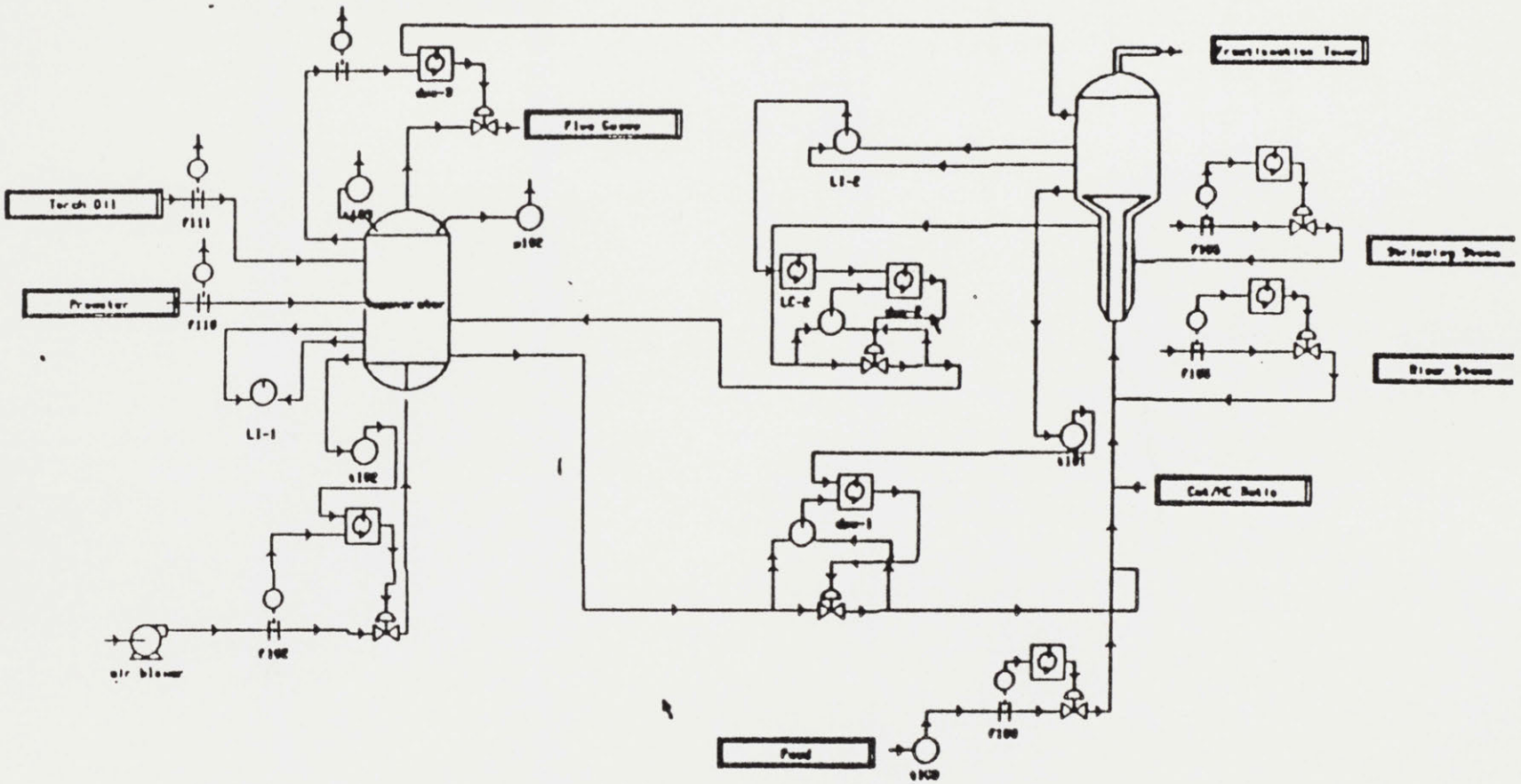
```
whenever regenerator-bed-temperature varies by 5 deg-f:
     if increase then request
       "Regenerator temperature has risen 5 degrees."
       and focus on reactor
       and focus on feed
       and suspect possibility-of-afterburn
     if decrease then request
       "Regenerator temperature has fallen 5 degrees."
       and suspect possible-behind-on-burn
       and focus on regenerator[22]
```

This rule is translated from the above format into LISP by PICON. This capability removes the error prone task of translating the description of the plant into the programming language while simultaneously preserving the 'knowledge' that the code represents for reference by future engineers.

The key advantage to a primary and secondary rule system is that it reduces the number of alarms which are sent to the operator, which allows the operator (and computer) to focus attention on the problem without being distracted by further alarms. PICON is able to handle the thousands of process variables by allocating the data collection to RTIME.

---

[22] , PICON Users Guide, Lisp Machine Incorporated, 1985, Page 76.



Courtesy Lisp Machine Inc.

Figure 2.3 Catalytic Cracker

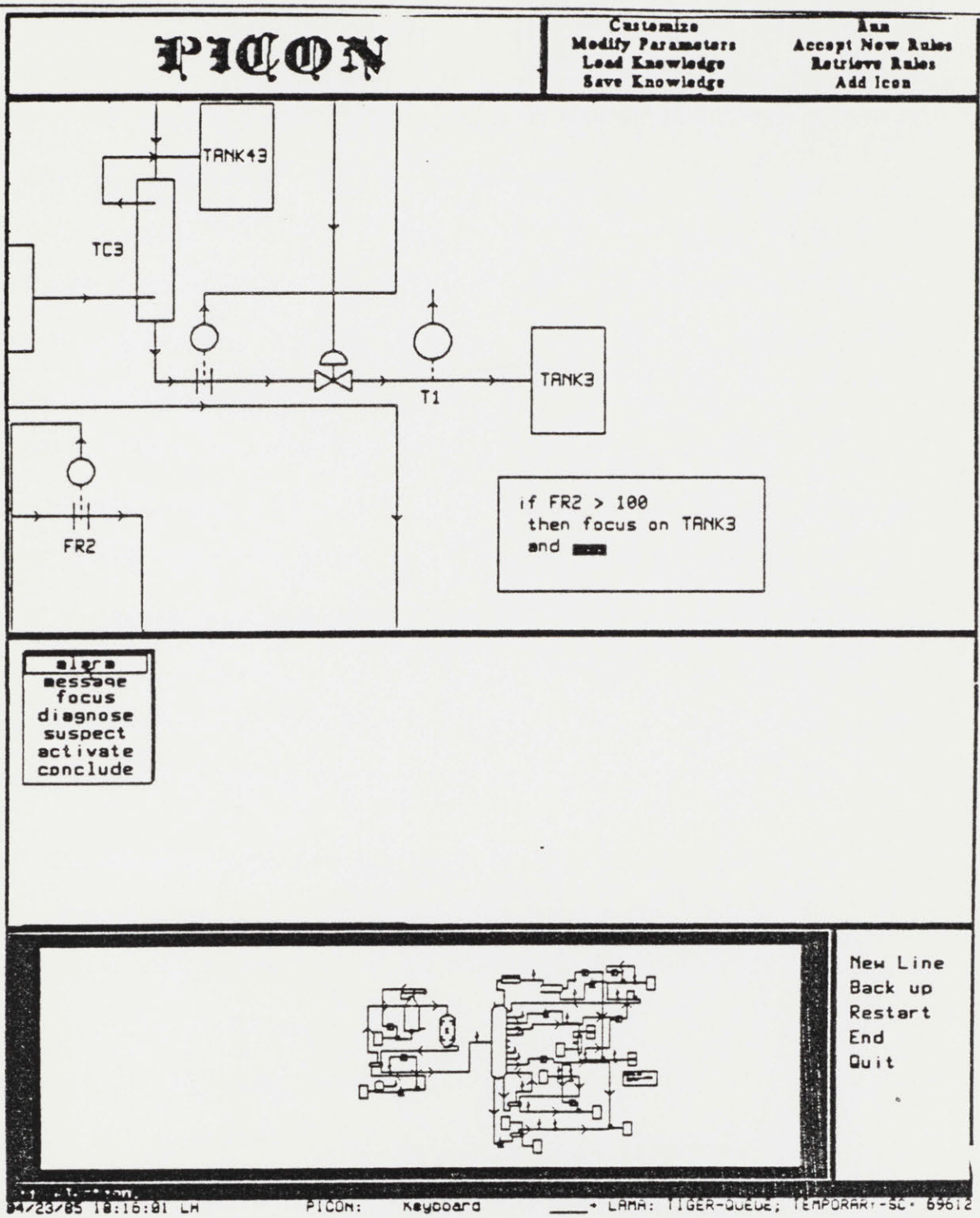


Figure 2.4 Creating a Rule

Courtesy Lisp Machine Inc

RTIME provides the real time link between PICON and the process control system, and it accepts instructions from the inference engine part of PICON. The inference engine tells RTIME how often data needs to be sampled, and what preprocessing is necessary for the data (such as smoothing the data over time, or signal validation). In addition to these functions RTIME will notify the inference engine when a specified condition has been reached. RTIME takes into account the frequency with which the data is needed and accordingly queries the process computer for the data. PICON's processing speed is capable of keeping all process variables current for a chemical plant, where typical sampling rates are on the order of a few seconds to hours. However, whether or not PICON's speed is sufficient for nuclear applications, where certain processes' time constants may be shorter, needs further investigation. Since one of the features of advanced nuclear reactors such as the LMR and HTGR is inherent, passive safety, in part through designed-in slow response times, this situation may be less onerous than that for LWR applications.

The knowledge base is developed and tested on a plant simulator for an application as complex as an oil refinery or nuclear power plant. If modifications are desired after PICON is installed at a plant, they would be first tested on a simulator before the PICON knowledge base is modified. PICON is currently (July 1985) being tested at a Texaco refinery in Texas with Texaco's simulator serving as the input device while the knowledge base is being fine-tuned. The successful use of a device such as PICON at an oil refinery will demonstrate that expert systems can be applied to industrial applications as complex and costly as a nuclear power plant.

2.3.2 Aerospace Applications

Airplanes and spacecraft, by necessity, employ digital computers for tasks such as navigation, engine control, and automatic guidance (auto-pilots). An aircraft such as a Boeing 747 cruising at 40,000 feet can not be manually flown with a straight and level attitude because the human eye can not sense small differences between the plane's attitude and the horizon. Automatic pilots were developed to both relieve the pilot from this tiring task and to increase the efficiency of long distance flying. Conversely, other tasks such as engine control and navigation were also delegated to digital computers for similar reasons. Spacecraft represent an even more demanding application since the launching and guidance of rockets require extremely precise firing of their engines to achieve the required trajectory. The Space Shuttle is completely computer controlled through launch to landing with the pilot only taking over control of the craft in the final moments before landing. The Shuttle could even land by computer control (as can the Boeing 747 and Lockheed L-1011), but pilots and passengers prefer human control during this last part of the flight.

Computer control for aircraft has extended sensor fault detection and identification technologies, and experience in this field has helped increase the reliability of digital control systems. The consequences of failure are high in both economic and human terms. Insurance premiums for aircraft and injury liability are on the order of 800 million dollars for 1985, and 1358 people have died in commercial aircraft accidents from January 1 to August 16, 1985.[23] Many of these crashes have been attributed to adverse weather conditions, such as the recent DC-10 crash in Dallas, Texas. Other crashes have been the result of multiple factors including weather and human error, such as that

[23], "Air Crashes hitting insurers heavily", The Boston Globe, August 16, 1985. Page 5.

involving the two 747's which collided on the runway at Tenerife Island, resulting in the death of 582 people. Of more relevance to control issues is the near fatal plunge of a 747 over the Pacific ocean in February of 1985.

A China Airline's 747 was cruising at 41,000 feet on autopilot when one engine lost power. The autopilot remained engaged and the plane subsequently plunged 32,000 feet in two minutes while rolling as far as 162 degrees to the right and nosing down 62 degrees. The incident appeared to be both a combination of pilot error and auto-pilot malfunction.[24] Experiences of this sort need to be thoroughly studied and demonstrated to either be in-applicable or of small probability before regulatory agencies will accept computer control in the nuclear field.

A more demanding application than an auto-pilot is an automatic landing system. A microwave landing system was developed for a Boeing 737 that incorporates analytic redundancy and an Extended Kalman Filter (EKF).[25] The EKF unit computes estimates for aircraft position, velocity, altitude, horizontal winds, and normal operating sensor biases on the assumption of no sensor failures. This result is then compared to new measurements using multi-hypothesis testing, and if it is inconsistent the multiple hypothesis test selects the most likely failure scenario and deletes the failed sensor making appropriate changes in the no-fail filter and detectors. This application demonstrates the modeling of a system and, using equations of motion, it predicts the future state of the system. This method of sensor validation and

---

24 , "NTSB Studies Reaction to Engine Loss in China Airlines Emergency Descent", Aviation Week & Space Technology, March 4, 1985. Page 29.

25 A.K. Caglayan, R.E. Lancraft, "An Aircraft Sensor Fault Tolerant System", NASA-CR-165876, Bolt, Beranek and Newman, Inc., Cambridge, MA. April 1982.

control is being developed for boiling water reactor level determination.[26] In the extreme, this method could be used to develop a complete neutronic and thermodynamic model of the multi-module reactor system, which could then be run in faster than real time to predict the future state of the power plant. However, this would require a system such as a Cray-1 or possibly a parallel computer which has specialized processors for solving the neutronics and thermalhydraulics equations. Nevertheless, this type of system may help to prevent unforeseen accident scenarios from endangering the system before the control system and operators can act.

The space shuttle Challenger experienced a control system failure on its July 29, 1985 launch. A temperature sensor (one of two) in its number two main engine (one of three) failed off scale. The other redundant sensor showed a temperature of 1850°R two minutes later, which caused the flight computer to shut the engine down. Emergency procedures were employed to get the shuttle into a safe orbit and to prevent the 39 ton external fuel tank from falling on Europe or the Middle East. As the remaining two engines continued firing the number three engine temperature sensor A failed and the other sensor began rising similarly to the previous fault in the number two engine. At this point the crew was instructed to inhibit the computer from shutting down the engine since the sensors were suspected of indicating false readings. This incident demonstrates the necessity of allowing the operators to override the computer. Since the shuttle launch requires faster than human action, the computer must be employed and allowed to act without pre-approval for every step. However, in nuclear power plants the time domain is much longer, and a more appropriate method would be to require the operator to verify the plant status in

[26] G. M. Garner, "Fault Detection and Level Validation in Boiling Water Reactors," PhD Thesis, Charles Stark Draper Laboratory and Dept. of Nucl. Eng., M.I.T., (September 1985).

various stages of operation before the computer is allowed to proceed with the next step.

The aerospace community has developed control systems that allow complete control of the aircraft by a relatively few number of people, while ensuring the safety of both the craft and its passengers. The techniques developed for sensor fault detection and isolation are directly applicable to nuclear power plants, and further developments for complex systems such as the space station promise to advance control technologies further.

2.4 Chapter Summary

Control technology both in and outside the nuclear industry has employed digital computers extensively. The chemical process control industry is making the most use of artificial intelligence techniques for control while the aerospace industry has made extensive use of sensor fault detection techniques. Canada and Japan both use digital computers for direct control of a nuclear power plant, and are advancing the technology of digital power plant control. One of the key applications of computer control is in chemical process plants, because of their many similarities to nuclear power plants, and because the large financial capabilities of the chemical industry promise to advance artificial intelligence techniques in process control considerably.

The joining of these advances with the latest techniques in fault tolerant computers, display and instrumentation technologies, and human factors engineering, will provide a sophisticated and reliable control system for a multi-module nuclear power plant.

Chapter 3

Review of New Technology

3.1 Introduction

Electronic and computer technologies are advancing at an ever increasing pace. In the field of personal computers, a machine introduced three years ago is outdated. Control technology is advancing similarly, as is demonstrated by three areas: computer networking, fault tolerant processing, and information display technology. Additionally, human factors engineers have begun to apply their expertise to the unique world of digital plant control, which is maximizing the use of the new technolgy to the utmost.

The use of many personal computers in one office complex has pressed the computer industry to network their machines together for office automation. On a larger scale, minicomputers in different buildings of a city are being networked via fiber optics for large, high speed data transfer. This technology is directly applicable to nuclear power plant control.

The defense, banking, and aerospace industries have motivated the computer industry to develop fault tolerant computers for their needs, which require the computer to have unavailability rates expressed in minutes per year. This type of computer is particularly well suited to power plant control. Addtionally, in the aerospace field, engineers have developed a variety of algorithms to analyze raw data for validity.

Finally, human factors engineers have made numerous studies as to which colors are best suited for different applications, the pros and cons of

various presentation schemes, and a host of parameters that impact an operator's efficiency.

The following sections give an introduction to all of these complex areas; more thorough explanations can be found in the references.

3.2.1 Data Communication and Analysis

Data Communication - Computer Networking:

There are many different methods of networking computers. These include simple low speed systems for personal computers, to high speed fiber optics. All of them, except fiber optics, are limited to a maximum transmission rate of 50 megabits per second, and are susceptible to electromagnetic interference (EMI). Rates of 50 megabits per second (Mbits/sec) are probably sufficient for power plant control, however immunity from EMI is required for nuclear power plant control applications. Thus, fiber optics is the medium of choice for a nuclear power plant. The only deficiency that fiber optics has is that its transmission clarity deteriorates in a high radiation environment. The American National Standards Institute is currently (February 1985) defining a standard for fiber optic networks called the Fiber Distributed Data Interface (FDDI).[27]

FDDI is a ring topology LAN (Local Area Network) designed for communication at rates up to 100 Mbits/sec over a distance of one to two kilometers. This is based on current fiber optics technology which is not as mature as other communication techniques. Fiber optics, when fully mature, will be capable of transmitting at a sustained rate of 80 Mbits/sec between 1000 nodes over a 200 kilometer path.[28]

---

[27] N. Makhoff, "LANs Team Up to Widen the Network Connection," Computer Design, Vol. 24, No. 2, (February, 1985). Page 108.

[28] Ibid 27

Data Analysis:

Several techniques have been developed to perform validation and verification of sensor data in control systems. They include voting, generalized likelihood ratio (GLR), multiple hypothesis, extended Kalman filter, the sequential probability ratio test (SPRT), and multifilter methods among others. All have their specific advantages and disadvantages, and are best suited to a particular application. A detailed explanation of each method is beyond the scope of this paper (see A.S. Willsky's survey for more information).[29]

Voting, the simplest method, is best applied when numerous identical sensors are available. Identical sensors have the same uncertainty and bias, and thus the data can be directly compared with the majority determining the true value. If the sensors were unlike, or if additional data was analytically generated, then a simple voting scheme can not be used because unlike data (different uncertainties, etc.) can not be directly compared. Thus, problems arise when the sensors are slightly different or when their values are a function of position, such as core power meters that measure the gamma ray flux. The other methods of determining sensor faults are variations of voting which try to improve the certainty of the result. Each of them will probably be used in various subsystems in the multi-module plant. For example, a fault detection and level validation method developed for BWRs considers the use of an extended Kalman filter or a nonlinear observer, for interpretation of the core liquid coolant level.[30] The data in a complex control system would usually be analyzed by in a digital computer, rather than in a hardwired logic system.

---

[29] A.S. Willsky, "A Survey of Design Methods for Failure Detection in Dynamic Systems", Automatica, Vol. 12, pp. 601-661. Pergamon Press, Great Britain. 1976.

[30] G. M. Garner, "Fault Detection and Level Validation in Boiling Water Reactors," PhD Thesis, Charles Stark Draper Laboratory and Dept. of Nucl. Eng., M.I.T., (September 1985).

3.2.2 Fault Tolerant Computers

A computer system that must be available continuously for the economic operation of a given process requires fault tolerance. Typical users of fault tolerant computers are airline reservation systems, and control systems for aircraft/spacecraft. There are many different techniques which can give a computer varying degrees of hardware fault tolerance. Hardware fault tolerance is different than sensor fault tolerance in that hardware faults occur within the computer, whereas sensor faults are external to the computer.

Fault detection techniques are of (roughly) two types. The first uses software to detect faults. This has been used since computers were first built, and is used to some degree on almost all computers. For example, in data communications, a parity bit is added to each byte that indicates whether the sum of all the bits in the byte are odd or even. If, at some point, the parity bit does not match its byte then an error has occured. Steps can then be taken to correct the byte, such as retransmission. Other more complex software techniques are "double checking", "check summing", "check-pointing", watchdog timers, and numerous others.[31] The second type of fault detection involves the use of hardware. This usually involves the replication of key components of the system for use as a backup or a check. When a checking method is used, the additional component is processing the same task and the results are compared to check for errors. This is known as self checking and is used only in systems that have at least three components processing the same task. Dual redundancy is used when the backup method is chosen.

---

[31] W. N. Toy, M. Morganti, "Fault Tolerant Computing," Computer, Vol. 17, No. 8, (August 1984). Page 6.

"Dual redundancy is the most common (hardware implemented) fault tolerance scheme."[32] A second computer system is in a 'hot standby' mode, and when the primary computer fails, the second computer takes over. This increases the availability of the computer substantially. A major disadvantage is that the control system is unavailable while control is being switched from the primary computer to the back-up computer. After the switchover any lost messages must be retransmitted and any corrupted data must be corrected.[33] This difficulty makes dual redundancy less than desirable for nuclear power plant control.

Triple modular redundancy avoids any momentary lapse of control due to a single error. In this method, the control computer and all its subsystems are triplicated. Each system is processing all signals and they periodically vote on the output. If one of the computers disagrees, its result is eliminated and the correct control output is still applied. "System availability with this approach is extremely close to 100 percent."[34] The disadvantage with this approach, as well as with dual redundancy, is that the software must be imbedded with routines to check when a failure in the hardware occurs (e.g. a vote occurs on the output to determine if one of the triad has failed). This unnecessarily complicates the development of software, and this could severely hamper the development of the complex operating routines necessary for complete control of a multi-module nuclear power plant. A solution to this is a method used by Stratus Computer* which is totally hardware dependent, and thus frees the software engineer from fault tolerance considerations.

---

[32] J. H. Wensley, "Redundant Modules May be Best for Control Systems," Computer Design, Vol. 24, No. 4, (April 1985). Page 121.

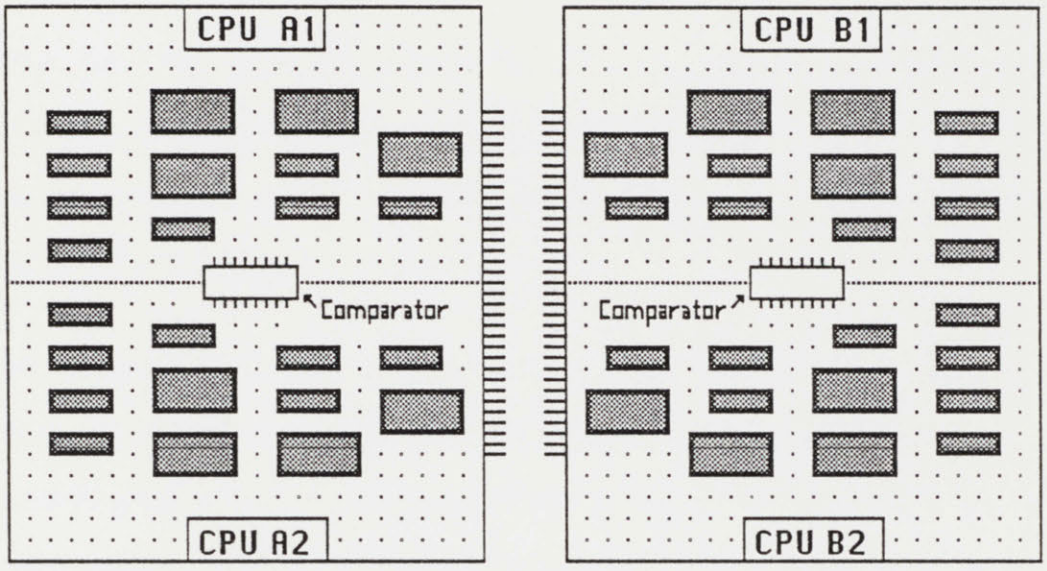
[33] Ibid 27

[34] Ibid 27, Page 122

* Natick, Massachusetts

Stratus Computer uses a technique called 'pair and spare', a subset of the 'self-checking' method. It is simple in concept and is illustrated in Figure 3.1.

Figure 3.1
Pair and Spare Strategy



The CPU board is shown. The CPU in a real system may actually reside on multiple boards, but the concept is still the same. As shown, the CPU is replicated four times, with CPUs A1 and A2 residing on a single board and CPUs B1 and B2 residing on the other, single, board. All four CPUs are executing the same task simultaneously and are sending the results onto the system bus (not shown). Before the results are put on the bus, they are first checked in the comparator (white rectangle) shown in the middle of each board. If there is a fault in CPU A2, it will not match the result from the correctly functioning CPU A1. The comparator prevents the error from entering the system bus. Since CPUs B1 and B2 are still functioning correctly, the system continues its operation without any degradation. Meanwhile, the faulty board

notifies the modem in the system that it has failed. The modem dials Stratus Computer's support center and a replacement board is sent to the customer via overnight delivery. The first time the customer realizes that something is wrong is when the new board arrives. The customer simply slides out the faulty board (the one with the flashing red light), and inserts the new one (while the system is running).

Only the CPU and memory boards use the 'pair and spare' approach, the rest of the system uses other self-checking techniques. This approach has proven quite successful in the marketplace, as Stratus' 1983 revenues were $20 million, its second year on the market.[36]

An important new fault tolerant design, that is bringing together fiber optics, fault tolerant computers, and sensor fault tolerance techniques is a generic distributed processing system being developed by the Charles Stark Draper Laboratory. CSDL's system is called AIPS - Advanced Information Processing System (shown in Figure 3.2; not shown on the diagram is a simple processor off one of the nodes).[37] It is a generic design intended for use on NASA vehicles. AIPS uses a fault tolerant processor (FTP) for critical control functions, with the degree of fault tolerance depending on the criticality of the function, i.e. a duplex FTP might be used for communications, whereas a triplex FTP might be used for life support system control . AIPS uses a central controller for supervisory control and distributed controllers for local intelligent control. Each card in the central controller is triply redundant, and the errors are detected by voting on the results of each calculation. If one card disagrees with

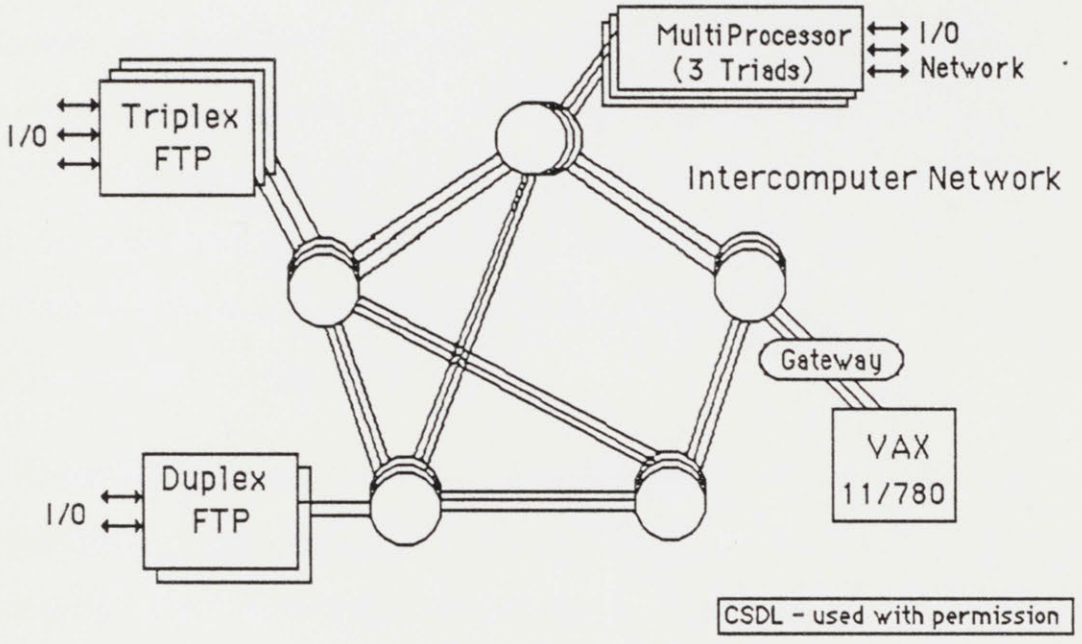
---

[36] O. Serlin, "Fault-Tolerant Systems in Commercial Applications," Computer, Vol. 17, No. 8, (August 1984). Page 24.

[37] The information on AIPS was supplied by Dr. John Hopps, Charles Stark Draper Laboratory in July, 1985.

the others, it is dropped out of the system and an online spare is picked up automatically to complete the triad. Additionally, each node in the network is triplicated for fault tolerance, and the communication medium between nodes will eventually be fiber optic. The latest design of AIPS (Fall, 1985) uses quadrex redundancy in both the central controller, and in the communication medium. AIPS represents the latest in distributed control systems, as it includes fault tolerance in all of its functions.

Figure 3.2
AIPS Proof-Of-Concept Configuration



3.2.3 Information Display Technology

A digital control system for a nuclear plant requires a special blend of display qualities that is only beginning to be met by new information display devices. The display qualities desired include: high resolution, color, implosion resistance, flicker free operation, and high luminance.

High resolution and color are needed because diagnosing a problem in a dynamic and complex system requires that the operators be able to discern the information quickly and accurately. Implosion resistance is required since earthquakes are considered in the design of a nuclear plant. Earthquakes can cause cathode ray tubes (CRTs) to implode, endangering the safety of both the plant and operators; however properly mounted CRTs are considered rugged enough to meet earthquake design requirements. Finally, flicker free displays with a high luminance prevent the operators eyes from tiring when looking at the display for long periods of time.

Current CRTs are able to provide high resolution and luminance, color, and relatively flickerless displays. However, CRTs are susceptible to implosion and are fairly bulky. In contrast, new flat panel displays overcome both of these difficulties.

There are four different types of flat panel displays; Liquid Crystal Display (LCD), Gas Electron Phosphor (GEP), plasma, and electroluminescent (EL). LCDs are commonly used in watches, calculators and portable computers, while the others are used only in larger, more expensive systems (except that Grid System's portable computer uses a plasma display, but it is quite expensive).

An EL display developed by Planar Systems has high resolution, high contrast, flicker free image, and ruggedness. It is able to withstand a shock of 100 g's.[38] The EL display consumes less power than a plasma display (which is not reviewed here because of its lack of color potential) and an EL display is capable of being fabricated with an area of up to one square meter using current techniques.[39] Whether or not the EL panel can be constructed in larger areas remains to be seen.

A GEP flat panel, developed by Lucitron Incorporated*, is able to produce a display as bright as a CRT. It has internal spacers which "support the envelope against atmospheric pressure, thus making possible displays of many square feet."[41] In this way, a GEP display could replace both the function and area previously taken up by annunciators in the control room, with multiple GEPs used to protect against a single failure incident. (It is interesting to note that the designers of this device expect it to be used in control panels at power plants and chemical plants.) While the current GEP displays lack both color and the resolution possible with CRTs, they are completely flicker free, since they do not use a scanning electron beam. Color GEP displays have been developed in the laboratory in the past using a technique similar to that used in color CRTs. A different method of producing colors is to use a phosphor that produces different colors as a function of the exciting current.[42] This approach only produces a limited number of colors, but human factors research has shown

---

38 C.N. King, et. al. "Development of a 256 x 512 Electroluminescent (EL) Display Monitor,"Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 76.

39 C. E. Mellor, et. al. "Fabrication of Electrode Structures On Very Large Electroluminescent Displays,""Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 66.

* Lucitron Inc., 1918 Raymond Drive, Northbrook, Illinois 60062

41 M. Dejule, A. Sobel, J. Markin, "A New Gas-Electron-Phosphor (GEP) Flat Panel Display - The Flatscreen panel, " Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 39.

42 M. Dejule, et. al. "Construction of the Flatscreen Gas-Electron-Phosphor (GEP) Display" Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 50.

that one should limit the number of colors when unambiguous discrimination is required.[43] Additionally, this approach to color does not degrade the resolution of the display. The GEP display is rugged and offers superior resistance to shock and vibration, and its small volume to display area ratio would cause the debris from an implosion to be less than a CRT's.[44]

A more futuristic display device which presents true three dimensional images has been developed by Gensico Computers Group. The SpaceGraph Terminal projects images from an electrostatic vector CRT (resolution of 4096 x 4096) located above the operator's head onto a flexible, variable focal length mirror. The "optical depth axis is created by slight changes in the curvature of the mirror, resulting in relatively large changes in its focal length and image area depth viewed by the user."[45] The operator sees different perspectives by moving his head in relation to the image. Three dimensional displays are being used in Great Britain to aid in refueling the Advanced Gas Reactors (AGR). The robots inside the AGR core are controlled using holographic projections.[46] This technology may find similar applications in multi-module nuclear power plants.

---

43 H. H. Miller-Jacobs "Color Displays and the Color Deficient Operator" Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 15.

44 Ibid 39, Page 47

45 , "Peripherals: Graphics and imaging system presents true 3-D display," Computer Designs, Vol 24, No. 4, (April 1985) Page 96.

46 E.W. Carpenter, "Carbon Dioxide Cooled Reactor Experience", paper presented at the 7th International Conference on the HTGR, Dortmund, Federal Republic of Germany. September 1985.

3.3 Human Factors Considerations

The most difficult and error prone task for a computer user to face is that of pressing the right button to accomplish a specific command. This task is compounded if the same action in two different applications, on the same computer, requires a different command. This is a common situation on microcomputers where different companies market software for the same machine. For instance, a database management program may use the control-q command for quit, while a word processing program may use control-e (end), and control-q may erase the file being processed. The problem is reduced by making use of the same command set for all applications as much as possible. Similarly, the digital control system interfaces at a power plant should share the same command set as much as possible, and avoid the use of different commands for accomplishing the same task. Likewise, any hardwired backup controls used should follow the digital control operating procedures as much as possible. This suggests that some mandatory standards are or will be required.

In order for the operator to properly control the power plant, he must first understand the state of the plant displayed on a CRT. CRTs have already been used for information display in nuclear power plant control rooms, and human factors engineers have extensively studied presentation methods for CRT displays. A paper by M. M. Danchak summarizes applicable human factor considerations for CRT displays in nuclear power plant control rooms.[47] These are: Format of information displayed, color, and density of information.

Color graphic CRTs can display alphanumerics, shapes (icons) and colors. Each of these formats is best suited to different tasks that an operator

[47] M. M. Danchak, "Effective CRT Display Creation for Power Plant Applications," Power Instrumentation Symposium, San Francisco, CA. May 1976.

must perform when he looks at the CRT. The operator must first search the screen. Next he must identify what he has located. Finally the operator must perform one of three tasks. He may have to compare the information presented (are all module's core powers equal?). Or, he may have to verify that a state has been reached (the isolation valve has opened). Or, he my have to count (how many valves are open?). Using text and shapes aids the search and identification tasks, with color and blinking serving in a redundant fashion. Numerics are required for comparing and counting, however it is feasible to use graphical methods such as bar charts for these tasks. For example a horizontal bar could be used to indicate primary coolant temperature with green, yellow, and magenta (see Table 3.1) regions marked, and with the numeric value listed below the bar in cyan.

The recommended maximum number of colors appearing on the screen at any one time is eight (more gets confusing, less is better). The colors and their uses are listed in Table 3.1. The specific colors for each task are open to a certain amount of interpretation, and those listed in Table 3.1 are from a report by Leonard C. Pugh.[48]

[48] L.C. Pugh, "Plant Operations and the Man-Machine Interface," General Electric, October 1981.

Table 3.1
Recommended Color Codes[49]

Color	Use
Black	Display background.
Green	Lines or symbols that are static such as pumps, motors, valves, and piping.
Cyan	A supporting color for alphanumeric identification, scales and borders.
Yellow	For all dynamic process variables such as bar graphs and digital data.
Red	Abnormal conditions.
White	Process limits or reference marks for bar graphs and scales. Also for low confidence data.
Magenta	Danger, immediate attention required.
Dark Blue	Not to be used due to low intensity.

The recommended density of information on the CRT display is summarized in Table 3.2. The amount of information that can be displayed on a screen without confusing the operator has been shown to be on the order of 25% of total display area.[50] The values cited for word and symbol size are a function of the amount of text the mind can process in a glance. The mind only sees information within a 5-degree solid cone with 50 percent accuracy when one stares at a point. This translates into 12 characters at a glance. If only four characters are used in a word (or number) the accuracy of the operator's glance rises to 90 percent. Thus alphanumeric information should be limited to 12 characters, and the fewer the better. Of course, this must be applied logically; Power is more intelligible than PWR.

---

[49] Ibid 48, Page 19

[50] Ibid 47, Page 4

Table 3.2
Recommended Values for Information Density[51]

Total display loading, maximum	25%
Dynamic display loading, maximum	8.75%
Text word size, maximum	12 characters
recommended	6 characters or less
Numeric word size, maximum	12 characters
recommended	4 characters or less
Symbol size, maximum	2 inches
recommended	1 inch
Word orientation	Horizontal
Word Spacing	2 inches
Preferred quadrant	upper right
(in order of preference)	upper left, lower left, lower right

Other human factors features beyond simple display considerations can be gained from experiences with digital computer systems currently in use at U.S. nuclear power plants. The Millstone Unit 1 plant, a General Electric BWR, recently installed a new ModComp process computer. When the computer engineers were confronted with the problem of how many significant digits to display for the recirculation pump speed, they decided to display as many digits as were supplied by the instrumentation. This proved to be a source of confusion to the operators, because the last three digits constantly fluctuated up and down. These last few decimal places were actually insignificant, but it resulted in the operators distrusting what they saw and ultimately ignoring the data, for they did not know if there was something wrong with the computer, the sensor, or the pump. If the computer engineers had been more familiar with plant operations and human factors considerations this situation could have been avoided.

---

[51] Ibid 47, Page 5

Human factors engineering is a crucial aspect of any control system design, and it is beyond the scope of this research to fully describe all relevant human factors considerations. The ideas presented here are given to address several of the key issues in order to highlight the importance of this area.

3.4 Chapter Summary

The advances made in computer networking, fault tolerant processing, information displays, and human factors engineering have brought digital plant control technology to the point where it can be successfully applied to nuclear power plant control, especially multi-module control. Fiber optics are particularly well suited to nuclear applications due to their immunity to electromagnetic interference and inherently high data transfer rates. Fault tolerant computing has made substantial progress since 1980, and the 'pair and spare' technique has the basic simplicity and elegance necessary for highly reliable and available computing systems. Finally, the new flat panel displays, combined with human factors design, promises to produce a more reliable and efficient means of presenting information to the plant operator.

Chapter 4

Conceptual Features of a Multi-Module Control System

4.1 Introduction

The advanced computer technologies, described in Chapter 3, when combined with the process control techologies, described in Chapter 2, can produce a control system for a multi-module plant that is reliable, flexible, automated, and easier to use than existing nuclear power plant control systems.

The characteristics of inherently safe reactors make it possible to delegate many of the usual control tasks to a digital computer. In addition, the complexity of the control system is reduced (as compared to present LWRs) since many, or all, of the active safety systems are not present in inherently safe reactors with passive emergency decay heat removal systems.

A suggested control system for a multi-module nuclear power plant is described in the following sections in order to illustrate how the latest technologies could be used. The control system described is only for illustrative purposes, and any specific design criteria such as the degree of redundancy, networking scheme, networking medium, etc. will have to be decided upon only after all qualities of the various alternatives have been researched.

4.2.1 LMR System Characteristics - PRISM & SAFR

The demise of the Clinch River Breeder Reactor program and a concurrent interest in small inherently safe reactors have led to a re-evaluation of the United States' breeder reactor program goals. Designs such as the Power Reactor - Inherently Safe Module (PRISM), and the Sodium Advanced Fast Reactor (SAFR) have been proposed in response to the perception that significant cost and risk reduction can be achieved by greater reliance on passive safety features.[52]

PRISM:

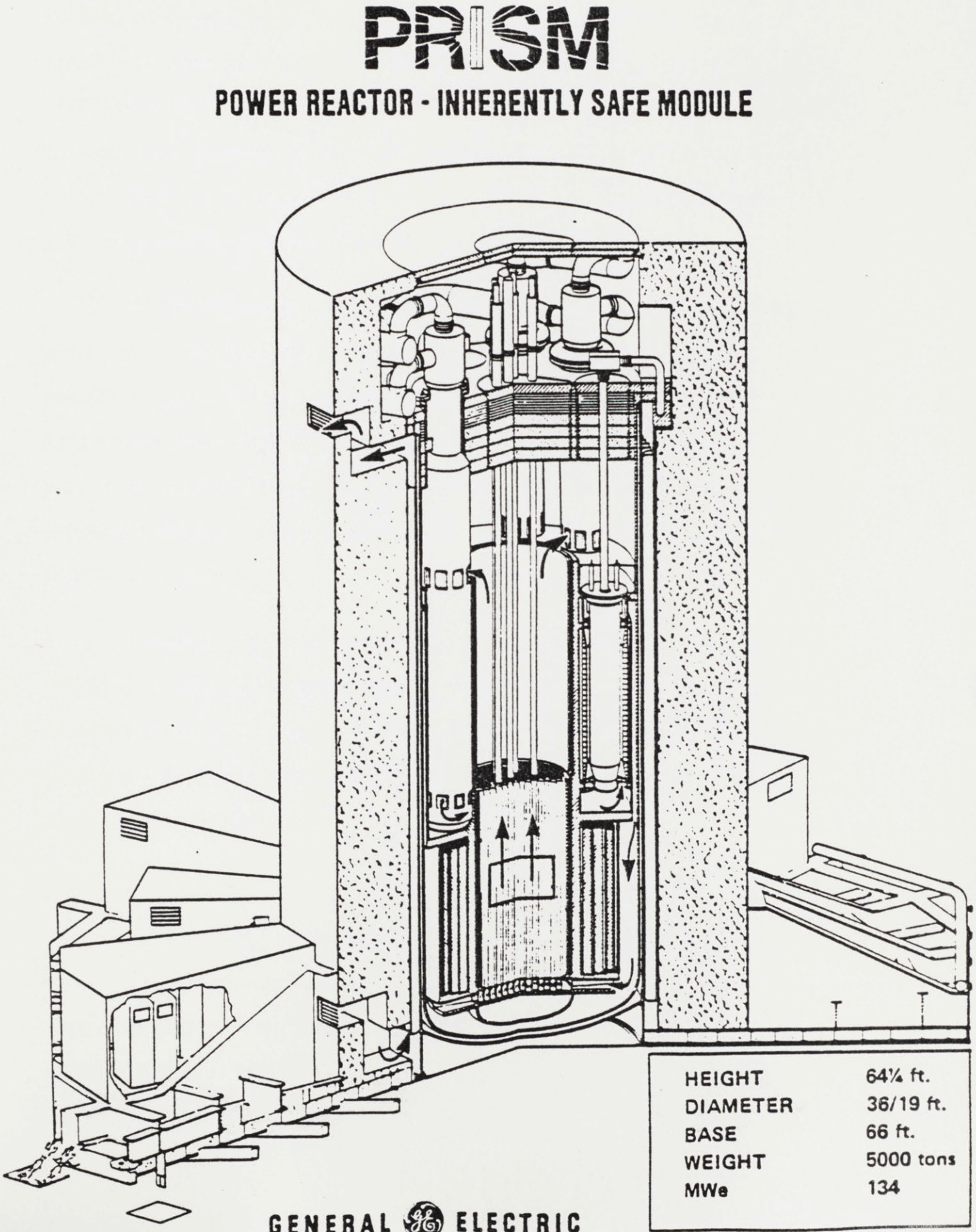
PRISM (see Figure 4.1 for a diagram of PRISM), proposed by General Electric Corporation, is a 134 MWe sodium cooled fast reactor in a 'pool' configuration. The neutronics and thermalhydraulics of the primary system are such that the reactor will shut itself down under required Anticipated Transient Without Scram (ATWS) scenarios. The large thermal mass of the pool, combined with the large surface area of the reactor vessel and the low specific power of the core allow the decay heat to be removed by purely passive means. The Radiant Vessel Auxiliary Cooling System (RVACS) constantly cools the reactor vessel via natural draft atmospheric cooling. The atmospheric inlets for RVACS do not have dampers, thus they can not be inadvertently closed. RVACS accounts for a 0.2 percent power loss during normal operations, and during severe loss of normal heat sink events, it removes enough decay heat to keep the sodium temperature below 1100°F at all times.

The PRISM modules are grouped so that they share major balance of plant (BOP) components, and thus capture the economies of scale of a larger

---

52 A. Cruickshank,"Advancing breeder reactor design in the United States", Nuclear Engineering International, February, 1985. Vol. 30, No. 365. Pg. 17

Figure 4.1


PRISM
POWER REACTOR - INHERENTLY SAFE MODULE
HEIGHT 64¼ ft.
DIAMETER 36/19 ft.
BASE 66 ft.
WEIGHT 5000 tons
MWe 134
GENERAL ELECTRIC

plant, without incurring the penalities associated with a larger core, such as the need for active emergency core cooling systems. A PRISM 'segment' consists of three modules feeding a single turbine-generator. A 1205 MWe plant consists of three segments (nine modules). Each segment will be a complete and independent power plant. Since the modules share major BOP equipment, a central control system is needed. Whether each segment will have its own independent control system will have to be decided. The characteristics of a possible control system are described in the following sections.

The PRISM module, like all modular designs, is sized so that nuclear safety related components can be factory fabricated, where quality can be controlled more readily than in the field. After the major components are made, they are transported to the site for rapid installation. This manufacture and construction method is expected to reduce the licensing effort, since the module will be pre-licensed and only site specific issues will be considered in the final licensing procedures.

The small size of a PRISM module enables it to safely ride out a loss of intermediate coolant flow event without active decay heat removal systems or active safety systems of any kind. It thus has the potential to make the overall plant more reliable and less demanding of the control system than a large, single reactor, plant.

SAFR:

SAFR, proposed by Rockwell International, is a 330 MWe modular design for a sodium cooled fast reactor. SAFR would need four, rather than nine modules for a plant electrical output on the order of 1200 MWe. Each SAFR module will have its own major BOP components, and will share only

auxiliary systems. This design, like all modular designs, reduces construction costs by adopting a compact layout for the nuclear island. The passive safety features of this design ensure that the BOP can not be an accident initiator, and thus the BOP can be built to conventional fossil-fired power plant standards.

Key safety characteristics of the system are listed in Table 4.1, and the shutdown heat removal systems are shown in Figure 4.2. The reactor is also pool-type with the inducer pumps and the intermediate heat exchanger immersed in the primary vessel's sodium. The natural draft heat exchanger, part of the DRACS (Direct Reactor Auxiliary Cooling System), is normally used for decay heat removal when the intermediate heat exchanger and steam generator loops are incapable of this task. The RACS (Reactor Auxiliary Cooling System) is always on line and fully assumes the task of decay heat removal if the natural draft heat exchanger is inoperable. These passive systems do not, by nature, require any active control signals, and thus they reduce the complexity of the control system.

Table 4.1

Safety Characteristics of SAFR

Reactor Shutdown:

- Redundant/diverse control rod systems, self actuating secondary system.
- Inherent thermal and nuclear feedback shuts down the unit after loss of flow without scram.

Decay Heat Removal:

- Natural air convection cooling of vessel (RACS).
- Na - Na - Air natural convection Direct Reactor Auxiliary Cooling System (DRACS).

Structural Cooling:

- Natural air convection cooling of deck and cavity.

Structural Integrity:

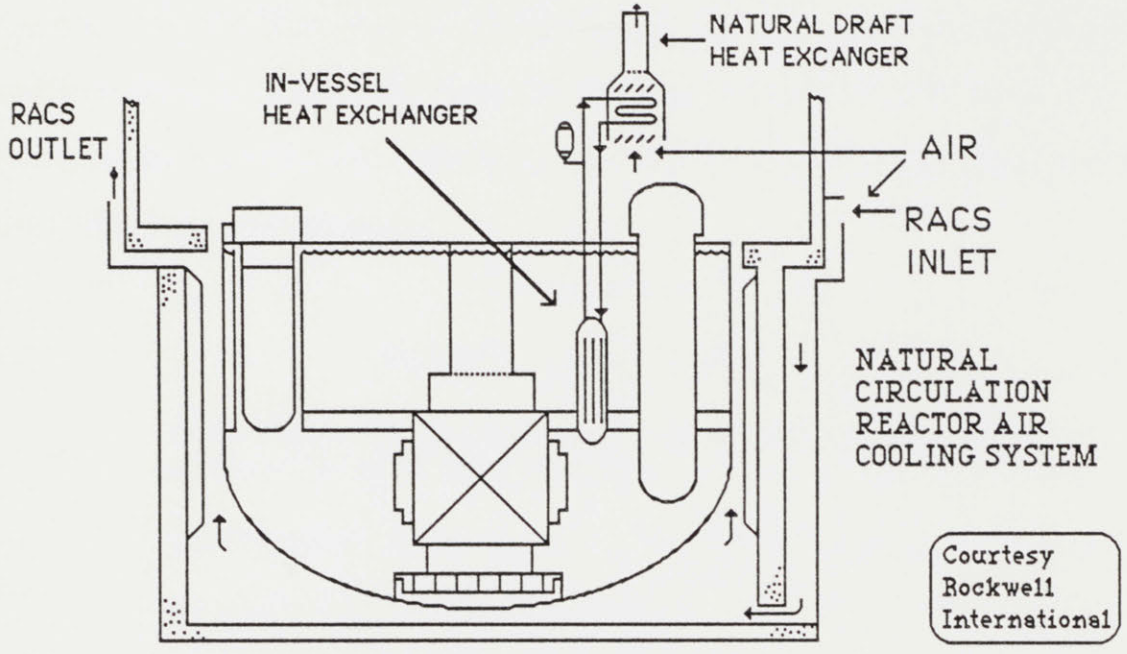
- Redundant beam deck structure, redundant monitorable core support system.

General:

- Low core energetics.
- Long grace period (>24 hr) for operator action.

Figure 4.2
SAFR Shutdown Heat Removal Systems

Natural Circulation Direct Reactor
Auxiliary Cooling System (DRACS)



The high capital and operating cost of a control room dictate that one control room be used for multiple modules in a multi-module plant. The SAFR design has one control board and control system for each module, with all four control boards within one control room. Since each module has its own turbine generator, there is not a high demand for a fully integrated centralized control system for the entire plant.

4.2.2 MHTGR System Characteristics

The Modular High Temperature Gas-Cooled Reactor (MHTGR) proposed by GA Technologies,[53] is a passively safe reactor with design goals as listed in Table 4.2. The MHTGR also has an experience base comparable to LMR experience to draw upon. The system described in reference 1 is based on technology derived from the operating HTGRs in both the United States and the Federal Republic of Germany.

Table 4.2

MHTGR Design Goals

- Essentially zero risk to the health and safety of the public - no public evacuation planning zone.
- Standardized plant from both design and licensing standpoints.
- Minimum financial risk to the utility.
- Assurance and protection of owners' investment by returning the plant to service shortly after a loss of coolant accident.[54]

The low risk to health goal is assured by relying on natural laws to remove the decay heat from the reactor, and thus keep the maximum core temperatures below the value that would cause the fuel pellets to fail. This capability reduces both the number of safety systems, and their complexity. Also, this can potentially aid in the licensing process, and help combat the 'diseconomies' of small scale.

The standardized design goal has numerous benificial effects. It allows the reactor to be licensed once, thus reducing the time it takes to order a plant and put it into operation. It also allows common procedures to be used within

---

53 C.F. McDonald, A.J. Goodjohn, F.A. Silady, "Small, Passively Safe, Modular Gas-Cooled Nuclear Power Plant with Pebble Bed Reactor", paper presented at the Joint Power Generation Conference, Toronto, Canada. October, 1984

54 Ibid 53, page 1.

the industry, such as operator training, maintenance, and component replacement. This will cause the industry to move up the learning curve, increasing the availability of the plant and lowering power generation costs.

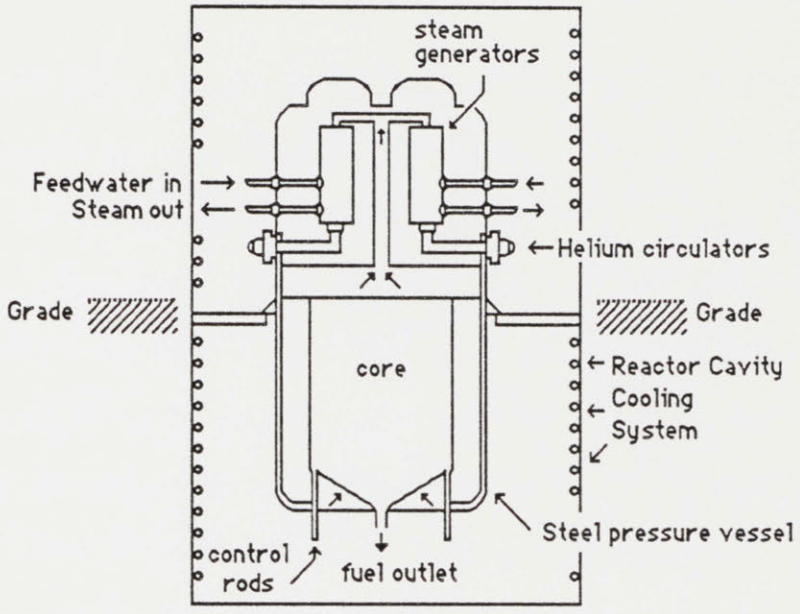
Finally, the owners' investment assurance goal is met by limiting the core power density and core total power. This is done so that even in the event of total loss of all active decay heat removal schemes, the maximum temperatures reached in both the fuel and system components are low enough to permit replacement and repair of damaged components and return the plant to service within a short time.

The specific design of the MHTGR is not finalized. The design described in reference 1 is a pebble bed reactor with four in-line steam generators located above the core (see Figure 4.3). It is a 250 MW(th) reactor (95 MWe). This low power limits fuel temperatures during the maximum credible accident so that no appreciable amounts of fission products are released. It also limits the pressure vessel diameter so that steel vessel technology from Light Water Reactor plants can be used, and so that the vessel may be transported easily by rail. Finally it allows reflector control.[55] This size limit, induced by passive safety considerations, inevitably leads to a multi-module reactor power plant design.

---

[55] Ibid 53, page 2.

Figure 4.3
MHTGR Primary System
Pebble Bed Core



The decay heat from the core is normally removed via the steam generators when the system is pressurized. It is not necessary for the helium circulators to be operable since natural convection will occur in this configuration. If the system is depressurized the Reactor Cavity Cooling System (RCCS) is used. The RCCS lines the confinement structure and is composed of water-bearing coils that remove the heat from the confinement building. There is a sixteen day inventory of water in this system, and no action is required to initiate or maintain operation. This scenario is termed the 'conduction cooldown accident.' In this mode, the decay heat is conducted radially outward from the core to the steel reactor vessel. The heat than radiates from the vessel to the concrete confinement walls, and is then removed from the reactor cavity via the RCCS. In the event that the RCCS is inoperable, the earth becomes the heat sink, and the maximum temperatures reached by the reactor vessel and the concrete confinement are higher. The fuel, vessel, and confinement structure

all maintain their structural integrity, but the vessel and confinement structure might have to be replaced before the system is returned to service. Since no fission products would be released this accident would not endanger the public.

This 250 MWth pebble-bed reactor is not currently the lead design in the U.S. Department of Energy (DOE) MHTGR program,[56] although pebble bed reactors are currently operational in the Federal Republic of Germany. The DOE lead design (November, 1985) is a 350 MWth annular core prismatic fueled MHTGR.[57] The power of the core was increased to 350 MW in an effort to try to capture some economies of scale. The core would be constructed in an annular fashion, with a central region of graphite. This keeps the peak temperatures in the core to the same levels as the 250 MW core in the conduction cool-down mode. However, the steel vessel and the reactor cavity walls would reach a higher temperature than previously (even though the vessel diameter is somewhat larger). If the RCCS were inoperable during a conduction cool-down event, the fuel would still not fail, however the vessel and concrete would be subjected to temperatures that may require substantial repairs before operation of the module can continue.

In addition to the higher power, the steam generator is no longer above the core. It is below and to the side of the core (a 'side-by-side' configuration - see Figure 4.4). In this configuration, natural circulation would not be possible for removal of decay heat, so a shutdown heat exchanger with its own helium circulator has been added below the core. This heat exchanger serves no safety functions, since the conduction cool-down mode removes the decay heat without danger to the public. However, the conduction cool-down mode is not

---

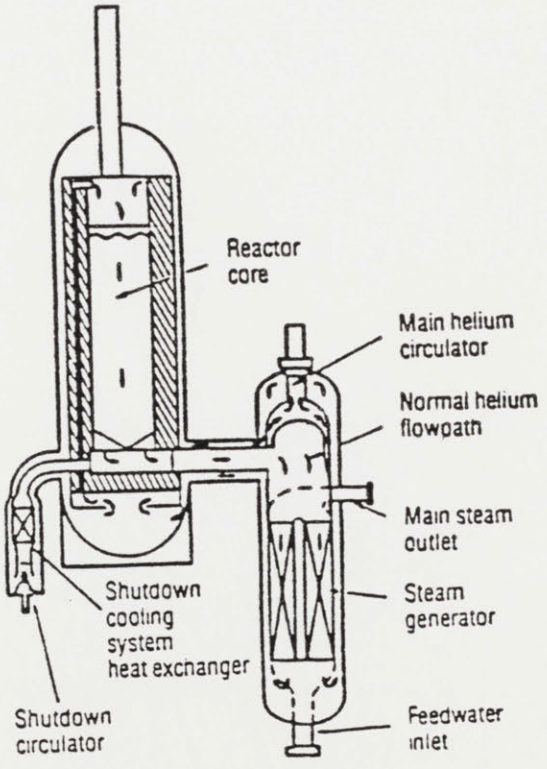
56 L.D. Mears, M.L. Brown, "America considers the modular HTGR", Nuclear Engineering International, October, 1985. Vol. 30, No. 373.

57 A.J. Goodjohn, GA Technologies, personal communication, November 1985.

beneficial to the reliability of the module components, so the shutdown heat exchanger has been added to reduce the liklihood of a conduction cool-down mode occuring.

The MHTGR, like the LMR designs, is a power system that can easily be built and controlled with minimal risk to both the owner and the public. The MHTGR is a small reactor, approximately the same size as PRISM, and hence its economic viability will depend on the ability to control several modules from one control room. In addition, the large thermal capacity of the graphite in the MHTGR produces slow response times analogous to the small LMR with its large thermal capacity of sodium. These long response times reduce the demand on an automatic control system.

Figure 4.4
MHTGR 'Side by Side Configuration'



4.2.3 Space Nuclear Power Systems

Another nuclear power technology development program is currently underway that has design contraints for its control system that are in several key respects similar to those of modular nuclear power plants. The program, known as SP-100, is a tri-agency (NASA, DOE, DOD) project for the development of space nuclear power systems.

The SP-100 program was started in 1983 with the objective of developing a small reactor and conversion system to provide 100 KWe for a variety of space missions.[58] The current primary candidate system is a liquid metal (lithium) cooled fast reactor with thermoelectric converters (see Figure 4.4). The thermoelectric converters are outside of the core and are heated by heat pipes, which in turn are heated by the lithium coolant. The thermoelectric converters are mounted inside the radiator panels. The radiator panels reject the waste heat of the cycle, and contain heat pipes to distribute the heat along their length. This design is for the initial, 100 KWe, power plant. Higher powers would be obtained by using the same basic design for the core, shield, and radiator, but the conversion system may be replaced by higher efficiency active cycles such as Brayton and Stirling.

A space nuclear power system will be unmanned and thus an automated control system is desirable. In particular, the reliability of communication systems between the spacecraft and the ground is low enough to warrant onboard control systems. In addition, military satellites may operate in regions of space, or under scenarios where communication with the ground is

---

58 A.D. Schnyer, et. al. "SP-100 Program Developments," Society of Automotive Engineers, IECEC Proceedings, 1985. Page 1.17

impossible. For these reasons, an onboard fully automated control system is needed.

One design constraint proposed for the control system is that it operate autonomously (without human or ground intervention) for up to thirty days. In addition to this it must control a system that has an operational life of seven years and a total orbital life of ten years.[59] These design contraints have led to specifications for the control system that are almost identical to those for the multi-module nuclear power plant. The specifications that are common to both control system designs are:

- The system control processor must be fault-tolerant to a certain degree.
- Hardware redundancies and reconfiguration control must be provided, especially in sensing, data acquisition, and signal conditioning.
- The processor must also have the capability to provide state-of-health monitoring on board, incorporate self-test features, and provide electrical load sequence and control.[60]

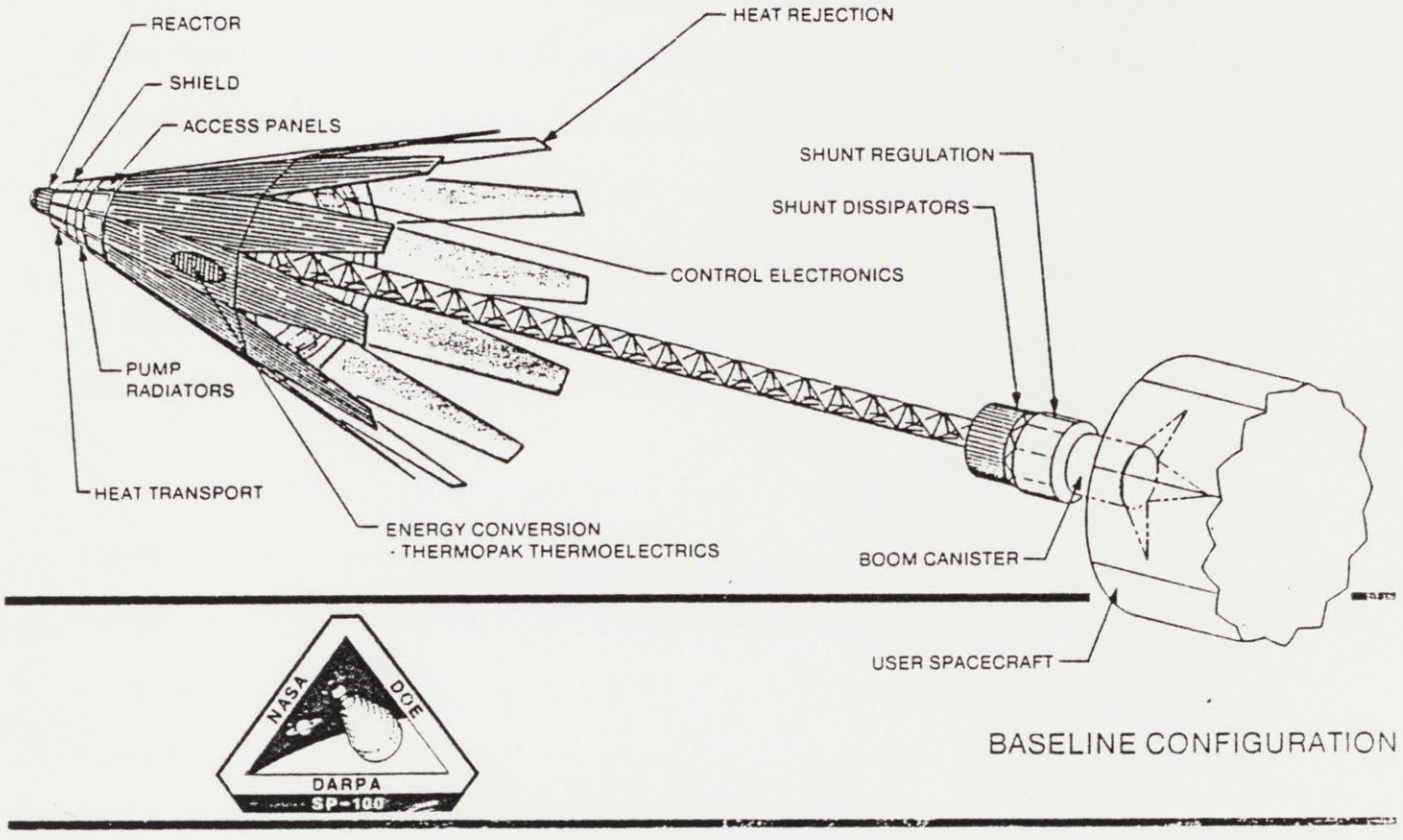
These considerations are generic in nature, and advances in these technologies will benefit both the SP-100 program and the multi-module nuclear power plant programs.

---

59 M.S. Imamura and J.H. Masson, "Autonomous Control Design Considerations for Space Nuclear Power Systems," Space Nuclear Power Systems, Orbit Book Company, Inc. Malabar, Fl. 1985. Page 115.

60 Ibid 59, Page 121

Figure 4.5
Proposed SP-100 Configuration (courtesy G.E.)



4.3 Relation of Passive Safety Features to Control

The passively safe reactor, such as PRISM (or an MHTGR), has inherent characteristics that lower the demand on the control system. The reactor's low power, combined with the metal clad fuel and sodium coolant, enables the decay heat power to be totally transferred out of the core by passive means. This reduces the complexity of the safety related control systems since it is not required to take an active course in the event of a scram or loss of flow incident. In addition, the number of active auxiliary cooling systems is drastically reduced as compared to a light water reactor, and thus the number of control parameters and signals is similarly reduced.

The inherent, passive safety features of the reactor may allow the control system to be totally outside of the safety related category if it is proven that the control system is not needed for the safe shutdown of a plant (discussed further in section 4.4.7). Furthermore, it will have to be proven that the control system could not be an accident initiator for the non-safety related classification to apply. If the control system is deemed non-safety related, the designer of the control system will have greater latitude. Also, the system will not be subject to safety grade codes and standards, which may be difficult to meet for a complex digital computer, and it may only be subject to tests deemed necessary by the utility for the economic operation of the plant.

A possible configuration of a computer based control system, described in the next section, assumes that the control system will not be safety related, and that it will be required to control most plant functions.

4.4.1 Architecture of Control System

The control system, outlined in this review for discussion purposes, is distributed but also has a centralized control function for overall plant coordination (see Fig. 4.6). The main computer receives information from the local module computers and displays this to the operators. The module computers respond to high level commands from the main computer, such as adjusting reactor power to a specific level. Each module has its associated simple sensors and intelligent subsystems such as flux mapping (see Fig. 4.7). These subsystems and sensors transmit their data to the module computer. The module computer performs the sensor validation routines, employing analytic techniques for added redundancy where appropriate. The status of the module is thus determined and this information is transmitted to the main computer.

Figure 4.6
Top Level Architecture of Control System

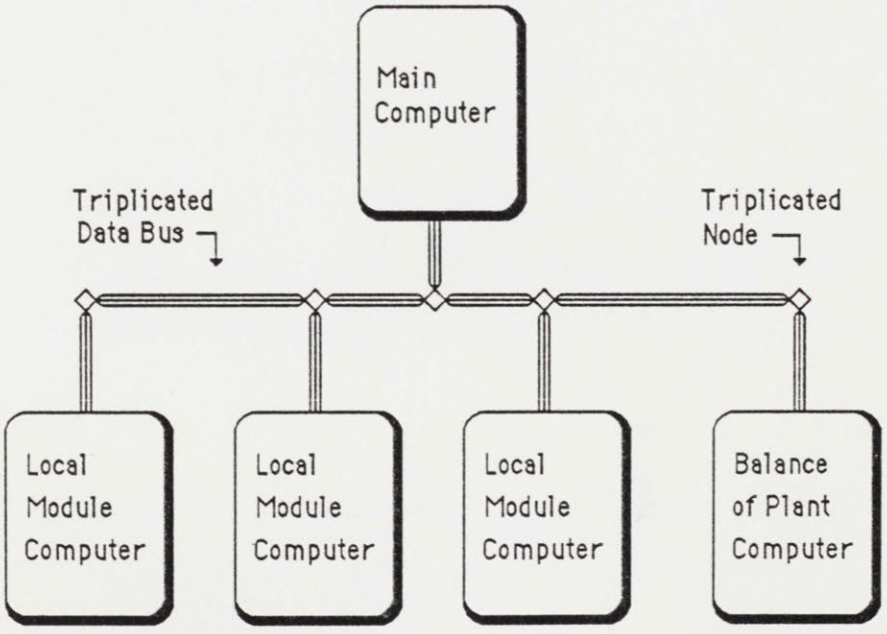
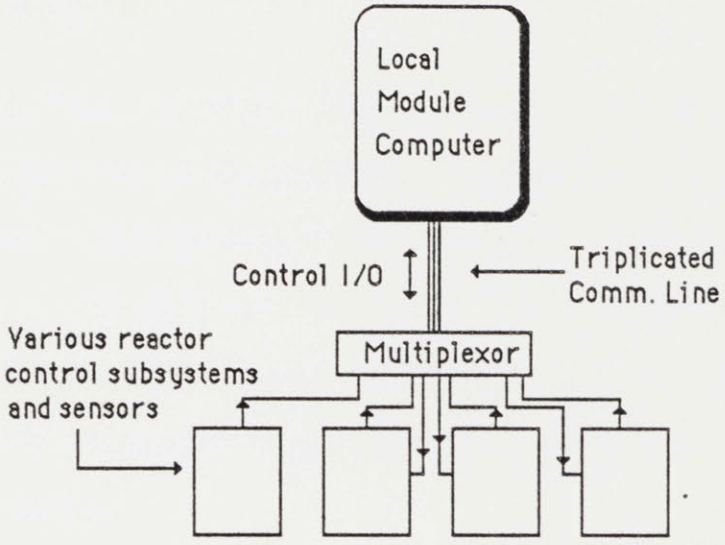


Figure 4.7
Module Level Architecture of Control System



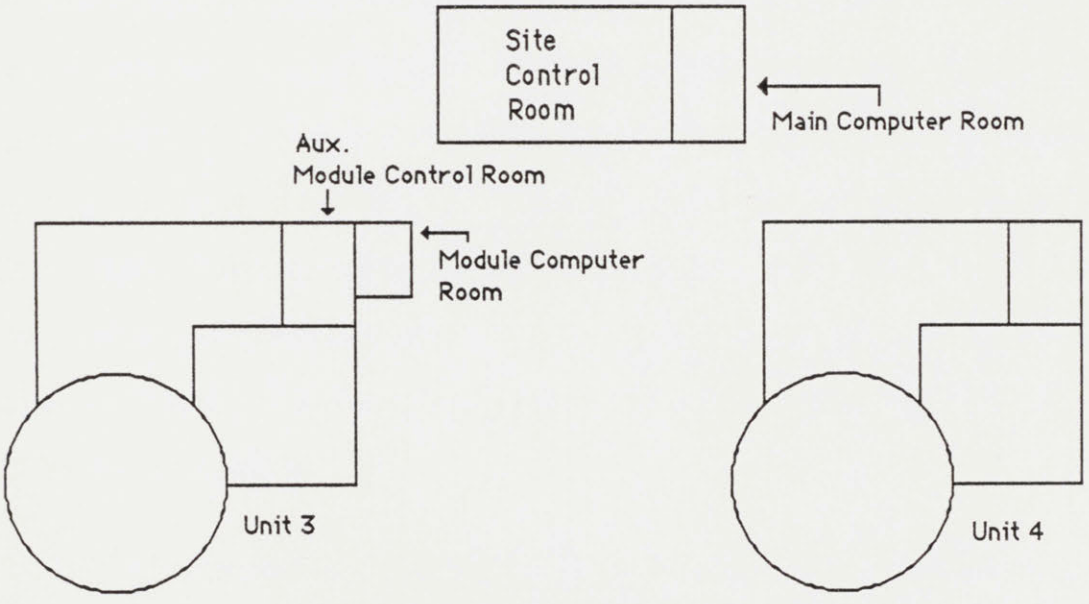
The operators control the plant through the main computer, and are able to focus in on any module from the control room. In the event of an extended abnormal condition in one of the modules, one of the operators can concentrate on the module via a dedicated console, while the plant computer runs the rest of the plant (with an operator monitoring the computer's actions). The shift supervisor has a console in his office with which he can monitor the plant. The number of additional reactor operators necessary to monitor the other units will depend on the level of automation, which is presently undetermined. The goal of General Electric's PRISM design is to minimize the number of operators necessary.

The distributed nature of the control system not only increases the reliability of the system, but also enables the control system to grow as modules are added to the site. Assigning a computer to each module protects the control system from faults in other modules. In addition, the module computer is located in a computer room at the module with an auxiliary control room and

console for use in the event that the communications link between the main computer and the module computer is broken (see Fig. 4.8 for computer room / control room locations).

In designing a computer control system for a multi-module nuclear power plant one is able to take advantage of the modular nature of the plant by designing a control system that is distributed and centralized, containing the best features of both. Consequently, the number of operators required is reduced, since normal operations of the plant are automated, and operators are only required for supervision of the computer and for control in the event of abnormal conditions.

Figure 4.8
Location of Main and Module Computers



4.4.2 Start Up / Steady State / Transient Conditions

The Japanese have developed and applied computers to start up boiling water reactors; thus the concept has been demonstrated in principle. Although their system did not move control rods, it regulated the core recirculation rate, which is a normal mode of plant control in BWR's. The Canadians have extensively automated their CANDU units; thus digital control without full hardwired backup control has been demonstrated. Additionally, MIT has demonstrated the use of a digital computer for transient control of the MIT reactor, hence in some respects a regulatory precedent has already been established in the United States.

A possible method of starting up a modular plant is similar to that for a multi engine aircraft: each reactor willl be started one at a time. The main computer instructs the local module computer to start up the unit. When this module is feeding its steam to the turbine, the other modules are sequentially brought up. In order to increase the plant capacity factor, a quicker method might be used, where a module begins its ascension to full power before the previous unit has reached full power. It may even be possible to start all of the modules in parallel to start the plant even more quickly than a single large plant could be brought online.

Steady state operations pose no difficulties, and one advantage of digital control may be realized here. Since the control of the plant is already remote in one sense, it may be feasible to allow the electrical grid dispatcher to adjust the plant power within limits. The dispatcher would send a command to the main computer to raise or lower power a given amount. The main computer would

tell the dispatcher how much capacity he can adjust based on the number of modules that are running and under computer control.

Finally, certain transients such as those caused by the tripping of another module, could be quickly and accurately controlled by the computer. This type of automatic control allows the operators to focus their attention on the tripped unit, while the computer adjusts the rest of the plant.

4.4.3 Accident and Post-Accident State Monitoring

Multi-modular control when all units are operating as designed may well be the least troublesome situation, since severe transients resulting in plant damage pose several difficult questions:

- The Three Mile Island Unit 1 and 2 precedent may preclude operation of undamaged units on the same site for consequences beyond some (ill-defined) threshold, regardless of the technical merit of the justification for continued operation.

- Non-routine repair on a damaged unit may raise questions as to the propriety of continued operation of the others because of the added labor force on site (security issues), and because of operations which might prove to be accident initiators. As a result of this consideration, there must be a capability to lock out the control of the affected unit from the remaining units.

- Discovery of a flaw in one unit would require the inspection and/or repair of all units (a problem for all standardized designs, large or small). If all flaws must be corrected before resumption of operation, the problem is more severe than if there is only one unit per site and a staggered repair schedule is adopted.

- Although the accident risk is reduced by passively safe module design, the investor's risk is not obviously reduced unless the availability of the multi-module equipment and control is shown to be very high.

The remote monitoring of key safety parameters is required by the NRC, and this capability could be enhanced by a digital control system. Additionally, it may be possible to transmit these safety parameters to NRC headquarters in real time. This may make a digital control system attractive to the NRC.

4.4.4 Level of Redundancy

The are two types of redundancy that need definition. These are the redundancy of the computers and the redundancy of the sensors and the communication network.

Redundancy that tolerates computer hardware faults can be implemented either through a hardware or a software approach or a combination of the two. The method that least affects the development of application software is best for complex systems since the programming of such systems is difficult even for machines with no fault tolerance. Additionally, the installation and testing of such complex systems is error prone, and being able to rule out the hardware as a source of errors is helpful.

All fault tolerant computers on the market in August, 1984 used some type of software method for detecting hardware faults except for one:[61] Stratus Computer uses the pair and spare technique described in section 3.2.2 to achieve a very high availability. (Stratus' method is discussed for illustrative purposes only)

The pair and spare method does not impact the programming method used on the system, nor does it allow any single hardware fault to corrupt the data being processed. This system will allow the plant operator (or possibly the Instrumentation & Control group) to be notified in the event of a hardware fault. The system announces which circuit board has failed, and its performance is not degraded while the faulty board is being replaced. The fact that the system need not be shut down while the board is removed and replaced increases the computer system's availability. The pair and spare technique is essentially a

---

[61] Ibid 36, Page 29.

quadruply redundant system, which should be sufficient, since the BWR plant digital feedwater controller developed by Toshiba (Japan) is a triply redundant package.

The Japanese design of the feedwater controller includes a 16 bit microprocessor, and fiber optic multiplexing for communication. The primary control loop has triplicated sensor channels and triplicated microprocessors. Triplicated units are used since this is the primary controller, while duplicated units are used in the secondary controller. Markov analysis has shown that the mean time between failures (MTBF) for the feedwater controller is $1X10^6$ hours.[62]

The communication network, medium and nodes, for the control system described, might be triply redundant for added reliability. It would be modeled after the AIPS (Advanced Information Processing System, a Charles Stark Draper Laboratories design), and the medium would preferably be fiber optic. Fiber optics have superior resistance to EMI (Electro Magnetic Interference), low bulk, and high data transmission capabilities.

Such a control system would have an extremely high availability because of quadruple redundancy in the computers, and triplex redundancy in the communication network. This high availability should be advantageous to the plant capacity factor.

The control system design could also draw upon fault tolerant control system work that has been done at the Massachusetts Institute of Technology.

---

[62] Seishiro Kawakami, et. al. "Reliability of BWR Plant Digital Control", Toshiba Corporation, Japan. March, 1985.

This work has demonstrated that a hardware fault tolerant digital computer with sensor fault tolerance can acitvely control a nuclear reactor.[63]

[63] A. Ray, J. Bernard, D.D. Lanning, "On-line Signal Validation and Feedback Control in a Nuclear Reactor," Power Plant Dynamics Conference. 1983

4.4.5 Degraded-State Control

The plant computer, by its pair and spare redundancy, would degrade without loss in performance if a single circuit board fails in a pair. That is one of each pair, the CPU, memory, disk controller, and I/O (input/output) boards may fail. However, if one of the remaining boards fails while its companion is being replaced, then the computer will fail completely. Since this event should be extremely rare, possibly occurring only once in the lifetime of the plant, it is reasonable to not design for this event, and scram the module affected.

If a reliability analysis shows that a double failure may occur more than once in the plant lifetime, then a third board for each subsystem (with two identical processors) may be added to the system to guard against this possibility.

Another issue affecting how the computer system might degrade is the software reliability. Complex codes such as those used for chemical process plant control are almost impossible to fully test, because the permutations of the plant state combined with the control software is almost infinite. New methods of generating software may help reduce the possibility of a software failure. For instance, PICON (described in section 2.3.1) is not programmed in the normal sense. The engineer describes the operating rules in a pseudo-english. This description is translated by another program into LISP, the programming language for PICON. This method may prove less error prone than conventional programming practices, and it is certainly less error prone to make revisions in the pseudo-english, since the operating rules are not buried in software. The software is also prone to errors originating in the storage medium. For instance, hard disks are susceptible to a variety of faults, and

certainly are not very shock resistant. Non-volatile memory systems might be used to replace the hard disk for critical software, while the hard disks are used for tasks such as data logging.

4.4.6 Degree of Automation and Hardwiring

The plant computer, in order to meet the requirements of reduced number of operators and minimum control room size, will have to control normal operations such as start up, steady state and transient operation, and shut down. Additionally, the plant computer will be required to respond appropriately to anticipated incidents such as loss of off-site power, loss of flow, loss of feedwater, etc. If anticipated events occur on a frequency less than a certain amount (needs to be defined), then the computer may not be designed to control these situations, and it may simply shut down the system or possibly reduce its power. Other functions which may be aided greatly are tasks such as refueling. The module computer could possibly be used to control the refueling machine (such as the In-Vessel Transfer Machine designed for the French Super Phénix).[64] The advantage of doing this is that the computer could precisely position the refueling machine over the fuel assembly, while keeping track of various fuel assembly parameters such as burn-up, decay heat power level at any time, and enrichment.

The degree of hardwiring desired is a difficult question. It will be hard for the operators and regulators to accept this new method of nuclear power plant control, because they both trust tried and true equipment, and would probably prefer to have complete hardwired backup control. However, this degree of hardwiring would unnecessarily complicate the construction and design of the control system, and allowing the operators hardwired control introduces another failure path in the control system. The Canadians, when they were first introducing digital control into their plants, used complete hardwired backup control and found it to be an unnecessary burden.

---

[64] A.E. Walter, A.B. Reynolds, Fast Breeder Reactors, Pergammon Press, New York, 1981. Page 485.

The degree of hardwiring is best kept at a minimum, and the degree of automation should be as high as possible, while meeting the regulation that the control and safety systems be independent. The operators should have, at least, a hardwired scram circuit for each unit. High automation is essential because of the need to reduce operating personnel for individual modules.

The passive safety features could allow for the possibility of no hard wired safety control system, or a minimal hard wired safety supervisory system set outside of the operating limits and below safety limits. All other control functions then need not be hardwired and could be digitally based. The minimal hardwired system would allow operators to verify that the system has reached a passive cooling state and would provide parameters such as control rod position and temperatures both in and outside the core. Additionally, for safety purposes, if this hardwired system is activated, the digital control system could not override it until certain safety conditions have been met. In summary, the passive safety features give potential benefits for justification of complete digital control systems.

4.4.7 Credit for Demonstrability

This is a key item: If one can demonstrate a "Total Loss of Instrumentation and Control Capability" without any safety limits being exceeded, then presumably one will be permitted greater latitude in control system design and operation.

Hence early attention to test program planning is needed. Since tests will undoubtedly be on a single module plant, potential multi-module interactions need to be identified and simulated. If any of these interactions would be purely a result of the control system, they could be simulated during the test by the computer controller.

One problem with this otherwise appealing approach is that it defers an important risk (of failure or an ambiguous result) until very late in the commercialization process, with attendant business risks. However, investor and public acceptance benefits may be very large if design goals are met or exceeded. Aggressive pursuit of this approach may be one of the more productive means of capitalizing on inherent safety features, whose economic benefits may otherwise not be fully realized (through shorter construction time, plant simplification, or higher capacity factor).

Multi-module effects are not seen to compromise the single unit results in any important way, but the stakes are so high that a definitive answer must be worked out in advance.

4.4.8 Nature and Degree of Unit Interconnections

The design of the interconnections between the modules will affect the control system, both in normal operation and in accident-state operation. Important questions are the number of reactor modules per turbine generator (T/G) unit, and whether there are cross connects, such as a common steam main. A common steam main would allow any reactor module to feed any T/G on site which may increase overall reliability: i.e. one could drop several reactors or one T/G off line and not have a total trip event. There may be both beneficial and detrimental aspects.

Another factor in the plant design is whether credit can be taken for one unit providing emergency power for others. If this is so and one unit is always running, then perhaps an onsite backup such as a diesel generator or gas turbine is unnecessary. The inherent safety features of the reactor in question may make this a more acceptable approach than at a multi-unit station of conventional LWRs (as is common practice in France and Japan, and in Canada with CANDU units)

Other generic questions are: How many units per control room? per control console? Can units be built and added while others in the same cluster are online? i.e. where is the connect/disconnect point which allows this - must a "signal main" be built into the original control room to permit this? It must be shown that connection is not a potential accident initiator or the connections must be done when all units are down (most likely a requirement!). For training and test purposes for the first plant, it may be desirable to have one real unit plus (N-1) simulated ones to simulate an N module plant, and thereby demonstrate all interaction effects.

4.5 Control System Design Standards

The IEEE and the NRC have issued various design criteria for control and safety systems in nuclear power plants. The applicable IEEE/NPEC standards for control systems in safety systems are listed in Table 4.3

Table 4.3
Applicable Standards for Control of Safety Systems

603/1977	"Criteria for Safety systems for nuclear power generating stations"
7.4.3.2/82	"Application criteria for programmable digital computer systems in safety systems of nuclear power generating stations"
730/1981	"IEEE standards for software quality assurance plans"
829/1983	"IEEE standards for software test documentation"
828/1983	"IEEE standard for software configuration management plans"[65]

In addition to these, the NRC sets both the general requirements for control and safety systems, as well as specific regulatory guides. The Code of Federal Regulations (CFR) Tile 10, Part 50 lists the general criteria for nuclear power plants. Criterion 24, "Separation of protection and control systems", states that any single failure of the control system, or any protection system component common to the control and safety systems, will not hinder the protection system in any of its requirements. Futhermore, interconnection of the protection and control systems will be limited so that the protection system is not impaired.[66] This criterion would be best met by complete independence of the control and safety features. In section 4.4.6 this separation is discussed in more detail.

---

[65] G. Chisolm, "FAFTRCS: Full-Authority Reactor Control System," Trans. Am. Nucl. Soc., Vol. 49, (June 1985) Page 376.

[66] , "General Design Criteria for Nuclear Power Plants," 10 CFR 50, Nuclear Regulatory Commission, (Dec. 1982).

4.6 Unresolved Issues Affecting Licensability

Control Systems:

If a digital control system is considered safety related, then quality assurance in the classical sense is impossible since one can not fully test a sophisticated piece of software.[67] The simplest solution to this is to assume that the safety features of the plant are not reliant on the control system. This removes the control system from safety assurance tests and the owner/operator of the plant would only put the control system through tests that ensure the economic operation of the plant. This seperation of active control systems from safety functions is possible because of the passive protection of the modules.

Modularity:

Current nuclear power plant safety systems are designed to limit the total exposure of the population to released radionuclides (source term) during the design basis accident. If future modular plants are required to meet these same goals (or other goals) will they be constrained by this regulation on a per unit basis or a per site basis? If the regulation is applied to each module, then the site will not be limited in the number of modules except by heat removal aspects, i.e. each module will be subject to a specific radionuclide release limit for the design basis accident. If the regulation is applied to the site, then the total source term from all units will have to be considered, and this may affect the design of mitigating systems on individual modules, i. e. the containment design may be more stringent for a module at a ten module site, than for a module at a four module site.[68]

---

[67] Bruce Bodnar, personal communication, Northeast Utilities, interview July 1985.

[68] Ray Coxe, personal communication, Massachusetts Institute of Technology, July 1985.

4.7 Chapter Summary

The combination of advanced process control techniques with new fault tolerant processors and advanced computer networking techniques creates a nuclear power plant control system that is particularly well suited to multi-modular control. There are numerous questions that need to be answered in the areas of degree of automation, level of redundancy, effects of interconnection on control, and the general architecture of the control system.

The largest impact on the control system design will be whether or not the control system is proven to be non-safety related. If this occurs the designer of the control system will have much greater freedom in the degree of automation, and type of control employed (digital, PID, etc.).

If part of the control system is classified as safety related, it may still be possible to use digital computers for control, since many of the issues of importance in the past no longer apply. For instance, the self checking technique used by Stratus Computer enables the computer to tolerate loss of components without any degradation of performance. Approaches like this one will enable the digital computer not only to be licensed for nuclear power plant control, but also for enhanced plant operation via automatic control.

Chapter 5

Summary, Conclusions and Recommendations

5.1 Summary and Conclusions

Small, inherently safe, modular nuclear power plants both require and allow the use of advanced digital control techniques for control. Since several modules must be coupled to a single turbine / generator for the economic operation of the plant, up to five modules might feed a single turbine, and there may be as many as three or four of these combined units operating at one site. This multitude of reactor cores and control signals dictates that automatic digital control must be employed. The use of digital control is less of a regulatory burden for an inherently safe reactor, than for a large LWR, because it may be possible to prove that the control system (not including the control of any safety systems), is non-safety related.

Other industries have extensive experience with digital control. Applications such as aircraft and chemical plant control have already used advanced methods such as artificial intelligence, and fault tolerant processing.

The space shuttle has five main computers operating in a voting fashion for error detection. A similar method called 'pair and spare', developed for the banking industry, detects and removes errors in the computer's hardware before they can propagate. These fault tolerant techniques are directly applicable to multi-module control.

In addition to this, artificial intelligence is being used as an operational aid in chemical plants in the form of expert systems. PICON is an expert system developed for real time process control. Not only does PICON provide expert

advice to the operators, but also it has the qualities of simplified programming using a pseudo-english, and simple modification procedures.

Other related new computer technologies, such as fiber optic communication, and advanced display devices, are able to meet the constraints of a nuclear power plant environment. New flat panel displays can provide high resolution, luminance, color, and flickerless displays. In addition they are shock resistant, and have a lower danger of damage from implosion than CRTs. Fiber optics also have the necessary qualities for nuclear power plants, in that they can provide data communication rates of up to 100 Mbits/sec, and are immune to electromagnetic interference.

These and other advances in the computer and digital control fields promise to speed the task of developing a digital control system for multi-modular control. These technologies will continue to be advanced by the market forces that produced them, and consequently, the nuclear industry will benefit by these advances.

Table 5.1 lists features of a possible multi-module control system derived from the considerations explained in the current review.

Table 5.1
Control System Features

Feature	Comment
Fault tolerant processor	Available from Stratus and others.
Sensor fault tolerance	Algorithms developed and advanced algorithms under development by NASA, CSDL, and others.
Fiber optic communication via a ring or bus network	Under further development by a variety of private companies.
Expert System derived control software (e.g. PICON)	Developed by Lisp Machine Inc.
High Automation	Similar to Canadian and Japanese approach.
Low number of operators	The use of automation allows this feature which is necessary for economic operation.

Based on our review it is concluded that the objectives of safe and economic control of multi-modular units using advanced control methods should be feasible.

5.2 Recommendations

The following is a list of issues and questions that have been identified as relevant to computer control of a multi-module nuclear power station. Group 1 issues are those that affect the way in which the plant will operate. Group 2 issues are those that affect the design of the plant and the control system. Group 3 issues are those that will either impact current regulations, or those that are affected by current regulations. There is, of course, considerable overlap in the classification of these issues; many issues have an impact in each category. For instance, plant automation not only affects control system operations, but also confronts current regulations on direct digital control of nuclear power systems.

Issues

Group 1 - Operational Issues

- It will be essential to automate the plant as much as possible, including at the minimum all routine operations, such as startup, shutdown, and also turbine/generator operations. Additionally, it appears highly desirable to automate non-routine operations such as the response to transients caused by the tripping of another module, loss of offsite power, refueling and other events that are expected to occur at least once a year. The high degree of automation is necessary to reduce the number of control room personnel.
- An overall system involving a minimum of operating personnel must be devised: possibly a base crew of four operators for a single module, plus an additional operator for each additional four modules.

Group 1 - Operational Issues (continued)

- There must be a capability to lock out the control of a module from the remaining units, so that operators can concentrate on a specific module, while the computer controls the rest of the plant.
- The strategy for separation of safety and control functions when the new digital control technology is used must be clearly defined.
- It may be feasible and preferable to give the electrical grid dispatcher the authority to adjust the plant power within limits.

Group 2 - Design Issues

- It may be desirable to have more than one control room on site (i.e. one control room with its set of operators for a segment (three modules) of a PRISM power plant). If this is true one must decide on how many units per control room, and on how many modules per control console.
- The remote monitoring of key safety parameters is required by the NRC, and this could be met by transmitting these parameters to NRC headquarters in real time. This may favorably dispose the NRC to the use of a digital control system.
- The level of redundancy for hardware sensors and signals (i.e. duplex, triplex, quad) needs to be defined.
- The extent of the control function permitted at the module itself (remote shutdown capability) needs to be defined.

Group 3 - Regulatory Issues

- It must be established whether requirements for emergency power can be reduced for passively safe modules. If the requirements are reduced, then perhaps credit can be taken for one unit providing emergency power for others.
- It may be desirable to plan for and perform a "Total Loss of Instrumentation and Control Capability" test on a single module that would demonstrate the inherent safety of the reactor and of the non-necessity of the control system's operation for safe shutdown of the plant.
- Careful delineation of how to simulate multi-modular effects if only a single unit is available for test must be made,
- If the control system is classified safety related, it will be extremely difficult to meet current standards because it is almost impossible to fully test complex software.
- It will be necessary to determine if connection (both steam system and control system) of a newly constructed module to existing modules is a potential accident initiator.
- It is necessary to establish how the limits on released radionuclides from the design basis accident will be applied. Will modular plants be constrained by this regulation on a per unit basis or a per site basis? If the regulation is applied to each individual module then each module will be subject to a set radionuclide release limit. If the regulation is applied to the site, then the total source term from all units will have to be considered, and this may cause more stringent design standards to be applied to the mitigating systems, such as containment and control systems, on individual modules.

In conclusion, a clearer definition of control system goals, requirements and design criteria must be established in the near future to permit realization of the goals of cost effective multi-module control.

Bibliography*

1 "Air Crashes hitting insurers heavily," The Boston Globe, August 16, 1985. Page 5.

2 "General Design Criteria for Nuclear Power Plants," 10 CFR 50, Nuclear Regulatory Commission, (Dec. 1982).

3 "NTSB Studies Reaction to Engine Loss in China Airlines Emergency Descent," Aviation Week & Space Technology, March 4, 1985. Page 29.

4 "Peripherals: Graphics and imaging system presents true 3-D display," Computer Designs, Vol 24, No. 4, (April 1985) Page 96.

5 The Petroleum Handbook, 6th ed. Elsevier Science Publishers, New York, 1983. Page 235.

6 PICON Users Guide, Lisp Machine Incorporated, 1985, Page 76.

7 A.K. Caglayan, R.E. Lancraft, "An Aircraft Sensor Fault Tolerant System," NASA-CR-165876, Bolt, Beranek and Newman, Inc., Cambridge, MA. April 1982.

8 E.W. Carpenter, "Carbon Dioxide Cooled Reactor Experience", paper presented at the 7th International Conference on the HTGR, Dortmund, Federal Republic of Germany. September 1985.

9 G. Chisolm, "FAFTRCS: Full-Authority Reactor Control System," Trans. Am. Nucl. Soc., Vol. 49, (June 1985) Page 376.

10 D. M. Considine (ed), Energy Technology Handbook, McGraw Hill Book Co., New York, 1977. Page 244.

11 A. Cruickshank,"Advancing breeder reactor design in the United States", Nuclear Engineering International, February, 1985. Vol. 30, No. 365. Pg. 17

12 M. M. Danchak, "Effective CRT Display Creation for Power Plant Applications," Power Instrumentation Symposium, San Francisco, Ca. May 1976.

13 M. Dejule, et. al. "Construction of the Flatscreen Gas-Electron-Phosphor (GEP) Display" Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 50

14 M. Dejule, A. Sobel, J. Markin, "A New Gas-Electron-Phosphor (GEP) Flat Panel Display - The Flatscreen panel, " Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 39

---

* The numbers listed here are not the same as those on the footnotes at the bottom of each page.

15 G. M. Garner, "Fault Detection and Level Validation in Boiling Water Reactors," PhD Thesis, Charles Stark Draper Laboratory and Dept. of Nucl. Eng., M.I.T., (September 1985).

16 F. Gibney, R. Pope, (editors), Catastrophe! When Man Loses Control, Bantam/Britannica Books, New York, 1979.

17 A. Hall, et. al. "The Intelligent Safety System: Could it Introduce Complex Computing into CANDU Shutdown Systems?,"Chalk River Nuclear Laboratories, Ontario. AECL-8561, (July 1984).

18 R. G. Hewlett, F. Duncan, Nuclear Navy, University of Chicago Press, Chicago, 1974. Page 280.

19 E. M. Hinchley, et. al. "The CANDU Man-Machine Interface and Simulator Training," Chalk River Nuclear Laboratories, Ontario. AECL-7768, (Sept. 1982). Page 2.

20 M.S. Imamura and J.H. Masson, "Autonomous Control Design Considerations for Space Nuclear Power Systems," Space Nuclear Power Systems, Orbit Book Company, Inc. Malabar, Fl. 1985. Page 115.

21 Seishiro Kawakami, et. al. "Operating Experience in Using Computerized Plant Automatic Start-Up Control System," Toshiba Corporation, Japan. (April, 1985).

22 Seishiro Kawakami, et. al. "Reliability of BWR Plant Digital Control," Toshiba Corporation, Japan. (March, 1985).

23 Takashi Kiguchi, et. al. "A Knowledge Based System for Plant Diagnosis," Energy Research Laboratory, Hitachi, Japan. (June 1985).

24 Mitsuo Kinahita, et. al. "An Event-driven Control Method for Automatic Operation and Control of Nuclear Power Plant," Energy Research Laboratory, Hitachi, Japan. (June 1985).

25 C. N. King, et. al. "Development of a 256 x 512 Electroluminescent (EL) Display Monitor,"Advances in Display Technology IV, Elliot Schlam, Editor, Proc. SPIE 457, 1984. Page 76.

26 N. Makhoff, "LANs Team Up to Widen the Network Connection," Computer Design, Vol. 24, No. 2, (February, 1985). Page 108.

27 C.F. McDonald, A.J. Goodjohn, F.A. Silady, "Small, Passively Safe, Modular Gas-Cooled Nuclear Power Plant with Pebble Bed Reactor", paper presented at the Joint Power Generation Conference, Toronto, Canada. October, 1984

28 L.D. Mears, M.L. Brown, "America considers the modular HTGR", Nuclear Engineering International, October, 1985. Vol. 30, No. 373.