Title
Reactor control system upgrade for the McClellan Nuclear Radiation Center

Author
Power, Michael A.

Publication Date
1999-03-10

Peer reviewed

ANL/NT/CP-97369

REACTOR CONTROL SYSTEM UPGRADE FOR THE McCLELLAN NUCLEAR RADIATION CENTER SACRAMENTO, CA

By

Michael A, Power

Nuclear Technology Division
Argonne National Laboratory-West
P. O. Box 2528
Idaho Falls, ID 83403-2528

To be presented
at
ANS 8th Topical Meeting On Robotics
And
Remote Systems

April 25-29, 1999
Pittsburgh, PA

* Work supported by the U. S. Department Energy, Office of Nuclear Energy, Science and Technology, and the Office of Environmental Management, under contract W-31-109-Eng-38.

DISCLAIMER

Reactor Control System Upgrade for the McClellan Nuclear Radiation Center Sacramento, CA

Michael A. Power (Argonne National Laboratory)
P.O. Box 2528, Idaho Falls, ID 83403
Email: power@anl.gov
Tel: 208-533-7952

ABSTRACT

Argonne National Laboratory is currently developing a new reactor control system for the McClellan Nuclear Radiation Facility. This new control system not only provides the same functionality as the existing control system in terms of graphic displays of reactor process variables, data archival capability, and manual, automatic, pulse and square-wave modes of operation, but adds to the functionality of the previous control system by incorporating signal processing algorithms for the validation of sensors and automatic calibration and verification of control rod worth curves.

With the inclusion of these automated features, the intent of this control system is not to replace the operator but to make the process of controlling the reactor easier and safer for the operator. For instance, an automatic control rod calibration method reduces the amount of time to calibrate control rods from days to minutes, increasing overall reactor utilization. The control rod calibration curve, determined using the automatic calibration system, can be validated anytime after the calibration, as long as the reactor power is between 50W and 500W. This is done by banking all of the rods simultaneously and comparing the tabulated rod worth curves with a reactivity computer estimate. As long as the deviation between the tabulated values and the reactivity estimate is within a prescribed error band, then the system is in calibration.

In order to minimize the amount of information displayed, only the essential flux-related data are displayed in graphical format on the control screen. Information from the sensor validation methods is communicated to the operators via messages, which appear in a message window. The messages inform the operators that the actual process variables do not correlate within the allowed uncertainty in the reactor system. These warnings, however, cannot cause the reactor to shutdown automatically. The reactor operator has the ultimate responsibility of using this information to either keep the reactor operating or to shut the reactor down.

In addition to new developments in the signal processing realm, the new control system will be migrating from a PC-based computer platform to a Sun Solaris-based computer platform. The proven history of stability and performance of the Sun Solaris operating system are the main advantages to this change. The I/O system will also be migrating from a PC-based data collection system, which communicates plant data to the control computer using RS-232 connections, to an Ethernet-based I/O system. The Ethernet Data Acquisition System (EDAS) modules from Intelligent Instrumentation, Inc. provide an excellent solution for embedded control of a system using the more universally-accepted data transmission standard of TCP/IP. The modules contain a PROM, which operates all of the functionality of the I/O module, including the TCP/IP network access. Thus the module does not have an internal, sophisticated operating system to provide functionality but rather a small set hard-coded of instructions, which almost eliminates the possibility of the module failing due to software problems. An internal EEPROM can be modified over the Internet to change module configurations. Once configured, the module is contacted just like any other Internet host using TCP/IP socket calls. The main advantage to this architecture is its flexibility, expandability, and high throughput.

1. Introduction

The McClellan Nuclear Radiation Center (MNRC) is a 2 MW TRIGA-type reactor located in Sacramento, CA. The MNRC is presently owned and operated by the United States Air Force (USAF) with a principle mission of neutron radiography. In more recent years, the capability of performing silicon transmutation doping (STD) of silicon ingots has been added to the mission. In the future, the mission shall be expanded further to include the capability of Boron-Neutron Capture Therapy (BNCT). These new missions have been added to the original mission in order to make the MNRC a more programmatically diverse facility with the capability of serving both the private and the military sector.

The ultimate goal of this diversification is to privatize the MNRC, causing the MNRC to transition from the ownership of the USAF to the ultimate privatizing partner.

To support the new scope and demands from the privatizing partner, the current MNRC control system is to be replaced since the current system generates spurious scrams, uses outdated software, and contains non-replaceable parts. The new control system will eliminate the problems of the current control system by using a Sun Solaris based control system and industry-standard interfacing software and hardware. A brief overview of the control system in terms of the method of upgrading the system and a description of the new control system hardware follows. A more detailed description of the new control system is contained in the following sections.

2. Description of Upgrade

There are three distinct phases associated with the upgrade of the control system. The first phase is the simulation-testing phase. In the simulation-testing phase, the control software, which includes the data logging, flux control, man-machine interface (MMI), and watchdog routines shall be tested using a DSNP simulation of the MNRC reactor hardware.[1] The I/O communication routines are not activated for this phase. In the place of the I/O communication routines, the control software shall communicate with a DSNP simulation of the MNRC reactor system using an internal communication interface. The physical effects of the reactor kinetics, thermal hydraulics, and control rod system are included in the DSNP simulation to test the proper operation of the control software. In this particular testing phase, the software routines and the simulation routines are developed by different groups according to the software specifications. This sort of double blind development and subsequent verification of software functionality helps assure the proper functionality of the software.

Once the control software has been initially verified by the simulation phase, the second phase of the installation is the piggybacking phase. In this phase, the analog and digital inputs of the system are connected in parallel with the existing control system, the I/O communication routines are activated and the simulation of the system deactivated. The licensed reactor control system is then run in parallel with the new control system for an appropriate length of time as to verify that the new control system performs as designed.

The third phase of installation is to disconnect the control signals from the old control system and to connect those control signals to the new control system. Following the installation of the new wiring, a full diagnostic of all systems must be performed with the control rods not connected to the rod drives. The rods must be run up and down in auto and manual modes in order to check the magnitude and direction of the control rod speed.

Since NRC approval has not been granted to perform the piggy-backing or the final installation, this paper discusses only the simulation and testing phase of the development.

3. New Reactor Control Computer

The MNRC control system consists of one Sun Microsystems workstation with two monitors, which shall be located in the reactor control room. The first monitor contains only real-time display information for the reactor flux, the reactor control rods, the reactor powers and the reactor temperatures, whereas the second monitor provides operator control input as well as additional topological data displays for accessing real-time and historical data. There is no need for any additional computers to be used for I/O interfacing, as in the previous General Atomics (GA) system, due to the type of data acquisition and control equipment selected for the project, .i.e., the Intelligent Instrumentation EDAS I/O system.

The seven Intelligent Instrumentation, Inc. EDAS modules, which shall be used for data acquisition and control, contain embedded processors to transport the data to and from the I/O terminations and control computer. The transport of data is simplified and standardized by using standard ethernet cabling and TCP/IP communication protocols between each of the EDAS modules and the control computer. The special terminations and rack-mount equipment that Intelligent Instrumentation supplies with the EDAS modules provide an extremely compact and organized method of implementing a data acquisition and control system.

Embedded within the EDAS data acquisition and control system is a hardware-based watchdog timer. This watchdog timer uses a zero-crossing detector to check for a regular occurring pulse originating from the control application. If the control application fails, the computer fails, or the network is lost, then the watchdog pulse is lost at the I/O system and the watchdog timer will time-out resulting in a scram of the reactor. The entire watchdog system is implemented by analog hardware to eliminate the possibility of a software failure of the watchdog.

The control system software operating on the Sun workstation includes a number of independent programs or processes: 1) a communication process to interface I/O devices with the workstations, 2) a low-level and a supervisor-level control process to control reactor power in auto, manual, square-wave and pulse modes to provide enhanced diagnostics of the reactor and to provide redundant software scrams, 3) a watchdog process to prevent the motion of rods in the event of a loss of communication to the I/O system or the failure of one of the control system processes, 4) an MMI process to control the system from a convenient graphical interface, and 5) a data archiving process to store process data on local hard-disks and to tape backup. In addition, the reactor control system includes a simulation of the reactor that tests the functionality of the control system.

A UNIX-based operating system, specifically the Sun Solaris 2.6 operating system, is used for the control computer since the UNIX operating system is a mature and robust operating system that has been in existence since the 1970's.[2] The UNIX-based implementation provides numerous capabilities to be described. These include a reliable and deterministic means of inter-process communication, timing, scheduling, and security.

3.1 Inter-Process Communication (IPC)

Although the overall reactor control system consists of independent processes for software reliability and flexibility reasons, a certain restricted amount of information must be passed between processes, resulting in the need for a reliable and fast form of inter-process communication (IPC). The Solaris operating system provides a number of different IPC options such as 1) semaphores, 2) messages, 3) signals, 4) pipes and 5) shared memory. All of these IPC's except for shared memory provide a means of queuing IPC's so that in the event IPC's arrive while the receiving process is busy, the IPC will wait in a queue until the receiving process has time to accept and process the IPC. In contrast, all of the IPC's except for shared memory are slow. For this control system, the major constraint is speed and therefore shared memory is used for IPC.

The decision to use shared memory forces the control code to handle IPC queuing. This is done by creating additional shared memory variables, which store the IPC information while the other processes are busy. Although the creation of these additional variables may seem laborious, it allows complete control, from the standpoint of the control software, over the flow of data and IPC information between processes. Thus, the decision to use shared memory as the means of data communication also removes possible queuing faults from an operating system queue overflow.

3.2 Timing and scheduling

Each of the programs that make up the control software is run at a fixed update interval. The way this is accomplished is by making a POSIX.4 (IEEE Standard) real-time call to the Solaris operating system. In the initialization section of each process, a call is made to initialize an interval timer with a predefined timer interval or sampling rate. Each of the programs wait for their respective timer signal and then run each program in a top to bottom fashion. Once the bottom of the program is reached, the process waits for the next timer signal. Therefore, each program does nothing until it receives the next timer signal. This operation results in improved CPU performance over a simple infinite loop plus delay type of control logic. The timer-based program is not using CPU cycles when it is waiting for the timer signal unlike the simplistic method of using an infinite loop. When an infinite loop is running, it is still using CPU cycles. In fact the delay loop may take up all of the CPU cycles if not properly implemented.

In order for more important processes to be run on schedule, the POSIX real-time calls have a priority level associated with them. These real-time (RT) priority levels vary from a maximum value denoted here by 0 and to a minimum value that depends on the operating system and hardware. The priority levels for the MNRC control system are contained in Table 1.

Table 1
Control Processes

Process	RT#	Timer Interval
Watchdog timer	1	20 msec
I/O communication	1	10 msec
Control routine	2	20 msec
Data Logger	2	20 msec
Control Supervisor	2	20 msec
MMI display	3	20 msec

The absence of a 0 level for any process is important since the operating system runs at level 0. It is always a good practice to not have an application running at the same level of the operating system. There are some processes that have the same priority level. The way the POSIX.4 implementation handles this situation is to run each process in a round robin-fashion. That is to cycle though all the processes running at the same priory level in a time-slice fashion until all the process have completed during a timer interval.

The way POSIX.4 decides to run applications at different priority levels is even simpler. If a RT process which is scheduled to run has a lower priority number than the processes which are currently running (except for those at the same priority level), then the process with the lower priority number will preempt the current processes until the process with the lower priority number is finished. This means that the lower the RT priority number, the more important the RT process. For example, the control supervisor may be running when the I/O communication task is schedule to be run. The control supervisor is put on hold until the I/O task is complete. Since the I/O communication task only takes fractions of msecs, the interrupted time is not very long, especially when compared to the timer intervals for the processes.

All of the processes have a 20 msec update interval except for the I/O communication task. The I/O communication task is run at two times the fastest update interval of the other processes because of the Nyquist sampling criterion.[3] In addition, an overall update rate of 20 msec meets with timing specifications of previous generation reactor control systems.

3.3 Security

In order to prevent unauthorized access of the reactor control system, the control system provides two forms of security which are incorporated into the control system: login security at the control console and login security over the ethernet. The security at the console is accomplished by requiring the operator to provide a valid login name and password before the reactor control program will accept any control inputs such as pressing the rod motion controls. Security for the ethernet is accomplished by not connecting the control computers to the Internet and by limiting the number of hosts that are physically connected to the control computers on its local ethernet.

3.4 Supplied Hardware and Software

The hardware and software that are included in the control system are as follows: a Sun Ultra computer with redundant disk drives for RAID level 1 compatibility, seven EDAS data acquisition and control modules and all the necessary termination hardware for I/O data acquisition and control, DataViews development license and run-time license for development and run-time capability of the MMI's, C and FORTRAN compilers, for software development and reactor control software which meets or exceeds all the requirements in the MNRC Safety Analysis Report (SAR).[4]

The control computer and the data acquisition hardware are shown in Figure 3.1. The control computer includes two monitors, a CPU, an external tape-backup unit and an external hard-drive unit. The CPU contains two Sun video cards, a 200 MHz Ultra-Sparc processor and two 4-GByte hard-drives. The disk drives inside the control computer contain the operating system and control application. These two hard-drives are mirrored and thus contain identical information. If a failure of one disk occurs, the other disk drive will continue to operate the entire system without interruption. The operating system is able to send a message that the one disk drive has failed and should be replaced.

The external disk drive is operated in a similar fashion. There are two 9 GByte hard-drives in the external disk-drive unit. Both of the drives are mirrored, like the internal disk drives. The external disk drives are, however, different in that the external disk drives are for storage of historical time-dependent data and historical logs, rather than for the operating system.

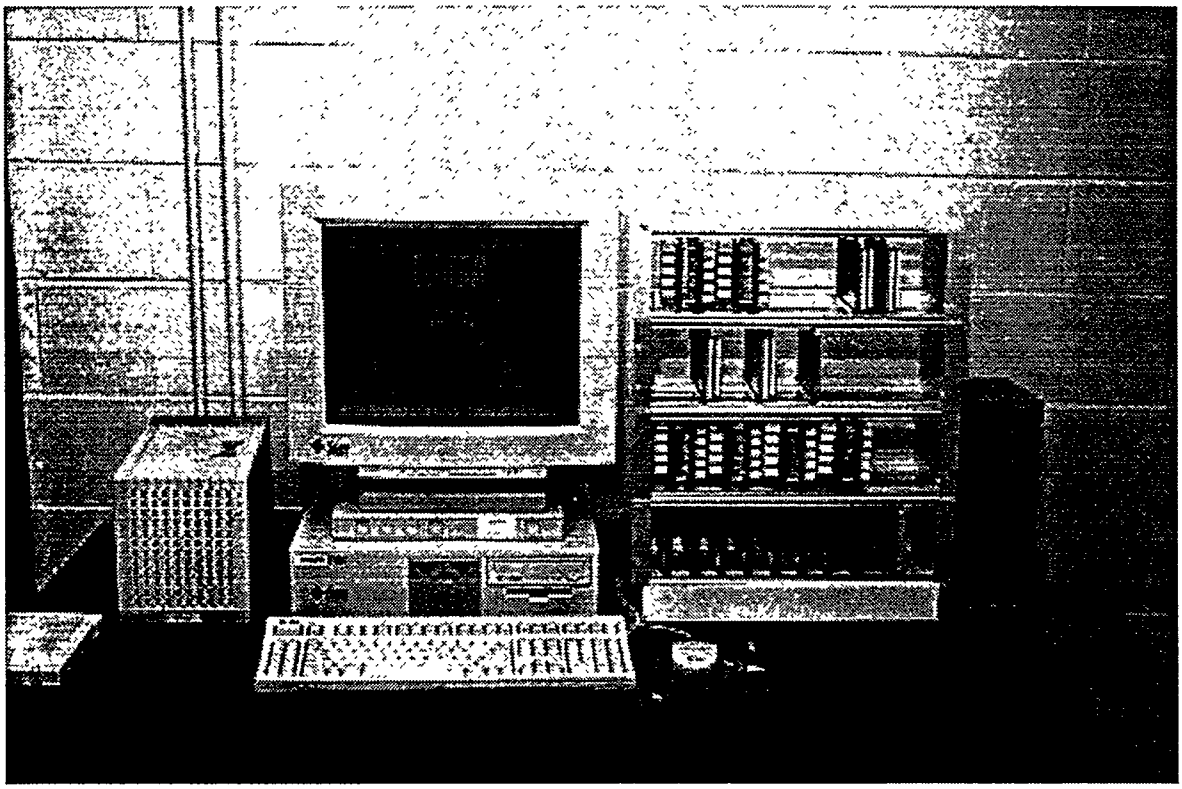

Figure 3.1 - Control Computer and Data-Acquisition System
(Shown in a Single-Monitor Configuration)

3.5 Safety Issues

The two main safety issues for the installation of the control system are the piggy-backing of the new to the old system and the eventual installation of the new control system as the NRC licensed control system.

The main safety issue related to the piggy-backing phase of the reactor control system installation is to assure that the new control system can not interact in any way with proper operation of the licensed control system. This is accomplished in two ways. First, only the control system inputs will be connected to the new system for piggybacking. Thus, the new control system cannot initiate any control commands to the reactor in any way. Secondly, the new control system will be opto-isolated from the old control system. This isolation will prevent any possible interference between the piggybacked inputs on the new control system and the inputs to the licensed control system. The reader is directed to the article on electrical independence for further information.[5]

The safety issues for the new control system when operated as the licensed control system are to control the reactor as specified by the SAR and to guarantee that the reactor is scrammed according to events listed in the SAR. The reactor control hardware and software will be tested throughout the development stage and then will be further tested under a software verification and validation (V&V) plan. Finally, the reactor control system will be operated in parallel with the licensed control system for a sufficient period of time to demonstrate that the new control system performs as required.

4. Simulation Testing And Description Of New Control System

In this section, the specific functionality of the various software routines is described. These routines are the data acquisition and control routine, the reactor control routine, the MMI routine, the data logging routine, and the reactivity computer routine. Following the description of the control software in Sections 5.1 though 5.5, the DSNP reactor simulation that is used to test the functionality of the control software is breifely detailed.

All of the software routines presented in this section are tesed using the DSNP simulation with the exception of the data acquisition and control routine. The data acquisition and control routine can be exhaustively tested by applying signals to the

system inputs and checking the corresponding value present in shared memory and by setting the system outputs in shared memory and then checking for the appropriate action at the physical outputs of the system.

4.1 Data Acquisition and Control System

The objective of the data acquisition and control software and hardware is to poll and to transmit digital and analog type signals between the MNRC primary and secondary systems and the MNRC reactor control computer. The physical hardware used for this I/O data transfer system are seven ethernet-based EDAS data acquisition and control modules and a Sun Microsystems computer. The EDAS modules are physically connected to the field terminations of the MNRC sensors and controls in the equipment room and at the control console, near the Sun control. The EDAS modules and the Sun control computer systems communicate with each other using standard TCP/IP communication protocol over the local ethernet. This removes the dependence of the IC-DOS communication protocol from the existing reactor control system, which is the cause of numerous unanticipated scrams. The I/O data transfer software, which runs on the Sun computer, is designed specifically for the MNRC reactor control system in order to make I/O polling and control of the MNRC systems transparent. The software routines communicate with each EDAS module once every 10 msec. Each of the individual inputs from the MNRC sensors is polled and the resulting value is written into shared memory on the Sun computer. At the same time the input sensors are polled, the output variables in shared memory are then sent out to the corresponding EDAS output modules. This process of polling and controlling occurs at a regular interval of 10 mseconds and continues until the system is shut down or a communication failure occurs.

If a failure occurs in the communication between any of the EDAS modules, then the watchdog routine detects this loss of communication and generates a watchdog scram within 40 mseconds. Since the communication occurs at a sampling rate of 10 mseconds, four consecutive failures must occur in order to cause a watchdog scram.

The remaining subsections for the data acquisition and control description further detail the user requirements, hardware interfaces, software interfaces, communication interfaces, and operations. This particular arrangement is based on the IEEE document given in [6] and shall be carried out throughout the software descriptions in this section when possible.

4.1.1 User Interfaces

No user interfaces are required since the user does not interface directly with the data acquisition and control hardware or software. The data acquisition and control routines interact with shared memory and the data acquisition and control hardware.

4.1.2 Hardware Interfaces

There are two locations for the EDAS hardware and one location for the control computer. The EDAS modules located in the equipment space are to poll and control the reactor primary and secondary systems. The EDAS modules in the control room are to poll and control operator generated responses and commands. The reactor computer will be located in the control room.

The layout of the modules, represented in Figure 5.1, indicates where the seven EDAS modules are installed. There are four EDAS modules in the reactor room for digital data and one EDAS module for analog data. The digital modules are further broken down into two modules for opto-isolated digital input which accommodate up to 64 DC inputs with a high-level input from 10 to 32 VDC and 4000V of input isolation, one module for relay-style digital outputs which accommodate 32 DC or AC outputs with up to 1 amp of driving capacity, and one module for non-isolated digital input or outputs which accommodate up to 16 digital TTL-level inputs or outputs.

The control computer is located in the reactor control room since the display devices used for the MMI are physically connected to these computers. In addition, audible warnings in the form of a beep are generated by the control computer, requiring the computers to be close to the operators. Maintenance and data back up are considered in the location of the control computers as well. Logged data is routinely backed-up by plant operators while they are monitoring the reactor.

4.1.2.1 General I/O System Configuration

The pin-outs for the inputs and the outputs of the various EDAS modules are related to a their shared memory, except for the special I/O's discussed in Section 5.1.2.2. The list is not presented in this paper.

4.1.2.2. Special I/O Interfacing

Most of the I/O interfacing system is constructed of industry-standard components. However, a few of the outputs have special hardware considerations. These are the watchdog timer outputs that drive the watchdog relays and the rod control outputs that drive the rod drive controllers.

4.1.2.2.1. Watchdog-Timer

The watchdog timer circuitry is bundled as part of the I/O system. The non-opto-isolated EDAS module, module #4, in the reactor room shall have a hardware-based watchdog timer connected to the first digital output. The watchdog timer receives a square-wave signal every 10 msec from the watchdog process running on the Sun computer as long as the system is functioning. An IC-based zero-crossing detector generates a high output and maintains power on the watchdog relay if the zero-crossing detector receives a pulse in 40 msec. If it does not receive a signal in 40 msec then the output of the zero-crossing detector is sent to low resulting in the watchdog relay to de-energize and thus remove power from the scram magnets.

A diagram indicating the hardware implementation is shown in Figure 5.2. The watchdog circuit takes as its input the first output of the EDAS #4. The RC time constant, formed by the combination of the discrete components R1 and C1, controls the amount of time that the zero-crossing detector (IC1) waits until the IC opens the relay contact R1. As long as there is a toggling signal being generated at output 0 of EDAS #4, the watchdog relay will be closed. Otherwise, the relay will open. As stated, the time constant for the MNRC control system is set for 40 msecs. Since the watchdog output will produce a square-wave signal with frequency of 10 msecs, there must be at lease four losses of the watchdog timer output at EDAS #4 [0] in order for the relay R1 to open.

In case of a failure of a single watchdog timer circuit, such as a relay that has inadvertently failed in the closed postion, two watchdog circuits are included as part of the control system. Thus, if one watchdog circuit fails to scram when required, then there is a redundant watchdog circuit to cause the scram. In the top of the diagram in Figure 5.3, a series connection of the two watchdog circuits is shown. The series connection of the two watchdog circuits then connects to the main scram loop. This places the two watchdog relays in series with the remainder of analog scram circuitry.

4.1.2.2.2 Motion Control of Control Rods

The existing control system currently uses a complex matrix of relays to apply square-wave signals produced by two pulse generators to provide rod control: one pulse generator for manual mode and one pulse-generator for auto mode. The matrix of relays are lined-up so that either the manual or auto square-wave signals are sent to the control rods for manual and automatic control. This means that separate pulse generators are required for the existing control system. A special feature of the EDAS modules is that they can be programmed to generate a square-wave signal with a specific frequency with up to eight different outputs. A hardware-based timer on the EDAS modules insures that the highest frequency that can be produced by the modules is 250 Hz. This is below the maximum allowable frequency for the MNRC control rod drive system.

By programming eight independent pulse generators, the eight possible control rods are manipulated independently. As shown in Figure 5.3, the new reactor control system directly controls each control rod through separate speed signals. These signals are sent from shared memory and are mapped to EDAS module #4. The EDAS module converts the analog signal from shared memory into a square-wave signal such that the square-wave frequency is proportional to the incoming analog signal. This is known as a pulse-width modulation (PWM). Since the rod drive controllers are designed to work with PWM signals, the hardware arrangement in Figure 5.3 takes better advantage of the PWM input of the rod drive controllers than does the current reactor control system. For example, if the reactor is in manual mode and a rod is moved, then a constant square-wave is generated at the EDAS module output. If the reactor is in auto mode and that rod is selected for auto control, then a square-wave signal with period proportional to the commanded rod speed is generated from the EDAS module.

The maximum allowable pulse rate of 250 pulses per second for the stepper motor controllers can never be exceeded by the EDAS modules, since the maximum achievable pulse rate for the EDAS modules in 250 pulses per second.

Due to the manner in which the motor controller for the rod drives are to be interfaced, both an up and a down rod control output is required from the new control system. To accomplish this type of control, two sets of relays are required for each control rod: one for up and one for down motion control. Since the EDAS #4 module is configured for only special digital outputs, the simple relay control is provided by the EDAS #3 digital output (relay) module. With the inclusion of the addition relays, at least two failures must occur for the rod control to be affected. For example, a continuous and unanticipated rod withdraw would require both the PWM output to fail in the on state as well as the associated up motion relay to stay activated, simultaneously. With two mutually exclusive failures required for a continuous rod withdraw, the probability of this incident, due to a coincidental mechanical failure, is low.

4.1.3. Software Interfaces

The data acquisition and control software uses the EDAS C-language libraries to provide communication between the host Sun computer and the EDAS hardware. The source code for these libraries are provided with the EDAS equipment and are locally compiled on the Sun computer platform. By locally compiling the original source code, platform-specific problems can be reduced (e.g., UNIX BSD/SVR4 differences in internet socket calls.)

The communication routines do have one external software interface to the watchdog routine. Every cycle through the routine, the routine toggles a bit in shared memory. If any one of the data acquisition and control routines fails, then the associated bit in shared memory stops toggling and the watchdog routines detects this effect after 4 misses. A system scram is sent from the watchdog routine until the respective data acquisition and control routine is restarted.

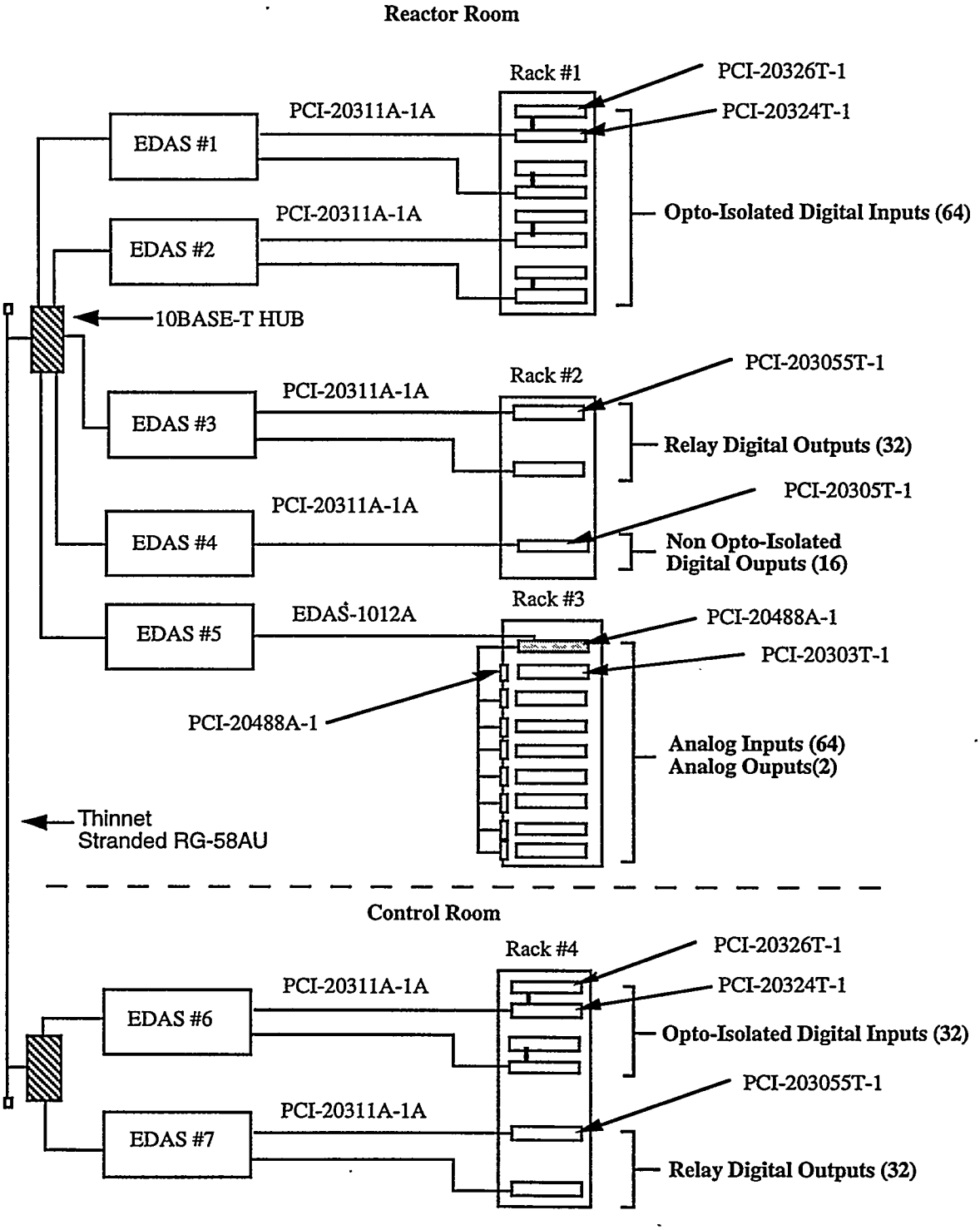

Figure 4.1– Network Topology for the Embedded Data Acquisition and Control Modules
(Sun Computer is not shown but is connected to the hub in the control room)

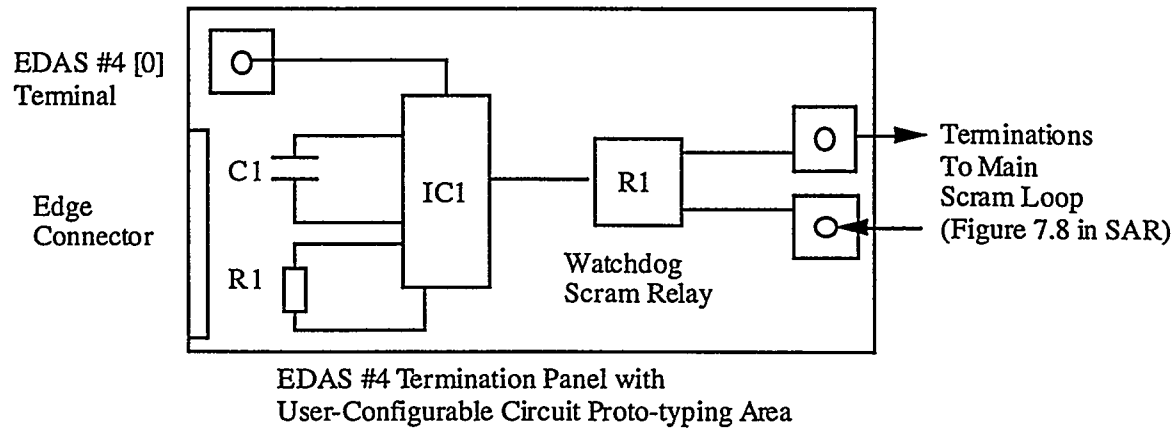

Figure 4.2 - Watchdog-Timer Circuit #1 for MNRC Control System

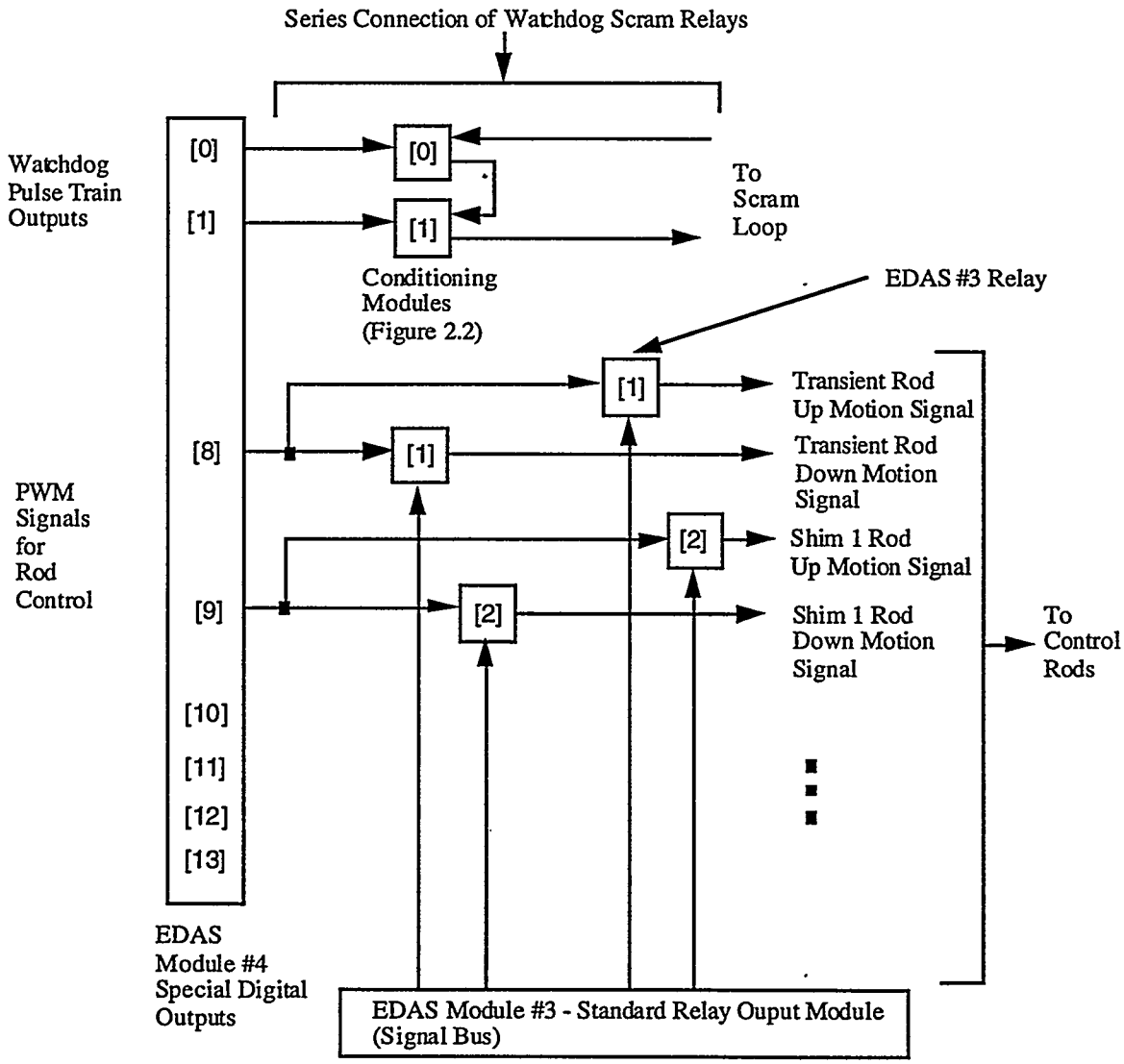

Figure 4.3 - Wiring Configuration for Watchdog Timer and Rod Drive Systems

4.2.1. Reactor Control Software

The reactor control routine has control over the motion of the control rods, the latching of the control rods and the scramming of the control rods. This is not to say that the reactor control code has ultimate control over the control rods. The new reactor control system will be in many ways similar to the existing control system in the respect that the control software only provides motion control signals to the control rod if the rod magnet power is latched. The rod magnet power can be removed at any time if any one of the low-level, analog-based scrams is activated. Thus, even if the scram and control software inadvertently fail after intense verification and validation (V & V) scrutiny, the control software cannot move any rods once a scram has occurred. Although the reactor control routine initiates scrams based on, for example, over-power and over temperature conditions, the reactor control software always operates on top of the underlying analog-based reactor protection circuitry.

Although most of the software routines described in this document are coded as state-machines, the reactor control routine is the essential state machine for the operation of the reactor. The reactor consists of many states in order to control the reactor flux in a manual or automatic fashion, to test the scram functionality or even to perform an automatic calibration of the reactor control rods.

4.2.2. User interfaces

The reactor control code takes some of its input from the user interface for mode control, automatic control functions, scram test, pre-start test, and rod calibration mode. As long as the appropriate conditions are met, the mode control buttons allow the operator to switch to reactor modes/states of operation such as: scram, manual, automatic, pulse, square-wave, pre-start checks, scram test, and rod calibration modes. Some of theses modes require additional operator input for system functionality. First, the automatic control mode requires an input of the number of rods, which are to be placed in auto control. The routine also needs an input of the demanded power that the reactor should operate. After the operator presses the accept button, from the auto control pop-up, the internal PID controller then regulates the reactor power at the demanded reactor power setpoint entered in from the pop-up window.

All of the scrams in the system are checked by the reactor control routine. The "Please Login" scram from the user interface interacts with the reactor control software. If the user is not logged in with an admissible password, then the "Please Login" scram is activated and the control routine will not let the operator switch out of shutdown mode. Once the operator logs into the interface, the "Please Login" scram is cleared and as long as the remainder of the scrams are cleared, the reactor can be switched into manual mode and started.

4.2.3. Hardware Interfaces

The reactor control routine does not directly control any hardware. All of the control outputs from the routine are sent to shared memory so that the communication routine can transport the data to the field devices.

4.2.4. Software Interfaces

The reactor control routine communicates with the man-machine interface, the watchdog routine, and the data acquisition and control routines. The man-machine interface and the reactor control routine communicate in a hand-shaking fashion to verify that the operators have acknowledged and cleared all of the system scrams before the reactor can be started. The reactor control routine can also communicate system messages, warnings, and scrams that have been initiated by the reactor control routine directly to the MMI. This is done by writing to a common file on the Sun computer. In fact, any of the routines have the ability to write to this file. To prevent two routines from accidentally writing to the file at once, the file is locked when a particular routine is writing to the file. To make sure that the other routines still send a message in case the file had been locked, a flag is set to one for each possible message. The flag is only cleared when the messages, warnings or scrams have been written to the file. On the MMI side, the file is locked, read, displayed at the interface and then deleted once read. The long term archival of these messages is handled by the MMI. The archival is also available though a local HTML server.

The reactor control routine also communicates to the watchdog routine. The watchdog routine monitors all of the different processes running on the computer and the I/O data acquisition models to determine if they are still functioning. This is accomplished by having a process on the computer toggle a bit in memory every 20 msecs and by having each of the I/O data acquisition modules report in every 10 msecs over the Ethernet. If any one of the processes does not report in or any one of the I/O data acquisition modules does not report in within 80 msec, then the watchdog timer routine will stop toggling a

digital output at the I/O data acquisition module #4. A zero-crossing detector, implemented in hardware, then detects the loss of the signal and opens the watchdog relay. The watchdog relay is in parallel with the magnet currents. Thus, causing the controls rods the fall into the reactor.

Finally, the reactor control routines communicate all input and outputs through the data acquisition and control routine for the control of the scram magnets, the control rod actuators, the pre-start and scram check controls and the pulsing controls.

4.2.7. Operations

The reactor control routine has two primary functions: to initiate a scram when the scram conditions are met and to control the state of the reactor. Two separate sections of the control routine comprise the complete reactor control code. These sections of the routine are the scram section and the reactor state controller section.

The scram section of the control routine controls the computer-initiated scram relay. Each cycle through the control routine, the routine checks the status of the scram inputs. The computer also compares the reactor power levels and the reactor temperatures to see if they are below the admissible scram limits. If any of the digital-based scrams are activated or any of the reactor indications are out of range, the scram section of the control routine sends a command signal to open the computer-generated scram relay which is in series with the main scram circuit. Simultaneously, it is presumed that the analog-based protection circuit will open its appropriate contacts and simultaneously scram the reactor. The rod magnet relays are also de-energized at the same time as the computer-generated scram relay is de-energized. Once the rods have been scrammed and the magnet power relays have been deactivated, the reactor operator must clear the scrams, switch the reactor back into manual and re-latch the control rods to cause any further rod motion.

The remainder of the reactor control routine has control over the states that the reactor can operate. The reactor control code contains various modes of operation: scram, manual, auto, pulse, square-wave, pre-start checks and control rod calibration. The different reactor control modes are coded according to the state transition diagram in Figure 5.5. The state transition diagram dictates the admissible states and the admissible state transitions; no other transitions can occur other than those defined in the diagram. This design methodology insures the reactor control system will always transition, in a deterministic fashion, from one state to the next state. Thus, guaranteeing the controller will always generate a known output for a set of inputs.

Starting at state 0 (initialization state) in Figure 4.5, the reactor control system performs the appropriate initializations, which consist of initializing the shared memory variables, initializing internal variables, setting up the interval timer, attaching to shared memory, locking the pages into memory, and switching to shutdown mode. Once the initialization is complete, the mode then transitions to state 1, the shutdown state. In the shutdown state, the reactor control code waits for the reactor operator to login with an admissible login. If the login is correct, the operator can clear the Please Login scram. Once the please login scram is cleared, the state of the reactor will transit to the scram mode (state 2). If the login is incorrect, the system stays in the shutdown state and the magnets cannot be energized. Assuming that the login was admissible, the reactor will now be in the scram state. Before the operator can go to any other state from the scram state, all of the scrams must be cleared and acknowledged. In addition, the reactor power must be above the predetermined, programmable setpoint for the lower power limit to switch to the manual mode. To switch to pre-start check or scram test mode the reactor can be at any shutdown power level.

To switch to manual mode, the operator must click on the manual mode request button from the user interface. Once clicked, the control routine will verify that the all conditions are met to make the switch and then switch to manual mode. If all of the conditions are met and the mode switches to manual mode, the operator still cannot startup the reactor. The rods must be re-latched to their lower-limit of travel position. This is accomplished by putting the key switch in to the reset position. If the rods are already latched; however, the reactor will scram upon re-latching the control rods. With the control rods latched, the operator can now move any single rod in the up direction. If the operator would like to move more than one rod in the down direction, this is an admissible control entry. If an up and down button are pressed simultaneously, however, the reactor control routine will send out a rod withdraw prohibit message to the MMI. Manual motion of control rods will only be allowed after all of the motion buttons are released.

To switch to pulse mode from manual mode, the reactor must be operating below 1 kW and must have a period of greater than +/- 26 seconds. If these conditions are met, the reactor can be switched to pulse mode from the MMI pull-down option. Once in pulse mode, the reactor can be sent back to manual mode at any time or be pulsed. The reactor can be pulsed after the fire button is pressed. Immediately, the transient rod is pulsed and a counter is started. When the counter reaches three seconds, the reactor is scrammed and the state is sent to scram mode.

If the operator wishes to switch to auto mode from manual mode, the reactor power must be between 10 and 100 percent of demand power. The operator must select the auto mode button and select the rods for auto control and a demanded reactor power. If less than three rods are selected for auto mode and the reactor power is between 10 and 100 percent, the auto mode can be engaged. The auto mode regulates the reactor power about the demanded setpoint. The reactor operator can choose any combination of any three rods at any time when in auto mode. This is a new feature of this control system. The control rods not selected in auto mode can be manually moved. This allows rod banking with automatic control of total reactor power. Finally, the reactor operator, at any time, can switch back to manual mode from the user interface.

If the reactor operator wishes to run a pre-start-test or run scram test, the reactor must be operating in the in scram mode (state 2). The pre-start mode and the scram test mode test the functionality of the scram hardware and calibration of the reactor power sensors and scram limits. The specific operation shall be the same as the existing control system. To switch back to scram mode, the operator simply presses exit from either the scam test window or the pre-start check window.

To switch into rod calibrate mode, the operator must be in manual mode, the reactor must be between 5 and 500 Watts and the reactor period must be greater than +/- 26 seconds. Once in rod calibrate mode, the control rods can be put though either a manual of automatic calibration. The automatic procedure uses a combination of rod bump with a determination of reactor reactivity from inverse kinetics. If a full calibration is requested, each control rod is bumped 10 increments along the full motion of travel and a reactivity estimate is calculated. The inverse kinetics method of obtaining reactivity is very fast as compared to the typical methods, which allows for much shorter rod calibrations. Once the rod calibration is finished, the new rod worths are store into shared memory and can be printed.

STATE FLOW DIAGRAMS

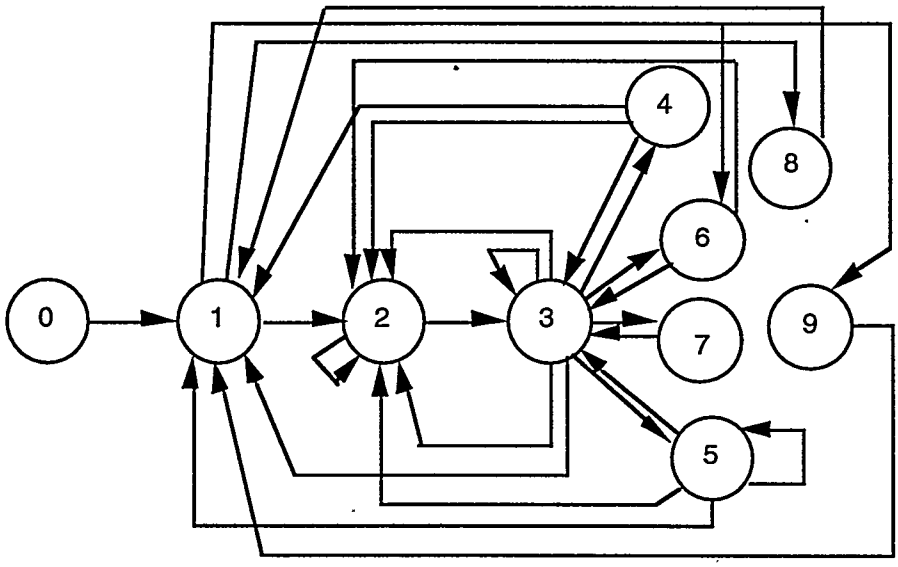

Figure 4.5 State Diagram for the Reactor Control State-Machine

0 – Initialization, 1 – Shutdown, 2 – Scram, 3 – Manual, 4 – Auto, 5 – Pulse,
6 – Square-Wave, 7 – Rod Calibration, 8 – Scram Test, 9 – Pre-Start Test,

4.3.1. Man-Machine Interface

The Man-Machine Interface (MMI) for the MNRC reactor control system consists of displays, which operate on two separate Sun Microsystems monitors. The first monitor is for reactor primary system display and the second monitor is for redundant monitoring and trending of plant data and for operator control input.

4.3.2. User interfaces

The first monitor has two screens: the first screen is for dynamic display of plant data and the second display is for system parameter tuning. The first screen on the control computer restricts the amount of information presented to the reactor operator so that only information, which relates to the proper operation of the reactor is displayed. This information consists of animated and text-based based data for the following systems: control rods, reactor primary process variables, and reactor mode, demanded reactor power. The second screen on the control computer is for tuning of parameters in the reactor control system. For example, the high radiation limit in the reactor room may be tuned from this screen. It is important to note that this screen can only be activated when the reactor is in shutdown mode. When the reactor is not in shutdown mode, only the main reactor screen can be displayed.

Animated screens are also be incorporated on the second computer screen. This monitor, however, is not intended for continuous monitoring of the reactor flux but rather for monitoring of the overall reactor system including primary and secondary systems. For instance, screen 1 is a plant overview screen that contains digital and analog meters for the various RAM's, CAM's, flow meters, power meters, and temperatures in the facility. The second screen provides trending of real-time and historical signals. This screen allows the operators to monitor the condition of the reactor over time. For instance, the pool temperature may be slowly approaching to the scram limit. By proper utilization of the trending screens, the operators can visually detect the not only the instantaneous temperature but also the rate of change of the pool temperature. The final screen provides historical access to plant data.

4.3.3. Operations

The operations of the screens can be broken down into the functionality from monitor one and the functionality from monitor two. In monitor one only one possible screen is available: the main reactor control screen. This screen is used to monitor the reactor flux, temperature and rod positions and is shown in Figure 4.6. If any messages, warnings, or scrams occur, a scrollable pop-up window displays the current list of messages in a fixed area on the screen that does not interfere with any of the other displays. The operator can either press the acknowledge button from the rod control panel or use the mouse on the screen to acknowledge each message. As each message is acknowledged, it is removed from the scrollable display. When all of the messages are acknowledged, the message board pop-up disappears.

The second monitor is for control input and additional display of plant data. The modes of operation as well as the available system options are selectable from a set of menu buttons which appear across the top of the screen. The reason for having buttons appear horizontal in stead of vertically, is so that the button, when displayed, never covers any pertinent information on the displays.

These buttons operate various functionalities of the control system. The selection of option buttons consist of browser, take rounds, system gauges, login, reactivity, trending, rod position control, and system administration. The buttons are displayed across the top of Figure 4.7. The browser launches a browser window and attaches to the local WEB server running on the control computer. All of the control system documentation, current status of system inputs and outputs, and the historical record of messages can be accessed through this WEB page. The second button is the take rounds button. This button, when pressed, reads all of the analog system values and prints the values to the local printer. A signatory line and date stamp is available on the print-out for accountability purposes. The third button, the system gauges button, displays a topological display of the overall reactor system. This screen is shown in Figure 4.8. The bay area RAM's, the reactor room gauges, equipment room sensors, balance of plant meters, demineralizer gauges, and control room data are all displayed on this screen. Referring back to Figure 4.7, the next option button is the trending button. Both real-time and historical trending are available. The real-time trending screen in illustrated in the same figure as the option buttons, Figure 4.7. Both linear reactor powers, both fuel temperatures, log power, and the system reactivates are displayed on this screen. Only four minutes worth of data are displayed to allow reactor kinetic transients to be viewed on a proper time scale. The second trending screen, the historical trending, is show in Figure 4.9. This display is essentially the same as the real-time trending screen with the exception that the historical screen requires an input of the time requested to be viewed. Again, only four minutes of data can be viewed at once. The rod position button, is a mimic of the hardware-based rod control panel. This panel was included for test-out purposes and shall be removed for the production version. The final option button is the system administration button. The system administration button provides access to the tape backups and the data logger deletion buttons. To make it more difficult for an operator to accidentally run these option, the operator must logged in as the super user to even launch the system administration pop-up window.

The mode control buttons are displayed on the top of the historical trending figure, Figure 4.9. The admissible modes are manual, auto, pulse, square-wave, rod calibration, tune parameters, scram checks, and pre-start checks.

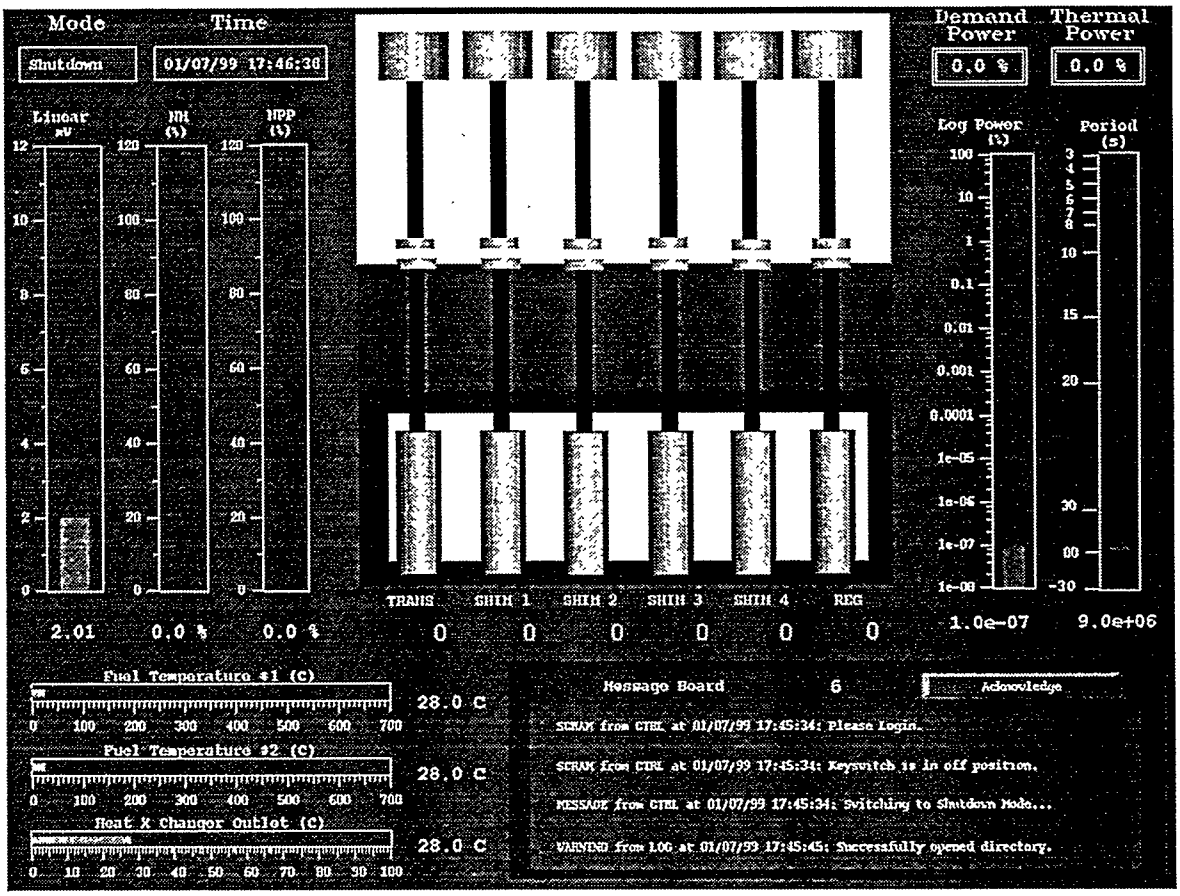

Figure 4.6 – Main MNRC Screen for Monitor 1

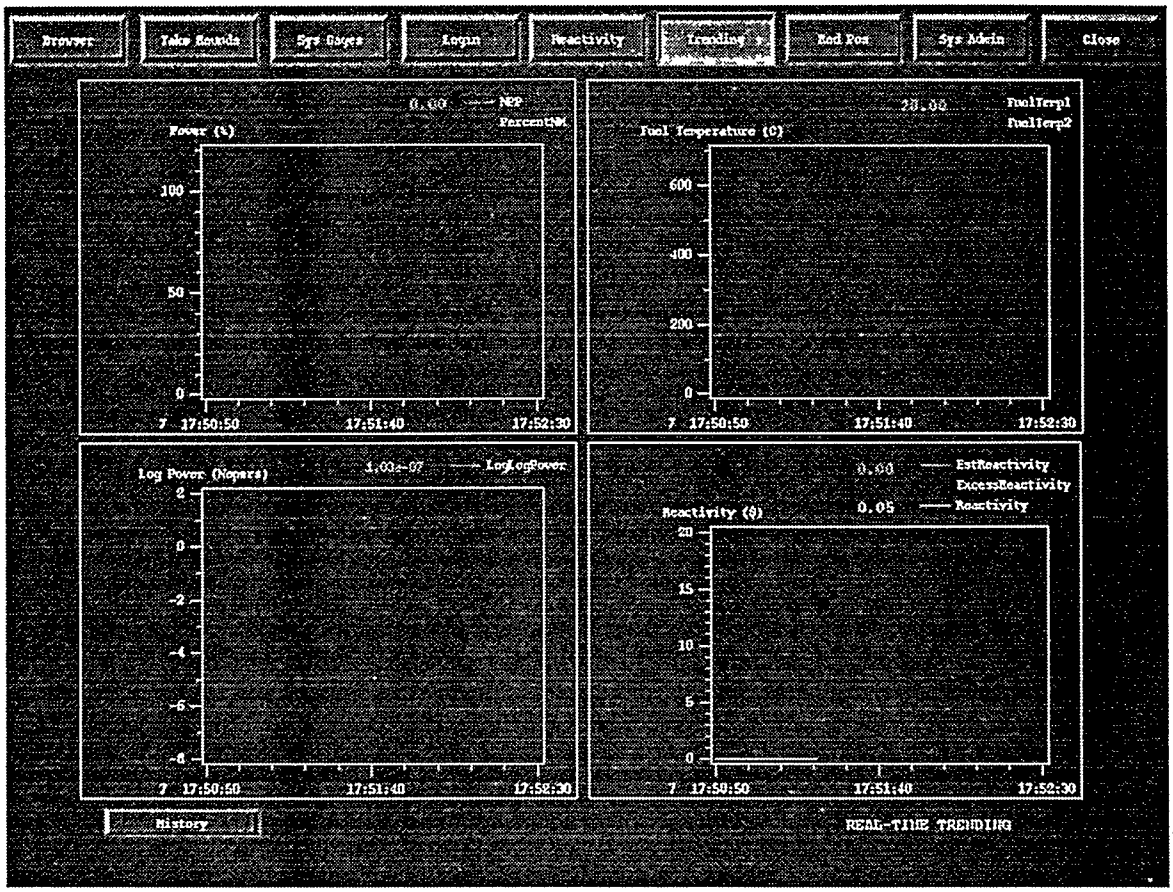

Figure 4.7 – MNRC Topological Display Screen for Monitor 2

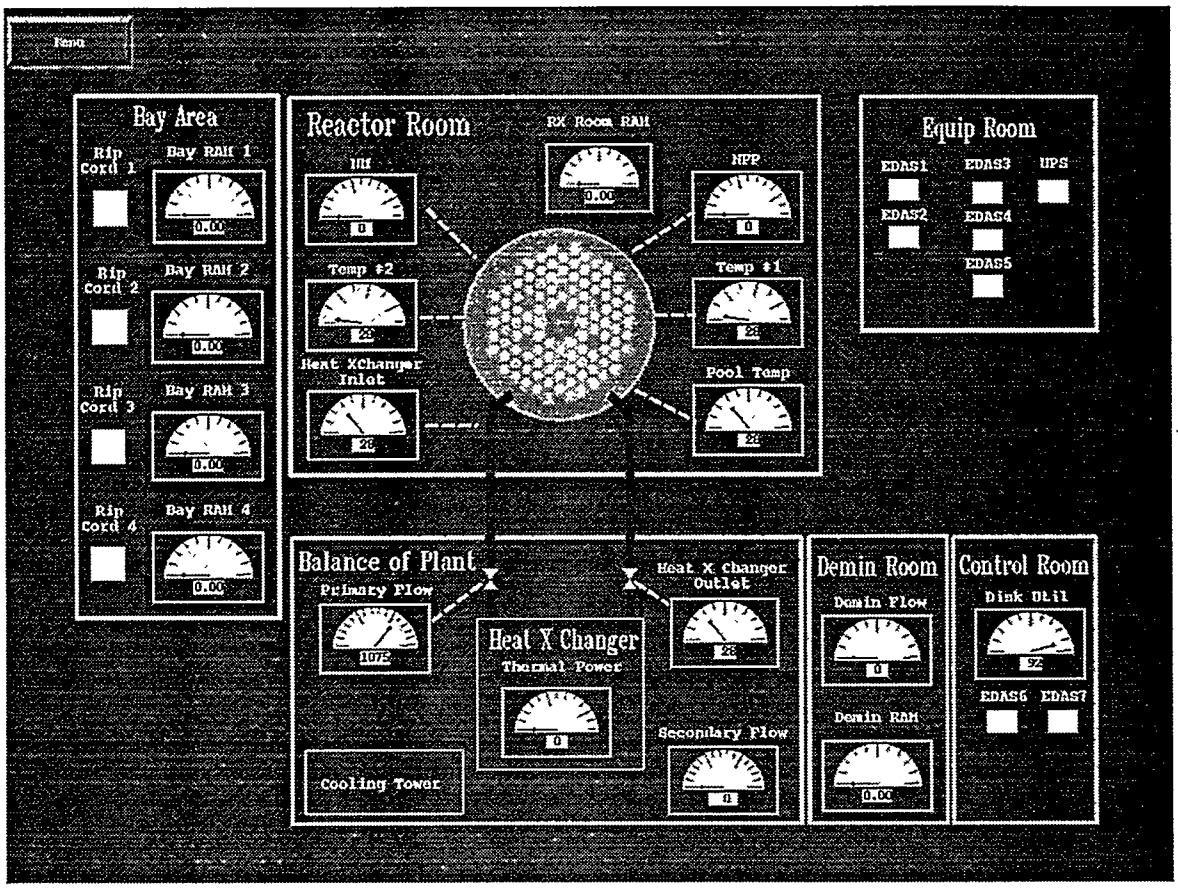

Figure 4.8 – MNRC Real-Time Trending Display Screen for Monitor 2

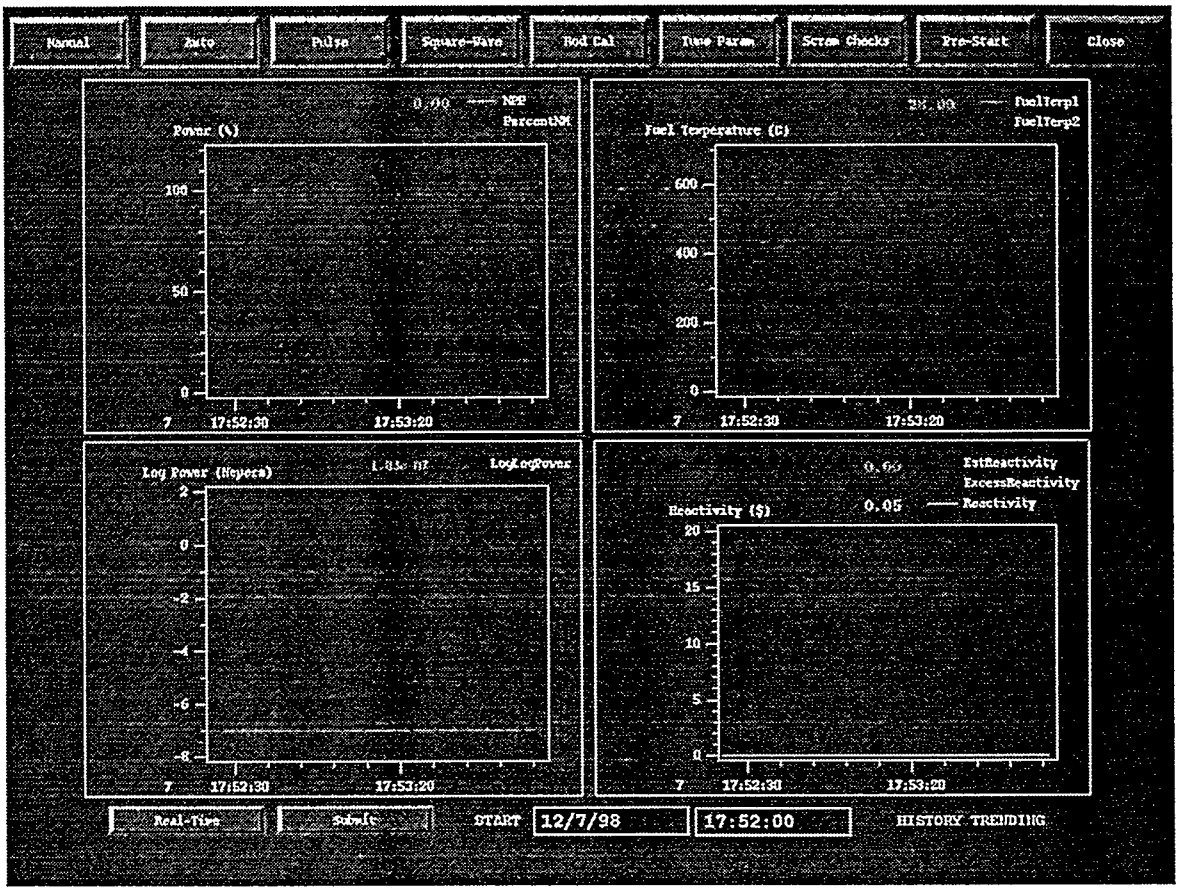

Figure 4.9 – MNRC Historical Trending Display Screen for Monitor 2

4.4.1. Data Logging System

The data logging system for the MNRC reactor control system will consist of three separate routines. The first routine is to archive scram data, the second routine is to store pulse data and the final routine is to store continuous real-time data for a selected number of the system inputs and outputs.

4.4.2. User Interfaces

There is one main user interface with the MMI that interacts with the data logging routine. The delete database command option can be accessed though the MMI if the operator is logged in with the correct superuser password. If the operator is not logged in as root, then delete database button can not be accessed. If the operator does select to delete the database, there is second window that appears asking "Are you sure?" Once the operator has pressed the "Y" option, the historical database will be deleted.

5.4.3. Operations

The main data logging routine has 5 states, as in Figure 4.10. In the first state, the routine attempts to open the data drive in which the database resides. If the data drive found, then the state is switched to state 1. In state 1, the database is opened. If the database can be opened, then the state switches to state 2. If the database cannot be opened, then the logger stays in state

1 until the database is opened. State 2 is the data logging state. Data is logged to disk and the state is switched to state 3, the data verify state. If the data is verified properly, then the state switches again to state 2 and the process starts again. If the data drive exceeds 95% utilization, then the state switches to state 4 where no data is logged. If the data drive return to below 85% utilization, then the state will switch back to state 0 and data logging process will re-initialize. No data will be lost through the initialization. The re-initialization is done as a precaution since the data logger may have been run in state 4 for an unknown amount of time before the data drive was cleared.

The pulse and scram data loggers are running continuously and storing data into an internal cache, until either a scram or a pulse occurs. When a scram or pulse occurs, the pulse and scram routines store their cached data and their data collected after the scram or pulse into their respective pulse and scram historical data files. At the same time, a message is sent to the MMI indicating that the data was stored and what the file identification number is for the pulse or scram.

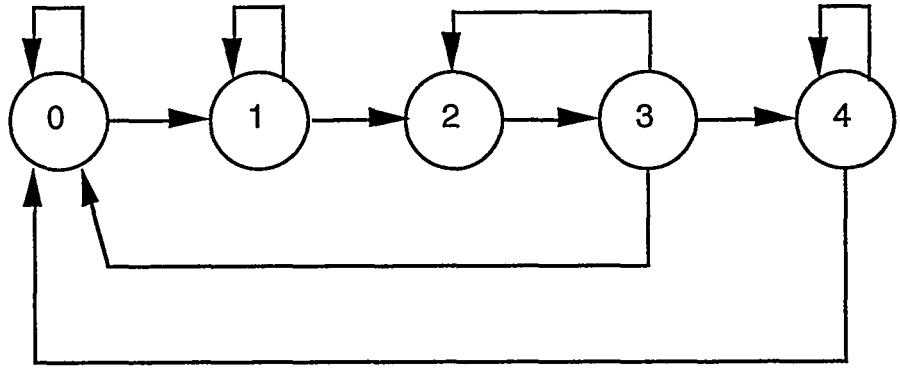

Figure 4.10 - States for the Historical Data Logging Routine

4.5.1. Reactivity Computer

The reactivity computer is designed to operate with the automatic rod calibration routine, which is part of the reactor control routine. This reactor computer uses a combination of inverse kinetics and low pass filtering to estimate the reactivity imparted into the core from control rods. This is done by analyzing the changes in the reactor power signal and inferring the reactivity that must have been associated with that change in reactor power. The reactivity computer can only be used in the intermediate range, i.e., 5 Watts to 500 Watts, since the reactivity computer does not incorporate sub-critical multiplication or temperature feedback in its model.

Since the reactivity computer is based on inverse kinetics, the reactivity estimate is fast. After the prompt jump/drop, there is no more information gained by the inverse kinetics for the reactivity estimate. Thus, the reactivity computer is designed to greatly speed up rod calibrations.

4.6.1. Reactor Simulation System

The reactor simulator is designed to verify the proper operation of the reactor control system and the reactor scram system. In addition, the reactor simulator tests out the functionality of the data archiving and signal processing functions.

Since a complete description of the simulator is out of the scope of this paper, the following list defines the requirements of the MNRC reactor simulator:

- Integrate existing reactor control system into shared memory,
- Make reactor simulator real-time,
- Must contain high-order, spatially resolved model of primary dynamics for source, start-up, and power ranges
- Must contain realistic control rod motion effects.

5.0 Conclusions

A new research reactor control system with expanded capabilities has been developed for the McClellan Nuclear Radiation Center in Sacramento, CA. These expanded capabilities include a Man Machine Interface (MMI) which incorporates more advanced information-based accessing of plant data, an automatic reactor control rod calibration system and a more reliable software and hardware platform in comparison to previous generation reactor control systems for research reactors.

Future work using this new control platform is to include a set of advanced control algorithms to mitigate the effects of plant uncertainty on the closed-loop behavior of the plant. These controllers shall be offered as an additional selection from the main pull-down options on the MMI. In addition, a set of signal processing algorithms for the detection of off-normal plant conditions shall be developed and deployed on this reactor control system.

REFERENCES

[1] Saphier, David, The Simulation Language of DSNP, Argonne National Laboratory, ANL-CT-77-20, August 1994.

[2] Curry, David, UNIX Systems Programming for SVR4, O'Reilly and Associates, Inc, Bonn, (1996).

[3] Oppenheim, Alan V. and Willsky, Alan S., Signals and Systems, Prentice Hall, Englewood Cliffs, NJ, (1983).

[4] Safety Analysis Report, Research Reactor Safety Analysis Services, Kennewick WA, (1997).

[5] IEEE Std 384-1992, IEEE Standard for Independence of Class 1E Equipment and Circuits, (1992).

[6] IEEE Std 830-1993, Software Requirements Specification (1993).