EBR-II Fuel Handling Console

Digital Upgrade

Gregory G. Peters
Darson D. Wiege
Lynn J. Christensen

Argonne National Laboratory
Integral Fast Reactor Operations Division
P. O. Box 2528
Idaho Falls, Idaho 83403-2528

ABSTRACT

The main fuel handling console and control system at the Experimental Breeder Reactor II (EBR-II) are being upgraded to a computerized system using high-end workstations for the operator interface and a programmable logic controller (PLC) for the control system. Two-dimensional (2D) and three-dimensional (3D) computer graphics will be provided for the operator which will show the relative position of under-sodium fuel handling equipment. This equipment is operated remotely with no means of directly viewing the transfer. This paper describes various aspects of the modification including reasons for the upgrade, capabilities the new system provides over the old control system, philosophies and rationale behind the new design, testing and simulation work, diagnostic features, and the advanced graphics techniques used to display information to the operator.

INTRODUCTION

Fuel Handling Equipment

EBR-II is a liquid metal fast reactor operated by Argonne National Laboratory for the U.S. Department of Energy and is located approximately 35 miles west of Idaho Falls, Idaho. An aggressive fuel unloading program has been initiated in preparation for the reactor's ultimate decommissioning. Reactor fuel and experiments are being exchanged with reflector assemblies in the reactor vessel via remotely operated fuel handling equipment which is submerged in a 26 foot diameter tank containing approximately 86,000 gallons of 700°F liquid sodium. As shown in Figure 1, the fuel handling equipment consists of all the components necessary to insert or remove

* Work supported by the U.S. Department of Energy, Reactor Research Technology under Contract NO. W-31-109-ENG-38.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

subassemblies from the reactor core and insert or remove them one at a time from the primary tank. This equipment includes the core gripper which can be rotated over any one of 637 subassembly locations in the reactor core and the transfer arm which transfers a subassembly between the core gripper and a temporary storage basket. After cooling in the storage basket for approximately two months, spent fuel is transferred from the storage basket to the transfer arm which transfers the fuel to the fuel unloading machine gripper which in turn pulls the fuel out of the primary tank through a nozzle in the top of the tank. The fuel is then placed in the interbuilding coffin where it can be transferred to another facility for processing and examination.

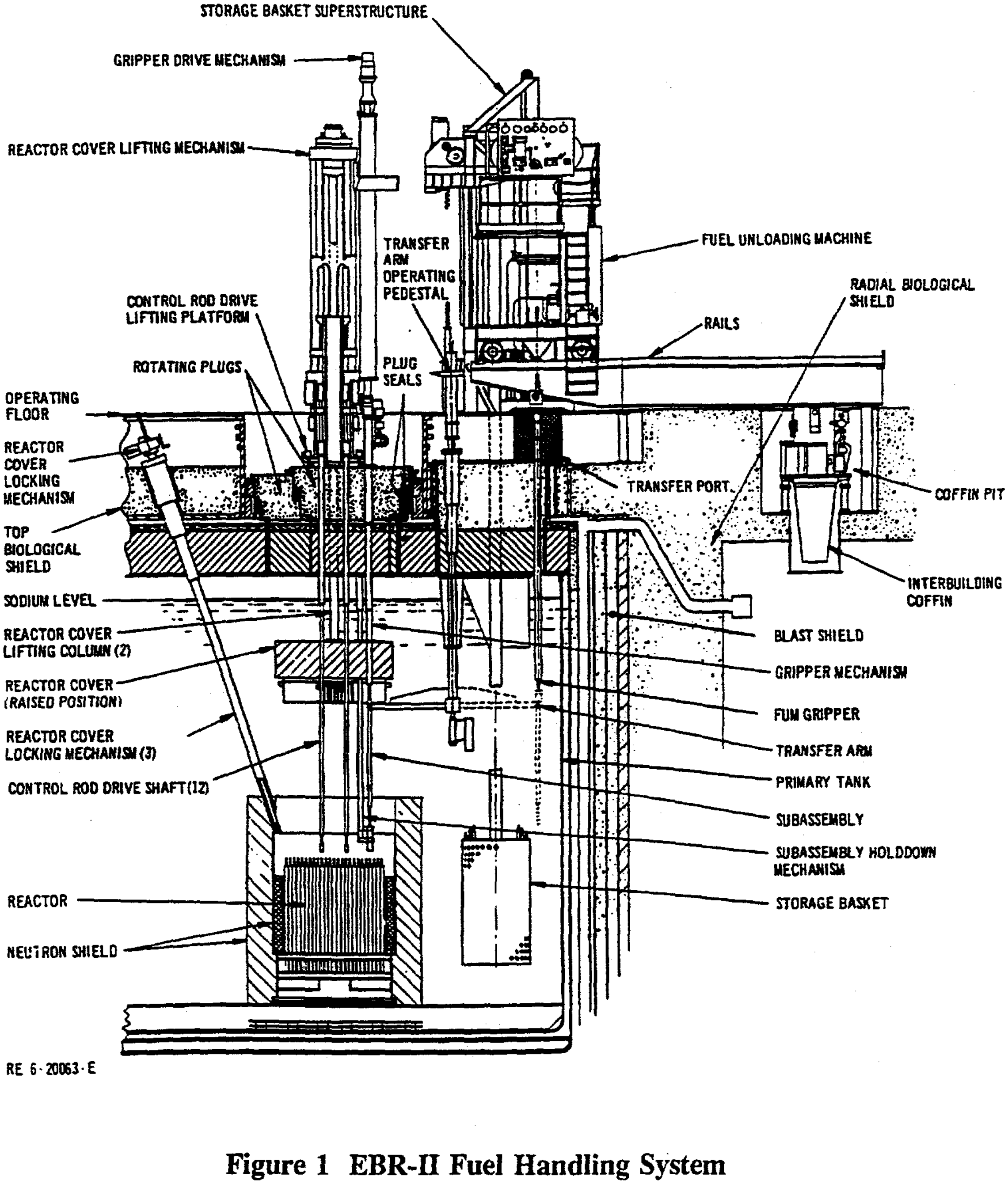
STORAGE BASKET SUPERSTRUCTURE
GRIPPER DRIVE MECHANISM
REACTOR COVER LIFTING MECHANISM
TRANSFER ARM OPERATING PEDESTAL
FUEL UNLOADING MACHINE
RADIAL BIOLOGICAL SHIELD
CONTROL ROD DRIVE LIFTING PLATFORM
RAILS
ROTATING PLUGS
PLUG SEALS
OPERATING FLOOR
REACTOR COVER LOCKING MECHANISM
TRANSFER PORT
COFFIN PIT
TOP BIOLOGICAL SHIELD
INTERBUILDING COFFIN
SODIUM LEVEL
BLAST SHIELD
REACTOR COVER LIFTING COLUMN (2)
GRIPPER MECHANISM
REACTOR COVER (RAISED POSITION)
FUM GRIPPER
REACTOR COVER LOCKING MECHANISM (3)
TRANSFER ARM
CONTROL ROD DRIVE SHAFT(12)
PRIMARY TANK
SUBASSEMBLY
SUBASSEMBLY HOLDDOWN MECHANISM
REACTOR
STORAGE BASKET
NEUTRON SHIELD
RE 6-20063-E

Figure 1 EBR-II Fuel Handling System

Control System Upgrade

The existing fuel handling system performs much of its control functions by means of complex networks of relays and limit switches. The system functions to automatically direct and limit the mechanical motions initiated by an operator to prevent a potentially damaging condition from developing. Because of its complexity, the system can be difficult to troubleshoot which results in extended down time.

A computerized fuel handling control system is currently being developed to improve system reliability and reduce maintenance. A block diagram of the hardware that will be used for the new control system is shown in Figure 2.

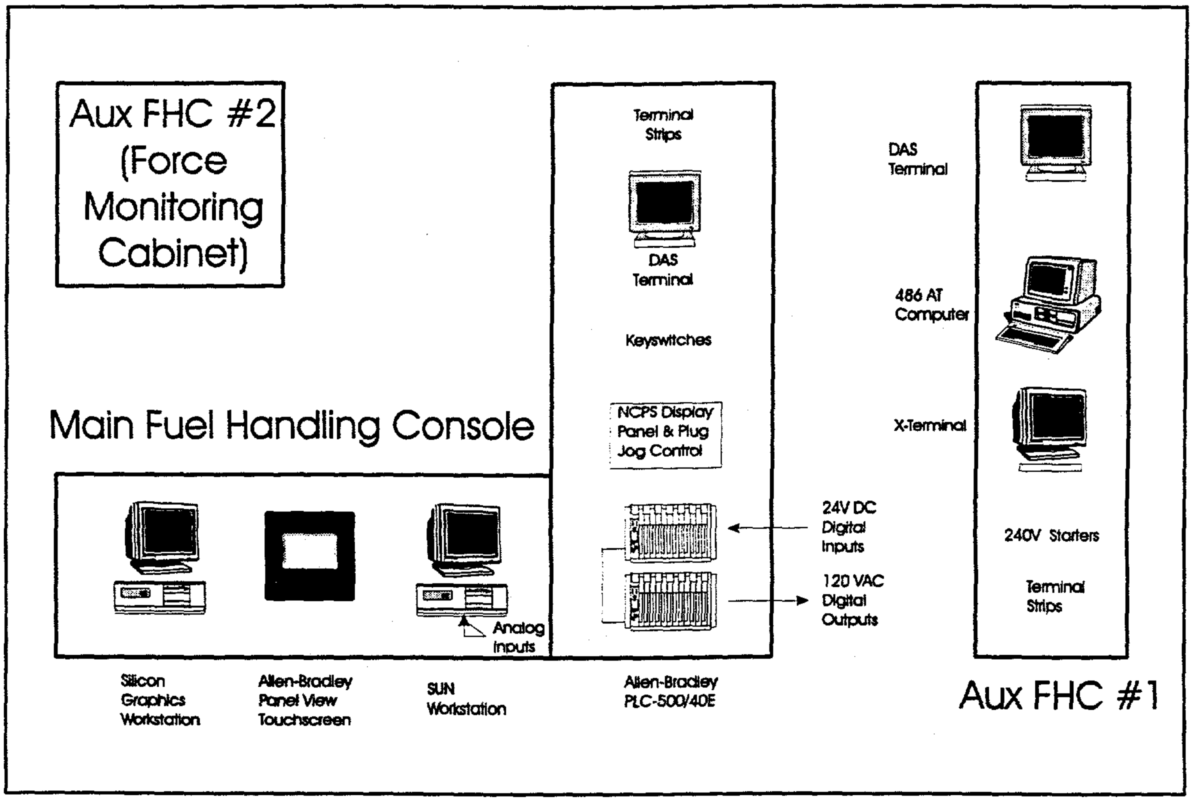
Aux FHC #2 (Force Monitoring Cabinet)
Main Fuel Handling Console
Terminal Strips
DAS Terminal
Keyswitches
NCPS Display Panel & Plug Jog Control
24V DC Digital Inputs
120 VAC Digital Outputs
DAS Terminal
486 AT Computer
X-Terminal
240V Starters
Terminal Strips
Analog Inputs
Silicon Graphics Workstation
Allen-Bradley Panel View Touchscreen
SUN Workstation
Allen-Bradley PLC-500/40E
Aux FHC #1

Figure 2: Block diagram showing major components in upgrade.

An Allen-Bradley PLC-5/40E Programmable Logic Controller provides the logical control and interlock functions. Approximately 320 limit switch inputs interface to the PLC and 145 digital output signals are sent by the PLC to control motors and solenoids. Operators input commands to the PLC control system via an Allen-Bradley PanelView™ touch screen panel. The color touch screen panel is programmed with multiple screens for each fuel handling sequence and provides indication as each step is completed. An IBM AT compatible computer provides the interface to the PLC for programming and diagnostic purposes. Ladder logic diagrams are developed and viewed graphically using ICOM's WINtelligent LOGIC 5 PLC programming software. The ladder logic diagrams update automatically with real-time information from the PLC by highlighting the current path through the logic. Thus, if a limit switch or some other interlock fails, the computer screen shows precisely where the problem is located.

A SUN Sparc 20 workstation provides graphical information to the operator concerning equipment position, limit switch status, alarms, etc. Instrumentation located outside of the primary tank has been designed to sense the positions of moving components. Signals from these instruments will interface directly with the SUN computer via A/D boards installed in the backplane of the computer. These signals are indicated as readouts on the 2D graphics display and are sent over the ethernet to the Silicon Graphics computer for updating the 3D model. A detailed computer model of the major components located within the primary tank was created using the original construction drawings and as-built dimensions taken before the tank was filled with sodium. Dynamic behavior of the moving components was then incorporated into the model so that the graphics can be animated in real-time in response to actual data.

PLC CONTROL SYSTEM

Control Hardware and Software

The control logic will be implemented using an Allen-Bradley 5/40E Programmable Logic Controller (PLC). The processor is programmed using ladder logic, a high level symbolic language commonly used for similar control applications in industry. A ladder logic program is similar to its physical relay counterpart in that it basically consists of two parallel vertical lines with many horizontal rungs each containing a "coil" at one end and a network of "contacts" at the other. Logical "AND" functions are performed using series connections for the contacts and logic "OR" functions are performed using parallel connections. The ladder logic programming approach was chosen over a general purpose programming language such as "C" or Fortran for the following two reasons:

1) The fuel handling control system contains long strings of extremely complicated logic which is easier to program in ladder logic than in a general purpose language.

2) There are no algorithmic type calculations that would require a general purpose computer to perform.

Operator Interface

The fuel handling operators will interface with the PLC through an Allen-Bradley PanelView touchscreen terminal. This terminal is a color touch screen monitor that operates just like the traditional control panel counterpart. Buttons can be maintained, temporary, toggle, interlocked, etc. and can change color. A variety of list selectors, multi-state indicators, and graphics and text are also available. The touchscreen terminal was chosen for the following reasons:

1) Approximately 128 pushbuttons and 280 lights are required to operate the system. Discrete components would have to be individually hardwired into I/O modules in the PLC. This results in a significant hardware and manpower cost.

2) The PanelView operator terminal is designed to communicate directly with the PLC, thus eliminating hardwiring each individual light and pushbutton and making it more flexible to design changes.

Fail Safe Design

An important design requirement for any control system is that it be fail safe. Fault tree analysis provides a systematic way of determining the potential hazards and the failures that could result in undesirable consequences. For this upgrade, a detailed failure analysis was performed and the results summarized in a fault tree format. Single failures that could result in damage to equipment or injury to personnel are easily spotted and the design can incorporate redundant features that require multiple failures to occur before an undesirable event occurs. For this upgrade, redundant hardwired interlocks have been designed in series with several of the PLC outputs to prevent a PLC hardware or software failure from spuriously energizing critical equipment. In addition, a hardwired emergency stop pushbutton has been incorporated which deenergizes control power to the motor control centers when pressed.

Another fail safe design strategy occurs with the use of limit switches in the ladder logic program. Limit switches usually have both normally closed contacts and normally open contacts available as inputs to the PLC. The programmer, therefore, must choose the most appropriate contact to use in the program for interlocks, indication, and control functions. The fail safe choice must take into account failures such as loss of power, broken or bent actuators, faulty wiring, loose connections, etc. Therefore, the following strategy was chosen for limit switch inputs:

> Normally open contact - Use when the limit switch performs the function of a permissive interlock. The limit switch must be closed before the equipment is allowed to operate. A loss of power, broken actuator, etc. will therefore result in the interlock failing and the equipment coming to a stop.
>
> Normally closed contact - Use when the limit switch performs the function of a destination switch which stops the equipment when it reaches the desired position. A loss of power or broken wire will appear as an open contact and the equipment will again be deenergized.

The above strategies, of course, assume that the deenergized state is the fail safe state.

OPERATOR GRAPHICAL INTERFACE

Overview

The main operator interface consists of a SUN Sparc 20 workstation computer which provides information to the operator via animated graphics, digital and analog position indicators, color dynamics, text changes, and sound. The graphics provide detailed images of the fuel handling equipment as it is operating so that the operator can quickly determine the position of each component in the system. The use of sound further enhances the operator's awareness of system status by alerting him or her to alarms and other events during operation of the fuel handling equipment.

Screen Layout

The SUN color graphics monitor screen is subdivided into rectangular regions called viewports which allow portions of the screen to be updated independently from the rest of the screen. The layout of a typical screen is shown in Figure 3.

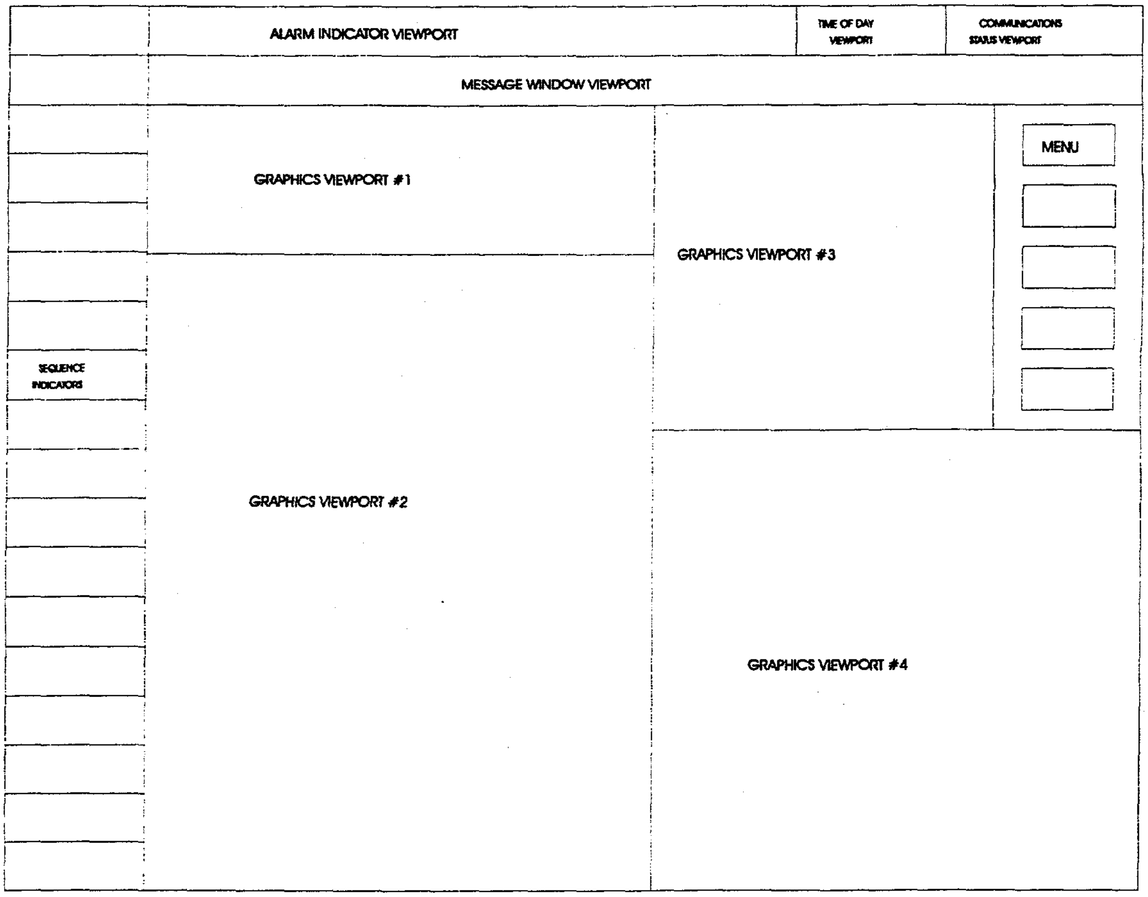

Figure 3: Viewport Layout

The screen is divided into the following viewports:

- **Graphics viewports:** Displays graphical information to the operator. Several different viewport areas are used for displaying plan and side view perspectives of the equipment as well as numerical and text format for sensor and operational data.

- **Menu viewport:** Used for manually selecting different views. The graphics viewports switch automatically to the appropriate view without operator intervention, but the menu viewport allows each view to be selected manually.

- **Time/date viewport:** Displays the current time and date to the nearest second. Besides providing time, the viewport gives an indication that the screen is updating -- if the time is not updating then the other viewports are not being updated.

- **Sequence pushbutton viewport:** Displays the status of each step in the current sequence. This viewport is for indication only. The actual pushbutton controls are located on the PanelView. However, since the PanelView can only show part of the sequence at a time, a sequence pushbutton viewport has been added to the SUN graphics screens to display the status of the entire sequence.

- **Alarm viewport:** Displays the status of alarms in the system. A blinking red alarm bar appears when new alarms have come in and need to be acknowledged.

- **Message viewport:** Displays alarm and status messages.

- **Communications viewport:** Displays the status of the communications with the PLC and A/D boards. The viewport is divided into two sections, one section shows the PLC communications status and the other section shows the A/D communications status. If no communication is received, then that section of the viewport is red. Normally the viewport sections are green.

All input and output signals to and from the PLC will be displayed on the graphics screens. This includes approximately 320 limit switch inputs and 145 digital outputs. In addition, 38 analog position signals will be displayed. In order to organize this large amount of information, multiple views must be created to subdivide the data into manageable chunks. The appropriate view will automatically appear when the operator pushes a button on the PanelView touchscreen. Information that is not needed at this point in the sequence will not be displayed. Some key information, however, is always available in dedicated viewports. This includes the alarm viewport, sequence pushbutton viewport, message window, time/date viewport, menu viewport, and position indicators for the major components. In addition, the operator may manually select any view he wishes to see.

Alarms

Alarms are indicated with both audible and visual indications. When an alarm is present in the system, the alarm bar located at the top of the SUN graphics screen will turn red and blink and an audible alarm signal will be played. The alarm message is displayed in a dedicated message window. The audible alarm is required to alert the operator when he is not looking at the screen. Once the alarm has been acknowledged, the audible alarm will cease and the alarm bar will stop blinking. However, until the conditions that caused the alarm are cleared, the alarm bar will stay red and the alarm message will remain displayed. The audible alarm will also cease if the conditions return to normal. If the alarm clears before it is acknowledged, the alarm bar will turn yellow indicating that the system is back to normal but still requires acknowledgement. In the case of multiple alarms, the message window indicates the next alarm as each previous alarm is acknowledged. The most recent unacknowledged alarm is always displayed in the message window. A screen may be selected by the operator which lists all of the past alarms, time and date of occurrence, their current status, and whether or not they have been acknowledged.

If the operator initiates an action which can not be performed because of an interlock, the cause of the problem will be displayed in the message window. Such messages are not necessarily classified as alarms and do not require acknowledgement. An example of this type of message would be alerting the operator that the emergency stop pushbutton is activated which is preventing the desired operation from taking place. However, if the prohibiting interlock is the result of a failure in the system, the cause of the problem will be displayed as an alarm.

The integrity of the limit switches is vital for the safe operation of the fuel-handling equipment. Therefore, whenever possible, the limit switch status is checked and alarms are set when a limit switch failure is detected. These checks are performed in various ways. One way is to compare the analog values within the range that a limit switch trip is expected. If the limit switch fails to trip within a specified range, a failure with the switch or with the interface to the switch has been detected and an alarm is set.

Another way limit switch integrity may be verified is by comparing the status of all the switches against a known set of states stored in a file for each step in the sequence. If any limit switch differs from the state specified in the file, an alarm is generated, alerting the operator to the failure before it becomes a problem.

Audio

The existing fuel handling console does not have audible alarms, which means that they occasionally go unnoticed for a period of time. The new system will have audible alarms to help the operator respond more quickly to abnormal events. In the new system, the SUN Sparcstation will be responsible for all alarm handling. Consequently, the audio port on the computer was chosen to generate the audio signal for the alarms. Because of the background noise present in the reactor building, an external amplification system is necessary to ensure that the alarm signal is loud enough to be heard. The SUN computer has an audio "line out" suitable for connecting to an external amplifier and speaker system.

In addition to alarms, there are other ways that sound may be used to enhance the operator's awareness of system status. For example, in the current system, an operator is able to tell that an event has occurred by the sound of the mechanical relays without even looking at the console. Various sound effects may be used to create a multimedia type operator interface by playing an appropriate sound whenever an important event occurs.

Analog Signals

All analog signals will interface with Analog-to-Digital (A/D) boards located in the SBUS of the SUN Sparcstation computer. These signals are digitized and stored in memory where they are digitally filtered and then displayed to the operator on the graphics screens. Animated graphics based on the analog signals are updated approximately 10 times per second while the digital readouts are updated 2 times per second to make them easier to read.

Three 16-channel analog boards will be located in the SUN computer allowing up to 48 analog signals to be interfaced with the system. The A/D boards are 16-bit, 16 channel, fully differential A/D converters which interface with -5 to +5 volt inputs. Each board contains an A/D with a sample rate of 166 KHz, which allows a throughput of over 100 thousand samples per second per channel. Analog signal conditioning modules isolate the signal from the computer in order to protect the computer A/D boards from voltage spikes.

Calibration

All analog signals will be calibrated in software. Some will be calibrated automatically and others will require the technician to initiate the calibration. Automatic calibration is performed using the limit switch inputs for zero and span points. A check will be made to verify that the calibration point is within a certain tolerance so that a failed limit switch can not invalidate the calibration. This allows the analog signals to also be a check for the correct operation of the limit switches by generating an alarm if a limit switch fails to trip at a certain point. Signals that require manual verification of mechanical position during calibration will be calibrated by a qualified maintenance technician using special calibration screens which will be password protected.

Silicon Graphics 3D Graphics Computer

Because the liquid sodium in the EBR-II primary tank prevents direct observation of fuel handling operations, a three-dimensional (3D) visualization technique has been developed to simulate direct visual observation of the transfers of fuel and experiments into and out of the reactor.

A detailed 3D computer model of the major components located within the primary tank was first created from the original construction drawings and as-built dimensions taken before the tank was filled with sodium. (See Figure 4). Dynamic behavior of the moving components was then incorporated into the model by creating links to database elements that define the translational and rotational movements of each component. A Silicon Graphics Indigo2 workstation is being used to display the three dimensional model. The model can be updated in realtime with analog data sent from the SUN workstation to the SGI 3D graphics computer via ethernet.

Ethernet Communications

A small local area network (LAN) will be installed in the reactor building to interconnect all of the computer systems and the PLC. Figure 5 shows a diagram of the network and the systems that are connected to it. Ethernet was chosen over other communication links such as serial RS-232 because of its high throughput (10 million bits per second) and because it is a standard interface which all of the systems support.

Software will be written to allow the SUN Sparcstation to receive data from the PLC over the network using Allen-Bradley's Interchange^{TM} software. The Interchange software is an Application Programming Interface (API) for the C language on the SUN Sparcstation. This allows a C program to make function calls to a driver supplied by Allen-Bradley which communicates with the PLC over ethernet. All of the I/O associated with the PLC will be transferred from the PLC to the SUN for updating the graphics screens.

Another benefit of the ethernet network is that it will support the use of an X-Terminal located away from the SUN computer. This allows a graphics terminal to be placed in another location without requiring another computer to drive it. The X-Terminal is driven by the SUN Sparcstation located in the main console. All of the graphics on the main console will also be available on the X-Terminal. The X-Terminal has its own trackball and will be programmed so that the screens can be selected independently from the main console screen. This way, the screen selected on the X-Terminal may be different than the screen selected on the main console.

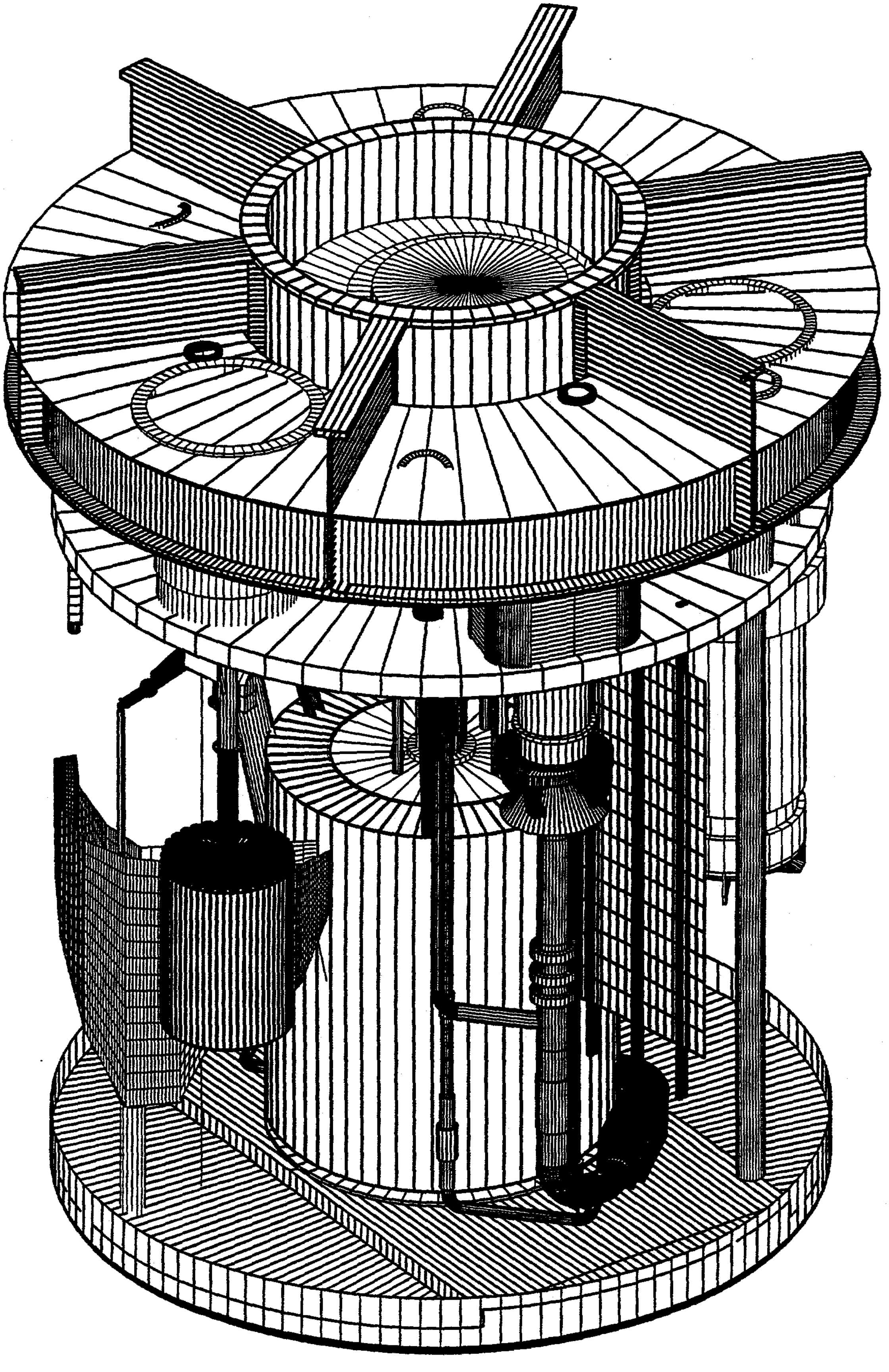

Figure 4: 3D computer model of EBR-II primary tank.

Software

The software running on the SUN Sparcstation will be divided into multiple processes sharing a common memory segment for interprocess communication. Each process will run independently from the other processes but will be capable of communicating with any other process via the shared memory area. Breaking the software into multiple processes makes the software easier to develop and maintain than it would be if it were written as one huge monolithic chunk of code. The code is broken up according to logical function which makes it more manageable. Following is a list of processes (or tasks) that are envisioned for this project.

Creator Task - This is the initialization task which creates the shared memory area, forks all of the other processes, and then monitors the process status to verify that all of the processes remain running.

Operator interface task - This task handles all of the screen updates and graphical functions required by the DataViews software. Graphical screen elements are tied to the shared memory area and update according to the data that is placed there by other processes. This task also handles operator menu selections, screen changes, and input, as well as the X-Terminal setup and display.

PLC communications task - This task will use the Interchange programming interface to receive digital I/O data from the PLC. After receiving and extracting the data, it will place it in the shared memory segment for other processes to use.

Analog data interface task - This task will initialize the A/D boards in the computer backplane and then read analog data from them. The data will be digitally filtered and then placed in the shared memory segment for other processes to use.

Alarm Handler - This task will analyze the shared memory data for abnormal situations and generate alarms when a discrepancy is detected. It will check limit switches for correct status and compare them with the analog data for consistency. When an alarming event is detected it will place the appropriate alarm message in the message window variable.

Data logging task - This task logs software/hardware error messages, normal system operational messages, and selected process data to files on the hard disk. The error message files can be used to help pin point malfunction or processing problems. The operational message files can be used to verify proper system operation and to assist in solving operational problems. The process data logging can be used for surveillance and troubleshooting.

Audio Task - This task looks at the shared memory area and when an alarm or other audio event occurs, sends the appropriate audio data to the audio port. On startup, the task initializes the port and then waits for an audio event to occur.

3D Graphics Interface Task - This task takes the data needed by the SGI 3D software from shared memory and puts it in the socket for ethernet communication to the SGI computer.

Data Communications

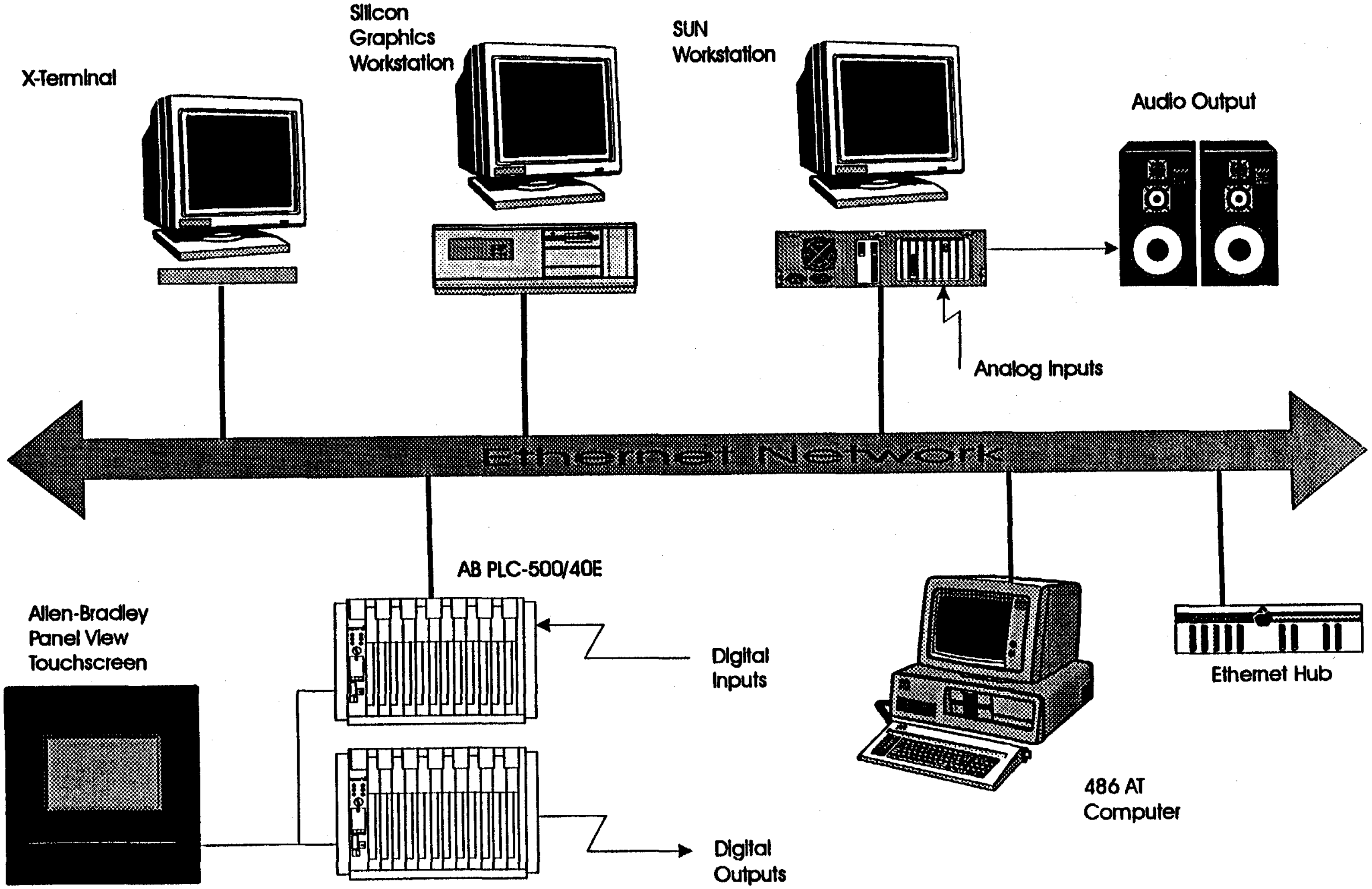

Figure 5: Ethernet Data Communications.

SIMULATION AND TESTING

Simulation software which models the fuel handling equipment controlled by the PLC will be written. This tool will be used to simulate system operation before it's brought on line. The simulator will use a software model of the plant to verify the control logic for debugging and safety reasons. The simulation software will read output data from the PLC's output data table and simulate the behavior of the actual fuel-handling equipment. As a piece of equipment, such as the storage basket or the gripper, moves within the simulation, sensors such as limit switches and potentiometers will be simulated. These generate feedback data about the position of the equipment which is then written back into the input data tables of the PLC. In this way, the PLC reacts as if it were connected to, and getting feedback from the actual equipment. At the same time, a graphical representation of the fuel-handling system will be linked to the database table of the PLC so the values in the database can be observed on the screen--both as numerical values and as animated behavior of the graphical images. These are the same screens that will be used to monitor plant behavior during operation. The user will also be able to set up operating scenarios to test the PLC and characterize plant operation before connecting the controller to actual equipment. This will allow the control system to be tested more thoroughly than would be possible once the system is installed.

CONCLUSION

The fuel handling console upgrade is a state-of-the-art control system design which makes use of the latest technologies including advanced PLC control and diagnostics software, 3D computer graphics, multimedia operator interfaces, and high-speed ethernet communications. Simulation software allows the new system to be thoroughly tested before it is installed in the plant. In addition, fault tree analysis has been used to create a fail safe design.

DISCLAIMER

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