CONF-881017--1

REMOTE CONTROL SYSTEM FOR A 2-MW RESEARCH REACTOR

R. E. Battle and G. K. Corbett
Instrumentation and Controls Division
Oak Ridge National Laboratory*

CONF-881017--1

DE88 011853

DISCLAIMER

Paper to be presented to the
IEEE Conference-23rd Annual Meeting
Pittsburgh, PA
October 2-6, 1988

*Operated by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under Contract No. DE-AC05-84OR21400.

REMOTE CONTROL SYSTEM FOR A 2-MW RESEARCH REACTOR

R. E. Battle and G. K. Corbett
Instrumentation and Controls Division
Oak Ridge National Laboratory
Building 3500
Oak Ridge, Tennessee 37831-6005

Abstract: A fault-tolerant programmable logic controller (PLC) and operator workstations have been programmed to replace the hard-wired relay control system in the 2-MW Bulk Shielding Reactor at Oak Ridge National Laboratory. In addition to the PLC and remote and local operator workstations, auxiliary systems include a video system, an intercom system, and a fiber optic communication system. The equipment has been designed with reliability and fail-safe features as important considerations. Significant features of the systems are described.

Introduction

This paper describes a digital remote control system to be installed in the Bulk Shielding Reactor (BSR) at the Oak Ridge National Laboratory (ORNL). The present reactor control system consists of a control panel with hard-wired connections to relays and control modules. The new control system consists of a triple-modular-redundant programmable logic controller (PLC) that will replace the relays and control modules, operator workstations that will replace the control panel, and audio and video systems to provide alternative means to obtain reactor status information. In a sense, all reactors are controlled remotely, but because of the increased distance to the BSR remote station (2.5 km), fail-safe features not normally used have been included in the BSR control system.

A digital control system was selected for several reasons, one of the more important being to limit the number of wires between the remote station and the BSR. A PLC satisfies this requirement because it can communicate to a workstation over one full-duplex channel, whereas many wires would be needed to connect a comparable system with switches and relays. Additional channels of information to the remote station have been included for diversity and redundancy. Other benefits of a PLC are that the system logic to be used can be designed and tested prior to installation. Likewise, operator training on the actual equipment to be used can be done prior to installation without the expense of an extensive training simulator. Disadvantages of using a PLC and computer workstations are that all the information is not immediately available to the operators as it would be on a full control panel, and there is a delay in updating the information displayed to the operators. However, because the BSR requires few operator actions during normal operation and because normal and emergency operation is simple, these disadvantages are acceptable. A fiber optic communications system was selected because it can transmit wideband video, data, and audio between the BSR and the remote station without repeaters. Fail-safe features have been designed into the system to trip the reactor if communications fail.

System Overview

The BSR is a 2-MW, pool-type research reactor used mostly by physicists studying superconducting material in a neutron flux.[1] The reactor is unpressurized, and the core exit water temperature is less than 125°F. Primary coolant flow is constant, but secondary coolant flow is regulated to maintain constant temperature at the heat exchanger primary coolant outlet. Thermal power is rejected to the pool and to water-to-air cooling towers. The reactor power level is controlled by positioning six shim rods during startup. When power is above 5%, one of the shim rods is regulated by a servomechanism to control the neutron flux at a set point. The reactor protection system, which is independent of the control system, protects the reactor against overpower. It has three channels arranged in 2-of-3 logic to trip the reactor. If two channels trip, the shim rods are inserted to shut down the reactor by interrupting current to the shim rod holding magnets.

The primary purposes of the new control system are to reduce operating costs and improve reactor reliability. Until recently the BSR was operated remotely from the nearby Oak Ridge Research Reactor (ORR), which was shut down in 1987. However, the remote system from the ORR had few capabilities: The remote operators could monitor the reactor over a closed-circuit television, perform minor shim rod adjustments, and shut down the reactor. Because the operating staff of the two reactors can no longer be shared, a new remote control system will be installed to share staff between the BSR and the High Flux Isotope Reactor (HFIR).

The previous remote control system was located 100 m from the BSR, but the new remote station at the HFIR is 2.5 km away. Because of this distance, the new control system includes fail-safe features and redundancy that were not in the old system. These features, outlined in Table 1, were designed into the remote control system to assure that the operators can monitor reactor conditions and that the reactor will shut down if a channel of control or monitoring fails. One of the more important safety features is the reactor itself--it does not require any active systems after it is shut down, as natural convection flow is adequate to cool the core.

The remote control system uses a fault-tolerant PLC, operator workstations, audio and video equipment, and fiber optic communication equipment. A block diagram of the equipment interconnection is shown in Fig. 1. The new control system is functionally similar to the present system, but implementation is different. Controls, displays, and indicators are in a video monitor and keyboard rather than in panel-mounted equipment. High-resolution cameras with pan, tilt, and zoom controls at the HFIR provide the remote operator with visual information of the BSR control room and reactor pool area. An intercom from the HFIR control room to the BSR is included to aid operation. A fiber optic system that multiplexes video, audio, and data provides communications between the two sites.

Safety Monitor and Fail-Safe Features

The heart of the remote control system is a triple-modular-redundant (TMR), fault-tolerant PLC manufactured by the Triconex Corporation. There are three independent channels from the PLC inputs to its outputs with 2-of-3 voting and a monitor to annunciate module failures. Communications to the operators' workstations are not redundant, but data transmitted between the PLC and the workstations are

Table 1. A Summary of Safety Features

Specification	Description of safety enhancement
Triple-modular-redundant PLC	Redundancy in the PLC implements reactor control without faults despite any single hardware failure.
Workstation control	Only the station selected by a remote/local switch can control the reactor. The other station can monitor only.
Limited shim rod manual control	During normal operation manual control of the shim rods from either workstation is limited to prevent a system disturbance caused by erroneous data entry.
Communication watchdog timer	Communications monitors in the PLC and each workstation ensure reactor shutdown and annunciation if the controlling workstation loses communication with the PLC.
Redundant remote shutdown	Fiber optic and telephone line channels transmit remote reactor shutdown signals over separate and diverse communication channels.
Shim rod seat switch monitors	Shim rod seat status can be verified via the workstation, closed-circuit TV, or a separate battery-backed system that communicates over telephone lines.
Independent control and protection	Isolation of the protection system reduces the probability of common-cause failure of control and protection.
Diverse information displays	Displays of reactor parameters on a workstation, closed-circuit TV, and on panel meters connected by telephone lines ensure the operators have valid information.
Redundant audio communication	Intercom (including PA), telephone, and radio ensure communication with a local operator monitoring the BSR and other facilities nearby.

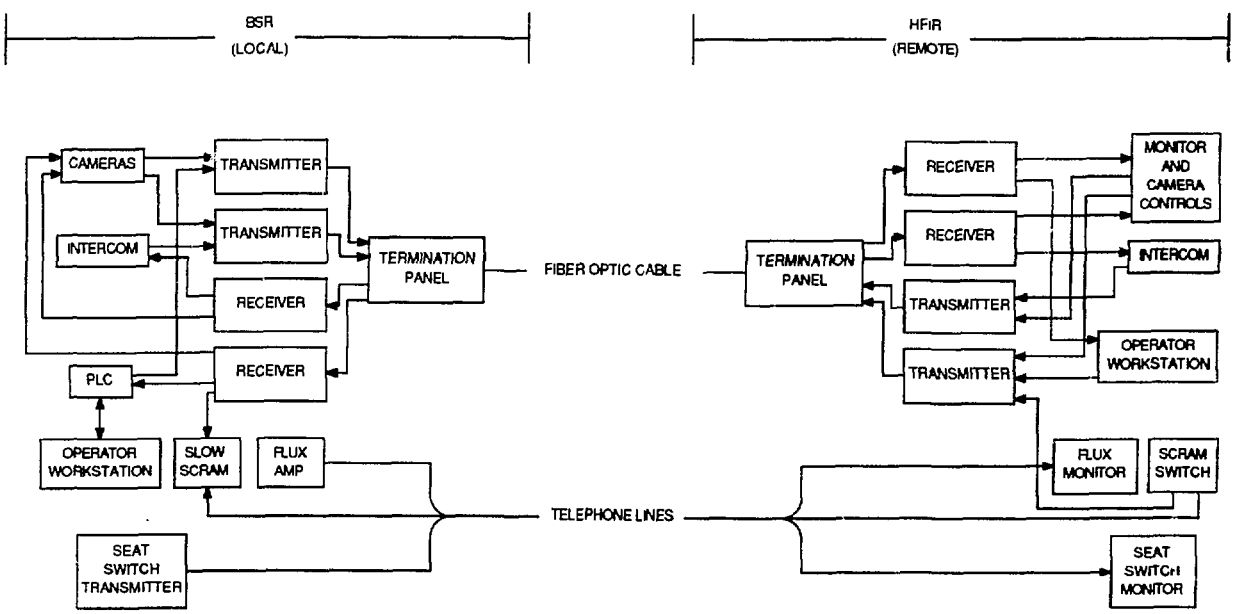

Fig. 1. BSR remote control system.

tested for accuracy with a "checksum" algorithm. If a "checksum" test indicates incorrect data have been received, the data are retransmitted before the PLC performs actions based on the instruction. There is no single component failure in the PLC that will cause it to implement the control logic improperly. The communications module is not redundant, but if it fails the PLC will continue to function without operator control until a "watchdog timer" (described below) trips the reactor. Failed components in the PLC are alarmed on the front panel of the PLC and in the operator workstation.

The PLC software also has features designed to avoid spurious challenges of the reactor protection system. One such feature prevents contention between the local and remote control stations. Because control signals can be generated at both the HFIR and the BSR, the PLC logic is designed such that action is performed only on signals originating from the site selected to control the reactor. Both the remote and local sites have separate driver points so that the PLC can identify and prevent simultaneous or contradictory requests from the two workstations. The local or remote control is selected with a switch in the BSR control room. Operator requests made from the remote station when local control is selected, or vice versa, are blocked.

Another protective feature of the system prohibits excessive rod movement caused by entering incorrect rod withdrawal information. The present rod control at the BSR uses toggle switches. These switches would have to be pushed forward for a relatively long time to withdraw the shim rods a large distance. However, with the new workstation, rods can be moved by entering a number on a keypad. If a decimal point were misplaced, a rod could move farther than the operator intended and thus cause a system disturbance. For this reason, rod movements requested from the keypads are limited to small increments except for conditions such as reactor startup or shutdown. Small increments are adequate for most situations, but for special situations, toggle switches can be used to manipulate the shim rods. One reason an operator would adjust the shim rods during operation is to balance the rods to cause an equal flux distribution across the core. For this purpose, a routine has been installed in the control system to balance the shim rods automatically by operator request.

The new remote control system is 2.5 km from the BSR, and the communications cables connecting the BSR and the HFIR are aerial cables. Fail-safe and redundant shutdown features are included to avoid control system malfunction caused by communications failure. A "watchdog timer" in the PLC receives a reset signal from each workstation which automatically restarts the timer at zero. If a timer is not reset within a few seconds, the control system will either shut down the reactor or annunciate on the active station that the inactive workstation communication has failed. The reactor is shut down only if the controlling station loses communication with the PLC.

The remote station has two redundant and diverse channels to manually shut down the reactor in the event of an emergency. One channel uses an optical fiber and the other uses telephone lines which are on a separate right of way. The optical channel transmits a tone that maintains a relay energized. If the tone is interrupted, the relay deenergizes and the reactor trips. The other channel uses a current loop to keep a different relay energized. If the current loop is interrupted, this relay is deenergized and the reactor trips. To deenergize both trip relays, the manual shutdown switch breaks the tone and the current loop. The fail-safe manual trip also protects against the most likely failures of cable damage or loss of power. Damage to either channel is sufficient to shut down the reactor if it is controlled from the remote location.

Because of the importance of confirming that the shim rods are seated, the seat switches are monitored via the workstations, the control room camera and monitor, and a system using telephone lines. Contacts from the six shim rod seat switch relays and a system monitor signal are inputs to a parallel-to-serial data transmitter that sends the seat switch data over telephone lines to the HFIR. The serial data are converted to parallel data to drive indicator lamps at the remote station. The system monitor consists of an astable vibrator at the BSR that switches the monitor lamp on and off. The blinking monitor indicates that the system is functioning. This seat switch indicator system is battery-backed so that operators can confirm the rods are seated if normal ac power fails. The battery has an undervoltage monitor that is alarmed through the PLC.

The most important safety system is the reactor protection system. This system is independent of the control system and will continue to function regardless of the condition of the control system. Signals passed between the protection system and the control system are isolated either optically or magnetically such that any failure in the control system will not cause the protection system to fail. The protection system is designed to continue to function after a single failure.

Programming the PLC

The relay ladder logic was written on an IBM/AT compatible computer and downloaded to the PLC for testing. The majority of the ladder logic program duplicates relay functions that will be replaced by the new control system. These functions include automatic startup, protection channel testing, fission chamber control, withdrawal and insertion of shim rods, alarm annunciation, and automatic initiation of power reduction modes. The fault-tolerant PLC will also perform servo control based on logic programmed in a Modicon PLC presently performing neutron flux regulation. The Triconex PLC can be programmed in BASIC as well as in ladder logic. BASIC was used to program control functions such as automatically balancing rods, positioning movable limit switches, and calculating set points to follow an exponential curve.

The PLC has 94 digital outputs, 127 digital inputs, and 71 analog inputs which are scanned every 120 ms. Each data point is configured and stored for program reference in the data dictionary. The relay ladder logic refers to the data point name, a seven-letter mnemonic, rather than the standard MODBUS number code. This makes the ladder logic program much easier to read because the relay's function is implied by its mnemonic. In addition, various functions are labeled as a group and can be searched for by simple names such as start, run, or servo. Every network in the PLC has comments embedded that describe the function and action that will occur if all permissives in the network are satisfied.

To verify the program code, the ladder logic was checked against a logic diagram of control, a sample of which is in Fig. 2. Software tests were conducted using an emulator that is part of the PLC programming system. The emulation mode displays in green the lines of logic that permit power flow and in red

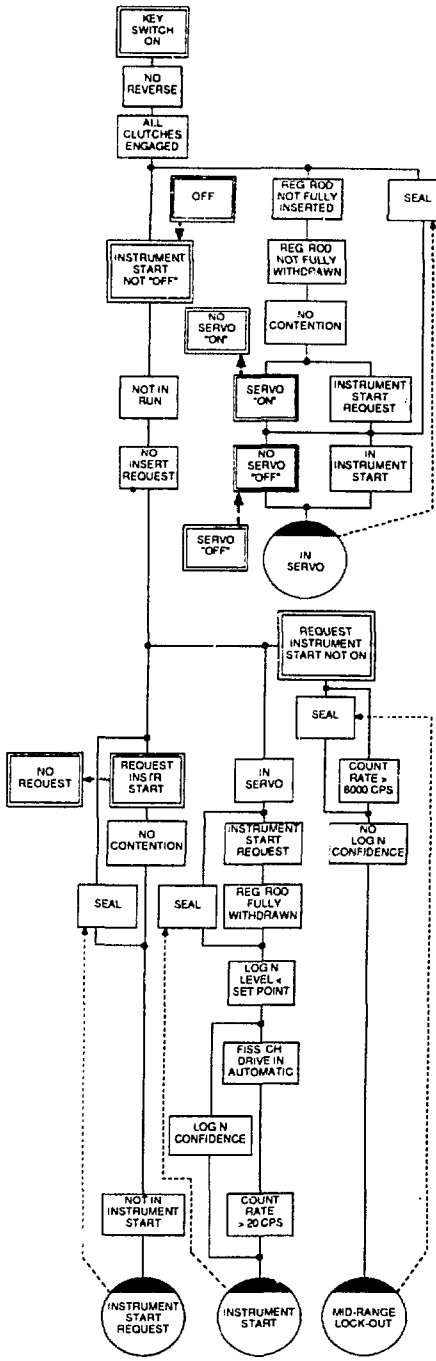

Fig. 2. Sample of logic diagram of control system.

those lines that block power flow. This facilitates debugging the control program. The control logic can run either single scan or continuous scan. Final tests were done by using toggle switches and adjustable voltages as discrete and analog inputs. These simulated input signals were adjusted to establish a desired operating condition, and the system operation was evaluated for each of these conditions. Block diagrams showing the flow of information were used to verify that the controller functioned properly.

Operator Workstations

Reactor operators will control the reactor from one of two identical workstations, each consisting of a special-purpose computer, color monitor, and membrane keyboard. The remote workstation in the HFIR control room and local workstation in the BSR control room are identical except that the station selected for control by a remote/local switch will be the active control station. The station not selected can monitor only. The functions available on the workstations are display and control of discrete and analog parameters in the PLC, page select, and alarm display and acknowledgement. Access for adjustment and display of analog or discrete points is dependent on which graphics page is displayed. Printers at each workstation document reactor status hourly or on demand.

Graphic pages can be selected with one or two keystrokes, and appear in about 1 s. There are five graphic pages available to the BSR operators, titled at the top as follows: (1) NUCLEAR SYSTEMS RUN, (2) NUCLEAR SYSTEMS STARTUP, (3) PRIMARY AND SECONDARY PROCESS, (4) PROTECTION SYSTEM, and (5) EMERGENCY. The functions of these pages are described below.

The page used most during operation is page 1, NUCLEAR SYSTEMS RUN, which can be accessed with one stroke of a dedicated key. This page is shown in Fig. 3. Displays and controls of the analog and discrete points needed for operation at full power are available on this page.

Reactor startup controls and displays are on page 2, accessed by two keystrokes from any page or by a "page-up" key from page 1. Displays and controls are similar to the first page except that a few of the "run" discrete permissive displays and controls are replaced with startup information.

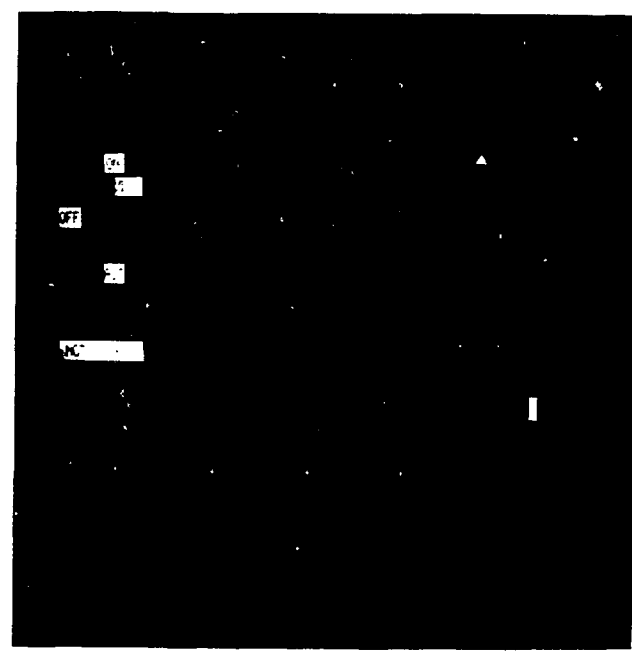

Fig. 3. Nuclear systems run screen.

A mimic of the primary and secondary coolant systems and associated subsystems on page 3 is shown in Fig. 4. On the mimic, positions of digital displays for measured parameters correspond to actual locations of sensors in the BSR. For instance, a pool temperature on the screen is displayed inside the picture of the pool. Decay tank water level is shown numerically and graphically with a mimic of a tank, and pump status is shown with graphics and text.

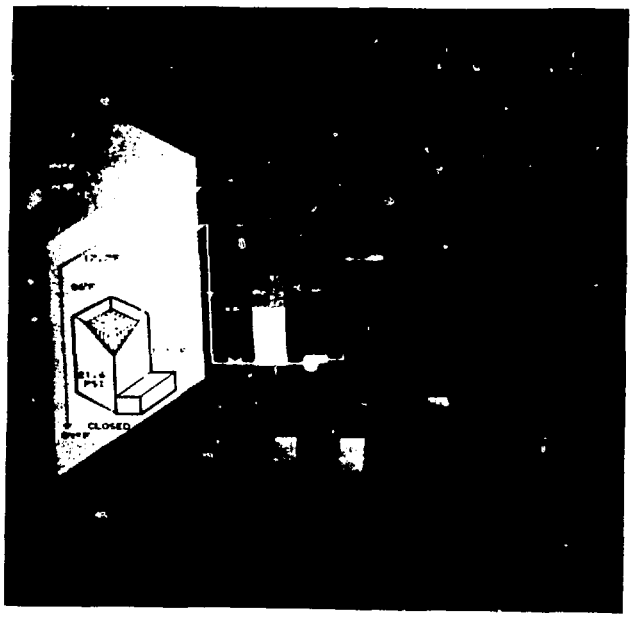

Fig. 4. Primary and secondary process screen.

A mimic of the four protection system chassis and modules is on page 4. When the magnets are deenergized, the control rods drop into the core. Indicator lamps on this chassis inform the operators of the presence or absence of magnet current. On this page, operators can test each channel separately on-line, observe the trip status of each module, and see the signal level displayed at which a channel trip, reverse, and setback occur. Reverse and setback are PLC-initiated power reduction functions which prevent unnecessary reactor trips. Startup tests of the protection system can be performed from this page by withdrawing one or all of the shim rods a few inches, tripping two channels, and confirming that the rods insert to their seats.

A page entitled EMERGENCY contains displays and controls that operators may need during an emergency. This page is divided into five sections as follows: shim rod seat indicators, containment radiation displays, containment controls, primary coolant and off-gas displays, and area temperatures and wind conditions. The single most important indicator is the shim rod seat status indicator. Seat indication is available on the workstation, a separate video camera system, and on a battery-backed system described later. Once the rods are seated, no active systems are required to cool the core. Containment and building evacuation manual controls are provided on the emergency page; there are also automatic containment and evacuation actuators independent of the control system. Radiation levels in the coolant and off-gas systems are displayed on this page.

Sixty conditions are alarmed in the new control system. The operator workstation replaces the annunciator panels with video displays of these alarms. At the bottom of each graphic page is space dedicated for three alarms. Unacknowledged alarms are displayed in this area in the order of occurrence, and additional alarms are displayed on an alarm page. To assist with alarm monitoring, a printer records the occurrence, acknowledgement, and clearing of each alarm. Acknowledged but uncleared alarms do not appear in the alarm area at the bottom of each page, but they do remain on the alarm page.

Reports are generated by a BASIC program running continuously in the operator workstation. This program prints hourly or upon demand from the operator.

Training

Operator training is an important aspect of the new control system. Because the method of control is changed radically, operators must receive extensive training. Training will begin by having reactor supervisors review and comment on the system. The operating manual will be modified for the new system, and operators must become familiar with it. Classes held to describe the system and provide hands-on training will permit operators to use the actual BSR control system before it is installed in the BSR. After classroom training is complete, the control system will be installed and the reactor operated from the local station. After operators are comfortable with operation from the local station, remote operation will proceed. Because remote and local operation are identical, the change to remote operation should not be difficult.

Human Factors

The graphics are designed, in accordance with human factors guidelines,[2] as follows:

1. There are seven or fewer colors on a page.

2. A dedicated area on each page is reserved for alarms.

3. Colors associated with displays are consistent on all pages (except when they appear on a mimic page).

4. Locations of displays are consistent on all pages (except when they appear on a mimic page).

5. Information needed most frequently and most rapidly is on page 1 and can be displayed with one keystroke. A page is displayed about 1 s after the keystroke.

6. Bar charts are used for data that are frequently compared.

7. Mimics of the process and instrument panels are used to enhance the speed of comprehending information.

8. Operators reviewed the graphics during system development. Their suggestions helped with the design and should ease the transition to the new system.

Auxiliary Systems

Auxiliary systems for remote operators include the following: video system to monitor the BSR control room and reactor bay; intercom system from the HFIR control room to the BSR control room, reactor bridge, experiment control room, and BSR public address system; and fiber optic communication system. A block diagram of these auxiliary systems and their interconnections is shown in Fig. 1.

The video system consists of high-resolution color monitors and cameras with pan, tilt, zoom, and focus controls. A camera in the control room provides the remote operator a redundant means of viewing recorders and indicators, including the shim rod seat lamps. An operator can zoom in and examine a recorder closely or zoom out and see several recorders simultaneously. All the information available to operators on the control room camera is also available on the operator workstation, but the camera provides a redundant means of checking the information. The camera in the reactor bay is used to survey the BSR pool and the reactor core. The camera can zoom in to inspect the reactor core, or it can zoom out to survey the pool area. Both of the cameras have 510 lines of resolution, which provides high-quality video to the HFIR control room. The video signals are transmitted over the fiber optic communication system.

The intercom system is provided to assist with operation and maintenance of the reactor. A remote operator can communicate to the roving operator at the BSR over the intercom or PA system. The HFIR control room is the master and the remaining stations are slaves. Because there are no wires to perform switching, calling is done using dual-tone multifrequency (DTMF) code. The audio is transmitted on subcarriers of the fiber optic communication system.

The fiber optic system between the BSR and the HFIR consists of an eight-fiber cable and terminal equipment with two communications channels in each direction. There are four spare fibers in the cable. Each channel can transmit a video signal, two data signals, and an audio signal, but all signals are not used in every channel. The video signal is wideband video (8.1 MHz). Audio and data are modulated onto subcarriers prior to conversion to optical signals. The optical transmitters use lasers operating at a 830-nm wavelength and 0-dB output. Optical losses are nominally 3 dB/km for the fibers plus 4 dB for splices and connectors, which results in approximately a 12-dB loss per fiber. The received signal is -12 dB; the receiver sensitivity is -30 dB for a 67-dB signal-to-noise ratio. The fiber transmitters and receivers have dual power supplies, one of which is adequate to operate the equipment. Failure of either power supply is alarmed through the PLC to the operator workstation.

Summary

A control system has been designed for remote or local operation of the Bulk Shielding Reactor (BSR). Remote operation is from the High Flux Isotope Reactor 2.5 km from the BSR. The control system consists of a programmable logic controller, operator workstations, and auxiliary equipment that provide redundant and diverse channels for operation of the reactor. The PLC is designed with triple-modular-redundancy to enhance its reliability over that of a single-channel PLC and to maintain reactor control if a single failure occurs. Fail-safe features, including a "watchdog timer" in the PLC, trip the reactor if communication to a workstation fails, and normally energized relays also trip the reactor upon loss of signal. However, the PLC and fail-safe features are not part of the reactor protection system. If the control system fails and causes a reactor excursion, an independent protection system will shut down the reactor.

The new control system is functionally similar to the old system, but displays and controls for the operators are different. The graphics have been designed with mimics of the process and of existing instruments to help operators adjust to the new system. Operator training will be done by simulating reactor conditions and having operators perform control as they would for actual operation.

The previous remote control of the BSR was limited to system monitoring and minor controls. The remote station was only 0.1 km from the BSR, and it was connected to the BSR control room with many cables for annunciation, cameras and camera controls, manual shutdown switch, and controls to reduce power only. Now, the new remote control system has identical control capabilities at both the remote and local stations. The capabilities of the remote station were expanded to match those at the local station because the increased distance makes it more difficult to go to the control room to make minor adjustments. The upgraded equipment will provide more information and control capabilities, and, because of redundancy in the system, reliability should be improved. Experience gathered from remote control of the BSR may supply useful information for the design of other reactors that require full remote control capability, such as space reactors or underground reactors.

References

1. A. E. G. Bates, "Description of the BSR 2 MW Reactor Control and Instrument Systems," ORNL-TM-2400, Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory, October 1, 1968.

2. P. R. Frey and W. H. Sides, Jr., "Computer-Generated Display System Guidelines, Volume 1: Display Design," EPRI NP-3701, Vol. 1, Palo Alto, Calif., September 1984.