CONF-881103--13

DE89 002349

DIGITAL, REMOTE CONTROL SYSTEM FOR A 2-MW RESEARCH REACTOR

R. E. Battle
G. K. Corbett

Oak Ridge National Laboratory*
P.O. Box 2008
Oak Ridge, TN 37831-6008

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 (BSR) at Oak Ridge National Laboratory. In addition to the PLC and remote and local operator workstations, auxiliary systems for remote operation include a video system, an intercom system, and a fiber optic communication system. The remote control station, located at the High Flux Isotope Reactor 2.5 km from the BSR, has the capability of reactor startup and power control. The system was designed with reliability and fail-safe features as important considerations.

Introduction

This paper describes a digital control system for local and remote control of the Bulk Shielding Reactor (BSR) at the Oak Ridge National Laboratory (ORNL). The digital control system consists of a triple-modular-redundant programmable logic controller (PLC) to replace the electromechanical relays and switches, operator workstations to replace the panel controls and displays, and audio and video systems to provide alternate means to obtain reactor status information. The remote control station can start up and adjust reactor power after the primary and secondary cooling systems are started locally. The local control station will be in the present BSR control room, and the remote station will be in the High Flux Isotope Reactor (HFIR) control room ~2.5 km from the BSR. Communication between the BSR and the remote station is over a fiber optic cable and copper wires. A block diagram of the control system, the equipment interconnections, and the redundant communications paths are shown in Fig. 1. All signals transmittad over the leased lines are also available on the workstations via the PLC.

The primary purposes of the new control system are to lower operating costs by reducing the number of operators needed for the BSR, to provide a highly reliable system, and to ensure safe operation. This system also provides opportunities for research, development, and testing of fault-tolerant control, remote control technology, and operator interfacing with visual display units (VDUs). A requirement for the new control system is to provide simple, automatic controls, and to provide the operators with the information and capability to interrupt the automatic systems and take over manually, or to shut down the reactor if necessary. To meet the design requirements, the control system must perform reliably and safely and be acceptable to the operators. However, the protection system is isolated from the control system so that the reactor remains protected after any failure in either the control system or its communications links. This paper describes

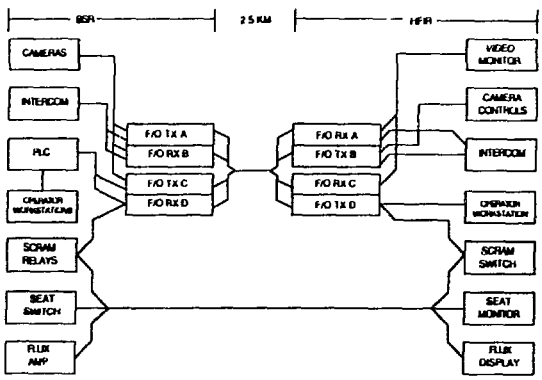

Fig. 1. Block diagram of BSR remote control system.

reliability and fail-safe features of the remote control system and human factors considerations for a digital control system for the BSR.

Until 1987, the BSR was operated remotely from the Oak Ridge Research Reactor (ORR), which is a 30-MW reactor located in a building adjacent to the BSR. The remote control station at the ORR included a scram switch, two video channels for monitoring, and limited shim rod and servo control. The BSR and the ORR shared operating staff, this arrangement being most beneficial to the smaller BSR. The ORR was shut down permanently in 1987. To keep BSR costs down, a decision was made to control it remotely from the HFIR. Because the HFIR is much farther from the BSR than the ORR and because installing a new remote control system involves reevaluating remote operation, the new design will have fail-safe and reliability features not included in the older system. The new remote control system must also be economical for the experimenters. The cost of remote operation depends on the number of operators who will be funded from the BSR account. Because BSR and HFIR operators will be shared, the funds for them will be prorated from the BSR and HFIR accounts. Because of the uncertainty of operating staff requirements at this time, this paper does not include a cost-benefit analysis, but it does describe design features that improve reliability and safety of operation.

System Overview

The BSR is a 2-MW pool-type research reactor[1] used mostly for irradiation damage studies. The most recently installed facility, the Low-Temperature Neutron Irradiation Facility, will be used to study superconducting material in a neutron flux. The reactor is unpressurized, and the core exit water temperature is <125°F. Primary coolant flow is constant, but secondary coolant flow is regulated to maintain constant temperature at the heat exchanger

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

primary coolant outlet. Thermal power is rejected to the reactor pool and to water-to-air cooling towers. It has six shim-safety rods, one of which also serves as the servo regulating rod. The reactor protection system now has three flux level channels arranged in 1-of-3 trip logic. Before installing the remote control system, the protection system will be modified to interface with the new control system through isolation devices. The new reactor protection system, which is isolated from the control system, has three channels arranged in 2-of-3 trip logic. The reactor trip function is independent of the control system. If two channels trip, all six shim rods are inserted by interrupting current to the shim rod holding magnets. The protection system also has setback and reverse contacts connected to the PLC through isolation devices to attempt to reduce reactor power to avoid a trip. Forced coolant flow is required for 2-MW operation, but natural convection flow is adequate to cool the core after it is shut down. No active systems are required to maintain fuel integrity after the reactor has been shut down. The reactor has some inherent safety features that have been verified by experiment. BSR fuel elements have been tested in the Short Period Experiment Reactor Test (SPERT) facility. These tests determined that the core could be put on a 14-ms positive period with the safety system defeated, and the power would be limited by self-shutdown with only slight damage to the fuel elements.[2] However, the minimum period that would occur during a startup run-away accident is 48 ms. Test results from the SPERT facility demonstrated that such an accident would not result in fuel damage.[3]

Fail-Safe Features

The likelihood of challenges to the protection system is reduced by designing a reliable control system with redundancy, diversity, and independence. Fail-safe features to protect against the most likely failures were designed into the control system such that the reactor will shut down if one of these anticipated failures does occur.

System reliability and fault tolerance are achieved by using a triple-modular-redundant (TMR) PLC that has three separate channels from input terminal to output terminal. A single failure is masked by a 2-of-3 vote among the three channels of the PLC, but the failure is annunciated by diagnostics software. Channel and module failures in the PLC are indicated by alarms on the front panel of the PLC and in the operator workstation. A failed module can be replaced without interrupting normal operation. Data transmitted between the workstation and the PLC are tested for accuracy with a "checksum" algorithm. If a "checksum" test indicates that incorrect data have been received, the PLC indicates to the workstation that bad data were received, and the data are retransmitted automatically. The PLC then performs actions based on the retransmitted correct instruction. In the PLC, no single component failure will cause it to implement the control logic improperly. However, the communication modules in the PLC and the connections to the workstations are not redundant. Therefore, a software watchdog timer was developed to monitor communications. If communications between the controlling workstation and the PLC fail, the PLC will continue to function based on the last instruction from the operator until the fail-safe "watchdog timer" trips the reactor.

Redundancy is not provided in the software. However, most of the PLC logic is based on the present control logic. Because the control logic is unchanged from the present and because the PLC is programmed in ladder logic with relays and coils, the PLC software is based on existing elementary diagrams. This fact simplifies programming the PLC and provides a means to verify the PLC logic. Simulated signals also were used to test the PLC and workstation.

The primary communications to the remote workstation are over fiber optic transmitters and receivers, each of which has two full-capacity power supplies on separate circuits to provide redundancy of power. Failure of a single circuit or failure of one power supply will not affect communications. Four optical fibers in one aerial cable are used to communicate data, audio, and video between the BSR and the HFIR. Because this cable is subject to failure, limited redundant, diverse, and independent communication channels are provided over leased wires on a right-of-way separate from the fiber cable. These leased wires transmit critical information that the operators will need if the fiber cable fails. This critical information includes neutron flux level indication and shim rod seat switch positions. A dedicated leased line and dedicated optical fiber are available for manual reactor trip. Both the fiber optic and leased-line remote, manual trip circuits are fail-safe in that the reactor is tripped if either is interrupted.

Two identical workstations control and monitor the reactor, one each at the BSR and the HFIR. The active workstation is selected by a remote/local switch on the BSR control panel. If the active workstation fails, the watchdog timer in the PLC will trip the reactor a few seconds after communications have ceased. Likewise, an annunciator in each workstation will indicate to the operators that communication with the PLC has stopped. If communications to the workstation not selected by the remote/local switch were to fail, this failure will also be annunciated at the active workstation, but the reactor will not trip.

Because the reactor control room will normally be unattended (except for a roving operator who will be in the vicinity), the workstations do not provide redundant control. However, information redundancy at the remote station is provided by several means. During normal operation, redundant and diverse sources of information can be used to check for consistency between displays. If one of the displays fails, the remaining displays are used to monitor the reactor. In addition to the remote workstation, which displays most of the information that can be obtained from the local control panel, there are two video monitoring systems. These video signals are transmitted over the same fiber cable used to transmit the workstation data. A camera in the BSR control room can be used to view any panel-mounted recorder or indicator in the control room. All of the racorders and most of the indicators now on the control panel will remain after the remote control system is installed. A second camera, mounted in the reactor bay, can be used to examine in detail the reactor bridge, the reactor core, and most of the reactor bay area. The lens on this camera can be zoomed from a focal length of 9.5 mm to view most of the reactor bay to 150 mm to examine reactor assemblies closely for proper position or operation. Each of the video signals is connected to its own monitor in the HFIR control room, and the HFIR has pan, tilt, zoom, and focus controls so that the operators can control the cameras. Also, an audio system is connected to intercom and public address systems at the BSR. Roving operators or maintenance technicians at the BSR can be summoned by the public address system, and they can communicate to the remote operator over a "hands-free" intercom system.

A redundant source of critical information is also provided over the leased wires. As described, these wires transmit neutron flux and rod seat switch positions to indicators on the remote control panel. The same parameters are also displayed on the workstation and the BSR control room video monitoring system. The local shim rod seat indicator lamps and the remote seat monitors using the leased lines are powered by an uninterruptible power supply to ensure that the operators know the rods are seated if alternating current power fails. If the shim safety rods are seated, there are no active shutdown systems to control or monitor because natural convection flow provides adequate cooling.

Operator Interface

The present method of controlling the BSR is by panel switches, recorders, and digital indicators located on a control panel. The new control system is functionally the same as the old, but the controls and displays for normal operation are located on a special-purpose keyboard and VDU. Selected panel controls and displays in the old system will remain, but they will not be used for normal operation. The new control system consists of five graphic pages, each for use at certain times during operation and a sixth page for annunciators. The five pages are "Nuclear Systems Run" for operation at power; "Nuclear Systems Startup" for control and monitoring startup until the "run" condition is achieved; "Primary and Secondary Process" for monitoring only; "Protection System" for monitoring and testing; and "Emergency" for monitoring critical parameters during abnormal conditions. The following section contains a review of human factors considerations for these graphic pages. The "Nuclear System Run" and the "Protection System" graphic pages are shown in Figs. 2 and 3, respectively.

Because the method of performing operations with the new control system is different than the old, the BSR operators have to learn new ways of controlling the reactor. Although implementation is different, functional control of the reactor is changed little. Therefore, training will involve learning a new operator interface only, rather than functional changes. Some of the generic changes for the operators include having less information displayed at any one time on a VDU than is now available on the full control panel; having a few seconds' delay to update the dynamic parameters on a graphic display rather than having information updated immediately, as on the present indicators and recorders; and performing controls with a special-purpose keyboard rather than with switches. Alarm handling will be different because alarms will be displayed on a workstation VDU rather than on annunciator panelboards.

The number of independently controlled workstations at the remote site was an important consideration for selection of the workstation to be used. Before selecting a workstation for remote control of the BSR, the requirements for operating the BSR were reviewed, and the costs and benefits of a number of independant control stations were considered. Because of the inherent safety of the BSR, because the operators do not have active systems to operate after the reactor is shut down, and because most of the operation is automated, one workstation, rather than two or more independent workstations, is adequate. Having only one workstation VDU requires more frequent switching between graphic pages, but except for the alarm page, each page used during normal operation has at least the critical information of neutron flux to indicate reactor power. The workstation selected can switch between pages within 1 s. The time spent observing the alarm page during operation should be short because the three most recent alarms are displayed on the bottom of each page, and all of the alarms are printed as they occur. Redundant indicators are also available for the operators to continuously monitor the reactor. The workstations also print a status report hourly or on demand. This report is now recorded by hand. In addition, the operators can monitor other parameters over the video channel. Because redundant workstations were not installed, a fail-safe feature was installed to trip the reactor if the controlling workstation ceases to communicate.

Another generic consideration is that the workstation displays an update of the dynamic parameters approximately every 2 or 3 s, which is slower than the recorders and indicators in the old system. Most of the monitored parameters change slowly enough that a 3-s delay is not a problem. However, neutron flux is a critical parameter that can change fast enough that a 3-s delay during startup could disturb an operator accustomed to faster updates. Therefore, it was decided to leave the recorders and indicators on the local control panel and to provide the remote operator with a video channel that can be used to monitor the faster responding parameters in real time. It is important that the operator monitor the neutron flux, but there is no safety consideration requiring that the operator be able to shut down the reactor for a fast transient; the independent protection system is designed to do that. The remote manual reactor trip is connected directly to the drop-out and make-up trip relays without going through the workstation and the PLC. Therefore, the reactor will trip within milliseconds of a manual scram.

The relative update rate of the dynamic parameters displayed on a workstation page can be selected during system design. The parameters such as neutron flux and period that are most important and that change rapidly are selected to be updated at the fastest rate. Primary and secondary coolant flow, and temperature measurements that change more slowly and are of lesser importance, are updated at a slower rate. Discrete parameters, such as the position of a flapper valve that cannot be moved without tripping the reactor, are updated at the slowest rate. The update rate does not affect the speed of control; it affects only the speed at which the parameters are updated on the operator workstation.

Use of a special-purpose keyboard to control the reactor is a difference that will require operator training. Although only a few of the control panel switches will be removed, the keyboard will be used for normal reactor operations. Most of the remaining switches, such as the rod control toggle switches, will be used for special tests. Because the workstations and the PLC are programmed and connected in a laboratory, operator training can be done using simulated signals before the equipment is installed on the reactor. This feature of the digital control system is an important one for initial operator training.

Alarm handling for the operators will be different because the alarms will be displayed on a workstation VDU rather than on annunciator panelboards. The main difference is that only the three most recent unacknowledged alarms will be displayed on the bottom of each graphics page, as pictured in Figs. 2 and 3. The remainder of the alarms are displayed on an alarm page. When an alarm

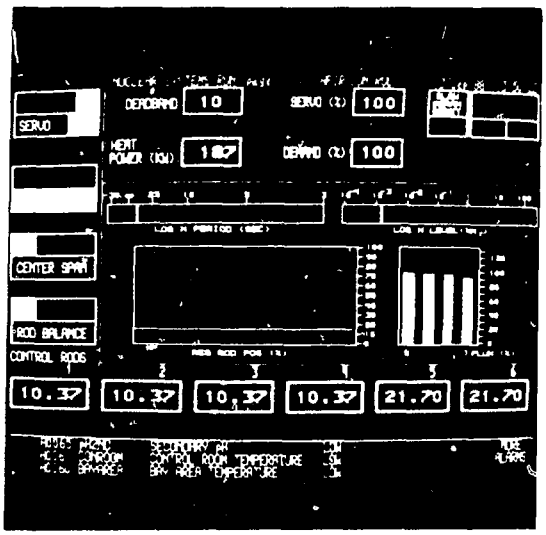

Fig. 2. Main graphics screen.

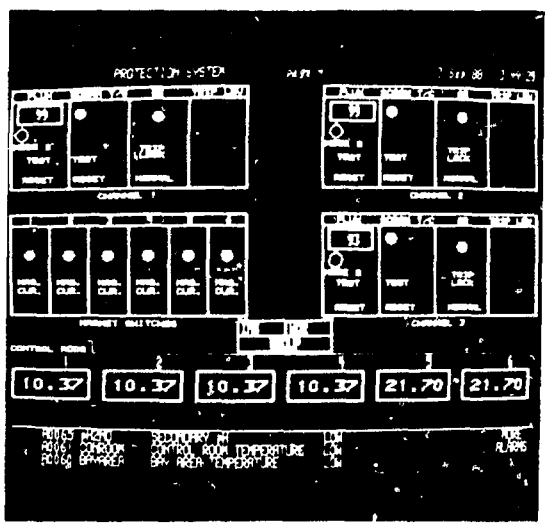

Fig. 3. Protection system graphics screen.

is acknowledged, it is moved automatically to the alarm page, and unacknowledged alarms move up on the bottom of the graphics pages. A disadvantage of this system is that reactor status cannot be determined at a glance as it could be with an annunciator panel. However, because the BSR has only 40 alarm points, of which only a few are usually in alarm during normal operation, this disadvantage is not significant. On the new system, the points now in alarm are displayed on the graphics alarm page, and they are logged on a printer as they occur. An advantage of the new system is that the printer records the history of alarms by printing the times of occurrence, acknowledge, reset, and clear of each alarm. Also, a bell alerts the operators to an alarm condition.

Screen Development

The workstation graphics are designed in accordance with human factors guidelines[4] as follows:

1. Seven or fewer colors are on a page.
2. A dedicted area on the bottom of each graphic age is reserved for alarms (see Figs. 2 and 3).
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 ~1 s after the keystroke to select it.
6. Bar charts are used for data that are frequently compared. (See the safety and servo neutron flux signals in Fig. 2.)
7. Mimics of the process and instrument panels are used to enhance the speed of comprehending information. A mimic of the protection system chassis is shown in Fig. 3.
8. Operators reviewed the graphics during system development. Their suggestions helped with the design and should ease the transition to the new system.
9. Functions are grouped on each graphics page such that to evaluate a particular system, an operator looks to a specific area of a page. The graphics are divided into five or six groups of related information. The mimic pages group displays by system rather than by related parameters from different systems.

Graphics pages are developed on an operator workstation using menu-driven software and a cursor. Programming graphics is time consuming, and most changes are not simple to make. Therefore, it is beneficial to draw the graphics on paper for review and comment before programming a workstation. The graphics can be saved to disk for reloading or off-line development.

Conclusions

Remote control of the BSR can be accomplished safely and reliably using a fault-tolerant programmable logic controller and fail-safe features to ensure reactor shutdown in the event of a control system failure. Redundancy of information to the remote operator is provided by a digital control system and a video system communicating over fiber optics, as well as dedicated panel displays communicating over leased lines on a separate right-of-way. This design provides operators with the necessary information without installing a separate fiber cable and a redundant control station at the HFIR. The control system is designed for reliable operation, but fail-safe features are included to shut down the reactor during a control system failure. A PLC failure is unlikely because it is fault-tolerant. Fail-safe features shut down the reactor if either of the communications channels fails or if the active workstation fails. The remaining communications channel can be used to monitor the reactor shutdown. After the rods are seated, there are no active systems to control for safe shutdown. Remote operation of the

BSR is feasible because of the inherent safety features of the reactor and the fail-safe features and reliability of the control system. However, after remote operation is begun, this system can be used to evaluate techniques for remote control of more complex reactors.

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

2. L. E. Stanford, T. P. Hamrick, and F. T. Binford, "Description and Safety Analysis of Significant Change of the Bulk Shielding Reactor for 2-MW Operation," ORNL-TM-2231, pp. 40-42, Union Carbide Corp., Oak Ridge National Laboratory, May 15, 1968.

3. L. E. Stanford, T. P. Hamrick, and F. T. Binford, "Description and Safety Analysis of Significant Change of the Bulk Shielding Reactor for 2-MW Operation," ORNL-TM-2231, pp. 42-43, Union Carbide Corp., May 15, 1968.

4. P. R. Frey et al., "Computer-Generated Display System Guidelines, Volume 1: Display Design," EPRI NP-3701, Vol. 1, Palo Alto, Calif., September 1984.

DISCLAIMER