MASTER

UCRL- 86066
PREPRINT

CONF-811040--45

PROGRAMMABLE CONTROLLERS REPLACE RELAYS IN MFTF-B PERSONNEL-SAFETY INTERLOCKS

James D. Branum

This paper was prepared for submittal to
9th Symposium on Engineering Problems
of Fusion Research
Palmer House
Chicago, Illinois
October 26-29, 1981

October 20, 1981

PROGRAMMABLE CONTROLLERS REPLACE RELAYS IN MFTF-B PERSONNEL SAFETY INTERLOCKS

James D. Branum
Lawrence Livermore National Laboratory
P.O. Box 5511, L-634
Livermore, CA 94550

Summary

Relays and hard-wired logic have been the mainstay in personnel safety interlock systems to date. Computers, if used, have generally been relegated to subordinate functions such as system status and hardware fault monitoring. Concerns regarding the potential failure modes of the computers and their solid-state hardware interfaces have been largely responsible for past decisions to limit the involvement of computers in personnel safety functions. As experiments have become increasingly large and complex, the capability of relay-based logic to reliably handle all of the decisions necessary to ensure the safety of personnel in a large facility has come under question.

This paper describes a new approach for implementing personnel safety interlocks logic using industrial-type programmable controllers. The logic for all personnel safety interlocks except those totally internal to a subsystem is implemented in two non-redundant controllers. A high degree of fail-safe reliability is achieved by augmenting the protective features intrinsic to each controller with those provided by a small amount of external support hardware. The controllers are interfaced to the host computer system via fiber optic data links to enable display of interlock and overall system status on the control room graphic displays. When fully implemented, the controllers will perform the equivalent of over 2000 discrete relay functions.

"Work performed by LLNL for DOE under contract number W-7405-Eng-48."

Introduction

Computers and solid-state electronics have been largely excluded from personnel safety interlock systems to date. Computers, when used, have generally been relegated to subordinate functions such as status and fault monitoring, or as backups to a primary, relay-based system. Concerns such as potentially unsafe failure modes, cost, susceptibility to electromagnetic interference, and the need for extensive software development and support have been largely responsible for past decisions to limit the use of computers in personnel safety applications. However, a properly designed safety interlocking and monitoring system based on presently available industrial-type Programmable Controllers (PC's) can also achieve high reliability and noise immunity, and at the same time provide substantial cost, size, adaptability and maintainability advantages over comparable discrete-relay systems. In fact, the high adaptability and maintainability inherent in PC-based systems can actually be exploited to achieve a higher degree of safety and reliability than is usually practicable with discrete relays alone. For example:

1. PC construction is modular. New modules can be added or types substituted as requirements change.

2. Control logic is not rigidly constrained by external hardware. Logic can thus be made as complex as the task requires without increasing the size or complexity of the external hardware or wiring. Logic changes can be implemented more quickly and with fewer errors than with discrete hardware, and can also be developed and verified independent of the external system.

3. Documentation of logic programming is automatic, and can be compared with the master version at any time. Safety hazards arising out of undocumented changes are thereby minimized.

4. System and interlock status can be reported directly to a host computer system. The need for a separate remote-monitoring system such as CAMAC is thereby eliminated.

The above advantages are particularly important for large experiments such as MFTF-B, which would otherwise require more than 2000 discrete relays plus associated CAMAC hardware to implement all anticipated interlocking, monitoring, and error detecting functions.

System Overview

The Personnel Safety and Interlocks System now being designed and installed in MFTF-B is illustrated in Figure 1. The logic for all personnel safety and warning functions except those built into each individual subsystem will be implemented in two non-redundant Modicon model 584 PC's. Each PC will serve approximately one-half of the total experimental area, and will function essentially independent of the other controller and of the main computer control system during normal operation. Exchange of essential safety information between system halves will be through a limited number of direct-wired crossties. Less-essential and backup communications will be accommodated via the main computer control system. A high degree of fail-safe reliability is achieved by augmenting the protective features intrinsic to each controller with those provided by a small amount of external external support hardware. These protective features are described in the next section.

Except for the logic-determining portion, the balance of system hardware is of conventional design. Standard switches will be utilized to monitor the individual positions of each gate, door, "crash button", etc. The status of hazards and hazard-producing equipment will also be monitored as directly as possible in order to minimize the possibility of incorrect system operation. This approach also reduces or eliminates the need to bypass interlocks because most, if not all, of the information necessary to determine the safety of a particular operation is directly available to the interlocks logic. All inherently safe operations can thus be permitted, with proper logic programming, without the need for human intervention.

Control outputs of the system are of three basic types: 1) Permissive signals to the controls for systems which produce hazardous voltages, radiation, etc.; 2) Control signals to audible and visual warning devices; 3)Control signals to system and hazard status displays. The basic power for all control and monitoring functions is 28 volts DC. The PC's communicate with the main MFTF-B control system computers located in the control room building via 9600 baud fiber optic links. The links are implemented using commercial

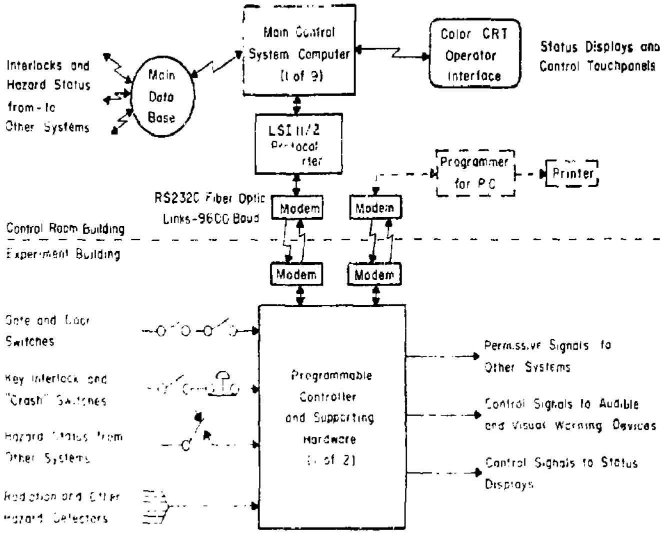

Figure 1. Personnel Safety and Interlocks System for MFTF-B

RS232C fiber optic modems. Separate links are also provided to enable remote connection of the PC programming-monitoring terminal and printer. A single LSI-11/2 microcomputer acts as a combination network master, protocol converter and buffer for both PC's. The LSI-11/2 requests each PC to transmit a preformatted block of status data approximately once every two seconds. Between transmissions, the data are examined for changes. Changed data are then processed into the main data base through one of the nine 32-bit computers which comprise the main MFTF-B computer control system. Safety-related data received directly from other systems via each system's individual control system interface are combined in this main data base with data from the PC's, and presented to control room operators through a color graphic display system. Touch-sensitive panels placed over other color CRT's enable operators to select from a variety of status display formats. The operator can also initiate a limited number of commands to the PC's; e.g., to turn off all permissives. Watchdog timer routines will run in both the main computer and PC systems to assure that only current safety status is displayed or acted upon.

Protective Features

Each PC is supported by a small amount of external hardware in order to assure a high degree of fail-safe reliability. The basic hardware configuration is illustrated in Figure 2.

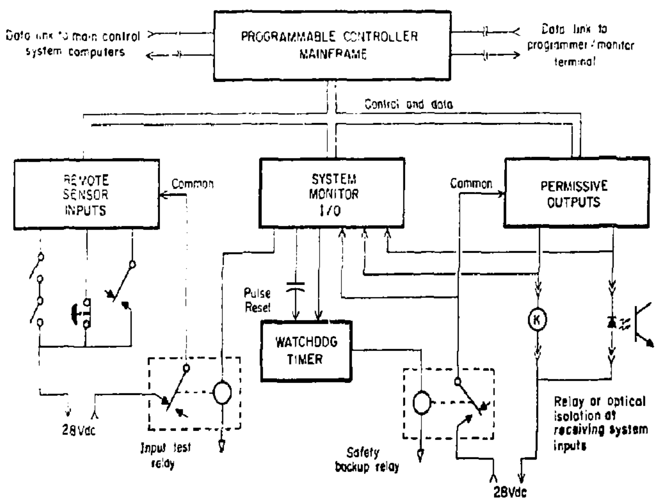

Figure 2. Programmable Controller and Principal Supporting Hardware

The Modicon 584 controller system protects itself against most internal faults. Detection of a fatal error such as a parity error in the PC memory will cause all outputs to turn off, a safe condition. Each I/O module also contains an internal watchdog timer which turns the module and any outputs off if communication with the mainframe is lost. Optical isolation, shielding, filtering, and multiple data transmission techniques minimize the possibility of false operation due to electromagnetic interference. Despite this robust construction, however, the PC does have two blind spots which must be guarded by use of external support hardware.

The first blind spot is in the remote sensor input section. The design of the Modicon input modules follows the fail-safe convention whereby current flow is equated to a logical one or "on" condition. An internal short circuit or chip failure could result in a stuck bit, however, which may not be detected by the mainframe's error traps. To counter this, sensor monitoring power is periodically removed from all input modules for about 200 msec by activation of the input test relay. While power is removed, the controller checks to see that all inputs go the the "off" state. Disruption of safety functions by the test is prevented by using the PC's "skip" programming function to temporarily suspend solution of all logic except that required to perform the test. If a stuck bit is detected, or if the controller hangs up in this test mode, the external watchdog timer will not be sent a reset pulse and will time out in two to three seconds. This will then cause the safety backup relay to drop out and remove power from all permissive outputs, a safe condition. Normal controller operation resumes if no stuck bits are detected. Tests will be performed at five minute intervals, the same frequency as for MFTF-B physics shots.

The second blind spot is in the user side of the output modules, for which the present module design does not include internal features for detecting an open, short, or excessive leakage failure of the output transistor or triac. To counter this, each permissive and warning output will be individually monitored by dedicated inputs. If the ordered and monitored states of these critical outputs are found to disagree for more than a few I/O read-write cycles, power will be removed from all permissive outputs as in the case of a failed input module. Interface standards on minimum operating currents have been established to assure that leakage failures will be detected below the switching thresholds of the relays or optical isolators used in the input circuits of equipment which receives safety permissive signals.

In addition to the protective features described above, limited backup protection will also be provided for the interlocks built into each MFTF-B system. The status of hazard-generating equipment and of safety permissive signals will be compared at both the PC and main computer system levels. Detection of an erroneous response to a permissive signal will cause the PC's to activate warning devices near the malfunctioning equipment. At the same time, the main control system computers will attempt to deactivate the malfunctioning equipment via the normal control interface. Alarm messages will also be sounded and displayed at the operator consoles to alert control room personnel, who can then take the necessary followup action to restore the facility to a safe status.

Conclusion

Industrial-type programmable controllers offer significant advantages in cost, size, adaptability and maintainability over conventional relay-based interlock systems, especially for large experiments. These advantages can be easily exploited to achieve an even higher degree of safety and reliability than is usually practicable with discrete relays alone. Careful attention must still be paid, however, to all aspects of the system design in order to assure that the system actually achieves and maintains the level of performance of which it is capable.