Design Lessons from Using Programmable Controllers in the MFTF-B Personnel Safety and Interlocks System

James D. Branum

Proceedings of the 10th Symposium
on Fusion Engineering
Fusion Energy Conference
Philadelphia, PA
December 5-9, 1983

November 29, 1983

[illegible]

[illegible]
Lawrence Livermore National Laboratory [illegible]
[illegible]
[illegible], CA [illegible]

Abstract

[illegible] programmable controllers [illegible] personnel safety and interlocks systems requires special consideration in the design of both hardware and software. [illegible] sneak circuits, even without component failure!

This paper presents the most significant lessons learned to date in the design of the MFTF-B Personnel Safety and Interlocks System, which utilizes two non-redundant programmable controllers with over 800 I/O points each. Specific problems recognized during the design process as well as those discovered during initial testing and operation are discussed along with their specific solutions in hardware and software.

"Work performed under auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under contract number W-7405-ENG-48."

Introduction

Industrial-type programmable controllers offer significant advantages in cost, size, adaptability and maintainability over conventional relay-based interlock systems, especially for large experiments such as MFTF-B. These advantages can be easily exploited to achieve an even higher degree of safety and reliability than is usually practicable with discrete relays alone. For example:

1. Construction is modular. New modules and accessories can be added, substituted or deleted as needs change.

2. [illegible] hardware. Logic can then be made as complex as the task requires without increasing the size and complexity of the external hardware or wiring.

3. Logic changes can usually be implemented more quickly and with fewer errors than with discrete relay-based logic. Development and basic checkout can also be performed independent of the external sensor hardware.

4. System and interlock status can be reported directly to a host computer, thereby eliminating the need for a separate monitoring system such as CAMAC.

Even with these great potential advantages, careful attention must still be paid to all aspects of the system design in order that the system will actually achieve and maintain the level of performance of which it is capable.

The purpose of this paper is to highlight the most significant insights and lessons-learned to date from the application of programmable controllers in the MFTF-B Personnel Safety and Interlocks system. Specific real and potential problems recognized during the design process as well as those discovered during the initial stages of testing and operation are presented along with their respective solutions in both hardware and software.

The following overview of the MFTF-B Personnel Safety and Interlocks System is provided to facilitate discussion of the specific problems and solutions which follow.

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 interlocking and warning

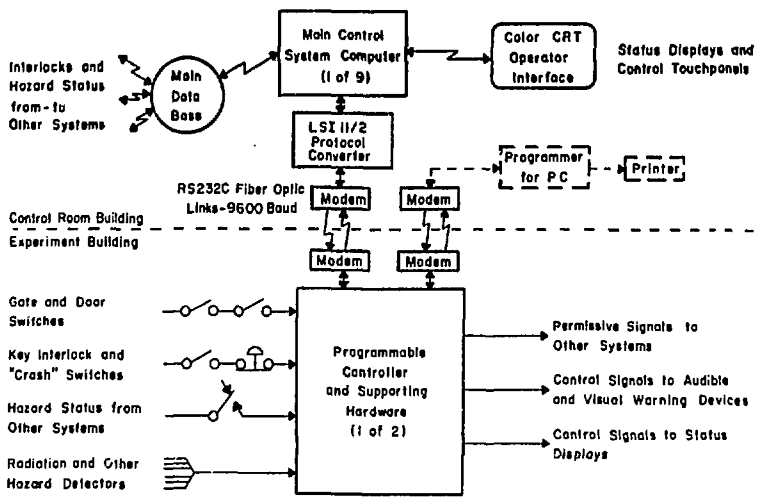

Figure 1. Personnel Safety and Interlocks System for MFTF-B.

[illegible]

The controllers, their I/O modules and ancillary hardware are housed in NEMA 12 cabinets (90" H x 72" W x 24" D) and standard 19 inch racks located at two different locations in the main equipment building. The main control system computers are located in a separate but adjacent building.

Except for the logic-determining portion, system hardware is of conventional design. Standard switches will be utilized to monitor the individual positions of each personnel access gate, door, "crash button", etc. The status of hazards and of hazard-producing equipment will be monitored as directly as possible in order to minimize the possibility of incorrect system operation. This approach also minimizes the need to bypass an interlock because most of the information necessary to determine the safety of a particular operation will be available in the controller logic, or in the safety logic of the individual subsystems themselves.

Control outputs of the system are of three basic types:

1. Permissive signals to the controls for systems which produce personnel hazards such as high voltage, radiation, etc.
2. Control signals to audible and visual warning devices.
3. Control signals to hazard status displays at the entry to the experimental area.

[illegible]

[illegible] Perkin-Elmer model 3250 minicomputers. The main control computer system also includes two of the faster Perkin-Elmer model 3252 minicomputers.

The main control system computers also receive safety-related information directly from the other MFTF-B subsystems. This information is collated with that received from the safety system controllers to produce color graphics and text displays at the control room operators' consoles. Installation of the interface between the controllers and the main control system computers will begin in early calendar 1984.

A high degree of fail-safe reliability for the system is attained by augmenting the protective features intrinsic to each controller with those provided by a small amount of external support hardware and the corresponding additional controller programming. The basic hardware configuration is illustrated in Figure 2. The principal elements are the Input Test Relay, the Watchdog Timer and the Safety Backup Relay. Especially note that safety permissives, and also the more important warning device control signals though not shown, are supervised by individual, dedicated inputs. The need for and function of these elements is discussed in the following section.

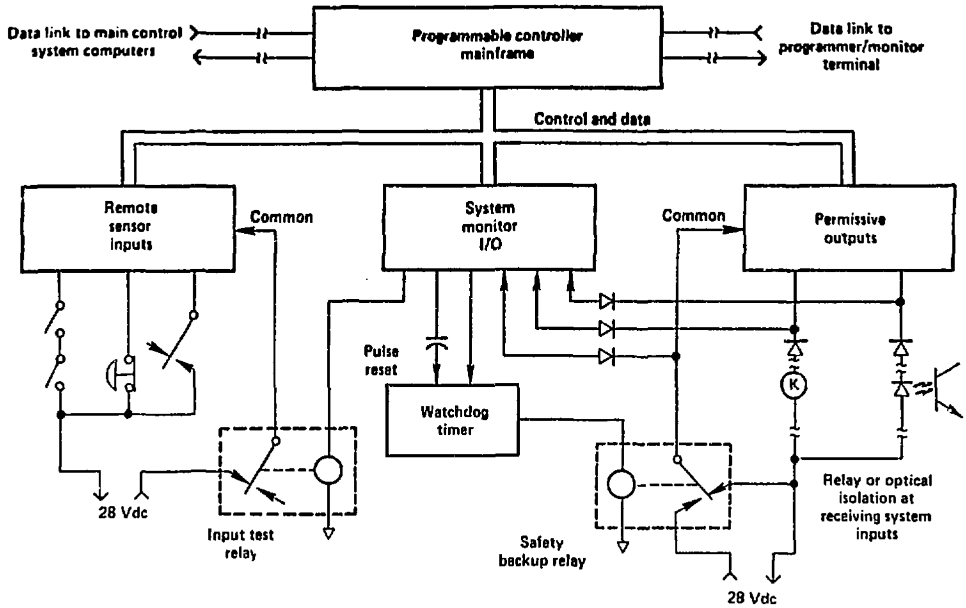

Figure 2. Programmable Controller and Principal Supporting Hardware.

[illegible]

Problem Description: The mainframe of the Gould 584 programmable controller contains extensive internal diagnostic features which [illegible] the program memory and communications with the I/O modules. Detection of a fatal error will cause the controller mainframe to turn off all output modules, a fail-safe condition in this application. Additionally, each I/O module contains its own internal watchdog timer which turns the module and any outputs off if successful communications with the controller mainframe do not occur more than about 250 msec. Successful communication requires that all data from redundant transmissions be identical. Several retries are attempted before the mainframe logs a communication error for that module in its internal status registers. If communications are successful, the mainframe will reset the module's internal watchdog timer. Despite this robust construction, the controller mainframe does have "blind spots" in its failure detecting capabilities which must be guarded through the use of external support hardware.

The most prominent blind spot is the inability of the mainframe to detect failures or malfunctions on the "field-side" of its I/O modules. For example, the output-type modules supplied by Gould for the model 584 are typical of the industry in that they do not contain internal circuitry to monitor for failure of the output control device. The control device is a power transistor in DC-type modules, and a triac in AC-type modules. Small, light-duty relays are also used in some module styles. These device-types are notorious for failing in a "shorted" mode, which generally is not a fail-safe condition. A similar blind-spot exists for input-type modules. Because the design of both the input and output stages is non-redundant (also typical), the failure of a single component could result in a potentially unsafe condition if compensating measures are not designed into the system.

Solution: These blind spots are countered in the MFTF-B Personnel Safety and Interlocks System as follows:

1. *Dedicated input modules were* added to supervise all critical output signals such as safety permissives. Additional logic within the controller compares the ordered and the observed state of each supervised output point. If a miscompare exists for a longer time than required for a state change to register, the controller's User Program *sets it own fatal error flag.* All such flags cause the safety backup relay, which is physically part of the external watchdog timer, to drop-out and remove power from the permissive outputs. A similar response will occur if the controller stops scanning for any reason because the external watchdog timer requires a pulsed reset signal. Upon loss of these safety permissives, all hazard-generating systems respond by going to their respective least-hazardous states.

2. *An "input test relay"* was added to permit the controller to periodically interrupt the contact-sensing current supplied to each discrete-type input module. While *current is interrupted,* which lasts several hundred milliseconds, the controller's user program checks for any inputs which remain "on". All inputs should register as *"off" because the style of modules being used requires* current flow for the "on" state. If any "on" states are discovered, the program sets a fatal error flag and all *safety permissives are removed, as described above. To* prevent disruption of outputs during this test, the program temporarily suspends performing of other control or test logic, and also the logic which updates the external watchdog timer. [illegible] the Gould 584 controller through use of the [illegible] function. [illegible] should the program fail to [illegible], the external watchdog timer will time-out and remove all safety permissives.

3. Program logic was added to check the controller's internal I/O communications status table. The Gould 584 controller features a function "STAT" or "get status" function which provides access to this table from the user's program. The controller mainframe, however, takes no action of its own if communications with a module are lost other than logging this fact in the status table. The user program written for the MFTF-B Personnel Safety and Interlocks controllers checks this table for error flags which indicate loss of communication with any I/O module. If found, a fatal error flag is set and safety permissives are removed.

Experience: Module failure history to date during independent system operation has clearly demonstrated the need for the corrective steps described above. Specifically, *five I/O module failures have been observed, two of which* were in non-fail-safe modes. In each case, the controller detected the failure and removed the "simulated" safety permissive signals. The two non-fail-safe failures were also of types which are not detectable by the controller's intrinsic protective features.

The first of the non-fail-safe mode failures occurred in a *24* volt D.C. style output module. The module outputs are "protected" by a single, collective fuse located in the negative common lead. *During* an evaluation test *for* this module style, the load connected to one output transistor was momentarily short-circuited. This was done to check whether or not a collective fuse could protect the *individual* output transistors, each of which had maximum current ratings which were well below the rating of the fuse. The result was that the fuse did not blow before the output transistor current-limited. After the short circuit was removed, the output transistor failed to respond to control signals from the controller mainframe, and instead continued to conduct several milliamps of current through its load. This leakage was detected by the supervising input module (only), and simulated permissives were removed by the safety backup relay. It was subsequently decided to purchase the more robust, and more expensive, 10-60 volt D.C. style modules which also had individual fuses for each of its 16 outputs. A repeat of the *shorted-load test revealed that this fuse would blow before* the output transistor will sustain damage. The need for output supervision still remains, however, because other *failure* causes such as *voltage overstress* could damage the output transistor.

The second of the non-*fail*-safe mode failures *occurred in* a 10-60 volt D.C. style input module. The symptom was failure of the test for stuck "on" inputs. Because the test program identifies the module position which contains the failed input, the apparently defective module was quickly replaced with a new module. Upon attempting to clear the error flag and restore normal operation, the same failure symptom appeared, but for a different module position located in the same I/O channel (1 of 4). That module was changed-out and the failure repeated a third time. Process of elimination finally uncovered the truly defective module, the diagnosis of which revealed a defective address decoder chip. The module had been answering-up for other modules in the same channel in such a way that even the controller's *intrinsic I/O communications diagnostic* did not reveal the problem. Were it not for the added test for stuck "on" bits, the failure could have prevented the opening of an *important interlock!*

[illegible]

[illegible]

[illegible]

1. Diodes are connected to each of the power bus common connections on the module in order to protect against voltage spikes from unsuppressed inductive loads.

2. An LED which is driven from an *external* power source is connected to indicate whether the output transistor is "on" (conducting).

In addition to the above internal connections, each "critical" output was connected to the input of a supervising input-type module, as discussed above. The circuitry of the input module "sources" current so that it can be connected directly to the open-collector type output modules, which in turn "sink" current.

During initial checkout of the MFTF-B Personnel Safety and Interlocks system, a design problem was discovered when test relay loads connected to several permissive outputs did not drop out when load power should have been removed by the safety backup relay. Investigation revealed that no component had failed; the test load relays were being held-in at reduced current by power which was being supplied from the output modules' internal LED status indicator circuit, and also from the connected input modules. When the safety backup relay opened, power from these sources flowed to the now-open (+) common load power bus through connected loads and the spike suppression diodes; that is, unless the particular output transistor was conducting. Enough power was supplied to sustain the load relays which were connected to conducting output transistors.

Solution: The sneak circuit discovered above resulted from the classic hardwire control design problem known as "breaking the neutral". This problem, however, is a built-in feature of the I/O system described above! Three design changes were made to counter this problem, as illustrated in Figure 2:

1. [illegible]

2. [illegible]

3. The circuitry for the safety backup relay was modified to both isolate and short the common power feed to the safety permissive output modules when the safety backup relay drops out. This provides additional protection against the failed-mode failure of a [illegible].

Experience: The above changes completely eliminated the problem.

Conclusion

Programmable controllers, by themselves, generally do not have sufficient capability to detect and counter failures on the "field-side" of their hardware. As a result, a programmable controller or *similarly-based system* which is used in critical applications such as personnel safety interlocks must be augmented by a combination of external support hardware and special program logic. Neglecting to account for predictable failure modes and sneak circuits can result in a system which is inherently less "safe" than intended. Careful design of the system hardware and software will both minimize the impact of this added complexity, and assure that the system actually achieves and maintains the level of performance of which it is capable.