

CONFIDENTIAL
TOP SECRET
MAILED

DCRL-89206
DD84 012596

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

Lawrence
Livermore
National
Laboratory

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

MASTER

DESIGN, IMPLEMENTATION AND PROBLEMS ENCOUNTERED IN THE DESIGN AND IMPLEMENTATION OF THE MFTF-B PERSONNEL SAFETY AND INTERLOCKS SYSTEM

By: David A. Weller
Lawrence Livermore National Laboratory
Livermore, CA 94550
(415) 422-2110, ext. 22100

INTRODUCTION

The design, implementation and problems encountered in the design and implementation of the MFTF-B Personnel Safety and Interlocks System is presented. The system is designed to provide a personnel safety and interlocks system capable of interfacing with an experiment computer and safety systems. The system is designed to provide a personnel safety and interlocks system capable of interfacing with an experiment computer and safety systems. The system is designed to provide a personnel safety and interlocks system capable of interfacing with an experiment computer and safety systems. Many of the most common types of logic modules can also eliminate potentially dangerous sneak conditions 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 E-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.

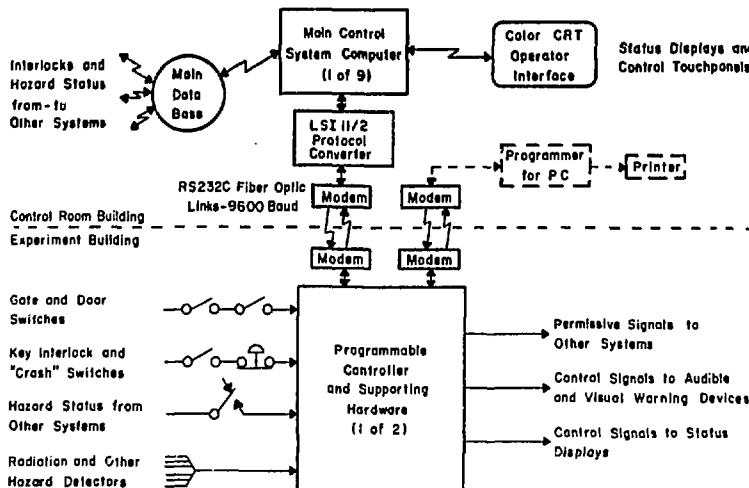


Figure 1. Personnel Safety and Interlocks System for MFTF-B.

2. Changes to logic can be easily implemented by external programmers. This makes the logic as simple as the logic of the host computer without the limiting 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

Each system will be programmed to provide a minimum of 1000 I/O capabilities, and the implementation of these requirements will be completed by 1986. The 8000 series has a maximum input capacity of 1000 I/Os, the 16000 series has a maximum input capacity of 2000 I/Os, and the 32000 series has a maximum input capacity of 4000 I/Os. The 8000 series will be the primary system for the first two years, and the 16000 series will be the primary system for the third year. The 32000 series will be the primary system for the fourth year, and the 64000 series will be the primary system for the fifth year.

The controllers, the I/O modules and auxiliary hardware are housed in 9.75" x 12" cabinets (10.5" H x 7.2" W x 24" D) and standard 19" inch racks located at two different locations in the main experiment building. The main control system computers are located in a separate but adjacent building.

Because 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, "trash button", etc. The status of hazards and other 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:

- Permissive signals to the controls for systems which produce personnel hazards such as high voltage, radiation, etc.

2. Safety outputs to auxiliary units and the input devices.

3. Control signals to the test facilities to trigger the circuit in the experimental area.

The logic within the system is based on logic functions as shown below:

Relationships between the controller and the main control system computers are summarized. Related to main computer operating at 16 MHz, a Digital Equipment Corporation (DEC) 32000 minicomputer acts as a protocol converter and buffer for the main computer, which is one of seven 32000 (Rev. B) and one model 3230 minicomputer. The main control computer system also includes two of the faster DEC minicomputer model 3232 minicomputer.

The main control system computers also receive safety-related information directly from the other MFTFB sub-systems. This information is collected 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.

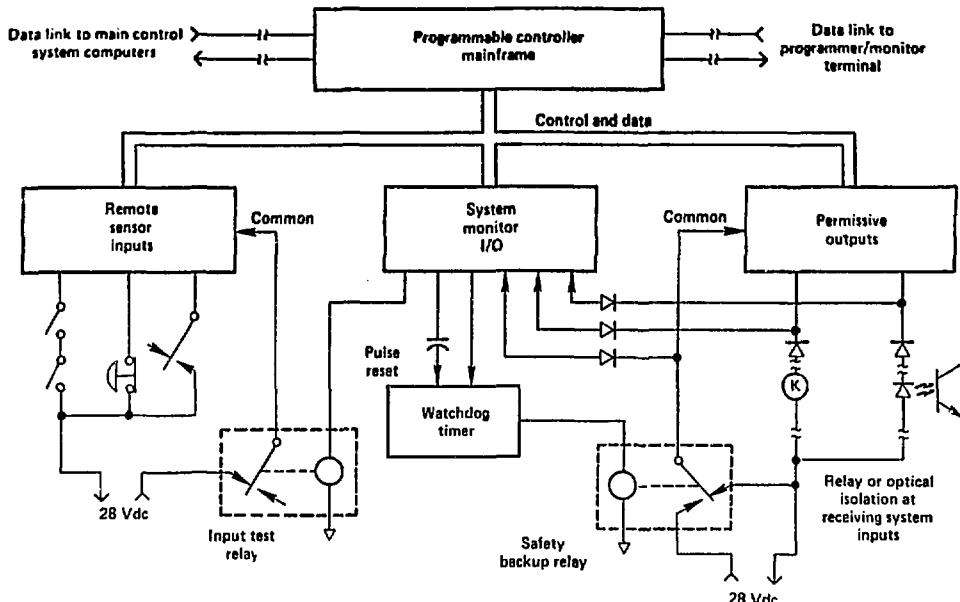


Figure 2. Programmable Controller and Principal Supporting Hardware.

Digitized by srujanika@gmail.com

Machine description. The backbone of the system is the programmable logic controller software, a Siemens model 343 diagnostic. Because the robot controller has no access to the program memory and can communicate only with the PLC module, the system is a "dumb" robot with a "smart" controller interface. The Siemens 343 has input modules, output modules, and an RS232C serial port. Additionally, each PLC module contains its own internal watchdog timer circuit. The module will self-diagnose all of its successful communications with the controller and become silent once more than about 200 msec. Standard diagnostic software programs that collect data from redundant PLC modules are used. Several articles are presented before the conference that are communication aids for that module in industrial status inquiries. If communications are successful, the backbone will reset the module's internal watchdog timer. Despite this robust construction, the controller interface does have "blind spots" in its failure detecting capabilities, which must be guarded through the use of external sensor 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 388 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.

Solutions: 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 its 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 original working paper. This is an established procedure of the Bank of Japan operated consistently for any reason that the Bank should change operating rules, namely, the system of operating rules of the bank and monetary policy instruments.

9. Diagnostic logic was added to check the controller's assigned IPID (minimum of three status bytes). The result of this function is the function "M150" or "P150 status" function which provides access to this table from the driver program. The driver then immediately, however, knows which table it is using and can read with a suitable number other than 1 (e.g. the last) on the status table. The same program written for the M150 will download safety and feedback controller checks this table for error flags which indicate loss of communication with any I/O module. If found, a total error flag is set and safety parameters 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 millamps 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!

Digitized by srujanika@gmail.com

Another change seen. The lipid droplets which contained the α -1 antitrypsin precipitates were not the same size. Smaller droplets were in the peripheral zone of the tissue. The size of the droplets decreased as the peripheral granules became confluent with the deeper, more centrally located granules. In this configuration, as in Figure 2, the small, peripheral granules were confluent with the deeper, more centrally located granules, and the entire tissue contained the α -1 antitrypsin precipitates both in the peripheral and in the deeper granules. The size of the peripheral granules was significantly smaller than the size of the deeper granules, and they also contained precipitates which were more numerous and more confluent than those in the deeper granules. The peripheral granules were confluent with the deeper granules, and the entire tissue contained the α -1 antitrypsin precipitates both in the peripheral and in the deeper granules. The size of the peripheral granules was significantly smaller than the size of the deeper granules, and they also contained precipitates which were more numerous and more confluent than those in the deeper granules.

After the end of the battle, Gaudenzio, a general, arrived at the scene and was struck by the beauty of the flower.

4. Diagnose and correct Bad To Faults in the power line & ground connection on the module in order to protect against static voltage from ungrounded and live lines.

3. **Q1** and **Q2** 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 output 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 hardware 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:

3. The unpaired α -HgII appearing clusters on the side which connects to the β -C terminal half possess this same character. This is probably a consequence of the fact that clusters are formed by using a multiple technique. The unpaired α -HgII appearing clusters are not as frequently as the paired α -HgII and β -C clusters with the oligopeptides, however.

4. The circuitry for the safety backup relay was modified to both isolate and short the common power feed to the safety generator output modules when the safety backup relay dropped. This provides additional protection against the shorted-mode failure of a generator module.

Experiments 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.

ANSWER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California, 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 the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government thereof, and shall not be used for advertising or product endorsement purposes.

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.