SLAC–PUB–4976
May 1989
(A)

PLC-based Interlock System for Superconducting Magnets*

Romain C. Agostini, Loy Barker,
Jim Hodgers, Daryl Reagan, Helmut V. Walz

Stanford Linear Accelerator Center
Stanford University, Stanford, California 94309

1. Introduction

Conventional interlock systems rely heavily on hard-wired electromagnetic relays. Although this approach is well understood and has proven to be reliable, several drawbacks plague the designer as well as the repair-man. If larger systems have to be implemented in relay logic, the complexity limit is soon reached; the systems become too bulky, and wiring expenses sky-rocket; moreover, the intelligence of those designs is limited in such a way that desirable features such as self-tests have to be left out. Additionally, relay interlocks are inherently inflexible: if the configuration of the system they protect has to change, a disproportional amount of time, work and money has to be invested in order to adapt the hard-wiring of the interlock system to the new requirements. Repair work is often unnecessarily delayed due to the lack of adequate documentation (especially referring to the 'temporary' patches in the wiring.

More powerful interlock systems can be built by using computer-based approaches. In this realm, programmable logic controllers (PLCs) represent the most cost-efficient approach. The interlock logic is no longer hard-wired, but coded in software. The PLC approach offers several advantages:

- flexible system configuration due to modular hardware and software
- regularly scheduled background tests of PLC system and sensitive I/O
- comprehensive system self-tests
- intelligent fault diagnostics simplify trouble-shooting
- easy reconfiguration of the interlock logic
- no mechanical wear and tear
- improved security due to logic encapsulation in firmware

Since PLCs, associated I/O modules and software are available off-the-shelf from major vendors, this solution doesn't require any major developments and becomes very attractive in price. This paper describes a PLC-based electrical hazard interlock system which is currently under development at SLAC (see figure 1); in addition to its obvious design goals, it is also intended as being a prototype PLC application in sight of a larger project [1], [2].

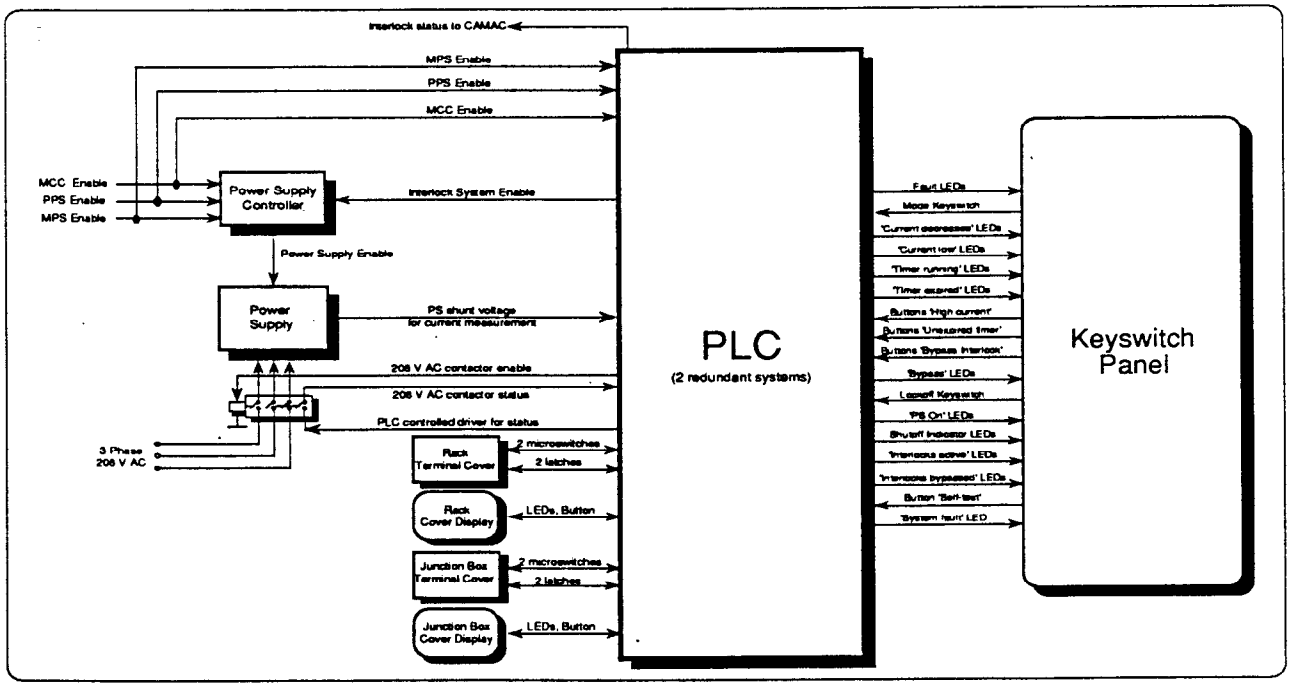


Figure 1: Block Diagram of the Interlock System for 1 magnet

*Work supported in by the Department of Energy, contracts DE-AC03-76SF00515

Presented at the Conference on Real Time Computer Applications in Nuclear Particle and Plasma Physics, Williamsburg, VA., May 16–17, 1989

2. Application Description

As part of the Polarization Project, SLAC is installing three super-conducting spin rotator magnets which are fed by dc power supplies providing 120 A at 20 V. Because of the large inductance of the magnet solenoids (16 H), a sizable amount of energy can be stored. This stored energy produces dangerous arcs if the leads from the power supply to the super-conducting solenoid are interrupted during normal operation, or after the power supply has been shut off and the current is decaying. As the power supply/magnetcircuit has two physical points where the terminals are accessible and can be disconnected (in the power supply rack and at the 'disconnecting and shorting facility', called 'junction box' hereafter), adequate safety measures have to be taken in order to avoid injury. This will be done by protecting the disconnection points with mechanical cover assemblies which can only be opened under the following conditions:

- The power supply has been shut off long enough to allow the circulating current to decline below a certain threshold
- The power supply is running, and the interlocks have been explicitly bypassed for 'hot' maintenance work.

In order to prevent any inadvertent opening of the terminal covers, they are mechanically kept locked by redundant plungers. In order to open them, associated electromagnetic latches have to be activated by pushbuttons which in turn are powered by signals from the PLC system (each PLC controls one latch at each cover). Voltage is present at the buttons only under the two conditions mentioned before.

The open/closed state of the covers is monitored by microswitches which are implemented and read in a similarly redundant fashion. Each microswitch is directly activated by the mechanical plunger of the latch assembly. If any one of the microswitches opens, the interlock systems detects this and shuts the power supply off in two redundant ways. One shutoff mechanism is a contact breaker which interrupts the primary 208 V AC power to the supply, and the other one is an enable/disable signal which trips the power supply controller. Each PLC has control over one of the shutdown mechanisms.

After an orderly shutdown of the power supply, a current monitor and a watchdog timer are started (each one again controlled by a different PLC). The current monitor compares readings from a shunt resistor (proportional to the power supply output current) to a predetermined threshold value, and the watchdog timer ticks for a fixed time, corresponding to the worst-case value for the current to decay to a harmless level. A restart of the power supply resets the timer. When both monitors indicate that it is safe to work with at terminals, a 'cover open' permit is generated by the software.

If maintenance work has to be done while the system is running, the interlocks for the covers to be opened need to be bypassed. This is accomplished by setting the system mode to 'Bypass Selection' with a keyswitch; the key is kept in the main control center and can only be checked out by qualified people. In this mode, any combination of covers can be selected from the central control panel; the actual bypass mode is not entered until the keyswitch is put into the 'Bypass' position. Further selections/deselections cannot be done in this position.

The central operator panel provides monitoring and control points for all three magnets (all functions described above refer to one magnet and are identical for the two others). LEDs show the state of the cover microswitches and latches and give interlock status and system information. Different power supply shutoff conditions are displayed as well as fault signals (see section 5 for more details). Another lockoff keyswitch which prevents both software and hardware from enabling the power supply is used while maintenance work is done at the system. Additional small displays are located at the covers; they provide information about the power supply operating modes, the interlock state, the microswitches and have a pushbutton for activating the latches in order to open the cover.

3. The PLC System

The PLCs utilized for this application represent a cost-efficient way to implement small control systems in this technique [3]. The version of the CPU module selected has the following characteristics:

- max. 4 k logic statements
- scan cycle time 350 ms
- 32 counters and 32 timers
- 1024 internal flags
- up to 256 digital I/O channels
- up to 16 analog I/O channels
- no interrupt capability

The I/O modules have a density of either 4 or 8 channels, and opto-isolation is available. Plugged into 'bus units' (which connect them electrically to the system bus and accommodate the I/O wiring), they can be easily exchanged for repair purposes. The bus units themselves are connected to a standard rail for rack mounting.

The PLC system is programmed with a proprietary Siemens programming language, called STEP 5, which comes in three flavors: ladder logic, control system

flowcharts and statement lists (STL). STL has been used for this application; it is a language similar to a simple assembly code, providing logical concatenation operators for I/O channels, comparisons, set/reset operators, and timer/counter manipulators.

The user program is developed in the STEP 5 programming environment under the S5-DOS operating system on a PC; S5-DOS in turn is an extension of the Personal CP/M-86 operating system which is required to be installed in a CP/M partition on the hard disk. During the test and development phase, the PC is connected to the PLC CPU module via a current loop interface, and the programs are downloaded into RAM. S5-DOS has some debugging features to help the designer developing application code. Once the software is finalized, it can be transferred into an EPROM or EEPROM module which is plugged into the CPU.

STEP 5 supports structured programming by providing software modularization by blocks. An overall (system) block called OB1 is cyclically executed by the runtime system; it calls up a succession of user program blocks or function blocks which implement the desired logic. Other OBs are called up during cold and warm starts in order to perform some initialization operations. STL on the S5-100 series is upwards compatible with higher-end models. Further details on STEP 5 and S5-DOS can be found in [2], [4].

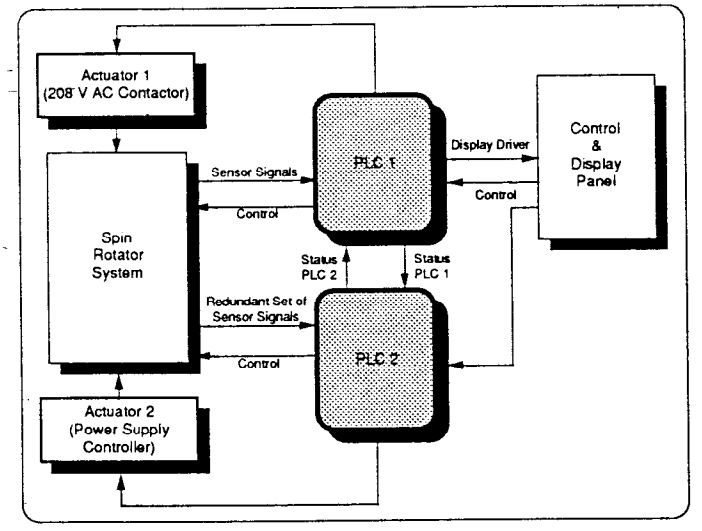


Figure 2: Redundant Processing with 2 PLCs

For redundancy purposes, the interlock system uses two distinct PLC systems with separate CPU modules (see figure 2). All relevant I/O signals and functions are redundantly monitored, processed and controlled, and logic results exchanged via I/O channels between the two CPUs. Each of the CPUs can initiate a system shutdown, but always will notify its counterpart so that the shutdown can be executed in a redundant way. As this is a safety system and as there are no requirements for keeping the system up in dubious situations, complicated voter schemes and other fault-tolerance mechanisms can be avoided: if an error is detected, a system shutdown is initiated.

4. Software Architecture

As outlined in the previous section, organizational block OB1 acts as a cyclically executed main program which calls up the different software modules of the user program. In order to modularize the code, the interlock system has been divided into several independent modules which communicate among themselves through global flags (variables). Each such module is a program block (PB) in the STEP 5 user program, and may in turn call up one or more function blocks (FBs) which implement the functionality of the module. This way, FBs may be replaced with minimal side effects by improved blocks with the same interface. Figure 3 gives an overview of the organization of the code modules.

The system selftest is not implemented yet; it will allow execution of basic system checks either on an automatic basis or by pressing a push-button on the main control panel. A blinking LED indicates internal problems. The polarity switcher module reverses for a short time the polarity of the output channels driving the microswitches (see section 5). The microswitch handler module determines whether all wiring to the switches is intact, whether interlocks are broken, and whether faults subsist long enough to reject transients (finite switching times have to be compensated for as well); flags are set according to the situation. Note that none of the modules takes any immediate I/O action. This is done at the end of the program in one single block in order to isolate external actions from the internal logic. No speed penalty has to be paid for this scheme, as the PLC runtime system only sets physical output channels at the end of each logic execution cycle.

The timer circuit module starts a watchdog timer when the power supply is shut off. If the timer expires, an internal flag is set. Every time the power supply comes up again, the timer is stopped and reloaded with its starting value. The current monitor continuously reads analog values coming from a shunt resistor in the power supply; this signal is proportional to the actual PS output current. If it drops below a fixed threshold value, a flag is set.

The interlock bypass request handler monitors the keyswitch which allows the spin rotator system to enter a hot maintenance state in which cover interlocks may be selected for being bypassed. Together with the flags set by the current monitor and timer modules, this information is used for generating opening permits for the terminal cover enclosures. This module also drives

LEDs on the various displays giving information about the present interlock status of the system.

The electromagnetic latch driver module provides dc power to the push-buttons activating the latches when the system determines it safe to do so. Additionally, a check detecting illegal power at latches is performed.

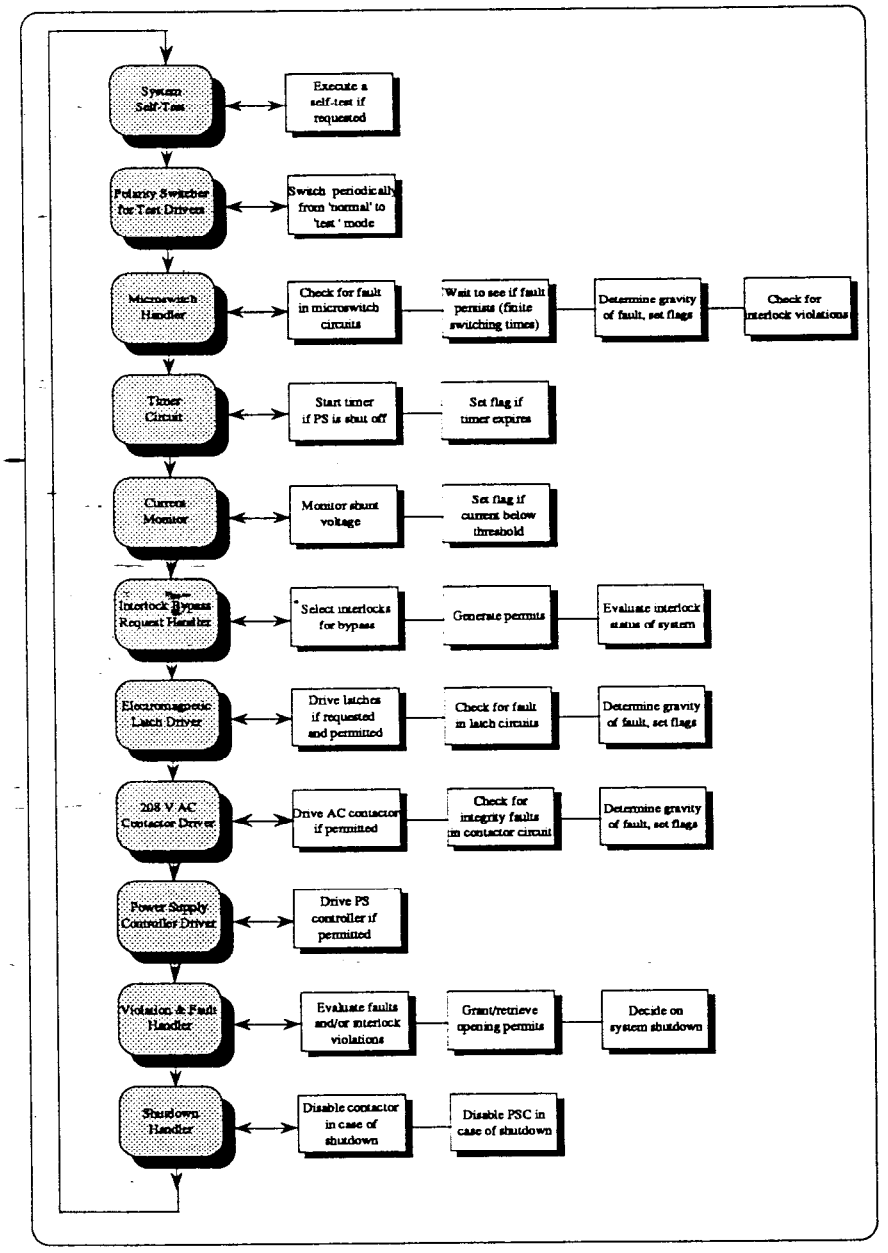


Figure 3: Structure of the Software

The 208 V AC contactor module controls one of the two enable/disable mechanisms for the power supply. If the logic determines that no interlock has been broken and no fault has been detected in the system, a permit is generated and the contact breaker is closed. A readback contact in the circuit breaker allows the PLC system to actually monitor the mechanical action. The other PLC generates an enable signal for the power supply controller at the same time.

The violation and fault handler module analyzes anomalities encountered and decides on whether to retrieve permits and shut down the power supply. This action would be performed by the shutdown handler module which either opens the contact breaker or disables the power supply controller, depending on the PLC system in which the program is running.

The same modules basically run on both PLCs, except for some LED drivers. If one PLC detects a problem, it notifies the other PLC through I/O channels, and appropriate actions are taken.

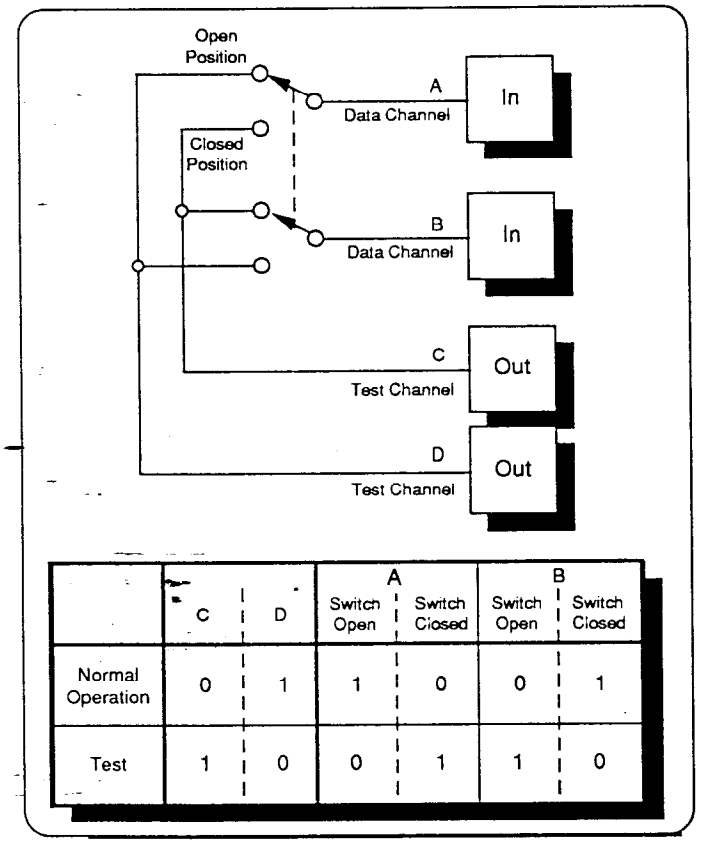
5. Hardware and Software Redundancy Schemes

As outlined in the previous sections, all vital I/O devices come in pairs, and each device of a pair is controlled by one of the two PLCs. Thus, breakdowns in the hardware do not lead to a hazardous situation. Due to the layout of the system, operations cannot continue if one of the CPU modules fails; such a fault leads to a shutdown (redundancy at PLC CPU level, but no fault-tolerance).

Wherever practical, readback channels have been implemented to monitor the behaviour of the devices controlled (e.g. power supply, contact breaker). Microswitches (C type) are wired with PLC test channels to support a test-verify capability that detects broken and shorted wires and some internal microswitch problems (see figure 4). The output channels have opposite polarities and are periodically reversed; due to the wiring scheme used, the data channels of a microswitch must also change polarities during the test phase. Identical polarities indicate a fault.

On the software side, integrity checks are performed whenever possible. For example, the user program verifies that no voltage is present at any of the elctromagnetic opening latches if no opening permit has been issued. If a fault is detected, an internal flag describing that fault is set, and the power supply is redundantly shut down by the two PLCs. In order to bring the system on-line again, a maintenance person first inspects the main control panel where LEDs indicate the nature of the problem (which PLC detected the fault, and whether it was an

I/O fault like a short, or an inconsistent interlock state or a disagreement between the two PLCs). For getting more refined information about the failure, it is possible to hook up a portable terminal to the PLCs and display the various fault flags. They convey enough information to adequately point to the cause of the trouble.



	C	D	A Switch Open	A Switch Closed	B Switch Open	B Switch Closed
Normal Operation	0	1	1	0	0	1
Test	1	0	0	1	1	0

Figure 4: Test/Verify Capability for Microswitches

6. Project Status

The development of the software described above has mostly been finished; this work has been done on a lab R & D system which consists of an IBM PC/XT running STEP 5, a rack with a S5-150U CPU crate and an associated I/O crate, and simulator panels with LEDs and switches mimicking the spin rotator environment. By exclusively utilizing STEP 5 language constructs available on the S5-100, software compatibility has been achieved. Processing and I/O scanning speeds are not crucial for this application, so that the slower execution of the program on the lower-end PLC won't affect its functionality.

At present, the S5-100 system is being procured, and the software is being partitioned into the two versions running on the redundant CPUs. As a new task, the inter-PLC communication has to be implemented. Once completed and tested, the interlock equipment will be wired to the actual magnets and power supplies, and tested to evaluate its behavior. Finally, the complete spin rotator system with interlocks will be installed at iin the accelerator.

7. Summary

SLAC is developing an electrical hazard interlock system based on dual redundant PLCs. Sensitive I/O is implemented and processed in a redundant fashion. The PLCs make sure that terminal covers cannot be opened while dangerous currents are flowing, and redundantly shuts off the power supplies if any interlock violations, faults in the I/O circuits or problems in the PLC system itself are detected. A first version of the software running on a single CPU has been developed, and is being adapted and finalized for installation in the final PLC systems.

8. References

[1] H.V. Walz, *Conceptual Design Report Distributed Supervisory Protection Interlock System DSPI*, Electronics Department Internal Report, SLAC, July 1987

[2] H.V. Walz et al, *Distributed Supervisory Protection Interlock System*, to be published in the Proceedings of the 1989 Particle Accelerator Conference, Chicago.

[3] Siemens Energy and Automation, Inc., Programmable Controller Division, S5-100 Series PLC, Catalog 52.1, Peabody, MA 01960, 1988.

[4] Hans Berger, *Programming of Control Systems in STEP 5*, Vol. 1 and 3, Siemens Aktiengesellschaft, Munich 1980.

---

* Work supported by the Department of Energy, contract DE-AC0376SF00515.