LCLS Personnel Protection System Architecture

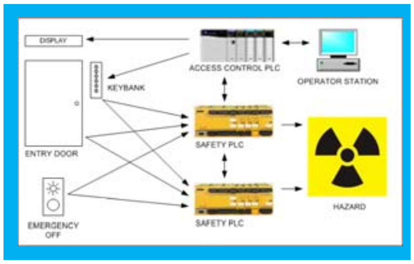
Patrick Bong, Enzo Carrone
SLAC National Accelerator Laboratory, USA

① Introduction

Programmable systems are becoming the *de facto* standard for Safety Interlock Systems, allowing for increasing complexity of personnel protection. The SLAC National Accelerator Laboratory has implemented a programmable safety interlock system utilizing a graded approach to protect personnel from exposure to prompt radiation.

The Personnel Protection System (PPS) architecture is based on two tiers of programmable systems performing access control and safety interlocks. The strategy consists in isolating the safety functions from the access control and system monitoring performed through EPICS. The isolation allows the safety functions to be guaranteed even in the absence of a fully working control system.

The safety functions are performed by redundant Programmable Logic Controllers (PLC) certified for safety applications. Each PLC was programmed by an independent engineer to provide some level of diversity and defense from coding errors. Functional testing was performed through a test bench and, after deployment, through a field checkout procedure designed to certify the system for operation. New processes were developed to manage the life cycle and the integration with existing installations.



② Overview

Operators remotely control access into the hazardous zone using an EPICS workstation. The Access Control PLC is an IOC on the controls network which controls the release of keybank keys and releases the magnetically locked door. The Access Control PLC also provides status to the Operator Station and personnel at the Entry Door.

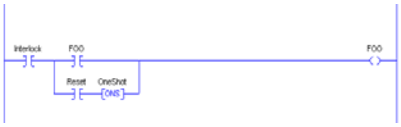
The redundant Safety PLCs monitor the interlock switches and inhibit the operation of the hazards. The Safety PLCs are cross interlocked such that if either PLC detects a fault the other PLC will also inhibit the hazard. A communication path between the Safety PLCs and the Access Control PLC allows the Operator Station to monitor the interlock status.

③ Two Subsystems

The PPS is divided into two subsystems: a basic process control system and a safety instrumented system. The purpose of the latter is to render the system to a safety state when predetermined conditions are violated.

Access Control and Status

Devices that are used to control the PPS or provide status to personnel in a PPS area but are not either redundant or interlocked for safety are wired to a single general use PLC. The PLC used for access control, local status and communications interface to the EPICS control system is an Allen-Bradley ControlLogix 5000, programmed in Ladder Logic.

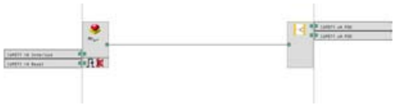


Ladder Logic

Ladder logic is a graphical based programming language based on schematic symbols used in relay-based hardware logic. In the logic above, Interlock must be high before resetting the output FOO. The Reset signal is buffered by OneShot that keeps FOO from resetting if the Reset signal is always high. FOO is used as an input to itself to perform a latching function.

Safety Critical Interlocks

All PPS hardware that is interlocked to the machine for the safety of personnel is wired to redundant safety PLCs. The two safety PLCs are programmed independently by two safety system engineers to reduce the risk of common mode errors. The PLC used for safety functions is the Pilz PNOZmulti programmable modular safety relay, programmed with Function Blocks (which are part of a limited variability language). The limited variability language is a set of well defined functions that are used to build an application within a structured framework.

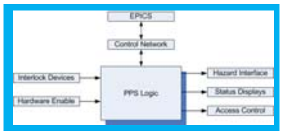


Function Blocks

Function block logic is a graphical based programming language based on block diagrams. In the logic above, Interlock must be high before resetting the output FOO. The Reset signal is defined as monitored and keeps FOO from resetting if the Reset signal is always high. This logic performs the same function as Fig. 2.

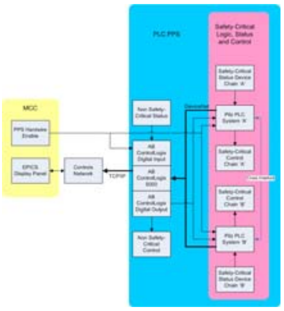
④ Communications

Data from the PPS are stored in an array on the Access Control PLC and retrieved by the control system through TCP/IP. Commands from the Master Control Center (MCC) are sent through an EPICS interface via TCP/IP. Commands are ignored by the Access Control PLC unless they are validated by a Hardware Enable, a signal that is hardwired to the PLC from the control center.



Control signals required for safe operation are hardwired from an output card on the Access Control PLC to an input on the Safety PLC. The Safety PLCs also receive a Hardware Enable for transient signal from the control system, such as reset commands.

Data from the redundant Safety PLCs are sent to the Access Control PLC through a dedicated DeviceNet network. The safety PLC application software cannot be modified through the DeviceNet network, but requires a serial link (which is disconnected while the safety system is in operation). The Safety PLC sets all outputs to a safe state when the application software is modified.


MCC
PPS Hardware Enable
EPICS Display Panel
Controls Network
TCP/IP
PLC PPS
Non Safety-Critical Status
AB ControlLogix Digital Input
AB ControlLogix 5000
AB ControlLogix Digital Output
Non Safety-Critical Control
DeviceNet
Safety-Critical Logic, Status and Control
Safety-Critical Status Device Chain 'A'
Pilz PLC System 'A'
Safety-Critical Control Chain 'A'
Safety-Critical Control Chain 'B'
Pilz PLC System 'B'
Safety-Critical Status Device Chain 'B'

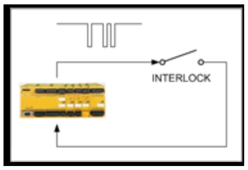
⑤ Cross Interlock

The Safety PLCs send a status bit to each other. The status bit is an indication that the controller is in a safe state and ready to permit the operation of the hazard. Each controller inhibits the hazard permit until the controller receives the safe state status bit from the other controller. The safe state status bit is asynchronous to the hazard permit.

⑥ Monitored Interlock Voltages

The Pilz Safety PLC has four outputs with a unique periodic pulse that are used as Monitored Interlock Voltages. Inputs are programmed to receive the diagnostic pulse. The controller fails to the safe state if the pulse is not detected or is not in the correct time frame.

The monitored interlock voltages are sensed by the inputs to verify that no cross wiring or short circuits have occurred. Each controller has four different monitored interlock voltages. The monitored interlock voltages are also used to make the Chain A and Chain B application software incompatible by applying the formula B=(A+2)modulo4. Inputs to the Chain B controller are powered by different monitored interlock voltages than in the Chain A controller.



Each diagnostic pulse has a unique timing pattern

⑦ Testing

Pre-startup acceptance testing is performed in stages. The safety PLC application software is bench tested before deployment in the field. The logic solver is tested against the specification and certified to be correct.

After the hardware configuration is verified to be correct, the safety PLC applications are loaded and the Access Control PLC application is loaded. The Access Control application is a grade lower than the safety application and is not bench tested.

The Access Control application and the EPICS interface are also tested against the specification and certified to be correct.

Once the application software is verified the Personnel Protection System is tested using an Initial Acceptance Test procedure. The Initial Acceptance Test is reviewed and verified to conform to the specification. After the Personnel Protection System is tested the system is certified for safe operation.

SLAC NATIONAL ACCELERATOR LABORATORY