

LOW ENERGY BOOSTER PERSONNEL ACCESS SAFETY SYSTEM

Richard R. Parry
Superconducting Super Collider Laboratory
2550 Beckleymeade Avenue, Dallas, TX 75237 USA

3.7 PERSONNEL ACCESS SAFETY SYSTEM

3.7.1. DEFINITION

The Low Energy Booster, like any high-energy accelerator contains serious personnel hazards with the potential for deleterious results if precautions are not implemented. Hazards for most accelerators include: electrical hazards (high voltage and high current), ionizing and non-ionizing radiation, flammable gases, and high magnetic fields. For the LEB, the predominate hazards of concern are electrical shock and ionizing radiation exposure to the primary beam, both of which can be obviated or mitigated by controlling personnel accesses into the tunnel enclosure. Outside the enclosure radiation levels are much less of a danger due to the radiation shielding. However, radiation interlocks are still used to insure the beam is inhibited at its source in the event of excessively high radiation levels outside the enclosure. The LEB Personnel Access Safety System (PASS) is used to protect personnel from these hazards in underground enclosures by controlling electrically hazardous power supplies and beam safety devices.

Electrical hazards are controlled by a robust fail-safe interface between power supplies and other similar devices. Specifically, the control point is as close as possible to the power source so as to bypass less reliable shut off mechanisms. In most devices this is the power supply contactor that turns off all power to the device. A contactor acts much like a relay. To further ensure the integrity of the interface, a feedback signal is provided by the contactor to sense that it functioned properly. In the event that devices are inhibited by the system and feedback from the system indicates a malfunction, an alarm is initiated and personnel access into the LEB tunnel is not allowed. The proton beam from the LINAC into the LEB is controlled in a similar manner. The devices used to control beam, typically referred to as radiation critical devices are power supplies that control bending of the beam into the LEB. By controlling and monitoring these devices, beam can be inhibited if necessary.

Although the actual design discussed herein was not implemented in the LEB, a very similar system was installed and remained operational for two years in the Accelerator Systems String Test (ASST) facility [1]. The ASST differs from the LEB in being smaller (600' in length) and does not produce radiation; however, in most other respects it serves as a testing ground for the LEB PASS and a proof-of-concept.

3.7.2. THE CONTROLLER

The requirements of a safety system are more or less well understood due to numerous other accelerators that have been previous built. However, the magnitude of the SSCL project places many unique requirements on the design. Each PASS (LINAC, LEB, MEB, etc.) at the SSCL is predominately independent; however, dependencies exist among the accelerators making communication between the systems necessary. It is therefore imperative that all SSCL safety systems work seamlessly together and can be easily integrated. Thus driving the LEB requirements in large part is the worst case design, namely the Collider system. The LINAC, LEB, and MEB are small enough to allow use of conventional technologies such as standard electromechanical relays with their inherent high reliability and fail-safe nature. However, the High Energy Booster (6.8 mile circumference) and the Collider (54 miles) force a different solution. Problems encountered with standard electromechanical relays include excessive voltage drops that are experienced over vast distances that would be prevalent in the enormous machine. In addition, a number of cables are necessary, again making relays an impractical solution.

An electronic implementation of the PASS using digital communication was therefore adopted. Large computer-based controllers such as CAMAC and VME systems are possible, but generally considered too flexible and difficult to manage for safety applications. Programmable Logic Controllers (PLC) have been available for many years and

have advanced to the point where they are being accepted as acceptable solutions in safety applications. The PLC solves many of the problems of relays and was therefore chosen as the controller for the system [2, 3, 4].

3.7.3. REDUNDANCY

The PASS must provide redundancy [5]. Redundancy takes many forms and varies with the application. In systems where safety is not the prime concern, redundancy typically takes the form of two independent systems with only one being operational at any given time. In the event one system fails, transfer of operation from one system to the other occurs. This type of system is also referred to as a 1 out of 2 voting system (one controller must function to keep the system running). Redundancy as used in safety critical applications and as used herein, means 2 out of 2 voting. Two controllers must function to keep the system running, if either system fails, the operation of the accelerator will shutdown. At one point in the design phase of the LEB PASS, a 2 out of 3 voting scheme was considered. This type of system has the great advantage of allowing a failure, while still remaining operational. Such high availability schemes are often implemented in systems such as the space shuttle, where the system must continue to run during a failure and possibly multiple failures [6, 7]. This design was eventually dropped due to cost and the questionable need for such a system.

This redundancy makes the system significantly more reliable from a safety stand-point which is our goal. Speaking strictly from a safety standpoint, reliability is the key issue: one must fail on the side of safety. However, doubling the number of components reduces the availability by doubling the number of components that can fail. In a very large system such as the SSCL, reliability is a key issue that must be addressed. Studies were conducted among various systems to maximize availability (no availability value was specified specifically for the LEB PASS). The investigation included obtaining manufacturer's mean time before failure (MTBF) data for various PLC modules and calculating availability [8, 9]. Although availability was a key issue, other factors entered into the decision making process such as availability of I/O modules, experience, support, software tools etc.

Wherever possible, the field devices are also redundant. For example, on each of the personnel access doors that leads into a hazardous area, two door sensing switches are used. One door switch serves as an input for one PLC and the other sensor is connected to the other PLC system. In those cases where two separate field devices are not practical, two signals are derived from a single point (e.g. two electrical contacts from a single emergency scram switch are used for control).

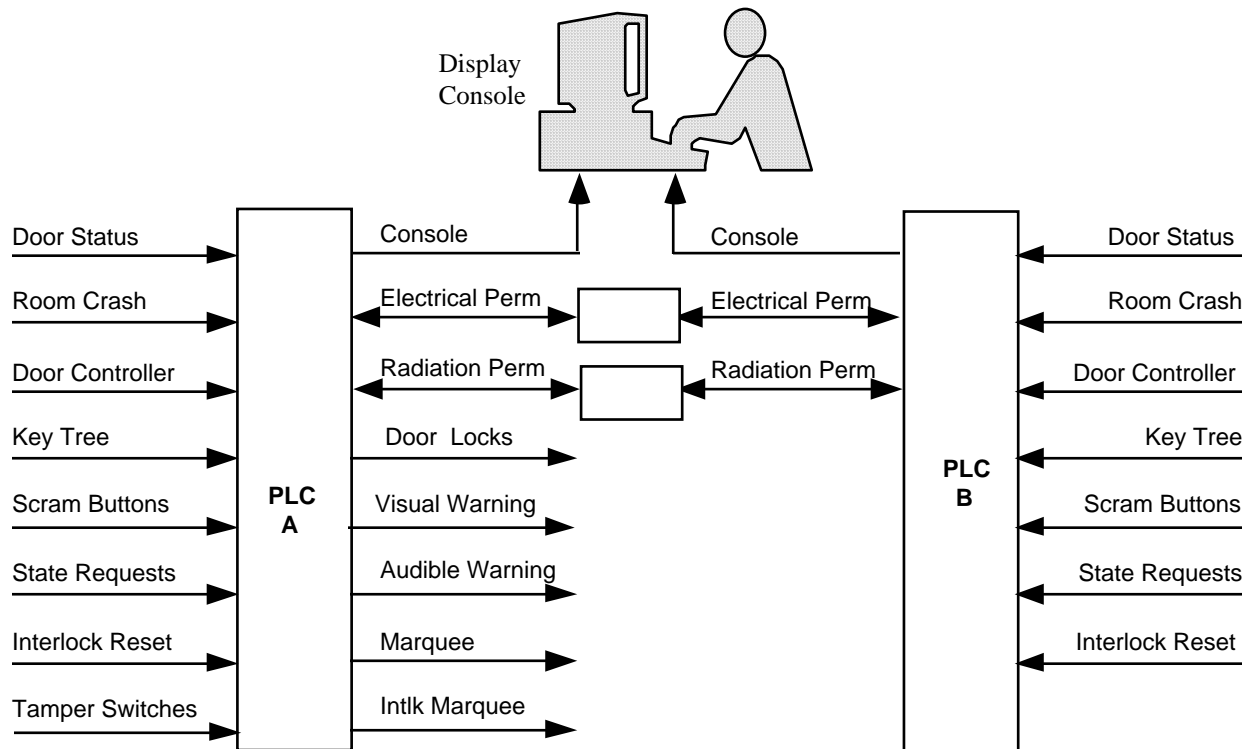


Figure 1. System Block Diagram. The system is comprised of dual redundant programmable logic controllers. Critical field devices such as personnel access door sensors are also redundant. Non-critical devices are not controlled redundantly which accounts for I/O points on PLC A which are not also on PLC B.

3.7.4. SOFTWARE

PLCs like all programmable systems carry the burden of being software driven. To increase software reliability, two individual programmers are used to program each of the controllers, the advantage being that two individuals are not likely to make the same error. In addition, the system is programmed in a graphical language called Relay Ladder Logic (RLL). The language shows visually the flow of control and therefore allows one more easily to detect errors than in conventional text languages. Other precautions used to insure software reliability are careful peer reviews, extensive software testing, and strict software configuration management. Configuration management refers to the administrative procedures developed to insure that the system is operating under the correct software.

The console display of information is implemented using Experimental Physics and Industrial Control System software (EPICS), which is also used from the accelerator control system. This software package is powerful and versatile, however, the sole purpose of the display subsystem is to monitor the PASS rather than to control. The safety and integrity of PASS is enforced by insuring that no control communication takes place between the PASS and the console.

3.7.5. FAIL-SAFE DESIGN

A fail-safe design is another major requirement for the LEB PASS. Designing a fail-safe system using standard electromechanical relays is relatively easy since they are inherently fail-safe. PLC based systems are somewhat more difficult to be fail-safe; however, many of the standard design concepts can be used such as insuring the devices are energized to remain operational. In this way a loss of power will cause the system to fail in the desired state. Other precautions implemented are “watchdog timers” or “heartbeats” that must be periodically pulsed to insure proper operation.

Other ways adopted to ensure that the LEB PASS fails safe include using commercially available devices that were specifically designed for safety and security systems. For example, the door access sensors are fail-safe and tamper proof.

3.7.6. MISCELLANEOUS SAFETY REQUIREMENTS

To prevent damage or tampering to the system, all cables are protected in their own dedicated electrical conduit. In addition, all relay racks, cabinets, and enclosures are locked and monitored. Only authorized personnel have access to safety system components.

In the event there is a need to make an emergency exit from the enclosure, emergency crash buttons located inside the enclosure are used to release locked doors and inhibit radiation and electrical hazards. This emergency switch bypasses the PLC control system completely, so even in the event of a dual PLC fail-to-danger state, emergency egress from the enclosure is possible.

There is a need to display critical information to the user in a clear and unambiguous manner. The LEB PASS design has gone to great lengths in this area. For example, above each of the personnel access doors is a large 4” x 36” scrolling marquee display to clearly indicate to personnel the state of the machine (i.e. open access, restricted access, etc.).

The Operator Interface or console display uses a Graphical User Interface to clearly display PASS information. Color graphic display screens are used which show the tunnel outlines with doors indicating their open or closed state graphically and in color.

A chief operator in the control room is responsible for the safety of personnel. All safety related control of the system requires a unique physical key (e.g. door access key), thereby preventing unauthorized control of the safety system. All personnel entering the hazardous area must be accounted for before the system is made operational. Accountability is accomplished by allowing only personnel who have taken a key to enter the area. Once a key is removed, the machine is disabled and cannot be run until all keys have been returned. In addition, only authorized personnel are allowed access. A computer database is scanned to assure that the individual wishing access has had the necessary training and is medically fit to enter the hazardous area.

Testing the system is performed routinely every 6 months. All modifications are strictly controlled and all changes result in the re-testing of the system.

3.7.7. PASS ACCESS STATES

The LEB PASS needs to accommodate various operating scenarios and modes. This is most easily accomplished by specifying several well defined states for the system. The LEB PASS is always in one of five states: open, restricted, search, controlled, and closed access. Each state relates to the type of access that is allowable.

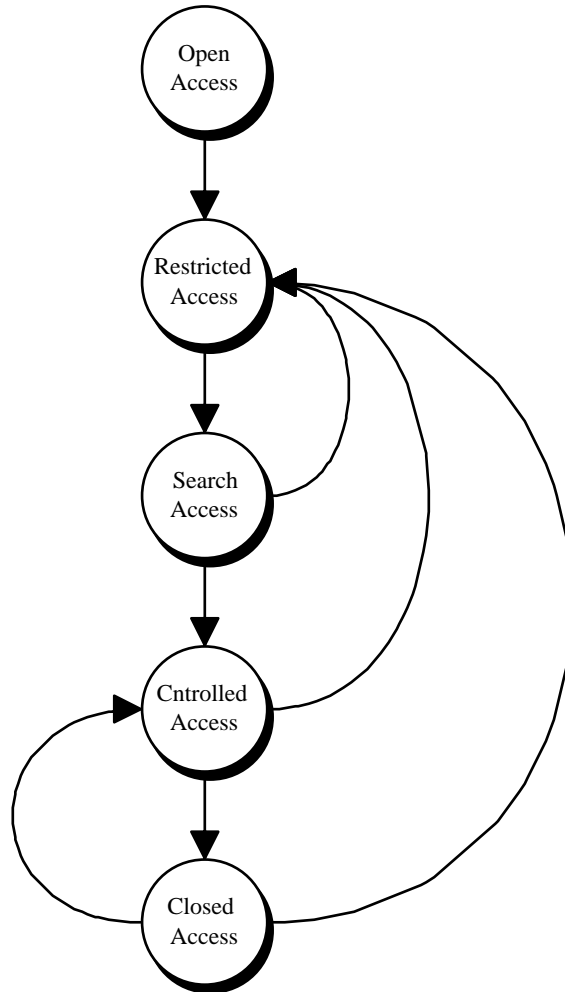


Figure 2. PASS State Diagram. Show above is a simplified state diagram which specifies allowable states and possible transitions between the states.

3.7.7.1. OPEN ACCESS

In the open access state, access into the area is void of electrical and radiation hazards. Thus open access would typically exist only during the very early stages of the prior to LEB commissioning. Once hazards are introduced into the tunnels, all personnel accesses are restricted.

3.7.7.2. RESTRICTED ACCESS

Restricted access is available to personnel during those periods when the system is “down” with electrical and radiation hazards mitigated. Personnel entering the area must be qualified and have required training. The PASS also provides the mechanism for logging personnel into and out of the tunnel.

3.7.7.3. SEARCH ACCESS

Before operating the LEB, all persons must be evacuated from the area. This is referred to as searching-and-securing and is accommodated by the PASS in the search state. The search of the area is a combination of administrative and electronically enforced procedures. Administratively a team of two qualified personnel search the tunnel moving from point to point resetting interlocks. As the search team proceeds through the area, they carefully inspect under and around all structures to ensure personnel are not present. Under no circumstances does the team proceed with the search leaving any personnel behind in the secured area. This team is authorized only after careful training in securing the area. During the time that the two person search-and-secure team evacuates the area of personnel, no further accesses are allowed.

Door-interlock boxes are located at each of the access points. These units sense the door's position via switches affixed to the door. They also serve as a means of forcing the search team to secure the area in a pre-defined sequence. The interlock boxes will not reset if an attempt is made to reset an interlock out of sequence. Any attempt to reset an interlock unit out of sequence will void the search and force the team to begin again.

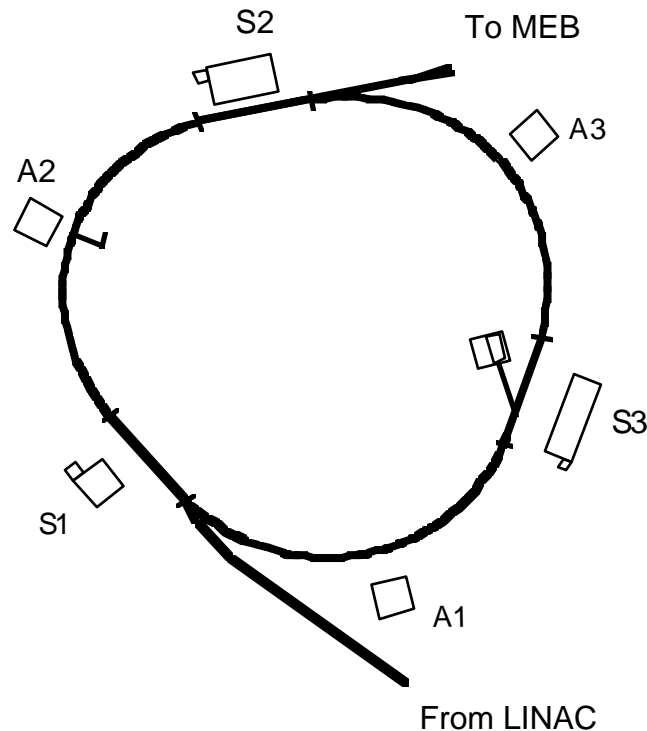


Figure 3. LEB service buildings and tunnel. The major access point into and out of the LEB is a building S3 where the controlled access booth is located. An emergency egress point is provided at A2.

3.7.7.4. CONTROLLED ACCESS

Controlled access is permitted for limited periods to allow personnel to enter the area in a carefully controlled manner without requiring the area to be secured again by a search-and-secure team. The PASS requirements include strict means of insuring personnel accountability for persons entering the tunnel. The exact controlled access procedure forces personnel to start at the control room where the chief operator on duty is responsible for the safe access of personnel. After being verified for proper training, personnel consisting of a minimum of two persons (buddy system) proceed to the Controlled Access Booth (Figure 4), often called a man-trap in the security industry. The procedure for entering and exiting is used extensively at high-security installations. At the SSCL, it is used as a means of assuring personnel accountability and safety. If the personnel wishing to make an access are qualified, the chief operator issues a key to each of the persons. A computer logbook is provided to keep a record of all accesses. The safety control system clearly displays all personnel who have keys along with the date and time the key was taken. This assures that at all times, the chief operator knows who is in the enclosure.

At door D1, personnel call the control room using the intercom and request that the door be opened. While watching the access via closed circuit TV, the chief operator enables the access by remotely unlocking door D1.

When personnel are in the booth with door D1 closed, the chief operator releases D2 which automatically locks D1. This technique assures that at all times the access is controlled and that at no time is it possible for unauthorized personnel to have access since the chief operator is always in control. When personnel are ready to exit, they signal the control room via the intercom inside the enclosure at door D2. The operator in the control room remotely opens door D2 which automatically locks D1. Again the chief operator must watch the controlled access booth to ensure no additional personnel enter. Exiting personnel return their keys to a key tree. The chief operator completes the controlled access by logging the access complete.

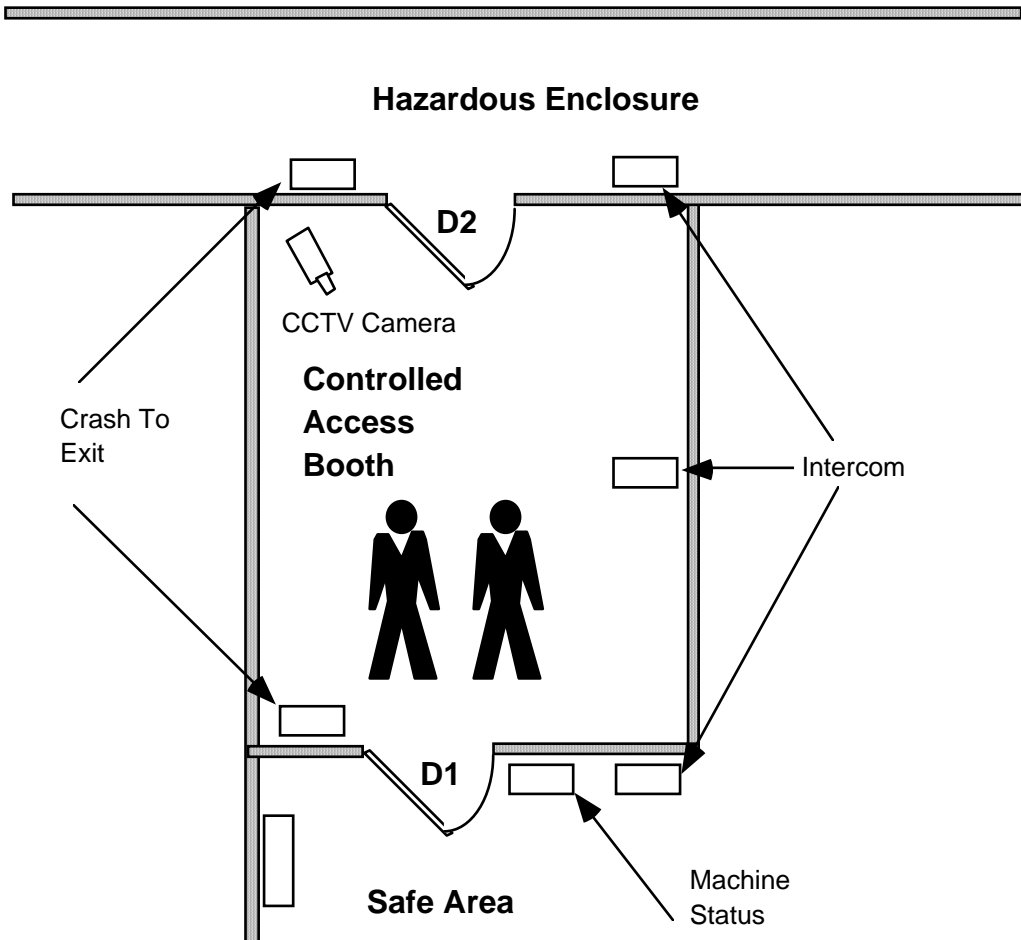


Figure 4. Controlled Access Booth (CAB). This 4' x 8' room is used to control accesses into and out of the area. The entire process is remotely controlled and monitored by authorized personnel in the control room. Note two crash buttons used to exit the CAB in the event of an emergency.

3.7.7.5. CLOSED ACCESS

Resetting the system in preparation for running the machine automatically triggers an audio message throughout the LEB enclosure. Therefore, in the unlikely event personnel are in the tunnel who have been overlooked by the search-and-secure team, they are given ample time to leave the area or actuate one of the numerous scram (crash) buttons located inside the LEB tunnel. After the audio warning time-out, the personnel access safety system enables power supplies and other hazardous devices allowing them to be safely energized. At this point the system is considered operational and no further access is allowed into the LEB.

3.7.8. CONCLUSION

The heart of the LEB PASS consists of the redundant fail-safe programmable electronic controllers which are used to control and monitor the many aspects of safety relating to electrical and radiation hazards within the enclosures. The system monitors personnel access points, emergency crash buttons, power supplies, radiation critical

devices, and numerous other devices to insure the safety of personnel entering the LEB tunnel. Although Programmable Logic Controllers are new to safety systems they have proven to be viable alternatives to traditional electromechanical relays and adequately meet the requirements of a large distributed safety system. The system permits quick and easy controlled access of personnel into and out of the underground LEB tunnel. Retaining strict and safe control of personnel is enforced by keeping the system in several well defined states. All the concepts and engineering discussed herein were proven at the ASST facility which proved to be an invaluable testing ground for the LEB PASS and all SSCL safety systems.

REFERENCES

- [1] R. Parry, "Personnel Access Safety Systems", *Proceedings of the Industrial Computing Conference*, Vol. 2, p 437, ISA 1992 – Paper #92-0467.
- [2] P. Gruhn, "Risks With Using PLCs for Safety Protection", *C & I*, September 1990, p 53.
- [3] B. Balls, P. Gruhn, "Design Considerations for High-Risk Safety Systems", *Intech*, March 1991, p 28.
- [4] T. Fisher, "Control Systems Safety," *ISA Transactions*, The Quarterly Journal of the ISA, Volume 30 Number 1, 1991.
- [5] "SSCL Site-Specific Conceptual Design", SSCL-SR-1056, p 580.
- [6] A. Frederickson, "Fault Tolerant Programmable Controllers for Safety Systems", *Programmable Controls*, March 1989, p 109.
- [7] R. Waterbury, "Fault-Tolerant / Fail-Safe Systems are Fundamental," *Intech*, April 1991, p 35.
- [8] PES – Programmable Electronic Systems in Safety-Related Applications, *Health and Safety Executive*, HMSO, London, UK, 1985.
- [9] R. Parry, "Personnel Electronic Safety Systems," Presented at the Particle Accelerator Conference, Washington D.C. 1993.