

PERSONNEL ACCESS SAFETY SYSTEM

Richard R. Parry

**Chief Design Engineer, Global Machine Safety Systems
Superconducting Super Collider Laboratory
Dallas, TX 75237**

KEY WORDS

Safety, Access Control, Oxygen Monitoring,
Programmable Logic Controllers,
Redundant, Fail-Safe

ABSTRACT

PROCESS

This paper describes the method and system used to control personnel accesses into hazardous areas at the Superconducting Super Collider. Hazards encountered are electrical (high voltage and high current), radiation (ionizing), cryogenic fluids (liquid helium and nitrogen), flammable gases, and ultra high magnetic fields. Although these are a diverse group of hazards, virtually all can be mitigated by controlling accesses into the hazardous enclosures. The Personnel Access Safety System (PASS) is used for this purpose. The system is comprised of dual redundant Programmable Logic Controllers (PLC) using 1oo2 voting (either system can bring the system down to a safe state). Numerous safety related hardware and software features have been built into this system to assure high reliability and availability.

INTRODUCTION

The Superconducting Super Collider Laboratory (SSCL) is a high energy research laboratory operated by the Universities Research Association (URA) under contract from the Department of Energy (DOE). When completed in late 1999, it will be the largest particle accelerator in the world (Figure 1). The laboratory is a complex of five proton accelerators: the Linear Accelerator (Linac), Low Energy Booster (LEB), Medium Energy Booster (MEB), High Energy Booster (HEB), and the Superconducting Super Collider (SSC). Each accelerator, more commonly called machines, accelerates

large numbers of protons (10^{14}) to speeds approaching the speed of light. The size of the five machines range from the modest Linac, 0.2 miles, to the massive Super Collider which measures 54 miles in circumference. To protect the environment and personnel from radiation, all five machines will be built below ground. The deepest is the Super Collider which varies in depth from 45 to 280 feet due to irregularities in the surface of the earth, rather than irregularities in the design of the Super Collider. When complete it will encircle the entire city of Waxahachie, Texas; dozens of smaller cities and towns, and travel under several lakes.

Superconducting Super Collider Laboratory

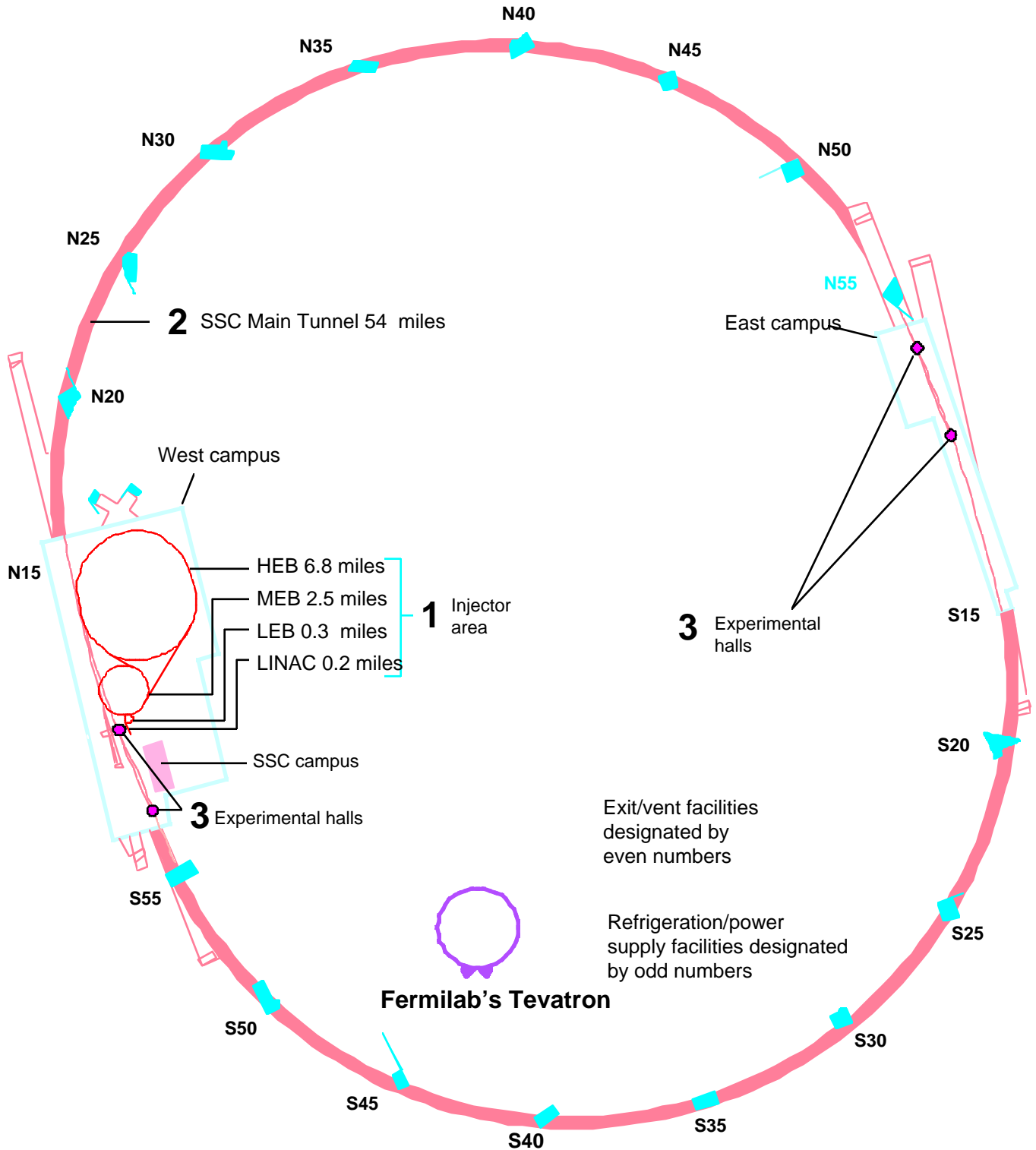


Figure 1. The Superconducting Super Collider Laboratory. The SSCL is a proton-proton collider operational in the year 1999 with a maximum collision energy of 40 trillion electron volts. 1. Protons will be collected and accelerated in the injector area. 2. They will be sent into two pipes and will circle in opposite directions in the main tunnel. 3. The beams will cross at experimental halls where the protons will collide. The Fermilab Tevatron is currently the largest accelerator in the US.

At this writing, these machines are still in the design phase. The commissioning dates extend over the period from 1994 to 1999. Before these machines come on line there is much design and testing to be performed. To aid

in this development, a special Accelerator Systems String Test (ASST) facility has been developed. This first system is operational and its design constitutes the remainder of this paper.

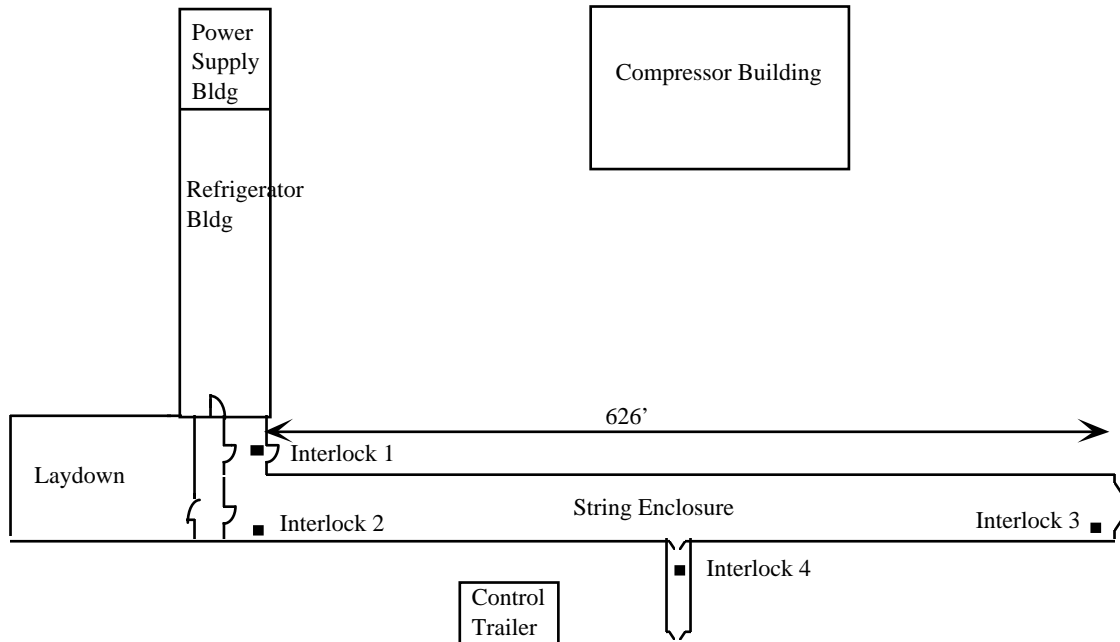


Figure 2. ASST Building. The number located next to each of the access points represents the search sequence used by the search team to evacuate the area. The controlled access booth is located in the niche in the center of the string enclosure.

THE ASST

Of particular importance to the success of the project are the superconducting magnets used in the Super Collider. Over 10,000 mammoth 50' long superconducting magnets weighing over 15 tons each will be installed in the tunnel. The primary purpose of the ASST is to test the design of this key component. It also serves as a test bed for the personnel access safety system that will be used throughout the entire laboratory complex to control personnel accesses into hazardous tunnel enclosures. Although similar to a security system, the system's goal is safety, not security.

The first phase of the SSC project is the installation, fabrication, and testing of a half cell of superconducting magnets at the facility located at ground level 6 miles west-southwest of the city of Waxahachie, Texas. A half cell string contains five dipole magnets, a quadrupole magnet, and three spool pieces which measures approximately 310'. The enclosure is 626' in length with provisions for an ultimate length of 1771'. The enclosure will easily accommodate a half or full cell string of magnets. Phase 1 of the project will demonstrate that a

half cell string of superconducting magnets can be installed, leak checked, cooled to liquid helium temperatures, energized, and safely quenched.

THE SAFETY SYSTEM

For the ASST facility, the purpose of a personnel access safety system is to prevent injury from electrical and oxygen deficiency hazards. This is accomplished by carefully monitoring and controlling elements such as the personnel access points leading into the hazardous enclosures, dangerous power supplies, and the flow of cryogenic fluids.

Personnel Access Safety System

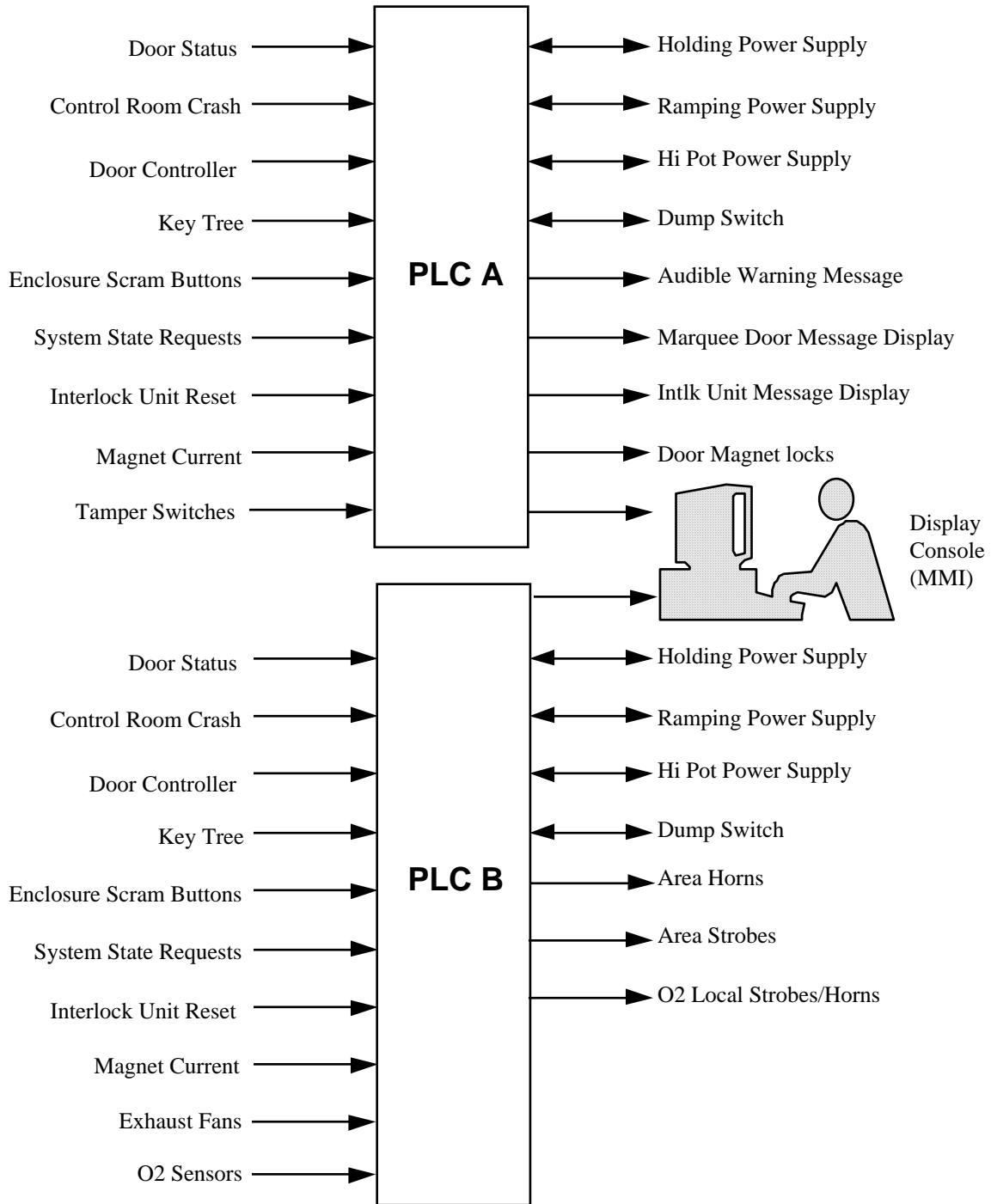


Figure 3. Personnel Access Safety Control System. The system is comprised of dual redundant programmable logic controllers. Numerous field devices are used to control personnel accesses into the area and assure the safety of individuals.

Heretofore, such safety systems have relied heavily on relay logic due to its inherent high reliability and fail-safe nature. However, the size and in particular the distances involved in the Super Collider mandate the use of newer technologies. For this reason, early in the project, the use of Programmable Logic Controllers was decided upon.

The personnel access safety system consists of dual programmable logic controllers (Figure 2) to monitor and control the myriad aspects of safety. An important field device is the interlock boxes which are located at each of the access points to monitor and control the doors. Equally important are the keys which are used to ensure that hazards cannot be enabled if personnel are inside the enclosure. This is accomplished by requiring each person that enters the area to take a key for his personal protection. The system has been designed not to enable hazards unless all keys are returned.

SAFETY FEATURES

By some standards, the system is small; it contains less than 300 I/O points. What makes the system unique is the hardware and software safety features that have been incorporated.

Redundant PLCs. Two complete programmable logic controllers referred to as PLC A and PLC B, are on line at all times using 1 out of 2 (1oo2) voting scheme, meaning any 1 system can cause the system to shutdown, or conversely both systems must be running for the system to be operational.

Redundant Software. Perhaps more unique is the software redundancy. Two programmers are used to program each of the PLCs. One person programs PLC A while the other programs PLC B. The idea behind this technique is to reduce common mode software errors.

Redundant Field Devices. Wherever possible, the field devices are duplicated as well. 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 PLC A and the other for PLC B.

In those cases where two separate field devices are not practical, two signals are derived from a single point. For example, a "scram switch" that disables the entire system in the event of an emergency, two electrical contacts from the switch are used.

Fail-safe. All components of the system are made of the highest quality materials. Where possible, fail-safe devices are used. For example, the switches that monitor the access doors are designed to be fail-safe and tamper proof. In addition, *trolley car* type scram switches located on the wall of the enclosure are used to shutdown the machine in the unlikely event that personnel are trapped inside. The scram switch consists of a 150 ft. long cable cord that one may pull to immediately inhibit hazards.

Here again a fail-safe design was used, if the cable should break the switch fails safe.

Equipment Protection. 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.

Emergency Egress. 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 the locked door. 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.

Status Signs. Clearly a safety system must be critically designed, but just as important is the need to display the information to the user in a clear and unambiguous manner. We have gone to great lengths in this area. For example, above each of the personnel access doors is a large 4" x 36" strolling marquee display using jumbo LEDs to clearly indicating to personnel the state of the machine (i.e. open access, restricted access, etc.).

Console Display. The Man Machine Interface (MMI) uses a Graphical User Interface (GUI) to clearly display information about the system. Many color graphic display screens are used. For example, one shows the building outline with the doors indicating their open or closed state graphically and in color.

Personnel Authorization. A chief operator in the control room is responsible for the safety of personnel. All safety related control of the system requires a unique key thereby preventing unauthorized control of the safety system.

Key Tree. All personnel entering the hazardous area must be accounted for before the system is made operational. This 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 by the individuals. 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.

Warning Message. Resetting the system in preparation for running the machine automatically triggers an audio message throughout the enclosure. Therefore personnel who may be inside are given ample time to leave the area.

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

SYSTEM STATES

The personnel access safety system may be considered a state machine consisting of five unique states, all relating to the type of access that is allowable.

Open Access. No hazards exist during the open access state, therefore personnel may enter and leave the area at will. Typically open access exists only during the very early stages of the project. Once hazards are introduced into the building, all accesses are limited and monitored.

Restricted Access. Restricted access is available to personnel during those periods when the system is “down” with the electrical hazards mitigated. Personnel entering the area must be Oxygen Deficiency Hazard (ODH) qualified and must log in and out of the area.

Search-and-secure. Before operating the machine, all persons must be evacuated from the area. This is referred to as searching-and-securing. During the time that the two man search-and-secure team evacuates the area of personnel, no further accesses are allowed.

Controlled Access. Controlled access will be allowed 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 purpose of this state is to expedite quick, yet safe controlled accesses by personnel into and out of the enclosure.

Run Mode. After a master reset is initiated by an authorized person, the personnel access safety system enables high current power supplies and other hazardous devices allowing them to be energized. At this point the system is considered operational. No access is allowed during this time.

SEARCH AND SECURE

Before power supplies can be energized, it is necessary to search-and-secure the area to ensure that personnel are not present in the enclosure while power supplies are enabled. A two person search-and-secure team is used to sweep the area looking for personnel.

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 must be previously authorized and trained in securing the area.

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 predefined 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 2 shows the building with 4 interlock units at the access points.

CONTROLLED ACCESS

The purpose of a controlled access is to allow personnel to quickly and easily enter the enclosure for brief amounts of time without requiring a sweep of the area. Personnel start the process 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 people (buddy system is strictly enforced) proceed to the controlled access booth (CAB), 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.

Entrance Procedure. 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 wishing to make the access call the control room using the intercom (Figure 3) and request that the door be opened. The chief operator enables the access by releasing 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.

Exit Procedure. 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.

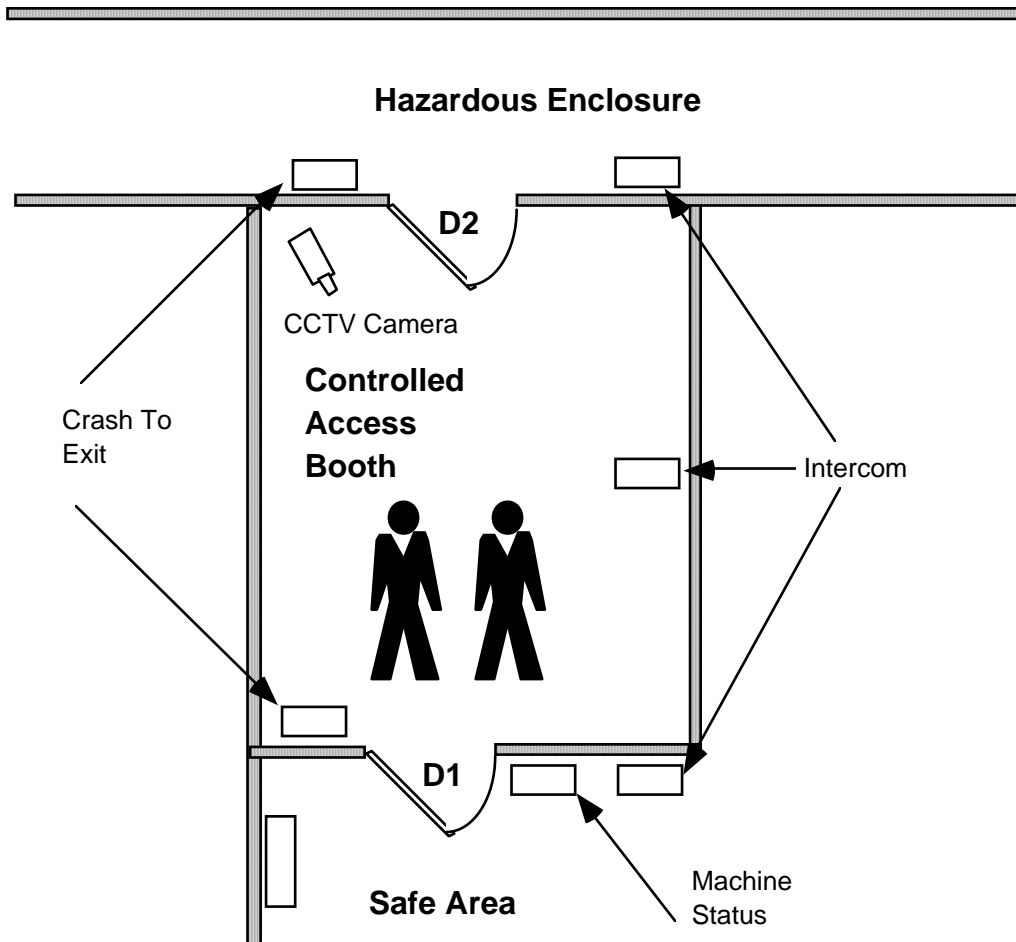


Figure 3. Controlled Access Booth (CAB). This 4' x 8' room is used to control accesses into and out of the area. The entire process is controlled remotely and is monitored by authorized personnel in the control room.

OXYGEN MONITORING

A potential cryogenic hazard associated with superconducting magnets is the accidental release of cryogenics (liquid helium or nitrogen) in the enclosures containing the magnets. The hazard could cause a precipitous drop in temperature over a small area and the local displacement of oxygen to less than life-supporting levels if the release were sufficiently large. The normal partial pressure of oxygen at sea level is 158 mm Hg (760 mm Hg x 20.8%). Deleterious effects due to a lack of oxygen do not occur in healthy individuals until the partial pressure is less than approximately 135 mm Hg which is defined as being an oxygen deficient atmosphere. The ASST oxygen monitoring system has O₂ sensors located strategically throughout the ASST complex. Specifically, the sensors are placed where the highest probability exists

for a leak. These are typically at valves, connecting joints, and other similar locations.

The cells are placed in pairs. One sensor near the ceiling to detect oxygen deficiencies due to a liquid helium leak (helium is lighter than air and rises) and the other near the floor to detect deficiencies from a liquid nitrogen leak (cold nitrogen is slightly heavier than air and falls). Wide area strobe lights and horns provide a visual and audible warning to evacuate the building. A small strobe and horn attached directly to the sensor indicates locally the status of the oxygen sensor and aids in finding the offending sensor from the many sensors located throughout the area.

Electrochemical oxygen cells are used to detect oxygen deficiencies. The more oxygen present, the higher the voltage output from the cell. Conversely, less oxygen

yields less output voltage. The output, nominally 20 mv, is converted to a standard 4 to 20 ma current loop using a signal conditioner. The console (MMI) converts the electrical current value to percent oxygen for display purposes.

The states for the oxygen monitoring system are: normal, warning, alarm, and malfunction. The *normal* state is represented by oxygen levels between 19.5% and 23%, strobe lights and audible alarms are not activated and cryogenic valves are open permitting cryogenics to flow. The *warning* state exists anytime the oxygen level is less than 19.5% and greater than 18.0%, the area wide visual and audible warning system is actuated to evacuate the area. The *alarm* state exists when the oxygen level decreases below 18%. In addition to the area wide visual and audible warning system being actuated to evacuate the area, a liquid nitrogen (LN2) cryogenic valve is closed to inhibit the flow of cryogenics into the building. A *failure* exists when the oxygen reading drops below 0%. This is considered a malfunction since the oxygen content cannot be less than zero. Since this is a safety system, we fail on the side of safety and evacuate the building even though we know the oxygen content is in error. Lastly, since an oxygen enriched atmosphere, one greater than 23% cannot exist, the system treats this state also as a malfunction.

CONCLUSION

There is much designing, testing, installation that must be accomplished over the next eight construction years of the project. The ASST facility is just the beginning. Extending the system to interface to the other larger machines while still keeping the high availability and reliability is of paramount importance. Adding fault tolerance, embedded smart monitors, and fiber optic communications to the system are high priorities that will be addressed in future systems.

ACKNOWLEDGEMENTS

I wish to thank Jay Heefner and Henry Robertson of the Continuous Electron Beam Accelerator Facility (CEBAF) in Newport News, VA for their pioneering work in using Programmable Logic Controllers in personnel safety systems at national accelerators.

Kudos also to Robert Landis, Joe Claborn, and Madhu Reddy of the Super Collider for their great help in developing this system.

