Programmable Electronic Safety Systems

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

Abstract

Traditionally safety systems intended for protecting personnel from electrical and radiation hazards at particle accelerator laboratories have made extensive use of electromechanical relays. These systems have the advantage of high reliability and allow the designer to easily implement fail-safe circuits. Relay based systems are also typically simple to design, implement, and test. As systems, such as those presently under development at the Superconducting Super Collider Laboratory (SSCL), increase in size, and the number of monitored points escalates, relay based systems become cumbersome and inadequate. The move toward Programmable Electronic Safety Systems is becoming more widespread and accepted. In developing these systems there are numerous precautions the designer must be concerned with. Designing fail-safe electronic systems with predictable failure states is difficult at best. Redundancy and self-testing are prime examples of features that should be implemented to circumvent and/or detect failures. Programmable systems also require software which is yet another point of failure and a matter of great concern. Therefore the designer must be concerned with both hardware and software failures and build in the means to assure safe operation or shutdown during failures. This paper describes features that should be considered in developing safety systems and describes a system recently installed at the Accelerator Systems String Test (ASST) facility of the SSCL.

I. INTRODUCTION

Incidents at Bhopal, India and Chernobyl, Russia and much closer to home, the Challenger shuttle disaster are extreme cases of failures that make one appreciate the need for safety systems to control a process. Particle accelerators do not present the same level of hazard. However, the importance of careful design of such systems to protect personnel from those hazards typically found at accelerators such as electrical and radiation, cannot be overlooked. To aid in the design of such systems, the performance goal and requirements must be quantified using reliability engineering and compared to an acceptable level of risk. The question to ask is not, *is it safe*?, but *is it safe enough*?

Using availability to quantify safety system performance, a casual manager might specify an availability of 99.9% thinking this is surely safe enough. However, relating this to the real world would result in 16,000 pieces of mail lost every hour, 22,000 checks deducted from the wrong account every hour, two unsafe landings at Chicago's O'Hare airport everyday, and one hour of unsafe drinking water every month.[1] These examples may seem extreme but they show the importance of developing an acceptable performance level for the process in question.

II. SAFETY SYSTEM DESIGN

A. Overt Failures

Several types of safety system failures have been identified which the designer must be concerned with and if possible prevent. An overt failure of a safety system results in a revealed, fail-safe action. At a particle accelerator this failure might take the form of a coil failure of a normally energized relay opening resulting in a critical power supply turning off. Since these failures result in a safe shut down of an accelerator, the system has failed-safe which is the first concern of the designer. However, these failures are costly as they directly affect accelerator availability. For reasons other than safety, these failure must be prevented.

Overt availability (A_O) can be defined using mean time between failure (MTBF) and mean down time (MDT).

$$A_O = \text{MTBF} / (\text{MTBF} + \text{MDT}) \qquad (1)$$

Since an overt failure is self revealing (i.e., machine shuts down when failure occurs), MDT equals the mean time to repair (MTTR) resulting in the following relationship.

$$A_O = \text{MTBF} / (\text{MTBF} + \text{MTTR}) \qquad (2)$$

B. Covert Failures

Covert failures on the other hand are far more dangerous and typically receive less attention. These failures are hidden and may not be found until a demand is put on the system or some unusual circumstance arises. Covert failures remain in the system and may only be revealed when the system needs to respond. Hopefully these failures are discovered during a system's test rather than an actual need for the system in which the system fails to respond.

Statistically speaking, faults can occur at any time between two successive tests, the average time of half the test interval (TI) must be factored into the equation resulting in the following equation.

$$A_C = \text{MTBF} / (\text{MTBF} + \text{MTTR} + 1/2\ \text{TI}) \qquad (3)$$

Therefore the more frequently a system is tested, the higher the covert system availability. For this reason, frequent testing cannot be overemphasized to discover covert failures. Heretofore systems using simple electromechanical relay logic for control required manual testing (typically at 6 months intervals). Modern electronic systems give greater flexibility and allow frequent automated testing.

[1] Is 99.9% Good Enough, *InTech*, 1989.

B. Common Mode Failures

If a single action can adversely affect the performance of a safety system, the potential for a hazard increases. A common mode failure can be defined as the failure of two or more independent items due to a common cause. Particle accelerator safety systems are typically redundant, but this does not make them immune to common mode failures. For example, two independent magnetically operated proximity switches used to sense an access door may fail to function properly when subjected to a single external stray magnetic field. Common mode failures may be prevented by using active parallel redundancy, in other words, completely independent systems. But even here a careful analysis of failure modes must be considered. For example, a simple solution to the failure of two magnetically operated switches is to use two different technologies for door sensing such as a simple mechanical switch and one magnetically operated proximity switch.

Other solutions include using active sensing rather than passive sensing devices. A conventional switch is static (passive) in sensing an access door's position. An electronic device that continually transmits signals and expects a response is an active solution that in essence "must work to work". This field device has the advantage of failing safe and failures are overt, they are discovered when they occur rather than during a system test that may detect only covert failures.

III. CONTROL TECHNOLOGIES

A. Electromechanical Relays

Heretofore, picking a control system for safety system applications was relatively simple since there were few solutions and it was often mandated that simple, reliable electromechanical relays must be used. Indeed relays have passed the test of time. These systems are unaffected by numerous types of interference, have a low initial cost, are easy to document, and, of utmost importance to safety system designers, they are 98% fail-safe with well understood failure modes.

However, the 98% fail-safe feature is a mixed blessing. It means relay based systems are prone to overt (nuisance) trips. In addition, they are inflexible. Inflexibility for safety systems is a plus, since errors are often introduced when changes are made and not properly tested or documented. However, the inflexibility also means that some useful, albeit unnecessary, changes that one may wish to implement are often not implemented due to the time and difficulty required.

B. Hardwired Solid State Controllers

Some of the deficiencies associated with relay based systems can be overcome by hardwired solid state systems. These systems consist of electronic logic devices hardwired in a specific configuration. In size and weight sensitive applications, these systems have an advantage over relay based systems and allow one to more easily develop redundant systems with low power consumption. Solid state controllers also allow on-line testing of input and output circuits either manually or automatically and therefore serve to increase covert (hidden) availability when tests are performed often.

C. Microprocessor

The microprocessor has come a long way since its initial introduction and has recently crossed the safety system barrier. Like hardwired solid state controllers, implementing automated testing of both the processor's internal health (i.e., memory tests etc.) and external field devices can be easily achieved. Adding an external "watchdog" timer (heartbeat monitor) is also easy to develop and serves as a guard of the overall system's integrity.

Programmable Logic Controllers (PLC) fall into the category of microprocessor based systems. In recent years these controllers have become very powerful and easy to use. Their use in industry for process control is widespread. In addition, these systems are at present in use or under development at several particle accelerator laboratories. However, not all PLCs are created equal and most are not suited for safety applications. Careful consideration must be given safety issues in selecting a specific PLC.

The microprocessor systems may be easily integrated into the main control system over a network. Amenities such as event data logging, simulated human speech announcements, and color graphic operator interface video displays can easily be implemented. Such extras could not economically be implemented in other technologies.

Microprocessors flexibility arises from its software programmability. This flexibility is both an asset and a major area of concern in safety applications. The safety system's designer has well founded fears relating to the reliability of software and its security. Numerous documented incidents of software failures have led to loss of life. Complicating the issue is that while well understood and accepted standards exist for evaluating hardware systems, there is no universally accepted standard for evaluating software reliability.

One solution to the problem of software reliability might be to develop two independent software programs for installation on redundant controllers. This approach has been adopted at the Continuous Electron Accelerator Facility (CEBAF) in Newport News, VA. and here at the SSCL (see Figure 1). The intent of such a philosophy is to prevent software failures, specifically common mode failures. Presumably a software error made by one programmer will not be made by another programmer. However, this method is not a solid solution. There is typically one requirements document developed for a system. One can make a cogent argument that a flaw existing in the specification, will flow into the both programs even though developed separately. Others argue that a careful review process of the software is a solution. Until a standard is developed the issue of software reliability will continue to be of great concern.

IV. ASST

A. Personnel Access Safety System

The Accelerator System String Test (ASST) facility is a surface enclosure measuring 626' in length located at the SSCL. The facility was developed to perform tests on a half cell of superconducting magnets. The hazards within the enclosure are electrical and cryogenic. The safety system consists of dual programmable logic controllers to monitor and control the myriad aspects of safety.

Two independent programmable logic controllers are on line at all times using 2 out of 2 voting (i.e., two of the two systems must be running for the system to be operational).

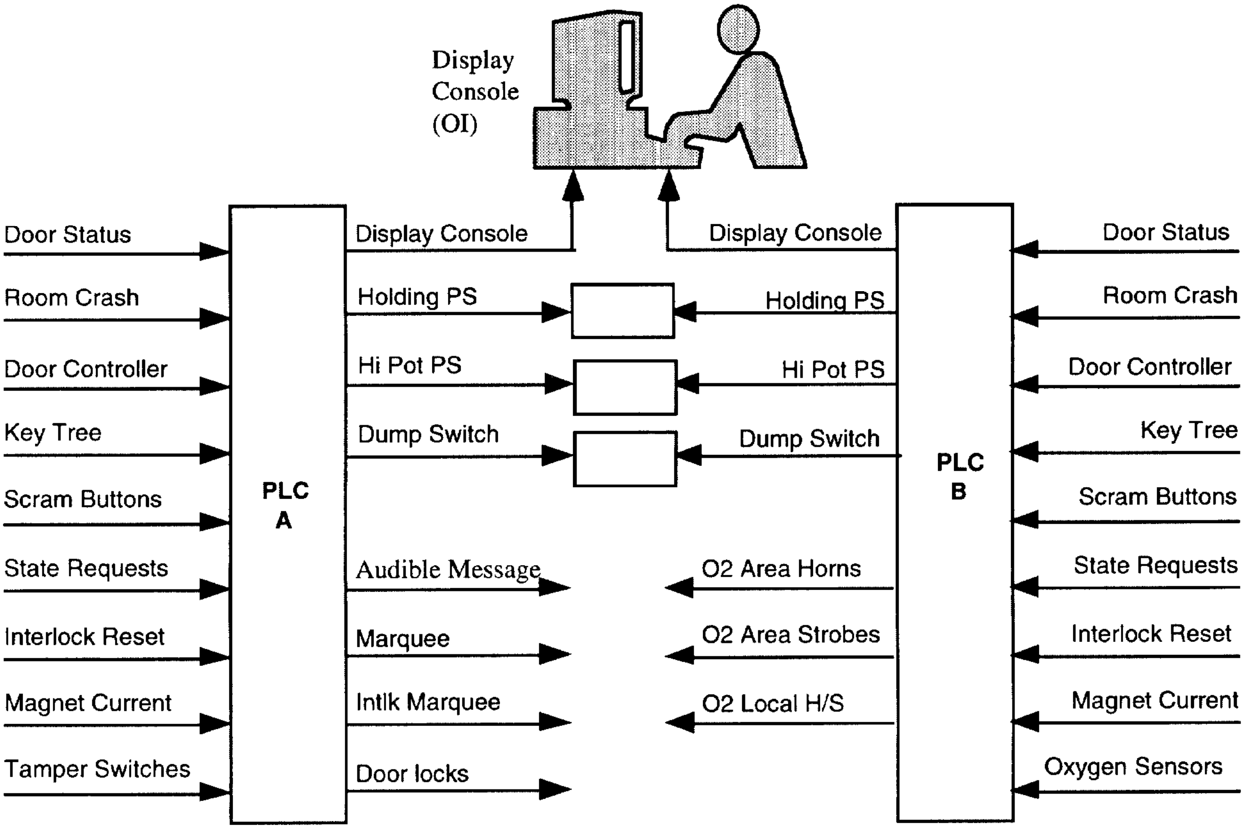

Figure 1. The system is comprised of dual redundant programmable logic controllers. Critical field devices such as personnel access door sensors are redundant. In those cases where two separate field devices are not practical, two signals are derived from a single point.

V. CONCLUSION

Numerous technologies exist today for the designer to solve complex safety problems. However, with the diverse number of solutions comes the need to systematically develop requirements appropriate for the hazards and their consequences. For this reason, a careful examination of availability requirements must be developed from the beginning giving careful consideration to overt, covert, and common mode failures. Equally important is the need to carefully select the technology appropriate for the application. If the solution uses programmable controllers, additional efforts must be given to the issues of software configuration management and reliability.

VI. ACKNOWLEDGMENTS

I wish to thank Jay Heefner and Henry Robertson at the CEBAF for their pioneering work in the use of Programmable Logic Controllers in personnel safety systems at particle accelerators.

Kudos also to Robert Landis, Joe Claborn, and Madhu Reddy of the SSCL for their great help in developing the ASST Personnel Access Safety System (PASS).

VII. REFERENCES

[1] B. Balls, P. Gruhn, "Design Considerations for High-Risk Safety Systems", *Intech*, March 1991, p 28.

[2] T. Fisher, "Control Systems Safety," *ISA Transactions*, The Quarterly Journal of the ISA, Volume 30 Number 1, 1991.

[3] A. Frederickson, "Fault Tolerant Programmable Controllers for Safety Systems", *Programmable Controls*, March 1989, p 109.

[4] P. Gruhn, "Risks With Using PLCs for Safety Protection", *C & I*, September 1990, p 53.

[5] *R. Parry,* "Personnel Access Safety Systems at the Superconducting Super Collider," *Proceedings of the Industrial Computing Conference*, Vol. 2, p 437, ISA 1992 – Paper #92-0467.

[6] PES – Programmable Electronic Systems in Safety-Related Applications, *Health and Safety Executive*, HMSO, London, UK, 1985.

[7] R. Waterbury, "Fault-Tolerant / Fail-Safe Systems are Fundamental, *Intech*, April 1991, p 35.