Survey of Electronic Safety Systems in Accelerator Applications

K. Mahoney

Thomas Jefferson National Accelerator Facility, Newport News, Virginia 23606

Abstract

This paper presents the preliminary results and analysis of a comprehensive survey of the implementation of accelerator safety interlock systems from over 30 international labs. At the present time there is not a self consistent means to evaluate both the experiences and level of protection provided by electronic safety interlock systems. This research is intended to analyze the strength and weaknesses of several different types of interlock system implementation methodologies. Research, medical, and industrial accelerators are compared. Thomas Jefferson National Accelerator Facility (TJNAF) was one of the first large particle accelerators to implement a safety interlock system using programmable logic controllers. Since that time all of the major new U.S. accelerator construction projects plan to use some form of programmable electronics as part of a safety interlock system in some capacity.

Introduction

To date, there are no basic requirements or generally accepted standards for the design of safety interlock systems in accelerators. Some specialized industries, such as medical accelerators have general guidance for interlocks for oncology machines, and more guidelines are under development (ref.1,2). Some standards which could be applied to safety interlock system design (ref.3) are under development but there are no guidelines or requirements for the application of these standards for accelerators.

The purpose behind a survey of accelerator safety system implementations was to provide some foundation for comparing "good practice" within the industry. To this end several different types of accelerators were chosen in order to have a comprehensive picture of the practices involved. Specific goals were to:

- Gather a wide variety of data on safety system applications within the accelerator community.
- Get an idea of the implementation methods used by safety system designers in diverse applications.
- Compare methods used in the design of accelerator safety interlock systems to those in other high risk industries.
- Compare attributes such as complexity, cost, reliability, and customer satisfaction between different machines.
- Form a basis of "good practice" which may then be used to develop standards and guidance applicable to accelerator safety systems.

The intended audience for the survey were the persons directly involved in the design, maintenance, and supervision of safety interlock systems. The focus of the survey was on those systems used to interlock prompt ionizing radiation hazards.

Survey Design

The survey was broken up into 100 questions divided into 4 categories.

- Background - What type of accelerator(s), energy, current, particles, … etc.
- Safety System Design Architecture - What types of design architectures are used. Redundant? Electronic? Relay based?…etc.
- Documentation - What type of documentation was used in the design, fabrication, review, testing,…etc.
- Administration - What policies are used in the administration of the system. What type of management support, funding, …etc., does the interlock system get?

Some Preliminary Results

There were over 40 respondents out of 150 surveys mailed. The respondents included a wide cross section of accelerator applications. Table 1 gives a breakdown of the type of applications.

Application	# Responding
Fundamental Research	22
Applied Research	17
Industrial Research	14
Medical Applications	12
Other Applications	1

Table 1. Applications

Table 1 includes responses from multipurpose labs which may have more than one application for the accelerator.

There are a few basic attributes which can be compared among safety interlock system implementations:

- Technology
- Redundancy
- Layering (multiplicity of devices)

- Diversity of components

Each of these attributes may or may not add to the safety or availability of a system. Some are a matter of practice. Typically, in fields which are highly competitive or under great scrutiny, the implementations are optimized for performance - both availability and safety. Examples of such applications may be the airline industry or nuclear power stations. For both to be economically viable, the safety system must be extremely reliable and also free of false trips. In applications which are less competitive, such as research physics accelerators, safety systems vary greatly in the implementation. Availability has historically not been a driving consideration in these designs.

Technology

A basic theme of one section of the survey was to determine what type of technology was used in the design of the system. Until recently, almost all safety interlock systems were designed using relay based systems. In contrast, the newer designs are using the advantages of programmable electronic based designs. In particular, programmable logic controller (PLC) based designs are becoming prevalent in the nuclear physics accelerators, while microprocessor based systems are used in industrial and medical applications. A pivot of 1990 was used to look at the breakdown of electronic vs. electro-mechanical (relay) based systems.

Implementation	Electronic/Programmable	Relay/Switch
Before 1990	13 %	18 %
After 1990	40 %	29 %

Table 2. Safety Interlock System Technologies

A majority of the electronic systems implemented after 1990 were electronic or programmable systems. Most of the relay based systems implemented after 1990 were extensions or upgrades to existing systems. The trend is to replace relay based systems with electronic systems when the cost and increased availability can be justified.

Architecture:

The most common architecture for accelerator safety interlock systems is the dual redundant arrangement. There are varying degrees of isolation between the two chains, however, there are typically two independent systems.

Architecture - Redundancy			
Single Channel	Dual Redundant	Triple Redundant	Other
32 %	62 %	3 %	3 %

Table 3. Safety System Redundancy

Most of the safety systems use layering of devices which are interfaced to, or controlled by the safety system. Layering of protection devices is used to achieve a diversity between protection devices so that the system is less susceptible to common cause failure modes. An example of layering vs. redundancy is shown in Figure 1.

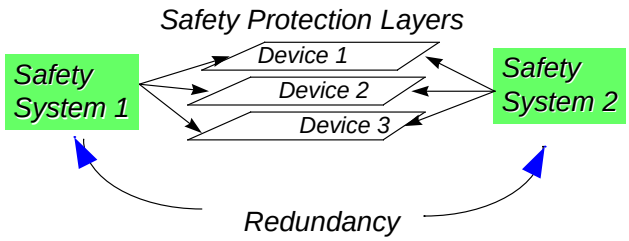

Figure 1. Redundancy vs. Layering

Architecture - Layering			
Single Layer	2 Layers	3 Layers	4 Layers
6 %	59 %	29 %	6 %

Table 4. Safety System Layering

The trend in layering is to have n+1 layers, where n is the level of redundancy. For example, a newly designed dual redundant safety system would tend to have three devices used to stop beam. Likewise, even a single channel system would use two different means to block or shut off beam.

Design Basis

The technology involved in the implementation of safety systems was relatively well understood. One of the survey questions asked "Was there a design goal for safety system reliability?" There were three basic types of responses. The most prominent were the qualitative response of "no failures," with 86% of those responding. The next two most common answers were quantitative with 14% giving a number of 10^{-6} failures per year and 4% giving a number of 0.5 - 1 failure per year. The disparity between the requirements again points to a lack of a common definition of safety reliability within the accelerator community.

Customer Satisfaction

Two of the questions had to do with the satisfaction with the safety system. One hundred percent of the respondents were satisfied with their safety system. The validity of this response comes into question when compared with some quantitative measure of satisfaction. For example, 20% of the respondents thought that their system was difficult to operate or to trouble shoot. Thirty-five percent had not done any type of reliability analysis of their system or the potential failure mechanisms. What was most surprising was that, while the majority of respondents set a criteria of "no failures"

and were "completely satisfied" with their system, 26% have actually uncovered unsafe failures in their system.

Comparing to Other Industries

Table 5 compares the approach taken by several different industries which use safety interlock systems for life safety. An important distinction between the applications is not necessarily the quantitative risk associated with the hazard, but rather the perception of the risk in the general public's eye.

Application	Particle Accelerator	Aircraft	Chemical Plant	Nuclear Power Plant
Type of Hazard	Prompt Radiation	Loss of Control/ Power	Chemical Release/ Explosion	Radioactive Release/ Exposure
Potential Consequences	Catastrophic to limited number of individuals. No long term hazard.	Extremely Catastrophic to hundreds of individuals. No long term hazard.	Extremely Catastrophic to potentially thousands of individuals. Possible long term hazard.	Very Catastrophic to potentially hundreds of individuals. Possible long term hazard.
Examples of Accident	Therac 25	Several	Bhopol	Chernobyl
Relative Importance of Reliability	Very	Extremely	Very	Extremely
Public Acceptance of Risk	Completely	Grudgingly	Grudgingly	None
Importance of Machine Availability	50 - 95%	100%	80-98%	98 - 100%
Safety System Architecture	Dual Redundant	3-4x Redundant	2-3x Redundant	2-3x Redundant
Hardware Diversity	Sometimes	Yes	Yes	Sometimes
Software Diversity	Sometimes	No	No	Yes

Table 5. Comparison of Accelerator Safety System Criteria with that of other Industries.

Note that the increased redundancy of the aircraft, nuclear power, and chemical applications is not necessarily to achieve an increase in the reliability of the safety system, but rather to achieve an increase in the availability of the system. A typical 3x redundant system would use a voting arrangement such that if one of the systems failed, the other two would still maintain the safety interlocks.

Administration

Administration of safety systems is an important factor when and if one considers incorporation of the system into a total quality management (TQM) frame work. It is a must if one considers working to the ISO 9000 series of standards. Only 6% of the respondents were ISO 9000 certified. Another 17% were either considering ISO certification or actively working toward ISO standards.

Other questions in the administrative section dealt with issues such as satisfaction with current funding (79%), and supportive management (95%).

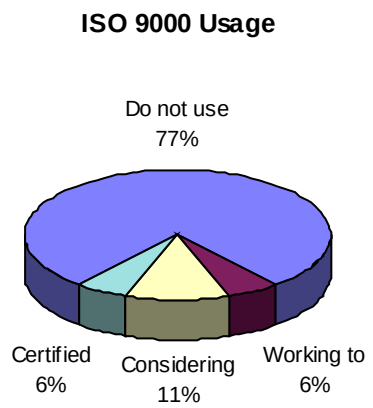

Figure 2. Usage of ISO 9000 Among Accelerators

Conclusions

The conclusions of the survey of safety interlock systems in accelerator applications are still preliminary. Much more analysis is required to come to a comprehensive understanding of the data. However, the following conclusions are evident from the data at the time of this publication:

- The trend in technology for the implementation of safety interlock systems is toward programmable electronic systems. The most predominant type of hardware is the industrial programmable logic controller (PLC).
- The architecture generally used is the dual redundant system with at least two safety layers. The trend in new designs is to use dual redundant/three layers.
- Requirements for system reliability are not well defined or understood in many cases.
- Perception of safety provided by a safety system is not always based on analysis or metrics of system performance.
- Safety System personnel are generally satisfied with management support and funding.

ACKNOWLEDGEMENTS

The author would like to thank all those individuals who took the time to complete and return the survey sheets. This work was supported by the U.S. DOE under contract number DE-AC05-84ER40150.

REFERENCES

[1] 'Design Control Guidance for Medical Device Manufacturers', March 1997, US Food and Drug Administration, Center for Devices and Radiological Health.

[2] 'ODE Guidance for the Content of Premarket Submission for Medical Devices Containing Software', US FDA Draft 1.3, August 1996.

[3] K. Mahoney, "Emerging Standards with Application to Accelerator Safety Systems," 1997 Particle Accelerator Conference, Vancouver, B.C., Canada.