Emerging Standards With Application to Accelerator Safety Systems

K.L. Mahoney, H.P. Robertson
Thomas Jefferson National Accelerator Facility
12000 Jefferson Avenue, Newport News, VA 23606

Abstract
This paper addresses international standards which can be applied to the requirements for accelerator personnel safety systems. Particular emphasis is given to standards which specify requirements for safety interlock systems which employ programmable electronic subsystems. The work draws on methodologies currently under development for the medical, process control, and nuclear industries.

Introduction

The CEBAF accelerator was one of the first large DOE labs to use programmable controllers for personnel safety applications. At the time the CEBAF Personnel Safety System (PSS) was designed, there were few documents which could be used as guidance to incorporate a PLC into the system.
Input was sought from experts at other labs in the design of accelerator radiation protection systems [1] in order to ensure that the appropriate steps were taken in evaluating the new system's reliability. A relatively new standard, developed by the U.K Health and Safety Executive [2] for the chemical process and petroleum industries, was also used as a guidance in the application of PLCs in the personnel safety system.

Over the last ten years several non-industry specific documents (consensus standards) have been developed which may be applied as guidance to the design of accelerator safety interlock systems. In addition to the general specifications there are also several industry specific documents which still provide a good measure of "best practice" applications of safety system design. Areospace, nuclear, and militarty fields are an example of industries that have had to incorporate electronic safety systems in life-safety applications. Other "low profile" industries such as train signaling systems are another source of industry specific safety system standards.

Generalized Safety System Standards

ISA-S84.01-1996 from the Instrumentaiton Society of America [3] is one of the most comprehensive general documents to be recently released. S84 covers the definition and requirements for electrical/electronic/ and programmable electronic based safety systems. Because the document is generic, it may be applied to both programmable based and conventional switch-relay based safety systems in a variety of applications.

The S84 standard defines requirements for the design, development, operation, and maintenence of a safety system which must meet a given safety integrity level (SIL). The safety integrity level is based on the probability of the safety system failing to respond to a demand (PFD)[4] to mitigate a hazard. Table 1 gives the PFD for the three safety integrity levels defined in S84.

Safety Integrity Level	1	2	3
SIS Performance requirements	Safety Availability Range		
	0.9 to 0.99	0.99 to 0.999	0.999 to 0.9999
	PFD Average Range		
	10^{-1} to 10^{-2}	10^{-2} to 10^{-3}	10^{-3} to 10^{-4}

Table 1. SIL levels defined in S84.

The safety availability (1-PFD) is related to the safety reliability of the system R_s by

$$R_s = 1 - \int_0 \text{PFD}\, dt$$

Where t is the time interval over which the reliability is being measured.
The R_s that the safety system is required to achieve over a period of time is usually defined at the beginning of the safety system design process. The combination of the PFD, the rate that the safety system may be challenged (demand), the severity of a the outcome of an accident, and the length of time the hazard persists [5] define the overall risk of the process. Usually the last three steps are minimized before the SIL of the safety system is defined. Not doing so leads to overly complex safety systems. PFD is specifically addressed by the S84 standard. Other factors that influence the overall safety of the system including design, commissioning, maintenance, and management of change, are also included in the standard.

A companion document to S84, Technical Report dTR84.0.02 is in draft from. TR84 gives examples of several methods which may be used to calculate the safety integrity level of a given safety system design.

Depending on where one is in the design process, they may need to define the SIL required, the R_s, the PFD, the mean time to failure (MTTF), or the system failure rate

(λ_s). For a constant failure rate model, these components are related by:

$$PFD = R_s\lambda_s = \lambda_s \exp(-\lambda_s t) \qquad \text{eq. 1}$$

where t is the time period over which the safety system is required to perform. This assumes any errors found during test are repaired and the "clock" is set zero. Most accelerator safety interlock systems are dual redundant systems in which both systems must fail simultaneously in order to allow a hazard to persist. The probability that both systems fail (PFD) within a given time period, t is given by the relation:

$$R_s = 2\exp(-\lambda t) - \exp(-2\lambda t) \qquad \text{eq. 2}$$

where λ is the failure rate of one of two systems.

If given the required safety reliability of the redundant system:

$$\lambda = \frac{-1}{t} \ln(1-\sqrt{1-R}) \qquad \text{eq. 3}$$

This would give the requirement for the failure rate for each of the redundant legs of the system.
Note that for a dual redundant system the MTTF is $\neq 1/\lambda$, but rather MTTF = $1.5/\lambda$.
Examples and methods for evaluating several types of safety system architectures are given in TR84. TR84 also includes more complicated reliability models which include effects like common cause failures and mean time to repair. For example, when one considers common cause factors for a dual redundant system:

$$PFD = \lambda^{DU} t \left[\lambda^{DU} t/3 + \lambda^{DD} MTTR + \beta + \frac{\lambda^{D}_{f}}{2\lambda^{DU}}\right] \qquad \text{eq. 4}$$

The superscripts DU and DD separate the failure rates into "Dangerous Undetected" and "Dangerous Detected" faults. λ^{D}_{f} is the dangerous common mode (systematic fault) failure rate.
Systematic failures are items such as specification errors, software errors, or other design errors which equally effect both channels of a redundant system.
β is a factor which represents the percentage of failures that impact more than one channel of the system. An example of a failure that may affect both channels of a redundant system are such factors as enviromental stress, lightning, or electromagnetic interference (EMI) **[6]**.

The S84 standard was designed to eventually be incorporated into a another more general standard, IEC-1508, currently under development by the european standards ageny IEC. The IEC-1508 covers all aspects of a safety system lifecycle for any safety related system. It also covers requirements for sensors and final elements used in safety system implementations. S84 does not cover sensors and final elements specifically. Chapter 12 of the S84 standard lists the current differences between S84 and IEC draft standard 1508. S84 will eventually become a process control industry specific standard, IEC-1511, which will fall under the umbrella of IEC-1508.

IEC-1508 is currently divided into seven parts.

1. General Requirements
2. Requirements for Elec./Electr./Programmable Electronic Safety Systems
3. Software Requirements
4. Definitions and abbreviations of terms
5. Guidelines for applicaiotn of part 1
6. Guidelines for applicaiton of parts 2 and 3
7. Bibliography of techniques

IEC-1508 also defines a SIL 4, probability of fail on demand of 10^{-3} to 10^{-4}.

One U.S. military standard, MIL-STD-883C **[7]**, published in 1993 may be genericly applied to the management of the safety system process and the management of safety systems in general. MIL-STD-883 defines the requirements fo evaluating hazards and steps that should be taken to make sure the hazards are properly tracked and addressed.

Industry Specific Standards

Until the advent of S84 and IEC1508, almost all standards up to this time have targeted a specific industry or application. To date, these standards have been applied mostly to the obvious "high risk" industries such as the nuclear and aerospace industries. Over the last 10-15 years more emphais has been placed on other areas with less obvious, but potentially just as high risk. Industries such as medical instrumentation, mining equipment and chemical processing all have specific standards for the use of programmable safety systems.

Nuclear Industry

Standards which describe the requirements for safety systems in the nuclear industries have been in circulation for several years. In an attempt to keep up with the rapid advance in programmable logic controllers and microprocessors, these standards are undergoing constant change. IEC880 **(8)**, is an especially good example of a safety related software standard.
The US Nuclear Regulatory Commission is currently taking comments on a draft of NUREG-0800 section 7, **[9]** which deals specifically with the use of programmable controllers in nuclear safety applications.

Medical Industry

The U.S. Food and Drug Administaration (FDA) has prepared new documents which provide guidance to the design and manufacture of medical instruments.
"Design Control Guidance for Medical Device manufacturers" **[10]** provides guidance for the manufacture of medical electronic devices. Other FDA draft documents **[11]** address the use of software in medical devices specifically.

Safety Lifecycle Model

A common factor found in many of the new standards is the concept of the safety lifecycle model. The safety lifecycle model describes a process by which the a safety system is defined, designed, and maintained through out the lifetime of the applicaiton. Feedback from the major steps are defined for all models.

Figure 1 shows a safety lifecycle model appropriate for application to an accelerator programmable electronic safety system. Note that the model applies specifically to the safety system and not other ancilliary or non-safety systems.

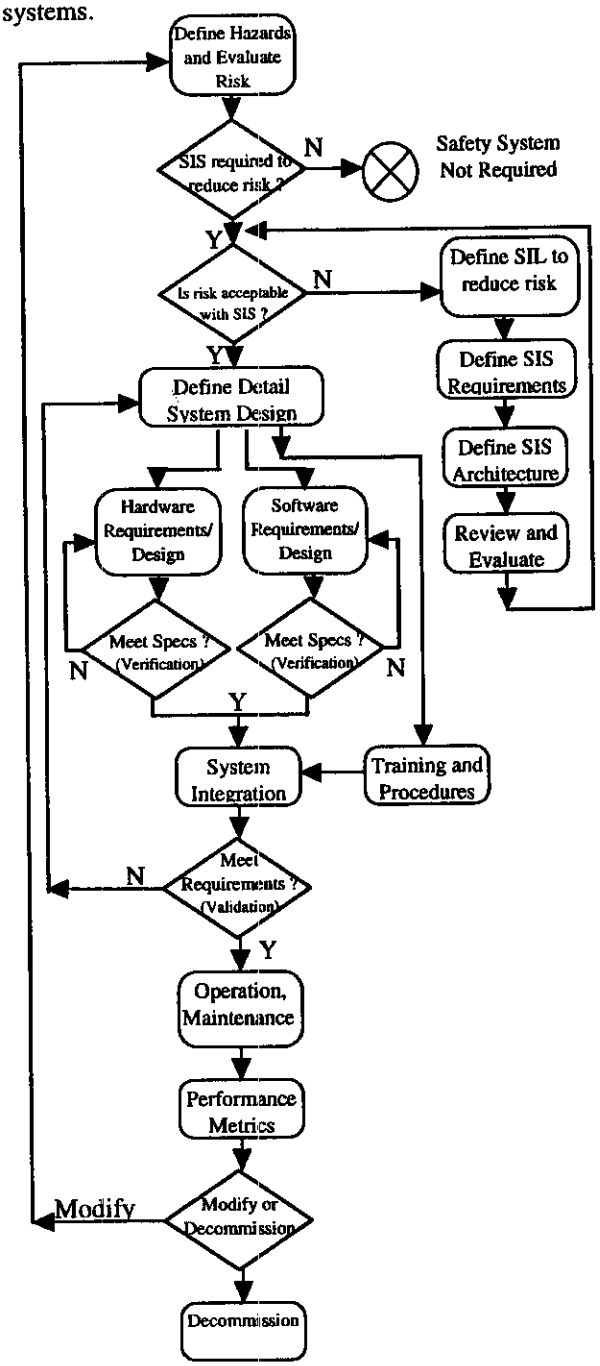

Figure 1. Safety Lifecycle Model Applicable to Accelerator Safety Systems

The safety lifecycle model is used as a framework to identify each step in the evolution of the safety instrumented system. In practice, each of the steps would have a detailed process associated with it. For example, the box titled "Define SIS Architecture" would involve the design tradeoffs of redundancy, diversity, and technology.

Summary

There are currently several international standards which may be adapted to accelerator safety systems. While several of the standards are intended for a specific industry, the approach taken to the safety system design is very similar in each case. The different approaches may be condensed into a safety system life cycle model appropriate for accelerators.

ACKNOWLEDGEMENTS

This work was supported by the U.S. DOE under contract number DE-AC05-84ER40150.

REFERENCES

[1] 'Workshop on Personnel Safety Interlocks' CEBAF TN-90-233

[2] 'Programmable Electronic Systems in Safety Applications', 1987, U.K. Health and Safety Executive, Library and Information Services, Broad Lane, Sheffield S3 7Hq, U.K.

[3] ANSI/ISA-S84.01-1996, 'Application of Safety Instrumented Systems for the Process Control Industry', February 1996, Instrumentation Society of America, 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, North Carolina, 27709

[4] ANSI/ISA-S84.01-1996, pp21.

[5] N.G. Leveson, 'Safeware: System Safety and Computers', Addison-Wesley, 1995, pp179.

[6] ISA-dTR84.02 'Electrical/Electronic/Programmable Electronic Systems - Safety Integrity Level (SIL) Evaluation Techniques', March 1997, Instrumentation Society of America, 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, North Carolina, 27709

[7] MIL-STD-883C, "System Safety Program Requirements", January, 1993.

[8] IEC-880 'Software for Computers in the Safety Systems of Nuclear Power Plants' 1986, IEC, Geneva, Switzerland.

[9] NUREG-0800 Section 7, Draft

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

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