P.15 Jefferson Lab Reliability Based Design Methods for Accelerator Safety Systems

Kelly Mahoney mahoney@jlab.org

What is a reliability based design method?

Reliability Based Design methods start off with a definition of risk and risk reduction factors to achieve target safety integrity level for a given safety function.
By minimizing the use of prescriptive requirements, the safety system designer has the latitude to design a protection system which meets the confluence of safety, reliability, and operability required of the system.

There exists a regulatory environment for several accelerator based prompt ionizing radiation sources that suggests or even mandates the use of safety interlock systems. However, little guidance is given for the design, evaluation, or even expected reliability of these systems.
The desire is to be able to design and evaluate these systems using methods generally accepted by the safety systems community.

The Jefferson Lab Safety Systems Group has been applying the reliability based design methods used in high risk industries such as petrochemical, chemical, semiconductor processing industries to name a few.

Performance Based Standards
A group industry experts, through the Instrumentation Society of America, has published performance based standard ANSI/ISA S84 which is generally applicable to safety interlock functions.

In this document the concept of a Safety Integrity Level (SIL) is introduced. An SIL is related to the probability of failure on demand of a given safety function.

Safety Integrity Level	1	2	3	4*
	Safety Availability Range			
SIS Performance requirements	0.9 to 0.99	0.99 to 0.999	0.999 to 0.9999	0.9999 to 0.99999
	PFD Average Range			
	10^{-1} to 10^{-2}	10^{-2} to 10^{-3}	10^{-3} to 10^{-4}	10^{-4} to 10^{-5}

*SIL 4 is included in the IEC 61508 definition only. It is not part of the ANSI/ISA S84.01

Jefferson Lab safety system designs adhere to 3 basic tenets:

Redundancy is the replication of interlock chains, ideally from the sensor through to the device that shuts off the hazard.

Multiplicity is the use of two or more methods to control the hazard.

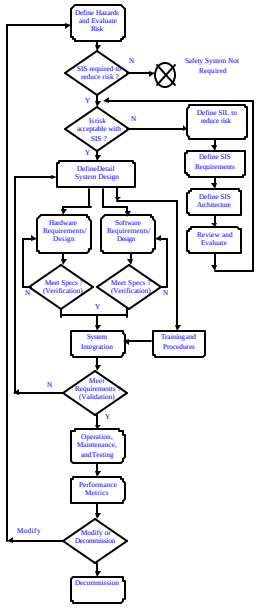
Diversity is the use of dissimilar technologies to accomplish a given task, for example beam shut down.

A safety interlock system may employ part or all of these methods to achieve a given safety integrity level for a safety function.

Table 3 Risk Code Assignment

		Personnel injury	Property loss or environmental impact				
Severity of outcome	IV	Death or permanent disability	> $100,000	1	3	4	4
	III	Hospitalization or absence > 5 lost workdays	> $10,000	1	2	3	4
	II	First aid or medical treatment required, but < 5 lost workdays	> $500	0	1	2	3
	I	First aid not required	> $500	0	0	1	1
			> 500 per	> 500 per > 10 per	> 10 per > 10 days	< 10 days	
				A	B	C	D
				Likelihood of accident (Estimated likelihood per full time active person)			

Example Risk Matrix



Lifecycle Model

Design and Evaluation of Software

The JLab Safety Systems Group applies the principles of Redundancy, diversity and multiplicity to the safety interlock software.

Critical safety functions follow diverse, redundant paths from the logic input to the logic output. These paths are evaluated usin g proven techniques such as fault tree analysis to verify proper coverage of critical functions.

Safety System Design Lifecycle Model

A model for the implementation of safety interlocks based in the ANSI/ISAS84 standard has been developed at Jefferson Lab. The figure to the left shows an outline of this model.

Note that management of change is an integral part of the design lifecycle. Experience has shown that improperly implemented change is responsible for numerous safety system failures in industry.

Jefferson Lab Safety System Design
Safety Systems are designed to meet all applicable statutory, regulatory, and best practice guidelines. However, latitude in the implementation is allowed as long as the system meets the defined safety integrity level for a given safety function.

For example, Jefferson Lab personnel safety interlock systems are designed to meet or exceed SIL 2 performance, PFD < $1x10^{-3}$. Note that this is the demand failure rate. If a continuous demand failure rate were used the criteria would be on the order of MTBFdangerous of < $1x10^{-7}$ per hour.

Example Risk Reduction Factor (SIL)

Risk without mitigation (Probability of failure)	$1x10^{-1}$
Minimum Tolerable Risk	$1x10^{-3}$

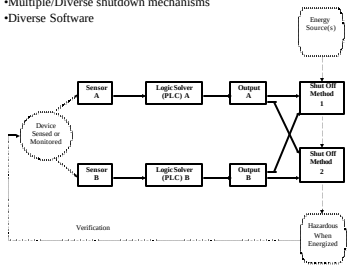
Risk Reduction Factor Required of the safety system = $1x10^{-2}$
i.e. the safety interlock system is designed to meet or exceed 10^{-2}
PFD = SIL2

During the life cycle the safety system design is evaluated to ensure that it maintains an SIL 2 performance or better.

Example 1:
Programmable Logic Controller Based Personnel Safety System- RF System Interlock

Hazard: Prompt Ionizing Radiation due to field emission.
Safety Integrity Level 2

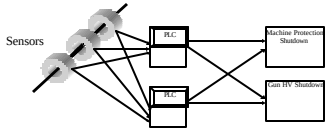
Implementation
- Full independent redundant interlock chains
- Multiple/Diverse shutdown mechanisms
- Diverse Software

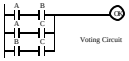


Example 2:
Programmable Logic Controller Beam Power Limit System

Hazard: Exceeding Safe Operating Envelope of Accelerator
Safety Integrity Level 1

Implementation
- Non-independent redundant interlock chains
- Single shutdown mechanisms
- Duplicate Software
- Voting inputs for increased up time





The reduced risk level defined for the safety function in example 2 allowed the system to be developed under much less prescriptive requirements than the critical system in example 1. This in turn allowed latitude in the selection of technology and implementation. The end result is a system with the desired performance without over design.

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