JEFFERSON LAB IEC 61508/61511 SAFETY PLC BASED SAFETY SYSTEM*

K. Mahoney, H. Robertson, JLAB, Newport News, VA 23606, U.S.A.

Abstract

This paper describes the design of the new 12 GeV Upgrade Personnel Safety System (PSS) at the Thomas Jefferson National Accelerator Facility (TJNAF). The new PSS design is based on the implementation of systems designed to meet international standards IEC61508 and IEC 61511 for programmable safety systems. In order to meet the IEC standards, TJNAF engineers evaluated several SIL 3 Safety PLCs before deciding on an optimal architecture. In addition to hardware considerations, software quality standards and practices must also be considered. Finally, we will discuss R&D that may lead to both high safety reliability and high machine availability that may be applicable to future accelerators such as the ILC.

INTRODUCTION AND BACKGROUND

The Jefferson Lab CEBAF Accelerator 12GeV upgrade will double the energy of the present accelerator. The project will also add a fourth experimental Hall D (See Fig. 1). The new safety systems for the Tagger and Hall D facilities will be based on IEC standard safety system implementation using certified safety PLCs.

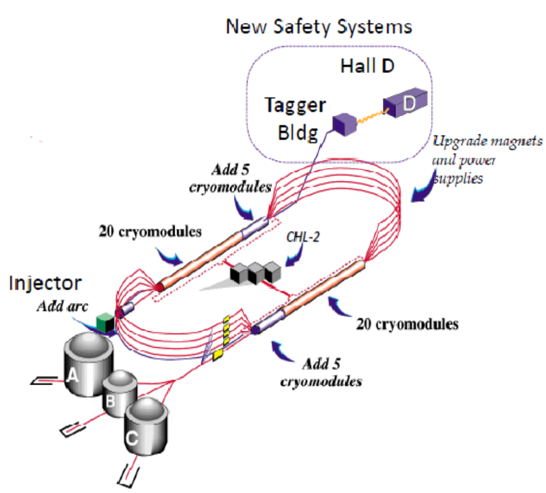

Figure 1: Jefferson Lab 12 GeV Upgrade.

The two primary standards in use today are the IEC61508 series "Functional safety of electrical/electronic/programmable electronic safety-related systems" and the ANSI/ISA S84.00.01/IEC61511 series "Safety instrumented systems for the process industry sector". Figure 2 shows the relationship between the standards.

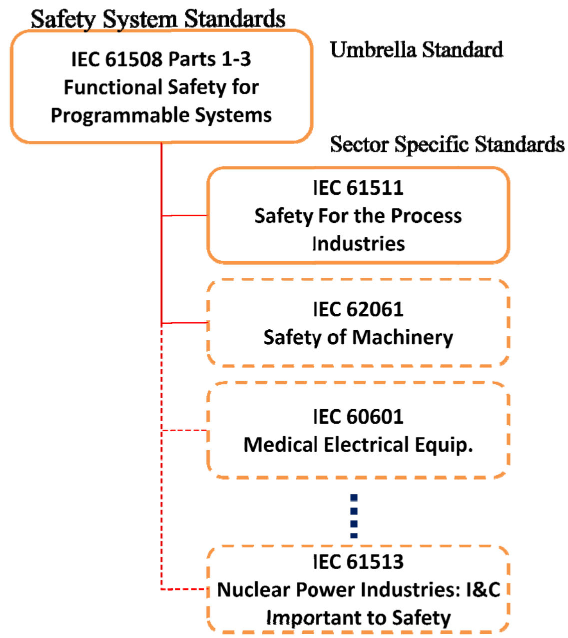

Figure 2: Relationship between IEC61508 and sector specific standards.

Safety Integrity Levels (SILs)

The IEC standards give requirements for managing a safety system over its entire lifecycle. A major theme introduced in the IEC 61508 standard is the concept of Safety Integrity Levels (SILs). Safety integrity is the probability that a safety system will perform an intended safety function over a given period of time [2]. A SIL is a performance requirement for a given safety function performed by a safety system. It is specified in terms of a number from one to four based on either the required average probability of unsafe failures on demand PFD_{avg} or an unsafe failure rate $\lambda_D(t)$. SIL 1 is the lowest safety integrity level with a target PFD_{avg} between 10^{-1} and 10^{-2}; SIL 4 is the highest with a PFD_{avg} between 10^{-4} and 10^{-5}. The requirements for SIL in terms of failure per hour, $\lambda_D(t)$, may be obtained by multiplying PFD_{avg} by 10^{-4}; e.g. the lower limit of SIL 1 expressed in failures per hour is $1x10^{-5}$ hr^{-1}. The standards use the concept of SILs to establish a graded approach to the requirements for safety system design, implementation, and management; the higher the SIL, the more rigorous the requirements.

Systems Engineering Approach

The IEC 16508/16511 standards in and of themselves do not provide a sufficiently rigorous process for managing the development project for an accelerator safety system. The safety standards are designed to provide requirements specifically for a safety system with

* Notice: Authored by Jefferson Science Associates, LLC under U.S. DOE Contract No. DE-AC05-06OR23177. The U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce this manuscript for U.S. Government purposes.

the presumption that other processes and mitigations are in place. In order to establish context for the 12GeV safety systems, the SSG is adopting ISO/IEC15288 systems engineering and ISO/IEC12207 software systems lifecycle standards. Key processes discussed in IEC15288 are [3]:

- Agreement Process
- Organization/Enabling Process
- Project Process
- Technical Process

In order to integrate the IEC 61511 standards compliance in to the 12 GeV PSS upgrade project, specific safety lifecycle steps were incorporated in to the project management plan as deliverables. This approach also ensured resources were identified and funded for the process.

COMPLIANCE WITH IEC61511

In order to comply with IEC61511, one must show compliance with the requirements of clause 5 through 19 [4]. The subject of each clause is given below:

IEC 61511 Clause # - Subject

5 – Management of Functional Safety
6 – Safety Lifecycle
7 – Verification
8 – Hazard and Risk Assessment
9 – Allocation of Safety Functions
10 – SIS Requirements Specification
11 – SIS Design and Engineering
12 – Application Software
13 – Acceptance Testing
14 – SIS Installation and Commissioning
15 – SIS Validation
16 – SIS Operation and Maintenance
17 – Modification
18 – Decommissioning
19 – Information and Documentation Technical Design

Each step of the systems design was benchmarked against the applicable requirements. The requirements for each phase were captured in the safety requirements specification.

In addition to the requirements given in the standards, the design had to consider safety functions not normally within the context of IEC61511. For example, actions that require human intervention such as ESTOP, are not addressed in the standard. These functions were incorporated as both part of the Layer of Protection analysis and assigned SILs.

The hazard analysis used FMEA methods to identify credible accident events and classify them using a risk matrix approach. The analysis captured pre mitigated risk, safety layers, and post mitigation risk. The requirements for safety layers were then translated in to safety functions in the PSS systems requirements specification. Each safety function was analyzed for the appropriate SIL level using several methods to benchmark the agreement among them. Ten safety functions were identified with the following SIL distribution:

1 SIL 3 Functions
4 SIL 2 Functions
5 SIL 1 Functions.

The single SIL 3 function is beam transport from a beam operations area to an access area. In this case, there is no opportunity for avoidance or credit for alarm and warning devices. The Risk Graph [5] approach was found to be the best overall method for the JLab applications. A risk graph spreadsheet function developed at JLab was used for this purpose

SYSTEM DESIGN

An early architecture decision in the 12 GeV PSS project was to use safety PLCs as the processing element. Safety PLCs are designed and certified for use as part of a given SIL safety function. They have specific design features intended to meet the failure rate, redundancy, and diagnostic test coverage requirements of an IEC61508 compliant system. . Although theoretically one SIL 3 safety PLC CPU is required, the Jefferson Lab design retains a fully redundant system architecture. This was done as a conservative measure until there is more Jefferson Lab experience with the new technology.

The manufacturer of the PLCS for the installed CEBAF safety system did not offer a safety PLC model. The SSG therefore explored the options available from several manufacturers. Models from two manufacturers were selected for evaluation. Both models were tested for failure modes and with JLab field hardware. Additional criteria in the evaluation included support, programming tools, available I/O and system performance.

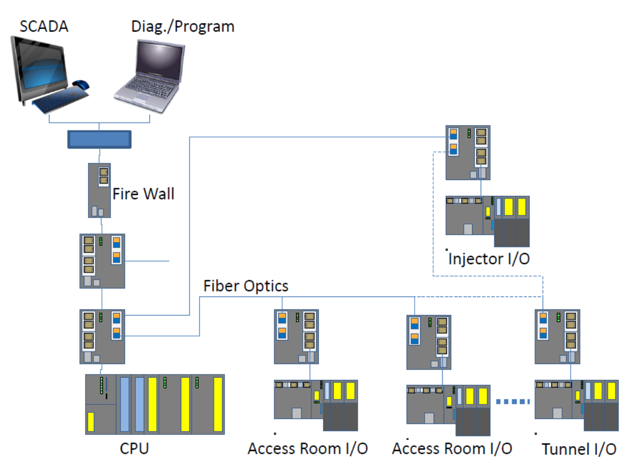

Figure 3: Safety PLC Remote I/O Topology. Note: Only one of two divisions shown.

Another basic design decision was to use a highly distributed remote I/O architecture (see Fig. 3). In this architecture, I/O to any field devices outside the beam enclosure is implemented in small, low I/O count safety modules. For example, each access room for the Tagger and Hall D areas has a dedicated safety I/O drop.

Likewise, there are remote safety I/O drops co-located with other PSS segment equipment where the Hall D exchanges hardwired signals regarding status operational modes. This architecture avoids sending status signals thousands of meters over copper wire.

Non-certified Equipment

The Jefferson Lab Safety Systems Group has had the opportunity to document failure data on hundreds of commercial and in-house components over hundreds of thousands of hours. This information is vital in order to qualify uncertified equipment as "proven in use" in order to meet the IEC 61508 standard requirements. An important factor is that the upgrade components will be used in the same way and in the same environment as the existing ones. In addition, all of the components were tested with the new PLC hardware over several months using a test stand built for this purpose.

Another consideration is the level of redundancy required for the field devices. IEC 61511-1 clause 11.4 specifics redundancy as hardware fault tolerance – the number of devices that may fail unsafe with the safety function still intact. For the JLab design, the following fault tolerance is required:

- SIL 3: FT of 2 (1oo3)
- SIL 2: FT of 1 (1oo2)

This is consistent with the number and types of devices used in the existing system; therefore there is no major change in the system architecture required for field devices.

STANDARDS BASED DESIGN TO BENCHMARK ALTERNATE ARCHITECTURES.

Given a risk performance specification in the form of SILs, one may investigate alternate configurations that provide better safety and machine availability. This is presently done at Jefferson Lab on a limited basis. The 12 GeV PSS design will incorporate some of this experience in to a function to measure and compare the energy settings of vertical and horizontal bend magnets in the Tagger building. For this function, the standard requires a 1oo2 sensor arrangement. However, by adding one additional sensor to move to a 2oo3 voting scheme, machine availability is increased without compromising safety availability. The arc current and the Tagger magnet current will be monitored with three current sensors each. Beam energy is calculated using a 2oo3 voting algorithm for each set of sensors. The resultant calculations are compared in the PLC logic and must agree within better than one percent. By using a 2oo3 voting arrangement, sensors can be tested and even replaced without shutting down the accelerator. This arrangement is presently used in the JLab Beam Envelope Limit System (BELS).

Conceptually, this concept can be extended to all types of sensors such as door interlocks. This type of arrangement, coupled with the highly distributed remote I/O, may be beneficial to facilities requiring high availability and/or large distances separate the access points. The architecture could also lend itself to automated self test; however, even with periodic self test, periodic proof testing (certification) is still required per the IEC standards and accepted good practice.

CONCLUSIONS

The Jefferson Lab Safety Systems Group has completed the design of a safety PLC based system designed to meet the requirements of IEC standards 61508 and 61511. In addition to the safety standards, systems engineering standards and practices were used to establish a long term framework for both the project and the overall system management. The design uses a highly distributed safety architecture replace long copper cable runs. This architecture increases reliability while lowering costs. The use of performance standards enables the designer to explore alternate architectures while maintaining or even enhancing both safety and machine availability.

REFERENCES

[1] "The programmable controller-based CEBAF personnel safety system." R. Bork, J. Heefner, H. Robertson, R. Rossmanith, (Jefferson Lab) . Oct 1991.Prepared for 1991 Accelerator Instrumentation Workshop, Newport News, Virginia, 28-31 Oct 1991. Published in *Newport News 1991, Accelerator instrumentation* 151-159.

[2] IEC61508-4. "Functional safety of electrical/electronic/ programmable electronic safety-related systems. Part 4: Definitions and abbreviations." Geneva, Ch : International Electrotechnical Commission, 1998.

[3] ISO/IEC15288 "Systems and software engineering — System life cycle processes", Geneva, Ch: International Electrotechnical Commission, 2008.

[4] IEC61511-1. "Functional safety - Safety Instrumented Systems for the process industry sector.. Part 1: Framework, definitions, system hardware and software requirements" Geneva, Ch : International Electrotechnical Commission, 2003.

[5] IEC61508-5. "Functional safety of electrical/electronic/ programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels." Geneva, Ch : International Electrotechnical Commission, 1998.