A STREAMLINED ARCHITECTURE OF LCLS-II BEAM CONTAINMENT SYSTEM

E. Carrone, M. Cyterski, J. Murphy, F. Tao
SLAC National Accelerator Laboratory, Menlo Park, CA 94025, USA

Abstract

With the construction of LCLS-II, SLAC is developing a new Beam Containment System (BCS) to replace the aging hardwired system. This system will ensure that the beam is confined to the design channel at an approved beam power to prevent unacceptable radiation levels in occupiable areas. Unlike other safety systems deployed at SLAC, the new BCS is distributed and has explicit response time requirements, which impose design constraints on system architecture. The design process complies with IEC 61508 functional safety standard. This paper discusses the BCS built on Siemens S7-300F PLC. For those events requiring faster action, a hardwired shutoff path is provided in addition to identical but slower safety functions within PLC; safety performance is enhanced, and the additional diagnostic capabilities significantly relieve operational cost and burden. The new system is also more scalable and flexible, featuring improved configuration control, simplified EPICS interface and reduced safety assurance testing efforts. The new architecture fully leverages the safety PLC capabilities and streamlines design and commissioning through a single-processor single-programmer approach.

INTRODUCTION

Beam Containment System (BCS) is employed at SLAC as a part of radiation safety systems. The objective of BCS is to ensure that the beam is confined to the designed channel at an approved beam power to prevent unacceptable radiation levels in occupiable areas. Major functions of BCS include limiting the beam power, detecting beam loss and preventing damage of beam line devices with personnel safety implications [1]. Taken these factors into consideration, BCS is undoubtedly a safety-critical system.

The existing aged BCS was developed with customized electronics, with its devices scattered around SLAC. Built with vintage parts that are obsolete and past their service lives, the system has limited diagnostics and lower reliability. As a result, the system needs lots of efforts on testing and maintenance. For example, potentiometers are used in BCS for trip threshold setup. Since potentiometers drift over time, they should be tested frequently to make sure the system function as desired. Similar situations exist within BCS, the old customized electronics do not provide the comparable diagnostics capabilities that typically provided by those commercial off the shelf products available nowadays. It results in lower confidence in system reliability. As the consequence, BCS has to be tested frequently to demonstrate its health and readiness. In addition to the annual testing by BCS engineers, operators have developed daily, weekly checklist for testing BCS components and it has become an operational burden.

Another drawback of the current BCS is configuration control. With the construction of the original LCLS (Linac Coherent Light Source), the re-commissioning of the FACET (Facility for Advanced Accelerator Experimental Tests) and the revival of End Station A, the operational requirements for BCS interlock and bypass logic have grown in complexity. This has pushed the limits of what can be implemented and maintained in a hard-wired system. This trend will continue through the construction and commissioning of LCLS-II.

A solution to address issues mentioned above would be a new fail-safe PLC based BCS. With the improved diagnostics capabilities provided by modern fail-safe PLC systems, common failures for discrete inputs and outputs such as broken, shorted or cross-wired conductors can be easily detected. In addition, SIL-rated analog modules can be used to read in trip setpoint for detection of electronics drift.

SLAC has adopted safety PLC as the technology to replace the old relay based safety system. After several years of operation, the safety PLC has proven its value in its fail-safe, enhanced diagnosis, simplifying the implementation, ease of installation, debug and logic modification. Especially the Siemens S7 safety PLC has been stably running for a couple years. With the confidence for this hardware platform, it has been decided to use the same Siemens S7 safety PLC to be the platform for BCS.

However, there are some unique requirements for BCS that will differentiate this system with other PLC based safety systems deployed at SLAC:

- Explicit response time requirement
- Distributed nature of BCS

For some inputs (e.g. PIC and LION), BCS is required to react to a beam containment fault in less than 300ms to prevent damage to passive beam containment devices including collimators. This response time requirement would be very difficult to satisfy if following the existing safety system architecture. In addition, the existing 3 PLC architecture is still based on the structure rather than the result of risk assessment. We believe if using the risk based approach to design the system, the new BCS can still be a safe one but may be less conservative.

A NEW DISTRIBUED ARCHITECTURE

Since the introduction of safety PLC in safety systems, some safety system engineering practice has been established in SLAC to ensure system safety and security. A typical architecture of Personnel Safety Systems

ISBN 978-3-95450-139-7

employed at SLAC is shown in Figure 1 with following features:

- Separation of safety critical functions and non-safety critical functions
- Air gap for safety systems networking
- Dual redundancy for safety critical systems
- Different programmers for redundant safety PLC to prevent common coding error

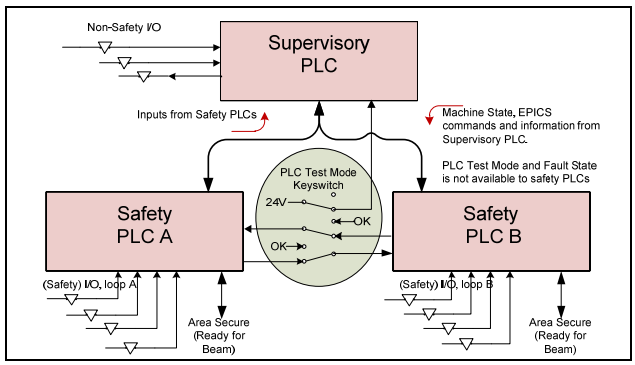

Figure 1: The typical architecture of SLAC safety systems.

Considering the distributed nature of BCS and the response time requirement, if to follow the same engineering practice, the new BCS would be very costly to build and maintain. Since at every location where exist BCS inputs or outputs, there will be a separate redundant safety PLCs and a non-safety. Especially when taking the asynchronized communication between multiple CPUs into consideration, satisfying the response time requirement would be more difficulty.

Therefore, a streamlined architecture of BCS is adopted, which not only satisfy those design constraints, but also without sacrifice of safety. The system diagram is shown in Figure 2. The rationales that justify the new architecture are explained below.

Architectural Constraints

Dual redundant architecture is very common for safety related control systems, regardless of the technology to be relay or PLC.

With the gradual adoption of functional safety along with the IEC 61508 standard family. The performance based functional safety standard take the place of those rigid architectural based standards. The transition began with the replacement of EN954 with ISO 13849. Now with the new ISO 17305 on the horizon, which will take effect in 2017, the SIL based performance based design criteria will be the only design criteria, which justify relax of dual redundancy requirements.

Using the SIL as the design criteria, adopting a non-redundant fail-safe PLC architecture is feasible. The S7-300 distributed safety platform has been certified to have a safety capability SIL3, and it has built-in redundant in coding execution, which is shown in Figure 3 [2].

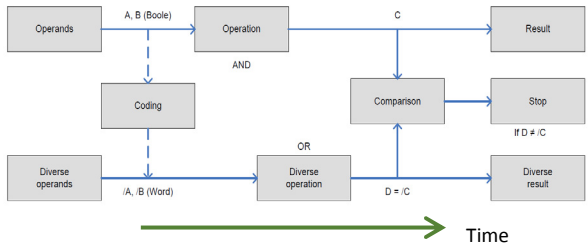

Figure 3: Time redundancy and diversity achieved in a single failsafe CPU.

Two Programmers

To eliminate the potential programming error, two PLC programmers are required to develop PLC for safety PLC of each chain. When configuring hardware diagnostics capability, such as test pulse, two PLCs are configured differently on purpose, such that two versions of program are not exchangeable. This practice would prevent that one version of program is mistakenly downloaded to both safety PLCs and become a potential source of common cause error.

Using two independent programmers for two different brands of standard PLCs was a typical practice for implementing safety functions in the 1980s. The rationale for this approach was that two completely unique PLC firmware and application versions should produce two "chains" with a minimal likelihood of common-mode failures. However, according to the newer version of IEC 61511 standard, program diversity has limited, if any, value in modern, real-world safety instrumented system implementation scenarios. It is said that where programming diversity is used, a great deal of overhead work is required for such diversity to actually enhance safety. Conversely, where resources are too constrained for the necessary controls to work effectively, programming diversity can create more problems than it solves [3].

It is also important to consider the constraints imposed by safety PLC manufacturers on the tools used to program them: safety PLC programming languages are limited to ladder logic and functional block diagrams. Both are classified by IEC 61508 as "limited variability programming" languages for systems with "limited application configurability" [4]. They are designed to minimize complexity, and to be easily read and reviewed. When combined with the well-established software quality assurance program that SLAC already follows, the likelihood of a programming error is significantly decreased [5].

Coexisting of Safety and Non-Safety Tasks

The constraints placed on safety programming by limited variability languages prevent non-safety functions such as status communication and reset signal distribution from being compiled into safety code. The Siemens S7 safety PLC supports concurrent processing of safety and non-safety tasks within the same system while providing

ISBN 978-3-95450-139-7

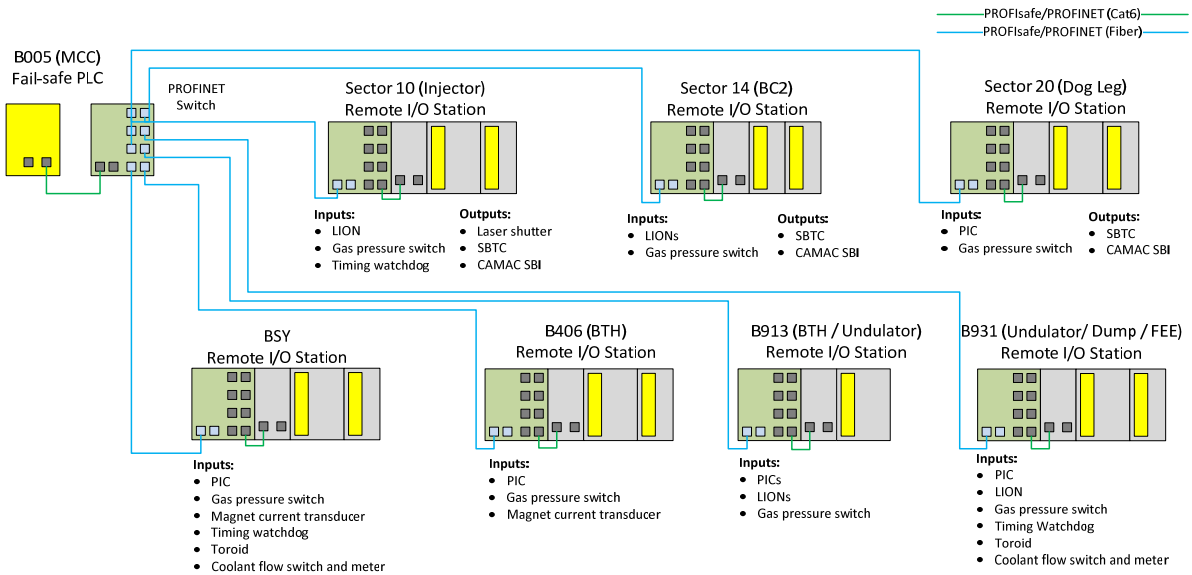

Figure 2: LCLS-II BCS distributed PLC architecture.

protected memory and processing time for the safety tasks [2].

This arrangement will significantly save the hardware implementation cost and the complexity of communication.

Siemens PLC will generate a unique signature for each functional block. The signature changes only if underlying code changes, enabling configuration control and prevent unintentional change of safety logic.

To sum up, with the new architecture of BCS, the system is scalable and has a much lower cost of ownership. If the system performance and the desired design features have been successfully demonstrated and proved in the field, the functional safety standard will undoubtedly become part of the foundation for design basis document for safety systems in SLAC.

ACKNOWLEDGMENT

The authors would like to thank Brian Bennett and Robert Ragle for their efforts in the radiation safety systems working group on BCS.

REFERENCES

[1] Radiation Safety Systems- Technical Basis Document, SLAC-I-720-0A05Z-002-R004, Dec. 2010.

[2] TÜV SÜD. "Report SN73331C: Report to the Certificate Z10 09 07 67803 003 'Safety-Related Programmable System SIMATIC S7 Distributed Safety', Rev 2.1." December 17, 2010.

[3] IEC 61511, Committee Draft of Ed. 2, “Functional Safety – Safety Instrumented Systems for the process industry sector”, International Electrotechnical Commission, 2012.

[4] IEC 61508, Ed. 2, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”, International Electro-technical Commission, 2010.

[5] Radiation Safety Systems Working Group Report, “BCS Upgrade: Hybrid Hardwired/PLC-Based Architecture”, SLAC, Dec. 2012.

ISBN 978-3-95450-139-7