ELECTRONICS FOR LCLS-II BEAM CONTAINMENT SYSTEM SHUT-OFF*

R. Kadyrov[†], E. Chin, C. Clarke, E. Rodriguez, F. Tao, D. Brown, M. Petree
SLAC National Accelerator Laboratory, Menlo Park, California, USA

Abstract

LCLS-II is a new xFEL facility under construction at SLAC National Accelerator Laboratory. Its superconducting electron linac is able to produce up to 1.2 MW of beam power. The existing normal conducting LCLS linac can operate concurrently in shared accelerator housing. A Beam Containment System (BCS) is employed to limit the beam power and prevent excessive radiation in case of electron beam loss or FEL breach. Fast and slow shut-off paths are designed for devices with different response requirements. The system is required to shut-off the beam within 200 µs for some of the fast sensors. The fast path is based on custom electronic designs, and the slow path leverages industrial safety-rated PLC hardware. The system spans 4 km of LCLS-II and combines inputs from about 150 sensors of different complexity. The architecture is based on multiple levels starting with summing sensor inputs locally and to converting them into permits for the shut-off devices. Each level is implemented redundantly. Automated and manual tests at all levels are implemented in the system. System architecture, electronics design and cable plant challenges are presented below.

INTRODUCTION

There have been multiple changes to the BCS architecture since it was presented to the community last time [1]. The hardwired shut-off for devices with fast response requirements has grown into the "fast shutoff path" subsystem comprised of custom electronic units with copper and fiber interconnections. The role of the PLC has been expanded to supervising, testing the fast path electronics and shut-off devices, and centralized bypass handling. Not all initiatives for the PLC implementation presented previously in [1] have been implemented, and the final design closely follows de-facto standards of safety systems implementation at SLAC with redundant implementation and diversity in programming.

SYSTEM ARCHITECTURE

The BCS sensors are divided into two categories by the shut-off time required. The first category includes sensors with response requirements of 500 ms or more that are connected to the "slow path" which is based on distributed Siemens failsafe PLC I/O and safety PLC CPUs. Magnet Current Monitors (MCMs), vacuum breach interlock system, cooling water differential pressure switches, bremsstrahlung radiation monitors and position indicators from beam stoppers provide inputs to I/O in the field, PLC CPU processes readings from the field I/O, evaluates interlock conditions, and issues slow path permits for the Shut-off chassis (SOC).

All sensors with shut-off time requirements below 500 ms are connected to the "fast path". The following sensors use the fast shut-off path: Average Current Monitor (ACM), Beam Loss Monitors (BLMs), and the Photon Absorber Burn Through Monitor (BTM). Faults from sensor electronics are summed in digital summary chassis (DSC) and passed to the SOC for permit generation. The subsystem with the fastest response required is the BLM. If beam is not mitigated in 200 µs after the beam loss, thermal damage to personnel protection equipment can occur at beam power above 250 kW.

Both paths are shown in Figure 1. Permits from the shut-off chassis are passed to the interface chassis that translates the signal levels and logic to be compatible with the shut-off devices.

A typical BCS installation combines sensors within reach of PLC I/O and DSC which corresponds to three to five 100-m sectors of the accelerator structure. Installation boundaries are defined based on signal density in each area and optimal cable lengths. Installation locations are selected such that the permitting signals are passed in the upstream direction towards primary shut-off devices to reduce the response time.

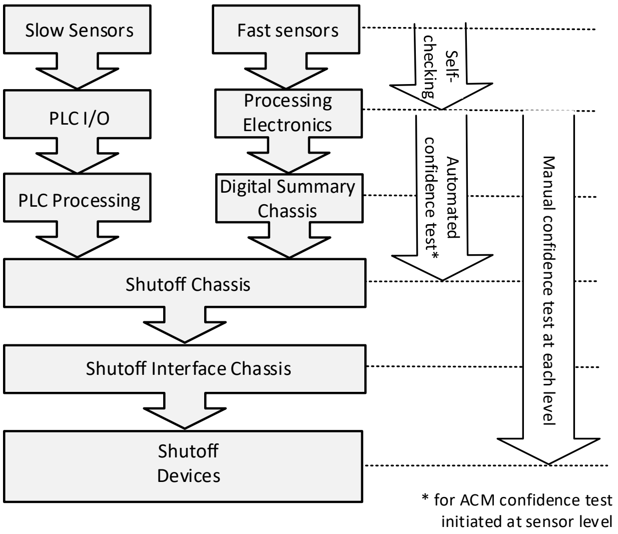
Slow Sensors
PLC I/O
PLC Processing
Fast sensors
Processing Electronics
Digital Summary Chassis
Shutoff Chassis
Shutoff Interface Chassis
Shutoff Devices
Self-checking
Automated confidence test*
Manual confidence test at each level
* for ACM confidence test initiated at sensor level

Figure 1: System fast and slow shut-off paths. Fast path diagnostics coverage.

* SLAC is supported by the U.S. Department of Energy under contract DE-AC02-76SF00515

[†] rkadyrov@slac.stanford.edu

Most installations have one or more DSC and PLC I/O heads installed in one or adjacent racks. Electronics for the sensors can be one or more 100-m sectors away. There are 11 installations planned in the system, they are shown in Figure 2.

SLOW PATH IMPLEMENTATION

The slow path is based on redundant PLC systems with two processors and two separate sets of distributed I/O systems. The PLC logic will be implemented by two developers independently following one programming specification document. The expected response time of safety runtime to a slow fault is below 200 ms. Regular runtime is used for fast path supervision, configuration and testing. A Human Machine Interface (HMI) is installed in a BCS rack close to the Control Room. It displays the current system state and allows authorized users to change the system configuration and interlock thresholds using the hardwired access key. One HMI communicates to both A- and B-chain PLC processors.

PLC I/O heads and the HMI operate on its own network infrastructure built on fiber optic. A circle topology is used for the PLC field I/O network to increase availability. The network and fiber used for the permit distribution use a fiber trunk shared only with other safety systems.

The changes to the PLC implementation since it was presented in [1] also include replacing the PLC processor to Siemens S7-1500F series and removing the third supervisory PLC. Changing the distributed I/O to ET200MP systems with increased maximum cable length reduced the number of BCS installations. At each location, regular and failsafe I/O are combined on the ET200MP rail. ET200SP rails are used in addition to ET200MP at locations where a failsafe 4-20 mA interface is required for MCMs.

A unidirectional serial interface is implemented in each PLC for EPICS status reporting. An ASCII string is sent periodically with encoded system status bits and registers to EPICS for monitoring and archiving.

FAST PATH IMPLEMENTATION

The basis architecture using a summary layer (DSC) and permit generating layer (SOC) was previously used in LCLS BCS. The following changes have been implemented to fulfil LCLS-II requirements. First, an additional permit path was added to allow each sensor to trip the superconducting (SC) linac, the normal-conducting LCLS linac, or both. Second, due to an increased sensor count, expandability is added at the DSC level when several DSCs can be daisy-chained together. All long haul connections are made with fiber optic, and regular copper cabling is used for local connections.

Digital Summary Chassis

The DSC acts as a middle layer node to interlock all BCS electronics and associated sensors that require fast shut-off in a given region. Each chassis is able to handle up to eight sensors. Inputs are optically isolated and protected from overvoltage and overcurrent.

Each input can be configured to inhibit beam in the two linacs independently by generating two permitting outputs. Since the SC linac shares accelerator housing with LCLS starting in the final third of the housing, the fault in sensors in the first two thirds of the housing removes the SC linac permit only. As BLMs detect losses of beam in all beam transport lines, all faults in sensors downstream of LCLS injector starting point revoke permits both from SC and LCLS injectors. The photodiode BTM is located in the soft X-ray (SXR) beamline and can be hit by FEL produced by either linac, thus it also revokes both permits. Some slow path sensors like MCM and water switches disallow beam production by one linac only if corresponding magnet power supply or cooling circuit is not shared between LCLS and LCLS-II.

DSC channel bypasses are centrally managed through the PLC. DIP-switches on the DSC main board are used for local bypassing of unused channels. These switches are not accessible from front or rear panels and are meant for initial configuration only.

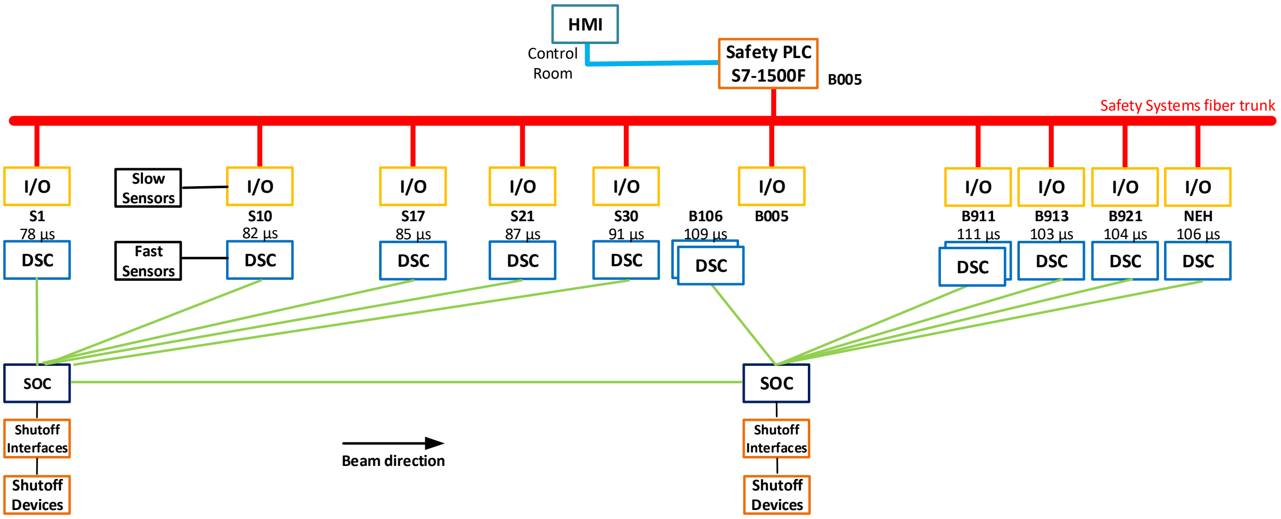

Figure 2: BCS Architecture Layout and expected response time at each installation.

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA066

Permitting outputs are generated as two redundant 1 MHz optical tones that are sent to one of two SOCs or another DSC. Test switches are available on the front panel for testing individual inputs as well as each of the four output permits.

A Beckhoff BK9000 Terminal I/O is used for status monitoring. Four KL1872 16-channel digital input modules report input sensor fault and bypass status, permit configuration and the status of output permits. A KL3002 analog input module is used for on-board voltage monitoring. The BK9000 communicates to EPICS softIOC via the controls network.

Shut-off Chassis

The SOC is the central node for BCS permit logic. It processes the inputs from DSCs at each installation and converts them into redundant permitting outputs for shut-off devices. There are two SOCs in the system, they share the design of hardware but run a different logic for each configuration.

The first configuration is installed in Sector 1, close to the SC linac injector shut-off devices. They are the Acousto-Optic Modulator (AOM), two Laser Safety Shutters (LSS), the Gun RF and the RF for first SC accelerating section. Another output is used to notify MPS and the timing system that the BCS trip has occurred. It requests to stop data buffering in fast diagnostics for post-trip investigation. This SOC takes inputs from DSCs at installations from the injector to Sector 30, 3 km away.

The other configuration is deployed in the Beam Switch Yard (BSY) and interfaces to the LCLS BCS, SXR/HXR kicker and septum sets. The last two are used as dedicated hardwired path for beamline safety stoppers interlock: if a stopper goes off the out limit switch, the permits to corresponding kicker and septum are removed. The BSY SOC covers installations from the BSY to the Near Experimental Hall. The SOC has inputs reserved for system extension to include LCLS-II Scientific Instrument (L2SI) BCS installation and LCLS-II High Energy (HE) upgrade.

Each SOC is able to process permitting inputs from up to eight summary chassis through 32 optical inputs for A- and B-chains separately for SC and LCLS injectors. All inputs are active and cannot be bypassed. Unused channels are disabled with DIP-switch on the mainboard inside the SOC at the time it is built. There is a bidirectional redundant handshaking interface between the two SOCs through optical fiber. The two chassis exchange permits for LCLS and SC linac operation.

Given the complexity of the interlock logic and possible changes to the requirements after design is complete and before the system is fully deployed, it was decided to implement the logic on a programmable device (CPLD). Both chains will run identical firmware which will be reviewed by an independent verification team.

Along with DSC inputs, the interlock logic takes inputs from the PLC. The slow-path permits are combined with fast path permits through this interface. In addition, the PLC is able to revoke the permit going to each shut-off device individually for testing purposes.

Cross-interlocking is implemented with sum A- and B-chain permits inside the SOC such that both redundant permits for each shut-off device are removed if either chain trips. This feature can be disabled with a front panel switch in order to demonstrate that each chain can functions independently during testing.

Outputs to the shut-off devices are 24 V DC voltage signals or “dry”-contacts that operate in failsafe logic: voltage level and close contacts indicate permitting condition. Front panel tests switches are implemented for output permits.

Similarly to the DSC, the SOC uses Beckhoff Terminal IO for status monitoring and relaying status to the control system.

Interfaces to Shut-off Devices

The laser used for the LCLS-II photo-injector incorporates an Acousto-Optic Modulator (AOM) which must be active for the laser pulse to be extracted. The BCS interfaces to the AOM through its External Modulator Efficiency control input. While no voltage is applied to the input, no laser output is generated. The BCS-to-AOM interface chassis is designed for fast control voltage removal. A dual trip mechanism is used with a fast analog switch connected in series with a slower but more reliable relay. The relay and the switch can be tested separately with buttons on the front panel. The modulator efficiency voltage during permitting conditions can be adjusted with a potentiometer. The AOM interface chassis combines BCS permits with MPS and Laser Safety System inputs that also use the AOM as primary shut-off mechanism. The AOM is the fastest shut-off device in the system. The last pulse on the laser output is observed 28 µs after the BCS permit is removed after which there is no laser extracted.

The Superconducting accelerating section RF and the LCLS-II Gun RF use the same solution for interrupting the RF path between the LLRF output and the Solid State Amplifier (SSA) input. A PIN diode is used with submicrosecond switching time. An RF coupler is installed after the diode and couples the RF signal back to the LLRF Precision Receiver Chassis to ensure that the RF signal does not reach the SSA while the BCS permit is revoked. The test switch on the front panel can be used to activate the trip.

The LCLS-II BCS has a single point of connection to the LCLS BCS from the SOC in the BSY to the legacy LCLS SOC. The two systems are decoupled otherwise.

Permits for septa are summed with other interlocks and passed to the enabling input of the power supply controller. Permits for kickers will be connected directly to the kicker interface chassis to enable kicker modulation.

The LSS controller chassis comprises laser shutter controllers and repeating relays. Each shutter is equipped with a set of switches which are replicated to PLC for confirmation that the shutters are closed. Otherwise the system generates an alarm.

More details on BCS shutoff devices and alarms can be found in [2].

Shut-off Time Calculation

The distance for signal propagation from the most downstream sensor to the SC electron gun is about 4 km which corresponds to 20 µs of signal delay assuming 2/3rd speed of light propagation speed in fiber or copper media. The AOM, the fastest shut-off device, is able to inhibit the beam production in less than 30 µs. Once safety margins and uncertainties are accounted for, 100 µs of the 200 µs overall response budget is left for the fast shut-off path electronics. It is split between the sensor response, signal latency in processing electronics, DSC, SOC and shut-off interface chassis. At the design stage, 10 µs was budgeted for each electronic unit, but the first articles build demonstrated even faster response. The response time of the electronics is mostly defined by the speed of optocouplers in input and output interfaces and the 1-MHz tone used for fiber optic connections.

Expected beam shut-off times for sensors at each installation are shown in Figure 2 and range from about 80 µs for sensors close to the AOM to less than 120 µs for distant sensors connected to first of two cascaded DSC.

Built-in Test Features

Testing capabilities are built in at each level of the system hierarchy. Manual test switches generate faults at the device, DSC, SOC and shut-off interface levels and allow testing the interlock propagation to lower levels down to each shut-off device. An automated test can be instigated by the PLC in device electronics. The PLC can also change the permitting outputs inform the SOC to the shutoff devices to test each device individually. The use of the PLC allows the interlock logic testing and bypass configuration verification to be done within minutes and is fully automated. For the ACM, the PLC requests a test tone to be injected in the RF cavity, which generates a trip in the ACM processing electronics, so in this case, the automated test covers the sensor level as well whereas for BLMs the test comprises an injected charge to the processing electronics only. In addition to these invasive confidence trip tests, all sensors connected to the “fast-path” are continuously self-checking, verifying the sensor health and connection continuity. Confidence tests and self-checking are diagnostic tools that cover all parts of the sensor electronics and shutoff architecture functionality. Diagnostic coverage for each level is shown in Figure 1.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

The FMEA identified numerous safe detectable and undetectable failures along with several dangerous detectable and three dangerous undetectable failures. Two of them pertain to shut-off devices that are not used as the primary shut-off mechanisms, and the third one deals with the response time of AOM, a sudden increase of which is not detectable with system diagnostics and therefore needs to be verified periodically through measurement. Currently statistics are being collected on how reliable the 28 µs AOM response time is. Based on the results, a decision on the periodicity of such test during operations will be made. Failures caused by continuity loss between layers are either safe because of positive logic of permitting signals or detectable by diagnostics embedded in failsafe PLC I/O.

The ability to instigate the test trip and the continuous self-checking at the sensor and electronics levels give a high diagnostic coverage of the system shut-off path and addresses most of failures listed in FMEA. This, in combination with redundant implementation (hardware fault tolerance of 1), ensures a high safety integrity level (SIL) which is commensurate with SIL-2 defined in IEC 61508. A specific SIL is not required, however the Radiation Safety Systems Technical basis document [3] indicates that SIL-2 is an appropriate design goal for the project. The slow path leverages an industrial safety-rated solution capable of delivering SIL-3 per Siemens PLC safety manual.

SUMMARY

The BCS combines about 150 sensors along all 4 km of the machine. Most of them are connected to a fast interlock path that consists of DSC, SOC, interface chassis and shut-off devices. There is in addition a slow interlock path based on distributed PLC I/O system and PLC processor units. The slow path shares the SOC, interface and shut-off devices with the fast path. Each level is implemented redundantly. Permissive signals from the sensor electronics are collected by the DSC or the safety PLC. Redundant signals from the DSC are inputs to one of the two SOCs which provide permitting signals through a shut-off interface chassis to the shut-off devices. The shut-off devices allow or inhibit the production of beam. The fast shut-off path is expected to stop the beam production within 120 µs for the most distant sensors. Debug hooks and test points are provided to streamline troubleshooting and certification including automated testing between the sensor electronics and the SOC.

REFERENCES

[1] E. Carrone, M. D. Cyterski, J. M. Murphy, and F. Tao, “A Streamlined Architecture of LCLS-II Beam Containment System”, in *Proc. ICALEPCS'13*, San Francisco, CA, USA, Oct. 2013, paper TUCOCA07, pp. 930-932.

[2] C. I. Clarke *et al.*, “LCLS-II Beam Containment System for Radiation Safety”, in *Proc. FLS'18*, Shanghai, China, Mar. 2018, pp. 187-192. doi:10.18429/JACoW-FLS2018-THP1WD02

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