ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA141

DYNAMIC SYSTEM RELIABILITY MODELLING OF SLAC's RADIATION SAFETY SYSTEMS

F. Tao†, K.W. Belt, SLAC National Accelerator Laboratory, Menlo Park, USA

Abstract

When the LCLS-II project is completed in 2020, there will be three major Department of Energy (DOE) beam programs occupying the same 2-mile long accelerator tunnel, e.g. LCLS, LCLS-II and FACET-II. In addition to the geographical overlap, the number of beam loss monitors of all types has been also significantly expanded to detect power beam loss from all sources. All these factors contribute to highly complex Radiation Safety Systems (RSS) at SLAC. As RSS are subject to rigorous configuration control, and their outputs are permits enabling beam production and transportation, even small faults can cause a long down time. As all beam programs at SLAC have the 95% beam availability target, the complex RSS's contribution to overall beam availability and maintainability is an important subject worth detailed analysis. In this paper, we apply the reliability engineering techniques to analyze the RSS reliability for all three beam programs. Both qualitative and semi-quantitative approaches are used to identify the most critical common causes, the most vulnerable subsystem as well as areas that require future design improvement for better maintainability.

INTRODUCTION

At SLAC National Accelerator Laboratory, there are multiple beam programs taking up part of the same famous two mile long linear accelerator (linac) constructed over 50 years ago. In 2020, when the second generation free electron x-ray laser powered by superconducting electron beam, e.g. LCLS-II, starts operation, there will be three large scientific research user facilities in SLAC, e.g. LCLS, LCLS-II and FACET-II. All those beam programs have their own dedicated beamline components, and share some infrastructure and supporting systems as well.

Being a user facility implies that the SLAC should deliver the beam to the user for their experimental use at a high availability. The availability target for both LCLS and LCLS-II is 95%. Unlike simpler synchrotron radiation facility such as SSRL in SLAC, LCLS and LCLS-II's x-ray laser are driven by an electron accelerator using normal conducting and superconducting RF technologies respectively. Those system are very complex as many subsystem must function in a coordinated manner for the successful system operation.

Among those systems, Radiation Safety Systems (RSS) including Personnel Protection System (PPS) and Beam Containment System (BCS) are carrying out safety critical functions, and play an important role in the system availability. Those reasons include:

- The outputs of RSS are permit signals, which are vital for the overall system operation. Without those permit signals, the beam cannot be generated, accelerated, and delivered to the end users.
- RSS are safety-critical systems with rigorous configuration control, the failed parts have to be isolated and/or repaired to restore the system to normal state. Bypassing faulty parts is generally not allowed, as this will disable the safety function or increase the potential radiation risks, which should be carefully evaluated.
- Unlike other critical systems such as RF, which has some level of redundancy, radiation safety systems are usually configured as one out of two (1oo2) or one out of one with diagnostics (1oo1D), any failure in the single chain will stop the beam operation, make it unavailable for user experiments.
- When RSS are tripped off for some reason, it usually implies there is something wrong, either lower level of control/protection system fails or there is some procedural violation. It generally requires operators to find out the cause of the trip, rather than simply pressing the Reset button to resume the operation. For this reason, the system restoration time is longer.
- With the rigorous configuration control, any invasive diagnostic/repair work requires "Radiation Safety Work Control Form", and need approval from various stakeholders before the work are permitted. This also contributes to the longer restoration time.

For reasons lists above, it is important to evaluate the RSS reliability as early as in the design stage, and constantly re-assess the situation during the entire lifecycle of the system, including operation, maintenance, and proof testing periods. Although the reliability assessment is generally for random failures, continuous assessment and failure analysis can help to identify the systematic failure causes. As a return, it can enhance the overall system safety, which definitely takes priority over the system availability.

Though both PPS and BCS are both safety-critical RSS, two systems are fundamentally different by following criteria:

- System topology: PPS is mostly a de-centralized system, is built upon each zone or region, higher level system will look at each area for decision making; BCS is a centralized system, individual sensor equally contributes to the system action.
- Technology used: PPS is not required to be fast, so they are typical electrical or programmable electrical systems. Electronics are often contained inside commercial-off-the-shelf (COTS) sensor and the signal

† Email address: fengtao@slac.stanford.edu

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA141

processing unit. BCS is mainly electronic systems with some programmable electronics for data acquisition.

There are already statistics on the LCLS beam program availability as well as the reliability metrics from each individual system including RSS [1]. However, such a long time statistics does not provide insight on the system design and provide guidance on system testing and maintenance. On contrary, the statistics approach often failed to take the effects of system upgrades into consideration. In another word, after a new system upgrade, some components are in the burn-in stage associated with higher failure rates. Therefore, we believe the reliability modelling approach is far more useful, and can reveal the system interdependency, provides insights on the vulnerabilities and point the direction for future improvements.

Once the reliability modelling is completed, the next step would be reliability prediction, which is to apply reliability data to predict the system reliability performance in terms of Mean Time Between Failures (MTBF) and Mean Down Time (MDT) etc. The reliability prediction is generally performed based on the assumption that system components have a constant failure rate, e.g. within their useful product life. Unfortunately this is not the case for some legacy PPS. In the middle section of linac, e.g. from Sector 10 to Sector 20, the PPS is 50 years in service built with mechanical relays. Obviously those relays are long past the useful life, and their failure rates are on the rise. Therefore, the reliability predication of these systems should be used with precaution.

PPS RELIABLITY MODELLING

PPS has three levels of implementation, from bottom to top are:

- Chassis/Assembly for a specific functionality, such as BSOIC (Beam Shutoff Ion Chamber), BTM (Burn Through Monitor), Stopper, Secure Loop, Set Entry Loop etc.
- Zone level PPS for a local zone control,
- System level PPS responsible for a particular beam program.
- RSS network infrastructure and operational interface

Network and Operational Interface

On the top level, there is a PLC based distributed system named as “Master Beam Control” (MBC), which includes a S7-1500 PLC system, and mobile HMI panels for operators to operate both PPS and BCS. For PPS, it transmits “Hardware Enable” signal to each local PPS system so that they can accept the operator commands from EPICS with the companion of this signal. For BCS, the “Beam ON/OFF”, “Reset” signals are also transmitter to BCS racks for beam operation. The mobile HMI panel, as shown in Figure 1, is also used for alarm display and acknowledge. During the LCLS-II construction, this PLC system has been expanded to cover every sector where exists RSS racks. The reliability can be calculated for this system, which include PLC CPU, I/O modules. The fiber optics media and the network switches are excluded from the evaluation as the system adopt a ring topology and is immune to single point failures. The mobile HMI panels (Fig. 1) are not included in the availability calculation as there are more than 10 panels, and a single panel failure has no impact on system operation.

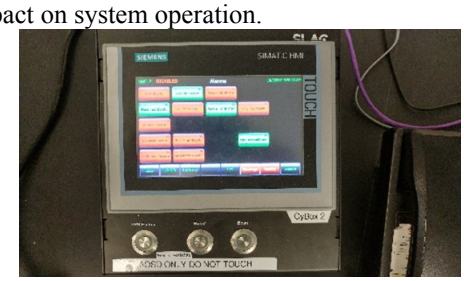

Figure 1: Mobile HMI Panel of MBC.

System Level PPS

There are three beam programs coexist in the accelerator: LCLS, LCLS-II and FACET-II. LCLS and LCLS-II use different injectors and accelerating RF structure. In the accelerator layout, the Cu beam from LCLS and SC (Superconducting) beam from LCLS-II can be delivered to either soft x-ray (SXR) or hard x-ray (HXR) undulator to generate x-ray laser and delivered it to 3 SXR experimental hutches and 5 HXR hutches. In the Near Experimental Hall (NEH), there exists all three SXR hutches and one HXR hutch. While all four hutches in the Far Experimental Hall (FEH) are for HXR experiments. The overall accelerator layout is shown in Fig. 2 below:

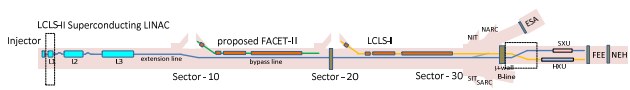

Figure 2: SLAC’s Accelerator Layout.

In the LCLS-II baseline design, SC beam can be delivered to HXR and SXR hutches, while Cu beam can only be delivered to HXR hutches. Another ongoing CLTS project enables the Cu beam’s delivering to SXR hutches as well. Combining both projects, both SC and Cu beams can be delivered to any SXR/HXR hutches for experimental use.

To meet this goal, beam stoppers and beam switching devices are critical. These devices locate from Sector 28 to the Beam Switching Yard (BSY) as shown in Fig. 3:

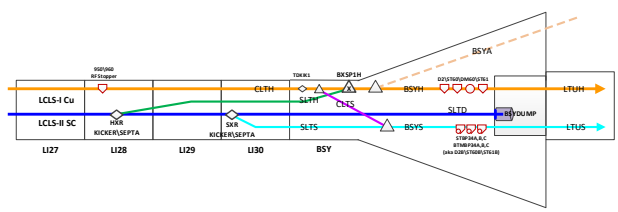

Figure 3: SC and Cu Beam Switching.

Global Beam Switching

As shown in Fig. 3, the beam switching involved the coordination of multiple devices including magnets, kicker/septum and stoppers. For this reason, a dedicated

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA141

safety PLC has been developed for this control. It is a Pilz PNOZMulti safety PLC system to make sure the correct action with correct sequencing. BCS also provide permits to those kicker/septum as a quicker shutoff to lessen the damage in case of beam mis-steering or larger than expected beam power.

BSOICs

BSOICs are beam loss detectors owned by PPS to detect the higher than normal radiation level (usually setpoint is chosen as 10mrem/hr) in areas accessible by people during beam operation. Depending on the location and detector type (Gamma or Neutron), a BSOIC's trip may trip off SC beam or both SC/Cu beam. For FACET-II beam program, there are only 3 BSOICs interlocking to the beam production and transportation. For the sake of simplification, we denote these BSOICs as Group D BSOICs. For LCLS and LCLS-II beam programs, there are far more BSOICs to detect the abnormal radiation dose level. Those instruments are divided into three groups, Group A interlocks to SC Injector and RF only; Group B interlocks to both SC and Cu Injectors and accelerating RF, and Group C interlocks only to Cu beam operation.

Historical data shows that BSOIC are generally reliable instruments with fewer issues, but they requires periodic calibration to ensure the accuracy.

BTMs

BTMs are used to detect mis-steered beam or equipment damage (e.g., stopper being burned through), where such would risk radiation exposure to personnel. They are typically associated with BCS collimators or insertable stoppers, and consist of a pressure-monitored gas-filled-bladder near or around the associated device. Beam impinging on the BTM causes minute holes which reduce the bladder pressure until the pressure switch trips. There are two types of BTMS: "fixed volume" BTMS which are sealed against incoming gas, and "flow-through" BTMS which allow a slight gas flow out. BTMS are "dual-chain" devices having redundant pressure monitoring switches tied to PPS.

As BTM is also called "Disaster Monitor" by other accelerator laboratories, which implied that a true BTM fault indicates something very bad has happened. For this reason, currently all BTM on LCLS and LCLS-II beamline trip off both SC and Cu beams. There are a small quantity of FACET-II BTMs only trip off FACET-II beam.

BTMs in the photon area often have small leakage issues, and need to be re-filled before they trip off the system. During the re-filling process, the PPS has to be switched to the "testing" mode, and make the beam program unavailable for experiments.

BCS RELIABILITY MODELLING

Unlike PPS, where there are multiple levels of control systems, BCS is a centralized system for each beam program. The exception is the Master Beam Control (MBC) PLC system, which crosses the boundary of individual beam program and shares the site wide RSS information.

LCLS-II BCS PLC System

The existing LCLS BCS and the new FACET-II BCS use customized simple electronics, hence the reliability is expected to be very high. The new LCLS-II BCS uses Siemens S7-1515F safety PLC and distributed I/O modules as the backbone for data acquisition and control. It not only perform interlock functions for slow BCS sensors, but also exchange configuration/control/status information with fast electronics associated with fast BCS sensors.

LCLS-II BCS has an output connecting to the LCLS BCS shutoff chassis, so that if the LCLS Cu beam is the source that cause a LCLS-II BCS fault, it can re-route the shutoff request to the LCLS BCS shutoff chassis to initiate the shutoff. For this reason, considering the fail-safe nature of the safety PLC, the PLC system failure will also make the Cu linac unable to operate.

Beam Loss Monitors (BLMs)

In addition to the existing point beam loss monitors (Protection Ion Chamber) and line beam loss monitors (Long Ion Chamber) installed for LCLS BCS, LCLS-II BCS will add a large quantity of Diamond sensor for point beam loss monitors and special fiber optics area beam loss detectors. Due to the high beam power of LCLS-II, the fiber optics has a full coverage from beginning to the end of the accelerator to detect the abnormal beam loss along the accelerator. The shutoff action for those beam loss monitors are targeted shutoff from beginning of the accelerator to Beam Switching Yard (BSY) as the accelerator till BSY is deeply buried underground, and the beam mis-steering is less dangerous than in other areas where the accelerator tunnel is close to the ground.

For this reason, we divide the BCS BLMs into 3 groups the same way as PPS BSOIC. Group A interlocks to SC linac only; Group B interlocks to both SC and Cu linac while Group C only interlocks to Cu linac.

RELIABLITY PREDICATION

With the PPS and BCS major component discussion in the previous sections. We can create a reliability block diagram for both x-ray laser and FACET-II experiments as shown in the Fig. 4 on the next page.

Since PPS is mostly an electrical system using COTS parts, reliability prediction is feasible if only the complete BOM is available. Legacy PPS uses electromechanical relays and timers to build the logic circuits. In a typical zone PPS, there is about 35 such relays involved in the safety functions, while others are used to either drive LEDs or for CAMAC communication. In a typical stopper chassis, there is 24 relays installed inside with only a few responsible for the safety control function as well. The typical "Parts Count" method can provide a quick but conservative estimation of the reliability performance for systems within this category. PPS sensors are mainly switches, e.g. pressure, position, keyswitch etc., whose reliability data is widely available from commercial reliability handbooks including [2], [3]. The only exception is BSOIC, whose processing unit is composed of simple electronics and an

ISBN: 978-3-95450-209-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2019-MOPHA141

8031 microprocessor. The field track shows that the BSOIC failure rates are very low.

There are three brands of PLC used in PPS and BCS: Allen-Bradley ControlLogix, Siemens Simatic S7 controllers and distributed I/O modules, Pilz PNOZMulti safety PLC. The reliability data of the first two brands can be easily obtained from [4] and [5] respectively. The reliability information for Pilz PLC is difficult to find, but as a SIL3 rated PLC, its SISTEMA library file contains dangerous undetected failure rates published, and as well as the Diagnostic Coverage (DC). From those information, we can calculate the failure rate reversely.

Reliability predication for BCS electronics is quite complex. For customized electronics with common electronic parts, the reliability calculation can use the same "Part Count" method using BOM of the design and reliability data handbook [6]. The difficulty come from sensors used in radiation detection, as they are new to SLAC and has no credible documented failure modes and failure rate information.

The overall RSS reliability modelling is shown in Fig. 4 below.

.

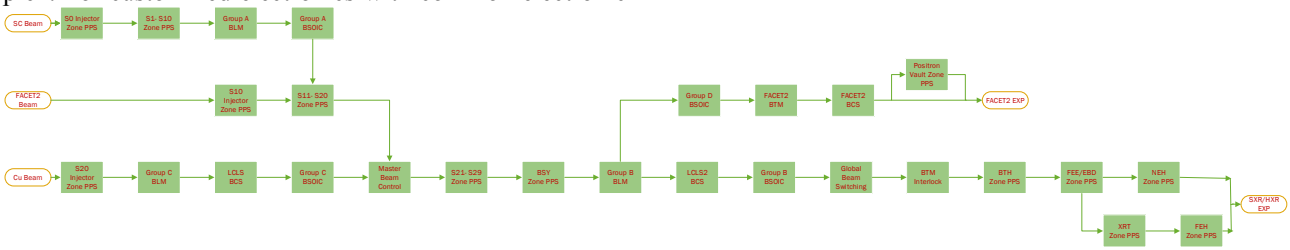

Figure 4: Reliability block diagram of SLAC's beam program.

CONCLUSION

In this paper, we analyze the SLAC's accelerator layout as well as the major systems of the RSS including PPS and BCS. For SLAC's three beam programs, FACET-II, LCLS and LCLS-II, their beam availability's dependence on RSS has been analyzed. There are several interesting observations:

- S11-S20 Zone PPS are legacy relay based systems. Their failure will prevent the SC beam's delivery to the x-ray laser experiment, regardless the high project cost;
- Master Beam Control (MBC) is responsible for the global RSS operation. Even though it is not a safety rated system, its failure will make it impossible to operate any SLAC's beam experiments.
- LCLS-I and LCLS-II are not independent, which is less desirable as their beam can both delivery to any SXR/HXR hutches.

REFERENCES

[1] W.B. Allen *et al.*, "Availability performance and considerations for LCLS X-Ray FEL at SLAC", SLC-PUB-144-22, Aug. 2011.

[2] *OREDA:Offshore Reliability Data Handbook*, SINTEF, 2002.

[3] *Safety Equipment Reliability Handbook*, 4th Ed, Exida, 2015.

[4] *Using ControlLogix in SIL2 Applications*, Allen-Bradley, Publication 1756-RM001E-EN-P, Nov. 2006.

[5] "Mean Time Between Failure (MTBF) - list for SIMATIC products", Siemens Download Entry ID: 16818490, Aug. 2019.

[6] *Electrical Parts Reliability Data (EPRD)*, Quanterion Solutions, Inc., 2014.