SAFETY INTEGRITY LEVEL (SIL) VERIFICATION FOR SLAC RADIATION SAFETY SYSTEM

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

Abstract

Safety Integrity Level (SIL) is a key concept in functional safety standards. SIL is a performance measure on how reliable a safety system is in performing a particular safety function. To comply with standards, during the system design stage, SIL verification must be performed to demonstrate that the SIL achieved meets/exceeds the SIL that was assigned during risk assessment. Unlike industrial applications, where safety systems are usually composed of certified devices or devices with long usage history, safety systems in large physics laboratories are less standardized and more complex in terms of system architecture and devices used. In addition, custom designed electronics, with limited reliability information, are often employed. Verifying SIL for these systems requires in-depth knowledge of reliability evaluation. In this paper, it is demonstrated how to determine SIL using SLAC radiation safety systems (Personnel Protection System (PPS) and Beam Containment System (BCS)) as examples. PPS utilizes commercial safety rated devices, while BCS contains customized electronics. Choice of standards, methods of evaluation, reliability data gathering process (both from industry and from hardware development) are also discussed.

INTRODUCTION

At SLAC National Accelerator Laboratory, there are three protection systems deployed to mitigate radiation risks: Machine Protection System (MPS), Beam Containment System (BCS) and Personnel Protection System (PPS). While MPS is focused on protecting equipment from getting damaged, the other two systems are critical to protect personnel and the environment from getting a radiation dose. In comparison with the MPS, PPS and BCS have very rigorous configuration control policies in place and follow all due diligence in engineering practices. For these reasons, these two radiation safety systems meet all definitions of safety-critical control systems.

Functional safety standards started in 1990's and now there are several critical standards have been developed and adopted worldwide. Such as IEC61508 [1] and corresponding sector specific standards IEC61511 [2] (process), IEC 62061 [3] (machinery). ISO also published a machinery safety standard ISO13849 and its relationship with IEC62061 is described in a IEC/ISO joint technical report ISO/TR23849 [5]. While industries have started following functional safety standards in implementing safety-critical control systems two decades ago, the natural question that arises is, are the same standards applicable to accelerator safety systems, and if the answer is yes, how are the standards applied so that we can learn from industries' long time experience with the engineering design and operation of safety systems.

As found in any functional safety standard, two key concepts are safety lifecycle and safety integrity level. The former describes a series of activities in system engineering and operation to make sure all risks are identified and properly mitigated. The latter is a measure of the reliability performance each safety function within the safety system, such that the design be precisely performance based and is less conservative than the traditional description-based approach.

In all functional safety standards, after the conceptual design stage, the SIL of the safety function must be verified to make sure it meets or exceeds the SIL assigned in the Safety Requirements Specification (SRS). In the case the safety system/function SIL level is not met, the safety system/function must be re-designed. For example, the following figure is from IEC 61511.

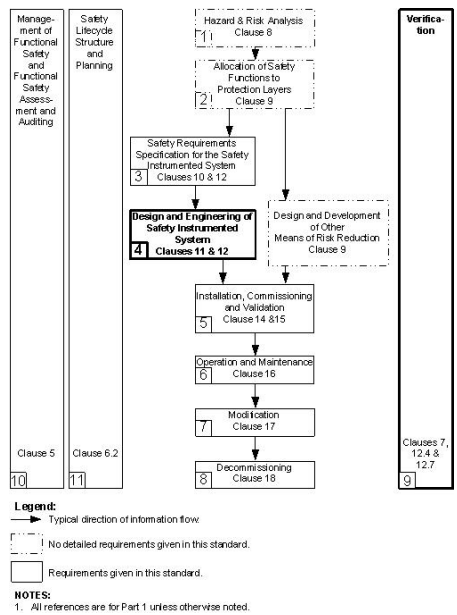

Figure 1: Safety System Lifecycle Phases.

Though PPS and BCS are both classified as safety-critical systems with the purpose to mitigate radiation risks, different philosophies and technologies are used. The majority of the PPS devices are commercial off-the-shelf (COTS), their reliability data can be obtained and the system level reliability block diagram (RBD) can be

ISBN 978-3-95450-148-9

quickly built. On the contrary, BCS has many accelerator unique sensors such as beam loss monitors, beam current monitors etc. The system needs to response to these sensor signals in a very short time, 100uS for the LCLS-II BCS, and bring the system into the safe state. Commercial off-the-shelf products do not meet the required shut off times nor are their interfaces compatible with unique sensors found in accelerators. These reasons contribute to the need for custom electronics designed hardware.

For these reasons, the SIL verification for these two systems face different challenges and need to utilize different methodologies.

PPS SIL VERIFICATION

The Personal Protection System (PPS) is responsible for keeping people away from beam. The system is composed of an access control systems and a safety interlock systems. At SLAC, this configuration is implemented with a 3 PLC architecture, one access control PLC responsible for access related functions as well as acting as a communication bridge between EPICS and safety controllers. For safety interlocks, there are two redundant stand-alone safety PLCs in an A/B chain configuration to independently monitor the safety interlock conditions. A typical PPS installation is shown in the following figure.

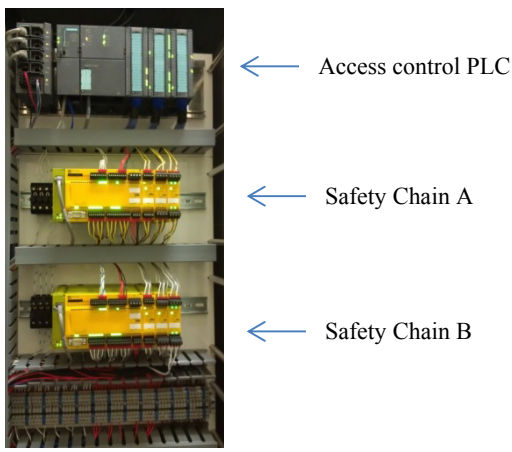

Figure 2: A Typical PPS Installation.

Access control functions are generally classified as non-safety critical, so usually no SIL number is assigned or verified during the design stage. However, if other systems such as Oxygen Deficiency Monitoring (ODM) system need to use "access control system" as one protection layer, the this system can be regarded as one protection layer with SIL1 capability if only the rigorous configuration control is in place.

Compared with access control functions, those interlock functions implemented within the PPS safety PLCs are more critical. Their major functions are to detect that the beam operation safety boundary is secured during beam operation, and that there is no excessive radiation in occupiable areas. Typical inputs for these functions are micro-switches and area radiation monitors whereas the outputs are stopper/RF permits.

Figure 3 shows the RBD for E-stop interlock in the photon area. In this example, inputs are Emergency Off buttons and the outputs are two solenoid valves. Pilz PNOZmulti safety controller can de-energize the solenoid valves and 2 beam stoppers will move in due to the gravity force.

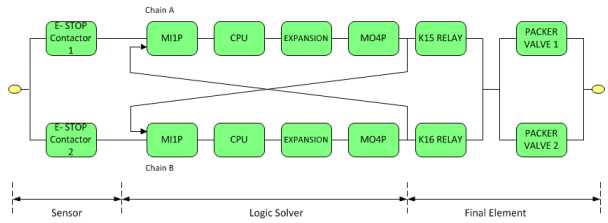

Figure 3: RBD for PPS E-stop.

As this is not a standard architecture that appears in any functional safety standard, its reliability cannot be calculated by using the standards or commercial software. However, standards do not expect a very accurate reliability calculation, but accentuate that the results must be conservative such that the safety system is not under-designed. Therefore, we can use the "cut set" concept in reliability engineering and quickly obtain the performance bounds of the above configuration:

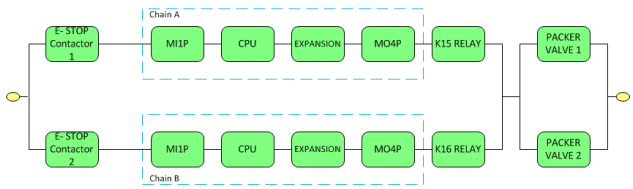

Figure 4(a): equivalent RBD with lower reliability.

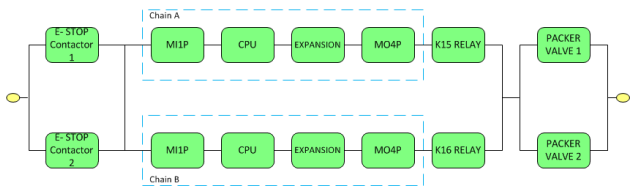

Figure 4(b): Equivalent RBD with higher reliability.

The two RBDs shown in Figure 4 are standard configurations, and their reliability can be calculated using the standard 1oo2 configuration formula. Since the configuration is redundant, the common cause failure dominates the reliability performance. In this case, with the common cause factor being considered, the difference between two bounds is small and we can simply use the result associated with Figure 4(a) as approximation.

The common cause/mode failure portion is usually represented as $\beta\lambda_{DU}$, where λ_{DU} is the dangerous undetected failure rate of a single channel. Common configuration is when two or more redundant channels are

ISBN 978-3-95450-148-9

identical, if this is not the case, the λ_{DU} can be replaced with the geometric average for two or more channels. On the other hand, in the existing formulae, if there are multiple redundant channels, common cause or common mode failures are less likely to occur at the same time and the system reliability is improved. To properly give the credit for this configuration, the modified Beta- method is given in [6] as:

$$\beta(MooN) = \beta C_{MooN}$$

Table 1: Common Cause Factors for Different Voting Logics

M\N	N=2	N=3	N=4
M = 1	C_{1oo2}= 1	C_{1oo3}=0.5	C_{1oo4}=0.3
M = 2		C_{2oo3}=2.0	C_{2oo4}=1.1
M = 3			C_{3oo4}=2.9

PPS interlock to electron stoppers are quite often triple or quadruple, and the modified Beta-method will be useful in the reliability calculation.

Another challenge for PPS SIL verification is to obtain the reliability data for some large accelerator unique equipment, such as modulator (providing the power to klystron) and Variable Voltage Substation (VVS) (providing the power to modulators).

To analyse the reliability performance for PPS functions interlock to these devices, we have to look into the detailed schematics of those devices to create the RBD and perform the SIL verification. For example, a control reliability analysis for a VVS was performed and it was found that the configuration is vulnerable to control power loss:

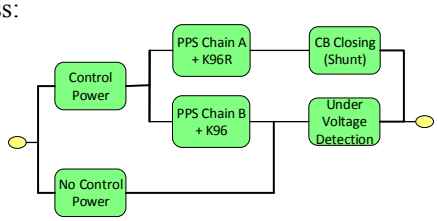

Figure 5: RBD for VVS interlock to PPS.

To calculate the reliability of such a scheme, we will need to substitute in the RBD into "PPS Chain A" and "PPS Chain B" to get the final results. A noticeable shortcoming of such a configuration is its dependence on control power. A simple solution to improve the overall system reliability would be power line monitor and alarming. So that the alarm will notify operators the power loss, and corresponding remedy actions can be taken to mitigate the risk.

For power system devices, their reliability analysis method as well as failure rates can be found in IEEE 493 standard. However, if the device is special, customized or has been modified, then site specific reliability data is more valuable.

In the VVS interlock case, the PPS Chain A controls a 2000A circuit breaker, whose failure rate can be obtained from IEEE 493, but the Chain B controls a SLAC modified device which is a customized modification. With the aid of SLAC CATER (Comprehensive Accelerator Tool for Enhancing Reliability), past 20 years of service records for that device can be found. Based on that data, the failure rate of chain B "under-voltage detection" mechanism can be calculated. This highlights the importance of keeping records of site specific operational data, which is valuable in system reliability evaluation.

A standard interface to modulators has been implemented as well. Commercial safety circuit breakers will be used to meet the PPS requirements on reliability and safety performance.

These breakers are designed to meet ISO 13849 machinery safety standards with manufacturer provided device failure rate data. The auxiliary contacts comply with IEC60947 standard, such that the contact can always provide the true status feedback to PPS for setting access to accelerator, which is also a safety instrumented function.

It should mention that when IEC 61508 was first published in 1998, there was no detailed explanation on how those equations in Part 6 were developed. It caused confusion and people made mistakes when trying to extend the results to non-standard configuration. With the Recent publications of technical reports and a research monograph [6-8], practitioners in this field will have better understandings on reliability modelling of safety systems.

BCS SIL VERIFICATION

The BCS for the LCLS-II project will adopt a hybrid architecture to meet safety, reliability and response time requirements. For those interlocks needs slow response times, sensor inputs directly connect to Safety PLCs. But for those fast sensors that require fast response times, customized designed electronics have to be developed and deployed to achieve these speeds.

Illustrated in Figure 6, the PLC architecture is not implemented in the same way as with the PPS. A partial reason for this is to reduce the system hardware cost but still follow the recommended configuration from the PLC manufacturer. With this PLC configuration, the system is still SIL-3 capable as suggested by the PLC safety manual.

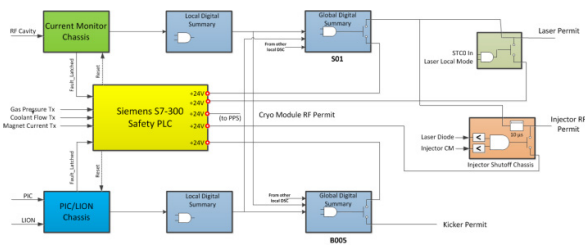

Figure 6: LCLS-II BCS Diagram.

ISBN 978-3-95450-148-9

For customized electronics, reliability data is not immediately available therefore the reliability data has to be estimated from the electronic design schematics. For this task, IEC 61508 has to be followed to make sure that other design requirements are met before the design is considered suitable to be used in SIL rated safety applications. In the design process, design for reliability should be established at beginning in addition to functional requirements. Failure Modes Effects and Diagnostics Analysis (FMEDA) should be carried out to get quantitative information of the design. Then Diagnostics Coverage (DC), minimal fault tolerance and Safe Failure Fraction (SFF) has to be calculated and comply with requirements from IEC 61508. Once the structural constraints are met, further details on reliability performance can be quantified. There are many data sources on electronic parts available, such as [9-11]. Hardware design engineers should combine these sources to get the reliability information requested by IEC 61508. Additionally, SIL verification can still follow the methodology given in standards, technical reports as if the data is provided by "manufacturer".

CONCLUSION

SIL verification is an important step in functional safety standard compliance. The main purpose is to evaluate the reliability of each safety function to make sure it meets the targeted risk reduction requirement. For safety systems composed of commercial off-the-shelf devices, we can build up the reliability block diagram and fill in the reliability data to get the result. Site specific reliability data is more valuable for site specific devices. For customized designed electronics, a rigorous IEC61508 development process needs to be followed to make sure the pre-determined SIL capability is obtained as well the reliability predication information of the overall design.

REFERENCES

[1] IEC 61508, "Functional Safety of Electrical /Electronic /Programmable Electronic Safety-related Systems", 2nd Ed, IEC, 2010.
[2] IEC 61511, "Functional safety - Safety instrumented systems for the process industry sector", IEC, 2004.
[3] IEC 62061, "Safety of Machinery- Functional Safety of Safety-related Electrical, Electronic and Programmable Electronic Control Systems", IEC, 2005.
[4] ISO 13849, "Safety of Machinery – Safety-related Parts of Control Systems", ISO, 2006.
[5] ISO/TR 23849, "Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery", ISO, 2010.
[6] ISO/TR 12489, "Petroleum, Petrochemical and Natural Gas Industries – Reliability Modelling and Calculation of Safety Systems", ISO, 2013.
[7] ISA-dTR84.00.02, "Safety Integrity Level (SIL) Verification of Safety Instrumented Functions", ISA, Jan. 2015.
[8] M. Rausand, "Reliability of Safety-critical Systems", John Wiley&Sons, 2014.
[9] Telcordia SR-332, "Reliability Prediction Procedure for Electronic Equipment", Issue 3, Telcordia, Jan. 2011.
[10] IEC TR 62380, "Reliability data handbook-Universal model for reliability prediction of electronics components, PCBs and equipment", IEC, 2004.
[11] "Reliability Modelling: The RIAC Guide to Reliability Prediction, Assessment and Estimation", RiAC, 2010.

ISBN 978-3-95450-148-9