ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA03

APPLYING LAYER OF PROTECTION ANALYSIS (LOPA) TO ACCELERATOR SAFETY SYSTEMS DESIGN

F. Tao, J. Murphy, SLAC National Accelerator Laboratory, Menlo Park, USA

Abstract

Large accelerator safety system design is complex and challenging. The complexity comes from the wide geographical distribution and the entangled control/protection functions that are shared across multiple control systems. To ensure safety performance and avoid unnecessary overdesign, a systematic approach should be followed when setting the functional requirements and the associated safety integrity. Layer of Protection Analysis (LOPA) is a method in IEC 61511 for assigning the SIL to a safety function. This method is well suited for complex applications and is widely adopted in the process industry. The outputs of the LOPA study provide not only the basis for setting safety functions design objective, but also a reference document for managing system change and determining test scope. In this paper, SLAC's credited safety systems are used to demonstrate the application of this semi-quantitative method. Those examples will illustrate how to accurately assess the hazardous event, analyse the independence of different protection layers, and determine the reliability of a particular protection function.

INTRODUCTION

Layer of Protection Analysis (LOPA) is a semi-quantitative method to analyse and assess the risk. It is usually carried out after the hazard analysis stage. For each identified hazard, a multi-disciplined team of experts will further identify enabling conditions, condition modifiers, prevention/mitigation layers existing or plan to implement. Participants of the LOPA study should determine the initiating event frequency, the performance of each independent protection layers (IPL) and the effectiveness factor of the condition modifier, so that the mitigated risk can be calculated. The result will be compared with the pre-defined tolerable risk target to determine if the actual risk is tolerable. If not, additional risk prevention/mitigation measures need to be implemented to further reduce the risk until the goal is met.

Compared to full quantitative risk assessment methods such as fault tree analysis, LOPA requires only level of magnitude accuracy, and puts more focus on identifying IPLs and evaluating their effectiveness hence avoiding the huge amount of details required for a full quantitative assessment. It does not require dedicated software tools to carry out the analysis and simple spreadsheets will work.

This method was first developed in the 1990s by process industries. Later, the method was systematically developed and documented in the conceptual book [1]. This method has been submitted to the IEC 61511 standard committee by the United States and eventually was included in the informative standard [2] as a method to determine the Safety Integrity Level (SIL) of Safety Instrumented Systems (SIS). After more than two decades of industrial application, LOPA has become the most popular risk assessment method used in process industries in North America. Based on the lessons learned and field application records, Center for Chemical Process Safety (CCPS) recently published two more guidelines to help users correctly apply the method [3][4].

LOPA BASICS

Modern safety system design has switched to a risk-based approach, e.g. determining the system functionality and architecture based on how much risk reduction the safety system should provide to mitigate the risk to the tolerable level.

LOPA starts with consequence-cause pairs which are obtained from the outcome of a what-if analysis, FEMA (Failure Mode and Effects Analysis), or HZAOP (Hazard and Operability) study. For example, for a process without any protection functions, the risk associated with a particular cause can be expressed as:

$$R_i = f_i C_i$$

For the i-th event, R_i is the risk and f_i, C_i represent frequency and the consequence. The total risk is the sum of all individual hazardous scenario is:

$$R = \sum_{i=1}^{N} R_i$$

LOPA will be able to answer following questions:

- How critical is the risk
- Dependability and independence between protection layers
- How many independent protection layers exist and how many extra layers are needed
- Is the process safe enough or additional protection measures are needed

There are two categories of protection functions that can effectively reduce the risk, one is through prevention, which works on the original frequency f_i to further lower the frequency of the system, and the other approach is mitigation, which will lower the consequence C_i. For the former case, the reduced risk would be

$$R_i^C = (\prod_{j=1}^{M} PFD_i^j \, f_i) \times C_i$$

and

$$R^C = \sum_{i=1}^{N} R_i^C$$

With the underlining mathematics being straightforward, the correct application of the methods depends on properly evaluating the effectiveness of each IPL as well as other adjusting factors such as enable conditions and condition modifiers.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA03

In the following sections, authors will use three safety systems at SLAC, e.g. Oxygen Deficiency Hazard (ODH), Personnel Protection System (PPS) and Beam Containment System (BCS) as examples to illustrate how to apply LOPA to the system design.

LCLS-II ODH

LCLS-II (Linac Coherent Light Source) project will have significant presence of cryogenics not only in a cryoplant, but also in the Linac and gallery. The detailed oxygen deficiency hazard assessment method was taken from the SLAC ES&H handbook [5], which is heavily influenced by the method adopted by Fermilab [6]. In this method, the ODH classification is made for each particular area. The risk measure to quantify is the expected probability of fatality, which is defined as:

$$\emptyset = \sum_{i=1}^{n} P_i F_i$$

where

$\emptyset$ = the ODH fatality rate (per hour)

P_i = the expected rate of the i type of event (per hour)

F_i = the fatality factor for the i type of event

And the summation must include all types of events that may cause an ODH and result in a fatality.

In the risk assessment process, effects of existing and planned alarm/control systems such as forced ventilation, controls generated alarms and ventilation are considered as well as their effectiveness (failure rate). In this particular project, it is assumed that active control and a monitoring system will be able to provide SIL1 safety functions related to ventilation.

The event rates come from FMEA as well as the equipment failure rate data from [6]. As shown in Figure 1, the fatality factor depends on the concentration of oxygen [5]:

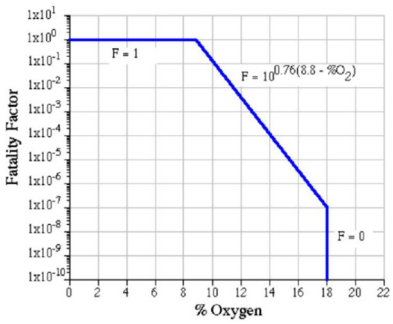

Figure 1: Fatality factor vs. the lowest attainable oxygen concentration that results from a given event.

Once the ODH fatality rate $\emptyset$ has been determined, the operation can then be assigned an ODH classification according to the criteria listed in the following table:

Table 1: ODH Fatality Rates and Classifications

ODH Fatality Rates	ODH Hazard Classification
$< 10^{-7}$	0
$10^{-7} \sim 10^{-5}$	1
$10^{-5} \sim 10^{-3}$	2
$10^{-3} \sim 10^{-1}$	3
$> 10^{-1}$	4

Table 2: Minimum Req'd Controls by ODH Classification

Engineering Controls	ODH Classification				
	0	1	2	3	4
Warning signs		X	X	X	X
Installed oxygen monitors		X	X	X	X
Ventilation		X	X	X	N/A
Personal oxygen monitor			X	X	X
Multiple person team			X	X	X
Unexposed observer				X	X
Self-contained breathing apparatus					X

In this system design stage, the assumption of SIL1 safety function, e.g. turning on ventilation during access to the accelerator tunnel, is being applied to as a risk mitigation for some faulty scenarios. It would be the responsibility of ODH/PPS to make sure that the SIL rating is achieved at the system validation stage.

LCLS PHOTON PPS

While the risk is quantifiable and there is an explicit tolerable risk target, applying LOPA always starts with calculate the risk. This is not always the case for complex systems or systems where somehow the risk target is vague. Under this circumstance, the best way to continue the risk assessment is to combine the LOPA with other qualitative approaches such as risk graph. In this section, we use the LCLS Photon PPS, also named as Hutch Protection System (HPS), as an example to demonstrate the key rules of LOPA application.

Considering the LCLS x-ray beam energy, for risk scenarios associated people in a hutch (experiment area) and exposure to the x-ray beam, applying risk graph criteria from IEC 61511-3, we have following risk graph

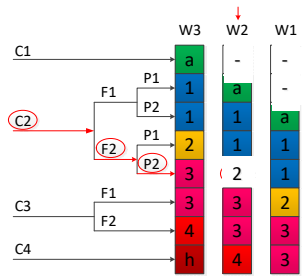

Figure 2: HPS SIL Assignment with risk graph.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA03

As shown in Figure 2, it is obvious that a SIL 2 level of protection is needed to prevent unsafe access of the hutch during beam operation. The next step is to identify all protection layers that prevent the event from happening. The detailed work table is shown in Figure 3 on the next page. In a HPS, the control system is composed of three PLCs. One Allen-Bradley ControlLogix PLC executes the access control functions, which is highlight in yellow. Safety functions are executed in dedicated safety PLC (Pilz PNOZmulti) in a dual-redundant configuration. There are several items worth further discussion:

- Generally speaking, an IPL implemented in non-safety PLC has the same level of magnitude risk reduction as a SIL1 function implemented in safety PLC.
- In case 1, function 3 and 4 combined together to fulfil a completed safety function. If the combined safety function has a SIL 1 rating, then both function 3 and 4 should meet the SIL 1 rating.
- The highest SIL is the function 3 in case 3. If this function can be reduced to SIL 1, then the overall safety PLC can be simplified to a SIL 1 system. To achieve this goal, additional measures should be taken so that one IPL can be credited and hence reducing the SIL rating of the safety interlock. For this particular case, we adopt an administrative approach by using a Zip Tie to limit the free movement of the emergency entry mechanism, as well as adding visible signage to remind people not to abuse it.

LCLS ELECTRON BCS

Compared to the electron beamline, risk along the photon beamline is relatively easy to analysis. Photon beam induced damage is limited, and the experimental area has limited entry points. For the electron side, the situation is more complex, and PPS is coordinated with BCS to mitigate radiation risks.

Both PPS and BCS are credited radiation safety systems at SLAC. BCS at SLAC ensures beam confinement within an approved beam channel at an approved allowed beam power and hence prevents the generation of excessive level of radiation within occupied areas. Not all US DOE laboratories have a BCS as credited safety system, and most commonly the functions of BCS is incorporated into the Machine Protection System (MPS).

For electron system radiation risk, we consider two representative hazardous scenarios here:

Case 1: Damage to a PPS Stopper

PPS stoppers are often used as a safety token for a worker to access downstream beamline areas. If the stopper get damaged, then depending on the downstream PPS zone access state, many people may get direct exposure to the electron beam, which is very dangerous. If too much beam power is the cause of the damage, there are the following protection layers that prevent/mitigate the risk:

1) A BCS interlock to bend magnet current (beam energy) and a BCS interlock to Average Current Monitors (beam current).
2) A BCS interlock of Protection Ion Chamber (PIC) (installed on stoppers).
3) The stopper set has two or three stoppers, there are at least two Burn Through Monitors (BTM) interlocked to PPS

Based on the redundant PPS safety PLC architecture, we can regard that each BTM interlock is a SIL 1 function, hence if only each BCS interlock function can be credited as one IPL, the overall number of IPLs would be four, which would be sufficient for the worst case. Again, for one IPL, since two BCS functions have no dependence, the system design is easier even without full compliance to the IEC 61508 standard for hardware development.

Case 2: Beam Loss in BTH

At SLAC, the accelerator tunnel is usually buried deep underground with the exception of Beam Transport Hall (BTH) area where beamline is actually above the ground, making this area sensitive and subject to induce radiation from beam loss.

To prevent the beam loss, Radiation Physicists strategically put Protection Collimators along the beamline in BTH area to intercept the mis-steered beam. In addition, there are the following active interlocks that can be credited as IPLs:

1) BCS interlock to PICs installed on protection collimators.
2) PPS interlock to BTMs on protection collimators, which will trip if the collimator get damaged.
3) BCS interlock to Long Ion Chambers (LION), installed along the tunnel wall, which can detect small amounts of beam loss.
4) PPS interlock to Beam Shutoff Ion Chambers (BSOICs), installed on the exterior wall of the accelerator housing.

Though it may seem that four IPLs can be credited as in the previous case, it should mentioned that in the LCLS BCS design, the PIC and LION monitors share the same chassis design, and may connect into the same chassis and issue the shutoff request using the same signal path. Therefore, to credit such a configuration as 4 IPLs, the BCS PIC/LION chassis must be designed as SIL2 capable, and need to compliant with IEC 61508 standard for the hardware development.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THCPA03

Case	Radiation Safety Risk	IPL	Safeguards	Creditable IPL	SIL Requirement
1	people trapped inside the hutch during beam operation	2	1. Training	No, given credit to reduce W factor	
			2. Search Preset and Search Reset	Yes (in access PLC)	
			3. Audio/Visual Warning	3 and 4 combined as one safety function	SIL 1 *
			4. E- Stop function	3 and 4 combined as one safety function	SIL 1 *
			5. Emergency Exit mechanism	No, mechanical means, depend on 3 , will have no SIL rating since it is not an I&C function	
2	people entering the hutch during operation through the sliding hutch door	2	1. Training	No, given credit to reduce W factor	
			2. Visual Warning (Y/M light)	No, given credit to reduce W factor	
			3. Key release function	Yes (in access PLC)	
			4. Key bank complete switches	Yes	4 or 5 need to be designed as a SIL 1 function
			5. Sliding door switches	Yes	4 or 5 need to be designed as a SIL 1 function
3	people enter the Hutch mistakenly via emergency entry mechanism	2	1. Training	No, given credit to reduce W factor	
			2. Visual Warning (Y/M light)	No, given credit to reduce W factor	
			3. Sliding door switches	Yes	SIL 2 for sliding door interlock
4	people enter the Hutch through rollup equipment door	2	1. Training	No, given credit to reduce W factor	
			2. Lock of the rollup door to ground	Yes	
			3. Rollup door magnetic switches	Yes	SIL 1

Figure 3: LOPA work table for LCLS photon PPS.

CONCLUSION

In this paper, the basic concepts of LOPA has been briefly introduced, three credited safety systems: ODH, PPS and BCS are used as examples to demonstrate how to apply this method to analyse the system with several typical configurations. LOPA promotes system level thinking rather than focusing on each individual subsystem. The analysis results provides a useful reference for safety system functional requirement development and process design improvement.

ACKNOWLEDGMENT

The authors would like to thanks for the helpful discussions with my colleagues at SLAC National Accelerator Laboratory, especially Radiation Physicists Shanjie Xiao, Johannes Bauer and Mechanical Engineer Phil Cutino.

REFERENCES

[1] Center for Chemical Process Safety, “Layer of Protection Analysis: Simplified Process Risk Assessment”, AIChE, New York, 2001.

[2] IEC 61511-3, “Functional Safety - Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels”, Ed. 2.0, International Electrotechnical Commission, 2015.

[3] Center for Chemical Process Safety, “Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis”, AIChE, New York, 2014.

[4] Center for Chemical Process Safety, “Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis”, AIChE, New York, 2015

[5] SLAC Environment, Safety, and Health Manual, Chapter 36, “Cryogenic and Oxygen Deficiency Hazard Safety”, 2015.

[6] Fermilab ES&H Manual, “FESHM 4240: Oxygen Deficiency Hazards (ODH)”, 2016.