

Session Fourteen: Layer of Protection Analysis and Common Mistakes

Paul Gruhn, P.E., ISA Fellow

Global Process Safety Consultant, ICS Triplex | Rockwell Automation

Abstract

Layer of protection analysis (LOPA) is a semi-quantitative method of determining/selecting the safety integrity level (SIL) of a safety instrumented function (SIF). The method avoids some of the pitfalls associated with older and simpler subjective, qualitative techniques. As a result, LOPA has become the preferred SIL selection technique with most organizations. A number of books and papers have been published describing the methodology. However, like any technique, the results it produces are only as good as the people using it. Judging from studies and discussions the author has been involved with, along with online discussions of people trying to utilize the method, there are a number of misunderstandings and potential misuses occurring. This paper will review the methodology along with some of the more common errors that seem to be occurring.

After all, would you rather learn from the mistakes of others, or make them all yourself? Hopefully this paper will assist you and your organization from making some of the more common mistakes when performing LOPA studies.

Introduction

LOPA was introduced in the 1993 AIChE CCPS (American Institute of Chemical Engineers Center for Chemical Process Safety) "Guidelines for Safe Automation" textbook (ref 1). A more complete textbook focusing on this specific subject was released by the CCPS in late 2001 (ref 2). LOPA is the preferred SIL selection technique with most organizations. LOPA overcomes many of the problems associated with older, simpler and more subjective qualitative techniques.

While entire books have been written on the subject, LOPA can be summarized with four bullet points, four tables and two graphics.

- How safe do you want to be (understanding that there is no such thing as zero risk)?
- How often does something fail or go wrong in your process?
- How many protection layers are there that could prevent the hazardous event from happening?
- How well do each of the protection layers perform?

How Safe Do You Want To Be?

While zero injuries may be a goal for many organizations, there is no such thing as zero risk. One is at risk merely sitting at home watching television. So how safe should a process plant be? Should the risk of working at a chemical plant be equal to that of staying at home, or driving in a car, or flying in an airplane, or skydiving? All things being equal, the safer a plant is, the more expensive it will be. There has to be an economic consideration at some point. Examples of risk criteria are shown in Table 1.

Determining tolerable levels of risk transcends engineering. Those interested in this topic can refer to reference 5.

Activity	Probability (per year)
Travel	
Air	2×10^{-6}
Train	2×10^{-6}
Bus	2×10^{-4}
Car	2×10^{-4}
Motorcycle	2×10^{-2}
Occupation	
Chemical Industry	5×10^{-5}
Shipping	9×10^{-4}
Coal Mining	2×10^{-4}
Voluntary	
The Pill	2×10^{-5}
Rock Climbing	1.4×10^{-4}
Smoking	5×10^{-3}
Involuntary	
Meteorite	6×10^{-11}
Falling Aircraft	2×10^{-8}
Firearms	2×10^{-6}
Cancer	1×10^{-6}
Fire	2.5×10^{-5}
Falls	2×10^{-5}
Staying at Home	1×10^{-4}

Table 1: Fatal Accident Probabilities (in the United Kingdom)

How Often Does Something Fail or Go Wrong in Your Process?

How often does a control loop fail, a pump spring a leak, or an operator make an error? Everything fails, it's just a matter of when. Multiple, independent safety layers are designed with the intent that if something fails, other layers will prevent the failure from escalating into a true hazardous event. Example of 'initiating event frequencies' are shown in Table 2.

Initiating Event	Frequency (per year)
Gasket / packing blowout	1×10^{-2}
Lightning strike	1×10^{-3}
BPCS loop failure	1×10^{-1}
Safety valve opens spuriously	1×10^{-2}
Regulator failure	1×10^{-1}
Procedure failure (per	1×10^{-3}
Operator failure (per	1×10^{-2}

Table 2: Sample initiating event frequencies

How Many Protection Layers Are There?

Figure 1 appears in a number of different formats in most safety documents and is referred to as the "onion diagram". It shows how there are various safety layers, some of which are prevention layers (the inner layers), others which are mitigation layers (the outer layers).

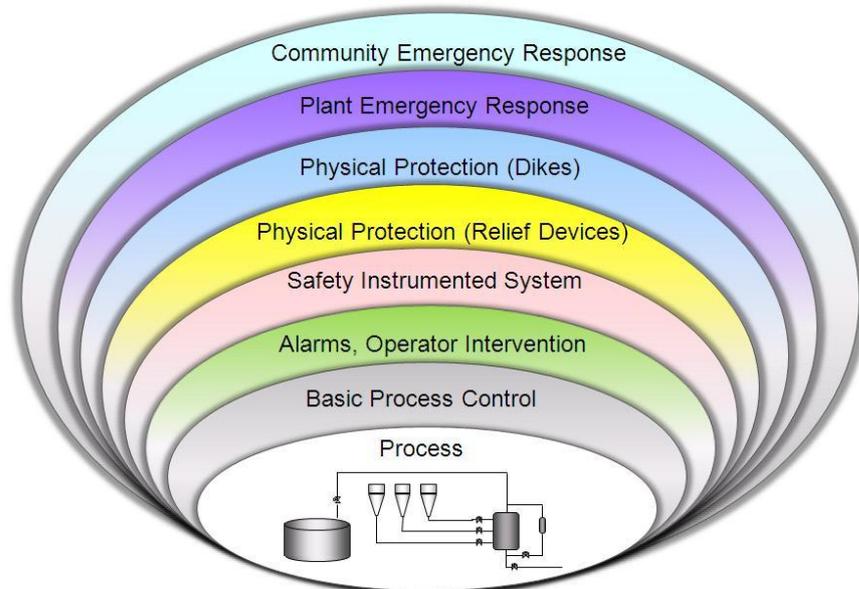


Figure 1: The Onion Diagram

Risk is a function of the probability (or frequency, or likelihood) of an event and its severity (or consequences). Multiple safety layers in any facility are designed to reduce one or the other (i.e., frequency or severity). Prevention layers are implemented to reduce the probability of a hazardous event from ever occurring. Mitigation layers are implemented to reduce the consequences once the event has already happened.

How Well do Each of the Protection Layers Perform?

It is first worth defining what an independent protection layer actually is.

- **A device, system, or action capable of preventing a scenario**

There are four rules or requirements for something to be considered an independent protection layer (IPL).

- 1) **Specificity:** An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event. Therefore, multiple event scenarios may initiate action of one IPL.
- 2) **Independence:** An IPL is independent of the other protection layers associated with the identified danger. The failure of one layer will not prevent another layer from working.
- 3) **Dependability:** It can be counted on to do what it was designed to do. Both random and systematic failures modes are addressed in the design.
- 4) **Auditability:** It is designed to facilitate regular validation of the protective functions. Proof testing and/or maintenance is necessary.

Table 3 is an example of the performance of various protection layers.

Passive Independent Protection Layers	Probability of Failure on Demand (PFD)	Risk Reduction Factor (I/PFD)
Dike	1×10^{-2}	100
Fireproofing	1×10^{-2}	100
Blast wall / bunker	1×10^{-3}	1,000
Flame / detonation arrestors	1×10^{-2}	100
Active Independent Protection		
Relief valve	1×10^{-2}	100
Rupture disk	1×10^{-2}	100
Basic Process Control System	1×10^{-1}	10

Table 3: Performance of Various Protection Layers

Let's combine these concepts with a simplified example and a graphic.

A company decides the level of risk in their facility should be roughly equal to that of driving a car (approximately 1 in 10,000 deaths per year). Assuming an individual is exposed to 10 hazardous scenarios, the target probability for each scenario would be 1 in 100,000 (1 E-5) per year. This represents the 'tolerable level of risk' toward the left hand side of Figure 2.

The initiating event for one particular hazard scenario might be 'human error' (e.g., closing the wrong valve, which results in no flow to a heater, which could result in tube overheating and failure, a fire, and a potential fatality). Let's assume an operator works 200 days per year and performs the action (closing a valve) every other day (100 times per year). Let's assume (as shown in Table 2) a procedural failure rate of 1 out of 1,000. This would mean the probability of an operator making an error (i.e., actually closing the wrong valve) would be 1 in 10 per year, assuming that such an error could escalate into a hazardous event. The 'initiating event frequency' shown on the right hand side of Figure 2 for this example would therefore be 1 in 10 per year.

Let's assume that the Basic Process Control System (BPCS) could detect the human error (e.g., closing the wrong valve, which results in low flow). We might credit the BPCS with a Risk Reduction of 10 (as shown in Table 3). This is the limit allowed by the ISA 84 (IEC 61511 standard. This now lowers our event frequency to 1 in 100 per year ($1/10 \times 1/10$). This does not meet our target of 1/100,000 per year. We need additional safety layers.

Let's assume an independent tube temperature alarm (as a result of low flow to the heater), that the indoor operator has enough time to respond, no other distractors, and an established procedure to follow. We might credit the operator with a Risk Reduction Factor of 10. This now lowers our event frequency now to 1 in 1,000 per year ($1/10 \times 1/10 \times 1/10$). This still does not meet our target of 1 in 100,000 per year, but we're getting closer.

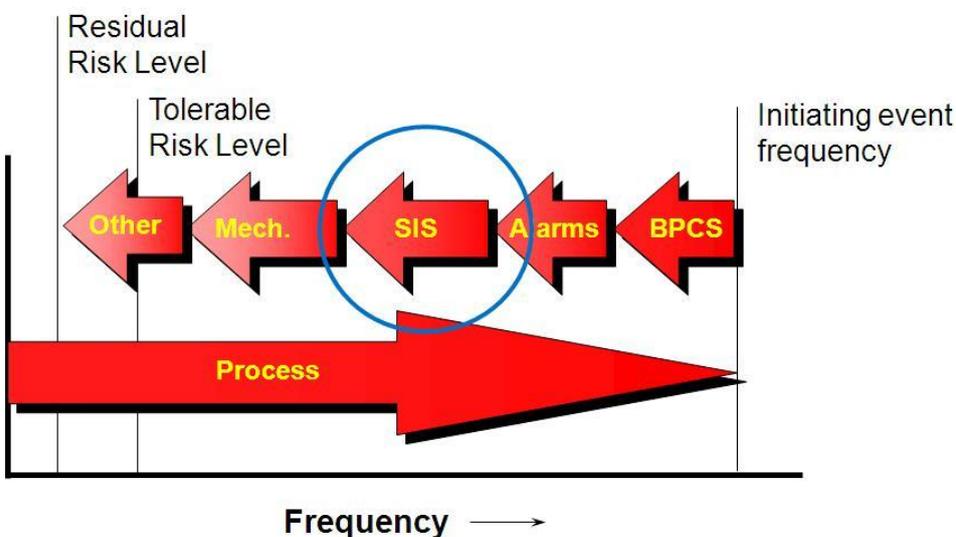


Figure 2: Risk Reduction of Multiple Layers

While Figure 2 shows ‘mechanical’ and ‘other’ protection layers, for this particular example there are no additional safety layers. Therefore the Safety Instrumented System (SIS) must provide all of the remaining risk reduction. The estimated event frequency of 1 in 1,000 per year must be reduced by a factor of 100 to reach the company target of 1 in 100,000 per year. A risk reduction factor of 100 equates to a SIL 2 system, as shown in Table 4.

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Safety Availability (1-PFD)	Risk Reduction Factor (1/PFD)
4	.0001 - .00001	99.99 - 99.999%	10,000 - 100,000
3	.001 - .0001	99.9 - 99.99%	1,000 - 10,000
2	.01 - .001	99 - 99.9%	100 - 1,000
1	.1 - .01	90 - 99%	10 - 100

Table 4: Performance Associated with Safety Integrity Levels

Common Mistakes in LOPA

The most common mistakes in LOPA involve violating the very definition and rules of what an independent protection layer is. What follows are the most common examples.

1) Considering Non-IPLs

Procedures are not IPLs

One company wished to consider ‘operating procedures’ as an IPL. This violates the definition of an IPL. Procedures are nothing more than written words on a piece of paper. How many procedures are you aware of in your own facility that are not actually followed? A procedure alone cannot prevent an accident. The intent here is really to consider operator action. There are cases where operator action is considered an IPL (covered below).

Maintenance is not an IPL

One company wished to consider maintenance as an IPL. This also violates the definition of an IPL. Maintenance by itself will not prevent an accident. Maintenance is expected on all equipment in order for it to work properly. When determining the probability of failure on demand of any protection layer, the maintenance test interval is part of the calculation.

Warning signs are not an IPL

A warning sign stating “This machine has no brain - use your own” is not an IPL. A sign by itself will not prevent an accident. How many warning signs and labels do you run across and ignore every day? Being inundated with warnings almost makes us immune to them.

2) Violating the Rule of Independence

The most common cases here are sharing sensors between the BPCS and SIS, sharing valves between both systems, or using the BPCS valve with a separate solenoid controlled by the SIS. If a shared device fails (and everything fails, it's just a matter of when), you will lose both systems. Accidents have resulted in all of the above cases (ref 6).

Another common 'independence' error is considering operator action twice. The operator responding to one alarm (e.g., pressure high) might be considered a protection layer under certain conditions (described in the next section). Considering an additional operator action for a second alarm (e.g., pressure high high) would be inappropriate. This violates the rule of independence; an operator is not 'independent' from himself. If the operator didn't respond to the first alarm, it's unlikely that he would respond to the second. No layer should be counted or given credit twice, often referred to as "double-dipping".

3) Inappropriate Operator Credit

Just because there may be an alarm, it does not automatically mean that a credit can be claimed for operator action. There are a number of rules that must be met in order to claim credit for operator action at all, such as:

- 1) The alarm must be capable of being monitored 24/7
- 2) The operator must have adequate time to respond (e.g., > 15 minutes)
- 3) There must be no other distractors (e.g., how many other alarms might be going off?)
- 4) The operator must be capable of taking actions under all conditions (e.g., you can't expect an operator to run through a fire, climb three flights of stairs, and manually close a 48 inch valve, all within 1 minute)
- 5) The operator must be adequately trained
- 6) There must be a written procedure (that *all* operators follow)
- 7) Audits must be performed to ensure the procedures *are* actually followed (as a procedure by itself is not a protection layer)

If all of the above rules can be met (which is rare), it is reasonable to claim up to a risk reduction factor of 10, no more. A risk reduction factor of 10 is the same as a probability of failure on demand of 10%, meaning that during an emergency an operator will do the correct thing 9 times out of 10. Do you *really* believe even *that* claim is reasonable?

There have been many cases where manually initiated safety functions have been assigned a SIL 2 target. Such a requirement borders on absurd. Does anyone believe that during an emergency an operator will perform the correct action 99 times out of 100? Studies in human reliability indicate that when someone is faced with a life threatening situation and must make a decision within one minute, the likelihood of making the wrong decision is 99%.

References

1. **Guidelines for Safe Automation of Chemical Processes**, American Institute of Chemical Engineers, Center for Chemical Process Safety, ISBN 0-8169-0554-1, 1993
2. **Layer of Protection Analysis**, AIChE CCPS, 2001, ISBN 0-8169-0811-7, www.aiche.org
3. **Safety Integrity Level Selection -- Systematic Methods Including Layer of Protection Analysis** by Edward M. Marszal, P.E. and Dr. Eric W. Scharpf, from ISA Press
4. **Reliability, Maintainability and Risk (Practical Methods for Engineers)** 7th Edition, David J. Smith, Butterworth-Heinemann, 2005, ISBN 0750666943
5. **Guidelines for Developing Quantitative Safety Risk Criteria**, AIChE CCPS, 2009, ISBN 0470261404
6. **Shared Field Instruments in SIS: Incidents Caused by Poor Design and Recommendations for Improvement**, Edward M. Marszal, "Texas A&M Instrumentation Symposium for the Process Industries" paper, 2012

Author Bio

Paul Gruhn is the Global Process Safety Consultant at ICS Triplex | Rockwell Automation in Houston, Texas. Paul is an ISA Fellow, a member of the ISA 84 standard committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, and the primary author of the ISA textbook on the subject. Paul developed the first commercial safety system modeling program over 17 years ago. He has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (P.E.) in Texas, and an ISA 84 Expert.