Opportunities for errors and omissions in the PHA to LOPA process for safety integrity level (SIL) determination

Jan C. A. Windhorst
WEC Inc
83 Dobler Avenue,
Red Deer, Alberta T4R 1X3
Canada
janwindh@telusplanet.net

Keywords: HazOp, LOPA, Safety Instrumented Systems, Safety Integrity Level, High Demand

Abstract

Current hazard identification processes often include some risk ranking tool for prioritizing and screening hazards, based on perceived risks. The process industry's PHA tool of choice towards the end of the engineering stage of a project, is a guideword-based Hazard and Operability (HazOp) review. Because of its inductive and incremental character, this approach can result in a failure to develop event chains to their ultimate consequence of interest.
The LOPA approach is often focused on defining, in a qualitative but numerical fashion, preventive or mitigative safety features that can lower the unmitigated event frequency and consequence of a particular scenario. The aforementioned safety features, also known as protection layers, need to have their aggregate reliability performance assessed by the application of redundancy rules to the reliability functions of the individual layers.
The $PFD_{avg} = 0.5\ \lambda T$ is found by integrating λt from t=0 to t=T and averaging over T.
Organizations often assign empirical PFD_{avg} values to protection layers in order to simplify their risk analyses. Another simplification occurs when a multi-tiered protection system has its aggregate PFD determined by multiplication of the PFD_{avg}s of the individual IPLs rather than through integration over time. This common LOPA approach violates the conditions under which simplifications were made, which can introduce significant errors. The paper discusses the necessity to ensure a HazOp takes a holistic approach and gives the results of a comparative system PFD analysis for several multi-layered protection systems; using LOPA's Boolean and two time-averaged integrated approaches, including a rigorous exponential integration.

1. Introduction

The process industry, also known as the chemical and oil refinery industry, puts a lot of effort in identifying hazard by means of deviation-based analysis tools. Foremost among these tools is the Hazard and Operability study, or HazOp, which has been around since the mid-seventies. Hazard identification is often only the first step in a company's risk

management program. A complete risk management program frequently will include LOPA, as the primary safety integrity determination tool; while more advanced risk analysis tools are not often used.

Safety integrity is the level of performance needed by a safety function to safeguard a process or part of a process [5]. If the safety function relies on electrical/ electronic/ programmable electronic components, also known as a SIS [6], then that function is called a Safety Instrumented Function or SIF. LOPA can be performed using a dedicated hazard-targeting analysis tool at the end of a process design. Unfortunately, many organizations prefer to forego this opportunity and wait until after the HazOp. Such an approach can be rationalized by the argument that only one formal hazard analysis, the HazOp, needs to be conducted. Potential LOPA scenarios would then subsequently be extracted from the HazOp report. This glosses over the shortcomings that are inherent to the HazOp process. The final LOPA report will therefore reflect the shortcomings of the LOPA process as well as the HazOp report's shortcomings.

2. HazOp Issues

During a HazOp study engineering drawings, specifically Piping and Instrument Diagrams (P&IDs) are subdivided into "nodes" that are to be subjected to deviation-based guidewords. It is not uncommon to have fifty or more nodes with many deviations per node. A deviation will or can be the starting point of a cause–effect chain that results in an ultimate effect that is of interest. Large number of HazOp entries can scatter identical ultimate effects throughout a HazOp report. This, in turn, makes it difficult to use that report for the purpose of defining a scope of work for LOPA. This is especially true when:

a) There are typos;
b) The wording for an ultimate effect has changed between nodes or even within the same node; e.g., explosion versus deflagration, detonation, pressure waves, etc.;
c) The effects were not always developed until the ultimate effect;
d) An ultimate effect is scattered over subscenarios;
e) Subscenarios are scattered over many nodes;
f) There are many standard-sized P&ID sheets and a single node can span several P&IDs. HazOp participants might need to flip back and forth between several P&IDs. In the past there were few but "monster-sized" P&IDs.

Where risk ranking is performed on identified cause-effect chains, extra difficulties can arise when:

a) The risk associated with several subscenarios stays below the Safety Integrity Level or SIL 1 (risk reduction factor required is ten or less) benchmark even though the aggregate can be well above the SIL 1 threshold [3].
b) Alternatively, it is possible that individual subscenarios score just above the SIL 1 threshold; causing an unnecessary increase of instrumentation and spurious trips.

Because a HazOp study's scope covers hazards as well as operability issues; it is possible that true hazard issues are being drowned out by operability issues. Finding the right LOPA candidates from among a multitude of HazOp cause-effect scenarios can be very burdensome. Furthermore, the LOPA results might not be of the desired quality then

besides the aforementioned HazOp and LOPA shortcomings the quality is also affected by the shortcomings of the LOPA scope selection process itself.

3. LOPA Issues

LOPA is a self-proclaimed simple semi-quantitative risk analysis method that, in order to avoid complexity, focuses on single "initiating event - loss event" relationships [1]. In case the scope was created by selecting "higher risk" HazOp cause–effect scenarios; the causes are usually the initiating events. Most LOPAs exercises use default value tables for initiating event frequencies and safeguards, also known as (Independent) Protection Layers (IPLs). Most LOPA books (e.g., [1]) have some default LOPA tables in them. Where these tables are used without considering their applicability, the final LOPA results will, at best, represent some qualitative analysis expressed in a numerical fashion.

The LOPA goal is to analyze selected single "initiating event-loss event" scenarios and assess whether the risk posed by each scenario has been reduced to a residual value that is deemed acceptable. In case of a new design, the achieved risk reduction is determined by assessing the performance of the defined IPLs. For an existing facility the IPL-assessment is conducted on installed IPLs. If after the IPL(s) assessment, the residual risk value is still too high, additional risk reduction measures need to be taken.
Relying on HazOp studies for scope definition means that the LOPA will occur at a rather late stage where a detailed design is close to being frozen or is frozen. Under those circumstances there will be a reluctance to redo part of the design and the preferred way of achieving risk reduction will by adding Safety Instrumented Functions (or SIFs), with an appropriate measure of safety integrity; i.e., more instrumentation.

3.1 Mutually exclusive events

Where several mutually exclusive initiating events result in the same ultimate consequence or loss event, LOPA's single "initiating event - loss event" strategy will result in an under-estimation of loss event likelihoods. Examples of such mutually exclusive events are parallel heat exchanger operations, pressure swing adsorption systems, etc. In such cases it is necessary to determine and apply an appropriate correction to initiating event frequencies. Failure to do so can, besides the aforementioned likelihood underestimation, result in a high demand operation being treated as a low demand situation.

3.2 High and low demand scenarios

IEC 61508-4 (2010) [7] defines a high demand mode as a condition where the frequency of demands is greater than one per year while a low demand condition has a frequency of no greater than once a year.
It is necessary to establish which mode is being considered, high or low, then low demand situations have a PFD_{avg}-based approach while high demand/continuous mode situations use a (λ_D) dangerous failure rate-based approach [2]. An example of a high

demand mode operation would be daily draining of spent lube oil from reciprocal hydrogen compressor coalescers (at high pressure) to a receiver vessel (at low pressure).

3.3 Parallel redundancy of IPLs

Parallel redundancy characterizes a situation where multi-tiered IPLs exist that each, individually, can prevent an initiating event from evolving into an undesired consequence. In essence all preventive IPLs must fail before the consequence can materialize. Ignoring Common Cause Failures (CCFs) and assuming an IPL that operates in a constant failure rate domain ($\lambda \neq \lambda(t)$), the *PFD*(t) of a single IPL is given by equation (1) [8]:

$$PFD^{IPL}(t) = (1 - e^{-\lambda t}) \quad (1)$$

The term $e^{-\lambda t}$ in (1) represents the reliability. It can be readily expanded without a major error as long as λt is sufficiently small; e.g., < 0.1. In such a case it is common to take the first two expansion terms; i.e., $(1 - \lambda t)$, which yields:

$$PFD^{IPL}(t) = \lambda t \quad (2)$$

An average IPL PFD for a time interval *T* can be calculated for (2) by integration from t=0 to t=*T* and division by *T*:

$$PFD_{avg}^{IPL} = \frac{1}{T}\int_{t=0}^{t=T} \lambda t \, dt = \frac{1}{2}\lambda T \quad (3)$$

Assuming absence of common cause failures, the aggregate or system PFD of a system consisting of a number of IPLs is defined by:

$$PFD^{System}(t) = \prod_{i=1}^{n} PFD^{IPLi}(t) \quad (4)$$

For a system protected by three parallel redundant IPLs, the system *PFD*(t) can be written, at any given time, as:

$$PFD_{1oo3}(t) = PFD^{IPL1}(t) \times PFD^{IPL2}(t) \times PFD^{IPL3}(t) \quad (5)$$

When assuming identical and constant failure rates the PFD_{1oo3}(t) can be rewritten as:

$$PFD_{1oo3}(t) = 1 - 3e^{-\lambda t} + 3e^{-2\lambda t} - e^{-3\lambda t} \quad (6)$$

$PFD_{1oo3}(t)$ in (Eq. 6) shows; however, that the system's aggregate failure rate will not be constant. Therefore time-averaged system *PFDs*, for systems with parallel redundancy, should be determined through proper integration and time averaging, as required by IEC [6].

LOPA ignores these requirements and calculates an aggregate system PFD_{avg} by merely multiplying the PFD_{avg} of the individual IPLs. This Boolean approach is not correct and

can result in a gross under-estimation of risk for a multi-tiered IPL system. Appropriate correction factors need to be applied in accordance with Table 1; e.g., the PFD_{avg} of a double-tiered IPL system would need to be multiplied with (4/3) [3]. Table 1 presents PFD_{avg} equations for systems that were determined by (i) rigorous calculations; i.e., without the series expansion, (ii) the IEC time-averaged integration approach and (iii) the LOPA Boolean approach.

Consideration of common cause failures (CCFs) can cause further PFD_{avg} increases. According to Sintef [9]; given a failure of two similar redundant components, the likelihood of having a simultaneous failure of a third added component will be 0.5.

Table 1. PFD_{avg} equations, without CCFs, determined by time-averaged integration of (i) exponential equations; (ii) expanded equations (IEC); and (iii) LOPA's Boolean approach.

Setup: 1oox	(i) PFD_{avg} determined by rigorous integration of exponential equations [3]	(ii) PFD_{avg} as per IEC: $\frac{1}{T}\int_0^T (\lambda T)^x dt$	(iii) PFD_{avg} Boolean: $\left(\frac{1}{2}\lambda T\right)^x$
1oo1	$\frac{1}{T}\int_0^T \left(1-e^{-\lambda t}\right)^1 dt = \frac{1}{T}\left\{\left(\frac{e^{-\lambda t}}{\lambda}+t\right)\Big\vert_0^T\right\}$	(1/2) λT	(1/2) λT
1oo2	$\frac{1}{T}\int_0^T \left(1-e^{-\lambda t}\right)^2 dt = \frac{1}{T}\left\{\left(\frac{e^{-2\lambda t}\left(4e^{\lambda t}-1\right)}{2\lambda}+t\right)\Big\vert_0^T\right\}$	(1/3) $(\lambda T)^2$	(1/4) $(\lambda T)^2$
1oo3	$\frac{1}{T}\int_0^T \left(1-e^{-\lambda t}\right)^3 dt =$ $\frac{1}{T}\times\left\{\frac{6\lambda t+2e^{-3\lambda t}-9e^{-2\lambda t}+18e^{-\lambda t}}{6\lambda}\Big\vert_0^T\right\}$	(1/4) $(\lambda T)^3$	(1/8) $(\lambda T)^3$

Graphic representations of PFD_{avg} of approaches (i), (ii), and (iii) for a time-averaged integration from 0 to 10 years are shown in Figure 1.

3.4 Maximum credit for a control system in LOPA (rounded off and using an annual rather than the hourly IEC basis)

The IEC's normative SIS standards [10] state that a BPCS shall be considered to be a SIS, subject to the requirements of a SIS, if an average Dangerous Failure rate per Year (DFA) [8] of less than 0.1 is claimed for a single BPCS function. IEC 61508 [11] goes on with stating that the BPCS is regarded as a SIS with SIL 1, if a $10^{-2} \leq \text{DFA} < 10^{-1}$ is claimed. The quoted values here are all point values, indicating a strict domain rule. However, the on demand SIL table [10] defines a SIL 1 as $10^{-2} \leq PFD_{avg} < 10^{-1}$ and because this is the lowest SIL number; protection layers with $10^{-1} \leq PFD_{avg} < 1$ are not safety related or have no special safety requirements [12]. The standards [10, 12] infer that combinations of control functions could claim an aggregate of DFA = 10^{-2} year^{-1}; as long as the functions are independent and separate.

These separation requirements apply also to the CPUs; a condition that is supported by recent Sintef CPU reliability data: $\lambda_D = 4.8 \times 10^{-6}$ per hour - in a programmable safety system [13]. Sintef's data contradict an opinion expressed in the original LOPA book [1]. The latter claimed that historical data from a number of companies suggest that the effective PFD performance of a BPCS logic solver could justify taking credit for two BPCS-based IPLs. This liberal approach is obviously not supported by reputable data.

It is therefore proposed to limit the dangerous failure rate of a single BPCS function to $\lambda_D = 1 \times 10^{-1}$ per year and to allow one extra credit of $PFD_{avg} = 0.1$ to be taken for an independent and separate control supervisory system. This would exhaust all BPCS credits at a DFA = 10^{-2} year^{-1}, additional instrumented safety systems would have a SIL rating of at least "1" one.

4. IEC and SIL Design Target Issues

The generic Hazard and Risk Analysis (H&RA), prescribed in the IEC standards, can be done quantitatively or qualitatively. Its results are a list of overall safety functions and safety integrity requirements that are to be allocated among different technologies. Allocation of an overall safety function with its integrity requirement, or part thereof, towards an instrumented solution creates one or more SIFs, each with its associated Safety Integrity Level (SIL). Most SIL analyses are done qualitatively, even if they claim to be semi-quantitative, using LOPA, SIL graphs and hybrids of these methodologies.

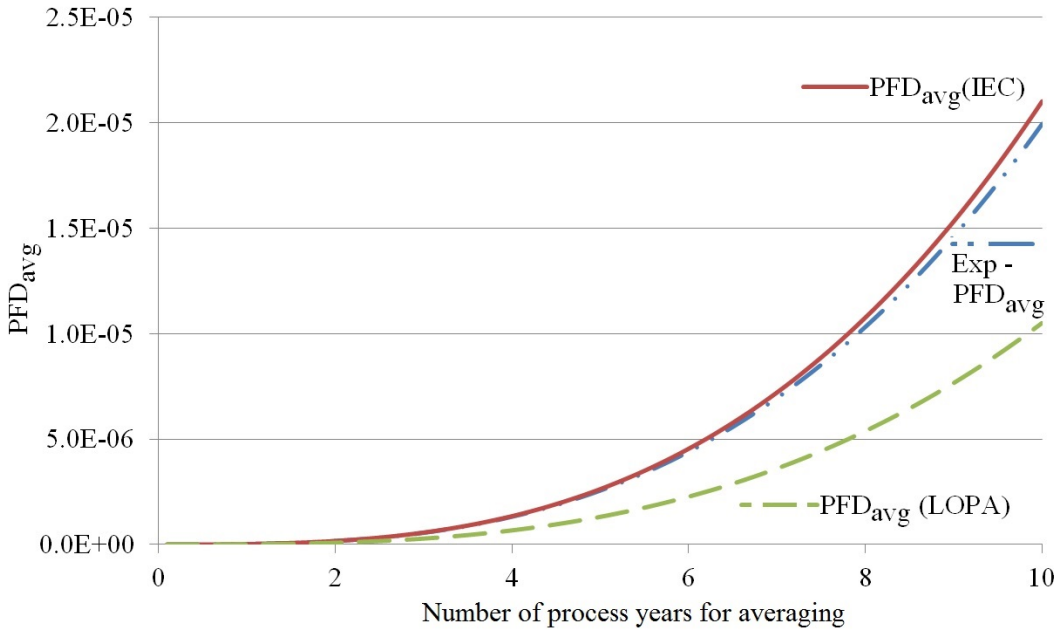

Figure 1: Multi-year PFD_{avg} curves, as determined by Exponential, IEC and Boolean determination methods, for a 1oo3 parallel redundant system ($\lambda_D = 5 \times 10^{-7}$ failures/hr).

4.1 SIL selection

While most practitioners involved with "SIL analysis" are clear about the purpose of a SIF; e.g., protection against overpressure, this is not necessarily true for SILs. The SIL selection serves two purposes:

1. it invokes a bundle of systematic support measures for the life cycle (and systematic integrity). This includes measures for fault avoidance and fault control; and
2. with respect to hardware safety integrity it calls for quantified reliability estimation techniques. This is needed in order to assess whether the target safety integrity, as determined by the risk assessment, has been achieved [14]. If a qualitative method was used that expresses the safety integrity requirement as a SIL number then the smallest average PFD_{avg} or failure rate for that SIL number shall be used as the SIS design target failure measure [15].

Table-2 gives a real-life example of a qualitative SIL analysis that resulted in an erroneous specification for the SIS design.

Table 2. Example of flawed "Required PFD_{avg}" statements in a SIF architecture table.

SIF Tag #	SIL target, determined by SIL-Graph PFD_{avg}	SIS designer specified "Required PFD_{avg}" (flawed)	True PFD_{avg} Target is	Acceptance PFD_{avg}	SIS designer Achieved PFD_{avg}
1	2	1×10^{-2}	1×10^{-3}	1.5×10^{-3}	3×10^{-3} [Fail]
2	1	1×10^{-1}	1×10^{-2}	1.5×10^{-2}	6×10^{-3} [OK]
3	2	1×10^{-2}	1×10^{-3}	1.5×10^{-3}	3×10^{-3} [Fail]

5. Discussion

Using HazOp, which is typically conducted towards the end of a project, as a hazard identification tool for LOPA purposes seems counter-productive. It delays the implementation of an overall process control safety strategy until after the HazOp. Unless standard SIFs were included, as part of a facility's design, there will be no concrete SIF/SIL information available to a HazOp team performing a PHA towards the end of the detailed design. This can result in a lot of time and effort being spent on a design by committee. In addition, the number of HazOp recommendations will proliferate, making their management cumbersome.

It would be more productive to conduct a separate process hazard analysis at the end of the process design stage that would generate SIF design input for P&IDs based on equipment information. An obvious hazard identification tool would be the Failure Mode Effect and Criticality Analysis or FMECA, which has an equipment focus, and is also a tool of choice to develop reliability data bases. Failure modes and failure rate data from

such data bases would then allow required integrity requirements to be quantified and expressed as a discrete numbers rather than a range, associated with a particular SIL.

The first two LOPA books [1, 16] claimed that LOPA results would be accurate to within an order of magnitude of a cause-effect scenario's true risk. However, because a LOPA study most commonly employs ten-fold differences for the frequency (or probability) as well as the consequence estimates there is leeway for teams to "play" with numbers. The aforementioned issues with hazard identification and PFD_{avg} handling indicate that the spread in results can be much greater than one order of magnitude.
Because of the uncertainty, it is considered prudent to risk-verify all LOPA analyses that yielded SIFs with a SIL 3 or higher; ideally this should be extended to scenarios with low probability and severe safety consequences.

Because qualitative SIL analyses set SIS design targets at the lowest PFD_{avg}, a SIL with number "*n*" (*n* = 1, 2, 3, 4) will require "*n*+1" protection layers (assuming a PFD_{avg} = 0.1). A SIL "a" or "0" requires therefore a single IPL with a PFD_{avg} = 0.1. This can be handled by a BPCS "supervisory" layer as long as it is independent and separate from BPCS parts that would have caused the failure and the maximum aggregate BPCS credit is not less than 10^{-2} DFA. If this is not possible then the SIF with a SIL "a" or "0" should be located in a SIS and be subject to the same restrictions as SIFs with SIL 1 and higher. These restrictions include maintenance by SIS qualified technicians only.

6. Conclusions

1. The actual risk reduction performance of multi-tiered safeguards' will fall short of what LOPA suggests, when using Boolean algebra. System PFD_{avg}s should therefore be corrected; e.g.,:
    a. One IPL; correction factor is 1.
    b. Two IPLs correction factor is 1.33.
    c. Three IPLs correction factor is 2.
2. Qualitative and "semi-quantitative" hazard analyses that rely on a "single initiating event - loss event relationships" can be subject to serious shortcomings when the analysis team does not account for mutually exclusive events leading to the same loss event.
3. Expressing a SIF's desired risk reduction in terms of a SIL number; i.e., a range, rather than an actual target value is makes risk management more difficult. It creates confusion and provides opportunities for errors in the design and risk analysis.
4. Because of the uncertainty in the SIL or LOPA analyses, it is considered prudent to risk-verify all LOPA analyses that yielded SIFs with a SIL 3 or higher; ideally this should be extended to scenarios with low probability and severe safety consequences

5. Considering the effort that goes into the verification of SIS designs; it would be good if the risk verification effort matched the design verification effort

7. References

[1] Layer of Protection Analysis: Simplified Process Risk Assessment; published by the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), 3 Park Avenue New York, New York 10016-5991 (2001).

[2] Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis (2015). Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

[3] Windhorst, Jan C A, Rigorous versus Simplified Protection Layer Reliability Calculations and Problems with Popular Risk Analysis Methodologies. Procedia Engineering 84, pp 47-54.

[4] IEC 61508-6 Ed. 2.0 (2010). Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010) – Clause B.2.2 pp 23.

[5] IEC 61508 Ed. 2.0 (2010) - Functional safety of electrical/electronic/programmable electronic safety-related systems: Parts 1 through 7. Published by the International Electrotechnical Commission (IEC): 3, rue de Varembé, P.O. Box 131, CH - 1211 Geneva 20 – Switzerland.

[6] IEC 61511 Functional safety instrumented systems for the process industry sector: Part 1: General framework, definitions system software and hardware requirements (2003-1); Part 2: Guidelines in the application of Part 1 (2003-7); Part 3: Guidelines in the application of hazard and risk analysis (2003-3). Published by the International Electrotechnical Commission (IEC): 3, rue de Varembé, P.O. Box 131, CH - 1211 Geneva 20 – Switzerland.

[7] IEC 61508-4 Ed. 2.0 (2010) Definitions and abbreviations – clause 3.5.16. Published by the International Electrotechnical Commission (IEC): 3, rue de Varembé, P.O. Box 131, CH - 1211 Geneva 20 – Switzerland.

[8] Smith, David J., "Reliability maintainability and risk". 8th edition, Published by Elsevier Ltd (2011) ISBN 978-0-08-096902-2.

[9] SINTEF: Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook (2010).

[10] IEC 61508-1: General requirements (2010) and IEC 61511-1: General framework, definitions system software and hardware requirements (2003-1). Published by the International Electrotechnical Commission (IEC): 3, rue de Varembé, P.O. Box 131, CH - 1211 Geneva 20 – Switzerland.

[11] IEC 61508-1: General requirements (2010) –NOTE to Clause 7.5.2.5.

[12] IEC 61508-5: Examples of methods for the determination of safety integrity levels (2010).

[13] SINTEF: Reliability Data for Safety Instrumented Systems - PDS Data Handbook (2010); section 5.2.2.2.

[14] IEC 61508-1: General requirements (2010) – NOTE4 to Clause 7.6.2.9.

[15] IEC 61508-1: General requirements (2010) – NOTE1 to Clause 7.10.2.7.

[16] Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis (2014). Published by John Wiley & Sons, Inc., Hoboken, New Jersey.