# LOPA for Required SIL Determination: adequate method application

Bleser, Cristina Simão; Pires, Marcela Mayo; Alvarenga, Tobias Vieira.
Det Norske Veritas Ltda., Brazil

## ABSTRACT

Layer of Protection Analysis (LOPA) is a widely known technique for semi-quantitative risk analysis. LOPA method is frequently utilized for a Safety Integrity Level (SIL) determination, since the amount of required risk reduction can be correlated to frequency reduction, and then with a SIL target - which is a measurement of performance required for the Probability of Failure on Demand (PFD) of a Safety Instrumented Function (SIF). This paper aims to discuss the hazardous events selection for Required SIL via LOPA evaluation, once a proper calculation of the frequency of a SIF demand is essential for adequate mitigation of the likelihood of an accidental scenario to acceptable levels or As Low As Reasonably Practicable (ALARP).

## 1. INTRODUCTION

Safety Integrity Level (SIL), as defined in IEC 61511 [1], is a safety performance measure for Safety Instrumented Functions (SIF). The standard IEC 61511-3 [1] suggests several methods for SIL determination, ranging from fully quantitative methods to fully qualitative methods. One widely used method in the Oil & Gas Industry for SIL determination is Layer of Protection Analysis (LOPA).

LOPA is a simplified semi-quantitative risk analysis that focuses on the evaluation of each scenario separately, taking into consideration the available Independent Protection Layers (IPLs) for single cause-consequence pair [2, 3]. If additional risk reduction is required and if it is to be provided in the form of a SIF, LOPA allows the determination of its appropriate SIL.

## 2. OBJECTIVES

This paper aims to discuss potential pitfalls when determining Required SIL via LOPA. It focuses on how outputs can vary when different triggering conditions (unwanted events) that demand SIF to actuate are assessed (when evaluating needs for minimum SIL). Thus, two SIF demanding conditions are evaluated: one where an undesired event demands one specific SIF (called "per scenario" condition); and one where multiple unwanted events demand the same specific SIF (called "cumulative" condition). For each condition a special attention is given to each “cause-consequence” pair. Then, results of these two different SIF demand conditions are compared and a rational of each consideration is presented.

## 3. METHODOLOGY

LOPA method is typically based on data developed during a qualitative hazard evaluation such as HAZard and OPerability (HAZOP) study, as described next.

### 3.1 HAZard and OPerability Study

As defined in IEC-61882 [4], a HAZOP study is a detailed Hazard and Operability problem identification process, performed by a team with the relevant technical and operating skills and experience. The basis of HAZOP is a "guide word examination" which is a systematic and structured search for deviations from the design intent, examination of their possible causes and assessment of their consequences, as well as identification of protection, detection and indication mechanisms for the deviation. HAZOP is particularly useful for identifying the weaknesses in a system, which may lead to suggestions of possible remedial/mitigating measures to improve safety and operability.

### 3.2 Layer of Protection Analysis

The hazard scenarios, when extracted from HAZOP, may have one or more initiating events (causes). LOPA focuses on each cause-consequence pair at a time [2, 3]. As described by TORRES-ECHEVERRIA [2] and CCPS (2001) [3], LOPA method consists on identifying (semi-quantitatively) the estimated likelihood and (qualitatively) the severity level of an initiating event, and calculating the modified likelihood of the hazardous event reduced by the probability of failure of applicable existing Independent Protection Layers (IPL). The Probability of Failure on Demand (PFD) gives the probability that the given IPL cannot prevent against the scenario and an unwanted consequence is reached that harms environment, personnel and/or business. To be considered as IPL, safeguards need to satisfy some characteristics, such as independence, specificity, dependability and auditability [1].

The resultant event likelihood is then compared against corporate criteria for tolerable risk to determine if additional risk reduction measure is needed. When risk reduction measure is necessary, it means that actions need to take place in order to the scenario meets the tolerable risk for a specific hazardous event [1]. Then, from a frequency driven scenario, additional IPLs must be considered to the design. If at this stage a SIF is required, it brings along the Risk Reduction Factor (RRF) needs, consequently it is associated to a SIL value (for this specific function) [6].

### 3.3 SIL determination using LOPA

The required Safety Integrity Level of a Safety Instrumented Function shall be derived by taking into account the required risk reduction that is to be provided by that function. The RRF is the inverse of Probability Failure on Demand (PFD), which is the reliability indicator of a SIF given by the average probability, in a given time interval, of such SIF to fail when demanded. The PFD of the SIF shall be equal to, or less than, the target failure measure as specified in corporate criteria. For each demand mode Safety Instrumented Function, the required SIL shall be specified in accordance with Table 1[1].

Table 1 - Relation between SIL, PFD and RRF (Source: IEC-61511 [1])

| LOW DEMAND MODE OF OPERATION | | |
|---|---|---|
| Safety Integrity Level (SIL) | Target Average Probability of Failure on Demand (PFD) | Target Risk Reduction (RRF) |
| 1 | $10^{-2}$> to <$10^{-1}$ | 10 to 100 |
| 2 | $10^{-3}$> to <$10^{-2}$ | 100 to 1,000 |
| 3 | $10^{-4}$> to <$10^{-3}$ | 1,000 to 10,000 |
| 4 | $10^{-5}$> to <$10^{-4}$ | 10,000 to 100,000 |

Risk is a measure of the frequency and consequence of a specified hazardous event occurring. The tolerable risk involves consideration of societal and political factors, among others. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the SIS can be allocated. Safety integrity is a measure of the likelihood that the SIF and other protection layers will achieve the specified safety functions. The total risk reduction provided by the Safety Instrumented Function(s) together with any other protection layers has to be such as to ensure that the failure frequency of the safety functions is sufficiently low to prevent the hazardous event frequency from exceeding that required to meet the tolerable risk and/or the Safety Functions modify the consequences of failure to the extent required to meet the tolerable risk [1].

Classic LOPA approach takes into consideration only one scenario at a time. However a hazard may contain several scenarios with the same consequence and same protection layer (same SIF for example). When the main objective of the evaluation is determining the required SIL for a SIF, two different approaches are observed: evaluation based on a "cumulative" or "per scenario" risk calculation condition [6].

In terms of calculations, if "per scenario" method is used, the overall target Risk Reduction Factor for a hazardous scenario is the maximum RRF calculated for each cause-consequence pair. In the case of applying “cumulative” method, the overall RRF calculated for a hazardous scenario is the sum of all RRF calculated for each cause-consequence pair [7]. This is shown in equations below, assuming two cause-consequence pairs that lead to the same hazardous scenario, as presented by BARADITS et al. [7]:

$$\mathrm{RRF}_1^{\mathrm{targ}} = \frac{\mathrm{F1}}{\mathrm{Ftol}} \tag{1}$$

$$\mathrm{RRF}_2^{\mathrm{targ}} = \frac{\mathrm{F2}}{\mathrm{Ftol}} \tag{2}$$

$$\mathrm{RRF}_{\text{per scenario}} = \max(\mathrm{RRF}_1^{\mathrm{targ}}, \mathrm{RRF}_2^{\mathrm{targ}}) \tag{3}$$

$$RRF_{cumulative} = \mathrm{RRF}_1^{\mathrm{targ}} + \mathrm{RRF}_2^{\mathrm{targ}} \tag{4}$$

The influence and implications of applying each method is discussed through a case study.

## 4. CASE STUDY- TANK OVERFLOW

The case study is based on a recurring accident, overfilling vessels. According to Institution of Chemical Engineers [8], 10 fatal accidents of tank overfill and ignition happened between 1970 and 2010, as shown in Figure 1.

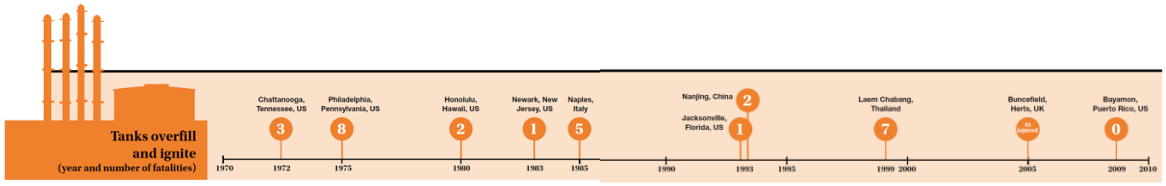


Figure 1 – Historical cases of tanks overfill and ignite (Source: Institution of Chemical Engineers [8])

Figure 2 presents the process schematic for the case study scenario (tank overflow).

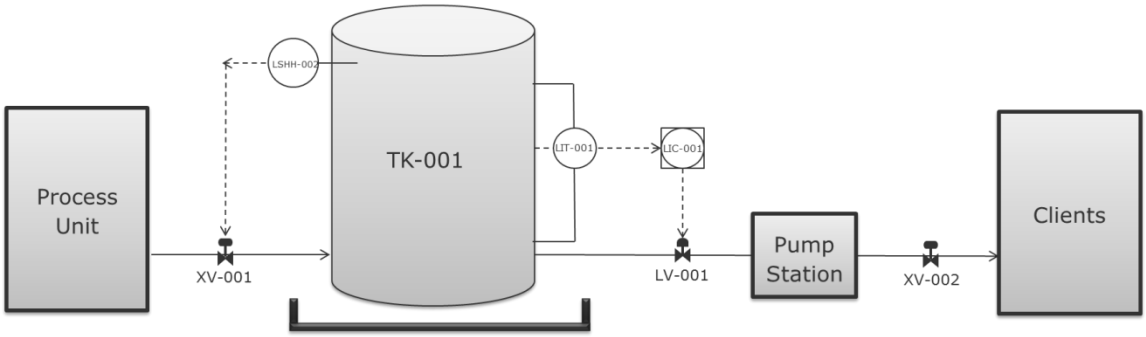


Figure 2- Case Study: Process Schematic

The process schematic represents the storage system to export oil produced in a process unit. The case study system is designed with a control loop with alarm to control the tank (TK-001) level, a high high level switch closing the valve XV-001 and one outlet motor valve (XV-002) to isolate the system in case of emergency.

A HAZOP analysis is structured to identify hazard scenarios for tank overfilling. Figure 3 presents a HAZOP spreadsheet for high level in TK-001 evaluation, which is adapted from IEC-61882 [4]. The causes and consequences are based on Loss Prevention Bulletin [8].The added columns, highlighted in blue, represent the risk classification for safety (S). The qualitative risk criteria are based on ISO/TR14121-2 [9] and the consequence category (Catastrophic) is assuming no safeguards.

| No. | Guide word | Element | Deviation | Possible causes | Consequences | Type | Risk | | | Safeguards | Actions required |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | F | C | R | | |
| 1 | HIGH | Tank TK-001 Level | High Level | - Control Loop failure (LIT-001/ LV-001)<br><br>- Operational error (flow path alignment, failed to gauge and monitor the tank according to procedures)<br><br>- Motor Valve failure (XV-002) leading to blocked outlet. | Possible Overflow leading to:<br>- people injury/fatality due to possibility of fire and explosion<br>-soil contamination<br>- severe damages to assets | S | Likely | Catastrophic | High | - Alarm (LAH-001)<br>- SIF: LSHH-002 closing the XV-001<br>- Dike | R1) Verify the Required SIL for SIF: High high level (LSHH-002) on Tank TK-001, closing the XV-001 to avoid overflow of tank leading to possible fire, injuries / fatality and soil contamination. |

Figure 3- HAZOP Spreadsheet (Source: IEC-61882 adapted [4])

For catastrophic HAZOP scenarios, a SIL via LOPA assessment is then performed for SIF: High High level on TK-001 closing XV-001. This analysis is carried out based on information from HAZOP (deviation, causes that may demand SIF actuation, consequence, qualitative evaluation of consequence and safeguards).

Figure 4 and Figure 5 presents SIL via LOPA assessment for the tank overflow hazardous scenario. LOPA spreadsheet assumed for this case study is adapted from IEC 61508 – part 5 [10]. The added columns represent the requirements of each cause-consequence pair in terms of PFD and RRF, when risk reduction is necessary (PFD =1/RRF). This is the $RRF_i^{targ}$ (i=number of cause-consequence pair under evaluation). The total requirements hazardous scenario column represents the Risk Reduction Factor ($RRF_{per\ scenario}$ or $RRF_{cumulative}$) for reducing the hazardous scenario likelihood.

This paper limits this analysis to personal injuries. The frequency of initial events and the PFD of IPL are based on CCPS [3, 11]. The presence of people in the affected area is estimated as time exposed to risk/total time. In this analysis it is considered that local operational maneuver (maintenance activity

performed by the staff in the storage system under evaluation) is about 1 hour every 2 days (column: "additional mitigation, restricted access"). The probability of ignition is based on IP Research report [12] (column: "additional mitigation"). The tolerable frequency for the scenario is based on CCPS – Appendix E [3], related to qualitative evaluation of severity.

For the tank overflow hazardous scenario, "per scenario" method is shown in Figure 4 and "cumulative" method is presented in Figure 5 (as defined in Chapter 3.3). The main differences in both spreadsheets are related to "total requirements for hazardous scenario" column (PFD and RRF calculations) and final "recommendations/comments":

| Impact Event Description | Severity Level | Initiating cause | Initiation Likehood (event/year) | Protection Layers (PLs) | | | | | Intermediate Event Likelihood (event/year) | Requirements | | Tolerable Mitigated event likelihood (event/year) | Total Requirements Hazardous Scenario | | Recommendations/ Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | General design | Control System | Alarms etc. | Additional mitigation, restricted access | Additional mitigation | | PFD | RRF | | PFDavg required for E/E/PES (and SIL) | RRF | |
| Overflow with possible fire | impact to people leading to injury and possible fatality | Control Loop failure (LIT-001/ LV-001) | 0.10 | - | - | - | 0.02 | 0.03 | 6.30E-05 | 0.16 | 6.30 | 1.00E-05 | 0.16 | 6.30 | NOTE: PFD is greater than 0.1. For the SIF "High high level (LSHH-002) on Tank TK-001, closing the XV-001." is allocated the classification "No special safety integrity requirements". |
| | | Operational error (failed to gauge and monitor the tank according to procedures) | 1 | - | - | 0.10 | 0.02 | 0.03 | 6.30E-05 | 0.16 | 6.30 | | | | |
| | | Motor Valve failure (XV-002) leading to blocked outlet. | 0.10 | - | - | 0.10 | 0.02 | 0.03 | 6.30E-06 | 1.59 | 0.63 | | | | |

Figure 4- SIL via LOPA Spreadsheet for Personnel – "per scenario" method (Source: IEC-61508 adapted [10])

| Impact Event Description | Severity Level | Initiating cause | Initiation Likehood (event/year) | Protection Layers (PLs) | | | | | Intermediate Event Likelihood (event/year) | Requirements | | Tolerable Mitigated event likelihood (event/year) | Total Requirements Hazardous Scenario | | Recommendations/ Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | General design | Control System | Alarms etc. | Additional mitigation, restricted access | Additional mitigation | | PFD | RRF | | PFDavg required for E/E/PES (and SIL) | RRF | |
| Overflow with possible fire | impact to people leading to injury and possible fatality | Control Loop failure (LIT-001/ LV-001) | 0.10 | - | - | - | 0.02 | 0.03 | 6.30E-05 | 0.16 | 6.30 | 1.00E-05 | 0.08 | 13.23 | 1) Implement required SIL 1 (PFD=7.56E-2) for the SIF "High high level (LSHH-002) on Tank TK-001, closing the XV-001." |
| | | Operational error (failed to gauge and monitor the tank according to procedures) | 1.00 | - | - | 0.10 | 0.02 | 0.03 | 6.30E-05 | 0.16 | 6.30 | | | | |
| | | Motor Valve failure (XV-002) leading to blocked outlet. | 0.10 | - | - | 0.10 | 0.02 | 0.03 | 6.30E-06 | 1.59 | 0.63 | | | | |

Figure 5- SIL via LOPA Spreadsheet for Personnel – "cumulative" method (Source: IEC-61508 adapted [10])

## 5. RESULTS

According to LOPA spreadsheet, if the "per scenario" method is used, the maximum RRF is 6.3 and no additional Safety Integrity Level is required for the related Safety Instrumented Function (SIF). On the other hand, when analyzing the scenario according to the "cumulative method", the total RRF is 13.23 and a SIL 1 is required for the SIF (High High level on TK-001 closing the XV-001).

These results differ basically because, when assuming "per scenario" condition, causes that trigger the same consequence are treated unconnectedly; potentially leading to a perception that the frequency of this specific consequence is lower than what is indeed practiced (once what is practiced is the sum of all possible triggers under the same risk scenario/ design intent/ deviation).

## 6. CONCLUSIONS

According to IEC-61511-3 [1], the demand rate is defined as "*the number of times per year that the hazardous event would occur in the absence of the Safety Instrumented Function under consideration. This can be determined by considering all failures which can lead to the hazardous event and estimating the overall rate of occurrence. Other protection layers should be included in the consideration".*

A SIF may exist in several scenarios that lead to the same hazardous event as a Safety Instrumented Independent Protection Layer. Thus, for a proper hazardous event frequency calculation, it must be taken into account all cause-consequence pairs that demand the same SIF. This is accounted only via the "cumulative method". As noticed through this simple case study, in some situations the difference between approaches may be significant, what could lead to a wrong SIL determination (such as the one achieved by the "per scenario" method).

Nevertheless, a clear understanding of how SIF demand frequency is estimated is essential to ensure that the Safety Instrumented Function will be properly specified to reduce the likelihood of an accidental scenario; and then to ensure acceptable scenario risk level or As Low As Reasonably Practicable (ALARP).

Adequate risk identification and assessment are keen for ensuring an effective risk reduction. Once some risk assessment methods and techniques are being spread implemented, it is becoming noticed circumstances where adequate competence to perform such assessments is neglected, embedded on improper adaptations of standards and methods. These degraded risk assessments open rooms for the industry to most likely be exposed to higher risks than the ones assessed, thus barely mitigated.

## 7. REFERENCES

[1] IEC-61511, *Functional Safety - Safety Instrumented Systems for the Process Industry Sector*, 1st Ed., IEC -International Electrotechnical Commission, Geneva, Switzerland, 2003.

[2] TORRES-ECHEVERRIA, A., "On the Use of LOPA and Risk Graphs for SIL determination", *Mary Kay O´Connor Process Safety Center, Texas A&M Engineering Experiment Station, 17th Annual International Symposium*, October 28-30, 2014.

[3] CCPS. *Layer of Protection Analysis*. Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 2001.

[4] IEC-61882, *Hazard and operability studies (HAZOP studies). Application guide*, 1st Ed., IEC - International Electrotechnical Commission, Geneva, Switzerland, 2001.

[5] RAMÍREZ-MARENGO, C., et al., "A formulation to optimize the risk reduction process based on LOPA", *Journal of Loss Prevention in the Process Industries*, 2012. http://dx.doi.org/10.1016/j.jlp.2012.07.009

[6] BARADITS SR., GY., MADÁR, J., "Cumulative LOPA method", *Hungarian Journal of Industrial Chemistry*, VESZPRÉM, vol. 37(1), pp.31-36, 2009.
[7] BARADITS, GY., MADÁR, J., BARADITS, Á., "SIL Determination according to IEC-61511-3: Cumulative LOPA method", *SIL4S Kft, VESZPRÉM, 8200, Hungary*.
[8] Loss Prevention Bulletin, "Recurring accidents: overfilling vessels", Peter Waite, *Institution of Chemical Engineers*, pp.40-44, March 2013.
www.icheme.org/sitecore/shell/Controls/Rich%20Text%20Editor/~/media/Documents/TCE/lessons-learned-pdfs/861lessonslearned.pdf icheme tce today march 2013 overfilling vessel
[9] ISO/TR14121-2, *Safety of machinery – Risk Assessment – Part 2: Practical guidance and examples of methods*, 2nd Ed., ISO - International Organization for Standardization, Geneva, Switzerland, 2012.
[10] IEC-61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 1st Ed., IEC -International Electrotechnical Commission, Geneva, Switzerland, 2010.
[11] AICHE. *Layer of Protection Analysis – Guideline for Initiating Events and Independent Protection Layer in Layer of Protection System*. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA (2005).
[12] ENERGY INSTITUTE, IP Research Report. "Ignition Probability Review, Model Development and Look-Up Correlations", 2006.