HUNGARIAN JOURNAL
OF INDUSTRIAL CHEMISTRY
VESZPRÉM
Vol. 37(1). pp. 31-36 (2009)

CUMULATIVE LOPA METHOD

GY. BARADITS SR.✉, J. MADÁR

SIL4S Ltd., H-8200 Veszprém, P.O. Box 1297, HUNGARY
✉E-mail: bgs@sil4s.hu

LOPA (Layer of Protection Analysis) is a simplified risk assessment method that is uniquely useful for determining how "strong" SIF (Safety Instrumented Function – "interlock") should be designed. LOPA is a semi-quantitative tool which is readily applied after the Process Hazard Analysis (PHA) – for example, HAZOP – and before Fault Tree Analysis/Quantitative Risk Assessment if needed. In most cases, the SIF's Safety Integrity Level requirements can be determined by LOPA without using the more time-consuming tool of Fault Tree Analysis or Quantitative Risk Assessment. The problem of classical LOPA approach is that it takes into consideration only one hazard scenario at a time. However a SIF may exist in several hazard scenarios, so in practice there is a need for a cumulative LOPA method where we can take into account all hazard scenarios in LOPA calculation which have identical SIF as a Safety Instrumented Independent Protection Layer. We lay down the mathematics of cumulative LOPA, and developed software called Tool4S which uses this mathematics. The article shows some example of the SW application.

Keywords: Process HAZOP, Process Risk, Risk Matrix, LOPA, cumulative LOPA, SIL, SIL calculation, cost reduction, Tool4S SW

Introduction

In the 1990s, companies and industrial groups developed standards to design, build, and maintain, that time called, ESD system focusing only the PLC part of the system. The PLC, in safety application, was classified according the German Standards [1-7]. The first general safety standard, the IEC 61508 1-7 [8], was issued in 1998, which in this topic dramatically changed the safety thinking both in general and industrial segment specific. In 2004 was published the IEC 61511 1-3, process industry sector safety standard [9], which is valid for Chemical, Petrochemical, Oil and Gas Industry. This standard firstly introduced the principle of Safety Instrumented Systems (SIS) and Safety Instrumented Function (SIF).

A key input for the tools and techniques required to implement these standards was the required Probability of Failure on Demand (PFD) for each Safety Instrumented Function (SIF). Process Hazard Analysis (PHA) teams and project teams struggled to determine the required Safety Integrity Level (SIL) for the SIFs ("interlocks").

Within these techniques, the concept of layers of protection analysis (LOPA) – an approach to analyze the number of layers needed to protect the process against the unwanted consequences of the Hazards – was first published by the Center for Chemical Process Safety (CCPS) in the 1993 book Guidelines for Safe Automation of Chemical Processes [12]. From those concepts, several companies developed internal procedures for Layer of Protection Analysis (LOPA) [13], and in 2001 CCPS published a book describing LOPA [12]. This paper briefly describes the LOPA process, and discusses experience in implementing the technique.

Procedure of SIL calculation

Based on the Safety Life Cycle, it is necessary to get convinced that the existing / designed SIS is appropriate for the particular process from the viewpoint of safety (pre-validation, validation). How does one get convince about it? Based on the IEC-61511 standard, one should perform the following steps:

- Hazard and Risk analysis
- IPL allocation and SIL calculation of SIFs
- Safety Requirement Documentation

The following figure shows this procedure (see *Fig. 1*).

What is LOPA?

Both in the IEC 61508 and IEC 61511, LOPA is mentioned as one of the methods, which gives possibility of calculation the required SIL value of SIF.

LOPA [14, 15] is a semi-quantitative risk analysis technique that is applied following a qualitative hazard identification tool such as HAZOP.

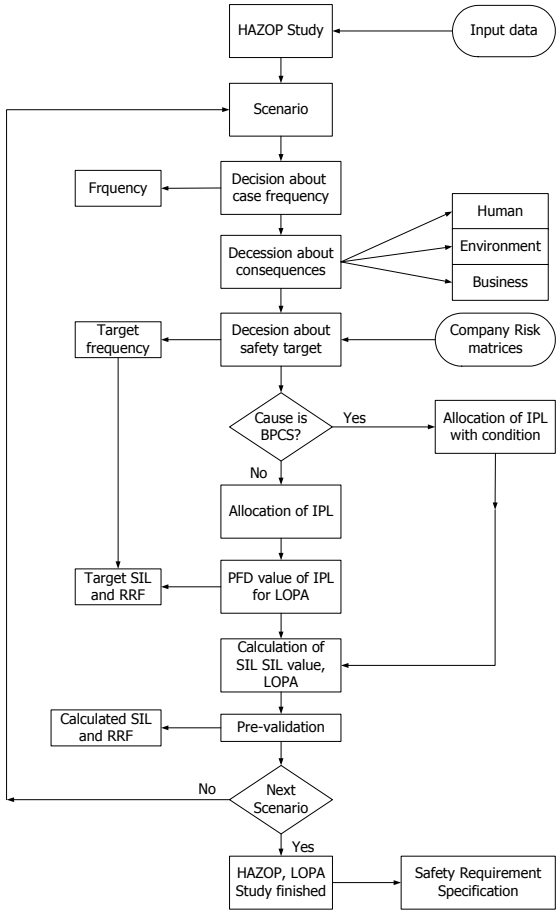


Figure 1: Method of SIL calculation

We describe LOPA as a semi-quantitative method because even if the technique does use numbers and generates a numerical risk estimation, the input numbers are approximate estimates, their accuracy is about at the order-of-magnitude level; and the result is intended to be conservative (overestimating the risk). But even if the LOPA is semi-quantitative, the estimated risk is usually adequate to understand the required SIL for the SIFs. If a more complete understanding of the risk is required, more rigorous quantitative techniques such as fault tree analysis or quantitative risk analysis may be required.

The main goal of LOPA to evaluate the risk of selected hazardous scenarios. Practically, the LOPA is used to determine that the identified (existing and/or proposed) protection layers are "strong" enough or not. I.e. the LOPA is used to make risk avoiding (protection and preventive) decisions.

LOPA starts with an undesired consequence – usually, an event with environmental, health, safety, business, or economic impact. The severity of the consequence is estimated using appropriate techniques, which may range from simple "look up" tables to sophisticated consequence modelling software tools.

A consequence always has one or more initiating events (causes). Each cause-consequence pair is called as *scenario*, and the LOPA focuses on one scenario at a time. The frequency of the initiating event is also estimated (usually from look-up tables or historical data).

After identifying all causes and consequences, the possible safeguards (protections layers) are evaluated for two keys characteristics:

- Is the safeguard enough effective in preventing the scenario from reaching the consequence?
- **AND**, is the safeguard independent of the initiating event and the other IPLs (Independent Protection Layers)?

If the safeguard meets both of these criteria, it is an Independent Protection Layer (IPL).

LOPA estimates the likelihood of the undesired consequence by multiplying the frequency of the initiating event by the product of the probability of failure on demand (PFD) of applicable IPLs:

$$F_{mit} = F_{initiating} \cdot \prod_j PFD_j .$$

PFD gives the probability that the given IPL cannot prevent against the scenario to reach the unwanted consequence. The smaller that value, the better the IPL.

The estimated likelihood of the undesired consequence is called as "mitigated consequence frequency" because the frequency is mitigated by the independent protection layers. That value should be compared to the company criteria for tolerable risk for the particular consequence severity. If additional risk reduction is needed, more IPLs must be added to the design.

The estimated likelihood of the undesired consequence is called as "mitigated consequence frequency" because the frequency is mitigated by the independent protection layers. That value should be compared to the company criteria for tolerable risk for the particular consequence severity. If additional risk reduction is needed, more IPLs must be added to the design.

Fig. 2 shows a simple diagram to illustrate how the probability of occurrence of the unwanted consequence decreases by using IPLs.

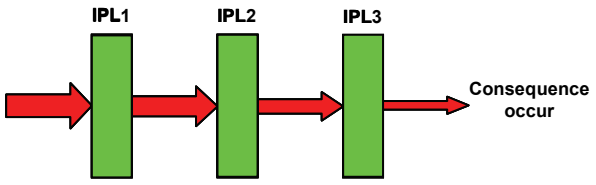


Figure 2: LOPA method

Why is LOPA?

The suggested methods in the IEC 61508 and IEC 61511 which gives possibility of calculation the target SIL value of SIF are split into three groups:

- Qualitative, like risk matrix, risk graph
- Semi quantitative, like LOPA
- Quantitative, like Failure Mode and Effect Analysis (FMEA) or MARKOV modelling

The qualitative methods are simply, inaccurate and too subjective, that is why they are not widely applied in the practice. On the other hand, the quantitative methods are just too complex and slow for practical usage. That is why the semi-quantitative methods, LOPA seems to be a good compromise.

However while the LOPA is semi-quantitative, we have some argument why using of LOPA is preferable:

- It is not as subjective as the qualitative methods.
- It needs Company Target Risk Matrix, so it increases the safety culture of the given company as the company needs to build up the Functional Safety Quality Manual.
- LOPA is the only method that is able to take into consideration the non-instrumented protection layers.
- LOPA gives the possibility of discovering all non-instrumented protection layers.
- LOPA gives the possibility of building up the most cost effective protection system including instrumented and non instrumented protection layers.

General method of LOPA

The LOPA main objectives are the following [16]:

- Identify the non instrumented safety protection layers.
- Allocate the safety functions to the protection layers.
- Determine if one or more safety instrumented functions (SIF) are required to achieve the target risk reduction.
- Determine for each SIF, if required, the safety integrity level (SIL).

Main steps of LOPA are the following:

- Develop each impact event scenario based on HAZOP.
- Evaluate the severity consequences for human, business and environment of the impact event scenario.
- Set the impact event scenario target likelihoods after mitigation, to meet the Company's Functional Safety Quality Management (FSQM) Target Safety matrix for human, business and environment.
- Identify and set the initiating event(s) and related enabling factors.
- Calculate the enabled initiating event(s) likelihood.
- Add independent protection layers (IPL) to mitigate the impact event scenario.
- Set the probability of failure on demand (PFD) values of IPLs.
- Set the impact event scenario mitigation credit factors.
- Calculate the likelihood of the impact event scenario after mitigation; and check if the likelihoods meet the company's target safety matrix. If one or more target likelihoods are not met, go back to beginning.
- If all the target likelihoods are met, assess the next impact event scenario (see also Fig. 1).

Problems with the simple LOPA method

The fundament of the LOPA calculation is the tolerable risk criteria. The typical risk criteria give the tolerable risk for a person, for a plant, etc. During the LOPA, one always compares the mitigated risk to the tolerable risk. If the mitigated risk is lower than the tolerable risk or at least it is "low as is reasonably practicable" there is no need for other protection layers. If not, there is a need for new protection layers and/or other risk reduction methods (see the "Main steps of LOPA" in the previous chapter).

The tolerable risk categories are always set up by the given Company and they must be involved in the Company Safety Policy. As the corporate criteria determine the tolerable risk values, practically the LOPA focuses on the calculation of the mitigated risk for the goal to determine the necessary risk reduction factor. However because the tolerable risk is based on a unit such as person, it is not enough to calculate the mitigated risk for every scenario and compare them to the tolerable risk value(s). This so-called "per scenario" method has the disadvantage that it cannot take into consideration that a hazard may contain several scenarios with the same consequence and same protection layer (a SIF, for example). In this cases, instead of "per scenario" method, one should use the "cumulative" risk calculation method.

Cumulative LOPA method

Because of the problems of "per scenario" method, we suggested here the "cumulative" method which can take into consideration all hazard scenario which is protected by the same SIF.

Let see an example about the difference between the "per scenario" and the "cumulative" method. Let assume that the hazard is high pressure of a vessel and there are two possible initial events:

- The pressure control fails. The frequency is F_1.
- The downstream line is blocked. The frequency is F_2.

Let us assume that the consequence is vessel rupture in both cases. Also let assume that there is an independent high pressure trip, i.e. a SIF which can protect against the high pressure in both cases, and there is no any other IPL.

If the "per scenario" method used, one will calculate in the following way: The necessary risk reduction factor (target risk reduction factor) for the first scenario is: $RRF_1 = F_1 / F_{tol}$, where the F_{tol} is the tolerable frequency for the given consequence based on the Company Safety Policy. The target risk reduction factor for the second scenario is: $RRF_2 = F_2 / F_{tol}$. The final

target RRF for the SIF is the higher RRF value. E.g. if $RRF_2 > RRF_1$, the final RRF will be:

$$RRF_{per-scenario} = RRF_2 .$$

In contrast, the "cumulative" method adds up all the RRF values, so the target RRF for the SIF will be:

$$RRF_{cumulative} = RRF_1 + RRF_2 .$$

This is higher value than the result of "per scenario" method.

That above mentioned difference is important because the IEC-61511-3 suggests calculating the total risk: "*The last step is to add up all the mitigated event likelihood for serious and extensive impact events that present the same hazard*". It means that the standard suggests the cumulative LOPA instead of the per-scenario LOPA.

The difference between the results of the two LOPA techniques may be very high when the given SIF can be found in several scenarios as IPL. This difference is usually much more than the uncertainty of the LOPA method, so the neglect of cumulative LOPA may lead to totally wrong SIL calculation.

In the next chapter, we will show how the cumulative LOPA is implemented in our Tool4S software tool.

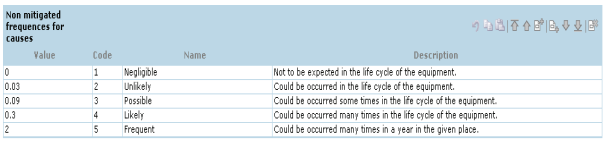
Cumulative LOPA method SW: the Tool4S

There are several software tools for making HAZOP and LOPA, but our experience has showed that most of them only can calculate the RRF value for a scenario (per scenario method) but do not accumulate them. So it is the task of the user.

Our experience has showed that a SIF can occur in several hazards in the process industry. If a user uses software which does not support the cumulative LOPA method, finally he/she will make mistakes or try to forget the cumulative LOPA method just because it is too tiresome.

Hence, we built the cumulative LOPA into our Tool4S software making the calculation automatic. In the following, it will be presented how the cumulative LOPA is realised in our software.

The calculation is based on the "non-mitigated frequencies" matrix for causes and the "tolerable frequencies" matrix of the given company. The non-mitigated frequencies matrix can contain one or more pre-defined likelihood values for the initial events (causes). *Fig. 3* illustrates an example. It is the user task to define this values, he/she can easily add or remove items to/from the matrix. Certainly it is not necessary to use this matrix for every case; the user can give a unique frequency value for every initial event if the pre-defined values do not fit to the given case.

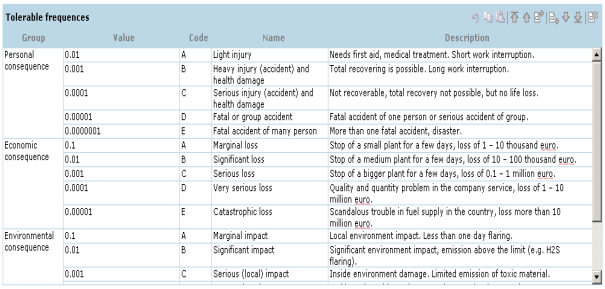


Non mitigated frequences for causes

Value	Code	Name	Description
0	1	Negligible	Not to be expected in the life cycle of the equipment.
0.03	2	Unlikely	Could be occurred in the life cycle of the equipment.
0.09	3	Possible	Could be occurred some times in the life cycle of the equipment.
0.3	4	Likely	Could be occurred many times in the life cycle of the equipment.
2	5	Frequent	Could be occurred many times in a year in the given place.

Figure 3: Definition of non-mitigated frequency matrix of causes

The tolerable frequencies are also user defined. The user can define the number of consequence types (the default is three: for human, for business and for environment), the possible severity categories, and the specific tolerable frequencies for each severity. *Fig. 4* shows an example.



Tolerable frequences

Group	Value	Code	Name	Description
Personal consequence	0.01	A	Light injury	Needs first aid, medical treatment. Short work interruption.
	0.001	B	Heavy injury (accident) and health damage	Total recovering is possible. Long work interruption.
	0.0001	C	Serious injury (accident) and health damage	Not recoverable, total recovery not possible, but no life loss.
	0.00001	D	Fatal or group accident	Fatal accident of one person or serious accident of group.
	0.0000001	E	Fatal accident of many person	More than one fatal accident, disaster.
Economic consequence	0.1	A	Marginal loss	Stop of a small plant for a few days, loss of 1 - 10 thousand euro.
	0.01	B	Significant loss	Stop of a medium plant for a few days, loss of 10 - 100 thousand euro.
	0.001	C	Serious loss	Stop of a bigger plant for a few days, loss of 0.1 - 1 million euro.
	0.0001	D	Very serious loss	Quality and quantity problem in the company service, loss of 1 - 10 million euro.
	0.00001	E	Catastrophic loss	Scandalous trouble in fuel supply in the country, loss more than 10 million euro.
Environmental consequence	0.1	A	Marginal impact	Local environment impact. Less than one day flaring.
	0.01	B	Significant impact	Significant environment impact, emission above the limit (e.g. H2S flaring).
	0.001	C	Serious (local) impact	Inside environment damage. Limited emission of toxic material.

Figure 4: Definition of tolerable frequency matrix

Every pre-defined non-mitigated frequency and tolerable frequency value has a code. The user can easily do the risk ranking by only selecting the appropriate code; *Fig. 5* shows an example.

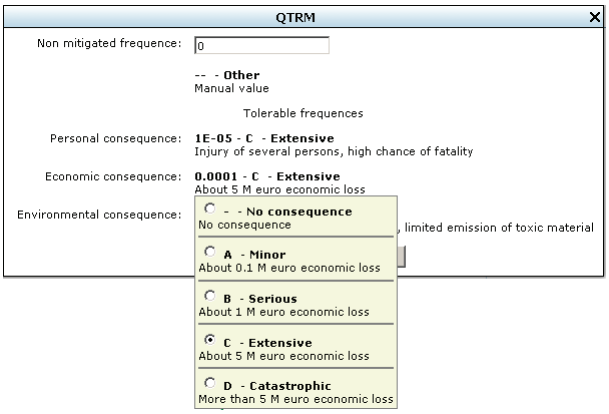


Figure 5: Example for risk ranking

The risk ranking must be done for every cause-consequence pair, but if the consequence is the same for more causes, the software will copy the consequence ranking information to save manual work.

The main concept in the software is that every SIF has a unique tag name and own SRS (Safety Requirement Specification). When a SIF is added into the HAZOP, the software automatically collect every scenario in which the SIF can be found, and calculates the cumulative RRF. The following figure *(Fig. 6)* shows an example from the software:

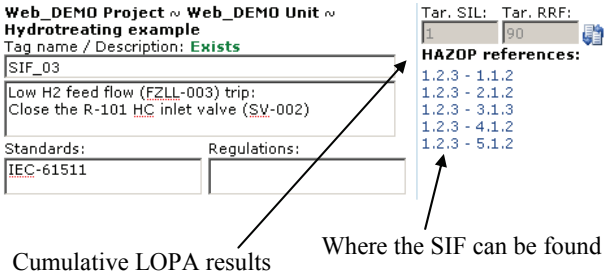


Figure 6: Example for result of a cumulative LOPA

In the followings, the algorithm of cumulative LOPA will be presented as it is realised in the Tool4S software.

Cumulative LOPA algorithm

First step
In the first step, the software takes the frequency of the cause. This is called as non-mitigated frequency. The software takes the cause frequency category and looks for the non-mitigated frequency value from the QTRM (Qualitative Tolerable Risk Matrix). The attributes of non-mitigated frequency:

Sign : $F_{non\text{-}mit}$
Name : Non-mitigated frequency
Unit : 1/year
Range : Real number, $0 \le F_{non-mit}$

Second step
The software takes the severity categories of the consequence, and look for the tolerable frequency value from the QTRM. In the QTRM, there are tables which inform about the tolerable frequency of different types of consequences. Typically there are three types of consequences:

- Human
- Business
- Environment

In the followings, we assume that these three consequence types are used. The attributes of tolerable frequencies:

Sign : $F_{tol}^{\text{human}}, F_{tol}^{\text{business}}, F_{tol}^{\text{environment}}$
Name : Tolerable frequency (target frequency to be reached)
Unit : 1/year
Range : Real number, $0 \le F_{tol}^{...}$

Third step
The software calculates the Scenario Risk Reduction Factor (without SIF) based on the PFD values of safeguards. The PFD values are manually given by the user in the HAZOP (*Fig. 7* illustrates an example). The attributes of PFD:

Sign : *PFD*
Name : Probability of Failure on Demand
Unit : -
Range : Real number, $0 \le PFD \le 1$

The attributes of scenario risk reduction factor:
Sign : RRF_{scen}
Name : Scenario Risk Reduction Factor (without SIF)
Unit : -
Range : Integer, $0 \le RRF_{scen}$

The calculation of scenario risk reduction factor is:

$$RRF_{scen} = \text{int}_{\text{up}}\left(F_{mit} / F_{tol}\right)$$

where int_{up} is an integer round up function ("ceil function"), and the F_{tol} and F_{mit} are calculated as:

$$F_{tol} = \min\left(F_{tol}^{\text{people}}, F_{tol}^{\text{business}}, F_{tol}^{\text{environment}}\right)$$

$$F_{mit} = F_{non-mit} \cdot \prod_j PFD_j$$

where j is a running index for the safeguards in the given Hazard scenario.

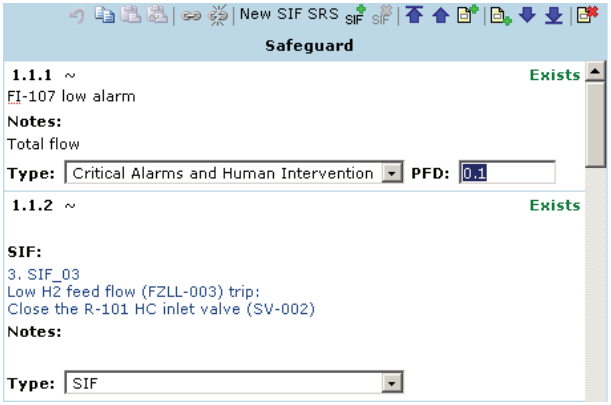


Figure 7: Edit safeguards in Tool4S SW

Fourth step
Finally the software calculates the cumulative target risk reduction factor and SIL value. Both values are calculated automatically for a given SIF based on all referenced Hazard scenarios (see Fig. 6). The attributes of target risk reduction factor:

Symbol: RRF_{tar}
Name : Target Risk Reduction Factor
Unit : -
Range : Integer, $0 \le RRF_{tar}$

The calculation of cumulative target risk reduction factor:

$$RRF_{tar} = \text{int}_{\text{up}}\left(\sum_i \left(F_{mit}^i / F_{tol}^i\right)\right)$$

where i is running index for Hazard Scenarios in which the given SIF can be found as safeguard.
The attributes of Target SIL:
Sign : SIL_{tar}
Name : Target Safety Integrity Level
Unit : -
Range : Integer
The calculation method of Target SIL:

$$SIL_{tar} = \mathrm{int}_{\mathrm{down}}\left(\log_{10}\left(RRF_{tar}\right)\right)$$

where $\mathrm{int}_{\mathrm{down}}$ is an integer round down function ("floor function").

Conclusions

In this article, we evaluated the existing methods which calculate the SIL value of SIFs within a HAZOP study using LOPA method. We has analysed the traditional LOPA method called "per scenario" in which only one scenario/SIF is taken into consideration. We showed that the result of this calculation is far away from to be considered as correct.

We suggested and analysed the "cumulative LOPA method" that takes into consideration all Hazard scenario which contain the same SIF as an independent protection layer.

This method has only one disadvantage that it is not easy to realise manually. That is why we developed our Tool4S HAZOP/LOPA study program, which automatically calculates the result of the cumulative LOPA method.

The Tool4S SW overcomes the problem of manual and very slow calculation, where the result is not always correct, mainly in case when the technology is difficult.

The Tool4S was tested over more than 100 HAZOP and LOPA study and proved that is fast, correct with high reliability.

ACKNOWLEDGEMENTS

Here we would like to express our acknowledgement to our colleges at SIL4S Ltd. for their continuous contribution to this development and the Department of Process Engineering of Pannon University, Veszprém taking part in the test of our SW and giving some development idea to us.

REFERENCES

1. TÜV Book, Microcomputer in Safety Application, Safety Classes 1…5 level, 1972
2. DIN 3100 – General Requirement, AK 1…8
3. DIN V VDE 081 Microprocessors in Safety Application
4. DIN V 19250 Basic Safety Evaluation for Measurement & Control
5. DIN V 19250 Requirements & Measures, Qualitative Consideration
6. VDE 0116 Electrical Equipment for Burner Application
7. DIN EN 954 Safety for Machinery
8. IEC 61508 1–7: Functional safety of electrical / electronic/programmable electronic safety - related systems.
9. IEC 61511 1–3: Functional Safety: Safety Instrumented Systems for the Process Industry Sector
10. IEC 61882: Hazard and Operability (HAZOP) Studies
11. ARTHUR M. (ART) DOWELL, HENDERSHOT D. C.: Simplified Risk Analysis – Layer of Protection Analysis (LOPA), AIChE 2002 National Meeting, Paper 281a
12. Safety Line Institute: Occupational Health & Safety Practitioner, management of major hazard facilities, London, 1998
13. Layer of Protection Analysis – Simplified Process Risk Assessment, American Institute of Chemical Engineers, New York, NY, 2001
14. Centre for Chemical Process Safety (CCPS), Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, New York, NY, 1993.
15. The Instrumentation, Systems, and Automation Society (ISA), ANSI/ISA 84.01-1996, Application of Safety Instrumented Systems to the Process Industries, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 1996.
16. Risk Guidelines as a Risk Management Tool, Prepared for presentation at the 1996 Process Plant Safety Symposium Houston, Texas April 1-2, 1996 Session 3