LOPA – A Method to Analyse Safety Integrity Systems according to IEC 61511

HOLUB P.[1, 2], BÖRCSÖK J.[1, 2]
[1] Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel
GERMANY

[2] HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Str. 28, 68782 Brühl
GERMANY

http://www.uni-kassel.de, http://www.hima.com

Abstract: - The Layer Of Protection Analysis, abbrev. LOPA, is a semi quantitative risk analysis method. The different layers, which are already applied or still in the planning phase will be analysed and evaluated via the LOPA in order to reduce the hazards for people, environment or machine to a tolerable residual risk. Herewith, one will consider any imaginable damage initiating events. With the adequate table of values for the occurrence frequency of such initiating events and for the failure probability of each protection layer, the remaining residual risk can be defined and compared to the required tolerable residual risk. Depending on the applications, some weighting factors having a corresponding risk reduction, such as for example the length of stay in a hazardous area, will be taken into account. Should the results show that the tolerable residual risk has not been achieved or has been under estimated, one would, in case no other constructive protection layers are possible, plan and apply a safety integrity system (SIS). The LOPA method allows defining the safety requirements in form of the necessary safety integrity levels SIL for the SIS.

Key-Words: - HAZOP, IEC 61511, Initiating Events, LOPA, Process Hazard Analysis (PHA), Protection Layer (PL), Risk Matrix, risk reduction, Safety Instrumented Function (SIF), Safety Integrity Level (SIL), Safety Integrity System (SIS)

1 Introduction

The aim of safety systems is to reduce an existing safety risk for people, machine, and/ or environment to an always residual risk. The term Safety-Risk associates the two words Safety and Risk. The IEC 61508 defines in paragraph 4 the term Safety as "freedom from unacceptable risk" and the term Risk as "the combination of the probability of occurrence of harm and the severity of that harm" [1]. Thereby the term Safety-Risk can be defined as a measure of combination presuming the probability that an unacceptable risk may occur with its consecutive effects. How much a risk is considered as tolerable is very subjective and depends on the people who are affected by its effects. A measure that will achieve the necessary risk reduction, set up with a safety function and processed via a safety system, constitutes the safety integrity, a probability.

This acceptable risk must be defined for the Overall Safety Cycle of a system. Thereby, within the different phases of a Life Cycle, one can set different limits for the Risk Acceptability. One can easily imagine that, for example, the risk during an operating phase will be lower classified during an Online proceeded modification or a later decommissioning because all the safety measures work well. Fig. 1 shows that the error contribution reproduces itself during the Life Cycle of technical systems.

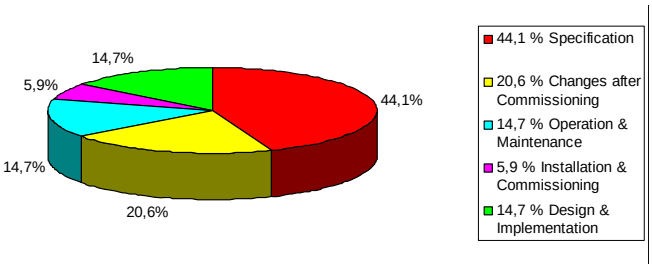

Fig. 1: Error contribution during a Life Cycle after examination of 34 accidents by the HSE (Health and Safety Executive) [2]

The IEC 61511 [3] distinguishes the following phases during a Safety Life Cycle.

- initial concept
- design
- implementation
- operation and maintenance
- decommissioning

In order to set up an acceptable risk, one has to examine the concept of the process with regard to the possible risks. Thereby, some historical notations regarding the existing processes will also count as data source. On a second step the real risk analysis will be performed. Once the risk of the process system EUC (Equipment under Control), which is going to be examined, has been defined, the real necessary and the risk reduction will be averaged, see Fig. 2.

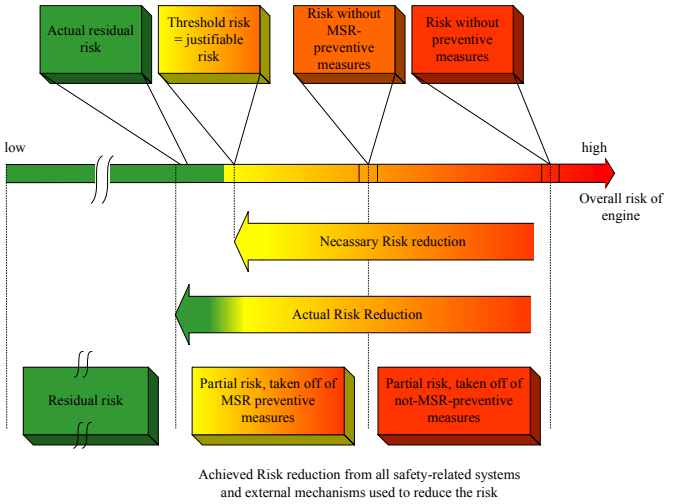

Fig. 2: Steps of risk reduction [1], [4]

The safety requirements result from the necessary risk reduction for the protection concept which can consists of different levels. Should a Safety Programmable System (SPS) be chosen as protection concept, it could therefore consist of single safety functions. In the 70s and 80s, terrible accidents occurred, one should not forget the Dioxin accident in 1976 in the Italian City Seveso or the explosion in 1984 in a pesticides manufacture. Those, as well as further accidents, lead to a lot of administrative measures whose goals were to reduce the risks for the people. As an example the US-Government created the OSHA (Occupational Safety & Health Administration), which is responsible for the safety and health of America's workers by setting and enforcing standards [5]. One could also mention the Seveso Directive II reviewed 1996, a Council Directive on the "control of major accident hazards involving dangerous substances and the measures of protection to limit their consequences on Human beings and environment, in order to guarantee in a common way a high level of protection" [6]

In 1985 the American Institute of Chemical Engineers (AIChE) funded the Centre for Chemical Process Safety (CCPS) in New York. In Europe, the European Process Safety Centre (EPSC) was grounded in Great Britain in 1992 (in [7] find some more Literature advises). Both Institutes deal with Process Safety especially in chemical plants and develop analytical methods, to describe the risk potential and thereby improve its control. Corresponding measures have been developed and are still being developed, as for example the LOPA, the Layer Of Protection Analysis. The LOPA concept was first described in den Guidelines for Safe Automation of Chemical Processes in 1993, whereupon the actual Director of the EPSC, Mr. R. Gowland, was involved, at that time, in the development of the method. [8], [9]. Since, this concept has been adopted by different companies which have adjusted it to their own applications [10], [11]. In 2001 CCPS published a book about LOPA [12]. This book as well as the IEC 61511 [13] constitutes the basis of this paper.

2 Objectives of LOPA

The aim of each Process Risk Analysis (PRA), also named Process Hazard Analysis (PHA), is to define the necessary and real Safety Integrity Level (SIL) for a Safety Instrumented Function (SIF) i.e. a Safety Integrity System (SIS). Instead, the user has quantitative as well as qualitative methods at his disposal. The Risk Graph (Fig. 3) and the Risk Matrix (Fig. 4) belong to these important qualitative methods

To both methods the combinations from different parameters will be assigned to different risk classes. On the Risk Graph these are parameter „C" (consequence) „F" (frequency and exposure time), „P" (possibility of avoiding hazard) and „W" (probability of the unwanted occurrence) [14], [15]. For the Risk Matrix the following parameters will be examined: "User defined likelihood/potential" and "consequences". The procedure for the Risk Matrix method will be described as for example in [16].

Among other quantitative methods, there are the failure tree, the reliability block diagram and the Markov-Model-Analysis. Especially for these methods the user requires the failure rate of each hardware, in order to define later, with the help of a mathematical equation, the failure probability. With the help of the Failure probability, which will be given according to the IEC 61508/61511 [1]/[13] via the PFD_{avg}-[1] or PFH-Value[2],

[1] PFD_{avg}: Average probability of failure on demand

[2] PFH: Probability of dangerous failure per hour

the risk class in form of a SIL Classification can be determined. Though, one must consider that according to the IEC 61508/61511 [1]/[13] both numerical values are not sufficient themselves to determine the SIL Classification. Instead, other aspects such as the architecture, the SFF[3] and the die DC[4]-measures must be taken into consideration.

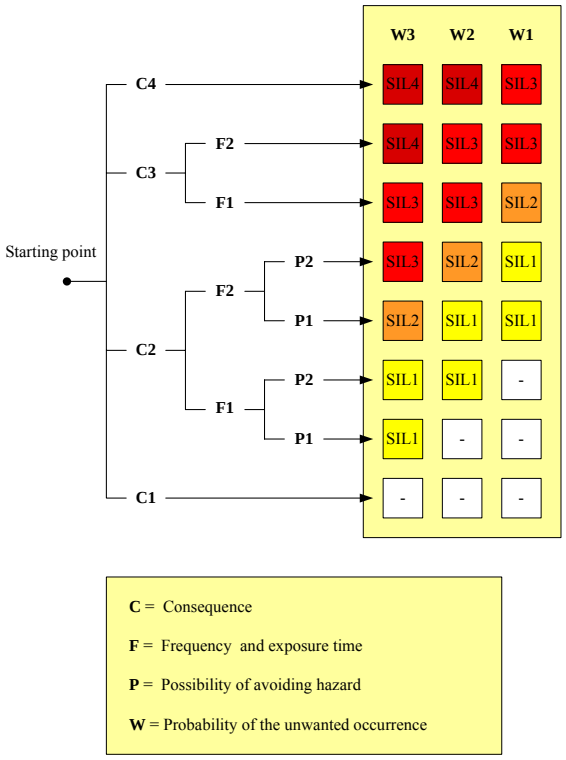

Fig. 3: Risk Graph

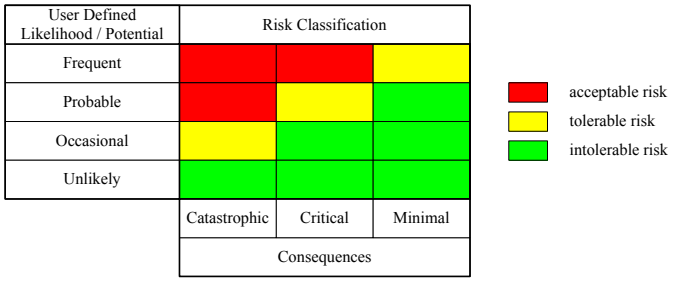

Fig. 4: Risk Matrix

LOPA counts among the semi-quantitative methods, which means that to determine the risk one requires the experience of the process engineer in regard to appreciation of the severity as well as the occurrence likelihood of a possible hazard. Therefore LOPA must be processed for each initiating event and its consecutive effects [17]. After processing the LOPA the

- specifications for the safety requirements of each protection layer

and/or, in case the protection layer that has been planed is not sufficient,

- the SIL Specification for a safety function

will be determined [13].

As a basis for a LOPA one uses in most cases a HAZOP-Study (HAZOP: HAZard and OPerability analysis). A HAZOP-Study consists of averaging the causes of the accidents, their consequences and severity. The protection layers that have been given/ planed do not belong to the Risk Matrix. With LOPA, it shall be justified that with the given protection layers, the planed risk reduction, – in LOPA defined as „Target Mitigated Event Likelihood“, abbrev. TMEL, is at least achieved or even outmatched. In addition the data from the HAZOP Study and the PFD-Value for each protection layer will be required.

3 Protection Layer

A Protection Layer (PL) consists of equipments and /or organisation measures to reduce the risk of an existing safety critical application. The risk reduction of a Protection Layer averages according to the IEC 61511 [13] at least the factor 10. Should a high risk for people, environments and machine threaten, as for example in the process industry, then several PLs shall be provided – as mentioned in the IEC 61511 [13] – In the process industry PLs exist in form of damage limitation systems, such as protection, control and operating systems. In addition there are also measures depending on the application, such as evacuation measures and public measures for emergences, as for example alarms via different information media (internet, television or radio). A PL displays the following criteria:

Specificity: a PL has been developed against a special hazardous event and its consequences. Thereby the causes responsible for that event can be different.

Independence: a PL must work totally independently from all other PLs, especially when the same fraught with risk scenario is being considered. Any protection systems or measures should be used together with other PLs.

Reliability: a PL must be reliable when protecting against any occurring hazardous events and/or their consequences. During the development of the PL one must make sure that systematic as well as random failures will be considered.

[3] SFF: Safe Failure Fraction, the ratio between safe plus dangerous detected failure rates to the whole sum of failure rates

[4] DC: Diagnostic coverage factor, this means the ratio between dangerous detected to the whole sum of dangerous failure

Verifiability: the function of the Layer of Protection must be tested and maintained safely. Recurring tests functions are necessary to make sure that a reproducible risk reduction will be reached at any time.

A PL will be described as an Independent Protection Layer (IPL) when, in addition to the above mentioned criteria, the following ones are given:

- The factor for the risk reduction averages at least 100.
- The availability of the PL is high, i.e. ≥ 0.9.

A Safety Integrity System (SIS) is to be considered as a specific IPL, when that one has been developed according to the IEC 61508 [1]. For a SIS and its Hardware the proof for specific criteria will be required. Especially the parameters PFD (Probability of Failure on Demand), SFF (Safe Failure Fraction), HFT (Hardware Fault Tolerance) and the SIL (Safety Integrity Level) will be put into evidence.

Process equipments can also be used as Protection layers. Those will be described as Basic Process Control System (BPCS). Though, according to the IEC 61511 [13] these layers can only be attributed to a risk reduction factor < 10. Thereby the safety access and a modification management must be secured. Therefore, within a PL, a BPCS can only be considered as one out of several protection systems. A BPCS and a SIS must be physical separated units, included their Hardware, i.e. sensors, logical units and actuators. A failure of a BPCS shall not be responsible for the release of an unintentional incident [18].

The term IPL will be used when the risk of a hazardous event reduces to a residual risk. An IPL can generally be used against several hazardous events. That risk will not always be minimised to a residual risk, but the protection layer do work as risk reducing. This is the reason why protection layers can be applied as two types: as IPL and as risk reducing PL. Through a risk reducing PL, additional safety units will be implemented. During a LOPA each IPL and each risk reducing PL must be exactly used once in the analysis [19]

4 Presentation

The different PLs will clearly be described with the onion skin model see Fig. 5. The single levels are independent of each other and physically separated. In addition to the Onion Model, the so-called LOPA Diagram will also be used to follow the event tree presentation. This one consists of two alternative symbols, an arrow and a block, see Fig. 6. The length of the arrow defines the extent of the failure whereas the strength of the arrow presents its frequency, in case the following IPLs would not work. The blocks show each IPL.

The LOPA-Diagram must be read from left to right. As for the event tree analysis, one starts with the occurring event. Should a PL exist, the effect of the PL on the event will be examined. If only one partial risk reduction occurs over the protection layer or if it completely drops out, the consequences out of it will be the event for the following PL.

For each hazardous initiating event and the consequences out of it, an independent LOPA must be performed as risk analysis. Especially when it deals with Common-Cause Failure, a separate risk analysis must occur for each single possible consequence. Should within a LOPA, the consequences of a Common-Cause-Failure not be considered separately, the result of the risk estimation would be too optimistic [4].

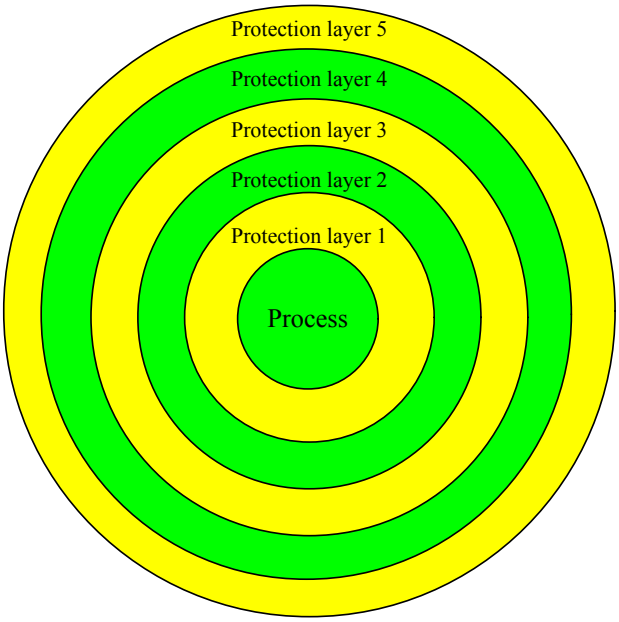

Fig. 5: Protection Layers according to IEC 61511 [4], [8], [9], [11], [13]

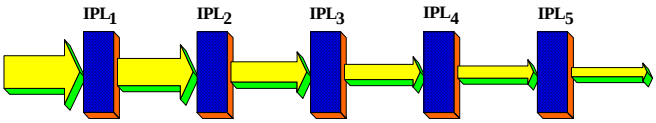

Fig. 6: Protection Layer Concept for five independent protection layers (USE), according to CCPS [4], [8], [9], [11]

5 Calculation

LOPA can be compared to an event tree analysis. One can define the frequency of an unintentional event considering the effects of the protection layer. If one compares the resulting frequency with the acceptable risk, one can define a SIL for a SIS, to become the necessary risk reduction. First of all one must define the frequency f_I of the initiating event.

In the LOPA guidelines by CCPS [8] three groups of initiating events are listed. On the one hand external events as for e.g. earthquakes, Planes catastrophes or sabotages, on the other hand human failures such as operational, maintenance or programming errors. To the third group belong technical failures in the control system where Software and Hardware failures differ from mechanic failures as for example humidity, corrosion or vibration. Near the fact that many groups have their own databank, with frequency data regarding the initiating events, there are also official databanks as for example the CCPS [12], the ISA [20] or data from the OREDA [21]. As an example a few data from [12] are given in Tab. 1

Table 1: Initiating events and frequency of failure f_I, from [12]

Initiating Event	**Frequency Range per year**
Pressure vessel residual failure	10^{-5} to 10^{-7}
Safety valves opens spuriously	10^{-2} to 10^{-4}
Pump seal failure	10^{-1} to 10^{-2}
Small external fire (aggregate cause)	10^{-1} to 10^{-2}

On a second Step the failure probabilities of each PLs i.e. their equipments will be defined. Requirement to define the failure probability is that no other PL exists, i.e. any previously existing PLs will be considered as fail or not existing. Thereby one avoids the low consequence frequency of a initiating event's consequences. Between the IPLs differ passive and active PLs. To provide a risk reduction, Passive PLs do not need any active part during their applications on the unit which is to be monitored. The main task of passive PL is to reduce the unintentional consequences which result from the initiating event. To the passive PL belong for example dikes, drainage systems or walls protection. However active PLs is engaged in the unit to be monitored. This lead to a state modification of the unit to be monitored. If an active PL acknowledges a hazard it brings the unit to be monitored in a safe state. BPCS and a SIS count among active PLs. In addition to the passive und active PLs there are also the so-called human IPLs, for example a supervisory staff (operator). These personnel should take the corresponding measures as soon as they get any signals of optical or audible alarms. Alarm scenarios must regularly be trained, so that any spurious actions from the personnel under pressure provoke bigger accidents. The CCPS notices in his book about the LOPA [12] concerning human IPLs: „Overall, human performance is usually considered less reliable than engineering controls and great care should be taken when considering the effectiveness of human action as IPL. However, not crediting human actions under well-defined conditions is too conservative."

In Tab. 2 *PFD-values* are given from [12] for different IPLs.

Table 2: Passive, active and human IPLs and its *PFD*-value, from [12]

Passive IPLs	***PFD***
Dike	10^{-2} to 10^{-3}
Blast-wall/Bunker	10^{-2} to 10^{-3}
Active IPLs	***PFD***
Relieve valve	10^{-1} to 10^{-5}
BPCS	$> 10^{-1}$ according to IEC
SIS	10^{-1} to 10^{-4}
Human ILPs	***PFD***
Human action with 10 minutes response time	1,0 to 10^{-1}
Human action with 40 minutes response time	10^{-1} to 10^{-2}

If one multiplies man the frequency of a initiating event with the chosen Protection Layers' failure probabilities, see Eq. 1, one obtains the Intermediate Event Likelihood, IEL, [13].

$$IEL = f_I \cdot \prod_{j=1}^{J} PFD_j = f_I \cdot PFD_1 \cdot PFD_2 \cdot \ldots \cdot PFD_J \quad (1)$$

with

f_I : Frequency of the initiating event

PFD_j : Failure probability of the Protection Layer j

IEL : Frequency of the initiating event's consequences

This IEL presents, from the side of its unity, a frequency which shows how often a consequence of a initiating event occurs anyhow when applying Protection Layers. Calculating the IEL a risk reducing effect via a SIS according to the IEC 61511 [13] will not be considered. Only after the following step, which will be performed, and only if a SIS has been integrated within the protections concept, the definition of the Mitigated Event Likelihood (MEL) for an event of the PFD-value of the SIS to Eq. 2 will be considered

$$MEL = IEL \cdot PFD_{SIS} \quad (2)$$

with

IEL : Frequency of the initiating event's consequence

PFD_{SIS} : Failure Probability of the SIS

MEL : Mitigated event likelihood corresponds to the frequency of the initiating event by given SIS

Should several different initiating events exist which do have, though as a consequence, an identical damaging event, then the single MEL-value will be added in order to define the overall frequency of the damaging event. The overall frequency will be defined as a risk in the IEC 61511.

In the following part the acceptance will be presumed that there is only one initiating event which leads to a damaging event

In the Process-Risk-Analysis one has defined the company individual acceptable risk with the index TMEL, see paragraph 2. If the IEL value is smaller than the TMEL-value, the actual risk reduction, via the protection layer, is bigger and the actual risk is, with the protection layer, smaller than the acceptable risk, See Fig. 2. Should IEL be bigger than TMEL, then further protection equipments would have to be planned, in order to become the required risk reduction. In the IEC 61511 [13] one finds the following statement: ”Inherently safer methods and solutions should be considered before additional protection layers in the form of Safety Instrumented Systems (SIS) are applied”. Despite this statement the possibility to implement a SIS will be examined in the following part. If a SIS has already been planned but the necessary risk reduction hasn't been achieved yet, the application of a SIS, which in comparison to the first SIS-Version has a smaller failure probability, will however achieve the necessary risk reduction. An improvement method consists in, for example applying a SIS, having a high valued Hardware-Architecture i.e. with a bigger Hardware Failure Tolerance (HFT). In order to make sure, from the very beginning, which risk reduction must be achieved through a SIS one can apply a LOPA.

To obtain the wanted PFD-Value for the SIS, the condition regarding the real risk reduction

$$MEL \le TMEL \tag{3}$$

must be fulfilled. Setting Eq. 2 in the Ineq. 3, with a $PFD_{SIS,\,new}$, one obtains the condition

$$PFD_{SIS,\,new} \le \frac{TMEL}{IEL}. \tag{4}$$

Should the following application configuration with:

$$TMEL = 10^{-3}\,\frac{1}{year}$$

And a calculated value for

$$IEL = 2 \cdot 10^{-1}\,\frac{1}{year}$$

be given, then thereby the Ineq. 3 will be fulfilled, the PFD-Value for he necessary SIS from Ineq. 4 will be averaged. One obtains

$$PFD_{SIS,\,new} \le \frac{10^{-3}}{2 \cdot 10^{-1}} = 5 \cdot 10^{-3}.$$

According to the SIL-Tables in IEC 61508/61511 [1], [13] this SIS must achieve a Safety Integrity Level Category SIL 2. With SIL 2, which correspond to a failure probability of

$$10^{-3} \le PFD_{SIS} \le 10^{-2}$$

the SIS achieves the requirements i.e. observes the TMEL- Value.

6 Modification

During an HAZOP-Analysis several scenarios presenting a risk for people, environment and/or machine will be considered. The result of HAZOP-Study is among other things the Risk Matrix see Fig.3. In this Matrix the combinations of an event User defined likelihood/potential and its consequences will be classified in risk classes, i.e. from A to F, whereupon A represents the higher risk. In the LOPA the risk classes help defining the parameters TMEL. This index describes quantitatively the tolerable risk, i.e. the frequency of a hazardous occurring event.

In the industry the parameter TMEL will also be presented as a tolerable occurrence probability, though the unit of the multiplicative inverse is a time specification itself. The higher the risk is, the more important the risk reduction will be to avert damages. A big risk reduction also means that the tolerable frequency occurrence TMEL of a hazardous event must be very small.

A risk scenario can have a different hazard classification for people, environment and machines. For example the release of toxic substances in rivers can lead to heavy consequences on the environment, but for people potable water supply be indirectly life threatening and lead to irrelevant damages on the machine outfit. In the industry one distinguishes three different Risk Matrices to present these circumstances and define the individual risk classes for people, environment and machine. Based on these three Matrices, there are therefore three TMEL-values for each scenario, each one respectively for human safety hazards, environmental hazards and commercial hazards. To prove that a risk reduction, as big, or even better, bigger than the required one, has been achieved with the given PLs, one will take out of the three TMEL values, the smallest one.

A further modification concerns the parameter f_I, which describes the frequency of the initiating events. The values given in the literature concerning the frequency of a initiating event, see e.g. table 1, generally refer to standard conditions, as for example continual activity and permanent presence of the working staff. In case of scenarios in which the standard do not completely or provisory match, the parameter f_I would be modified.

This could happen with a so-called weighting coefficient. A time factor or a length of stay factor is an example for it. Through the time factor π_t, the real duration, in which the risk initiating event exists can be regarded. With the help of the length of stay factor π_o, the duration in which an event could really endanger the employees can be considered. The modified parameter $f_{I, mod}$ will be calculated as follow:

$$f_{I,\,\mathrm{mod}} = f_I \cdot \pi_t \cdot \pi_o \qquad (5)$$

Should further weighting coefficient be applied, they will be taken into account in Eq. 5.
One must be very careful when applying such weighting factors, then the following errors can easily occur:

- The risk reduction presented with weighting factors will be wrong implemented in scenarios, which do not acknowledge such factors.
- The influence of the risk reduction will be overestimated

Or even worse

- The same risk reduction will be used several times by different weighting factors.

Thereby one obtains for the frequency of the initiating event $f_{I, mod}$ a far too small value, with the consequence that the overall risk will be underestimated

7 Advantages and disadvantages

LOPA is a risk analysis method which fulfils the requirements according to the IEC 61511 [13] – described in part 1, clause 8 and 9. Therefore the risk and hazard that come out of a process can be evaluated according to clause 8. To those belong, among others, the determination of hazards and sequence of events, the process risks determination, the safety functions required to achieve the necessary risk reduction and the evaluation of safety instrumented functions that will be applied through the SIS. Further, with LOPA the descriptions in clause 9 of the IEC 61511 about "the classification of Safety Functions for Protection Layers" occur. LOPA is not a tool which helps finding errors, especially Common-Cause-Error", for this purpose one will perform an FMEA (Failure Mode and Effect Analyse) and its modified methods [4]. With LOPA one can indeed define the risk i.e. the risk reduction considering its severity. In most cases this indication is generally sufficient for simple safety structures. Also for more complex safety structures the LOPA is certainly better adapted as semi-quantitative method to define the risk as a qualitative risk analysis as for example the Risk Matrix. LOPA provides for a realistic risk evaluation and a more precise Analysis as it would be possible with the help of a Risk matrix, since more parameters can be taken into account. However, if one would define the risk more precisely with a mathematic formula, one would choose as a method of analysis a quantitative risk analysis, as for example with the Fault Tree or the Markov-Analysis. Considering the expenditure of time, one needs less time with a LOPA than with a quantitative Risk analysis, but more than with a proper qualitative analysis. This statement is valid for simple structures. For more complex structures LOPA would be very complex, since for each combination "Initiating event – Damages consequences" an analysis will be performed.
Another aspect that, in the choice of the method of analysis, must be taken into account is the question concerning the required risk reduction. Since using LOPA evaluations are necessary – also when tables of values exit one must always consider the real application –, for example one can make very optimistic evaluations by the initiating event's frequency. This means that a calculated risk reduction is too optimistic and that it does not achieved i.e. surpassed in reality the wanted necessary risk reduction. This is especially hazardous, when a high risk reduction is required because the consequences can be very severe. Therefore in such cases one should apply a quantitative method, i.e. with the help of the Markov-Model or the Reliability Block Diagram to define the failure probability. The IEC 61511 [13] notices that: "A qualitative method may be used as a first pass to determine the required SIL of all SIFs. Those which are assigned a SIL 3 or 4 by this method should then be considered in greater details using a quantitative method to gain a more rigorous understanding of their required safety integrity."
As for any other risk analysis method it is important that the hazardous scenarios should be compared to each other only when the LOPA has been consistently used.

As for any other risk analysis method it is important that the hazardous scenarios should be compared to each other only when the LOPA has been consistently used

8 Conclusion

LOPA allows performing a risk analysis in a process operating system. Thereby the initiating events and the given Protection Layers will be given and classified. The result is an evaluation of the Functional Safety. In this evaluation it will be define whether the requirements will be fulfilled according to the necessary risk reduction or if further protection measures, for example a SIS with a corresponding SIL will be necessary. Though the instructions to perform a LOPA are simple, one must know the respective applications very well during a risk analysis using LOPA. There, it is an advantage when a team, constituted of specialists skilled with special technical and safety knowledge of the implemented

technology also show understanding for the consequences of a damaging event.

A possible extension of the LOPA method which has been applied up to now, would be that the human influence during a risk analysis should be more analysed. At this stage some criteria would be created, which would precise and give a sense to the existing subjective evaluations concerning the evaluation of human influences. On the other side, the fact remains, fortunately, that a human being is not a machine.

If one compares the risk analyses which have been created with a LOPA between themselves, one can notice a few differences. This is a consequence of the subjective evaluation of damaging events, which are not listed in a table or are provisory evaluated by a company for intern specific needs regarding the application. Here are proper quantitative methods better appropriated, whereupon there can be a few differences in the figures used. Would LOPA be compared with another risk analysis method such as the HAZOP, one could see that they are both interesting. Both methods have their strengths and weaknesses. The method which seems the more appropriated to the application should be applied. Generally one can make the statement that qualitative, semi-quantitative methods complement one another, and should be applied for a risk analysis depending on the problem.

References:

[1] IEC 61508, International Standard 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Geneva, International Electrotechnical Commission, 2000.

[2] HSE, Health and Safety Executive, *Out of Control*, HSE Books, 1995.

[3] IEC 61511, International Standard 61511, *Functional safety – Safety instrumented systems for the process industry sector*, Geneva, International Electrotechnical Commission, 2003.

[4] J. Börcsök, *Functional safety systems*, Hüthig Verlag, 2004.

[5] www.osha.gov

[6] *Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen*, Amtsblatt Nr. L 010 vom 14/01/1997 S. 0013 - 0033.

[7] H. J. Pasman, *Risk informed resource allocation policy: safety can save costs*, Journal of Hazardous materials, Elsevier-Verlag, Jg. 71, pp. 375 - 394, 2000.

[8] Center for Chemical Process Safety (CCPS), *Guidelines for Safe Automation of Chemical Processes*, American Institute of Chemical Engineers, New York, NY, 1993.

[9] R. Gowland, *Practical experience of applying layer of protection analysis for safety instrumented Systems (SIS) to comply with IEC 61511*, Chemical Engineering Transactions, pp. 29 - 36, Vol. 5, 2004

[10] A. M. Dowell, III, *Layer of protection analysis: A new PHA tool after HAZOP, before fault tree analysis*, International conference and Workshops on Risk Analysis in Process Safety, CCPS/AIChE, 1997.

[11] A. M. Dowell, III, D. C. Hendershot, *Simplified risk analysis – Layer of protection analysis (LOPA)*, AIChE 2002 National Meeting, Paper 281a, 2002.

[12] Center for Chemical Process Safety (CCPS), *Layer of protection analysis, simplified process risk assessment*, American Institute of Chemical Engineers, New York, NY, 2001.

[13] IEC 61511, International Standard 61511, *Functional safety – Safety instrumented systems for the process industry sector*, Geneva, International Electrotechnical Commission, 2003.

[14] J. Börcsök, *Electronic safety systems, hardware conscepts, models and calculations*, Hüthig Verlag, 2004.

[15] DIN V 19250; *Grundlegende Sicherheits-betrachtungen für MSR-Schutzeinrichtungen*, Beuth Verlag, Berlin, 1994.

[16] P. Gruhn, H. L. Cheddie, *Safety Instrumented Systems: design, analysis and justification*, 2nd Edition, ISA – The Instrumentation, Systems and Automation Society, 2006.

[17] G. G. Young, G. S. Crowe, *Modifying LOPA for Improved Performance*, Proceedings of the 2006 ASSE Professional Development Conference, 2006.

[18] J. Börcsök, *Grundzüge der LOPA*, Invited lesson at BP Gelsenkirchen, Germany, 29.10.2007.

[19] F. P. Lees, *Loss Prevention for the Process Industries*, London, Butterworth and Heinemann, 1992.

[20] ISA-TR84.00.02-2002, Parts 1-5, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*, 2002.

[21] SINTEF Technology and Society, *OREDA, Offshore Reliability Data Handbook*, 4th Edition, 2002.