MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

17th Annual International Symposium
October 28-30, 2014 • College Station, Texas

On the Use of LOPA and Risk Graphs for SIL determination

Alejandro Torres-Echeverria
Risktec Solutions Inc.
1110 NASA Parkway, Suite 203
Houston, TX 77058

Abstract

Safety Integrity Level (SIL), as defined in ANSI/ISA S84.00.01 (IEC 61511-mod), is a widely used safety performance measure for safety instrumented functions. The standard ISA S84.00.01 suggests several methods for SIL determination, ranging from fully quantitative methods to fully qualitative methods. The large number of safety functions to evaluate during plant design and the need to integrate multidisciplinary design and operation knowledge to achieve effective risk reduction, has made necessary the use of multi-disciplinary-team workshop approaches.

Two widely used methods in the O&G industry for SIL determination are Layer of Protection Analysis (LOPA) and Risk Graphs. Each of these methods has their own advantages and disadvantages. LOPA allows the required risk reduction to be incorporated into the SIL values with higher precision. This enables a more detailed consideration of the available protection layers and leaves an objective traceable record of the decision-making process.

In contrast, the simplicity of Risk Graphs makes them convenient for screening a large number of safety functions. This can make Risk Graphs useful as a first screening pass prior to using LOPA. However, Risk Graphs are still widely used as a stand-alone method.

This paper seeks to explore the differences between LOPA and Risks graphs and to investigate whether the Risk Graphs method can provide the same level of SIL determination rigor as LOPA. The paper aims to determine if the simplicity of Risk Graphs can make that method more efficient for cases when the number of safety functions to evaluate is considerable.

Keywords

Safety Instrumented Systems (SIS), Safety Integrity Level (SIL), Layers of Protection Analysis (LOPA), Risk Graph

1. INTERNATIONAL STANDARDS' REQUIREMENTS

The international standard IEC 61508 [1] addresses the requirements for safety related system based on electrical, electronic and programmable electronic technology. This is a generic document, non-specific and relevant to a wide range of different sectors. The international standard IEC 61511 [2] was created as a derivation of IEC 61508 to cover specifically the process industry. Standard ANSI/ISA-84.00.01 "*Functional safety: Safety Instrumented Systems for the Process Industry sector*" edition 2004 [3] has adopted the standard IEC 61511 in its entirety with some minimal modifications. Therein, any reference to ISA-84.00.01 is equivalent to refer IEC 61511 and vice versa.

A Safety Instrumented Function (SIF) is a safety protective function implemented by a Safety Instrumented System (SIS), composed of any combination of sensor, logic solver and final elements (e.g. valves). A SIF must achieve a specific level of integrity, represented by the Safety Integrity Level (SIL). Notice that the SIS, and thus the SIFs, is independent from the plant control functions performed by the Basic Process Control System (BPCS).

Per ISA-84.00.01, definition of any SIFs must be based on a previous risk assessment. The risk assessment would determine the current level of risk presented by the facility. This would be compared against a tolerable risk level. The gap between the actual risk level and the tolerable risk is the required level of risk reduction (Fig. 1), also called the Risk Reduction Factor (RRF). The RRF is the relation of the actual risk presented by the facility and the risk that must be achieved as a target based on the acceptance criteria:

RRF = Actual Risk / Tolerable Target Risk

An important consideration is that the tolerable risk level to be used as baseline for risk assessment must be set by each individual organization specific to each process or facility as their Corporate Risk Criteria [Refs. 5, 6].

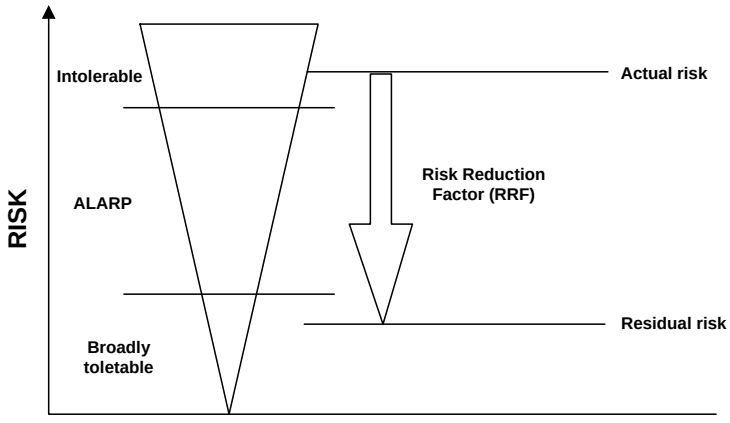

Figure 1. Risk Reduction Factor Concept

2. SAFETY INTEGRITY LEVEL CONCEPT

SIL stands for "Safety Integrity Level", which is a discrete performance measure that indicates the range of maximum acceptable probability of failure of a SIF to perform its intended function

upon a demand to do so. The SIL levels are defined in terms of the average Probability of Failure on Demand (PFD_{avg}) for systems working on demand mode of operation.

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{avg})	Risk Reduction Factor
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤100
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤1000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤10,000
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤100,000

Table 1. Safety Integrity Levels

3. SIL DETERMINATION METHODS

SIL Determination refers to the activity of selecting the required SIL for a SIF. SIL determination is usually done after the risk assessment has been performed and the SIFs required in the plant have been defined. There are several methods suggested in ANSI/ISA-84.00.01 (IEC 6511) and IEC 61508 for SIL determination. These methods go from quantitative, semi-quantitative to qualitative. The most rigorous and comprehensive methodology is based on a fully quantitative analysis (see IEC 61508 Part 5 Annex D [1], and ISA 84.00.01 Part 3 Annex B [4]), such as a Quantitative Risk Assessment (QRA). However, this method is not frequently used because it is resource intensive. Two widely used approaches in the Oil & Gas industry are Layers of Protection Analysis (LOPA), Risk Graphs and Safety Layer Matrix. The latter is briefly explained next, while LOPA ad Risk Graphs are fully described in Sections 4 and 5.

Risk Matrix. This is a qualitative method described in IEC 60508 Part 5 Annex G [1] and ISA 84.00.01 (IEC 61511) Part 3 Annex D [4]. ISA 84.01 calls it Safety Layer Matrix, while IEC 61508 names it Hazard Event Severity Matrix. This method is based on qualitative knowledge of the likelihood and consequences of hazardous events, as well as the number of layers of protection available. It is based on the assumption that each added protection layer provides a risk reduction of one order of magnitude. The matrix is presented Fig 2. The factors used in the matrix are:

- Severity rating
- Likelihood of the hazardous event
- Number of independent protection layers for the specific hazardous event.

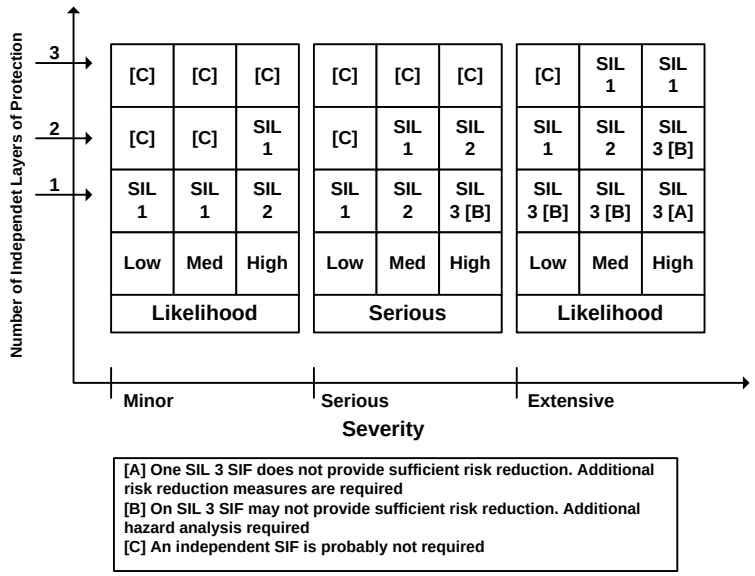

Figure 2. Safety Layer Matrix [Ref 4]

4. LAYER OF PROTECTION ANALYSIS (LOPA)

Layers of Protection Analysis (LOPA) is a simplified semi-quantitative risk analysis methodology. This method is presented in both IEC 6508 Part 5 Annex F [1] and ISA 84.00.01 (IEC 61511) Part 3 Annex F [4]. LOPA is described comprehensively in the CCPS book [Ref. 5]. The 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 existing independent protection layers (IPL). The resultant event likelihood is then compared against corporate risk criteria to determine the required additional risk reduction that would be provided by the SIF.

Figure 3 shows LOPA table example. The function of the table columns are described next.

1	2	3	4	5	6	7	8	9	10	11	12	13
Impact event description	Severity level	Initiating cause description	Initiation likelihood (freq per year)	Protection Layers (probability of failure)				Conditional Modifiers		Itermediate event likelihhod	Tolerable risk likelihood	Risk reduction factor
				Control system failure	Alarms & operator action	Other protection devices	Other mitigation measures	Occupancy factor	Probability of iginition			

Figure 3. Example of LOPA worksheet

- Accident event and the potential severity level (columns 1-2). These come from a previous hazard identification study; e.g. HAZOP, HAZID, etc.
- Initiating cause description and its likelihood (columns 3-4). The single cause of the hazardous event. The likelihood is usually expressed and frequency per year.
- Independent Protection Layer, IPL (columns 5-8). These columns include the protection layers to prevent or mitigate the accident event. An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independently

from the initiating event and any other layers of protection. An IPL must meet these conditions: 1) Must be effective in preventing the consequence; 2) independent from the initiating event (and other protection layers); and 3) auditable (its effectiveness must be capable of validation in some way).

- Conditional modifiers (columns 9-10). One of several probabilities included in scenario risk calculations that modify the frequency of the hazardous event having consequences.
- Intermediate Event Likelihood (column 11). The calculated frequency at which the hazardous event frequency would occur with all the IPLs in place (excluding the SIF which SIL is being determined).
- Tolerable risk likelihood (column 12). The likelihood corresponding to the specific event severity according to the corporate risk criteria.
- Risk Reduction Factor (column 13). This is the RRF to be achieved by the SIF (as discussed in Section 2), when calculating $PFD_{avg}=1/RRF$.

The analysis starts by recording the risk, severity and likelihood, of the initiating event of the hazardous scenario (columns 1-4). It then calculates the likelihood of this event by multiplying it by the probability of failure of the available IPLs (columns 5-8), and by the likelihood of enabling events and conditional modifiers (columns 9-10). Subsequently it compares the resultant risk likelihood (11) against the tolerable risk level (12) to determine if additional risk reduction measures are needed. If so, it evaluates the required level of risk reduction (RRF (12)).

LOPA is based on simplified assumptions regarding the numerical values of each of the components of the hazardous scenario. These simplifications are intended to be conservative [5]. The method allows to identify the layers of protection that are in place and to identify if additional layers of protection are needed. The risk of the hazardous scenario is approximated using orders of magnitude categories for each of the considered factors (IPLs, modifiers, etc.).

5. RISK GRAPH METHOD

The original Risk Graph is in principle a qualitative method. It was primary published in the standard DIN V 19250 [Ref. 6]. The method was subsequently included in IEC 60508 Part 5 Annex E [1] and ISA 84.00.01 (IEC 61511) Part 3 Annexes D and E [2, 4]. The Risk Graph method is described by some standards as qualitative [1] and by other as semi-quantitative [4]. There is, however, not substantial modification between the two graphs.

This method allows selection the SIL level by a simplified analysis based on the knowledge of the risk factors associated to the process and its control system [4]. The method consists of a tree-like graph where each stage represents one risk factor and the branches the different values that each factor can take. A Risk Graph intends to make a graded assessment a hazardous scenario based on a series of parameters that represent those risk factors considering that there is not a SIF in place. The SIL is worked out selecting each parameter from a pre-determined set of values. Figure 4 shows an example of Risk Graph from ANSI/ISA 84.00.01 Part 3 [4].

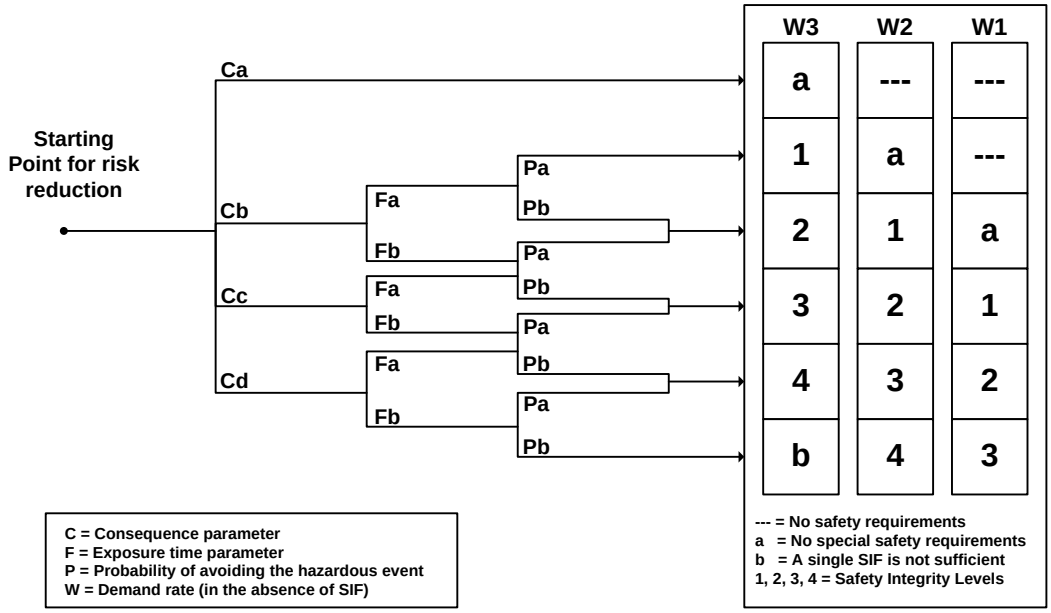

Figure 4. Risk Graph in ISA 84.00.01 (IEC 61511 Mod) Part 3 Annex D [4].

As defined by ISA 84.00.01 [4], the factors used in the graph are:

- Consequence factor C (severity). This parameter accounts for the potential number of fatalities and serious injuries when the area is occupied. It should consider the area affected by the hazard and the vulnerability of the personnel (i.e. C = No. People x Vulnerability).
- Occupancy factor F (frequency and exposure). Probability (based on fraction of time) that the exposed area is occupied at the time of the hazardous event. Typical values are: a) less than 10% of the time, and b) 10% of the time or more.
- Probability of avoiding the hazard P. This is assuming that all protection systems fail to respond. The likelihood of personnel being able to avoid the hazard is dependent on available IPLs alerting the exposed people, the ability to shutdown the process such that the hazard can be avoided or to enable personnel to escape to a safe area, and availability of means of escape. The parameter's value is actually the probability of failing to avoid the hazard.
- Demand rate W. This is the likelihood of the hazardous condition occurring in the absence of a SIF, usually in frequency per year. This is determined by including all failures that can lead to the hazardous event and estimating the overall rate of occurrence. The W factor should consider "external" (mitigation) risk reduction facilities.

The target SIL is determined by following the path as per the selected parameters. The value in the box under the W parameters (Fig. 4) indicates the target SIL. If the box shows an "a" there is no specific requirement for a SIL value. If the box shows a "b", this indicates that a single SIF is not sufficient to provide the required risk reduction.

The parameters of the graph can include numeric factors or just be qualitative. In any case, the values of the parameters should be derived by calibrating the Risk Graph against the corporate risk criteria. Calibration refers to assigning numerical values to each of the Risk Graph parameters. Thus, corporate risk criteria indicating risk tolerability levels would be embedded

into the calibrated graph parameters. Qualitative parameters' calibration is quite subjective and requires considerable judgment. When numerical values are assigned to the Risk Graph parameters, this becomes a semi-quantitative method (named a Calibrated Risk Graph in Ref [4]). Ref. [7] considers that a Risk Graph can be considered semi-quantitative only when it is properly designed and calibrated. Table 2 presents the example of calibration provided by ISA 84.00.01 [4]. This is a summary made by the author for this paper. Please refer to the original source for the full table.

Risk Parameter	**Classification**	**Notes**
(C) Consequence Related to No. of fatalities C = No. People x Vulnerability	▪ Ca - Minor injury ▪ Cb - Range 0.01 to 0.1 ▪ Cc - Range >0.1 to 1.0 ▪ Cd - Range >1.0	The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: • V = 0.01 Small release (flammable or toxic) material • V = 0.1 Large release (flammable or toxic) • V = 0.5 As above but also a high probability of catching fire or highly toxic material • V = 1 Rupture or explosion
(F) Occupancy	▪ Fa - Rare to more frequent exposure in the hazardous zone. Occupancy < 0.1 ▪ Fb - Frequent to permanent exposure in the hazardous zone	
(P) Probability of avoiding the hazardous event	▪ Pa - Adopted if all conditions in column 3 are satisfied ▪ Pb - Adopted if all the conditions are not satisfied	Pa should only be selected if all the following are true: • Facilities are in place which alert the operator that the SIS has failed • Independent facilities are provided to shut down, such that the hazard can be avoided or which enable all persons to escape to a safe area • The time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions.
(W) Demand Rate	▪ W1 - Demand rate <0.1D per year ▪ W2 - Demand rate ≥0.1D and <D per year	For demand rates higher than 10 D per year higher integrity shall be needed D is a calibration factor. The value of D is to be determined such that the Risk Graph results in tolerable level of residual risk, considering other

	▪ W3 - Demand rate ≥D and ≤10 D per year	risks to exposed persons and corporate criteria.

Table 2. Example Risk Graph Calibration from ISA 84.00.01 [4]

It is important to mention that this method does not take into account CCF (although neither LOPA does). The Risk Graph method is not suitable for demonstrating if residual risk has been reduced to a specific tolerable value.

For a properly calibrated Risk Graph, corporate risk criteria indicating risk tolerability levels is embedded (non-explicit) into the graph parameters, in contrast to LOPA where risk criteria is explicit. Qualitative parameters calibration is quite subjective and requires considerable judgment, which should be based on the corporate risk criteria, even if qualitative.

6. SIL METHODS AND PHASED APPROACHES

There is no a single approach that is appropriate for every SIL determination situation. Marszal et. al. [8] proposed a phase approach *that utilizes simpler techniques to screen lower risk operations and systematically progresses to more complex techniques to optimize the SIL selection process.* This approach uses three levels of screening, going from qualitative, semi-qualitative, to fully quantitative. The latter is for high risks with high SIS costs. ACM [9] defines the rigor of a method based how quantitative it is and its completeness for safeguards evaluation.

A fully quantitative technique provides a method that is explicit, a documentation framework that allows good traceability of the activities and the decision-making process, and a better system for lifecycle management [10]. A fully quantitative technique is, however, resource intensive. Other less intensive techniques, like semi-quantitative and qualitative ones require fewer resources and are simpler, but they may provide less rigorous and traceable processes.

Qualitative techniques, such as Risk Matrix and Risk Graph, tend to provide more conservative results (higher SIL). They have, however, not clear connection to tolerable risk levels. These techniques may *make the analysis easier; nevertheless the increment of costs for each SIF can be significant, tens of thousands of dollars, when increasing the SIL just one level* [11]. *Using a more comprehensive analysis upfront can provide important savings.*

It is under a phased approach that Risk Graphs are sometimes used for a first pass screening that allows analyzing a large number of safety functions. A second pass for the SIL-rated safety functions can be done using a more rigorous method. Gruhn [11], however, mentions that several main players in the Oil & Gas industry and chemical industry have a preference for LOPA. Also, ACM [9] believes that preference for the Calibrated Risk Graph method has waned and LOPA is becoming more popular, and that one factor driving this change is the growing needs of companies to have a more defensible numerical approach that satisfy stakeholders such as management and regulators. Dowell [12] highlighted that inconsistency in determining SIL

often comes from a lack of clarity for the frequency of the initiating cause and the target mitigated event frequency for which the risk is viewed and tolerable.

7. DISCUSSION ON LOPA

7.1. Advantages

LOPA is a more quantitative method than Risk Graph, which allows documenting all considered factors and the rationale of risk decisions, enabling traceability for proving due diligence. It is adequate for demonstrating that risk levels have been lowered to satisfy tolerable risk criteria.

LOPA facilitates the inclusion of all prevention and mitigation measures [13], providing a clearer picture of safeguards and initiating events [9]. In contrast, Risk Graph methods can incorporate mitigation measures, such as alarms and relief valves, only as additional adjustments [13]. LOPA includes its own calibration and facilitates the use of corporate criteria in a clear explicit way. Since it is more quantitative than Risk Graphs is then more precise, but less resource demanding than fully quantitative methods. Other authors [9] agree that LOPA is more rigorous and provides more defensible conclusions.

De Salis [7] believes that the Risk Graphs provided as examples in the IEC standards fail compared to LOPA. His argument is that LOPA enables to 1) define the frequency of the hazardous event, 2) as well as the likelihood of each available layer of protection; and 3) calculate the probability of the unwanted event with these layers of protection and then make an explicit comparison against the corporate risk criteria.

Summers [14] brings to attention how difficult is for a team to perform assignment of likelihood. This requires from the team to have a general understanding about the frequency of past incidents in the facility and the industrial group. Summers believes that LOPA to some extent eliminates this burden.

7.2. Drawbacks

As described above, LOPA has important advantages. Nevertheless, some authors have highlighted that LOPA still has some drawbacks. Compared to methods such as Risk Graphs, the method can be slower to be applied, time consuming and demand more resources on the assessment team [13]. The overall effort involved can be higher [9]. De Salis [7] comments that LOPA needs a specialist to execute the method, and also special skill is needed to source the likelihood numbers, discriminate which numbers to employ and format them. These figures are hard to find and require skills to be interpreted and converted. In addition, he believes that the numbers may be based on educated guesses and can give an illusion of accuracy, since the final answer only gives an order of magnitude assessment rather than an accurate calculation. He also states that one of the most significant drawbacks is that LOPA does not take into account Common Cause Failure between risk reduction measures.

8. DISCUSSION ON RISK GRAPHS

8.1. Risk Graphs published in IEC standards

Risk Graphs have became known to many people from IEC 61508/61511. It is worthy highlighting that the Risk Graphs shown in IEC standards are examples not intended to be used as they appear in the standard without further design and calibration [7]. These examples are not designed nor calibrated, nor even properly fully documented, as an assessment tool for specific cases. They do not have relation to any specific tolerable risk criteria or plant conditions case. ACM [9] agrees that, in general, step-by-step directions to perform all the (SIS lifecycle) steps are not explicitly contained in the IEC 61511 standard.

De Salis [7] analyzed the IEC 61508 Risk Graph. He criticized that the Risk Graph does not include the availability of most of the risk reduction measures (prevention and mitigation), nor the probability of failure of the BPCS. Since their action reduces the potential demand rate, hese would need to be included in the assessment of parameter W. Furthermore, the IEC 61508 Risk Graph has no separate parameter for the probability of presence in the danger zone. He believes that the simple range of the three columns W3, W2, W1 *is not enough to give sensible answers*.

8.2. Advantages

The simplifications inherent to the Risk Graph method actually constitute some of its advantages. The method is simpler to apply, and thus requires less time, making more amenable for application to analysis of a large numbers of SIFs (which is not uncommon in process plants). It is a graphic method that allows visualizing to some extent the mechanism of hazards unfolding into potential consequences.

8.3. Drawbacks

Baybutt, [15] considers that, overall, *conventional Risk Graphs are a simple but subjective way of determining SILs*. He finds that there are not well defined consistent standards or guidelines for the method. He highlighted some disadvantages such as: Factors such as enabling events and conditional modifiers are not considered; the parameters lump together several factors, which is difficult to visualize (such as the parameter F including frequency of presence in the hazard area and potential exposure time); some parameters being limited to only two values may give over conservative or over-optimistic results; definition of parameters can be misleading by not differentiating between frequency and probability units. In a subsequent paper [16] he added that the simplicity of risk matrices and Risk Graphs makes them appealing, but that, in contrast, they present some difficulties that discourage their use. These difficulties include they limited capacity for accommodating hazardous events, the calibration by allocating risk tolerance criteria is challenging and consideration of overall facility risk. The author considers LOPA and other more quantitative methods more capable of handling these issues.

Risk Graph is a coarser method than LOPA. Its results can be more inconsistent since much of the process is difficult to record and depends to great extent on the expertise of the team [10]. The assessment has to be adjusted in several ways to include consideration of existing protection and mitigation measures [13]. Risk Graphs are generally subjective when evaluating initiating events likelihood and frequency values. Furthermore, calibration and allocation of corporate risk criteria is challenging [16]. Corporate risk criteria has to be embedded implicitly in a Risk Graph. In contrast LOPA can use tolerable risk criteria in an explicit way.

8.4. Risk Graph conservatism

Baybutt [15] commented that Risk Graphs' emphasis on consequences can lead to domination of too conservative solutions. He considers that the parameters definitions (as provided by DIN V 1950 [6]) *are highly subjective and can lead to inconsistent results and possibly conservatism that may result in SIL overestimation*. De Salis [7] agreed that the IEC 61508 Risk Graph will usually provide SIL numbers that are higher than actually needed. Notice, however, this conservatism is an assumption that needs to be verified by ensuring that it gives conservative assessments indeed. The inherent uncertainty in the range of residual risk (in Risk Graphs) can be managed to produce a conservative outcome [13]. Some measures include *calibrating the graph so that the mean residual risk is significantly below the target, and selecting the parameter values cautiously, i.e. by tending to select more onerous range whenever there is an uncertainty*. Do not forget, in contrast, that this conservatism can incur a financial penalty in terms of higher SIL requirements. Per Gullad [13], Risk Graphs *must be calibrated on a conservative basis to avoid the danger they underestimate the unprotected risk and the amount of risk reduction required. Higher SIL requirements (i.e. SIL 2 or higher) can incur significant capitals costs (for rigorous engineering requirements and redundancy) and operating costs.* At the end of the day, high reliability functions are costly, and the reliability required commands a proportional cost [7].

8.5. Risk Graph Parameters

ACM [9] considers that the inherent nature of Risk Graphs is qualitative although some quantitative additions can complement them. Rating of parameters is usually made subjectively based on engineering judgment and experience. In addition, he states that the theoretical foundations of both methods have been questioned by some authors. Gulland [13] considers that Risk Graphs are very useful but coarse tools for assessing SIL requirements.

Summers [14] mentioned that in the Risk Graph method the likelihood (of the demand rate) and consequences can be determined by considering the independent protection layers during the assessment. The demand rate parameter W can accommodate prevention protection layers since they reduce the frequency of the initiating event, and the consequence parameter C can accommodate mitigation layers since they reduce the consequences of the hazardous event. Gulland [13] agreed that the C and W parameters are those mostly available to accommodate the graph calibration, since F and P are typically a two-range. A properly evaluated Risk Graph requires this extra effort by considering those protection layers implicitly to determine the C and W values. In contrast, LOPA makes consideration of these layers explicit and numeric, and thus clearer and less subjective. Additions to the Risk Graph method made to determine and record these factors add complexity and resources requirements, thus closing the gap with the LOPA resources demand.

Albeit layers of protection can be embedded mainly in the parameter W, consider, though, that estimating the demand rate W is actually one of the most notable difficulties of Risk Graphs [7]. De Salis emphasized that *the demand rate is a concept that is difficult for people to put numbers to when they are asked to say what its value is.* The demand rate *is the frequency with which the safety function has to act as last resort, which is not the same thing as the initiating event. It is actually the number of times per year that all other safety layers fail and the safety system actuates as the last resort.* In contrast, LOPA actually calculates the safety function's demand

rate [7]. *LOPA users are calculating the required probability of failure on demand without asking about the demand rate at all.*

8.6. Risk Graph calibration

Risk Graph requires being designed and calibrated in order to compete with LOPA. In contrast, LOPA does not require much more design and calibration, since it is a quite developed method as it stands in the CCPS book [5].

Although there is much criticism for Risk Graphs, De Salis [7] advocates that a well designed Risk Graph can provide a better assessment. He said that only a well designed and calibrated Risk Graph can deliver a proper semi-quantitative risk analysis, otherwise this only provides a very coarse risk assessment. He affirmed that a Risk Graph that is designed and calibrated with a sound method can actually compete with LOPA and deliver similar results. This may also eliminate the need for a phased approach (a first screening pass and then using a second method).

According to De Salis [7], **c**alibration in a Risk Graph entails to design a graph structure that include all relevant parameters, and allows their proper definition with the possibility of assigning them real values. The designer of the graph must consider how to ask the team sensible questions, against which they can give meaningful answers. The definition assigned to each parameter must *lead to the mathematical values to be used for that parameter*. Each of the parameters will provide pre-determined data values such that *the SIL requirement is determined as an order of magnitude final answer* (similar to LOPA, although LOPA explicitly provides the required RRF and PFDavg).

The process proposed by De Salis [7] for designing a Risk Graph is:

1) Choosing the right structure with sufficient parameters that allow a full assessment.
2) Define each parameter with and adequate range to allow the risk to be properly assessed.
3) Calibrate the answers.

9. ALTERNATIVE RISK GRAPHS

Some authors have developed enhanced alternative Risk Graphs. The approach and characteristics of these Risk Graphs are summarized below. The reader wishing to know further details is referred to the original sources of these works.

Baybutt [15] proposed an alternative Risk Graph that intends to use the same theoretical foundation as LOPA and QRA. The author mentions that this method can be used a first screening, and that those scenarios requiring a SIL rated risk reduction can be further analyzed using LOPA or QRA.

- This Risk Graph is focused on scenario risk rather than consequences. The graph starting point is the type of initiating cause rather than its consequences (similar to LOPA). These initiating cause categories are descriptive hazard scenarios provided for each value of the parameter based on frequency values. The frequency values are hidden (*not readily apparent to the analysts, but built into the table*).
- The parameters used are Initiating causes (I), Enablers and conditional modifiers (E), Safeguards (S) and Consequences (C).

- Passive and active safeguards are treated by a different rank in the S parameter (different PFD/risk reduction can be claimed).
- The values of the parameters are also based on order-of-magnitude values.
- The S parameter allows taking credit for up to two safeguards, being *a deliberately conservative approach since not all safeguards fail independently of each other* (i.e. CCF).

The alternative Risk Graph proposed by De Salis [7] is also based on the same principles as LOPA. It has the following features:

- It mixes the IEC Risk Graph and safety matrix features to include a more comprehensive set of parameters.
- It incorporates a parameter for including layers of protection into the assessment.
- Uses the potential SIS initiating event frequency instead of the safety system demand rate W. It is more feasible to assign values to the initiating frequency than to the final demand rate.
- Discards the visual linearity of IEC 61508/61511 Risk Graph. The graph is a step sequence rather than visually linear. The author considers that a truly linear Risk Graph is not visually linear, since this linearity is mathematically false, which has created confusion resulting in publications offering flawed Risk Graphs (such as IEC 62061).
- Is based on a calibration axis line that incorporates the tolerable risk value.
- Assign values that are kept as a record. Although the values are hidden from the user of the graph, a calibration record is kept.

De Salis emphasizes that the Risk Graph has to be designed/calibrated according to corporate practices and criteria for specific facilities.

10. A NOTE ON COMMON CAUSE FAILURE

As discussed above, one of the main pitfalls of LOPA is its failure to take into consideration Common Cause Failure. Nevertheless, CFF cannot be handled by Risks Graphs either. Ref. [7] says that for LOPA, either numbers can be adjusted to account for CCF when this is not significant, or discount one of the CCM layers in order to make a conservative assessment. In contrast, a Risk Graph makes the numbers used in the mathematics more rigid; unless the Risk Graph is specifically designed to allow application of CCF factors there is no means of adjustment. In any case the inability of including CCF is a drawback shared by both methods. Other quantitative methods, like Fault Tree Analysis, are required to quantify CCF.

11. CONCLUDING REMARKS

Risk Graph methods are intended to be simple and conservative. Compared to Risk Graphs, LOPA is considered, in general, more rigorous, more precise and more resource intensive. Since no single technique is adequate for every SIL determination situation, Risk Graphs are still considered a valid method.

Risk Graphs can be useful as a first screening tool in a phased approach, especially when a large number of safety functions needs to be analyzed. This would screen out safety functions that do not require being SIL rated. The SIL rated functions can then be re-assessed using a more rigorous method.

Risk Graphs tend to be more conservative than LOPA. Conservative results can entail a considerable financial cost, since SIL rated equipment is costly and require higher implementation, maintenance and inspection costs. In any case, the analyst must not just assume, but verify, that the Risk Graphs are calibrated to give results on the conservative side rather than not.

Risk Graphs presented by the IEC standards are examples not to be used un-calibrated. Risk Graphs must be designed and calibrated for the specific application in order to provide a proper risk assessment, what becomes even more important if the they will be used as a standalone method (rather than in a phase approach).

Risk Graphs can be improved by appropriate design and calibration, and complemented with an adequate documentation framework. This framework must record the design process, calibration rationale and discussions for decision-making. This has the potential to enable Risk Graphs to become closer to LOPA in rigor and results, but also equivalent in level of effort and resource needs. This extra effort may eliminate its inherent benefits of simplicity and lower resource requirements. It may necessary to evaluate if the effort will be cost-effective, for instance in cases where LOPA may require considerable higher resources for data gathering, conversion and interpretation.

Even properly designed, Risk Graphs do not allow demonstrating explicitly that the residual risk has been reduced to a specific tolerable value in accordance to the corporate risk criteria.

Risk Graphs and LOPA Methods share similar limitations regarding the the inability of including Common Cause Failure (CCF) quantification.

12. REFERENCES

1. IEC 61508. *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related systems, Parts 1-7, 2nd Edition*. International Electrotechnical Commission, Geneva, Switzerland, 2010.
2. IEC 61511. *Functional Safety - Safety Instrumented systems for the Process Industry Sector - Part 1: Framework, definitions, system, hardware and software requirements*. International Electrotechnical Commission. Geneva, Switzerland, 2003.
3. ANSI/ISA 84.00.01-2004 (IEC 61511 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements*. The International Society of Automation, North Carolina, USA, 2004.
4. ANSI/ISA 84.00.01-2004 (IEC 61511 Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels*. The International Society of Automation, North Carolina, USA, 2004.
5. CCPS. *Layer of Protection Analysis. Simplified Process Risk Assessment*. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 2001.
6. DIN V 19250. *Control technology: Fundamental Safety Aspects to be Considered for Measurement and Control Equipment*. German Institute for Standardization (DIN), Berlin, Germany. 1994.

7. De Salis, C. *Using Risk Graphs for Safety Integrity Level (SIL) assessment - a user-guide for chemical engineers*. The Institution of Chemical Engineers, UK, 2011.
8. Marszal, E. M., et. al. *Comparison of Safety Integrity Level Selection Methods and Utilization of Risk Based Approaches*. Process Safety Progress, 1999. 18(4): 189-194.
9. ACM Facility Safety. *SIL Determination Techniques Report*. ACM Automation Inc., 2006. White paper available online at http://www.iceweb.com.au/sis/ACMWhite-PaperSILDeterminationTechniquesReportA4.pdf.
10. Bhimavarapu, K., Stavrianidis, P. *Safety Integrity Level Analysis for Processes: Issues and Methodologies*. Process Safety Progress, 2000. 19(1):19-24.
11. Gruhn, P. *Different SIL (Safety Integrity Level) Selection Techniques can Yield Significantly Different Answers*. ISA Automation West, 2004.
12. Dowell III, A.M. *Layer of Protection Analysis for Determining Safety Integrity Level*. ISA Transactions, 1998. 37(3): 155-165.
13. Gulland, W.G. *Methods of Determining Safety Integrity Level (SIL) Requirements – Pros and Cons*. Practical Elements of Safety. Proceedings of the 12th Safety-Critical Systems Symposium, Birmingham, UK, February 2004. Redmill F. and Anderson T. (eds.), pp 105-122. Springer-Verlag, London, UK.
14. Summers, A. *Techniques for Assigning a Target Safety Integrity Level*. ISA Transactions, 1998. 37(2):95-104.
15. Baybutt, P. An *Improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs)*. Process Safety Progress, 2006. 26(1): 66-76.
16. Baybutt, P. *The Use of Risk Matrices and Risk Graphs for SIL Determination*. Process Safety Progress, 2013. 33(2):179-182.