Use of Simplified Risk Assessment Methodology in the Process Industry

Mardy Kazarians[a]*, **Kirk Busby**[a]
[a] Kazarians & Associates, Inc., Glendale, United States of America

Abstract: The process industry, which includes chemical processing and manufacturing, and petroleum refining, has used various risk assessment methods for at least four decades. Over this time, the methodologies employed have evolved considerably from qualitative approaches [e.g., Hazard and Operability (HAZOP) study] to Quantitative Risk Analysis (QRA), which uses a detailed evaluation of the risk. A simplified approach to risk assessment, known as Layer of Protection Analysis (LOPA), has been developed in the last twenty years and is widely used in the process industry today. LOPA is a simplified risk quantification method which is used to estimate risk and identify effective system improvements in a consistently. The LOPA methodology and supporting data is discussed in this paper. Examples from the industry are provided to demonstrate how the methodology is applied. The various rules established by industry sources and large corporations are summarized and their merits are discussed. Potential pitfalls in applying the LOPA methodology to safety risk decision making are also discussed.

Keywords: Simplified Risk Analysis, Layer of Protection Analysis (LOPA), Chemical Processing

1. INTRODUCTION

The process industry, which includes chemical processing and manufacturing and petroleum refining, has used various risk assessment methods for at least four decades. Over this time, the methodologies employed have evolved considerably. Initially, qualitative approaches were used. The most common approach was the Hazard and Operability (HAZOP) study [1], in which a team of experts conducted brainstorming sessions to identify potential hazard scenarios. To discriminate among safety risk scenarios, the team used their personal experiences and understanding of the safety risks to estimate the likelihood and severity of each scenario. Using a risk matrix, the severity and likelihood estimations were combined to arrive at a risk ranking, which could determine whether the team must recommend changes in system design and operational conditions to improve safe operation.

These methods relied heavily on the team's understanding, experience and judgement, which sometime led to inconsistencies among studies in defining the safeguards that influence individual chains of events and understanding the effectiveness of each safeguard. Additionally, it was unclear whether sufficient safeguards were in place to reduce the likelihood of occurrence of a postulated scenario to an acceptable level.

A simplified risk assessment methodology known as Layer of Protection Analysis (LOPA) has been developed to overcome these pitfalls and provide a consistent decision-making tool to identify safety risks and effective system improvements [2]. LOPA is a risk quantification method, often using order of magnitude values for the various parameters that influence risk. By applying the LOPA methodology, the owners and operators of a process can determine whether they have sufficient layers of protection for postulated scenarios. If it is concluded that the layers are insufficient, LOPA assists the analysts to define the scope of the needed safeguard, by establishing the necessary reliability of automatic shutdown systems or other protection layers. Because of this and to ensure consistency, many large corporations have developed their own internal rules for conducting LOPA for their processes.

* Email: mkazarians@kazarians.com

The LOPA methodology, its history, and supporting data are discussed in this paper. In Section 2, the history of risk assessment in the process industry is discussed, along with some of the pitfalls which led to the need for LOPA to be developed. In Section 3.1, background is given on the development of the LOPA methodology, and in Section 3.2 the LOPA methodology itself is defined. Section 3.3 discusses the order-of-magnitude approximations in LOPA, and the uncertainty introduced by their use. Finally, Section 3.5 discusses the usage of LOPA within the chemical process industry, and some of the limitations of the methodology.

2. RISK ASSESSMENT HISTORY IN THE PROCESS INDUSTRY

Risk assessment has been an evolving field within the process industry. As a response to major incidents in the early 1980s, the American Institute of Chemical Engineers (AIChE) established the Center for Chemical Process Safety (CCPS) in 1985 in order to analyze and discuss methods for chemical accident prevention. The first project completed by the CCPS was the publication of the first edition of *Guidelines for Hazard Evaluation Procedures* [1]. The methodologies presented by the CCPS, and those which were predominantly used in the process industry, were all qualitative in nature. The most common methodology is the Hazard and Operability (HAZOP) methodology, which was developed in the late 1960s, and is still in common use today.

The HAZOP methodology is based on the notion that deviations from design intent have the potential to cause an adverse condition [1]. It was discovered that if a standard set of seven guidewords are applied to each design parameter (e.g., temperature), all relevant deviations of the parameters can be identified. Table 1 provides the standard set of guidewords with example applications for four design parameters (e.g., No Flow, Higher Temperature, etc.). These deviations are used to systematically identify hazard scenarios throughout the process under review.

Table 1: Examples of Parameters Deviation Matrix

		Guidewords						
		No	**Less**	**More**	**Part of**	**As Well As**	**Reverse**	**Other Than**
Parameters	**Flow**	No Flow	Less Flow	More Flow	Misdirected Flow Out	Misdirected Flow In	Reverse Flow	Integrity Failure
	Temperature	N/A	Lower Temperature	Higher Temperature				
	Pressure	N/A	Lower Pressure	Higher Pressure			Vacuum	
	Level	No Level	Lower Level	Higher Level				

It is common to divide a process into *nodes* (segments) based on specific function of that part of the process. A set of design parameters are examined for each segment and the standard guidewords are applied to them to arrive at potential deviations. For each deviation of a node, the causes and consequences are identified, to generate a list of the potential hazards presented by the process. It is common to limit the cause to the node itself and to take the ensuing chains of events to a final conclusion to identify the worst case adverse conditions regardless of the node boundaries. To identify the worst outcome, it is also common to assume that none of the existing safeguards are functioning or are in place.

HAZOP uses a team of experts in brainstorming meetings facilitated by a HAZOP leader to review a process and identify potential cause and consequences scenarios. Existing safeguards are identified for all scenarios that can lead to an adverse condition. Safeguards are features that can mitigate or minimize the safety, environmental, or major asset damage concern.

Once a potential scenario of concern is identified, a risk ranking process is used to determine whether the scenario presents a significant risk to the facility, and whether additional safeguards or design modifications are necessary for a given event. In HAZOP, the risk ranking process is normally fully qualitative [1]. Typically, a risk matrix is used (see Figure 1 for an example) in which the severity and likelihood pair of the event are assigned a risk ranking (e.g., *Marginal*). The risk ranking is used to determine whether the risk presented by a scenario can be considered tolerable as-is, or whether additional protection features are required. Figure 1 provides an example of a risk matrix that has been used at a number of facilities. Figure 1 provides a set of definitions of various risk variables (i.e., consequence severities and likelihoods) and the risk matrix. Each consequence severity and likelihood pair is ranked in terms of "Critical", "Undesirable", etc. The required action for each ranking level is also provided.

A risk matrix is a decision-making tool. It is common practice that it is developed at the corporate level and all facilities and operations of the company use the same matrix to determine the risk level of the scenarios identified in their HAZOP studies.

The assignment of severity and likelihood rankings, and the resulting risk level, is fully dependent on the judgement of the risk assessment (HAZOP) team. Typically, some form of guidance is provided to ensure consistent evaluation of the risk, but the decisions regarding the risk level are ultimately influenced by the experience and understanding (i.e., understanding of the design features of the process) of the individuals conducting the study. This has the potential to lead to significant inconsistencies among similar scenarios in different studies, or even those within the same study. These inconsistencies in risk ranking can lead to significant discrepancies between facility designs, as some studies may lead to recommendations to add or modify safeguards, while others may indicate that such measures are not needed. Additionally, when using qualitative risk criteria, it is difficult to establish the necessary reliability of new or existing safeguards, as no concrete measure of their effectiveness is available.

In instances where a more thorough understanding of risk is required, Quantitative Risk Analysis (QRA) has been used in the process industry for specific applications. Rooted in the nuclear and aerospace industries [3], QRA provides a more rigorous framework for risk analysis. In QRA, risks are identified and evaluated using probabilistic methods to determine the frequency of occurrence. While QRA is capable of providing detailed quantitative results, the methods involved require large investments in time and manpower to complete. Typically, QRA is only used in the process industry for special circumstances, when a highly detailed risk analysis is required.

3. LAYER OF PROTECTION ANALYSIS (LOPA)

3.1. Background and Development

In order to avoid the inconsistency inherent in qualitative risk assessment without the large diversion of resources required for a detailed quantitative risk assessment, and to have clear and consistent bases for recommending additional safeguards, various simplified methods were proposed. The most widely-used simplified approach, as noted above, is LOPA [2]. Evolving from similar early methods developed in the 1990's, LOPA is a tool which uses specific risk tolerance criteria to determine the adequacy of existing safeguards, and the required reliability of additional safeguards proposed as a result of the analysis [2].

The CCPS published *Layer of Protection Analysis – Simplified Process Risk Assessment* [2] in 2001 to define and outline the key features of LOPA studies. Since that time, LOPA has been adopted by numerous large chemical facilities to augment their existing risk assessment studies and to have a common and consistent basis across different facilities and operations to identify risk gaps and to propose plant modifications to close the gaps. Recently, in October of 2015, regulatory updates in the State of California have mandated that all petroleum refineries in the state must perform LOPA (or a similar methodology) as part of all hazard analyses conducted at their sites [4].

Figure 1: Example Risk Matrix

Consequence Severity Categories

Category	Safety	Environmental	Economic
A	Multiple fatalities	Major release requiring multiple years to remediate	>$500 million
B	Single Fatality	Major release requiring a year to remediate	$100-500 million
C	Permanent Partial Disability	Release requiring months to remediate	$30-100 million
D	Recordable Injury	Release requiring days to remediate, repeat permit violation	$10-30 million
E	First Aid Injury	Environmental permit violation	$2-10 million

Likelihood Categories

Category	Occurrence	Description
1	$\geq 10^{-1}$ per year	Likely – Expected to occur multiple times in the life of the facility
2	$\geq 10^{-2}$ per year	Moderately Likely – May occur once in the life of the facility.
3	$\geq 10^{-3}$ per year	Unlikely – May occur once when the life of 50 similar facilities is considered.
4	$\geq 10^{-4}$ per year	Very Unlikely – Known to have occurred within the industry.
5	$<10^{-4}$ per year	Improbable - Has not occurred in the industry or has occurred, but current safeguards make the event less likely

m

Example Risk Matrix

		Likelihood				
		5 (10^{-5})	4 (10^{-4})	3 (10^{-3})	2 (10^{-2})	1 (10^{-1})
Severity	A	Marginal	Undesirable	Undesirable	Critical	Critical
	B	Marginal	Marginal	Undesirable	Undesirable	Critical
	C	No Action	Marginal	Marginal	Undesirable	Undesirable
	D	No Action	No Action	Marginal	Marginal	Undesirable
	E	No Action	No Action	No Action	Marginal	Marginal

Risk Category Definitions

	Required Action
Critical	For an operating system, management shall consider shutting the system down until proper measures are implemented that will reduce the risk to “Marginal” level or better.
Undesirable	Measures shall be implemented that will reduce the risk to “Marginal” level or better.
Marginal	Those risk reducing measures that do not severely impact the economics of the business may be considered for implementation.
No Action	This risk level is tolerable. No further action required.

3.2. LOPA Methodology

LOPA is an analytical tool for estimating the risk and assessing the adequacy of protection layers used in mitigating process risks. It is relatively simplistic in nature, in that while frequency and probability values are established using industry and manufacturer data, they are used in LOPA as order-of-magnitude approximations to maintain simplicity in the analysis. The goal of LOPA is to determine whether an event has sufficient independent protection layers to meet the risk target specified for that event.

LOPA is not a hazard identification tool, meaning that it must be used in conjunction with another methodology (such as HAZOP) to generate the hazard scenarios to be evaluated. Once the scenarios of interest have been determined, each is reviewed in specific detail according to the following general steps:

1. Establish Target Event Frequency (TEF)
2. Estimate Initiating Cause Likelihood (ICL)
3. Establish Enabling Events (e.g., time at risk)
4. Establish Conditional Modifiers (e.g., ignition probability)
5. Identify the existing safeguards for each initiating cause and establish Independent Protection Layers (IPLs)
6. Estimate Probabilities of Failure on Demand (PFDs) for the IPLs.
7. Calculate the Mitigated Event Frequency (MEF)
8. Compare with Risk Target

Each step is further discussed below. The steps are conducted by a team of experts in a brainstorming session, similar to HAZOP, who are familiar with the design and operation of the system under review. The session is led by an expert in the LOPA methodology itself.

3.2.1. Target Event Frequency (TEF)

A risk target, or Target Event Frequency (TEF), is established by a decision-making body (e.g., corporate management). It is common that the risk matrix, discussed above, is used for this purpose. Corporate management may stipulate that all scenarios that fall in a risk matrix bin that is not acceptable (e.g., other than *green* and *blue* in Figure 1) must be considered for additional measures to reduce the risk to an acceptable level (e.g., *green* and *blue* in Figure 1).

Table 2: Example Target Event Frequencies (TEF)

Consequence Severity	TEF (per year)
A (most severe)	1×10^{-5}
B	1×10^{-4}
C	1×10^{-3}
D	1×10^{-2}
E (least severe)	1×10^{-1}

As it can be seen in Figure 1, TEF depends on the consequence level. For example, in the case of Consequence Category B, the management may stipulate that the likelihood of scenarios, that is TEF, should be less than 10^{-4} per year. Therefore, for each scenario, based on the severity assigned to the consequence as part of the hazard identification process, the applicable TEF should be established prior to the initiation of LOPA. The TEF is expressed in units of events per year and determines the allowable frequency of occurrence for an individual scenario of a given severity level. It will determine the number of protection layers necessary to adequately mitigate a risk to the tolerable range. As noted earlier, the TEF is established based on the individual risk tolerance of the company for which the study is being performed. Table 2 presents a typical example of Target Event Frequencies. Note that the example provided in Table 2 follows the order-of-magnitude structure.

3.2.2. Initiating Cause Likelihood (ICL)

Each initiating cause of a hazard scenario of interest is assigned a frequency of occurrence (in terms of events per year as noted above). This frequency is called “Initiating Cause Likelihood” (ICL). These causes must be clearly defined single failures, operator action (often error) and events, such as valve malfunction, equipment failure, or individual human error. Each ICL, in principal, should be estimated based on the specifics of the postulated event. However, in practice, often corporate management provides a suggested list of events and their suggested frequencies. The person responsible for a specific LOPA must justify deviations from the suggested values. The suggested values are generally expressed in terms of orders of magnitude. Examples are provided in Table 3, which contains a list of common ICL values [5].

Table 3: Examples for Initiating Cause Likelihood (ICL) Values

Event	ICL (per year)*
BPCS Control Loop Failure	0.1
Human Error (action performed more than once per month)	0.1
Human Error (action performed less than once per month)	0.01
Pressure Regulator Failure	0.1
Pump or Compressor Failure	0.1
Localized Loss of Power	0.1
Single Check Valve Failure	0.1
Dual Check Valve in Series Failure	0.01

*Adopted from Reference 5.

3.2.3. Enabling Events

Enabling events are factors that address conditions that make the initiation and progression of a scenario possible. The most common example is the time at risk factor, which stands for the fraction of the time that a system is operated in a specific configuration, or under a specific condition. For example, if a vessel is in use only one month out of every two years and it is not operated the rest of the time, the *time at risk factor* for this vessel becomes 1/24 = 0.04. To match order-of-magnitude protocol, a time at risk factor of 0.1 would be included in LOPA. Another common example is an operator error during start-up. For example, operators may be trained to not re-introduce fuel gas if the firebox of a fired heater is not adequately purged. An additional factor of 0.1 captures the possibility of an error by operators when relighting a furnace.

3.2.4. Conditional Modifiers

Conditional modifiers are used to establish the probability that an event or condition exists during the course of an event which allows the event to progress to its hazardous endpoint. The two most common conditional modifiers are:

- Occupancy Factor
- Ignition Probability

Occupancy Factor – This factor is the conditional probability that, given a release has already occurred, there would be a person within the hazard zone of the release. In a large operating facility, a fire or a release of hazardous chemical does not necessarily mean that personnel will be in the hazard zone during an event. This is specifically true for parts of a facility where access is strictly controlled (e.g., near a flare tower). For scenarios in which an occupancy factor is taken, the hazard zone is evaluated to determine the probability someone would be present within the hazard zone.

Ignition Probability – This factor is the conditional probability that, given a release of flammable material has occurred, an ignition source is encountered that initiates a fire. Various ignition probabilities may be taken, and can be calculated based on the type of material released, quantity released, electrical classification of nearby equipment, etc. Ignition probability is generally not taken when a large release of volatile hydrocarbons occurs, as it is expected that the size of the resulting vapor cloud would lead to an ignition at some point during the vapor dispersion.

3.2.5 Independent Protection Layers (IPLs)

Identifying Independent Protection Layers (IPLs) and quantifying their failure probabilities are one of the most important tasks in the LOPA process. To determine which safeguard qualifies as an IPL, the safeguard must meet a set of specific criteria. The criteria for IPLs has evolved over the years. The number of criteria has expanded from an original set of three [2] to the current seven [5]:

- *Independence:* The safeguard must be independent of all other safeguards credited as IPLs, as well as the initiating cause. Typically, demonstrating independence is one of the more difficult and time-consuming aspects of initial IPL identification, and the one that is the most discussed during LOPA sessions. Devices which share the same transmitters, computers, or in some cases, the same service, may not be sufficiently independent of each other to be credited as IPLs. Detailed analysis of instrumentation architecture may be necessary to determine whether two devices can be considered sufficiently independent.
- *Functionality:* The safeguard must be capable of totally preventing or mitigating the postulated consequence. It must be capable of detecting an upset condition and acting quickly enough to prevent the process from reaching an unsafe state.
- *Integrity:* The safeguard must be designed and maintained to reduce the risk by a known risk level. The minimum necessary risk reduction is defined during the LOPA process. Each IPL must be capable of meeting the Probability of Failure on Demand (PFD) as described below.
- *Reliability:* The safeguard must respond in a consistent manner to process upsets. Reliability ensures that the safeguard is in place and active whenever it may be needed (i.e., minimal outages for maintenance, bypass, etc.), and that it will not activate spuriously when not needed.
- *Auditability:* The safeguard can be tested periodically to ensure that it is functioning as intended.
- *Access Security:* The safeguard is protected by physical or administrative controls which prevent unauthorized changes to the configuration, which could render the safeguard ineffective. Software setpoint changes or physical security devices are examples of measures which may be taken to prevent unauthorized change.
- *Management of Change:* The safeguard is part of a formal configuration control (Management of Change) program, to ensure that all system changes are rationalized and fully documented. Proposed changes must be reviewed with all applicable levels of the organization (e.g., operations, engineering, management, etc.) to ensure that changes are well understood, and their potential impacts on the proposed IPL are documented.

Those safeguards that meet all seven criteria may be listed as IPLs for a given scenario. These IPLs represent the significant risk prevention measures present within the system. Given their importance to safe operation, and to meet the criteria of *Integrity* and *Reliability*, identified IPLs are often included in critical equipment lists to ensure high priority in maintenance and inspection.

3.2.6 Probabilities of Failure on Demand (PFDs)

Each device credited as an IPL must be assigned a Probability of Failure on Demand (PFD). The PFD is a measure of the reliability of the IPL, and quantifies the probability that the device will fail to perform its intended safety function when a scenario requires it to act. PFDs are based on industry data, manufacturer data and facility experience with the specific device or system. Similar to the ICLs, it is common for corporate management to provide suggested values and the person responsible for LOPA must provide justification if they deviate from those value. Also, similar to ICLs, it is common to express them at order of magnitude level. Examples of PFDs of typical devices can be found in Table 4[5].

Table 4: Common Probability of Failure on Demand (PFD) Values

Event	PFD*
Safety Interlock	0.1
Spring-Operated Pressure Relief Valve	0.01
Dual Spring-Operated Pressure Relief Valves	0.001
Check Valve	0.1
Human Response to an Abnormal Condition	0.1

*Adopted from Reference 5

3.2.7. Mitigated Event Frequency (MEF)

Mitigated Event Frequency (MEF) is the frequency at which a given hazard scenario will proceed all the way to the worst-case consequence, given the protection layers in place to prevent that scenario. Once the ICL, frequency modifiers (i.e., enabling events and conditional modifiers), and the PFDs are estimated, the MEF can be calculated using the following formula:

$$MEF = ICL \times FM \times PFDs$$

Where:

MEF = Mitigated Event Frequency (events per year)
ICL = Initiating Cause Likelihood (events per year)
FM = Product of applicable frequency modifiers (e.g., time at risk, occupancy factor, etc.)
PFDs = Product of the PFDs for each IPL identified in the scenario

3.2.8. Meeting Risk Target

The final step in the LOPA process is to compare the MEF of a hazard scenario with the target frequency (TEF). This will determine whether the current system design is considered adequate or there is a risk gap, that is, whether additional features must be considered to reduce the risk. The LOPA Ratio is a tool that is often used for this purpose. The LOPA Ratio is calculated as:

$$LOPA\ Ratio\ = TEF/MEF$$

Using this formula, a LOPA Ratio less than one indicates that there is a risk gap and there are insufficient protection layers to prevent the postulated event. A LOPA Ratio greater than or equal to one indicates that the risk target has been met, and according to the management guidelines no additional layers are required. If additional protection layers are deemed necessary, the LOPA ratio also indicates the level of reliability which those additional layers will be required to meet. For example, if LOPA Ratio = $10^{-4}/10^{-2}$ = 0.01, then the recommended safeguards should collectively have a PDF = 10^{-2} or smaller.

3.3. Order of Magnitude Approximation

When conducting LOPA, common practice is to utilize order-of-magnitude approximations for all values included in the LOPA calculation [2]. This practice has been adopted by several large corporations because it allows them to provide a consistent value of the various parameters of LOPA across all operations and facilities. It also provides some level of assurance that all risk estimations are generally conservative. It also reduces the need to expend resources in evaluating the risk in a greater level of detail than order of magnitude, which in most cases would not make a significant difference in the final decisions.

Because often LOPA is used to establish the level of protection layer necessary to adequately close the risk gap of a given scenario, order of magnitude approach creates a simplistic method to easily determine the number of protection layers (expressed in terms of orders of magnitude) in place or needed to be proposed that meets the risk criterion. Additionally, the order-of-magnitude approach allows the study to use values that approximate the industry or operational experience, without the rigor required for a thorough QRA.

Use of the order-of-magnitude approach does introduce additional uncertainty into the risk estimation. However, typical practice is to ensure that values always default to the more conservative magnitude. For example, in the event that failure history data indicates that an IPL has a PFD of approximately 0.07, the order-of-magnitude approximation would still conservatively estimate the PFD as 0.1 for the purposes of LOPA. This conservative approach ensures that facility risk tolerance will be met for all scenarios which pass LOPA and of course it introduces the possibility of recommending additional safeguards when lesser ones would have been sufficient.

3.4. Usage and Limitations

Given its ease of use and relatively consistent results, LOPA has become one of the most commonly used tools in the process industry for evaluating process risk. Typically, LOPA is used to supplement a hazard identification process such as HAZOP. Companies may choose to perform LOPA on a specific subset of scenarios identified in the HAZOP, such as those which have been assigned a high severity ranking, or those which the study team feels require additional evaluation beyond simple qualitative analysis. To facilitate the study, and to maintain consistency between studies, many companies have chosen to develop internal LOPA guidance standards, which dictate corporate policy on items such as event frequencies, acceptable IPLs for specific scenarios, and typical severity rankings for common events.

As mentioned in Section 3.2, LOPA is often used to establish the reliability requirements for additional safety features recommended as a result of the analysis. Installation of Safety Instrumented Functions (SIFs) [6] is common practice in the process industry to address high severity safety risks. SIFs are instrumented trip functions which are independent of all other control and monitoring equipment, and which are designed and maintained to ensure they meet a specific reliability level. The reliability level is referred to Safety Integrity Level (SIL).

The International Society of Automation (ISA) provides specific guidance and standards on how to designate a system as an SIF and how to establish its SIL level. ISA has defined several SIL levels [6] that are based on order of magnitude spans (i.e., 0.1, 0.01 and etc.). LOPA is recognized as an effective tool for establishing the SIL level required to meet the target frequency (i.e., TEF). After LOPA has been conducted, the size of the remaining gap between the MEF and the TEF can be used to establish a SIL rating for a proposed device. For example, in the event that a scenario results in a LOPA Ratio of 0.01, the proposed SIF will be required to be designed to meet a PFD of 0.01, which is referred to as SIL2.

These benefits, coupled with the relative ease of use, have made LOPA into an integral part of risk assessment process in the chemical industry. However, there are some limitations to the methodology that the users must understand. These limitations are briefly noted below:

- There are a few types of scenarios for which the LOPA methodology may not provide meaningful results. For example, given their nature, corrosion issues are difficult to address through LOPA. Although industry data can be used to establish the frequency of occurrence of a given corrosion mechanism, most protection layers against corrosion (i.e., inspection activities) will not fulfill the criteria to be Independent Protection Layers. Therefore, most corrosion issues which could lead to a significant safety concern will not be able to pass LOPA, despite the fact that inspection and maintenance activities may provide sufficient protection against such events.

  There are a variety of scenario types which have similar issues to the example given above. In these instances, companies may choose to rely on qualitative methods, or they may choose to perform in-depth QRA to accurately determine the risk of such events. Another example of cases not subjected to LOPA include natural hazards such as severe flooding. When preparing to conduct a LOPA study, it is critical to define the scope of the analysis beforehand, including which scenario types will not be addressed using the methodology, and how to go about assessing the risks they present.

- Time at risk is often not considered in the decision process. In other words, if under certain operating conditions, the level of safeguards in place is in adequate, the management considers that situation as unacceptable regardless of the fraction of time that a system is operating in that mode.
- Common cause events need to be incorporated into the probability and frequency evaluations. For example, if redundant devices are credited in a scenario, their joint probability of failure on demand should include the possibility of failure of the redundant devices due to the same cause.
- Comparison of single scenarios MEF with TEF may not provide a broader picture of the risk. Operators should be aware of the various scenarios that use the same set of safeguards to meet the TEF. If a relatively large number of scenarios require the same set of safeguards, the SIL level of that set may need to be made more stringent.

4. CONCLUSION

The process industry has used various risk assessment methods for at least four decades to understand and mitigate potential safety and other risks. Over this time, the methodologies employed have evolved considerably. Initially, qualitative approaches were used. The qualitative approaches provided valuable insights but were deficient in consistently providing the bases to identify risk gaps and ensuring that sufficient safeguards have been considered.

Layer of Protection Analysis is a simplified method for risk assessment that has proven to be a useful tool in providing a robust basis to identify the levels of risk gap. Results of LOPA can be used to recommend sufficient features to close the gaps. Its simplistic nature minimizes discrepancies between different study teams. It allows for clear quantification and analysis of the existing and added protection layers which act to prevent hazard scenarios. Because of these benefits, LOPA has been adopted for use throughout process industry, particularly by the petroleum refining. Companies have made LOPA an integral part of their facility risk assessment policy, and have developed specific guidance on proper methods to conduct the analysis. The use of LOPA at these facilities has led to improved understanding of the reliability of existing protection layers and has provided a rational basis for recommendations to improve facility design for added safety.

References

[1] Center for Chemical Process Safety of the American Institute for Chemical Engineers, *Guidelines for Hazard Evaluation Procedures,* Third Edition, CCPS, 2008, New York, NY.

[2] Center for Chemical Process Safety of the American Institute for Chemical Engineers, *Layer of Protection Analysis – Simplified Process Risk Assessment,* CCPS, 2001, New York, NY

[3] Center for Chemical Process Safety of the American Institute for Chemical Engineers, *Guidelines for Chemical Process Quantitative Risk Analysis,* Second Edition, CCPS, 2000, New York, NY.

[4] California Code of Regulations, Title 8, Division 1, Chapter 4, Subchapter 7, Group 16, Article 109, Section 5189.1 *Process Safety Management for Petroleum Refineries.* Revised September 26, 2017.

[5] Center for Chemical Process Safety of the American Institute for Chemical Engineers, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis,* CCPS, 2015, New York, NY.

[6] ANSI/ISA-84.00.01-2004 Part 3, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels*. ISA, 2004, North Carolina.