Pitfalls of Using the Wrong Risk Matrix
In PHA and LOPA

Kirk Busby
Kazarians & Associates, Inc.
100 West Broadway
Glendale, CA 91210
Kirk.Busby@kazarians.com

Mardy Kazarians
Kazarians & Associates, Inc.
100 West Broadway
Glendale, CA 91210
mkazarians@kazarians.com

Prepared for Presentation at
American Institute of Chemical Engineers
2018 Spring Meeting and 14th Global Congress on Process Safety
Orlando, Florida
April 22 – 25, 2018

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

Pitfalls of Using the Wrong Risk Matrix In PHA and LOPA

Kirk Busby
Kazarians & Associates, Inc.
100 West Broadway
Glendale, CA 91210
Kirk.Busby@kazarians.com

Mardy Kazarians
Kazarians & Associates, Inc.

Keywords: Hazard Identification and Risk Analysis, Risk Matrix, Process Hazard Analysis and Layer of Protection Analysis

Abstract

A Process Hazard Analysis (PHA) is an important tool for identifying and managing the hazards associated with a chemical process. Hazards may include safety issues, environmental impacts, business impacts, or reputational issues. It is now common to use a risk ranking scheme to discriminate among the potential hazard scenarios so that resources to reduce risk are allocated on a rational basis. Additionally, the PHA methodology has been extended to Layer or Protection Analysis (LOPA), which allows quantification of risk gaps based on a consistent methodology and industry data. The risk ranking process is driven by a company's individual Risk Matrix, which governs the decision-making process and ultimately determines the extent of mitigation measures necessary to reduce risk. If the risk matrix used during a PHA or LOPA session has not been carefully reviewed to ensure applicability, a number of issues may arise over the course of the study. On several occasions, the authors of this study had to request that company management revise their risk matrix to avoid unintended conclusions and decisions during the study. This paper aims to identify some of these traps and unforeseen consequences of using a risk matrix in PHA and LOPA.

Typically, hazard scenarios of the most interest in a PHA are those which have a high severity and a low likelihood of occurrence. Such scenarios are often subjected to the LOPA process to ensure that sufficient safeguards are in place. When looking at high severity, low likelihood scenarios, it is easy to unintentionally demand an overly conservative risk criterion. When this criterion is applied in a PHA or LOPA study, the results can lead to dramatic measures for risk mitigation, as a result of unacceptable risk levels or requirements for added safeguards which may not be warranted. Difficulties that the authors have faced in using corporate risk matrices have included (a) overly conservative risk ranking of high severity, low likelihood scenarios, (b) improper decision granularity (c) risk matrices unsuited for the specific operation under review (d) Severity and Likelihood Categories with Uniform Risk Decisions and (e) Increased Risk Decisions for Lower Severity, Higher Likelihood Scenarios. These and other related issues are addressed with specific examples from PHA and LOPA projects conducted by the authors.

1. Introduction and Background

Process Hazard Analysis (PHA) and Layer of Protection Analysis (LOPA) are critical tools for identifying and managing the hazards associated with a chemical process. Once a hazard scenario has been identified, a risk ranking process is used to categorize the risk of the scenario [Reference 1]. Typically, a pre-developed risk matrix is used to classify the severity and likelihood of each hazardous event, and to assign risk ranking. The risk matrix is often developed by company management as a decision-making tool to determine what represents a tolerable risk.

Risk matrices have been in use for many years, and have been adopted by a wide variety of industries. They provide a simple framework for performing a systematic review of risks, and are an approximation of the more rigorously developed risk contours using Quantitative Risk Analysis. Despite the length of time risk matrices have been in use, detailed analysis of their theoretical structure has only been undertaken in the last 15 years. Several authors, including Tony Cox [Reference 2] and Paul Baybutt [Reference 3] have explored the mathematical limitations and potential errors involved in using a risk matrix to quantitatively compare and rank risks in the process industry. In addition to the limitations and potential errors noted in those two articles, practical pitfalls have been noted by the authors of this article. Practical examples are given to illustrate some potential issues which may be encountered when using a risk matrix in PHA and LOPA.

When developing a risk matrix, there are a number of factors which must be considered in order to arrive at a matrix which is rational and appropriate for a business. In particular, the following conditions may lead to unintended consequences when performing a hazard analysis:

- Overly conservative risk ranking of high severity, low likelihood scenarios
- Risk matrices unsuited for the specific operation under review
- Improper decision granularity
- Risk decision not impacted by the severity and likelihood combination
- Potential to miss medium severity, but high risk scenarios

Using a risk matrix which has not been carefully selected can cause a PHA or LOPA study to severely over- or under-estimate the risks involved in a process, resulting in an unsafe or over-designed system. Careful consideration of the above points must be made when developing a risk matrix to ensure that the matrix is suitable for the particular operation under review.

2. Risk Matrix Construction

A risk matrix is typically presented as a table in which severity and likelihood rankings are assigned for a given scenario, and the combination is used to arrive at a risk level (sometimes called a risk decision). The first step in creating a risk matrix is defining individual distinct tiers for the severity and likelihood categories.

Severity of Consequences

When defining consequence severity categories, it is important to consider the full range of potential impacts on a system or operation. When dealing with hazardous chemicals or processes, it is important to consider impacts on safety and the environment, as well as business operations. Some companies choose to include a distinction between impacts to facility personnel and impacts to members of the public. Additionally, some companies also include severity categories for economic impacts (e.g., asset damage, loss of production, etc.). Table 1 provides an example set of severity categories for a large facility such as a refinery.

Table 1. Example Consequence Severity Category Definitions

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

This table represents one example of a severity definition matrix. Each company will have their own set of categories, which is relevant to the operation at hand. For example, some facilities do not differentiate between one fatality and multiple fatalities, while others may choose not to define separate categories for economic impacts – instead focusing their hazard analyses toward safety and environmental risks.

Likelihood Levels

Likelihood categories are defined in a similar manner. Typically, orders of magnitude are used to describe the potential yearly occurrence of an event. Some guidance may be provided to assist the PHA team in identifying the likelihood category most appropriate to a given event. Table 2 provides an example set of likelihood rankings.

Table 2. Example Likelihood Categories

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

Risk Levels

The selected severity and likelihood categories are then combined through the use of the risk matrix. The result will determine the risk level of a given scenario. Risk levels can be used by company management to determine which scenarios will require additional mitigation. Figure 1 presents an example of a risk matrix which may be used at a facility during a PHA or LOPA session.

		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

Figure 1. Example Risk Matrix

In Figure 1, four risk levels are defined in the risk matrix: Critical, Undesirable, Marginal, and No Action. It is important to clearly define the required actions associated with each risk level. Table 3 provides an example of required actions for each of the above risk levels.

Table 3. Example Risk Levels and Required Actions

	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.

Monotonic Nature of Risk Levels

Cells in the risk matrix should be assigned risk levels to follow “iso-risk contours” [Reference 2]. An iso-risk contour represents the line along which the risk presented by the combination of the severity and likelihood is the same. In the example presented above, the risk level increases from left to right and bottom to top, mirroring a set of monotonic iso-risk curves. In other words, in order to form a rational risk matrix, the risk level must continually increase when traveling along a single row or column in the matrix. This approximates what is commonly used in quantitative risk analysis (QRA) where the risk is estimated quantitatively in much greater level of detail.

Risk Tolerance Level

One of the most important distinctions on the matrix is the separation point between tolerable and intolerable risk. Similar to the risk level definitions and their assignments within the risk matrix, the separation point between tolerable and intolerable risk is selected by developers of the risk matrix. For example, in Table 3, the boundary between Undesirable and Marginal risk can be chosen for the separation point between “tolerable” and “intolerable” risks. This separation point is termed the “risk target.” Scenarios which fall above this boundary (i.e., Critical or Undesirable risks in the case of the example) require additional mitigation to ensure that they fall into the Marginal or No Action risk levels, while scenarios which fall into these lower categories may be considered to be “tolerable risks.”

Definition of the risk target is one of the critical decision points when developing a risk matrix. This target will determine the required protections to reduce risk to tolerable levels, and will have a large impact on the protection features implemented at the facility. This decision is a judgement made by company management on the level of risk the company or facility can tolerate.

Improper definition of any of the elements of a risk matrix will lead to poor hazard analysis results, and may lead to decisions which carry excessive risk, or which spend resources ineffectively in pursuit of reducing a risk that should be considered tolerable.

3. Common Risk Matrix Pitfalls

3.1. Overly Conservative Risk Ranking of High Severity, Low Likelihood Scenarios

The top left corner of the example risk matrix presented in Figure 1 contains the highest severity, lowest likelihood events. By their nature, these events can be the most difficult to analyze, as they are typically events which have never occurred, and are in a frequency range which is possible, but is often inconceivable to the analysts. These events represent a company's worst-case risk scenarios, such as a major release of toxic chemicals, resulting in multiple fatalities or wide-spread health impacts to the surrounding community. Such events are typically prevented by a number of protection layers installed specifically to ensure that the events are very unlikely to occur. The required protection level can be established using the risk target for a given consequence severity.

As an example, in the matrix defined in Figure 1, for a Severity A event, the corresponding risk target can be likelihood category 5 (i.e., $1x10^{-5}$ per year). A company using this matrix must provide sufficient protection layers to ensure that the scenario under consideration will not happen more frequently than once in 100,000 years. In this extremely low likelihood range, however, it is difficult to grasp the differences between various occurrence frequencies. This is experienced by the author and acknowledged in the literature [Reference 4]. That is, it may be difficult to conceptualize the difference between an event which presents itself once every 10,000 years, once every 100,000 years, or even once every 1,000,000 years.

This difficulty in grasping the extremely low likelihood regime can make it easy to develop an overly conservative risk target for the highest severity scenarios. Because these scenarios represent the most severe consequences, it is a natural tendency to want to require the likelihood of these severe events to be as low as possible (e.g., $1x10^{-6}$ per year.) While mitigating these events to be as infrequent as possible is a positive goal, care must be taken when setting these targets to avoid unanticipated consequences on facility design. It is possible to set a goal which will require an excessive number of protection layers (controls, trips, etc.), which may not significantly alter the risk decision.

In an example taken from industry, PHA and LOPA were to be conducted on the Front-End Engineering Design (FEED) of a proposed chemical production facility. The results of the LOPA would also be used to determine the necessary Safety Integrity Level (SIL) rating for instrument trip functions to be implemented at the facility. The PHA was to use an existing corporate risk matrix as the foundation of the analysis. In this case, the risk target for the most severe event (the equivalent of Consequence Severity A) was $1x10^{-6}$ per year. While performing the analysis, it was determined that the required risk target was leading to a large number of recommendations to add additional protection features, or to increase the SIL rating for a number of trip functions. When compared with current industry standards and best practices for facilities of a similar design, it was determined that the risk matrix was driving the facility to implement excessive instrumented features to meet the risk target of the owners.

In this example, the corporate risk matrix had been designed with overly conservative definitions for high severity, low likelihood events. The risk target for these events had to be carefully selected to ensure that it generates useful results. Selecting a highly conservative risk target, as it was shown in that case, will lead to addition of a large number of protection features in facility design. These features will help to prevent high severity scenarios, but may not be necessary according to common practices. In other words, these additional safety features may be protecting against concerns which are already sufficiently mitigated by existing safety features per accepted industry practices. Clearly, adding additional protection layers can greatly increase cost, and the analysts may need to examine the possibility of unanticipated safety concerns due to spurious trips or additional maintenance hazards.

Ultimately, placement of the risk target is a company-specific decision which requires careful consideration to avoid unintended consequences. The risk matrix must be reviewed to ensure that its effects on the operation under review are understood, and do not lead to unanticipated consequences on risk or facility design.

3.2. Risk Matrices Unsuited for the Specific Operation Under Review

When beginning a PHA for a specific facility or system, it is critical to ensure that the risk matrix is suitable for the size and scope of the review. In the above example, a company-wide risk matrix for a large corporation with multiple interests across various fields was used for the PHA and LOPA analysis. The matrix had not been reviewed to ensure that it was applicable to the facility under review.

In a similar vein, other portions of the risk matrix must also be reviewed to ensure that they are appropriate for the operation under review. For example, in addition to safety concerns, many companies choose to risk rank the impact of hazardous scenarios on facility assets or production time. Typically, the consequence severity categories for these events are assigned based on the dollar value of the impact. For example, in Table 1, a Severity A event is defined as an event which results in a loss of more than $500 million. While this may be appropriate for a large scale corporation, smaller operations may consider a significantly smaller loss to still result in a catastrophic impact on the business of that operation.

Conversely, if a matrix is designed such that the highest possible severity ranking is much too low, it may result in extreme protective measures to mitigate small operational concerns. For example, a theoretical company produces $10 million annually, and operates using a risk matrix in which the highest severity ranking correlates with a loss of $100 thousand. In this case, almost any event which results in plant downtime for a few days will be given the highest possible consequence severity rating, and will require the corresponding protection layers to prevent such events. The resulting analysis will be forced to recommend significant changes to system design and operation to avoid shutdowns, which will dramatically increase cost, while protecting against events which in reality have already adequate protection.

3.3. Improper Decision Granularity

Similar to the scenario described above, improper decision granularity can also lead to over- or under-estimations of the risk posed to a facility by a given scenario. If the severity or likelihood category scales are too broad, a hazard analysis will be unable to distinguish between high and low risk scenarios, which will result in a tight grouping of a majority of all scenarios within the same risk category (and therefore with the same risk target). In this event, high severity scenarios may not receive sufficient prevention or mitigation features, while low severity scenarios may require excess additional protection layers. Practical examples are provided below. Mathematical treatise of this concern is addressed in Reference 2.

It should be noted, however, that just because a majority of scenarios fall within the same risk category does not mean that the decision granularity is incorrect by default. Some facilities with simple processes, or with similar hazards throughout the process, may find that by the nature of the facility, a majority of risk will be categorized with the same risk ranking. Improper granularity is only a concern when risks of differing magnitude are grouped into the same risk category.

For example, take the same facility from Section 3.2 which generates $10 million annually. If this company uses the consequence severity categories presented in Table 1 of this report, an event which causes the facility to shut down for a year will be considered a category D event, while nearly all other less severe losses would constitute a category E event – the lowest possible scenario. However, in reality, a year-long plant shutdown would have serious impact on the company’s finances, with the potential for the loss of ability to operate in the future, and should require sufficient protection layers to significantly reduce the likelihood of such an event.

3.4. Risk decision not impacted by the severity and likelihood combination

Some risk matrices may include severity or likelihood categories in which the risk decision does not change, no matter what ranking it receives. As an example, consider the following example risk matrix, with similar risk definitions as Figure 1:

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

Figure 2. Conservative Example Risk Matrix

This matrix is skewed toward high risk scenarios. In particular, for Consequence Severity A, there is no possible risk ranking which falls into the tolerable range. This implies that if a Severity A hazard is identified, measures must be taken to totally eliminate the hazard from the design, rather than add protection layers against the event. In some cases, this decision may be intentional, if it has been determined that the facility cannot tolerate an event of a given magnitude, no matter how rare. However, it may also be the case that the risk matrix was designed to be highly conservative, without fully realizing the consequences implied for Severity A.

In his article "What's Wrong with Risk Matrices?", Tony Cox demonstrates that for an ideal risk matrix which minimizes the potential for risk ranking errors "all cells in the left-most column and in the bottom row are green (lowest-priority)" [Reference 2]. In Cox's example, he uses a risk matrix containing only three risk levels (i.e., only three color categories). When defining a risk matrix with more than three risk levels, this statement can be taken to mean that all cells which fall in the lowest likelihood or severity category should also fall within the tolerable risk range.

3.5. Potential to miss medium severity, but high risk scenarios

Risk matrices may also be arranged such that the risk decision for less severe consequences presents a higher risk than a more severe, less likely event. To illustrate, consider the risk matrix in Figure 4.

		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	Undesirable	Undesirable	Undesirable
	D	No Action	No Action	Marginal	Marginal	Undesirable
	E	No Action	No Action	No Action	Marginal	Marginal

Figure 4. Risk Decision Example Risk Matrix

Using this risk matrix, consider an example from industry in which a fire at a relief valve vent may lead to a fatality (Severity B) when personnel are working on an elevated platform near to the vent, or to a severe injury (Severity C) at grade. When evaluating such a scenario with multiple potential safety outcomes, typically the worst-case consequence (the fatality in this case) is evaluated to ensure that the facility is adequately protected against such an event. In this example case, the analysis determines that given the safeguards in place, the likelihood of personnel exposure in the remote area which results in a fatality is $1x10^{-4}$ per year, while the likelihood of personnel exposure at grade, leading to injury, is $1x10^{-3}$ per year. Using the risk matrix in Figure 4, we can see that this leads to a Marginal risk for the fatality case, but an Undesirable risk for the injury. If only the worst-case event was considered in this analysis, as is typically practiced, an undesirable risk may have gone undetected.

In this example, the risk matrix has been designed in such a way that a lower severity event may lead to a higher risk ranking than the worst-case event. Careful consideration must be taken when assigning risk definitions such as the one in Figure 4, to ensure that such decisions are noted and are adequately supported by the decision makers. In addition, it is critical to ensure that the hazard analysis methodology employed is capable of identifying events with multiple outcomes which fall into varying severity of likelihood categories, to ensure that the scenario which poses the highest risk is identified.

4. Conclusion

The concept of the risk matrix has proven to be a simple but useful tool in managing risk. It has been adopted by a wide range of diverse industries. It is an approximation of the more rigorously developed risk contours using Quantitative Risk Analysis and because of that it has some theoretical limitations that have been studies by various authors. However, given the number of facilities and processes within the process industry that must make risk decisions, the risk matrix approach has proved to be a useful approximation tool.

In applying risk matrices developed by various owner and operator companies, several discrepancies have been noted that have led to improper or overly conservative decisions. When developing a risk matrix, consequence severity and likelihood categories must be carefully chosen to ensure that they are applicable to the facility or system under review. These categories must accurately reflect the potential range of consequences possible in the system, and should be segregated based on the potential impact on continued operation of the facility.

The risk matrix is a critical tool in the hazard analysis process, and has a wide-ranging impact on system safety and design. When applied correctly, the risk matrix is a powerful tool in ensuring that a facility is operating at a tolerable risk level. However, using the incorrect risk matrix during a hazard analysis can result in systems which are significantly under-protected against process hazards, or may lead to a large number of recommendations for protection layers which do not alter the risk decision, and which may be costly and difficult to implement or maintain.

Before beginning any hazard analysis, whether in the design phase or for an existing process, the risk matrix to be used must be reviewed and evaluated to ensure that it remains applicable to the system to under consideration in order to obtain meaningful results.

5. References

[1] CCPS. *Guidelines for Hazard Evaluation Procedures*. Center for Chemical Process Safety. American Institute of Chemical Engineers. 3rd Edition. New York, NY. April 2008.

[2] L. A. Cox. “What’s Wrong with Risk Matrices?” Risk Analysis 28, No. 2 (2008). 497-512.

[3] P. Baybutt. “Designing Risk Matrices to Avoid Risk Ranking Reversal Errors” Process Safety Progress 35, Issue 1 (2016). 41-46.

[4] CCPS. *Guidelines for Developing Quantitative Safety Risk Criteria*. Center for Chemical Process Safety. American Institute of Chemical Engineers. New York, NY. 2009.