ioMosaic®

Minimizing risk. Maximizing potential.®

Designing an Effective Risk Matrix

An ioMosaic White Paper

Introduction

Risk assessment is an effective means of identifying process safety risks and determining the most cost-effective means to reduce risk. Many organizations recognize the need for risk assessment, but most do not have the tools, experience and resources to assess risk quantitatively. Therefore, these organizations use qualitative or semi-quantitative risk assessment tools, such as risk ranking.

Although risk matrices are easy to use, unless they are designed properly, they can create liability issues and give a false sense of security. An effective risk ranking matrix should have the following characteristics:

- Be simple to use and understand
- Not require extensive knowledge of quantitative risk analysis to use
- Have clear guidance on applicability
- Have consistent likelihood ranges that cover the full spectrum of potential scenarios
- Have detailed descriptions of the consequences of concern for each consequence range
- Have clearly defined tolerable and intolerable risk levels
- Show how scenarios that are at an intolerable risk level can be mitigated to a tolerable risk level on the matrix
- Provide clear guidance on what action is necessary to mitigate scenarios with intolerable risk levels

Risk ranking uses a matrix that has ranges of consequence and likelihood as the axes. The combination of a consequence and likelihood range gives an estimate of risk or a risk ranking. Although there are many risk matrices that have been developed and published, the development and application of risk matrices present their own challenges.

Construction of a risk matrix starts by first establishing how the matrix is intended to be used. Some typical uses for risk ranking are process hazard analyses, facility siting studies, and safety audits. A key initial decision that has to be made is to define the risk acceptability or tolerability criteria for the organization using the matrix. Without adequate consideration of risk tolerability, a risk matrix can be developed that implies a level of risk tolerability much higher than the organization actually desires. Another key aspect of risk matrix design is having the capability to evaluate the effectiveness of risk mitigation measures. The risk matrix should always allow the risk ranking for a scenario to move to a risk tolerable level after implementation of mitigating measures. Otherwise it may be difficult to determine the effectiveness of mitigation measures.

The next step is to define the consequence and likelihood ranges. A typical risk matrix is a four by four grid. Larger matrices usually have more likelihood ranges. First determine what are the consequences of interest. These can include personnel safety, public safety, environmental impact, property damage/business interruption, corporate image and legal implications. Each consequence of interest may have a different definition for a specified consequence category. For example Table 1, which is taken from MIL-STD-882D, shows an example of multiple consequences that can be defined for a single consequence range.

Table 1: Example of Multiple Consequences for a Consequence Range

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost workdays(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Source: MIL-STD-882D

In this example, each consequence range includes consequences for personnel safety, environmental impact and property damage. One potential downfall of equating consequence criteria for property damage with personnel death is that some might equate this to the value the company puts on human life. Once the consequence ranges have been defined, the corresponding likelihood ranges can be defined. The risk tolerability of events with different potential consequences should be different. For example, no organization would tolerate having a high likelihood of having a Bhopal type event where thousands of public citizens were killed or injured. However, every organization recognizes that use of hazardous materials poses a risk that cannot be eliminated, but only controlled. Few organizations have established corporate risk tolerability criteria and thus have not defined a common basis for making risk decisions.

Table 2, also taken from MIL-STD-882D, provides an example of suggested probability (likelihood) levels.

Table 2: Example of Likelihood Ranges

Description*	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur more than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

Source: MIL-STD-882D

*Definitions of descriptive words may have to be modified based on quantity of items involved.

**The expected size of the fleet or inventory should be defined prior to accomplishing an assessment of the system.

In Table 2, likelihood is defined in terms of a probability that the potential consequences will be experienced during the life of the item. For most process facilities, the item of interest is the plant, process or unit being reviewed. Assuming a typical design plant life of 20 years, the probabilities given in the above table can be converted into frequencies by dividing by 20. Therefore, category A would have a frequency of greater than once every 2 years. In moving from the Frequent to Occasional likelihood range, the frequency drops by a factor of 10 for each range. However, in moving from the Occasional to the Remote likelihood range the frequency changes by a factor of 1000. This arrangement creates likelihood ranges that are narrow at the more frequent end of the scale and very broad at the less frequent end. The other problem with likelihood categories that are defined in terms of frequency is having the relevant data to quantify the frequency of realizing the potential consequences. Generally, this involves determining the frequency of the initiating event and then determining the probability of all other contributing events. Without extensive experience in quantitative risk assessment and a comprehensive database of failure rates, this becomes a judgmental activity and may result in assigning frequencies to scenarios that are much lower than would be determined through quantitative analysis. Because risk ranking is a semi-quantitative tool, it must be conservative and in some cases assign higher than actual frequencies to scenarios. In those cases ,the company may choose to conduct a quantitative risk analysis to refine the number before investing considerable resources to mitigate that risk.

The final step in developing the risk matrix is to translate the tolerability criteria onto the matrix. At a minimum the risk matrix must have clear blocks where the risk is tolerable or intolerable. Another matrix taken from the CCPS *Guidelines for Hazard Evaluation Procedures, Second Edition,* is shown in Table 3.

Table 3: Example Risk Ranking Matrix

Consequence *Frequency*	1	2	3	4
4	IV	II	I	I
3	IV	III	II	I
2	IV	IV	III	II
1	IV	IV	IV	III

Source: CCPS Guidelines for Hazard Evaluation Procedures, Second Edition

There are some issues with this example. First, in the first row of the risk-ranking matrix (Table 3), the risk rank changes from a II for consequence category 2 to a IV for consequence category 1. This creates a disconnect in the risk ranking as there is no risk rank of III for events with a frequency of 4.

Table 4 provides a description of the risk ranking categories used in Table 3. For risks ranked I or II there is a time period specified for implementation of mitigation measures. This is a sure way to violate your own procedures and incur the associated liability by recommending mitigating measures that may take longer than the specified time to implement, especially if it requires approval of a capital project. Therefore, special procedures and approvals need to be put in place to waive the time limits for those situations. Also in Table 4, the description of Risk Rank III is defined as “Acceptable with controls”. This is somewhat confusing as all scenarios are acceptable with the proper controls. That is the whole point of risk assessment. Do we assume that there is no need to verify that procedures and controls are in place to mitigate scenarios with a Risk Rank of IV?

So how do we avoid these pitfalls and still have an effective risk-ranking tool for use in making risk decisions in day-to-day operations, such as during hazard and operability (HAZOP) studies? One option is to avoid using quantitative frequencies or probabilities for the likelihood ranges and use a layer of protection analysis (LOPA) approach as shown in the Table 5. This approach is not perfect, but it is simple to implement and easy for most HAZOP participants to understand. The highest likelihood range (level 4) is defined by the likelihood of the initiating event (e.g., human error, control failure). Then for each level of protection that exists the likelihood range is reduced one level. This approach assumes that each level of protection has a similar failure probability, which is generally acceptable for rough risk screening such as HAZOP risk ranking. Some failures have fairly well defined frequencies and can be used directly as shown in the table. For example, the spontaneous failure of a pressure vessel has a frequency in the range of 10-5 per year and thus by itself would qualify as a level 1 likelihood. Similar likelihood levels can be defined for other common equipment loss of containment failures like pipe and hose leaks and ruptures.

Table 4: Example Risk Ranking Categories

Risk Rank	Category	Description
I	Unacceptable	Should be mitigated with engineering and/or administrative controls to a risk ranking of III or less within a specified period such as six months
II	Undesirable	Should be mitigated with engineering and/or administrative controls to a risk ranking of III or less within a specified period such as 12 months
III	Acceptable with controls	Should be verified that procedures or controls are in place
IV	Acceptable as is	No mitigation required

Source: CCPS Guidelines for Hazard Evaluation Procedures, Second Edition

Table 5: Likelihood Ranges Based on Levels of Protection

Likelihood Range	Qualitative Frequency Criteria: Typical Scenarios
Level 4	▪ Initiating event or failure ▪ Hose leaks/ruptures
Level 3	▪ One level of protection ▪ Piping leaks
Level 2	▪ Two levels of protection ▪ Full-bore failures of small process lines or fittings
Level 1	▪ Three levels of protection ▪ Tank/process vessel failures

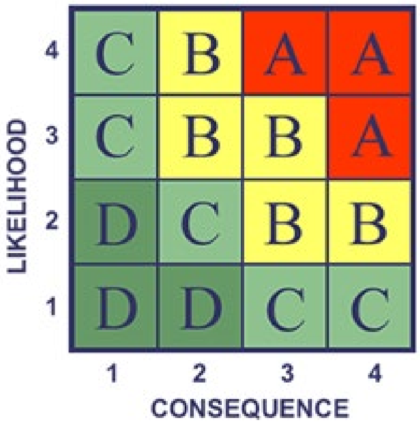
Note: The below likelihood ranges can be used in conjunction with typical consequence ranges shown in Table 6

Table 6: Typical Consequence Range Criteria

Consequence Range	Qualitative Safety Consequence Criteria
Level 4	▪ Onsite or offsite: Potential for multiple life-threatening injuries or fatalities. ▪ Environment: Uncontained release with potential for major environmental impact ▪ Property: Plant damage value in excess of $100 million
Level 3	▪ Onsite or offsite: Potential for a single life-threatening injury or fatality. ▪ Environment: Uncontained release with potential for moderate environmental impac ▪ Property: Plant damage value in the range of $10-100 million
Level 2	▪ Onsite or offsite: Potential for an injury requiring a physician's care. ▪ Environmental: Uncontained release with potential for minor environmental impact ▪ Property: Plant damage value in the range of $1-10 million
Level 1	▪ Onsite: Potential restricted to injuries requiring no more than first aid. ▪ Offsite: Odor or noise complaint ▪ Environment: Contained release with local impact ▪ Property: Plant damage value in the range of $0.1 to 1 million

The resulting risk matrix is shown in Figure 1.

Figure 1: Risk Matrix



LIKELIHOOD				
4	C	B	A	A
3	C	B	B	A
2	D	C	B	B
1	D	D	C	C
	1	2	3	4
	CONSEQUENCE			

In order to develop effective mitigating measures, it helps to understand how different layers of protection are challenged as a typical incident develops. Table 8 provides the typical activation order of different layers of protection in response to a process deviation. A failure (the initiating event) occurs that takes the process outside of its normal operating range. The basic process controls, alarms, interlocks and operator supervision are the first to respond by adjusting process parameters to return to normal operating range. As the process reaches one or more of its operating limits, the SIS or ESD systems activate to maintain the process in a safe condition by shutting down all or part of the process. This is the last point at which the chemicals in the process can be kept in their primary containment systems. When the process parameters reach the equipment design limits the relief systems are the next to activate. Once a loss of containment incident has occurred, the only option is to try to reduce its consequences through emergency response.

And the action required based on the risk ranking is shown in Table 7.

Table 7: Risk Level / Action

Risk Level	Action Required
A	Risk mitigation required to risk level C or D
B	Risk mitigation required to risk level C or D
C	Risk mitigation to risk level D is optional
D	No further risk mitigation required

Table 8: Expected Activation Order of Layers of Protection

1	Process or equipment designed for process operating limits
2	Basic process controls and alarms, and operator adjustments to process deviations
3	Critical alarms and operator response to process approaching operating limits
4	Safety Interlock Systems (SIS) or Emergency Shutdown (ESD) systems take action at operating limits
5	Relief systems that activate aft equipment design limits
6	Mitigation systems that contain the effects of incidents
7	Plant emergency response to control the effects of incidents
8	Community emergency response to protect the public from the effects of an incident

Table 9: Strategy for Reducing Risk

1	Inherent (eliminate the hazard by using less hazardous materials, reducing inventory, operating
2	Passive (minimize the hazard through process and equipment design by making the equipment
3	Active (detect and control process deviations to avoid exceeding operating limits and
4	Procedural (prevent or control incidents through administrative controls, such as procedures,

As mentioned earlier, different mitigating measures can provide different levels of protection. Table 9 provides a typical strategy for developing recommendations to mitigate scenarios with intolerable risk levels. The most effective mitigation is to make the process more inherently safe. The next most effective mitigating measures are passive systems that do not require any external means of activation, followed by active systems. The least desirable option is to use administrative controls. The latter are prone to failure from either a breakdown of management systems or human error.

The approach presented in Tables 5 and 6 and Figure 1, addresses the main issues associated with the development of risk matrices and simplifies the use of this tool without the need to establish corporate risk tolerability criteria.

- It allows different risks (personnel, public, environmental and business) to be identified and mitigated.
- It is simple to use and does not require expertise in quantitative risk assessment

- It allows recommendations to be prioritized (from A to D) based on risk level.
- It allows all scenarios to be mitigated to a tolerable (C or D) risk level, and to show on the matrix how the risk was reduced (by reducing likelihood, consequence or both)

The key to risk management is to identify risks that are intolerable and to mitigate them to a tolerable level. In a PHA study, teams can usually identify ways to reduce the risk of any scenario. The benefit of using a risk matrix is that it identifies those risks that need to be mitigated and therefore allows for more cost-effective risk mitigation. This is becoming increasingly important as companies have reduced their operating budgets and have limited resources to manage risk.

Additional Resources

1. Henry Ozog, 2009