Risk Criteria, Protection Layers and Conditional Modifiers

Angela E. Summers, Ph.D. PE
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX 77034
281-922-8324 (phone), 281-922-4362 (fax)
asummers@sis-tech.com

William H. Hearn, PE
SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX 77034
281-922-8324 (phone), 281-922-4362 (fax)
whearn@sis-tech.com

Keywords: Risk criteria, risk analysis, hazards, hazardous events

Abstract

Risk analysis assesses the likelihood and consequence of events. The acceptability of the identified risk is determined by comparing it to a specified risk tolerance. The criteria applied depend on the analysis boundary, which may be loss of containment or extend to the harm posed by the loss of containment. Risk analyses generally begin with a determination of the likelihood that a hazardous event could result in loss of containment or some other undesirable consequence. These analyses require estimation of the likelihood that the initiating event will occur and the probability that the protection layers will not operate as required. Conditional modifiers are considered when the analysis is evaluating the likelihood that harm may be caused by the loss of containment.

Various methods for performing risk analyses are discussed in several CCPS publications including Chemical Process Quantitative Risk Analysis (1), Hazard Evaluation Procedures (4), and Layers of Protection Analysis (8). However, the link between the selected risk criteria as described in Guidelines for Developing Quantitative Safety Risk Criteria (3) and the factors considered in the analysis is not clearly described in these texts. Recognizing this opportunity, this paper begins with a brief introduction to risk analysis concepts to provide a foundation for a discussion of the typical analysis boundaries and associated risk criteria. Then, it discusses how the analysis boundary and risk criteria affect the consideration of protection layers, enabling conditions, and conditional modifiers.

1. How is risk measured?

Risk is the result of deviations from expected operation and is intimately related to the process design and site safety culture. Loss prevention seeks to identify these deviations and to reduce their frequency of occurrence or impact should they occur. The result of each deviation can be judged by analyzing the design and historical performance. Some process deviations are significant enough that a hazardous event occurs. An effective process safety management program prevents deviations from propagating into hazardous events. The rigor of the management system determines whether the hazardous event risk is reduced as low as reasonably practicable.

The level of a process risk is directly related to the frequency of process deviation and the consequence of exceeding the equipment safe operating limit. Process risk can be minimized using inherently safer principles in the design of the process to reduce the magnitude of the consequence and in the operational and management strategy to reduce the process deviation frequency (7). Varying levels of rigor are applied in estimating the risk from hazardous events (4). Generally, the specific method is chosen based on the following considerations:

- Regulatory requirements
- Company policy
- Lifecycle phase
- Information available
- Process complexity
- Previous experience with process
- Required degree of risk discrimination
- Consequence severity

Risk ranking within the Process Hazards Analysis (PHA) has traditionally been qualitative, supported by a risk matrix that relates frequency and consequence to priority (Figure 1). The risk rank is used to determine the priority and criticality of recommendations made to reduce risk and to address safeguard deficiencies.

The event likelihood (Figure 1) is estimated given the listed causes and identified safeguards that prevent the deviation from exceeding the safe operating limit or reduce the hazardous situation that leads to harm. The frequency estimate is complex, because it requires that team members estimate the likelihood of simultaneous failure of many systems that rely on manual and automated actions. Significant consequence events often have multiple safeguards with varying degrees of independence, diversity and capability. The difficulty for the team in performing the estimate is that hopefully the hazardous event has never happened and given the number of things that must go wrong seems unlikely to ever happen. Process upset, shutdown, near miss, and incident investigation reports can be used to better understand the likelihood of various aspects of the event, such as cause likelihood or safeguard failure (5).

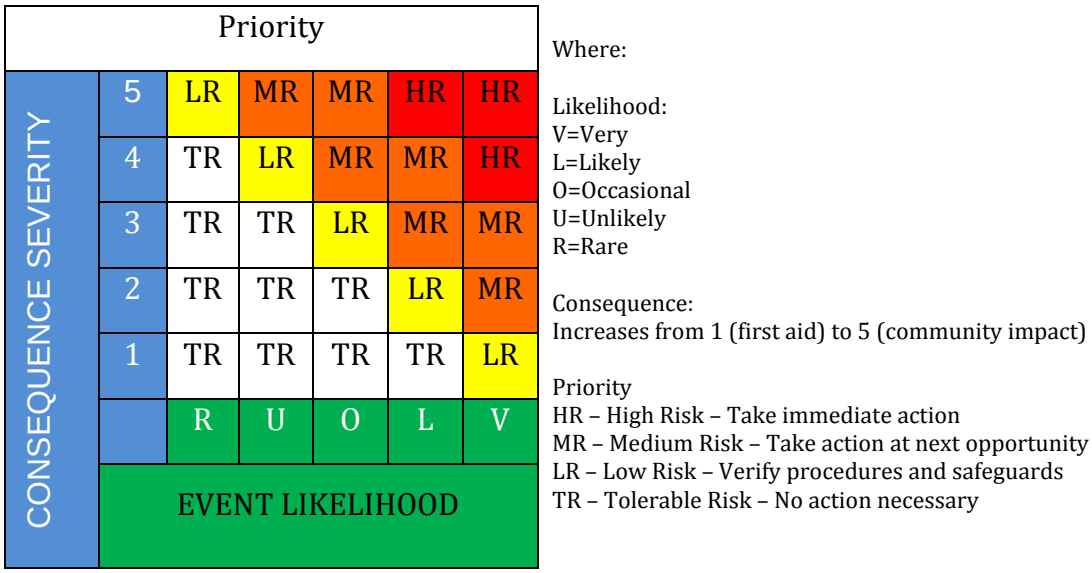

Figure 1: Example PHA Risk Matrix For Ranking Hazardous Event Risk

The team qualitatively ranks the consequence severity (Figure 1) by considering the hazardous situation posed by the event. The consequence severity ranking must not consider the action of safeguards; it should be ranked based on the harm that results when everything that could go wrong, has gone wrong. The inherent difficulty is that team experience and incident records include the operation of safeguards that can reduce the harm caused by hazardous situation, such as fire and gas systems or emergency response procedures. Since consequence severity is often used to screen events for further analysis, it is important that the documentation reflect the hazardous situation without consideration of any safeguards including proactive, reactive, and emergency response activities. Consequence modeling can be used to better understand the hazardous situation and impact zone (2,10).

The next level of risk analysis rigor estimates the event likelihood using a semi-quantitative technique (8) called Layers of Protection Analysis (LOPA). LOPA allows the risk to be estimated at various points along the incident sequence, so it can provide quantitative estimates of the process risk, hazardous event risk, and harmful event risk. LOPA is generally applied to hazardous events that have a consequence severity involving:

- Community injury or fatality
- Serious worker injury or fatality
- Significant environmental impact
- Significant business interruption or equipment damage

In LOPA, the team examines how causes lead to process deviations (or initiating events) to understand how they propagate into a hazardous or harmful event. The analysis may include enabling conditions that are required for the deviation to propagate, such as environmental conditions, co-incident equipment failures, and process operating

conditions. Evaluating enabling conditions is critical to understanding multiple (generally double) jeopardy events, i.e., more than one thing must be wrong for the process deviation to occur. The risk rank is generally performed using a risk matrix or by calculation (Figure 2).

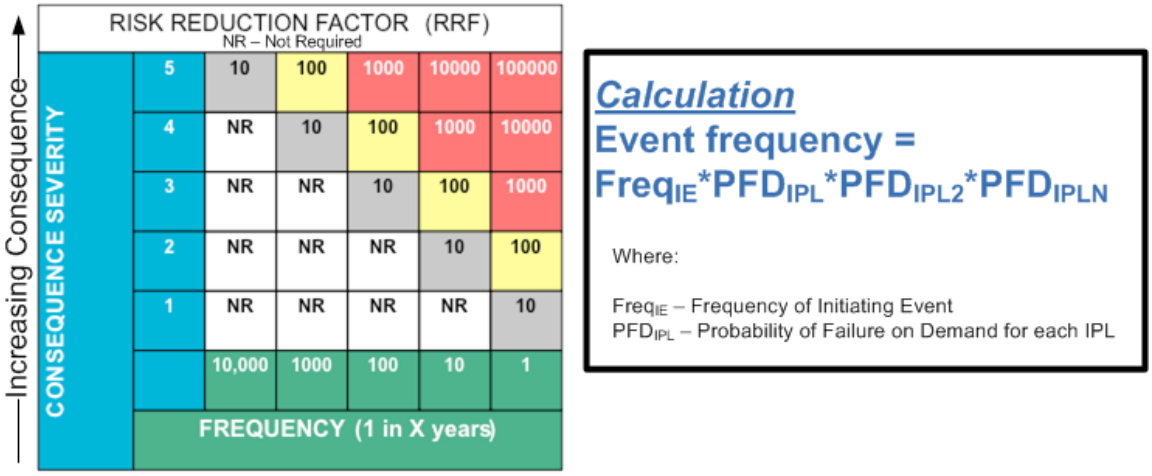

Figure 2: Example risk matrix and risk equation

Some events are too complex for the team to estimate the likelihood using qualitative or semi-quantitative (e.g., LOPA) methods. As examples, runaway reaction events may cause extremely high pressure initiated by multiple independent causes, or flare load mitigation systems may be restricted by system design that limits the number of vessels that can simultaneously relieve. Qualitative risk estimates and semi-quantitative evaluations need clear independence, a small number of causes, and low complexity protection layers in order for the simplified rules and estimation techniques to be effective. Quantitative risk analysis (QRA) techniques, such as fault tree analysis, should be used to determine the frequencies of these more complex events (3). Due to the analysis complexity, QRA requires personnel with special training and expertise, rather than the diverse team used in the case of PHA and LOPA risk ranking.

2. How is risk reduced?

The event risk is compared to the company risk tolerance to determine whether additional risk reduction is required. The selected risk tolerance level should fall within the range of internationally accepted risk measures as discussed below in “What are typical target risk criteria?” If the process risk does not satisfy the chosen risk criteria, independent protection layers (IPLs) are used to close the gap by decreasing the hazardous or harmful event frequency. IPLs are engineered and/or procedural safeguards that are designed and managed to meet seven (7) core attributes: independence, functionality, integrity, reliability, auditability, management of change, and access security (8, 6).

IPLs are intended to stop propagation of the hazardous event to the probable harm caused by the event. An onion-skin diagram (6) is often used to illustrate the typical order of IPL

deployment (Figure 3). As the event propagates through the onion-skin of IPLs, the impact on the process operation becomes greater as does the uncertainty of the final outcome.

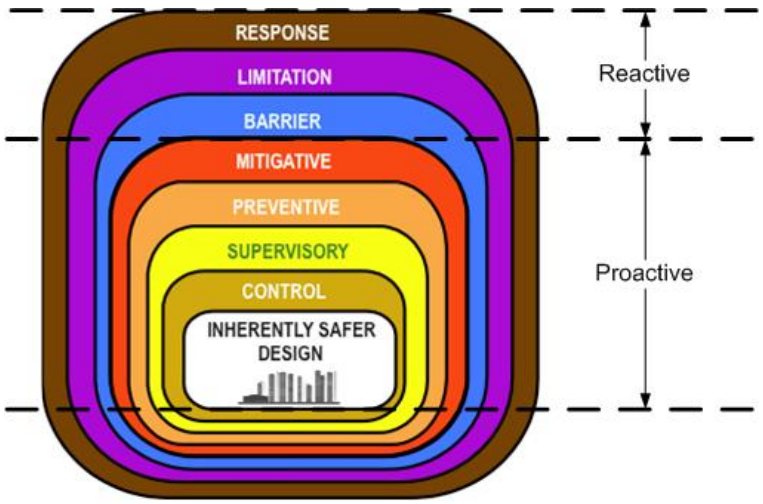

Figure 3: Protection layers represented as onion-skin

Some layers stop a process deviation from exceeding the equipment safe operating limit. The inherently safer design, control, supervisory, preventive and mitigation layers proactively avert loss of containment or equipment damage (Figure 4). A well-designed function acting to prevent the hazardous event can have a high certainty of effectiveness, since the function can be designed specifically for the purpose and the outcome can be predicted using engineering principles.

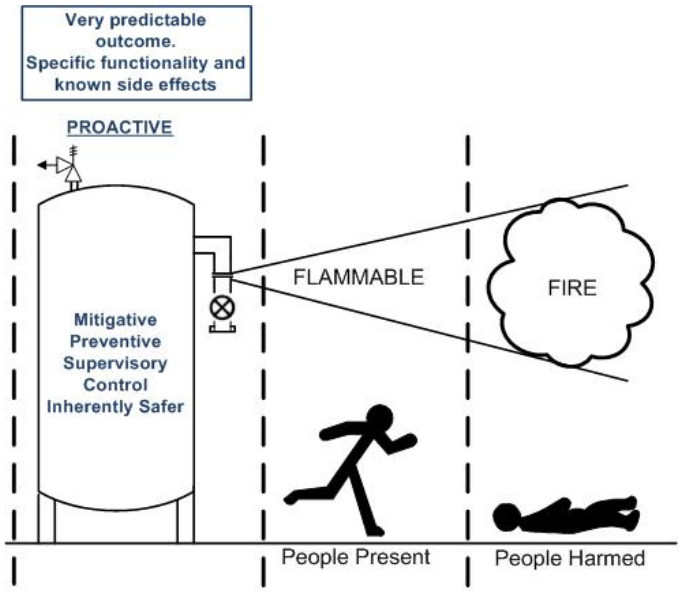

Figure 4. Relationship Between Proactive IPLs and Hazardous Event Risk

Other layers moderate the hazardous situation after a hazardous event (release) occurs (Figure 5). A hazardous situation may expose people, property or the environment, etc. to one or more hazards. Barriers and limitation layers are reactive layers and take action after loss of containment has occurred. Barriers contain the released materials (or energy) and must be designed specifically for the situation to be effective. For example, the design of an explosion barrier must consider the degree of overpressure created by the hazardous event. Limitation functions principally act to reduce the severity of the hazardous situation by monitoring for unacceptable atmospheres and taking action to isolate/de-inventory and/or to evacuate non-essential personnel. Functions acting to moderate the hazardous situation have more uncertainty in their outcome, because their effectiveness is impacted by the specific hazardous situation.

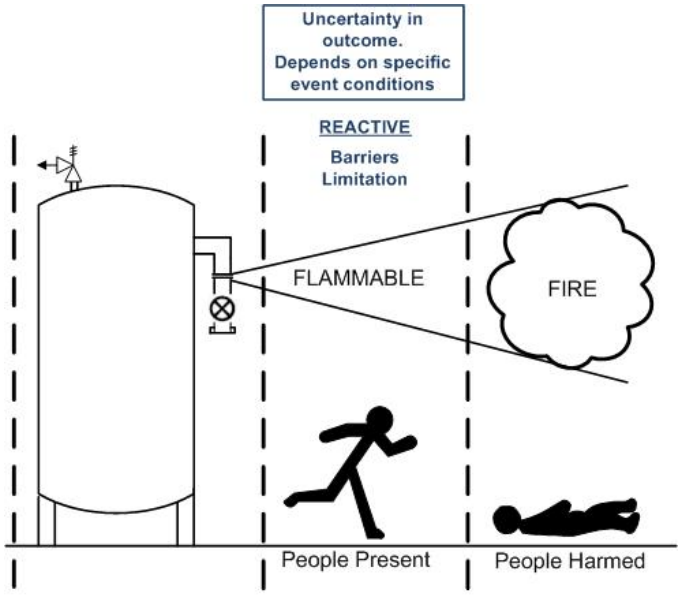

Figure 5. Relationship Between Reactive IPLs and Hazardous Situation Risk

Finally, a properly executed emergency response plan can reduce the harm caused by the hazardous situation by preventing escalation of the situation (Figure 6). For example, putting out a fire stops the exposure to surrounding equipment and structures, preventing further damage. Emergency response plan activities have the highest uncertainty, since they act when the hazardous situation has already started causing harm. Essentially, these activities prevent a bad situation from getting worse. Unfortunately, there are many cases where emergency responders have been injured during response. Effective planning, training, coordination, and communication are extremely important to succeed in ending the incident with minimal loss.

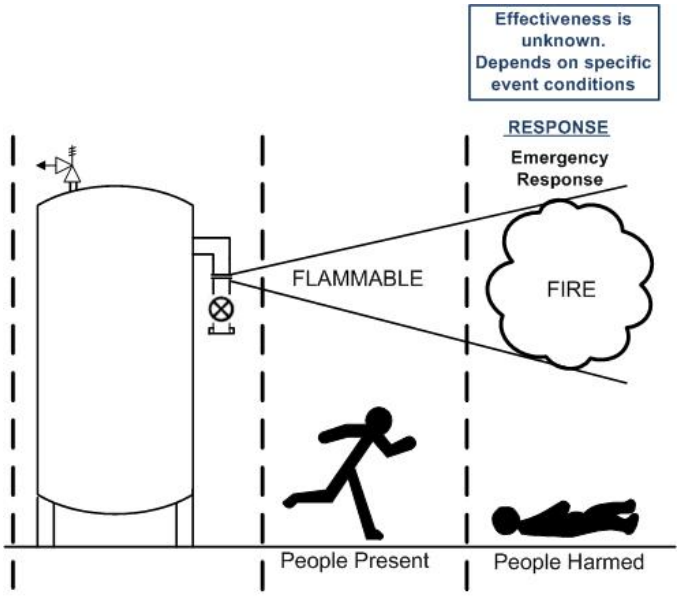

Figure 6. Relationship Between Response IPLs and Harmful Event Risk

3. What are typical target risk criteria?

Guidelines for Quantitative Safety Risk Criteria (CCPS SRC) discussed several criteria used to judge the acceptability of process risk (3). Precise definition of the scenario and proper use of the risk evaluation boundary is critical to the proper application of the risk criteria. The risk criteria depend on the analysis boundary (i.e., the scenario definition). As the boundary moves from measuring hazardous events to measuring harm, more complex analysis is required.

The owner/operator's risk tolerance establishes the minimum required risk reduction and enables prioritization of investments related to IPLs. Internal practices should explain how the criteria are used throughout the lifecycle to ensure consistent application. The risk should be reduced below the tolerable risk level, unless a deviation is justified and formally approved by management.

Many different criteria are applied in risk analysis throughout the world. Some are mandated by government regulation or industry practice. This section presents some order of magnitude risk criteria found in CCPS SRC Section 4.10. Similar data is presented in CCPS Layers of Protection Analysis (8) Appendix E and CCPS Safe and Reliability Instrumented Protective Systems (6) Table 3.1. This data pertains to fatality risk only, but similar criteria can be established for injury, environmental, and economic risks. *The data presented is intended to provide examples of the type of criteria used in various risk analysis and should not be considered a requirement from any publication.*

Typical criteria used in process risk (Table 1) vary by orders of magnitude depending on the analysis boundary. The maximum frequency of each hazardous event focuses on prevention of loss of containment events (i.e., the hazardous event risk). In contrast,

maximum individual risk focuses on reduction of harm (i.e., the harmful event risk). The criterion for maximum individual risk assumes that no individual person is exposed to more than 100 hazardous events that could result in a fatality.

Table 1: Example Risk Criteria (3)

Criteria	**Worker**	**Public**
Maximum Individual Risk - All events	10^{-3} fatality/yr	10^{-4} fatality/yr
Maximum Individual Risk - Each event	10^{-5} fatality/yr	10^{-6} fatality/yr
Maximum Hazardous Event Frequency – Each event	10^{-4} event/yr	10^{-5} event/yr

3.1 Hazardous event criteria

Hazardous event criteria focus on preventing initiating events (or deviations) from propagating to loss of containment, thereby reducing the frequency of releases and the resulting hazardous situations (Figure 7). Effectiveness can be tracked using operational records and near miss/incident data (5). Hazardous event criteria may consider enabling conditions that are necessary for the propagation of the initiating event to the hazardous event. As discussed previously, proactive IPLs are used to stop the propagation of the initiating cause to the hazardous event. Typically IPLs are selected to reduce the frequency of the hazardous event to less than 10^{-4}/yr where a worker fatality is deemed possible and 10^{-5}/yr where a community fatality is possible.

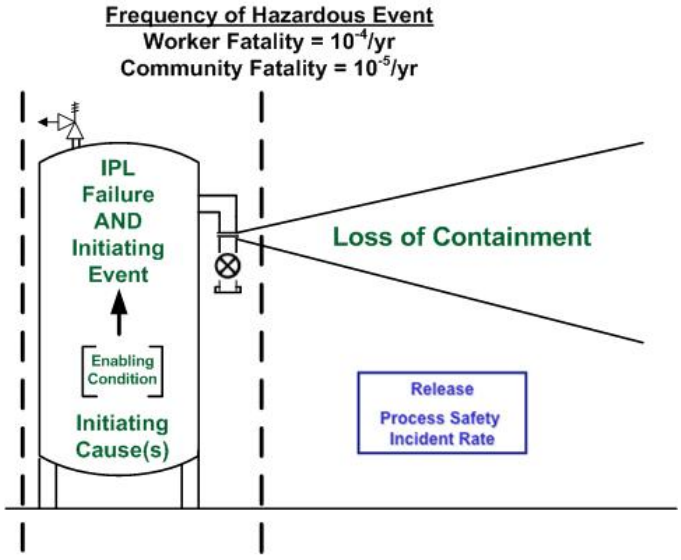

Figure 7. Single Hazardous Event Criteria and Analysis Boundary

3.2 Harmful event criteria

Harmful event criteria are generally based on maximum individual or societal risk and may be apportioned to different external events, such as electrocution, falling, or impact, and process events, such as loss of containment (3). These risk statements focus on fatality rates, which can be verified using injury statistics (5).

The analysis of harmful events extends the evaluation beyond loss of containment to the harm posed by the incident. Consequently, the analysis will often take into account reactive IPLs, in addition to proactive IPLs and enabling conditions that occur prior to or concurrent with the initiating cause. When cumulative risk is evaluated, the fractional time spent in each operating mode may also be considered. Since harmful event analysis is estimating the risk of direct harm, conditional modifiers are often evaluated, such as probability of occupancy, ignition, and fatality.

Misuse of conditional modifiers and enabling conditions can result in underestimation of the risk (9). Conversely, when conditional modifiers and enabling conditions are not included in the analysis of harmful events, the risk estimate will be conservatively overstated, as these modifiers are implicitly assigned a value of unity (≈ 1). The value assumed for any enabling condition or conditional modifier should be justified by analysis and the basis documented to support plant policies and procedures. For example, if occupancy is considered, unit access procedures, impact zone analysis and historical access records should substantiate the occupancy assumptions. Operating modes, conditional modifiers, and reactive and response layers are highly interrelated, so the consideration of these factors in the risk analysis should be performed by a skilled analyst to ensure that the factors are not taken into account multiple times.

Risk is a function of frequency and consequence. This paper is primarily focused on frequency estimation and the different techniques in evaluating its acceptability. However, consequence severity is often used to screen events for more rigorous frequency analysis. The PHA team is generally asked to estimate the consequence severity without the operation of safeguards. Since the team relies on operating experience and incident history to make their determination, they holistically include various factors that influence the severity, including operating modes, reactive and response layers, and conditional modifiers. The analyst should ensure that the estimated consequence severity does not take these factors into account before using them for frequency reduction. For example, if the consequence severity associated with a release of a toxic material considered the presence of gas detection systems that prevent entry into an area, the likelihood estimate should not also consider the system's presence.

The evaluation of harmful event frequency may consider reactive and response layers, i.e., actions to reduce harm, in addition to proactive layers. It is important to ensure the independence of these layers and the conditional modifiers, since they are often interrelated. For example, a fire and gas detection system may be used to initiate evacuation of personnel, thereby reducing occupancy. The risk evaluation should not use

both a lower probability of occupancy term and the fire and gas system as an IPL, since the reduced occupancy is the outcome of the successful activation of the fire and gas system. Likewise, the use of classified equipment could be part of the basis for the likelihood of ignition, but then cannot also be considered as a separate protection layer. Due to the complexity of distinguishing the protection layers from the conditional modifiers, procedures must consider how reactive layers and conditional modifiers will be treated in the risk assessments.

Harmful event criteria are applied in 2 ways: single scenario risk or cumulative risk.

- Single scenario risk assesses individual harmful events, e.g., high pressure leads to a release of flammable material exposing an operator to a fire (Figure 8). Typical risk criteria for single harmful events are a maximum individual risk of 10^{-5}/yr and a maximum societal risk of 10^{-6}/yr.

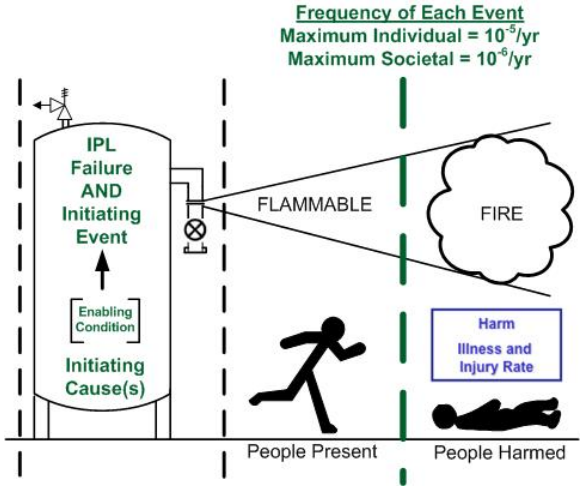

Figure 8. Single Harmful Event Criteria and Analysis Boundary

- Cumulative risk sums all hazardous events that an individual could be exposed to and determines an overall frequency (Figure 9). Since it is adding the risk associated with all of the events, cumulative risk estimates may consider the fraction (%) of time that the process is in certain operating modes. The operating mode may affect the occupancy, so occupancy should be assessed separately for each operating mode rather than using an average occupancy. All operating modes should be considered so that the overall risk of the process operation is determined.

  Cumulative risk analysis is complex, since it requires skills to assess the independence of the events and to account for common cause and systematic failures between events and protection layers properly. These analyses are best performed by specialists rather than by a team of diverse personnel. Typical risk criteria for cumulative risk are a maximum individual risk of 10^{-3}/yr and a maximum societal risk of 10^{-4}/yr.

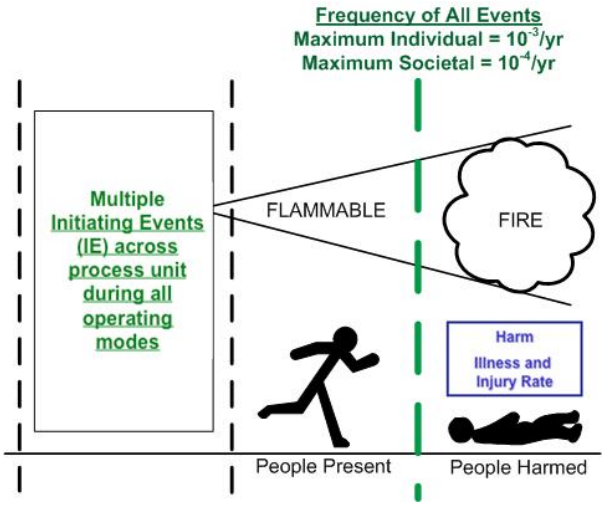

Figure 9. Cumulative Harmful Event Criteria and Analysis Boundary

3.3 Comparison of Risk Criteria

The CCPS Safety Risk Criteria Book provides two examples to illustrate the relationship of maximum hazardous event frequency and individual risk. These examples are provided below:

Maximum Hazardous Event Frequency to Single Event Criteria for Worker

Maximum Hazardous Event Frequency for Worker = 10^{-4} events/yr

- Probability of Ignition = 1.0
- Probability of Occupancy: Operator works 40 hrs/wk = (40/168) = 0.24
- Probability of Fatality: Has 50:50 chance of surviving incident = 0.5

Maximum Individual Risk for Worker: 10^{-4} events/yr * 0.24 * 0.5 = 10^{-5} fatality/yr

Maximum Hazardous Event Frequency to Single Event Criteria for Public

Maximum Hazardous Event Frequency for Public: 10^{-5} events/yr

- Probability of Ignition = 1.0
- Probability of Occupancy: Person at home = 1.0
- Probability of Fatality: Has 90% chance of surviving incident = 0.1

Maximum Individual Risk for Public: 10^{-5} events/yr * 1.0 * 0.1 = 10^{-6} fatality/yr

4. Summary

The risk analysis associated with many PHAs, such as HAZOP and What-if/Checklists, focuses on preventing loss of containment and uses criteria related to maximum hazardous event frequency. Alternatively for significant consequence events, some owner/operators and regulatory authorities require the assessment of direct harm (i.e., injury or fatality rate) and use criteria related to harmful event frequency, such as maximum individual risk or societal risk.

Depending on the analysis boundary, the factors considered during the risk assessment change. For hazardous event criteria, the assessment considers factors that affect the potential for loss of containment and release of hazardous chemicals. These factors may include proactive layers that stop the propagation of the hazardous event and enabling conditions that are necessary for the event to occur. Conditional (or frequency) modifiers are not applicable to hazardous event risk.

When harmful event criteria are used, additional factors that reduce the potential harm may be considered. These factors may include enabling events affecting the hazard presence, reactive layers including barriers and limitation systems that reduce the magnitude of the hazardous situation, and conditional modifiers affecting the likelihood of harm, such as the probability of occupancy, ignition and fatality.

5. References

[1] CCPS/AIChE, *Guidelines for Chemical Process Quantitative Risk Analysis*, Second Edition, New York (2000).

[2] CCPS/AIChE, *Guidelines for Consequence Analysis of Chemical Releases*, Second Edition, New York (1999).

[3] CCPS/AIChE, *Guidelines for Developing Quantitative Safety Risk Criteria*, New York (2009).

[4] CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008).

[5] CCPS/AIChE, *Guidelines for Process Safety Metrics*, Wiley-Interscience, New York (2010).

[6] CCPS/AIChE, *Guidelines for Safe and Reliable Instrumented Protective Systems*, Wiley-Interscience, New York (2007).

[7] CCPS/AIChE, *Inherently Safer Chemical Processes: A Lifecycle Approach*, Second Edition, Wiley-Interscience, New York (2009).

[8] CCPS/AIChE, *Layer of Protection Analysis: Simplified Process Risk Assessment*, Concept Series, New York (2001).

[9] Chastain, Wayne, "Use and Misuse of Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis (LOPA), American Institute of Chemical Engineers, 2010 Spring Meeting, 6th Global Congress on Process Safety, San Antonio, Texas, March 22-24, 2010.

[10] Summers, Angela, Bill Vogtmann, and Steve Smolen, Consistent Consequence Severity Estimation, American Institute of Chemical Engineers, 2010 Spring Meeting, 6th Global Congress on Process Safety, San Antonio, Texas, March 22-24, 2010.