Zeroing in on the Correct Risk

Jack Chosnek
Knowledge*One*
jc@knowledge1.net

Presented at
The 2012 Mary Kay O'Connor Process Safety Center International Symposium

Abstract

Keywords: PSM > Technical > Risk > LOPA

During either hazard identification (HAZID) or process hazard analysis (PHA) a measure of risk has to be determined by the team. Except maybe in the cases of full Quantitative Risk Assessment (QRA), the risk determination is somehow subjective and dependent on the composition of the team doing the analysis. One of the problems is arriving at the right consequence. Although Consequence Analysis (CA) will provide the potential effects of a release, it doesn't provide a definitive answer (the ultimate consequence will depend on factors such as early or late ignition, presence of personnel, etc.) and this uncertainty can result in choosing the wrong risk. Complicating matters, the team has to decide whether to use a consequence with personnel impact, or one with economic, environmental, or perhaps company reputation, in arriving at the risk. The decision may rest between a low consequence-high probability personnel impact and a high (or very high) economic consequence with lower probability. The solution resides in applying Layer of Protection Analysis (LOPA) in a judicious manner. We can't apply LOPA to all the scenarios discovered by the PHA team as it would be extremely time consuming. Most teams will select high risk scenarios to apply LOPA. This could lead to the determination of the wrong risk because the team has already assigned a perceived probability to the consequence when they chose a consequence level. For example, the team decided that a personnel injury would not be half as severe as the resulting economic damage for the particular scenario. By selecting only the economic scenario for further analysis because the other *seems* to have a low risk, a potentially high risk could be ignored. Only by doing LOPA for the high-consequence-level scenarios rather than the high-risk scenarios the uncertainty of the risk can be reduced. The paper will expand on this concept and show that a more effective PHA, both from the risk and the time efficiency considerations, can be conducted this way.

Introduction

In conducting a Process Hazards Analysis (PHA) it is our desire to prioritize hazards in order to resolve the potentially most dangerous first and, if resources

are available, work on the others. This prioritization not only makes sense, but it is absolutely necessary to eliminate or mitigate the high hazards given that resources are limited and not all the hazards can be worked on. Risk, a function of consequence and probability, is the most used criterion for prioritization and it is an appropriate one since we want to mitigate the high consequence events, but we will want to put our efforts on this endeavor only if these events are probable. That is, since we need to choose, we want to work only on scenarios or events that have high consequence and a high probability of occurring, or in other words, high risk. But what if we can't assess those risks correctly? Are we leaving behind potential events with hazardous consequences that may have a reasonable probability of happening?

In order to be sure we could conduct Quantitative Risk Assessment (QRA), but this process is very laborious and expensive and cannot be justified for regular PHAs. It is possible that after going through the process of zeroing on the correct risk we will find a risk that is inordinately high and has to be reduced. If we can focus on these risks then QRA may be the appropriate tool for their reduction or mitigation. On the other hand as we will see, we can be selective and apply judiciously a semi-quantitative analysis such as Layers of Protection Analysis (LOPA) ending with a better risk assessment without incurring the expense of QRA.

Erring on Assessing Risk

For most companies in the process industries assessing risk is almost a continuous practice brought about the realization that due to the intrinsic nature of the business incidents can happen with potential loss of life or injury, harm to the environmental, and/or grave economic loss. Thus, PHAs have become a way of life for these reasons, augmented by the existing regulatory requirements (e.g. the PSM Standard 29 CFR 1910.119, RMP, and others for specific industries), and the need to properly manage change in the face of complex operations. This is a positive development as identifying hazards and reducing risks obviously increases safety and wellbeing for everybody.

The increased activity in the process hazards analysis area though brings some dangers. Companies have not yet fully factored in their planning the necessary resources for conducting PHAs and resolving their recommendations. Pressures abound to minimize the time spent on PHAs and even more on coming up with fewer recommendations. The result is a tendency to underestimate risk either consciously or subconsciously, the latter being probably still the more prevalent mode. Even when the company is prepared to spend the time and money there may not be enough trained and experienced people to set up a knowledgeable team or there may not be a well-qualified and experienced facilitator available.

How is risk underestimated? Since risk is a function of consequence and probability, we can underestimate consequences or underestimate probability or

even worse, underestimate both at the same time. Probability underestimation is enhanced by overestimating the effectiveness of safeguards. These will be discussed further. It is not uncommon, though, to be using a risk matrix that has ill-fitting consequence and probability levels. Although building a proper risk matrix is outside the scope of this paper, the influences of the matrix on the behavior of the team that leads to the wrong assessment will be discussed.

Even though underestimating risk can lead to operating under higher risks than thought, overestimating risk can also have negative effects as it can lead to significant overwork or on the other hand, paralysis, if all risks are indistinguishable high and it's impossible to know where to start to reduce risk.

The basis for analyzing hazards and correctly determining their risks is the discipline brought about by the PHA process. Whether the PHA is conducted using a HAZOP, a 'What If' or any other methodology, a consequence scenario needs to be developed first from a proposed deviation, the level or severity of the consequence determined next without consideration to safeguards, then followed by listing the safeguards that specifically prevent the scenario from occurring or that mitigate the consequence, and only then determining the probability of the event. Deviating from this procedure can contribute to risk assessment errors as will be seen.

Erring in Assessing Consequences

Even when formal consequence analysis (CA) is performed, only the possible ultimate effects of a process release are learned. The PHA team still needs to develop well a plausible scenario and arrive at the suitable and correct ultimate consequence. Most of the time it is a team member having direct or indirect experience with a similar scenario, or the facilitator, that will dictate the ultimate consequence. Since a process failure or deviation can result in many paths, it is important for the team to decide which path will be followed and which the most probable outcome is.

As opposed to QRA where an Event Tree can be designed to include all of the (reasonably) possible outcomes and assign a probability fraction to each branch of this tree, in a qualitative assessment a choice has to be made among the most probable outcomes. This is the where the team can go astray as the experience of the team members will weigh heavily on this decision.

We have two common types of errors in describing consequences: vagueness and undeveloped scenario.

1. **Vague Consequences**
   In this case the consequence is not well defined either due to the company's requirement to categorize consequences (e.g., safety, environmental,

economic, company reputation, etc.) and the mixing of many categories into one outcome, or lack of definition on what the outcome really is.

An example of the first type would read like this:
"…closure of valve XV-xxx would lead to loss of reflux with potential overpressure of the column T-xxx, column damage, loss of production, potential loss of containment, fire, explosion, and personnel injury."

When the team is trying to determine the level of the consequence, for example using definitions as in Table 1, it will be difficult to decide what is being rated: safety or economic loss. The difficulty lies in that one type of outcome may be more probable but less severe, while the other more severe but less probable, both estimations being dependent on the experience of the team members. If tower damage was the intended consequence the rating could have been 'Marginal' (level 2), while if there had been fire and explosion the resulting rating could have been 'Severe' (level 3) or even 'Catastrophic' (level 4).

The same example can be used to describe lack of definition. Let's suppose that the team decided that the outcome falls in the health and safety category. The outcome is still very vague because we don't know if we are rating the impact of a fire or an explosion on personnel, or on equipment reverting to an economic consequence. If the team has little concept of the radiation produced by a fire, or the impact of overpressures from an explosion, the rating of the consequence will have a very wide range.

Table 1. Consequence and Probability Definitions

Consequences	Probabilities
1. Low Safety– Light Injury/ illness Economic – Loss of <$100M	**P1. Improbable** Not expected to occur in 1,000 years.
2. Marginal Safety– Lost time injury/ illness Economic – $100M < Loss <$5MM	**P2. Rare** Not expected to occur in the life of the plant
3. Severe Safety– Significant injury/ disability Economic – $5MM < Loss <$50MM	**P3. Occasional** Likely to occur once or more times in the life of the plant but less than once in 10 years
4. Catastrophic Safety– One or more fatalities Economic – Loss of >$50 MM.	**P4. Probable** Likely to occur more than once in 10 years

2. Undeveloped Scenarios

An example of an undeveloped scenario would be half of the description of the previous example: "…closure of valve XV-xxx would lead to loss of reflux with potential pressurization of column T-xxx." It is implied here that there are no real consequences from this failure. The thinking may have been that the controls would correct the situation and nothing further would happen. The description could have gone a step further and still not accomplish the task: "…closure of valve XV-xxx would lead to loss of reflux with potential overpressure of the column T-xxx and loss of containment". We still don't know what the effect of loss of containment would be and any rating of this consequence at this stage would be untrustworthy to say the least.

The extreme of assuming that the outcome is just a pressure rise without pursuing the scenario further would only result from a very inexperienced team. This eventuality is possible but not the most probable. It would be hard to dismiss the consequences of a failed shut-off valve in a reflux line without some good explanation. If the consequence stood as just an operational upset, it wouldn't get rated or get a rating of 'Low'.

This scenario could easily have the complete range of outcomes, from 'Low' as indicated above, to a possible 'Marginal' or 'Severe' if the outcome was purely economic, or 'Severe' to 'Catastrophic' if the outcome was safety related.

Erring in Assessing Probabilities

If assessing the correct consequence is difficult, then assessing the correct probability is more difficult when doing it qualitatively. Since we typically look at failures that occur less often than the life of the process, it would be hard to find even an experienced worker that would have seen many failures of the same kind in his plant (if he has seen too many, it is time to leave his current employment – it is not a safe working place!). Thus we have to rely on experts that know the failure rates in their fields, or look for data.

So here is the first reason we underestimate probability: the experienced people in our plant may be very good at process design, or inspections, or chemistry, or environmental laws and calculations, or how things operate, but have not much experience on how, and how often, things fail. In addition, all have been trained to make things work no matter the difficulties, and are reluctant to accept the idea of processes or equipment failing or trained people making mistakes. Thus, they will tend to assign a low probability to most failure scenarios, unless having personally witnessed the failures or read about them. Even then, it will be in their own area of expertise, so the less multidisciplinary the team is the higher the chance that probability will be underestimated.

Another reason that leads us to underestimate probability is the overuse and misuse of safeguards. The more safeguards that we list, whether they are

applicable or not, the more we will get the feeling that the probability of the scenario is low. The type of safeguards that are overused (they are considered much more effective than what they really are):

- Alarms
- Operator training
- Operating procedures
- Maintenance program
- Inspection program
- Lockout/tagout program (LOTO)
- Carseal program

In reality, as CCPS points out [1], training, operating procedures, maintenance, and inspections are already built in into the published failure rates. Having them doesn't further reduce the probability of the event; not having them would increase its probability. The only time that any of these items or programs would add to reducing the probability is if the program is specifically geared towards the scenario. For example, if loss of containment is caused by corrosion due to the presence of hydrogen sulfide and sometimes water, an enhanced inspection program of the parts of the process where this is possible would indeed reduce the probability of piping failure.

The LOTO program is a good safeguard if it is well established program and the safeguard is being applied to valve misalignment resulting from incorrect operations/maintenance interactions. It many times gets misapplied because the scenario where it is used doesn't involve a handover between maintenance and operations, but an operational error during normal operation. As far as the carseal program, it many times is given a higher value than it deserves, as many of these programs are not audited frequently enough.

Alarms is another safeguard that is often overestimated. The team needs to question whether the alarm will be effective in eliciting a response from the operator (will the alarm be silenced and forgotten?), whether the operator will have the time and wherewithal to identify the potential hazard and respond, and lastly, whether the operator has the time and means to stop the sequence of events that are leading to a potentially catastrophic event. Sometimes it just means closing a manual valve but that valve may be 20 feet up in the air, or it may be a very large valve, or if it involves opening a valve against high pressure, it may not be possible to accomplish without mechanical help.

The existence of a risk matrix with risk levels that require certain actions can also influence the team's behavior and lead it to evaluate a lower probability in order to arrive at a lower risk. This results because the team believes that a given scenario shouldn't have such a high risk, or because management has provided guidance to minimize the number of recommendations which will depend on the risk level. Doing away with the risk matrix is definitely not the way to correct this.

On the other side of the coin, overestimating probability has its own problems as it distracts us from addressing the correct critical consequences.

Zeroing on the Correct Risk

Avoiding the pitfalls described above will lead to a better risk assessment but it may not be enough. When faced with potentially high consequences we should take a second look at their description and their category. If we have doubts on the final outcome, consequence analysis with the help of models may be desirable.

Let's consider the example of loss of reflux discussed above. We weren't certain if the consequence was level 3 or 4, and in assessing probability the team hesitated between level P2 and P3 (Table 1). Looking at the risk matrix shown in Table 2, we can see that if we have just one level of uncertainty each in selecting consequence and probability we could have risks ranging from 'A' (Critical) to 'C' (Moderate). If we selected a consequence of level 4, we could have risks of level 'A' or 'B' and if we selected a consequence of level 3, we could have risks 'B' or 'C'. If we had arrived at a risk 'C' we wouldn't be obligated to do anything to reduce risk and would continue to operate under a high risk. If we had arrived at a risk 'B' and the real risk was 'A', we could be operating under a very grave risk for a significant amount of time.

Table 2. Risk Matrix

Probability	1	2	3	4
P4	C	B	A	A
P3	D	C	B	A
P2	D	C	C	B
P1	D	D	D	C

Consequence

Table 3. Risk Definitions

A	Critical – risk has to be reduced before continuing operations
B	High – risk has to be reduced within a year
C	Moderate – risk should be reduced if cost effective
D	Low – risk is acceptable and no action is required

Therefore, if the same scenario can lead to two (or more) severe consequences, one should not be chosen over the other, but the two should be analyzed further.

Given the uncertainty of assessing probability we could be missing some critical risks if we don't do this. In order not to disrupt the flow of the PHA, the worksheets could be marked for further analysis at the end of the PHA, maybe with the addition of more knowledgeable team members.

In effect, any scenario that leads to a severe consequence of the highest levels should be marked for further analysis. In the case of the example all consequences having a level 3 or 4 should be analyzed further.

The correct risk from these cases with high consequence will depend on how well we assess their probability. For this we can improve the process by using LOPA. With LOPA we can analyze each safeguard (layer of protection) and better determine if it is specific to the scenario (no generalized protections), independent of other safeguards (no double-dipping) and how robust it is by looking at its probability of failure on demand (pfd) [1].

Besides improving the descriptions of the consequences, we should also strive for better description of the safeguards as it will lead us to a better estimation of the probability and will ultimately improve the LOPA process [2].

Why not use LOPA for all the scenarios? This could be done but the time invested in hazards analysis could triple. The risk reduction that can be obtained from the low consequence events doesn't justify this extra effort.

Conclusions

We are aware of the uncertainties in assessing risk when performing PHAs. In order to arrive at a better determination of risk it is necessary to avoid pitfalls in assessing consequence and probability.

For estimating consequence we should:

- Conduct some Consequence Analysis for outcomes that result in toxic dispersions, fires or explosions to better understand their effects.
- Avoid vagueness in describing the consequence. The outcome should be clear enough to easily assess its severity.
- Develop all scenarios to their end in order to achieve a good understanding of the steps in the sequence of events and properly assess their probability.
- Separate consequences which fall into more than one category (safety, economic, etc.) for individual review.
- Consider separately consequences within the same category that could reach different probable levels, if those levels are high.

For estimating frequency we should:

- Avoid generalized safeguards and use only specific safeguards for the scenario.

- Apply a reasonable value to the robustness of the chosen safeguards.

Finally, select all the scenarios that have the top two levels of consequence (the worst consequences) and conduct a LOPA on them.

References

1. Center for Chemical Process Safety (CCPS), Layer of Protection Analysis, Simplified Process Risk Assessment, AIChE, New York, NY 2001.
2. Bayutt, P., “Conducting Process Hazards Analysis to Facilitate Layers of Protection Analysis”, Process Safety Progress, Vol. 32, No. 5, p. 282-286, September 2012.