Risk Reduction Decision Making

Workshop on Risk Assessment and Safety Decision Making Under Uncertainty

Examples from the Chemical Industry – the DuPont Corporation – One Company's Approach

September 21 and 22, 2010

Stanley A. Urbanik
Process Safety & Fire Protection Engineering
DuPont Engineering Technologies
Wilmington, Delaware

Stanley A. Urbanik
Senior Consultant

Education

- Bachelor of Engineering – Stevens Institute of Technology - 1970

Experience

- 38 years DuPont service
  - ❖ 10 years at a plant site – Dacron Manufacturing – both technical and manufacturing roles
  - ❖ 9 years in Project Engineering as Lead Project Engineer and Process Engineer

    Projects were global and were executed using “in house” as well as Full Service Design Contractors
  - ❖ 19 years in current role as Process Hazards Analyst and Consultant. Almost exclusively for DuPont operations.

Current Roles and Responsibilities

- General Process Hazards Analyst for the Corporation – new projects and existing plants.
- Risk analysis when needed – primarily LOPA (Layer of Protection Analysis). Fault Tree and Event Tree Analysis.
- CCPC (Center for Chemical Process Safety) book Committees for LOPA.
- Corporate LOPA Team Leader and Technology Guardian.
- Corporate Trainer for the internal 4.5 day PHA course.
- Corporate Trainer for the one day LOPA course.

Corporate Risk Reduction Decision Making

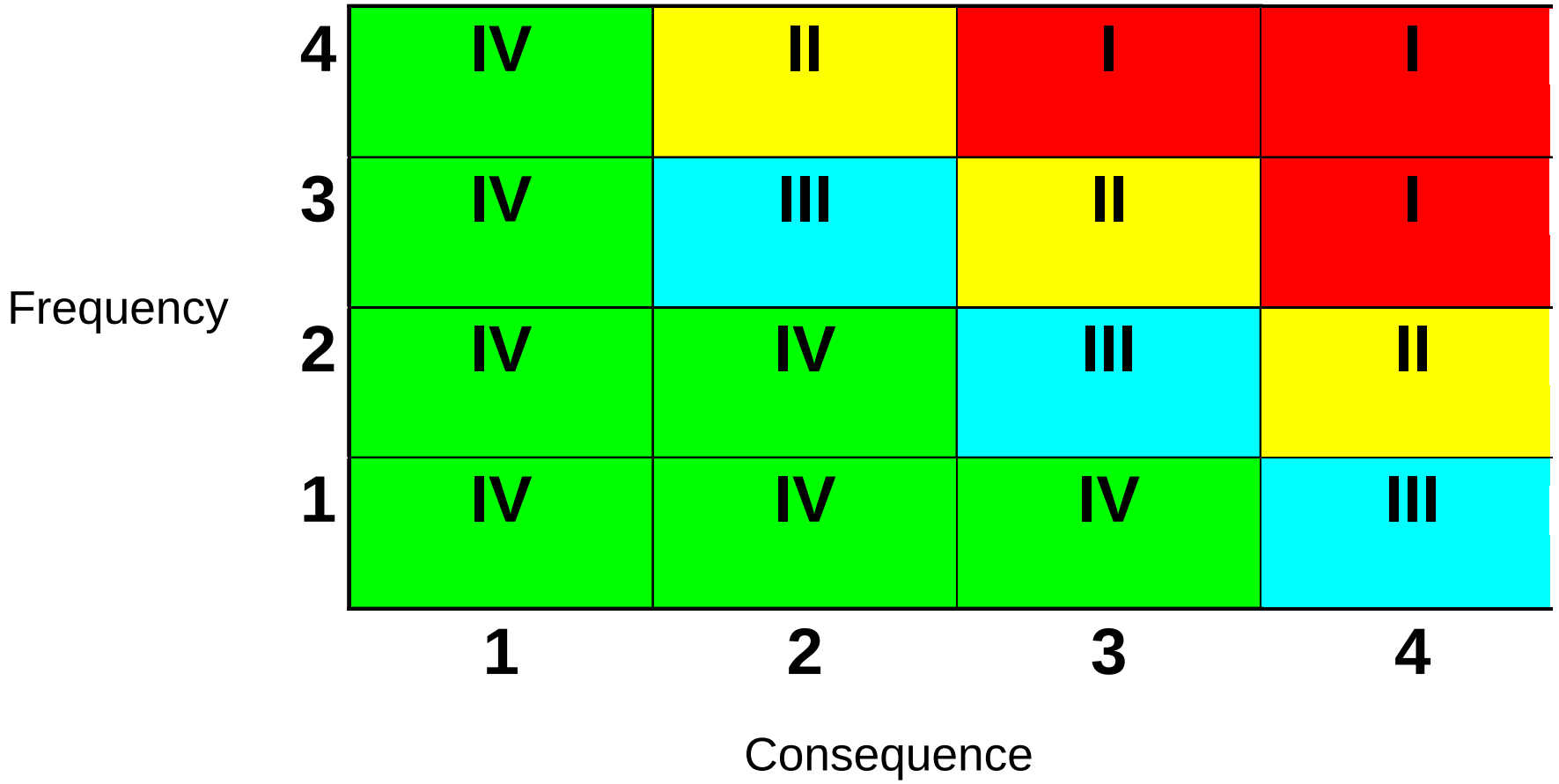
As part of general PHA activities PHA teams are expected to evaluate risk in a qualitative (or semi quantitative) manner and make appropriate recommendations to reduce risk.

Scenario (event) evaluation requires a classification of consequence usually in terms of significant injury or fatality. However, significant environmental consequences are also evaluated in this context.

The frequency (or likelihood) of occurrence of the consequence is determined by an evaluation of the complexity of the process control and safety layers (including human interaction).

The following graph shows the relationship between frequency and consequence to arrive at a “risk” level for the event.

Risk Graph for Scenario (or event) Evaluation



Risk Graph Information

Consequence ranges from 1 to 4. 4 is the worst consequence typically one or more fatalities.

Frequency ranges from 1 to 4 and generally represents the following order of magnitude ranges:

1. Very unlikely usually less than 10^{-4}/year.
2. Unlikely 10^{-4}/year to 10^{-3}/year.
3. 10^{-3}/year to 10^{-2}/year.
4. Greater than 10^{-2}/year or within the next 100 years.

Risk Ranking and Recommendations

Risk categories range from I to IV

- A risk ranking of IV is considered low enough not to require risk reduction recommendations.
- A risk ranking of III is considered manageable so long as all relevant engineered and administrative controls are identified and kept in a reliable state.
- A risk ranking of II suggests that a risk reduction recommendation should be made and acted on in a reasonable amount of time (usually within one year).
- A risk ranking of I requires an immediate risk reduction recommendation and should be in place within six months. This risk ranking may also lead to further analysis though tools such as LOPA or fault tree analysis.

A Word about Fault Tree Analysis

- Fault Tree analysis is used sparingly and has its best impact when used to compare process design, control, and/or safety instrumented function design (reliability).
- Using a fault tree solely to generate a “Top Number” that fits into a pre-defined risk criteria is OK but can be miss leading depending on the chosen failure rate values.
- The top event should be defined in terms of the frequency of the explosion event or toxic release event. Conditional modifiers such as the chance of people being present or the chance of the wind direction blowing towards a populated location should be evaluated in the discussion of results.

Example 1: Fault Tree Results used to Recommend Additional Safety Layer

Situation:

•Plant with very high pressure process and highly flammable/reactive process material was found to have marginal or inadequately designed rupture discs protecting a specific piece of process equipment.

•If the vessel failed during a high pressure event such as a decomposition the release of process material would lead to a very large vapor cloud. This size vapor cloud and its proximity to high temperature equipment almost guarantees a vapor cloud explosion (probability of ignition assumed to be 1.0).

•Vessel strength and connected piping dynamic analysis concluded a rupture at the bottom connection of the vessel was the most likely release point. Also a decomposition event would produce high enough pressure to exceed the yield strength in this part of the system design.

Example 1: Fault Tree Results used to Recommend Additional Safety Layer (con't)

Analysis:

•Plant personnel had prepared a fault tree analysis for this part of the process. The fault tree contained several branches describing other possible outcomes other than a partial confined vapor cloud explosion that could result in a fatality such as a major fire in place of the explosion.

•All of the branches modeled the route(s) to the fatality consequence by adding to the analysis conditional modifiers such as the chance of people present or fire fighters in the area when an explosion occurs. The analysis also included branches that accounted for the release occurring at elevations where the chance for enough cloud confinement made the likely-hood of significant overpressures minimal.

•The inclusion of conditional modifiers in the fault tree allowed a casual observer to conclude the risk was not very high so a redesign of existing rupture discs was not necessary.

Example 1: Fault Tree Results used to Recommend Additional Safety Layer (con't)

My Analysis and Recommendation:

- The branch that modeled a ground level release was also the branch with the highest frequency contributing to the top event.
- The branch could not take credit for overpressure protection via the rupture discs since the effectiveness was questionable.
- When looking at the branch frequency without conditional modifiers the frequency of this large vapor cloud release was once every 275 years (0.0036/year). This frequency was the result of the plant experience in terms of actual decompositions per year and one safety instrumented system that detected the high temperature associated with decomposition and opened a dump valve to de-pressure the process to a safe location.

Example 1: Fault Tree Results used to Recommend Additional Safety Layer (con't)

My Analysis and Recommendation:

I presented my way of looking at the situation in the following way:

•Having a loss of containment event due to internal decompositions once every 275 years is unacceptable because the rest of the analysis depends on luck.

•The fact that we are solely dependent on one safety layer (the safety instrumented system) is not acceptable when we know that industry practice includes the use of properly sized rupture discs.

•If the rupture discs are properly sized and discharge to a safe place, credit for this safety layer can be conservatively taken as a pfd of 0.01. This would be a frequency reduction of two orders of magnitude. The resultant frequency would be 0.000036/year or once every 27,500 years.

Example 2: LOPA Results Used to Reduce the Reliability Requirements of a Proposed SIF.

Situation:

•A plant site currently runs a process that produces large amounts of a highly toxic gas. This gas can be used in Industry and it is piped to an adjacent facility that processes the gas into a useable and saleable product.

•A release of this gas through the process vent will impact the surrounding community. Therefore it is essential the gas is destroyed if the neighboring plant stops taking the gas.

•Typical scrubbing with caustic solutions will destroy this gas. The process has a scrubbing system available to receive the diverted gas flow and destroy the toxic component before the gas stream exits through the vent.

•The scrubbing system is “ON” whenever the process is running. Meaning the caustic recirculation pumps are running and all controls that monitor flow and caustic condition are active. If anything goes wrong with the scrubbing system the process will be shut down until the scrubber is fixed. This means the scrubbing system has “announced failures” with relatively short “repair times” (relative to the operation of the process). This is not a typical “standby” system where failures are typically unannounced.

Example 2: LOPA Results Used to Reduce the Reliability Requirements of a Proposed SIF (con't).

- The caustic recirculation tank is monitored for concentration and when needed additional (higher concentration) caustic is added.
- There is a toxic gas analyzer exit the scrubber that will detect the toxic gas. If the concentration measured in the scrubber exit exceeds a certain value the process is interlocked down. This is a SIL 1 interlock (pfd assumed to be 0.1 for this analysis).
- During a cyclical PHA the plant team recommended to interlock the higher concentration caustic on high toxic gas concentration exit the scrubber. The interlock action will be to inject through a separate line directly from the high concentration tank to the scrubber. After performing a LOPA they concluded this interlock needed to be SIL3.

Example 2: LOPA Results Used to Reduce the Reliability Requirements of a Proposed SIF (con't).

My Analysis and Recommendation:

•Since the scrubber is in continuous operation while the process is running the typical analysis for a standby system characterized by the term "undependability" did not apply. There is no pfd (probability of failure on demand) component and the only concern is if something like the circulation pump failed during the time the scrubber is needed to destroy the gas. The question is: How many hours during the year is the scrubber treating the toxic gas? Typically the customer taking the toxic gas will know in advance the need for us to divert to the scrubber for some time (usually 2 to 3 hours) while they work on their process. These outages typically number 4 to 5 times per year. Therefore the total time at risk for the operation is approximately 15 hours per year. We assumed 90% plant utility so the total hours of operation are 7884 hours. The fraction of time the plant is at risk is calculated to be 15hours/7884hours = 0.0019.

Example 2: LOPA Results Used to Reduce the Reliability Requirements of a Proposed SIF (con't).

My Analysis and Recommendation:

•We now look at the range of failures that could occur during the time the system is in operation (such as pump failure, control loop failure, etc). Account for the plant's actual experience with this system. We assumed an unexpected failure that would stop toxic gas destruction once every 5 years (0.2/year).

•If the scrubber fails while treating the toxic gas the failure is likely to be detected by operations through flow and pressure indications. Operator's attention to scrubber operation is sharpened during known treatment times. We assigned a 0.1 pfd to this operator action.

•The frequency of an off plant release of toxic gas at this point is: 0.2/year X 0.0019 X 0.1 = 3.8 e -5/year or once every 26,000 years.

Example 2: LOPA Results Used to Reduce the Reliability Requirements of a Proposed SIF (con't).

My Analysis and Recommendation:

- The proposed SIL3 SIF is excessive. A SIL1 SIF would conservatively decrease the event frequency by another order of magnitude or once every 260,000 years. When the SIF is designed the actual pfd could be significantly better then the assumed 0.1 providing a final event frequency close to 1 e -6/year or once every 1,000,000 years.
- It should be noted that the SIF to stop the process is initiated on the same exit analyzer used in the proposed new SIF. Since the two interlocks are not "independent" only the new SIF would be counted in this analysis.


DUPONT
The miracles of science™