ioMosaic®
Minimizing risk. Maximizing potential.®

Part 2 How Much Safety Is Enough?

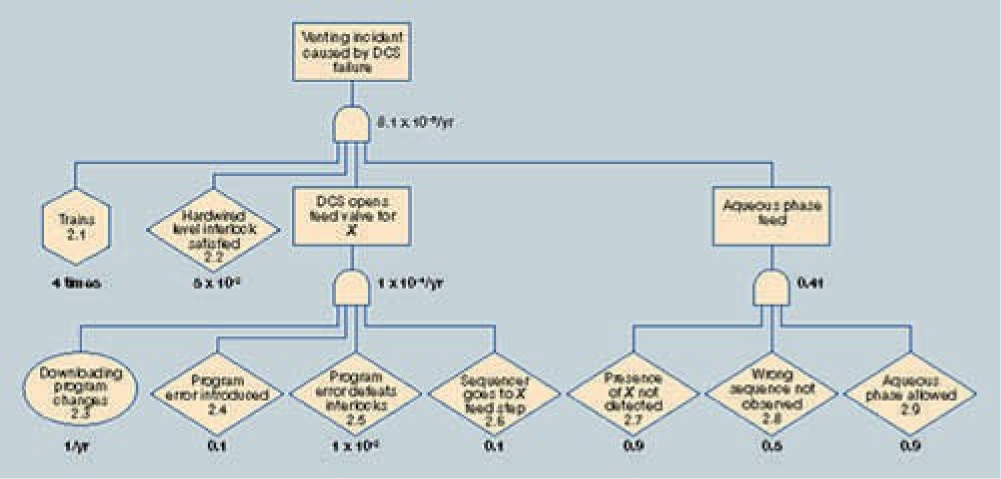
2023-06-01 - Corporate Communications - Comments (0) - News

In this second installment, Georges A. Melhem, Ph.D., FAIChE, and Pete Stickles continue their discussion on using a risk-based approach to cost-effectively meet required safeguards without compromising operating safety.

Fault Tree Analysis (Continued)

Fault tree analysis can also be applied to situations involving a combination of human error and control system failures (Fig. 1). The process analyzed in this fault tree involves batch chemistry in which one of the reactants (chemical) reacts violently with water. The concerning issue is feeding an aqueous phase into a reactor filled with a chemical. One scenario investigated was initiated by a distributed control system (DCS) failure. The fault tree in Figure 1 depicts the failure sequences for an uncontrolled process venting in such a scenario. The frequency of the top event is less than 1 x 10-5 /yr, which complied with the established critical-event tolerability criterion.

Figure 1. Layers of Protection


Venting incident caused by DCS failure
8.1×10^{-6}/yr
Trains 2.1
4 times
Hardwired level interlock satisfied 2.2
5×10^{-2}
DCS opens feed valve for X
1×10^{-4}/yr
Aqueous phase feed
0.41
Downloading program changes 2.3
1/yr
Program error introduced 2.4
0.1
Program error defeats interlocks 2.5
1×10^{-2}
Sequencer goes to X feed step 2.6
0.1
Presence of X not detected 2.7
0.9
Wrong sequence not observed 2.8
0.5
Aqueous phase allowed 2.9
0.9

Another technique that falls between qualitative and fully quantitative methods is a Level of Protection Analysis (LOPA). The approach begins with identifying a hazard scenario that consists of an initiating cause (loss of coolant circulation) and a corresponding undesirable consequence (vessel rupture due to runaway reaction). Scenarios may be drawn from other process safety endeavors, such as a Process Hazard Analysis (PHA), risk surveys, or Management of Change (MOC). The likelihood of the cause is established in terms of a failure rate or pre-established likelihood ranking criteria. The assigned likelihood value only considers the initiating cause frequency and excludes any existing Independent Protection Layers (IPLs).

Next, the number and type of IPLs are determined. IPLs can be engineered (equipment) or administrative (procedural) controls. However, all IPLs are not created equal. Some measures (probability of failure, unavailability) of the protection afforded by certain IPL types must be assigned (Dowell, 1997). For example, a procedure involving operator intervention (e.g., 0.1) will provide less protection than an independent interlock (e.g., 0.01). Using the number of IPLs and the assigned protection credits, a numerical measure of the total protection can be calculated. The product of this value and the cause frequency provides a likelihood estimate that can be compared to the tolerance criteria. If the likelihood is judged as intolerable, another IPL should be considered.

Risk Tolerability

This example of risk tolerability involves using the critical-event tolerability criterion. For process facilities, experience suggests that values for critical-event criteria fall in the range of 10-4 /yr to 10-5 /yr. Consequently, the frequency of any fault tree top event with the potential for fatality or off-site health impact should be less than the specified criterion. Some companies have a maximum individual risk (individual at maximum risk) criterion of 10-5 /yr, and use the same value for critical-event criteria. This criterion is based on the rationale that if the event frequencies are 10-5 /yr, the individual risk criterion for all events should be achieved. One of the worked problems in API RP– 752(5) uses these individual risk criteria:

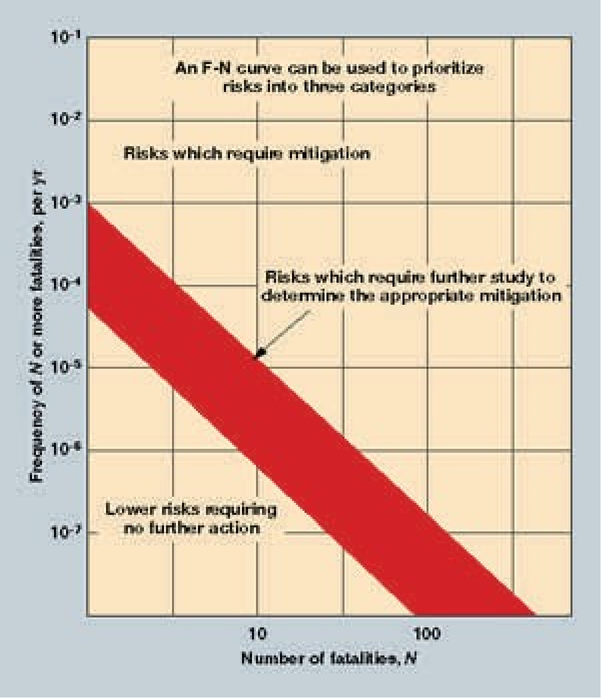
- >1.0 x 10-3 — Risk mitigation or further risk assessment is required
- 1.0 x 10-3 / to 1.0 x 10-5 — Risk reduction should be considered
- <1.0 x 10-5 — Further risk or assessment reduction need not be considered

While these criteria are presented in API RP 752 as an example, the magnitude of the values is consistent with other references (Bendixen, 1987).

When catastrophic events at process facilities can potentially impact the general public, require regulatory agency involvement, or require senior management reassurance regarding its risk exposure, a fully Quantitative Risk Assessment (QRA) is appropriate. The QRA is considered a tool for analyzing tertiary levels of safeguarding. It should account for other primary and secondary safeguards designed in facility equipment and management systems. Again, this raises the issue of suitable tolerance criteria. Since QRAs often address the risk to society in addition to individual risk, the criteria must be appropriately crafted (for example, in terms of the frequency of one or more impacts).

Two common methods of presenting QRA study results include Individual Risk Contours and F-N (Frequency-Number) for societal risk assessment. A typical individual risk criterion might be that the 10-6 /yr contour should not exceed the facility fence line. For societal risk, criteria often take the form of a line of demarcation or bands on an F-N plot, as illustrated in Fig. 2.

Figure 2. Individual Risk Contours and F-N (Frequency-Number)

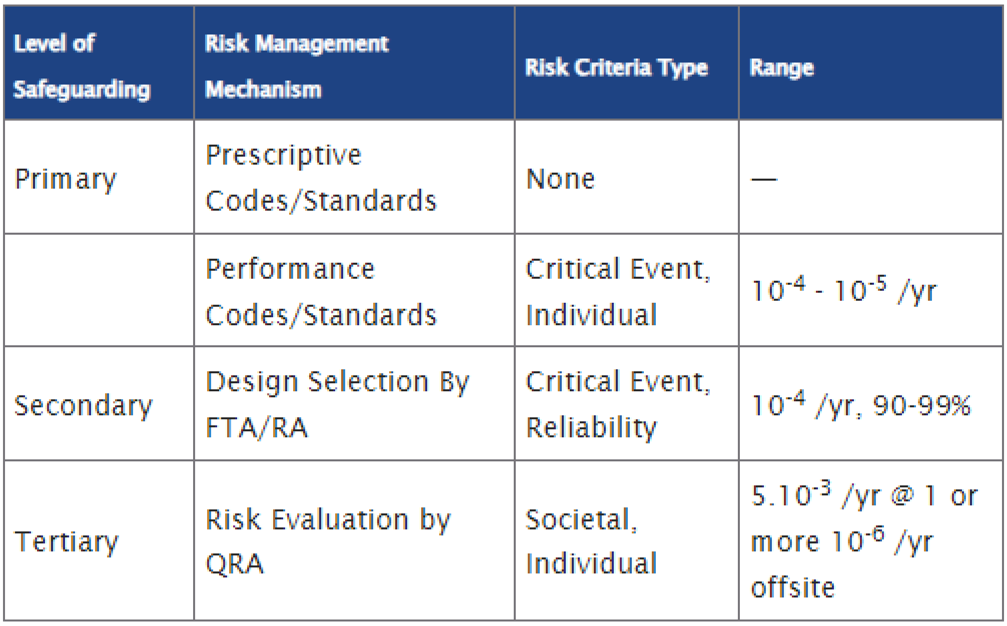


Calculated risk profiles that fall above the top line are considered intolerable and must be corrected. Profiles found below the bottom line require no further mitigation. For profiles between the lines, additional mitigation should be investigated, with the goal of moving the profile closer to the tolerable region.

Weighing Risk

Multiple levels of safeguarding can be used to manage process risk, depending on the potential consequences. In general, the greater the perceived catastrophe, the more layers of protection are required. This trend is away from only relying on prescriptive codes and standards for protection from major incidents, to using performance-based standards for process risk management.

Table 1. Safeguarding Selection Criteria



Level of Safeguarding	Risk Management Mechanism	Risk Criteria Type	Range
Primary	Prescriptive Codes/Standards	None	—
	Performance Codes/Standards	Critical Event, Individual	10^{-4} - 10^{-5} /yr
Secondary	Design Selection By FTA/RA	Critical Event, Reliability	10^{-4} /yr, 90-99%
Tertiary	Risk Evaluation by QRA	Societal, Individual	5.10^{-3} /yr @ 1 or more 10^{-6} /yr offsite

To make rational risk decisions regarding the needed various levels of safeguarding, risk criteria are required. Such criteria are not only useful but essential for making rational cost-benefit decisions regarding how much safeguarding is reasonable.

We Can Help

A QRA is an invaluable method for making informed risk-based process safety planning decisions, as well as being fundamental to any facility siting decision-making. The ioMosaic team has performed such assessments on a wide range of facilities such as refineries, chemical plants, pharmaceutical plants, tar sands, crude oil refineries, and more. Contact us at **1.844.ioMosaic** or **send us a note** via our online form for answers to questions about your risk management needs.