How Much Safety Is Enough?

2023-03-24 - Corporate Communications - Comments (0) - News

Current design codes and standards primarily seek to mitigate catastrophic consequences from process incidents. The standards guide engineers on equipment to avoid failures. Since the focus is on consequences, these design specifications may not fully address incident frequency and provide coverage for double or triple jeopardy. Although, in many instances, the motivator for developing and adopting these guidelines was due to high equipment failures.

Consequently, companies that seek sound guidance to correctly assess cost and benefit from loss control measures must broaden the approach and consider risk-based evaluation techniques. Using a risk-based approach on processing systems, engineers can cost-effectively meet required safeguards without compromising operating safety.

Risk-based Approach

Existing performance-based codes and standards provide primary and secondary levels of safeguards. For example, ISAS84.01 and API RP-752 essentially codify risk management criteria. However, companies should also consider ways to assess the costs and benefits of loss control measures through risk-based decision-making methods. A risk-based approach incorporates failure analysis coupled with risk tolerability criteria. This method provides an inclusive means to reach a decision.

Codes and Standards

The goal of avoiding multiple injuries and fatalities has guided the development for many current codes and standards (see Table 1). While the probability of multiple injury/fatality incidents such as tunnel fires, bridge collapses and nuclear reactor containment failures is low, the public shows a consistently high intolerance for these incident types. A sequence of single-fatality incidents resulting in the same total number of fatalities is somewhat more readily tolerated — even though the frequency and likelihood of each incident are greater. The result is a nonlinear value function that has encouraged the codification of mitigation measures or engineered controls to avoid high-consequence risks.

Until recently, most risk-avoidance codes and standards had a prescriptive nature. They prescribed in exacting detail how to design a system or piece of equipment. Now, performance-based design guidelines and standards are beginning to include risk management decision-making concepts.

Performance-based design guidelines and practices include:

- ISA-S84.01 — 1996 Design of Process Safety Instrumentation
- CCPS — Guidelines for Design Solutions for Process Equipment Failures
- API-RP752 — Management of Hazards Associated with Location of Process Plant Buildings

These practices provide designers and managers some flexibility to trade off risk reduction benefits, design complexity, and cost. At the same time, they presume that overall safety will not be compromised. To achieve this goal, applying these practices requires a risk tolerability benchmark against which to judge the risk level achieved by a given design.

Table 1. Unreliability Of Level Interlock Systems With Consideration Of Common Cause Failures

Code	Description	Avoided Incident
ASME Section VIII	Unfired pressure vessels	Pressure vessel mechanical failure
ANSI B31.3	Chemical refinery piping	Piping mechanical failure
NFPA 68/69	Venting/containment of deflagrations	Equipment failure due to internal explosions
API 650	Atmospheric storage tanks	Tank mechanic failures
API 752	Facility siting	Plant building fatalities
API 2510	LPG installations	Flammable vapor clouds and BLEVE (boiling liquid expanding vapor explosion)

Deming said about manufacturing processes, "What you don't measure, you can't manage." The equivalent of the risk management process would be, "Without tolerance criteria, you can't make rational risk decisions." While it is not the intent of this discussion to address developing suitable risk tolerability criteria, however, organizations that intend to adopt performance-based design practices must tackle this issue. Without tolerability criteria, it will be impossible to obtain consistent decisions regarding safety design. Furthermore, once such criteria have been established, they enable process safety designers to optimally use other quantitative tools, such as fault tree analysis, reliability analysis, and quantitative risk assessment (QRA) and apply them in risk management situations.

Fault Tree Analysis

Designers, familiar with the traditional prescriptive codes, know that they focus heavily on the risk from mechanical and electrical causes of initiating events and less on events induced by process-control failures and human error. **However, in today's operating environment, highly automated processes and fewer operators (hence, more demands per individual) are common.** Currently, companies must also manage the risk of incidents from these causes. Fault tree analysis can be effective in establishing the relative frequency of potential incidents associated with base-case and alternative design concepts. The technique is versatile; it can handle equipment and control failures and human errors. A good example of the application of fault tree and reliability analysis for evaluation of safety interlock systems has been reported by R. Freeman.

Different integrity levels for an interlock can be established:

- Class A — Fully redundant
- Class B — Redundant final element
- Class C — No redundancy

In Table 2, Freeman demonstrates the level of reliability analysis that can be applied. Also, Table 2 provides the decision-maker with a good measure of the reliability trade-offs for a given mission requirement.

Table 2. Unreliability Of Level Interlock Systems With Consideration Of Common Cause Failures

Mission Time	Mission Time, HR	Unreliability % Class C	Unreliability % Class B	Unreliability % Class A
1 shift	8	0.010	0.007	0.005
1 day	24	0.0290	0.020	0.016
1 week	188	0.200	0.140	0.110
1 month	720	0.870	0.610	0.490
1 quarter	2,160	2.610	1.840	1.490
6 months	4,320	5.220	3.690	3.030
1 year	8,760	10.580	7.540	6.390
18 months	12,960	15.660	11.220	9.780
2 years	17,520	21.160	15.270	13.720

Freeman, R.A., "Reliability of Interlocking Systems," Process Safety Progress, Vol. 13, No. 3, July 1994.

This methodology also offers a means of setting reliability tolerance criteria for different classes of interlock integrity level (e.g., Class A — fully redundant). For example, Table 3 presents the interlock reliability (1 — unavailability) for the three level interlock classes as a function of proof testing interval.

Integrity Level	Redundancy	Test Interval	Reliability, %
Class A	Full	Monthly Quarterly Annually	99.5 98.5 93.5
Class B	Final Element	Monthly Quarterly Annually	99.3 97.8 90.9
Class C	None	Monthly Quarterly Annually	99.1 97.4 89.4

The data accounts for common mode failures. As seen in Table 3, there is a tradeoff between testing frequency, and the advantage gained by selecting the next integrity Class. With monthly proof testing, the gain in reliability between Class A and Class C is only 0.4%. Therefore, cost-benefit considerations would suggest quarterly or yearly proof testing. Alternatively, if a Class 1 interlock is intended to be 99.5% reliable, then monthly proof testing must be mandatory. By performing similar analyses for flow, temperature, and pressure interlocks for a specified test interval, the designer can set generic reliability criteria for each interlock integrity level, allowing latitude for achieving the required reliability.

Stay tuned for the second installment, where Georges A. Melhem, Ph.D., FAIChE, and Pete Stickles continue with fault tree analysis and risk tolerability.

We Can Help

We can help you comply with internal company standards and global industry standards. ioMosaic is at the forefront of process safety management (PSM) proficiency, having worked with numerous industry groups and companies to develop safety and risk management systems, guidelines, standards and audit protocols. Contact us at **1.844.ioMosaic** or **send us a note** via our online form. We would love to hear from you.