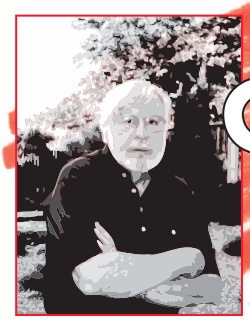

Outside the Lines

"Problems cannot be solved by thinking within the framework in which the problems were created." – Albert Einstein

by Ira J. Rimson and Ludwig Benner, Jr.

Follow-Through: It's Good for Golf; It's Great for System Safety

"If you keep doing what you did, you're gonna keep getting what you got."
– Yogi Berra

System Safety's Expectations

In system safety, we analyze hazards and risks, both before systems become operational and after. At least, that was system safety's original concept. Predictive safety analyses provided initial baselines for designs against which operating experiences could be tracked and assessed. Unexpected operating experiences generated re-examination of the predictions. Actions were then taken to improve system performance by modifying operations to ameliorate risks that had not been recognized by the pre-operational analyses, or which had crept into the system unanalyzed. If needed, pre-operational analyses were updated. That's the way life-cycle system safety management is supposed to work. Does it?

Procedures Get "Tweaked" After Predictions Fail

Once a system becomes operational, system safety practitioners' skills and efforts are typically redirected. Instead of continually feeding deterministic operational data back through original predictive analyses, it is more common to view disparities as nothing more than operators "failing to do what's expected of them." Corrective actions can then address others' aberrant behavior which, after all, is much easier to change than correcting a fundamental flaw in an analyst's system's design.

Dr. Vernon Grose, in his volume on loss prevention, explained the current approach toward corrective action:

"We all share a natural tendency to want to take a deep breath after instituting a corrective or preventive action — and consider it done with. Having wrestled either with a loss or with its hypothetical scenario and decided on what you will do to mitigate it, you cannot help having a certain sense of relief and security. A preventive action — once implemented — is often treated as "out of sight, out of mind." Unless an accident or loss occurs which that action was supposed to have precluded, it is simply left in place to function." [1]

In efforts to minimize disruptions, most post-operational functional changes are made incrementally, trading off marginal risk avoidance with marginal operational interference. The result of these reactive "tweakings" is often what we would characterize as "suboptimization by substandards," an approach that not only fails to correct the original system deficiency, but often generates new risks from new, unanalyzed intrasystem interactions.

Sometimes Systems Get Shaken Up

Sometimes changes occur that challenge systems' designers or managers to re-examine system fundamentals, so as to instantiate new technology or new operational concepts, with remarkably efficient results. Shifts from vacuum tubes to transistors, from manual inventory audits to bar codes, typewriters to computers, film to digital cameras, drawing boards to CAD, and gas stoves to microwave ovens are all examples of new system approaches that followed creative change.

---

[1] Grose, Vernon L. *Managing Risk: Systematic Loss Prevention for Executives.* Chapter 30, "Assuring 'Preventive' Preventive Actions," p. 344. Englewood Cliffs, New Jersey: Prentice Hall, 1987.

System Safety Shook Up the Safety Field Once

System safety can claim credit for a major shake-up in approaching risk management: developing and applying predictive logic tree-based safety analysis methodology. Today that methodology base is approaching its 40th anniversary. Does it need re-examination? Our observations suggest that critical re-evaluation of the efficacy of current system safety approaches to risk management is overdue. In its original concept, system safety analyses were applied throughout systems' life cycles, an application that seems to have fallen out of favor. One of the marks of professionals is that they continually engage in examining and revalidating their work. Are system safety analyses continually being validated? Examples of accidents suggest not.

Is Another Shake-Up Needed?

In our opinion, Dr. Grose was an optimist. Cursory review of *recent* U.S. Chemical Safety and Hazard Investigation Board (CSHIB) reports indicates that "risk managers" rarely bother even to try to ascertain common threads that carry through multiple repetitious mishaps. The following accident examples should motivate questions about how well they understand the nature of their responsibilities, and how the effectiveness of current safety management methodologies suffers as a result.

Example #1: Report No. 2001-03-I-GA:

"¶4.3 In the 1990 HAZOP, the team identified failure of the extruder drive as a condition that could create a 'no flow' situation, in which case it was recommended that the polymer flow be stopped. The polymer catch tank and the reactor knockout pot were the only possible destinations to which the flow could be diverted. However, the HAZOP team did not consider this situation as a possible cause of excess polymer accumulation and level in either vessel. The 1990 HAZOP study did not completely evaluate the extruder. The team noted that insufficient design information was available to conduct a full analysis and recommended a follow-up HAZOP of the extruder once the engineering drawings were finalized. This analysis was never conducted.

"¶4.4 In a 1993 incident, the polymer catch tank was overfilled when the extruder malfunctioned. Polymer was carried into the vent line and solidified, and the line had to be cut. Nevertheless, the 1999 HAZOP still failed to identify the means by which an excess level could occur in the vessel."

These precursors to the fatal explosion that occurred as the subject of this CSHIB investigation demonstrate unequivocally that none of the responsible safety analysts or managers took prior events seriously enough to examine the system's operation in sufficient detail to identify the existence of a potentially disastrous risk absent system change. Shortcoming: Failing to recognize that when a hazard isn't identified, fixed ***and*** monitored, the risk remains.

Example #2: Report No. 2001-05-I-DE:

"The [M] MOC [Management of Change] procedure allowed the change initiator to request a process hazard analysis (PHA) from the site PSM [Process Safety Management] coordinator. However, it provided no guidance on when to request a more comprehensive hazard analysis, such as a hazard and operability (HAZOP) study. The MOC for the tank conversion did not request a more thorough PHA."

In this case, the company's procedures allowed for initiating a new PHA, but didn't spell out to the manager how, when or why to do it. Apparently, upper management assumed that was something a professional safety analyst would be able to figure out for himself. Guess what? Shortcoming: Assuming that the safety analyst would recognize the hazard and do something about it without having to be led by the hand.

Example #3: Report No. 2003-01-I-MS:

"FCC performed a process hazard analysis (PHA) of the equipment in the batch process in March 1996. The PHA included literature searches on the thermal stability of MNT, as well as data from previous incidents involving the material. As a result of this effort, operating limits were added to the procedures, and recommendations were implemented that resulted in additional safeguards being added to the batch vessel. However, there was no system to apply evaluation results from the batch process to continuous processing equipment. No hazard analysis system was in place for the continuous MNT distillation columns because — in this older, ongoing production process — the potential hazards were not fully recognized."

In this case, the process changed from batch to continuous processing, and operational managers *assumed* that the hazards were constant despite the change in operational process. Shortcoming: Lack of hazard recognition because of ignorance of the hazard differences between the processes, and lack of follow-up once the new process was initiated.

Example #4: Report No. 2002-01-I-AL:

"Root Causes[2] *... Neither the chemicals that could be introduced into the sewer nor the hazards of their interac-*

[2] Assignment of Root Causes is *always* conjecture. For example, let's start with the definition of the term, which (as far as we can determine) has at least a dozen definitions, depending on which training course the originator is trying to sell you.

tions were identified. No formal hazard review or MOC analysis was conducted when connecting sewer lines from the tank truck unloading and chlorine dioxide areas to the acid sewer. Consequently, no scenarios leading to the possible release of H_2S were identified, nor were warning devices placed in the area."

In this case, we'd suggest that the safety analysts were depending on prayer or rune casting in preference to actually doing their jobs. Shortcoming: Failed hazard recognition as a result of misunderstanding, neglect or stupidity.

Example #5: Report No. 2003-06-I-TX:

"CSB concluded that neither the liquid waste hauler nor the disposal facility emphasized the importance of minimizing the inadvertent collection and disposal of crude oil or condensate when removing BS&W (basic sediment and water) from production storage. … more than two-thirds of [Exploration and Production personnel] interviewed stated that they believe all BS&W possesses a negligible flammability hazard."

Misunderstanding and misperceptions run rampant — the "everybody knows" defense of technical incompetence. Shortcoming: Hazard recognition — but give us a break, folks. Even a kid with no high-school chemistry should have been suspicious.

Example #6: Report No. 2002-02-I-NY:

"The containers gathered for consolidation on the day of the incident had been unused in the workplace for many years. The lead worker . . . assumed that the containers . . . contained spent etching solution..."

When mixed, they reacted violently. You know what they always say about the verb "assume," but in this case they actually risked their asses. Shortcoming: In the absence of usable information and knowledge at the site, the hazard and attendant risks were unrecognized.

Example #7: Case Study No. 2003-03-C-OH:

*"¶**5.3.1 Process Hazard Analysis.** The … process hazard analysis (PHA) team acknowledged that liquid nitric oxide presented an explosion hazard; however, the team did not understand the significance of the risk to employees. Although at least two PHAs documented that detonation of liquid nitric oxide is a 'credible scenario,' neither analysis comprehensively addressed the previous incidents involving NO detonation."*

Looks like the "Gee, it's only going to be a small explosion" thinking. Shortcoming: Hazard recognition — they knew that the hazard was there; they just didn't recognize that it posed a risk to real live people.

Example #8: Report No. 2003-07-I-NE:

"[The] MSDS for zinc stearate slurry — used by [W] corporate personnel to evaluate the material as an antitack agent — did not include combustible dust warnings."

Aha! The old "if it's not in the regs, it doesn't exist" excuse for not bothering to thoroughly analyze the hazards critically. Shortcoming: Hazard recognition — failing to recognize hazards because they're not recognized by the Supreme Authority. About as useful as, "We're from the government and we're here to help you."

Example #9: Report No. 2003-09-1-KY:

"[C] did not have effective procedures for evaluating the hazards associated with nonroutine operating conditions."

Of course, the only way this could occur was for the safety analysts to *assume* that conditions on the line were perpetually constant, including the people. Shortcoming: Hazard recognition, due to blind faith in the *assumption* that once the process commenced operation, it continued uninterrupted and unchanged in perpetuity, and the failure to see that the possibility of new hazards arising from changed conditions demanded contemplation.

Example #10: Report No. 2004-01-I-IN:

"A hazard review of the scrap system might have revealed significant hazards, especially if the review was repeated after the system was operating. In such a review, experienced employees with hands-on knowledge can discuss the difficulties inherent in operating and maintaining a system — which provides an opportunity to recount past incidents, such as those at the [H] facility mentioned earlier in this report."

Classic example of the "out of sight, out of mind" faith-based theory of safety management. Shortcoming: Failing to recognize hazards because of faith in the idea that inherent risk avoidance can be achieved by geographic separation, and then forgotten. "It happened there, but it can't happen here, because that was there and this is here."

While each case above involved different circumstances, each demonstrates a common shortcoming: Unrecognized hazards that were controllable by anyone who actually took the time to look for them, and used effective tools to do so.

So What?

Were all these hazard-recognition problems the result of discrete individual shortcomings amenable to "tweaking?" Or were they evidence that system safety practitioners have been willing to ignore the follow-through required to assure safe system operations throughout their life cycles? You know our call. What's yours?