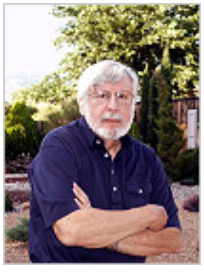
System Improvement *Should Be* the Objective of Investigations



by Ira J. Rimson and Ludwig Benner, Jr.

"All the successes of engineering as far back in history as the pyramids and as far into the future as the wildest conceptions of mile-high skyscrapers may be imagined to have begun with a wish to achieve something *without failure*, where 'without failure' to the engineer means not only to stand without falling down but also to endure with what might be called 'structural soundness.'"[2]

In a 1996 paper[3] , we urged system safety practitioners to view operational system mishaps and their subsequent investigations as opportunities to evaluate the validity of their predictive analyses. Since then, we have observed that the utility of many investigation reports for assessing predictive analyses is compromised by systems managers' vagueness in specifying desired investigation outputs. By looking for "fault" and "blame" rather than for how to improve system performance, investigators mire themselves in myriad events that didn't happen rather than the one set of events that did. Only the events that *did* happen can confirm your predictions or tell you what needs to be changed, both within the system and within your *a priori* analysis.

"By looking for 'fault' and 'blame' rather than for how to improve system performance, investigators mire themselves in myriad events that didn't happen..."

Predictive analyses are designed to estimate the probabilities of as many alternative scenarios as imagination can generate.[4] Some of those scenarios will happen, some can but probably won't, and some cannot happen at all. Predictive analyses predict what *might* happen. They don't explain what *did* happen. Once a mishap occurs, the probability of those specific interactions and outcome happening is P=1.0. The probability of any other confluence of

events producing that specific outcome is P=0. Statistically derived probabilities aggregated from prior occurrence data are meaningless once something happens. Furthermore, each false lead (P=0) of the probabilistic methodology must be explored to determine that it didn't occur — which brings us to a major deficiency of most mishap investigations: The Dreaded "Did Not."

---

[1] "Problems cannot be solved by thinking within the framework in which the problems were created." — Albert Einstein.

[2] Henry Petroski, *To Engineer is Human*. New York, Vintage Books, p. 53, 1992.

[3] Subsequently published in *Hazard Prevention*, vol. 33, No. 1, pp. 10-13, First Quarter 1997.

[4] Rimson, I.J., "Why Accident Investigations Don't Prevent Accidents." Presented at the Texas A&M University Center for Process Safety, 2003.

It's much easier for the mishap investigator to specify what didn't happen, because there are so many more "didn't happens" than "did happens." In fact, there are (∞-1) events or scenarios that didn't happen, and only one that did. System safety practitioners need to demand robust evaluation of their work to ensure it improves the system. It's not comfortable to tell the boss that you don't know *why* your predictive analysis did not forestall the undesired system operation.

Let's take a look at a specific government accident report in which the investigators' "did nots" stifled the understanding needed to improve both process efficiency and safety analyses.[5] ("Did nots" are identified in italics.) Chapter 4.4, "Process Hazard Analysis," states:

> "During design in 1990 and again in 1999, after several years of operating experience, Amoco conducted process hazard analyses[6] of the Amodel process using hazard and operability (HAZOP) techniques.[7] Both the polymer catch tank and the reactor knockout pot were considered during the analyses, but *credible scenarios that could lead to excess pressure or level were not identified*."

This vague "did not," in the passive voice, asserts that anyone and everyone who performed the HAZOP analyses (more than one) *did not* identify any scenarios that led to undiscovered pressures which might expel the contents of the process vessel. We don't know *why* these scenarios weren't identified; was it faulty investigation methodology, or the way it was implemented?

---

[5] U.S. Chemical Safety and Hazard Investigation Report No. 2001-03-1-GA (June 2002): "BP Amoco Thermal Decomposition Incident, Augusta, GA, March 13, 2001."

[6] A Process Hazard Analysis ("PHA") is a structured examination of a chemical process to identify factors that have the potential to create hazards; to uncover credible sequences of events (scenarios) that could result in undesired consequences; to evaluate the consequences of these scenarios should they occur; and to propose improvements, as warranted, to equipment, procedures and management systems that reduce or eliminate the

hazards, prevent the scenarios from occurring, or mitigate the consequences.

[7] HAZOP makes use of guidewords to help identify deviations from normal, intended operation that could result in potential hazards or operating problems.

> "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.*"

This statement, in contrast, is unambiguous and explicit, yet once again omits any rationale for *why* the HAZOP team did not consider the scenario that precipitated the mishap.

> "The 1990 HAZOP study *did not completely evaluate* the extruder. The team noted that insufficient design information was available … and recommended a follow-up HAZOP of the extruder once the engineering drawings were finalized. *This analysis was never conducted.*"

"If we don't know why the system broke, we can't define the problem and fix it."

Here is an example of a multiple "did not." Although the first states explicitly that the study's evaluation was limited and why, the second is a vague, passive-voice statement that lacks any assignment of accountability that might provide insights into what happened.

> "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.*"

The authors inserted the literary surrogate "failed to" in place of "did not," a common misdirection that, in addition, interjects the opinion of the report's author(s) that a perpetrator strayed from the expected standard(s) of conduct. ("Nevertheless" is a clue that a value judgment is about to follow.)

“Overfilling contributed to the March 13, 2001, incident because it was partly responsible for plugging the vent and relief piping – which confined the mass of plastic to the polymer catch tank. *If the HAZOP studies had identified credible scenarios* involving vessel overfilling and overpressurization due to extruder malfunctions, [then] additional safeguards *could have been recommended* to reduce the probability or severity of the hazards. *If overfilling had been effectively controlled,* [then] the sequence of events that led to the March 13 incident would have been less likely – even without knowledge of the decomposition hazard.”

This illustrates the "if – then" syllogism form of the "did nots;" e.g., HAZOP studies missed credible scenarios of vessel overfilling because of extruder malfunctions, which we now know are credible because they happened. That leads to the "double conditional negative"; *i.e.*, the HAZOP didn't identify the scenario, so it didn't recommend appropriate safeguards. But why? This is also known as the "if we had some ham, we could have had ham and eggs, if we had some eggs" analysis.

> "During the 1990 HAZOP, the team recognized that *high pressure could occur in the reactor knockout pot if the emergency pressure relief system discharge line was plugged* with solidified polymer. A recommendation was made to provide a system to ensure the line was clear during operation, *but no such system was established.*"

This exemplifies the reverse syllogism: "then – if," compounded by the passive-voice whine that somebody (who?) didn't establish a feasible system to avoid the mishap.

> "In the 1999 HAZOP, the team determined that the emergency pressure relief system was an adequate safeguard in the event of plugging the normal vent. *They did not recognize the credible scenario that both the normal and emergency vents could simultaneously plug with polymer,* as occurred on March 13."

This "did not" lets the HAZOP team off the hook by stopping the investigation report before it gets to the critical answer to *why* the team didn't recognize a credible scenario. Was it ignorance of the system's operational characteristics? Or lack of imagination? Or missing design data? Or cover-up for institutional deficiencies? If we don't know why the system broke, we can't define the problem and fix it.

These are a few of the forms of “did not” that are inserted into mishap reports to avoid identifying explicit deficiencies or behaviors that need changing. Will any of these conclusions help improve the system’s operation? Don’t bet on it. Stick your neck out and specify to the investigators that you need them to identify *what happened*, define specific deficiencies – without “did nots” – and make specific recommendations to change the behaviors that produced the mishaps.