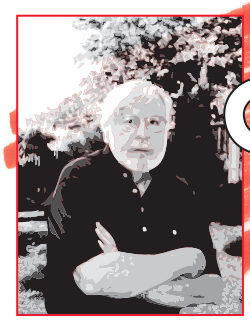

Outside the Lines

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

by Ludwig Benner, Jr. and Ira J. Rimson

Hazard Analysis for Dynamic Systems

"Prediction is very difficult, especially about the future."
— Niels Bohr

How do you, as system safety analysts, approach the task of identifying hazards in systems? How do you find out the attributes and behaviors of a system or operation you will analyze? Do you apply similar analytical methodologies once systems have entered operation as you did earlier in their development, when they were mere concepts? How trustworthy are your analyses and recommended actions, and how long are they valid? How do you demonstrate to managers that they should act on your analysis of a system?

Hazard identification and remediation are predictive analytical tasks. Any predictive task is challenging. Its difficulty increases and its accuracy decreases as the complexity and ambiguity of the system and its operation increase. Systems' operations are processes, and processes are dynamic. They involve interactions among constituent components. As a general principle, the more ambiguous the definitions of a process's interactions, the less trustworthy are predictions of its future behavior. Predicting behavior of ill-defined processes or systems' operations becomes a subjective guessing exercise, making it impossible to validate or verify analytic results.

We would not dispute that system safety analyses ideally should begin as early in new systems' development as feasible. Let's look at the inputs system safety analysts deal with during their analyses.

Early efforts usually envision a new system as a collection of unique bits and pieces, which have been assembled to fulfill a specific purpose. Designers typically describe and document conceptual stages of systems development in natural language, or schematic or flow charts that depict components and their interactions statically. Those descriptions pose an immediate problem for system safety analysts; hazards are dormant in stasis. Hazards only become threats to successful achievement of designers' objectives after systems commence operation. It is unlikely that systems designers eagerly await analyses of in-service mishaps to discover how, when and where their inventions will fall victim to the unintended consequences of systemic fragility. System safety analysts need better data and information with which to make the transition from descriptions of static system architecture to definitions of dynamic system operation.

In a paper presented to the System Safety Society more than 10 years ago, Benner identified these information barriers between system designers and system safety analysts, and proposed that they could be minimized by standardizing specifications for system definitions and descriptions:

"System definition vs. system description. … I discerned a distinction between requiring definitions of the system operation, and descriptions of the system attributes:

A *system definition* identifies each component of the system or subsystem, and what it must do, when it must do it, and on whom or what it must act to produce the desired outcomes. A system definition describes *dynamic interactions,* among people, procedures and things — and their influences on the outcomes.

A *system description*, on the other hand, may describe the system in terms of its components and their specifications, functions, physical or spatial relationship to each other, content flows, accident experiences, failures, failure rates or other *static attributes, rather than*

interactions.[1] [Emphases in original and added.]"

Components' applications within new systems' configuration and operation are usually original to those systems. Robust definitions of the systems and their operation may not yet exist. System safety analysts often must assume that data from seemingly similar components, systems and operations are appropriate for adoption as surrogates for selected components or operations in the new system.

The limitations of definition data provided for safety analysis require analysts to try to visualize the system both statically as described, and dynamically in operation. They may then attempt to discern the system's planned behavior and unintended occurrences that might pose threats to its components, its operation, or its environment. Adamski and Westrum call this ability to foresee hidden traps "requisite imagination."[2] We concur that an active imagination is an essential prerequisite to successful safety analyses. However, identifying dynamic system hazards is clearly too important to be left solely to the vagaries of analysts' imaginations. Safety analysts rarely possess sufficiently detailed knowledge of systems' conceptual designs to define their dynamic operations accurately enough to perceive all potential hazards. Too many opportunities arise for ambiguous, incompletely defined or poorly documented system dynamics to invite oversights and omissions in hazard analyses. Their outcomes are left to be discovered during consequent mishaps and their investigations.

The U.S. Chemical Safety and Hazard Investigation Board's (CSB) investigation of a breakdown that occurred at Augusta, Georgia, on March 13, 2001, documents an example of omissions that resulted from unidentified scenarios leading to an unplanned, fatal outcome.[3] In its report, the CSB devoted sections to both Process Hazard Analysis and Design Deficiencies:

"4.4 Process Hazard Analysis
During design in 1990 and again in 1999, after several years of operating experience, Amoco conducted process hazard analyses[4] of the Amodel process using the hazard and operability (HAZOP)[5] technique. 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."

The report also described how the lessons learned from operating experiences did not find their way back into the facility's safety analyses. The CSB published schematic illustrations and a narrative description of the process, but did not report exploring the system description that was supplied to the HAZOP analysts, or the reasons for the HAZOP oversights. These undiscovered and uncompleted scenarios indicate that the operating dynamics of the system, and potential deviations, were left to be postulated by the analysts, rather than included in the system definition, both before and after design changes were introduced.

The incident raises other questions, e.g.:

- If the systems analyzed are ambiguously defined, are uncertainties about their assumed behavior(s) communicated adequately up the line to those who could take actions based on the results of those analyses?
- Are the ambiguities of systems' definitions taken into account in analysts' predictions of undesired outcomes?
- How do analysts persuade management that their analyses are trustworthy, and a valid basis for action?
- If analysts suspect that potential hazards exist within the framework of their assumptions of the systems' dynamic operation, what obligation do they have to confirm the validity of their speculation?
- If designers want to introduce new designs to the operation, do they know what change data

---

[1] Benner, L., "System Safety Analysis Pitfalls," *Proceedings of the 15th International System Safety Conference*, Washington, DC, August 13-17, 1997, pp. 393-398. See: http://www.iprr.org/papers/SS97lb.pdf.
[2] Adamski, A. J. and R. Westrum. "Requisite Imagination: The Fine Art of Anticipating What Might Go Wrong." *Handbook of Cognitive Task Design*, Erik Hollnagle, Ed.; Lawrence Erlbaum Associates, 2003, p. 193 *et seq*.
[3] U.S. Chemical Safety and Hazard Investigation Board. "BP Amoco Thermal Decomposition Incident," Report No. 2001 03-I-GA, June, 2002. See http://www.chemsafety.gov/index.cfm?folder=completed_investigations&page=info&INV_ID=2.
[4] 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 their consequences.
[5] HAZOP makes use of guidewords to help identify deviations from normal, intended operation that could result in potential hazards or operating problems.

should be fed back to the safety analysts?

The need for good system definitions should be self-evident. Unfortunately, system safety analysts have yet to develop requirements for definitions of dynamic systems' operations that they are called upon to analyze.

Curiously, the CSB report cited design deficiencies *after* its discussion of BP-Amoco's process safety analysis. There, too, the evidence pointed to the fact that hazard analysts found it impossible to make a transition, from *assumed* similarities extrapolated from prior seemingly relevant operations to the new environments posed by the fully dynamic commercial operation:

"4.5 Design Deficiencies

… The design for the commercial manufacturing facility was based on several years of experience in pilot-plant and semiworks (sic) operations. …

The polymer catch tank level indicating instrument was unreliable and prone to false indications. Additionally, it often broke when waste plastic was removed from the vessel, and frequently it was not replaced before restart.

Spring-operated pressure relief valves on the polymer catch tank and the reactor knockout pot were intended to protect the vessels from overpressure. However, neither relief valve was shielded from the process fluid by a rupture disk."

All of these operational failures derived from the inability of the hazard analysts to imagine the new system's definition. Lacking the requisite imagination, they fell back on assumptions that the new system was functionally equivalent to what they'd seen in the past. It was likely that the new system's designers were equally blindsided by the system's unanticipated behavior. They, too, had neglected to develop and complete an accurate exposition of the system's definition.

From the olden days, in the memories of us olden guys, we can remember listening to Ella Fitzgerald as she sang:

I blow thru here
The music goes 'round and around
Whoa-ho-ho-ho-ho-ho
And it comes out here.
I push the first valve down
The music goes down and around
Whoa-ho-ho-ho-ho-ho
And it comes out here.[6]

Systems' designers should be similarly specific in defining their systems' operations.

[6] "The Music Goes Round and Around," by Mike Riley & Eddie Farley, lyrics by Red Hodgson, published in 1935.