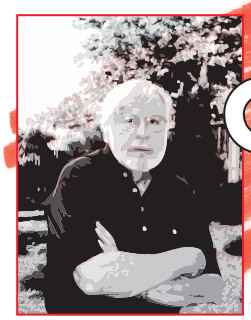

Outside the Lines

"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.

Introducing the X-Tree

"Hell is other people." — Jean-Paul Sartre

"Especially when they don't do what you expect them to do." — Rimson's Corollary to Sartre

"Human operators instantiate infinite variance into otherwise rational systems." — Chernowitz's Third Law of Mathematical Reality[1]

In his "TBD" column in a recent *Journal of System Safety*, Charlie Hoes identified a serious inadequacy of conventional system safety methodologies as follows: "Of course, we will do everything we can to prevent an air leak, but all of those efforts will be at lowering the probability of having an event, not in providing safety should an event occur." Hoes might have illuminated one of system safety's Blinding Glimpses of the Obvious had he not continued: "Reducing the likelihood of an air leak into the system helps reduce the risk. However, we believe that we cannot lower the probability of an event enough by controlling air leaks. Additional risk-reduction measures are needed."[2]

What additional measures? Unfortunately, he didn't elaborate. His assurance that risk reduction measures *will* be found reflects the conventional wisdom of system safety practitioners, who focus predominantly on modifying event probabilities.

The obvious next question is: "Why?"

At what point have we "lower[ed] the probability of an event *enough*..."? Lowering the probability of occurrence to some arbitrarily acceptable level does not prevent an undesired event from occurring. The ugly truth is that if an event *can* happen, regardless of how infinitesimal its likelihood, then professional responsibility demands that its occurrence be considered to have a probability (P=1), at least until analysis of the severity of its occurrence is established, and appropriate action taken to mitigate any critical effects.[3]

This appears to be yet another example of the 10-to-the-minus-pick-a-number *reductio ad absurdum* that makes a system "safe enough" to be acceptable. Lowering probability of occurrence to some arbitrarily acceptable level does not relieve system designers from providing for reactive risk-mitigating operating practices *after* a critical undesired event occurs.

The "Tree" △ or "Top-Down" Fallacy

System safety's trees, charts, graphs and analyses are currently designed primarily for analyzing and revising systems so that a negative occurrence with assumed consequences will happen less frequently than some arbitrarily assigned number. This results from deeply ingrained

[1] The late George Chernowitz, Founder and CEO of American Power Jet Co.
[2] Hoes, Charlie, "TBD." *Journal of System Safety*, V. 42, No. 5, Sept.-Oct., 2006, p.5.
[3] C. O. "Chuck" Miller, often regarded as the father of system safety, frequently observed that, "The only accident that *won't* happen is the one that *can't* happen."

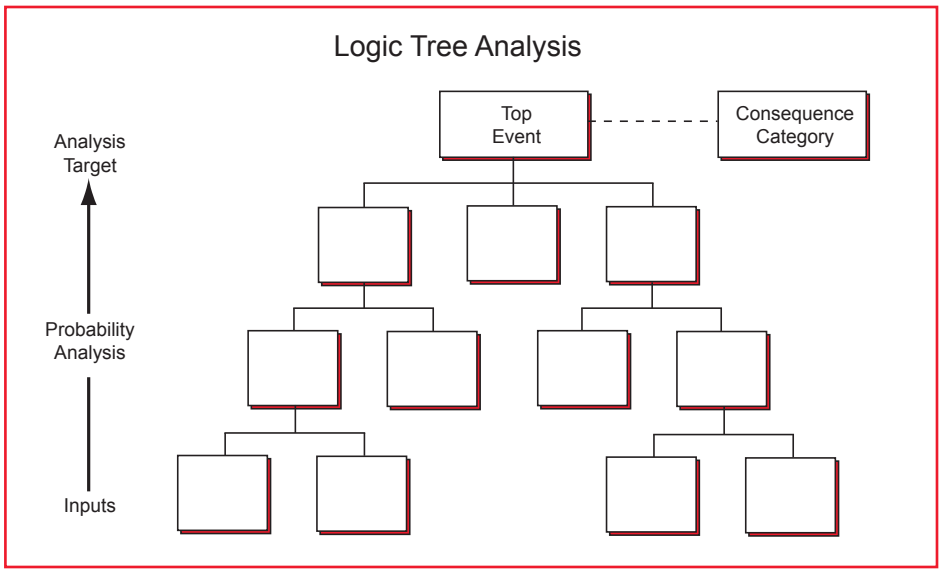

Figure 1 — Logic Tree Analysis.

40-year-old thinking that has evolved from dominant analysis tools such as Fault Trees[4], Failure Mode and Effects Analyses[5] and HAZOPs[6].

In fault trees, "top events" are the focal point of system safety analyses. Avoiding or minimizing the probability of an undesired top event or condition has become the *de facto* system safety goal. In criticality analyses, consequences of undesired top events are assigned one of a limited number of alternative assumed consequence level categories, rather than specifically defined outcomes.[7] For example, in system safety's Risk Assessment Code (RAC) matrices, analysts guess at severity levels to determine the consequence coordinate rather than specifying worst-case scenarios. By accepting a generic "severity" rather than defining specific events, attempts at remediation focus on changing the probability of the top event's occurrence, rather than mitigating the increased risks that result therefrom.

Where people are involved in outcomes, the probability that top events will occur is almost infinitely variable. Nevertheless, analyses can lead to standardized behaviors that can reduce variance. The same is true when anticipating how people will react after a top event occurs.

Principal system safety objectives can encompass *both* minimizing the probability of undesired top events' occurrence *and* minimizing the negative effects of those occurrences. Rather than continue analytical exercises that support only binary solutions — complete prevention or accepted loss — the current focus on top events might easily be aimed toward controlling the variability of human operator reactions to mitigate risk when undesired top events do occur.

The X-Tree: Another Approach

One approach toward expanding the current top-down analytical framework to encompass both before-the-fact probabilities and after-the-fact mitigation alternatives is to rotate the current logic tree orientation 90° clockwise from vertical to horizontal, and add the divergent outcomes, as in the X-Tree illustration below. Everything to the left of the X's intersection at the point/time of the undesired top event's occurrence is the current probabilistic analysis; to

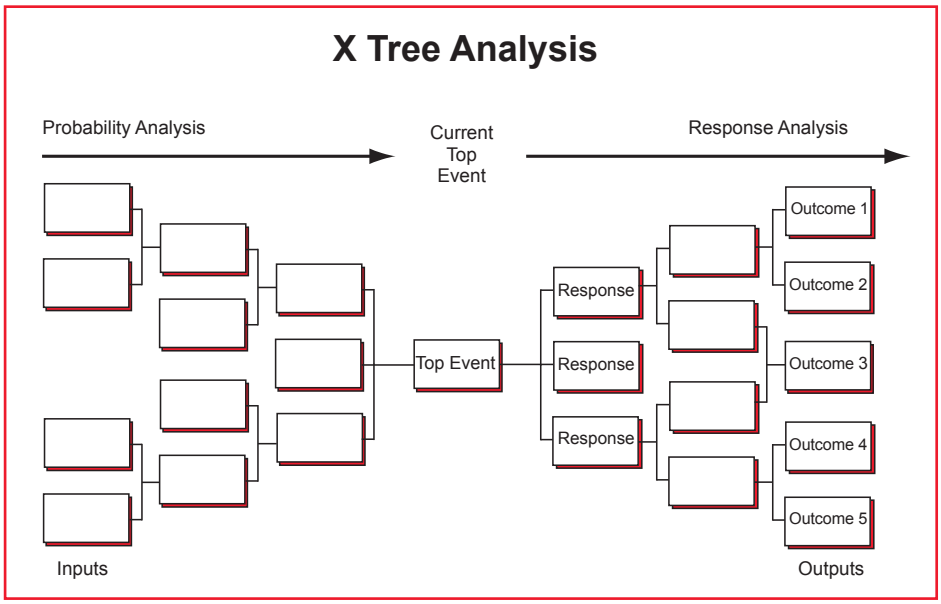

Figure 2 — X Tree Analysis.

[4] "The purpose of a Fault Tree Analysis is to assess a system by identifying a postulated undesirable end event and examining the range of potential events that could lead to that state or condition." — *System Safety Analysis Handbook*, 1999, p. 3-132.
[5] "The purpose of the FMEA is to determine the results or effects of sub-element failures on a system operation and to classify each potential failure according to its severity." — *Id.*, p. 3-119.
[6] "HAZOP, the Hazard and Operability Study, is a method of group review of the significance of all of the ways that a process element can malfunction or be incorrectly operated." — *Id.*, p. 3-148.
[7] "The FMECA is an analysis procedure which documents all probable failures of a system within specified ground rules, determines by failure modes analysis the effect of each failure on system operation, identifies single failure points, and ranks each failure according to a severity classification of failure effect." — *Id.*, p 3-123.

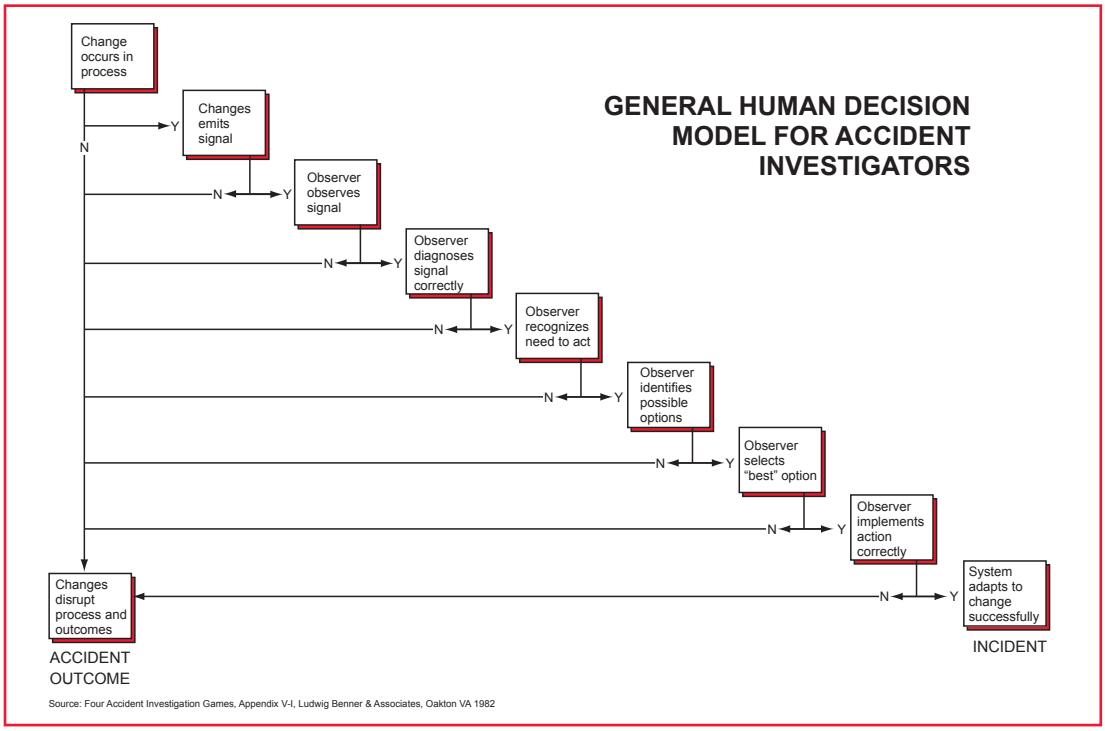

Figure 3 — General Human Decision Model for Accident Investigators.

the right are analyses of likely *post-facto* responses and outcomes when the event actually occurs.

This approach guides analysts toward considering both pre- and post-top event continua. A secondary benefit of the change is adapting the current analysis into a timeline, which becomes essential when analyzing alternative recovery reactions from an undesired top event that happens at a time-critical juncture.

This approach has been applied effectively in the past to identified undesired top events. In the hazardous materials transportation field, safety efforts traditionally were directed at preventing hazmats from being released. When releases occurred, local emergency responders were expected to cope with the consequences. The large number of casualties that resulted from this *ad hoc* approach demanded attention. Analysis and documentation of the behaviors of released hazardous materials identified ways to reduce both their physical uncertainties and the resulting casualties. New methods for approaching responses were defined, which resulted in much more successful outcomes for the responders: casualties during subsequent responses among properly trained responders dropped nearly to zero.[8,9]

A recent occurrence in aviation operations illustrates the need for "Outcomes" analyses when traditional system safety analysis accepts the probability of a deadly "top event" without examining potentially mitigating reactive behaviors — such as when flight crews select the wrong runway to taxi, take off or land their aircraft.

Comair Flight 5191 was scheduled to fly from Lexington, Kentucky, to Atlanta, Georgia, on the morning of August 27, 2006.[10] The crew had been cleared on 7,000-foot Runway 22, which was long enough to accommodate the take-off. After confirming Runway two-two," the captain taxied onto Runway 26, an unlit secondary runway only 3,500 ft. long, which was not long enough to accommodate the take-off. Without stopping the airplane, he turned the controls over to the first officer. Subsequent flight data and cockpit voice recorder analyses had no indication that either pilot tried to abort the takeoff, *even though the first officer remarked that the runway lights were off.* The aircraft overran the end of the runway before it could lift off, and 49 of the 50 people on board died.

When human behavior is involved, an analytic approach frequently used retrospectively — Exceedence Analysis, as incorporated in Flight Operational Quality Assurance (FOQA) programs — can also be applied prospectively. It requires that boundaries to normal behavior be established so that criteria for recognizing departures from expectations can be taught to the human subsystems: "The objective of a FOQA program is to use flight data to detect technical flaws, unsafe practices, or conditions outside of desired operating procedures early enough to allow timely intervention to avert accidents

[8] "The Story of GEBMO (General Hazardous Materials Behavior Model)" at http://www.iprr.org/HazMatdocs/GEBMO/GEBMO.html.

[9] Although the X-Tree bears superficial similarity to the *System Safety Analysis Handbook's* Event Tree Analysis (*Op. cit.* p.3-103) and Consequence Analysis (*op. cit.* p. 3-25), event trees analyze "single initiating events"; whereas in the Consequence Analysis, the "event of interest is a fault event of equipment failure" and the analyst chooses "specific accident consequences" to relate to "their many possible causes." Neither deals specifically with effects within integrated systems' operation or human behavior, and both continue to rely on probabilities of occurrence rather than assigning (P=1) to events that can occur.

[10] Information derived from NTSB reports. Accident Identification: DCA06MA064.

and incidents."[11] It requires that a set of discrete "expectations" be established for each critical operational phase. These expectations can be inserted into a decision model, which describes an expected response process when operators encounter change.[12]

Expected behaviors represent optimum human contributions to systems' operation. If the expected behaviors are not implemented, unexpected responses to change can produce undesirable outcomes. Attempting to use the wrong runway introduces such a change to the expected human decision model. The crew didn't recognize the potential criticality of the outcome.

Human operators can be trained to identify and recognize departures from expectations, and to react in predetermined ways that will mitigate undesired consequences. Examples abound of departures from expectations that resulted in undesired top events, which had negative effects that could have been lessened had systems analyses encompassed such an "outcomes approach"; e.g., Chernobyl; Three-Mile Island; *M/V Herald of Free Enterprise*; and numerous medical "misadventures."

Face the Facts, and Take Actions

The first step toward analysts' mitigating the effects of undesired top events is to acknowledge that those events *can* occur irrespective of the results of probabilistic "top event" risk assessments, and that the associated risks should not be considered acceptable without thorough analysis of alternatives.[13]

The next logical step is to analyze the ways that undesired top events can be initiated, and to identify evidence by which their occurrences can be recognized.

After those steps have been accomplished, human operators can be taught to recognize the evidence and react in ways that mitigate the outcomes. Appropriate responses will depend on circumstances: who, what, when, where, why and how, and available response time; e.g., the crew of an airplane cruising at 38,000 feet has substantially more reaction time available than one halfway down the wrong runway on take-off.

System safety analysts need to go beyond analyzing merely the probabilities of "top events" occurring, to ensure that systems' operations encompass actions to mitigate risks should an undesired top event occur. Because, unless it *can't*, it probably will.

---

[11] U.S. G.A.O. Report "GAO/RCED-98-10: Efforts to Implement Flight Operations Quality Assurance Programs, p. 3, at http://www.gao.gov/archive/1998/rc98010.pdf.

[12] "Model of Human Decision Process for Investigators" at http://www.iprr.org/3PROJ/3humdecn.html. (Although the model was developed to assist investigators retrospectively, it can be as useful prospectively for identifying responses to changes from expectations.)

[13] See Benner & Rimson, "Whose Risk Is It Anyway?" *JSS* V. 41, No. 6, Nov.-Dec., 2006.