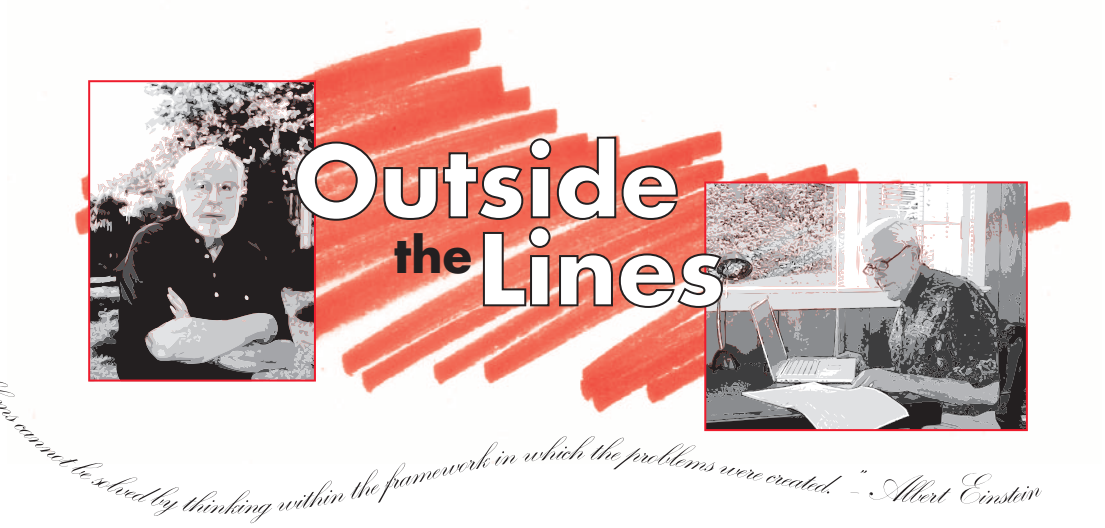

"Problems cannot be solved by thinking within the framework in which the problems were created." – Albert Einstein

by Ira J. Rimson and Ludwig Benner, Jr.

The X-Tree: Part 2

Get yourself a pessimist to tell you what could go wrong, and an optimist to tell you what could go right. And once you have both, if the answer isn't obvious, then you need a new question.

— Dale Dauten, *The Corporate Curmudgeon*

In our last column[1], we introduced X-Tree. It proposes a new methodological approach that would extend traditional system safety top-down models to analyze unplanned and undesired outcomes that could result after a "Top Event" occurs during a system's operation.

The idea that there is some accurately predictable minimum level at which catastrophic risks become arbitrarily acceptable has been disproved time and again. Unpredicted and unexpected deviations from planned systems' performance have resulted in tragedies, and subsequent demands to "do something" about them. Most unwanted outcomes result from unpredicted human responses to unexpected occurrences. X-Tree is predicated on the belief that human subsystems can minimize unwanted outcomes if they are adequately prepared to recognize deviations and react appropriately. Undesired Top Events and their precursors emit noticeable signals. Operators can be trained to perceive, recognize and act on those signals to minimize consequent harm. When signals of unplanned and undesired Top Events or precursors are determined to be below thresholds of human detection, designers can take steps to ensure their elevation to more obvious levels.

At the time we conceived X-Tree, we weren't aware that a similar-appearing analytic technique already exists. It's called BowTie™. It, and its derivatives Black BowTie™ and Black BowTie XP™[2], have been in use in the European community for more than two decades[3]. It's also used as an investigation tool in conjunction with Tripod™ and Tripod Beta™.[4,5]

BT offers a number of useful features, particularly its linking tasks to barriers and controls that can minimize or prevent hazards from evolving into risks to life and property. It considers hazard release to be the Top Event, also described both as "the accidental event" and "a loss of control."

BT's developers have also addressed post-Top Event consequences: "Each accidental event (loss of control situation) may lead to unwanted consequences." BT's derivation from Reason's model leads it to treat post-hazard-release barriers and controls identically to pre-release actions:

For any barrier there may be internal or external factors which influence its effectiveness. These are modeled as escalation factors (failure modes) each of which can be controlled by a suitable barrier. Similarly, if all barriers are breached, and the Top Event (loss of control) is reached, then

---

[1] "Introducing the X-Tree," *Journal of System Safety*, V. 43, No. 2; March-April 2007, pp. 4-7.

[2] See bowtiexp.com and governors.nl.

[3] Lewis, Steve and Cheryl Hurst: "Bow-Tie an Elegant Solution?" *Strategic Risk*, November 2005, pp. 8-10. See strategicrisk.co.uk/.

[4] See tripodsolutions.net.

[5] Henceforth, BowTie™ and its derivatives will be referred to collectively as "BT," and the "trademark" symbol will be omitted.

recovery measures should be provided to mitigate unwanted consequences. Recovery measures may have escalation factors (failure modes), and are treated in the similar way as barriers.[6]

BT addresses the need to recover from Top Events by using barriers and controls to mitigate the effects of a Top Event. Unfortunately, barrier-based analysis-and-control strategies limit the alternative options available to analysts and operators.

In contrast, X-Tree focuses on alerting operators to the need to take control of their systems' operation. Operators would be trained to recognize signals that precede, or emanate from, a Top Event. They would be prepared to apply the most appropriate of all available strategies, depending on the peculiarities of each situation, to achieve a successful outcome within their available resources.

X-Tree recognizes that human operators are the most variable of all system elements. Paradoxically, they are also the last line of defense against undesired outcomes evolving from Top Events into harm-producing processes. X-Tree emphasizes that human operators must understand in minute detail how systems are intended to operate in order to recognize deviations and intervene successfully. It acknowledges that operators within the system are the key barriers to arresting the progress of Top Events and their consequent undesired outcomes, and empowers them to recognize and deal with it.

"X-Tree recognizes that human operators are the most variable of all system elements. Paradoxically, they are also the last line of defense against undesired outcomes evolving from top events into harm-producing processes."

The significant differences between X-Tree and BT are that X-Tree practitioners would analyze how Top Events occur within their systems, and then provide alternative responses which operators can choose to avoid undesired outcomes. In contrast, BT focuses on extrinsic barriers to prevent precursors from escalating into Top Events/Accidents, then tries to anticipate and control the consequences *after they happen* with additional barriers, rather than training system operators to mitigate the consequences.

Most readers recall that nuclear plant operators at Chernobyl didn't foresee the disastrous consequences of the experiment they launched early on the morning of April 26, 1986. Despite changes to the testing schedule that previous shift operators had neglected to communicate to the oncoming shift, a sufficient number of deviations from the system's expected behavior were available to alert the crew that something was gravely amiss. The crew either did not recognize them as portents of impending disaster, or rationalized them as adjuncts to the planned experiment and dismissed them.

The Web page at en.wikipedia.org/wiki/Chernobyl_disaster describes the progress of the accident process. X-Tree, or similar analysis and training that prepared operators to recognize deviations from acceptable operational envelopes and opportunities for intervention, would surely have lowered the magnitude of the eventual outcome, or prevented the occurrence altogether.

It is a rare mishap investigation report that does not contain the conclusion that, "Operators *failed to recognize*…" or its equivalent. It is equally rare, in our experience, for similar reports to contain a phrase like, "System specifiers/designers/builders (etc.) *did not adequately prepare the operators to recognize deviations from expected operational behavior and provide appropriate actions to limit subsequent harm*."

Humans recognize situations that they have practiced, or about which they have been forewarned, much more readily than those which they have not; e.g., the pilot who is advised by air traffic control that he has "…traffic at 10 o'clock, opposite course…" is much more likely to spot the aircraft after it is pointed out, than if it was not. Similarly, rail-to-vehicle mishaps are much less frequent at level-grade crossings that are signaled with gates, flashing lights and clanging gongs than at those with silent signs whose warnings are illegible.

Another benefit of X-Tree-based analysis is its usefulness in determining the potential magnitudes of undesired outcomes. Taleb posits that in the event of asymmetric odds — i.e., non-normal distribution of outcomes, or "skewness"[7] — the frequency or probability of the loss is irrelevant, unless it is evaluated in connection with the magnitude of the outcome.[8] The closest system safety comes to this is through Criticality Analysis or, in more specific cases, by FMECA. Unfortunately, neither provides a robust quantitative product. By attaching a real value to each potential alternative outcome, risk managers can identify immediately a hierarchy of severity

---

[6] See risk-support.co.uk/Active%20Bow%20Tie.htm.

[7] Characteristic of all Rare Events.

[8] Taleb, Nassim Nicholas, *Fooled by Randomness: The Hidden Role of Chance in Markets and in Life*. New York, Texere, 2001. ISBN 1-58799-071-7. p. 82.

in terms of actual costs, providing them with a metric that is much more realistic than current "guesstimates" from "A-B-C-D" risk matrices.

Risks can take different shapes, but catastrophic results are remarkably similar, whether the losses are human, material or financial. No amount of probabilistic analyses can identify all alternate outcomes before systems begin operation. Even then, undesired outcomes — and their precursor signals — cannot all be predicted until they happen. Trained operators who know and understand their systems' operation will be prepared to recognize and deal with any deviations from normal when they occur.

Financial precursors to operational risks are also amenable to X-Tree analyses. This exchange followed the announcement in late 2006 that incompatible versions of software had been incorporated into mating sections of the Airbus AB-380. Consequent costs were estimated to reach to billions of U.S. dollars:

First:

Risk is typically defined in terms of a combination of the probability and the magnitude of the consequence (expected value) so that even events with small probability of occurrence but with large consequence need to be considered important. Given this definition, USD 19 billion would be the risk if the probability is assessed to be 1.[9]

Response:

Given that revenue loss is estimated at USD 19 billion until end 2006, the wiring-harness installation problems that are technically at the root of the delivery delays is a very expensive reported consequence of a problem with SW. Is it the most expensive such consequence to date, or is there something worse? Late or difficult SW development is not an unknown phenomenon. ***Airbus must have known a long time ago about the state of development of their wiring mock-up SW and apparently did not mitigate the business risk.*** [Emphasis added.][10]

Even if it were attainable, calculating an accurate metric of "acceptable risk" would be a fool's errand, dependent as it is on the choice of definition of "acceptable." Taleb calls attention to the mathematical truth that if time were extended to infinity, all rare events would happen irrespective of their calculated probability.[11] Relying on probability that a catastrophic event might occur but once every 100,000,000 units is meaningless. No analyst can foresee, or predict with any more rigor than chance, where or when during a 100,000,000-unit life cycle that first rare event will pounce.[12]

After that, all bets are off.

[9] Yet another example of misconstruing an arbitrary "acceptable risk" as assurance that an undesired event will not happen. "The only accident that won't happen is one that can't happen." — C.O. Miller.

[10] Personal communication.

[11] Taleb, op.cit., pp. 85-86.

[12] And, of course, then there is the question of the definition of the "units" — but we won't open *that* can of worms here.