

Expecting the unexpected: New culture to push next level safety

Risk assessment is conceptually very simple. We are looking for the answers to three questions: What can go wrong, how likely is it, and what are the consequences?

But can risk analysis, and standard safeguards based upon such assessments, protect us from the unexpected?

Imagine a complex and potentially dangerous facility, such as a nuclear power station or an offshore oil rig. Assume that the plant's equipment is highly reliable, its workers and managers are vigilant in testing and other procedures, and training is thorough. If an unforeseen accident does occur, will these high standards lower the likelihood that it will be severe? Surprisingly, the answer is no.

Origins of failure

In 1991, I was doing an assessment of the software for the main engines of NASA's space shuttle. I came upon an article by Herb Hecht of SoHaR, a U.S. provider of reliability software. In the article, titled "Rare Conditions and their Effect on Software Failures," Hecht makes four interesting points:

1. In well-tested systems, rarely executed code has a higher failure rate than frequently executed code;
2. consequences of rare failures in well-tested systems are more severe than those of other failures;
3. when there is a failure in a well-tested system, it is significantly more likely to be caused by a rare event;
4. the inability to handle multiple rare conditions is a prominent cause of failure in well-tested systems.

In short, we have tested out all of the easily found errors. What we are left with are rare errors with severe consequences.

Do Hecht's observations about software apply to other technological systems? I believe they do.

Nuclear plants, for example, regularly assess the risk of unwanted events that should be eliminated entirely. Through exceptional planning, maintenance and organizational development, the foreseeable problems are vanquished.

But they have to draw the line somewhere. Some events are of such a low likelihood -- say, 1 out of 1 million -- that they are considered acceptable. These are the unexpected, rare events. If there is a failure, chances are it will start with such an event.

Snowball effect

Hecht makes another noteworthy observation in his study: All software that failed from three rare events also failed, perhaps less severely, from two. And three-quarters of the software that failed as a result of two rare events also failed, again perhaps less dramatically, from one.

Think of it this way: If all proper procedures and conditions are in place, and if symptoms of an unwanted event begin to take us onto a failure path, it could very well be the start of a severe accident scenario. Perhaps more failures will occur to compound the situation and form a scenario that may have never been imagined, or was previously dismissed as improbable. There will be no procedures, experience nor training to aid in recovery.

Basically, the first rare failure has a good likelihood of being a harbinger of a much worse situation. The three-stage accident at Japan's Fukushima Daiichi nuclear power plant was exactly this type: earthquake, tsunami and hydrogen explosion.

Risk assessments focus almost entirely on known dangers. As a result, procedures, training, regulations and methods of operation are all designed to guard against these same threats. Rarely does an organization explore novel possibilities for failure -- scenarios that change critical assumptions, have slightly different symptoms, or include multiple failures. The myth of safety only reinforces this attitude.

To be sure, without this focus on checklists and protocol, controllable situations could easily escalate out of control, undermining day-to-day safety. Still, a second culture is also needed -- a culture of expecting the unexpected.

This requires playing "what if" with the risk model, questioning assumptions and looking at possible (if unlikely) scenarios. When there are initial indications that a system may be going astray, the second culture should kick in. This is called "having requisite imagination."

Safety is connected not only to risk but also to expectation. In operations like nuclear power plants, oil refineries or chemical production facilities -- all of which are in the well-tested category of engineering enterprises -- we must be ready for the rare events in order to defend against them.

Woody Epstein serves as manager of risk consulting at Lloyd's Register Consulting Japan. From 2011 to 2012 he was also a visiting scientist at the Ninokata Laboratory of the Tokyo Institute of Technology, where he was involved in analyzing the Fukushima disaster. The opinions expressed in this regular column do not reflect those of his employers, their affiliates or clients.