Is Estimating Probabilities the Right Goal for System Safety?

Nancy G. Leveson

In a paper about evaluating the risk of operator error, Swain suggested that probabilities for each operator action in specified procedures be evaluated and then combined. He said, however, that if the analyst goes into a nuclear power plant and sees that the labeling on the control panel is poor, the probability of an operator error should be increased, If the labeling on the control panel is good, then the probability of an error can be decreased.

Alternatively, why not just improve the labeling? Sometimes we get so caught up in an assumed goal that we lose sight of the bigger picture. The goal is not to get a probability of operator error but to reduce errors. If there is enough information to determine the probability of a design error, the better choice is to fix the problem, not adjust probabilities. This fact is true for all design errors. Our goal should be to reduce or eliminate design errors, not to measure them. As an aside, after Three Mile Island engineers took control room design much more seriously and operator errors were reduced significantly.

As another example, consider the recent Boeing 787 lithium-ion battery problems. The system was certified on the basis of an estimate that there would be no more than 1 fire in 10,000,000 flight hours. Instead, two fires occurred in the first 50,000 hours. Rumor has it that manufacturing and design flaws were not considered in the calculation. Both of these factors are difficult if not impossible to assign a probability to. The battery problems created large losses for Boeing in terms of money, schedule, and reputation. When the fix for the problems was created, the fix was certified (as I understand it) not on the basis of a probability calculation (as in the original design) but on the basis of a design analysis.

I usually hear two arguments in favor of the use of probabilistic risk assessment. One is that regulators do not know enough about the systems they are certifying to understand a qualitative analysis. I would counter that if they do not understand the design and cannot understand a qualitative analysis of it, then they cannot evaluate the correctness of any probability they are given. Simply accepting any number provided by the applicant does not justify having a certification authority.

The second argument is that without a probabilistic risk analysis or preliminary hazard analysis (PHA), management cannot decide how much effort should be put into controlling hazards and what compromises should be made in the design stages. A preliminary hazard analysis usually combines severity and likelihood. The problem is that before the system has been used for a significant amount of time, likelihood is unknowable. So people make up numbers. For systems that are basically the same as existing systems for which historical behavior is available, relatively good likelihood estimates can be used. But for new systems and systems using new technology (such as software, which is almost always created anew for each system), there is no historical information to mine for likelihood. In practice, these estimates usually are made for political reasons, with the (unstated) goal of reducing the amount of effort put into safety engineering as much as people can get away with. The whole exercise usually reduces to a fantasy with political and cost overtones. What seems most bizarre about the whole

thing is that PHA is usually performed without considering the cost of eliminating or controlling the hazard. Often, this cost is minimal and if the potential losses are severe and the cost of eliminating the hazard cheap or nothing, why not eliminate the hazard anyway regardless of the estimated likelihood? These likelihoods have proven to be so wrong in the past (judging by the number of accidents occurring that were given no chance to occur by the PHA) that it seems foolhardy to make decisions simply on likelihood (and severity) and not mitigatibility and cost of elimination.

Accidents and recalls (like the Boeing 787) are very expensive. Management needs to consider not just the cost of fixing the problems in the design stage, but the cost of *not* fixing the problem in the design stage. This cost goes beyond just the severity of the accident as used in traditional PHAs.

Computer scientists are comfortable with designing systems without the use of probabilities as they have never had them and, because software is pure design abstracted from any physical realization, such probabilities are unattainable. But engineers of physical systems have, in the past, been able to get most design errors out through analysis and testing before the system is put into widespread use. They are left only with random component failure, which can be predicted probabilistically.

Unfortunately, the world of engineering is changing. New systems contain lots of software and are so complex that they cannot be exhaustively tested. Design errors have become a significant problem in operation, and accidents are increasingly caused by unintended interactions among components and not just by component failures. This fact leaves us with two related choices if engineers want to make decisions on the basis of probabilistic risk analysis:

1. Reduce the complexity of the systems we build, use only proven technology, and do not use computers. In other words, build only systems where acceptably accurate probabilities can be obtained.
2. Only build systems where the uncertainty associated with the probabilities is small and there are few or no unknowns. For example, oil exploration and production on land and in shallow water has been done so long that there are well-bounded probabilities. In contrast, deepwater exploration has large uncertainties and many unknowns and the experience in shallow-water does not apply without having very large uncertainties in the calculations.

The alternative to these two choices is for engineers to accept that qualitative analysis will be necessary for new systems and to get used to making decisions based on it.

One additional thought: all PRA starts with a qualitative analysis so using and improving qualitative analysis is important anyway. A goal we might set for ourselves is to figure out how to make decisions based on that qualitative analysis without having to take the extra step of translating the qualitative analysis into a probabilistic one. The extra quantification step introduces so many uncertainties and inaccuracies that it undermines any safety-related decision process based on it.