TBD

by Charles Hoes

I have noticed that industries "new" to the concepts of system safety seem to have trouble understanding the implications and meaning of the risk assessments that are performed as part of a system safety analysis. For us old hands in the profession, these concepts are second nature and, therefore, we tend not to discuss them. I think that maybe it is worth revisiting these basic concepts from time to time. Who knows, maybe we (I) have been off base for all these years, and we might all learn something new from a discussion.

The basic definition of risk — a combination of the severity of a mishap and the probability that the mishap will occur — seems clear, especially when combined with the definition of a "mishap" as "an event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment" (as defined in MIL-STD-882E).

Apparently, risk also has something to do with unintended negative impacts, the severity of those impacts and the likelihood that these negative impacts will occur. This is pretty close to an everyday use of the term. It is not quite as obvious as it looks, however, when attempting to assign a risk to an identified bad outcome.

The first problem that I always run into has to do with which bad outcome I am going to use to represent a particular event or series of events. One example might be a stepladder falling over when a person is using it. One line of the analysis has to do with finding the ways (events) that might cause the ladder to fall over. This usually opens up a long list of possible proximate "causes," such as a broken part, a slippery surface, the ground giving way, users losing their balance and a whole bunch of other interesting ways that ladders can fail to maintain an upright position. For the sake of argument, maybe a specific series of events has been envisioned. Maybe this series of events involves the specific failure of a particular mechanical part. This is certainly useful, but we are attempting to figure out the outcome. Falling from a ladder, even a short one, can have a wide range of outcomes, ranging from nothing at all to broken bones or possibly death. Because I did a stint as a construction contractor/carpenter/laborer, I have personally fallen off ladders numerous times. So far, I have never died — in fact, I have never been injured beyond a sprained ankle. Lucky. However, I know of people who have had much worse outcomes, including people who have died from falling off three-foot-tall ladders.

So, we have an event, or series of events, that can result in a wide range of outcomes. Which one do we pick? If we pick the worst case, we will find that almost all mishaps that we can dream up can result in death — often multiple deaths. That doesn't seem useful. However, that statement brings up a whole new set of considerations concerning the question, "useful for what?" I will get to that a little later. Right now, I will assume that there is something useful or important about identifying the severity of an occurrence. I have heard the idea that the severity that should be used is the highest "credible" severity. Oops, I just introduced a highly subjective term into the process — "credibility." I guess that means the most likely expected outcome. That means that not only is risk a function of severity and probability, but "severity" is itself defined in terms of a probability — maybe the same one used for determining risk, but maybe not. As unsatisfactory as it seems, generally, the severity of the outcome is the one that the analyst, team or outside agency wants to include. The choice is highly subjective.

Assuming we have found a way to select the severity of the outcome to our satisfaction, we are then faced with the daunting problem of calculating (or guessing at) the probability part of the risk assessment. To stay with the ladder example, I am going to assume for the moment that "death" is the worst credible outcome — it is the severity that I want to consider. But then what series of events do we use? Maybe a broken ladder rail would cause the ladder to fall over. If so, we can calcu-

“This leads us to a rather uncomfortable state of affairs. Our highly ‘objective’ and ‘scientific’ approach for performing system safety analyses and risk assessments appears to be based on many highly subjective decisions, engineering estimates and outright guesses. Maybe it isn’t so ‘scientific’ after all. If it is not based on solid, objective science, what good could it be?”

late the probability of a broken rail — or can we? What might cause the rail to break? Manufacturing errors, damage during use, incorrect use or something else. Now we are faced with selecting the most likely cause resulting in the mishap. That means we have introduced yet another subjective guess in order to focus on which probability we want to include for the “falling over” part of the problem. But then we have to add an adjustment for the conditional probability of being killed, given that the ladder has fallen over.

This whole thing seems to be getting extremely subjective, especially since it is supposed to be a “scientific” mathematical analysis. For the sake of argument, what if we actually have some sort of objective method for determining the severity and the entire set of events that could lead to the undesired outcome? Now it is starting to sound like a fault tree analysis (FTA) since we are talking about “sets” of events (as in “cut sets” in an FTA) and “undesired events” (the top event in an FTA).

That sounds good. Maybe we can use the logical structure of an FTA to get out of the subjective nature of the analysis. However, an FTA rapidly branches out as it goes closer and closer to the “basic events” at the bottom of the tree. Knowing where to stop in digging deeper and deeper is an art in itself — do we have to worry about the art (and hence subjective nature) of knowing when to stop? Maybe we can stop when we get to the point where we have reason to believe that we know the basic probabilities. Unfortunately, in any reasonably complex system, we almost always find ourselves in a situation where we don’t actually have good probabilities and we end up using values that are general and don’t really reflect the true nature of “our” system. We purchase all kinds of hardware, materials and devices that are more or less understood. If we are lucky, we might know something about the mean values, but usually, we know nothing about things such as the standard deviations of the loads, strengths or fatigue properties.

Since the failures of low-level parts and actions make up the “basic” events that support the entire FTA analysis, the plethora of unknown standard deviations propagates up through the tree to the probability of the top event. Generally, we end up with a scientific and rigorous analysis that sits on pretty shaky supports. That doesn’t mean that FTA isn’t a useful and powerful tool — it is. However, in general we can’t afford to do the science and engineering required to be “accurate” nor can we afford the time and effort to develop the tree down to the actual basic events. We stop our analyses somewhere in the middle of the fault tree logic. Therefore, while there is a tremendous amount of value in this approach, we need to maintain some healthy skepticism concerning the validity of the probability number that we generate using this technique. In the end, these analyses are usually based on many subjective decisions (guesses).

This leads us to a rather uncomfortable state of affairs. Our highly “objective” and “scientific” approach for performing system safety analyses and risk assessments appears to be based on many highly subjective decisions, engineering estimates and outright guesses. Maybe it isn’t so “scientific” after all. If it is not based on solid, objective science, what good could it be?

I contend that there are many extremely important reasons for using this approach to identifying and resolving safety problems. For one thing, it provides a

structured approach to searching for and resolving hidden safety problems. It also provides a structure that we can expand on and go into greater depth when necessary, without getting lost in the details. It creates something akin to a checklist of concerns, without the downside problems associated with following a checklist. We can build our own checklist as we go. The process of performing system safety analyses sets us up to think in ways that help us identify, categorize and solve potential safety problems. Perhaps more important, the process provides an effective means of communicating with others.

I mentioned earlier that I was going to discuss the usefulness of the risk assessment process. The usefulness is that it entices us into thinking about, and communicating, our understanding of the level of danger that we believe is associated with a given item or process. It helps us prioritize our findings and forms a structure to help others understand what we have learned. It helps sort out what we have determined to be "really bad" things from the "not so bad" things.

At the end of the day, risks are almost never driven to zero. For that to happen, hazards must be completely eliminated, and that means that not much happens. Sometimes, we can do things like switch from one source of energy to another, thereby eliminating a particular hazard, but we almost always add a different hazard in the process. What happens is that we find ways to reduce the risks associated with the plethora of hazards that we uncover. We attempt to bring the risks to a low level, one that is going to be "acceptable" to everyone involved. This sounds like reducing the risks to some low level that is sometimes designated "as low as reasonably achievable (ALARA)." ALARA sounds like it describes a reasonable safety goal. However, it is my opinion that it is not an achievable, affordable or appropriate goal. We really don't want to reach a state of ALARA; what we really want to do is get to a situation where everyone agrees that the risk is "worth it."

Deciding whether the residual risk (the risk that remains when we decide to stop driving it lower) is acceptable is a uniquely human activity. It is not, and cannot be, based on an objective risk value because risk values are ultimately subjective, or at least have a large subjective component. The "risk value" is a measure of someone's opinion, and it provides a helpful means of communicating that opinion to others. This subjective nature of risk assessments is the reason why a simple 4x4 or 4x5 matrix of "likelihood" versus "severity" is sufficient. The risk can be stated simply as high, medium, or low. But the risk value on the matrix does not represent a scientific certainty. The risk value represents the best opinion available at the time. Breaking the risk number into finer and finer categories, or adding additional dimensions to the equation, adds very little value. In fact, doing that tends to degrade the communication aspects because it obfuscates the reality of the state of knowledge by making the answer look much more scientific and absolute than it really is. I call it "pretend science" when too many numbers and calculations are used with insufficient knowledge to support the calculations. I see a lot of "pretend science" being used in the system/product safety world these days. Often, when I take the time and effort to dig down to the probabilities of basic events, I find that they are based on shaky data and questionable assumptions.

I think that we have to remember that just because a risk number is "low," it doesn't mean we shouldn't do something to fix it. For example, a painful pinch when using a tool is an extremely low risk; there are almost no negative medical outcomes. That doesn't mean it doesn't warrant our attention as a safety issue. On the other hand, some high-risk systems, equipment or processes are so important and valuable that they are acknowledged as worth it; the risks are judged to be acceptable. The value of risk assessments isn't that they can be used to automatically make the risk acceptability decision. Rather, their value is that they help communicate the risks to the accepters and others who might find the information useful. Often, the level of risk is a useful measure for mapping the process that needs to be followed for determining acceptability, and is useful for determining who (which level of management or governmental agency) needs to be brought into the decision-making process. However, using risk values as a proxy for a person (or group) is almost certainly a formula for accepting too much risk, or for putting too many resources into further risk reduction than is warranted.

This discussion has not even broached the topic of overall system risk, the sum of all of the risks associated with an entire system. At some point, a decision needs to be made about whether the overall system risk is acceptable, even though it is possible that each identified risk has been judged to be acceptable. In addition to this problem, the fact that any given foreseen event is likely to have a wide range of outcomes and injuries leaves us questioning how we can judge the total risk. We don't know how to add together the various possible outcomes. In fact, we are not ever sure about the appropriate mathematical process for combining the multiple risks of mini-scenarios that have different probabilities and different outcomes.