TBD

by Charles Hoes

As a long time, System Safety engineer, working on major programs that implement system safety programs in accordance with Mil-Std-882, I understand that the topic of this post is rather controversial since it questions one of the main tenets of the profession – that a formal risk assessment based upon a pre-established Risk Assessment Matrix is a necessary part of the process.

For those that might not be "in the know", in the world of system safety risk is considered to be the probability and severity of the outcome of an "accident" or undesired event. The idea is that if something goes wrong (perhaps the rung of a ladder breaks while someone is using it) it will result in an injury or damage of some kind. Thus there is a severity (damage or injury) aspect, such as a broken bone, and a probability aspect – the probability of the hypothesized outcome.

The system safety process is most effective if it is begun while the system being investigated is still just a concept, before the concept has been turned into detailed designs or implemented into a product. Thus, at the beginning it involves the investigation of ideas. The "system" (whatever is being considered) is evaluated or studied in an attempt to find as many hazards, and thus potential accidents, are lurking in the design. Each of these potential accidents is evaluated to determine the severity of an injury and the probability of that injury occurring to determine the potential risk.

The risk is assigned a code typically taken from a table such as this:

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

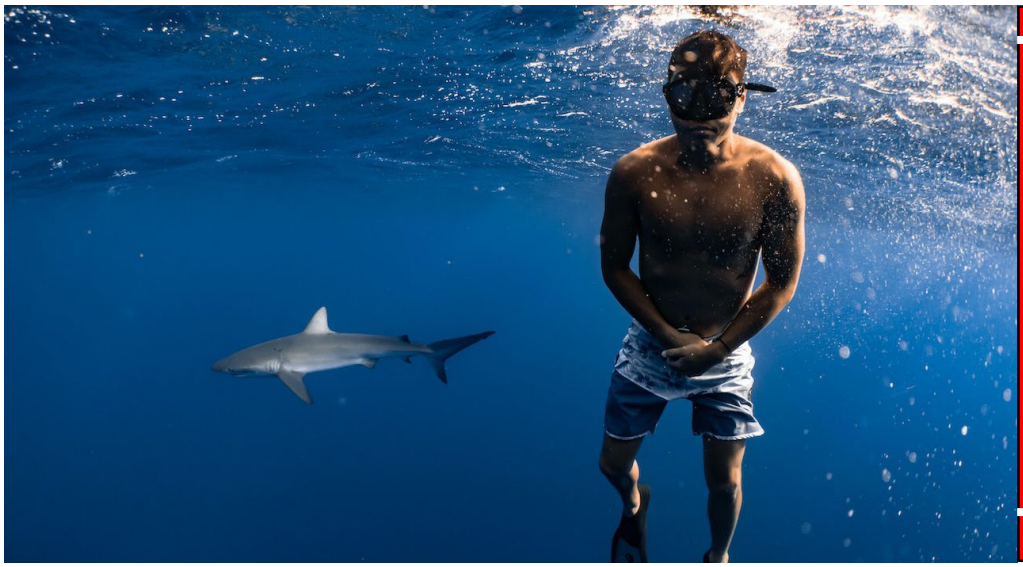
Sample Risk Assessment Matrix

The risk descriptions land somewhere on the table, indicating the "level of risk "of the hypothesized event. A central idea about this process is that level of risk can be the same (or similar) for various combinations of severity and probability. The idea is that a frequent outcome having a negligible injury might be equivalent from the risk management point of view as one that has a catastrophic outcome that is unlikely to ever occur (improbable). The hope is that this approach provides a consistent means for prioritizing efforts to reduce the overall risk. The seemingly obvious result of this is that if resources are scarce (which is always the case), then it is better to put your effort into eliminating "serious" or "high" risks than "low" ones. In fact, it might be a policy that "high" risks are not allowed and must be reduced to a lower level, or the project can't go forward.

This all makes perfectly good sense and gives the appearance of being objective and therefore somehow "scientific." Certainly the idea that risk is related to the combination of severity and probability makes sense. It appears to be a straightforward cost-benefit evaluation. However, there are many problems with actually using a table such as this for making decisions.

The definition of risk being a multiplication of probability and cost comes from financial risk management where all of the severities (costs) are described in terms of economic value (dollars), while probability is taken from a statistical evaluation. Modern economists treat this as a calculus problem of adding (in a calculus fashion) all of the possible outcomes and associated cost to find an "expected" value for the investment. As long as the expected value of the return is greater than the expected value of the costs of the associated risks it is judged to be a "good" investment. Many millions of dollars are invested in the process of estimating the expected values costs and returns in an attempt to find the "optimal" investment choices. The concept behind this process is pretty apparent and "scientific". If you want to understand which option has the least risks, all you need to do is figure out the projected dollars lost and the probability of each. Simple, except that even with economic decisions it is not so easy to predict either of these values or understand the statistics behind them.

However, safety risk assessments are much more difficult when there are illnesses and injuries being considered. Assuming that the probability of postulated outcomes can be determined (no small feat in itself), attempting to put a rational value on the severity of the postulated outcomes is fraught with difficulties and uncertainty. For example, I am not sure how many broken fingers equals a broken foot, or how many broken feet are the same as death. I can't multiply the severity of a broken foot by the probability of that broken foot and get a meaningful answer – in order to perform this operation, the severity needs to be a numerical value, usually dollars. Insurance companies place a value on body parts, but I don't find this particularly satisfying. I am not comfortable about performing cost/benefit analyses based upon my opinion of the value of someone else's foot. I am not convinced that I can properly determine how much each of these types of outcomes is "worth". When I ask the question of how much *my* life is worth there is nothing with a higher value. There is no inherent cor-



"Assuming that the probability of postulated outcomes can be determined (no small feat in itself), attempting to put a rational value on the severity of the postulated outcomes is fraught with difficulties and uncertainty."

Photo: Pexels

respondence between an injury or illness and its dollar value. There are pronouncements, regulations and actuarial tables, but these are just made up by people, there is no inherent measuring stick.

In addition to the problem that you can't actually multiply probabilities by an outcome (even if you find a way to quantify the outcome) the outcomes being investigated almost always have a range of outcomes. Using the previous example of the broken ladder rung, this might lead to a range of injuries ranging from none to death. This would result in a separate risk assessment for each hypothesized outcome – the total risk associated with falling off the ladder is the sum of these risks, but we don't know how to add risk categories because we don't know how to properly quantify severity. A common approach to solving this problem is to use a value that is considered to be the highest "probable" or "credible" risk. I really don't know what the most credible means beyond the probability of the event, it sounds like circular logic to me.

It seems to me that rather than going down the path of trying to find more rational, scientific, or supportable values for the risk assessments, perhaps we should examine the purpose of the exercise to see if we can find a better solution.

A common assumption is that risk assessments are performed in order to prioritize actions to reduce the risks of the overall project. The concept is that resources are always limited, therefore it is important to take care of the high risk concerns first. This "seems" logical, but is it? It implies that we can ignore low risk hazards until all of the higher ones have been resolved. However, in an actual design/development project that doesn't, and shouldn't, happen. Complex design/development programs don't follow a linear process. Instead, many parts and pieces are developed in parallel by many individuals. Features of controls are identified and integrated as the program develops – controls for all levels of risks are not "prioritized" – they are either found and integrated into the design, or not. Therefore, the risk table is NOT an effective prioritization tool. Potential risks need to be identified and controlled to a level that is deemed to be "acceptable" – regardless of the level of risk involved. They are not "prioritized."

If risks are not prioritized using the risk matrix, perhaps the matrix can somehow be used to determine when the risk has been reduced enough to be considered "acceptable." Maybe it can help with determining how much risk is "acceptable." A lot of engineers, managers and regulators like the idea of defining levels of risk that are "acceptable" and therefore don't require further efforts to reduce them. This might be an appropriate solution if we have confidence in the determination of the risk parameters (probability and severity of an unwanted outcome). However, as discussed earlier that is fraught with difficulties and quickly becomes unaffordable. This is seldom a viable solution because of the unknowable aspects of the process.

Even if it were somehow feasible to accurately determine the risk in terms of probability and severity, there is still an open question about how to determine "acceptable" risk levels. Safety risks pose dangers to many different stakeholders in a decision. The company developing the project has financial (and moral) risks, the program manager another set of concerns, the development team another, the user another, society in general yet another. Those that might be directly injured may have different acceptance criteria than those that intend to make a profit from the program/product. Not only that, but there are many different things that come into play when making the determination of "acceptability" including things such as utility, perceived value, dread of the type of injury, social norms, and many others. There is no single, universally agreed upon method to determine "acceptable." It always involves opinion, ethics, morality, cost, and perceptions – in other words, personal judgment.

Instead of using the risk matrix as s measure of acceptability, perhaps it might be useful as a communication tool assisting the safety engineer to express an opinion about the resulting risks. The risk code and/or position on the risk matrix table can't be used to determine "acceptability", it can't be used to determine a "priority" for action – it really can't be used for much, except that it might help inform the decision makers about the "importance" of an identified hazard. That in combination with a lot of other information can help make the ultimate decision about whether or not to spend time and money to fix a potential problem.

I wonder if there is sufficient value in doing "false" risk quantification to offset the many abuses to the process that have occurred in the past. The reason that I call them "false" isn't that I think anyone is attempting to hide or obscure anything. My conten-

tion is that they are seldom more than an expression of "engineering judgment". It might be better to express that judgment in a format that clearly identifies it as a judgment, rather than in a form that has the appearance of a "quantified truth."

Most managers and regulators are looking for a quick, simple and responsibility-free (and hence liability-free) means of deciding the question of acceptability. Abuses abound, showing up as a regular feature of in-depth accident investigations showing that the "acceptable" decision was determined by whether or not the anticipated risk code fell within an essentially arbitrary criteria. While the criteria may have been met, the risks were not acceptable as evidenced by the outcome. There are far too many examples of these categories being converted to elements of a cost/benefit analysis showing that solving the problem is more expensive than the cumulative costs to the unknown future injured parties. Unfortunately this use of the risk codes can lead to rationale along the lines of, "I can't afford to reduce the risk because it would cost me more than your cost of your injuries." This is a rather odd risk acceptance criteria, but common.

I wonder if it might not be better to drop the risk matrix entirely and instead use an interactive process where "experts" (stakeholders) with a range of points of view come together to achieve a unified decision concerning the acceptability of the risks. All of the stakeholders need to agree that the risks are acceptable, not just a subset – and definitely not because they met an existing criteria. This idea is close to the "old" approach of "concurrent engineering" in that all of the stakeholders are included in the decision making process at the same time, rather than each group working separately and then "throwing" a finished project "over the wall" to be accepted or rejected by the using community. The idea of "consilience" comes close to what I have in mind. One definition of consilience is, "the perception of a seamless web of cause and effect." This is opposed to the often used idea of a single cause and effect genesis leading to accidents. A single cause is seldom "the" cause of an accident, it is much closer to a seamless web of cause and effect.

Perhaps the risk matrix might be used as a communication tool, but the real risk acceptance process brings into consideration many, many important considerations that were not included in that part of the safety assessment. To minimize confusion and misuse, perhaps it would be best to drop the use of the matrix entirely, using well thought out rationale statement and studies instead of attempting to over-simplify the process.

Land a job or Find Your Next Team Member!

Whether you are an employer or job seeker, the ISSS Jobs board can help in your search. There is no cost for job seekers to use this service, and you can subscribe to get emails with new job postings! ISSS member employers pay as little as $99 per job posting, and the plans start at $199 for non-members. While most postings on our site are for system safety engineer positions, other career titles related to system safety are also welcome. Get started today!

http://tisss.webscribble.com