TBD

by Charles Hoes

I have been noticing a definite uptick in the number of industry groups that are talking about the benefits of system safety. Many of them don't know that they are "inventing" an approach that has been successfully used for almost 100 years on millions of projects with a combined value of tens of trillions of dollars. It seems that many of these groups believe they came up with the "new" idea that designing safety into projects is better, less expensive and results in fewer false starts than traditional safety approaches — not to mention that it is also more effective in reducing accident losses.

System safety is an engineering process that starts as early as practical and continues throughout the project's life until there is no longer value in continuing. Conceptually, system safety consists of three simple steps:

1. Identify potential hazards.
2. Control the risks associated with those identified hazards to acceptable levels.
3. Repeat.

Over the past 90 or so years, the system safety profession has developed many tools and techniques to assist with that process. It isn't something that needs to be "invented" — it is something that can be learned.

I am happy that people believe they invented an important new approach because that might finally result in them "buying in" to the concepts and the processes that have been shown to be highly effective in reducing accident rates and associated costs.

There are a few places where a conversation with system safety engineers could help industries new to the ideas from going down some unproductive, and disappointing, paths. System safety engineering has been in the business long enough that it has a lot of history and experience experimenting with ideas that just don't work out.

One of the really big ideas that keeps coming up is that "risk assessments" can be used to determine what is "safe enough" under the misunderstanding that "risk" (safety risk) is quantifiable. It seems like it should be quantifiable since it is expressed in terms of "probability" (a number) and "severity" (severity is not a number unless it is translated into a numerical value such as dollars). "Severity" clearly does not mean dollars lost; it means something else, more closely aligned with pain and suffering than economic cost. For example, how much is a lost finger worth? For the person paying for a lost finger, it is commonly valued at around $2,000. I wonder what it is "worth" to the person who lost the finger in terms of immediate pain and suffering, plus the lost capability for the rest of their life. While converting this kind of severity to dollars makes it easy to settle an insurance claim, I don't believe it accurately reflects the meaning of "severity."

The reality is that neither probability nor severity can be accurately determined in the messy and very cloudy "crystal ball" used to predict the future event(s) associated with any design decision. For one thing, there is almost always a range of outcomes, each of which has a different probability of occurrence, even if they appear to be identical. For another thing, assigning a dollar value to an outcome is arbitrary at best, capricious at worse. Knowing how to properly add up the potential outcome multiplied by the probability combinations is fraught with difficulties that take more effort and research than is normally available. Assuming that it is possible to make this determination, the costs of accurately predicting the "risk" associated with any decision or design feature is so high that it is only attempted in cases of extreme risk, and then only to the point that everyone agrees that it is "good enough" to be used to guide a decision.

The idea that risk is somehow quantifiable, and can therefore be used as the sole (or major) element in making safety decisions, has resulted in many questionable decisions. It certainly "feels" good to use a number as a surrogate for making a decision. After all, this approach eliminates the cloud of being responsible for making a "bad" decision. The risk acceptance criteria were made long before the actual situation was known, therefore they are somehow judged to be "dispassionate" and therefore "correct." However, once an undesired outcome occurs, the problem of whether or not the correct criteria were used comes home to roost.

Some common examples come to mind. One thing that has always amazed me is the prevalence of railroad grade crossings in the United States. These are those places where vehicles drive across railroad tracks with the

only "protection" being either a sign, a sign plus a pair of flashing lights, or perhaps those signals plus the addition of a couple of thin wooden arms that block the traffic lane — but with sufficient space to easily drive around the arms to get across the railroad track even though the lights are flashing and the arms are down. That situation results in about 2000 collisions per year resulting in about 200 deaths in the United States. There are also a number of spectacular collisions each year where a car started to cross with an "all clear" signal, but failed to complete the crossing before a train crashed into them. This, of course, could be prevented by eliminating all such crossings, thus eliminating the event of a highway vehicle being on a railroad track. It would be expensive, but Europe has managed to do that – they don't allow railroad crossings. It is all about the "value" of the risks involved.

Railroads aren't liable for the cost of accidents like these unless a signal has malfunctioned — therefore, they put all of their efforts and money into making sure the signals don't fail. As long as the driver has been "warned," the responsibilities of actions to avoid the hazard are judged to rest with the driver. In addition, my guess is that the "irresponsible" driver is also liable for costs that their "error" caused to the railroad.

Is the cost of solving the problem worth the costs of the lives and injuries? In the United States, the decision has been that the cost of the negative outcomes is "acceptable." I am not sure who it is acceptable to, but clearly those that are in a position to make that decision have done so.

The same answer was not reached in many other countries around the world. Those countries have decided that the risks are not acceptable and it is the responsibility of the rail owners and the municipalities to pay for the protection as part of the costs of running their business, instead of injured parties paying in terms of their deaths and injuries (and destroyed vehicles). The decision is about "risk" but it is not just about a number; it is more about a philosophy or point of view.

We have made a decision that it is not "feasible" to eliminate the risks of death at railroad crossings (the first priority in the hierarchy of system safety control); it is only feasible to implement the lesser levels of the hierarchy, placing the onus on the driving public to be "careful."

Another example that I find interesting has to do with the risk of falling when working on roofs. In the United States, about 150 deaths per year are caused by construction workers falling from roofs. OSHA considers this to be within the top 10 "avoidable" causes of death in the construction industry. I don't have the statistics, but my guess is that perhaps 10 times as many of the falls result in serious injury, but not death.

On a population basis we know that there are about 150 deaths from roof falls per year. We also know that each death costs the insurance companies about $150,000. So the cost of "risks" to the industry might be expressed as $22,500,000 per year. The AGC (Associated General Contractors of America) has 27,000 members, representing a portion of the licensed contractors. My guess is that there are perhaps 50,000 contractors that do at least some of their activities on roofs where workers are potentially exposed to fall hazards. That means that the average contractor's exposure to roof fall hazards is perhaps $450 per year ("shared" among them as part of the cost of insurance). If labor costs $50/hour, that is about 9 hours per year per contractor. If they spend more than $450 (including lost productivity) enforcing fall protection provisions, it is costing them more than it is saving. The correct action to control their financial risk is to do nothing.

The risks in terms of cost and severity are biased in favor of not providing protection. OSHA recognizes this problem; therefore, they institute a system of fines for gross violations of the standards. Thus the "risks" to the contractor are the risks of getting caught not following the regulations, rather than the actual risks associated with falling. This turns the "risk acceptance" criteria once again into a social issue rather than a safety issue. We have taken the position that it is acceptable to kill 200 people a year in railroad crossing accidents, but not acceptable to kill 150 people a year from falling off of roofs. I am not making a judgment here; I am just pointing out that risk acceptance decisions are not as simple as just knowing the risk in terms of probability and severity.

It occurs to me that perhaps it is not feasible (and maybe not even possible) to design out the fall hazard when working on sloped roofs. OSHA has a number of requirements (laws) concerning the use of various types of fall protection devices, mostly depending upon various systems of belts, harnesses, lanyards and ropes. There are many problems with these systems, not the least of which is that it is extremely difficult (and dangerous) to do the necessary work while wearing these protective devices. It is difficult and expensive to provide adequate attachment points (particularly for existing roofs), the ropes get in the way and create a lot of "working around" problems that put people in harm's way, they make it hard and slow to maneuver, and do a poor job of protecting people from falling. All of these problems, plus more, result in extremely low compliance with the regulations. I often stop to watch how this is being implemented and find that either no fall protection provisions are provided — or, the rope lanyards are clipped directly back to the worker's belt so that they are just an extra thing to carry around. They are often not connected to anything.

I have little hope in any system of fall protection devices or equipment being capable of providing anything near "continuous" fall protection on sloped roofs. I think the only real solution is to avoid walking on sloped roofs. There are a number of possible solutions to accomplish

such as solution. One solution might be to provide a mechanical device (crane type equipment) that provides a protected, level surface to work from. This sounds good until you realize that the surface being accessed would have to be lower than the working surface, making it very difficult and inefficient to do work. Maybe some sort of robot could be developed to do the work in place of people. With all of the advances in drones and autonomous machines, maybe something useful, and affordable, will be developed — but this seems unlikely to me.

Perhaps the only "good" solution is to avoid building sloped roofs. Sloped roofs are only used because they are the accepted "style" in the United States. There are many countries, and many places in the American Southwest, where the accepted style is a flat roof, usually with a parapet around the edges. People use these rooftop spaces for many purposes besides keeping rain out of the house. They have gardens and entertain on their roofs. There is much value in terms of adding usable space, while virtually eliminating the risk of falling from the roof. At one time sloped roofs made sense because available roofing materials were inherently "leaky" in the horizontal position; their function depended upon "shingling" the materials to let water run off. That is no longer a necessity — there are many cost effective solutions for constructing flat roofs.

Once again, the risk acceptance criterion is more of a social issue than a technical one. Is it "worth" changing to flat roofs? It would save a few hundred deaths a year, but those that are saved are normally unknown strangers. The decision is an esthetic one associated with the look of a flat roof versus a sloped one; it is not about costs, risks, reduction in deaths or anything else. It is all about what the building looks like.

The point of this is to act as a "warning" to those that are new to the field of system safety (reducing risks to an acceptable level through design) that "risk" assessment and risk "acceptance" are not easily defined processes, and they do NOT remove people from the onus of having to make risk acceptance decisions. The values that are created in the risk assessment process are useful to provide some information about the level of risk involved, but that information is far too sketchy and poorly understood to be usable as the risk acceptance criteria. At best, it is a means to communicate an engineering judgment to the risk acceptors; at worst, it is an unsupported guess. It is just another piece of information that used in conjunction with many other pieces of information, can provide assistance to the "risk acceptors" as to whether or not they can move forward with the design decisions. System safety is a very powerful tool, but it does not answer the difficult question of "is it safe enough?"