TBD

by Charles Hoes and Lee Flint

During the past couple of years, I have been involved with things such as introducing system safety concepts into engineering courses. This, and other activities, has caused me to question what it is that makes the profession of system safety "special" — or at least different — from other approaches to achieving safety. My first reaction is that it is something you recognize when you see it. It usually takes only a quick review of a safety plan or effort to determine if it is a "system safety" effort. This isn't always helpful when talking to those that haven't "seen the light." I wonder if there isn't something fundamentally different between "traditional" safety (whatever that might be) and "system safety."

NOTE: I should clarify a point about my use of the word "guess" in what follows. While my use is meant tongue in cheek, I know the term tends to raise hackles for some people. I don't mean "guess" in a wild, uncontrolled way. I mean that no matter how much we try to study, understand and analyze, at some point we always seem to face unknown and unpredictable elements — meaning there is always residual uncertainty in our understanding and solutions. We have many effective and valuable tools and techniques to minimize uncertainty, but in the end, we still have to make guesses (hopefully, "educated guesses"). We may tend to use something like the Fermi Estimate approach to get to "pretty good" estimates quickly and cheaply. That works for achieving "pretty good guesses" — sufficient for some purposes, but not for others. For those others, we dig deeper and study harder, but in the end, we still have some amount of uncertainty that we just have to live with. (The story goes that Fermi used this approach to estimate the number of piano tuners in Chicago. He estimated 225, but there were actually 290 tuners. I consider that to be a "pretty good" guess, based on broad and intuitive guesses at the number of homes, pianos per home, tuning frequency and time required to tune a piano.)

Perhaps one of the biggest differences between system safety and other safety approaches is the idea of a "risk-based" approach, in which risk is assessed and judged to be acceptable or not. What this really means is that it is an "analysis" or "engineering" approach. Rather than striving for a one-size-fits-all solution, system safety seeks a solution that fits the problem. It is based on analysis, rather than compliance with pre-existing solutions. For example, it is more about "is that ladder safe (enough) to use?" versus "are the rungs on the ladder spaced according to a specific OSHA regulation?" In the first case, risk is determined based on analysis of the situation. In the second case, it is assumed that meeting a specific design requirement will make the ladder safe.

While this seems intuitively simple and straightforward, there are many questions that immediately crop up when attempting to judge whether something has a low enough risk to be considered "safe enough" (acceptable).

One of the first major problems that appears is determining the level of risk. For example, MIL-STD-882 provides the following interconnected set of definitions:

- **Risk:** "An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability."
- **Hazard Probability:** "The aggregate probability of occurrence of the individual events that create a specific hazard."
- **Hazard Severity:** "An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard."
- **Hazard:** "A condition that is prerequisite to a mishap."
- **Mishap:** "An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Accident."
- **Risk assessment:** "A comprehensive evaluation of the risk and its associated impact."

“Even in the ‘simple’ case of the risk of falling off a ladder, we find a plethora of possible outcomes. A person can fall off a ladder and die by hitting their head on the ground, be permanently disabled by injuries received from the fall, be temporarily incapacitated by a sprain, or have no injury at all. Not only that, but apparently, we are expected to somehow add up (aggregate) the totality of these unknown and unpredictable outcomes. Obviously, we can do no such thing.”

These all sound reasonable and consistent, until you actually attempt to use them in practice. There are some sneaky terms used in these definitions. For example, if we are considering the design of a ladder to be sold in hardware stores to the general public, how would we address *any* of the issues? We have no idea about the specifics of any hazard. We don’t know how the ladder will be used, what sort of foundation will support it, what the person might be doing on the ladder, the size of the person, the environment or much of anything else. We certainly have little to no information concerning future unknown events or series of events. We can guess, but we don’t actually know much. When attempting to aggregate the probability of events leading to death, injury or damage by using the ladder, we are at a complete loss. When attempting to aggregate the severities of the various possible outcomes, we know even less. While this is obvious in the case of consumer products, it turns out to be the case for almost every project we work on. The actual conditions of use are difficult to predict, leaving us in a state of great uncertainty with regard to each of the elements making up the assessment of “risk.”

Even in the “simple” case of the risk of falling off a ladder, we find a plethora of possible outcomes. A person can fall off a ladder and die by hitting their head on the ground, be permanently disabled by injuries received from the fall, be temporarily incapacitated by a sprain, or have no injury at all. Not only that, but apparently, we are expected to somehow add up (aggregate) the totality of these unknown and unpredictable outcomes. Obviously, we can do no such thing.

Instead, we start decomposing events to identify smaller issues, such as falling off the ladder because an unexpected deviation in rung spacing causes a misstep or because a rung breaks due to … well, lots of possible reasons. While it makes sense to develop a design based on the concepts contained in the various definitions shared earlier, it is practically impossible to do so. Many assumptions and shortcuts are required.

Even if we could figure out *how* to figure out the hazards and risks, still we are faced with the problem of what to do with that information. The simple goal of achieving an *acceptable* level of risk opens up yet another set of imponderables. For example, who determines what is *acceptable*? Acceptable to whom? We could attempt to pre-determine some risk levels that define *acceptable* but may find that to be a fool’s task. We will find that there are many different people with opinions about what is acceptable, depending on things like whether they are the ones exposed to the risk. Injuries that are acceptable in one situation may be totally unacceptable in another, even if we could prove that the probabilities and severities are identical (which can never be done in actual practice). It isn’t so easy to determine the boundary lines between acceptable and unacceptable.

Rather than belabor the problems in attempting to follow guidelines such as MIL-STD-882, perhaps it is best to concede that it is impossible (or at least impractical) to comprehensively and unambiguously achieve the goals in various system-safety related standards and guidelines. Perhaps the best we can do is admit that we are making decisions in a state of uncertainty.

I have been wondering if the thing that sets system safety apart from other approaches is our understanding that we are usually — or perhaps always — working in great uncertainty. Uncertainty exists in all

aspects of our work, including the parts that appear to be "scientific" and based on mathematical principles. Of necessity, we create estimates, bounding conditions and worst-case scenarios to guide our work and the decisions that are implicit in our analyses. In the end, we are really just guessing — with the hope that our guesses come close to the facts. Maybe the answers to these questions aren't as important as the process used to evaluate and enhance safety.

A while back, I heard an interesting story that illustrates a related problem with our profession. The story was about a new rocket system that blew up moments after launch. Given the timing of the event, there was a lot of evidence strewn on a nearby beach upon which to base an investigation. The conclusion of that investigation was that one of the nuts on a small diameter pipe connection had worked loose because of a failure to install a locking wire. It was a big failure caused by a small detail. Would we have found it? I think so because this is exactly the kind of thing system safety folks look for, based on a kind of "mental" (or actual) fault tree. Would traditional safety/engineering efforts have found this? Perhaps, because it is a common problem. However, in this particular case, there was no system safety effort and the problem wasn't caught. That specific potential problem had not been identified and controlled, leading to the loss of the rocket (and payload).

> "...(MIL-STD-882) is an interesting document that makes good sense once you are inculcated into the system safety paradigm, but it is confusing and inconsistent to those who have not yet taken the leap into the world of system safety."

Personally, I have found it difficult to even do something as simple as prioritizing my efforts. My approach might best be described as a fault tree where I mentally start with various top-level undesired events (based on what is possible, given the characteristics of the system), and then follow the tree down toward the "causes" — until such time as I can go no further or don't need to get into more detail because the lower levels of the logic tree are effectively blocked. In some cases, whole branches of the tree are "blocked" by complying with existing standards (such as OSHA regulations), but in other cases, the problem gets pretty deep into the details of the design. The issue is not so much prioritizing the concerns being evaluated as it is determining which ones are adequately controlled to acceptable levels. *All* hazards (and risk) are included in the scope of the effort. Some might be more difficult to assess and control than others, and some might end up existing in the final product because they are inherent in the intended functioning of the system (implying that the safety of these elements will be largely based on "procedures").

This brings me back to the beginning of this paper — what is it that allows me to recognize a system safety effort? I think it has to do with understanding that each system requires individual effort and analysis; existing conformance-based standards and/or requirements might be useful, but in the end, safety depends upon knowledge and understanding. Ultimately, the determination of what is acceptable needs to be based on human judgment.

A safety program based on system safety will include analysis, understanding and in-depth investigations. Solutions to identified safety problems depend on the specifics of the situations and might be newly created or based on existing knowledge, such as that contained in OSHA regulations and thousands of standards and specifications. If a hazard can be adequately controlled using existing ideas, that is great. However, complying with existing standards and regulations is in no way indicative of hazards being adequately controlled. Codes and standards can be useful tools, but complying with them does not equal being "safe enough."

In many cases, complying with existing codes and standards can actually result in a more dangerous, less safe condition. Because "the law" must be followed, it can become quite difficult to change the design in a way that results in safety while meeting the codes and standards.

I believe that we (system safety managers and engineers) need to be clear about our core beliefs with regard to how excellent — or at least "acceptable" — safety is achieved. We must make sure that our safety plans, as well as project engineering and management activities, achieve the desired ends. I think there is a great need for the members of the International System Safety Society to develop clear descriptions of the core beliefs that make up the system safety paradigm. Unfortunately, our main guiding standard, MIL-STD-882, falls far short of this goal. It is an interesting document that makes good sense once you are inculcated into the system safety paradigm, but it is confusing and inconsistent to those who have not yet taken the leap into the world of system safety. We should attempt to create a standard that is an umbrella above MIL-STD-882 and the many industry- and country-) specific system safety-related standards.