TBD

by Charles Hoes and Lee Flint

Lately, I have been wondering about the apparent decrease in interest in the International System Safety Society (ISSS), judging by the sharp decrease in membership and conference attendance during the past decade or so. Fairly obviously, the government's sequester policy had a lot to do with the decrease, starting around 2008. However, while the overall economy has slowly recovered and government budgets are largely restored, our membership has remained flat or has slowly declined from year to year.

This got me thinking that perhaps we are not promoting the importance of our profession, approach and Society as effectively as we can. It seems like we are promoting ourselves as the "owner" of our traditional approach of performing detailed, highly documented safety investigations and analysis reports. This makes a lot of sense, given the relationship between government and its contractors, especially in the realms of the Department of Defense, the Department of Energy and NASA. All three of these organizations tend to develop detailed specifications for entire systems, and then contract with a company to meet those specifications. They have a stake in obtaining systems that are "safe enough," and are willing to pay for the work that goes into achieving that condition. Because they are the users of these systems, they are the ones who actually experience the impacts of any safety deficiencies, and are willing to help define what it means to be "safe enough" for their needs. This means that they want — and demand — detailed insight into decisions impacting safety, making it imperative that safety efforts are documented in sufficient detail to achieve the desired level of transparency. In addition to the government demanding that it be included in the safety decision-making process, contractors benefit greatly from this approach because of the "government-contractor" defense, whereby contractors are immune from liability when creating systems based on government specifications.

This system safety documentation effectively creates "derived" specifications when the government representatives are informed about issues and proposed solutions, and — importantly — accept those solutions as necessary and sufficient. The system safety process and documentation creates a powerful liability defense for contractors. The system safety program is required by the terms of the contract, and the costs of the program are explicitly paid for by the customer. If done carefully, safety is greatly enhanced when hazards are identified and known residual risks are communicated to, and accepted by, the customer.

This approach to system safety within government acquisition contracts has been honed during the past few decades to meet the needs of both the customer and the contractor. What might appear to be "excessive" creation of analysis reports and other safety documentation is actually useful to the government in understanding the details of the systems they are purchasing. This documentation is also extremely valuable to contractors, providing a means to engage their customers in sufficient detail to meet their customer's needs while also providing the benefit of the contractor defense.

The situation for commercial products and systems is different. Rather than leading to a solid liability defense, extensive documentation has the potential to open up the decision-making process to scrutiny, allowing future juries and judges to make determinations about such things as whether the company's opinion about what is "safe enough" was appropriate. The main defense against liability from residual risks is providing warnings to the user, and violation of this can result in the most common product liability judgment of "failure to warn."

My opinion is this creates a tendency to "over warn," but that is a discussion for another time. After failure to warn, the existence of a "product defect" (which includes defect warnings) is the most common source of liability losses. Negligence is a third source of liability, bringing the additional sting of potential criminal prosecution. Absent detailed documentation, it is extremely difficult to get sufficient detail concerning the engineering and management decision process. It is therefore difficult to prove negligence as the source of errors leading to accidents. However, there is a potential concern that this

could become an effective course of litigation, should the documentation and rationale for decisions be uncovered during discovery.

Creating "too much" visibility into the design and development process has the potential to increase exposure to all forms of product liability. This can lead to a feeling that our "traditional" approach has a tendency to create too much documentation. Besides the concern that system safety generates useless (and potentially dangerous) documentation, there is a common feeling that engineering design teams are already perfectly capable of identifying and controlling hazards associated with their designs. The value of adding significant extra costs with safety engineers may not be obvious.

That said, there is a growing understanding that complex systems may contain many system-related hazards that cannot be adequately identified and controlled by various specialty engineers. There is a recognition within most industries of the need for safety engineers charged with ensuring the safety of the entire system, and a recognition that hazards are usually more than merely the sum of the hazards of the parts. "Prevention through design" concepts have gained much traction in recent years and are generally understood to be a necessary part of any complex design process.

"We are specialists not only in analyzing and evaluating the safety of entire systems, but also in developing many proven systems for performing analyses and assisting management in getting the necessary controls implemented and verified as effective."

This is where we come in.

We are specialists not only in analyzing and evaluating the safety of entire systems, but also in developing many proven systems for performing analyses and assisting management in getting the necessary controls implemented and verified as effective.

Unfortunately, there seems to be a belief that we (system safety engineers) tend to use a sledgehammer in cases where a tack hammer might be more appropriate.

My point is that I think we might not be effectively promoting the value of system safety in the commercial environment. We tend to focus on the idea that we help control costs by reducing liability and by reducing the plethora of costs associated with preventing accidents. While this is true, perhaps it is not really what most concerns our potential clients (I use the term "client" to include employers for companies that use direct hires and those that depend on the use of consultants and specialty contractors for their safety program needs).

Sometimes, I get into conversations with potential commercial clients concerning the importance of reduced liability as an important benefit. Often, their view is that they purchase liability insurance for most problems, and that if the liability extends beyond the levels of insurance, they will just go out of business. They are often not particularly concerned about reducing liability exposure below what their insurance will cover. What they are interested in are things such as increased productivity, reduced development times, greater customer satisfaction and improved product placing in the marketplace. Sure, they also want to do the morally and ethically right thing, and they would like to reduce liability exposure, but perhaps these are not their overriding concern. For example, liability costs are just a part of the cost of doing business that they have already taken into account. However, customer satisfaction and reputation translate into increased future success — which they are definitely interested in.

If my thoughts are correct and many of the advantages of a strong system safety program for military and other government acquisition programs do not directly apply to the typical commercial development program, then perhaps it is time for us to revise and upgrade our message. I am wondering what might be most important to our commercial customers and employers. The suggestions I am offering here are just that — suggestions and hopefully food for thought. I do not claim that they are complete, accurate or even correct. However, I am convinced that if we are to take system safety to the next level where it is used and supported by all industry, we need to become much clearer about the message of how our profession can help meet their needs. Perhaps it is time to get out of the box and think about it all from a different point of view.

Note: I am going to use the term "product" to mean whatever project is of concern, whether it is a product, system, process, operation or a combination of all of them. I am using this term as a shorthand notation, understanding that it applies to most anything that has a system safety element to it.

A few obvious needs are:

- Ensure that the product is safe enough to avoid claims of a safety-related product defect. These are generally understood to be situations where the product is more hazardous than generally would be considered "acceptable." It is a moving target, changing over time with public perceptions and opinions. Wikipedia defines a "product defect" as "anything that renders the product not reasonably safe." This can be a design defect, a manufacturing defect, defective instructions and/or a failure to warn.

- Develop a documented process for identifying safety problems and implementing necessary corrective action to inform future projects, but perhaps more important, to create a defense against a claim of negligence. It is one thing to make an error; it is an entirely different situation not to try to prevent an error. The point of this defense is to show that everything that normally would be expected to be done to identify and control hazards was done. This is a powerful defense against claims that can easily become criminal, with implications of "be a manager, go to jail."
- Provide a professional resource to assist team members and management in identifying and understanding safety issues, including codes, standards and good engineering practices, as well as in performing analyses to help uncover potential hazards and safety issues.
- Provide training for engineers and managers to assist them in identifying and solving safety problems and/or recognizing when it is best to obtain the assistance of an experienced system safety engineer.
- Provide them with the ability to create or have access to standards that are aligned with the needs of their industry sector to better define what is meant by good practice and to help "level the playing field" between competing companies.
- Provide a venue for staff to learn about system safety, and to train system safety engineers.
- Help ensure there are sufficient numbers of qualified system safety engineers to meet their needs.

Clearly, there are no new items on this list and there may not be any new items on any list we come up with. I don't believe we need to create anything new in particular; I think we just have to take some time to do a better job of mapping our strengths to the client's needs. We also need to clarify that we can do our work within an existing management structure, without adding unnecessary or unproductive tasks. We can, and do, focus our attention narrowly to what is necessary and adds value.

Currently, we are facing charges that system safety programs simply rehash long-known items and create reams of reports that nobody reads or uses. This should not be the case and does not need to be the case. We need to promote the ideas that we enhance and streamline the process, rather than just add another unnecessary layer of cost.