TBD

by Charles Hoes and Lee Flint

I believe the most important initiative that the International System Safety Society (ISSS) has agreed to undertake is the creation of a new, high-level system safety standard. It seems to me that this new standard should describe the system safety process with enough clarity to provide an "outsider" with a description that lets them understand the philosophy and approach of what we call "system safety."

In an attempt to figure out what this might consist of, I started to write what I assumed would be a rather simple description of my experiences in working a system safety program. If I can describe a few different types of programs, I might be able to identify what is common between them, and perhaps identify elements that are critical to the implementation of a system safety program. I wanted to describe my efforts, as well as the efforts of others who are included in the process. My idea was to write a simple narrative, starting when I first hear about the need for a system safety program and following it through the time when the project is completed and finally dismantled or disposed of. I was thinking of "cradle to grave" descriptions for a few different programs, from the highly complex to the simple.

My first attempt was to write a short description of a "typical" (as if there is such a thing) military acquisition process. As a consultant, the first that I usually find out about the project is when I am asked to assist in responding to a Request for Proposal (RFP) for a piece of hardware or other system that includes a requirement to implement a system safety program. The RFP normally includes a relatively complete description of the desired system safety program, including references to MIL-STD-882x tasks such as TASK 102, System Safety Program Plan; TASK 105, Integrated Product Team/Working Group Support; TASK 106 Hazard Tracking System; TASK 108, Hazardous Materials Management Plan; TASK 201, Preliminary Hazard List; TASK 202, Preliminary Hazard Analysis; TASK 205, System Hazard Analysis; TASK 301, Safety Assessment Report and TASK 401, Safety Verification (along with others that have been deemed necessary by the customer).

An interesting aspect of this list of required tasks is that the selection is up to the discretion of the managing authority (MA; i.e., the customer). That means my first view into the project isn't the beginning of the system safety effort; by the time an RFP is released, the MA has already done a lot of work to determine which of the long list of potentially very expensive tasks apply to the project under consideration. Clearly, there have already been important analyses, studies and trade-off assessments made that will critically shape the structure, comprehensiveness and cost of the system safety effort (as well as the system under development). For my story to be complete, it needs to start much earlier than at the point where I become involved. It needs to start at the point where the RFP is first developed by the customer.

Actually, the system safety effort begins even before the stage of specifying system safety requirements in an RFP. It starts at the concept level, where many safety problems can be introduced, or eliminated, by the selection of the overall conceptual framework used in developing the idea to which the RFP applies. The safety efforts, required analyses and safety verification requirements can vary considerably based on what appear to be rather simple differences in the underlying design approach. It is not unusual for the prime contractor (my customer) or subcontractors to have additional system safety requirements for their internal purposes; these are not just driven by their customer's demands.

My approach to responding to an RFP on a complex government acquisition is to develop a System Safety Program Plan (SSPP), regardless of whether it

is specifically called for in the RFP. The SSPP is the place where the tasks, level of effort, scheduling and interactions with key team members are spelled out. The SSPP must include all key activities, including integrating customer and contractor efforts into the overall system safety effort.

Determining which parts of the system safety effort to "flow down" to subcontractors is an extremely important part of designing an effective system safety program. Not all system safety requirements are appropriate to flow down to subcontractors; in many instances, none should be passed on to a subcontractor because it is understood that the subcontractor does not have the expertise to perform the analyses. In these situations, arrangements must be developed to allow the in-house system safety team adequate access to design details and decisions. In some situations, the safety aspects of a particular subsystem can be better ensured through the imposition of other types of requirements (such as complying with applicable UL standards).

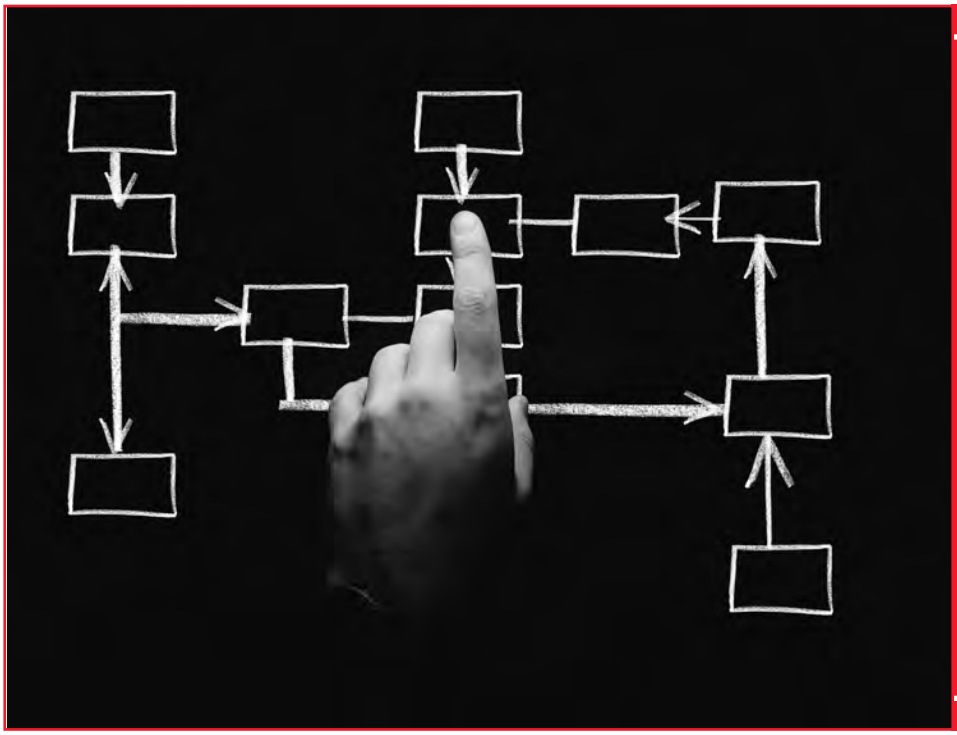
The SSPP is used as the basis for specifying contract obligations concerning things such as staffing, scheduling, required submittals and more. Once all of this is in place — agreed to by many levels of management and then funded — the "rest of the story" unfolds in the details of doing that work. Setting up the effort appropriately is key to ensuring an adequate level of funding, staffing, management involvement and scheduling.

This discussion applies to traditional government system safety programs specified by knowledgeable and informed customers, management, engineers, subcontractors and others. However, this may not be the situation for commercial projects or products. One of the significant differences between a government-funded and managed program and a strictly commercial system safety effort relates to the fact that there may be no knowledgeable, or identifiable, customer (such is the case with consumer products). In these cases, there are typically no RFPs, few if any system safety requirements, and no known users to negotiate with. The result of this is that there are no official system safety requirements at all; it is up to the system developer to decide what should, or should not, be included in a system safety program (or even if there is to be a system safety program at all). In these situations, the details of a system safety program are very much at the discretion of the development team.

One of my major clients hired my firm to join their design team as the "safety eyes" of their projects. This means we were never funded, or requested, to implement a formal system safety program. Rather, we were funded to be there and do what needed to be done on an ad hoc basis. We reviewed plans as they were developed, investigated the applicability of international standards, helped create design approaches and/or philosophies that "harmonized" apparently conflicting standards, participated on change control committees, assisted the technical writers with developing safe operations and procedures, and performed research and analyses resulting in the creation of safety white papers for the team, etc. Sometimes this work entailed using system safety tools such as Preliminary Hazard List (PHL), Preliminary Hazard Analysis (PHA), fault tree analyses, bent pin analyses, human factors assessments and others to fully understand a specific problem or to help identify hazards.

My point is that, while we did the kinds of things that are expected in a system safety program, there was no program. Artifacts such as System Safety Program Plans, formal hazard reports or any of the other obvious signs of a system safety program were either non-existent or done for small, highly specific tasks as needed. The tracking and documentation required to ensure that safety recommendations were implemented became project requirements and, therefore, trackable items that were integrated into the overall project management effort. Memos, emails and white papers/position papers were used in place of formal system safety reports. The entire system safety effort was highly fluid and accomplished by a number of individuals, with assistance from outside companies such as UL or TUV on an as-needed basis.

All of this effort took place in a manufacturing environment that allowed for a constant and continuous evolution of product versions to meet the needs of an aggressive and fast-moving industry. The design team, manufacturing facilities, tech support team and all the managers worked in close and continuous interaction with each other. While this made it easy to know the various experts and fostered an environment where the safety team was integral to activities, it also meant that it was impractical to maintain an orderly and well-planned system safety effort. We depended a great deal on the expertise of the safety and design team to identify safety problems and quickly prioritize elements and solutions.



> “Determining which parts of the system safety effort to ‘flow down’ to subcontractors is an extremely important part of designing an effective system safety program. Not all system safety requirements are appropriate to flow down to subcontractors; in many instances, none should be passed on to a subcontractor because it is understood that the subcontractor does not have the expertise to perform the analyses.”

This “catch-as-catch-can” approach to system safety pushes the limits of what should be called a “system safety program.” The approach we used followed the guidelines of performing hazard/risk-based analyses, creating recommendations to mitigate the identified hazards, testing, and verifying that the recommendations were validated and implemented, etc. As far as I could determine, all the engineering and management activities were implemented as part of the stream of product development. It was just that the artifacts and structured flow of the system safety efforts were not clearly evident.

My question was, and still is, whether this sort of ad hoc safety program is something that should be included in what we consider to be system safety with respect to our proposed new System Safety Standard, our System Safety Institute, or even as support for being considered a certified system safety person. How much do we want to focus on the artifacts versus the approach and activities? Is system safety somehow defined as the sum of the reports, analysis types, hazard-tracking approach, etc. — or is it more a philosophical approach to ensuring safety of systems? In the case of the work that I have just described, an auditor of our work would not have found many (perhaps any) of the artifacts of a typical government-funded system safety program. However, I am completely confident that we were, in fact, doing system safety and we were doing it to a depth and quality that was appropriate for the system(s) under consideration.

There are examples of other system safety jobs that didn’t even include this level of program interaction. It is common for a manufacturer to request assistance with what amounts to an annotated “Preliminary Hazard List” or perhaps, a Preliminary Hazard Analysis. Manufacturers often engage my firm in the early conceptual design stage to assist them in understanding the types of safety problems they are likely to encounter. This helps them make good early decisions, reducing or eliminating safety problems that might otherwise become evident (and very costly) in later stages of the project. Clearly, this is somehow related to system safety, but done internally as part of the normal design and development practices with the assistance of system safety specialists. They hire me because they assume (or hope) that I have specialized knowledge and experience to help them identify hidden or unexpected problems, but they implement the system safety program as an integrated part of their design and development activities. I am unclear as to whether this could be considered a “system safety program” covered by our new standard.

I think we should spend some effort in determining the scope and breadth of our new safety standard. Who is it intended for? What will they do with it? How are we going to use it? We must clearly understand some of the most fundamental questions concerning this standard, and therefore, our profession. I look forward to interesting, and probably rather heated, discussions on these topics.