From the Editor's Desk...

JSS Technical Editor
C. G. Muniak Ph.D.

A Good Question

Ludwig Benner's letter to the editor in this issue of *Journal of System Safety* asks the question of whether there have been "definitive vulnerability assessments of the predictive system safety analysis tools, like HAZOPS, PHA, FEMA and PSSA." It's a good question.

This issue's first technical paper, "Improving the Standard Risk Matrix using STPA" by Professor Nancy G. Leveson, gives at least a partial answer to Ludwig's question.

The second technical paper, "Harnessing Uncertainty in Autonomous Vehicle Safety" by Stephen L. Thomas and Dirk J. Vandenberg, provides a survey of the role of uncertainty in safety assurance, including the critical role of the safety case in identifying and reducing uncertainty.

In the third technical paper, "Model Based Systems Engineering for System Safety: An Introduction," Patrick R. Oliver describes how system safety integrates within a model-based system engineering development activity.

In his "TBD" column, Charlie Hoes discusses some important things happening within the ISSS — with particular emphasis on the Conference.

In their "System Safety in Healthcare" column, Dev Raheja and Dr. Maria C. Escano discuss telemedicine, a field that has grown tremendously over the past few years and has had huge impact on the healthcare environment.

As usual, I welcome your comments and letters to the editor on these or other topics. I also welcome your article submissions.

Regards
Chuck

Letters to the Editor

Vulnerabilities of System Safety Analysis Methods?

While engaged in a study involving the assessment of the use of causal statements in investigations, I recently found an article that contains an excerpt about cause usage that I will reference in that study report. However, the article was actually focused on another issue that I believe is very important for system safety practitioners. The article, "Reverse Engineering the Causal Links Reveals Safety Analysis Issues," appears on page 19 in the April-June 2017 issue of the ISASI Forum. It is written by Sébastien David and David Romat, senior safety investigators for the French Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA). In the article, they discuss a FEMA/PSA/SSA/PSSA safety assessment process in relation to a missed deficiency in a piece of equipment that played a role in the incident they investigated. They concluded:

"The investigation therefore revealed that for a complex system like the primary flight control system, the safety assessment process is vulnerable to errors or inaccuracies. They can arise at various stages of the process, including:

- Imprecise assessment of the effects of the failure types identified in the FMEA, validation of the FMEA, and, in general, the varying results of FMEAs even when using the same methodology (human and equipment manufacturer organizational factors)
- Lack of mechanisms for detecting potential critical errors in equipment manufacturer FMEAs during the aircraft safety assessment and certification process
- The design organization's capability of managing and supervising design when equipment (espe-

cially critical equipment) is designed by partners or subcontractors
- Limitations in the SSA verification process by the aircraft manufacturer and in the approval process by EASA
- Limitations of the safety analysis, like FMEAs, which were developed a few decades ago for traditional hardware system and not for advanced avionics and computer-based fly-by-wire systems"

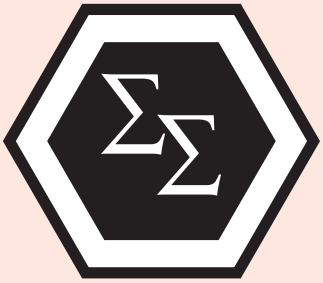
During the time I was an active investigator, system safety analytical thinking was important in my work. For example, in one case, Emerson Harris and I did a fault tree analysis — using the evidence available — that showed how a tugboat probably sank; years later, when the tug was salvaged, that turned out to be what actually happened. In one railroad hazmat accident investigation, the death of an instructor who taught conventional emergency response safety procedures to others prompted investigation of the procedures and analyses leading to their adoption. That eventually led to new thinking and a paradigm shift in hazmat emergency response analyses and practices that eliminated previous responder fatalities when the new practices were applied. In a few other cases in the 1970s, I should have, but did not, pursue indications of safety analysis inadequacies during investigations.

Another kind of experience occurred later during one of my system safety analysis projects. The project involved moving an existing hazardous operating system to a new location. The system had been subjected to previous system safety analyses. For my analysis, I needed to understand how the system worked, so I turned to the system operating manuals for needed data. Using an investigation method rather than a traditional hazard analysis tool to model the system from the operating procedures, it took six drafts before I could get concurrence from the operators that I had accurately defined the system. This raised questions in my mind about the adequacy of the prior analyses: surely, they would have produced a more realistic and definitive operating manual, but again I did not pursue the issue.

On another occasion, I was studying the use of two different methods to investigate an accident where a tank vessel head unexpectedly blew off the end of the tank, fatally injuring three individuals who were attempting to unbolt the head from the tank. For inputs, I used the data from what I considered a very good accident report for the alternative investigations. In this case, investigated by a major government organization, the report noted that the type of accident that occurred was missed by HAZOP system safety analysis. However, the report did not pursue whether the missed scenario was attributable to an analysis process shortcoming, an analysis implementation shortcoming, or something else.

When I did system safety analyses during my career, like other analysts, I encountered various challenges, such as system definition, scenario development, problem discovery and definition, and risk level determination. But I viewed these problems as personal implementation challenges of existing analysis methods, rather than possible vulnerabilities of the methods themselves. I have been retired from the system safety and investigation business for more than 25 years, but I don't recall seeing any Journal of System Safety articles with definitive vulnerability assessments of the predictive system safety analysis tools, such as HAZOPS, PHA, FEMA, PSSA, FTA and others before I saw this definitive BEA investigators' article. I am not aware of any initiatives by the system safety community to demand that investigators provide feedback on safety assessments — when they have been performed. To me, it seems reasonable to expect that if these assessments were performed well, the accident should not have happened. Nor have I seen any tendency by accident investigators to raise any inadequacies of these methods in their reports. If I missed them, perhaps someone could pull together any work that has been done to compile a summary of the analytical vulnerabilities so that system safety analysis practitioners can be aware of them and try to produce better analyses.

— Ludwig Benner Jr.



Have an Opinion?

Sound off on issues regarding your profession, industry, standards and regulations or other system safety topics. Send your 700- to 1,000-word articles to Chuck Muniak, Technical Editor, at journal@system-safety.org.