In his "TBD" article in the May/June 2012 edition of JSS, Charles Hoes raised a few professional questions of introspective nature that indirectly invited a forum for discussion. With this understanding in mind, I am writing this letter to provide an opinion to some of his posed questions.

There is a subtle difference between "competency" and "qualification." Competence means "the ability to do something successfully or efficiently," which implies accumulated knowledge. Qualification means "pass of an examination or an official completion of a course, especially on conferring status as a recognized practitioner of a profession or activity." In the absence of an accredited organization that could administer an examination to qualify a safety professional, we are left with an assessment of "competency."

As an example of such an assessment, the article mentions NASA's view on system safety competencies. I believe that the five categories identified in the NASA chart are correct. They mirror the development lifecycle of a safe product. Here is the reasoning:

- **System Safety Analytical Methods.** Safety must be embedded in the design and safety must be predictable; hence, the need for analytical methods. Since safety is often the result of vertical and horizontal interactions within a system, the safety is designed and analyzed primarily from a system perspective.
- **Mathematical Skills.** These skills are required to be able to describe a system. System engineering and applied math have had a long history of cross-fertilization. A system that has a validated mathematical model is likely to have most of its safety issues resolved at the design phase. It is noted that as systems become more complex, a validated system model is becoming the exception rather than the norm.
- **System Safety in Operational Management.** This refers to contributions made by safety practitioners that test the system in the field. This is a safety "hands on" field of knowledge that encompasses operations.
- **System Safety in Acquisition.** Since this view is coming from NASA, which is known to integrate many smaller subsystems, it is important that when a specification is issued, the safety requirements are specified at the acquisition level.
- **System Safety Rationale.** The rationale must be available during the integration of a complex system to ensure proper system validation.

Thus, I believe that the NASA categorization is the most complete one. When applied to engineering domains other than NASA, these categories should be tailored as applicable. As far as I know, we do not have in safety engineering a situation of "one size fits all."

The work done by the International System Safety Society's "Competency Committee" is valuable. It shows the complexity of the subject and the difficulty of defining a "system safety competencies chart." I notice that if safety management is left to specific industries and associated standards, education and training is left to universities — with the ISSS potentially providing curricula guidance — and certification is left to accredited organizations, then ISSS could be in a better position to define safety engineering as a profession in the realm of safe product development. This appears to be a goal that could lead to practical classifications of competencies.

The paper goes on to describe with professional passion "… one of the most important areas of (safety) competency is having a solid technical and scientific background concerning how things work." Without engaging in the semantics of "solid technical and scientific background," I would like to point out that what glues together the knowledge of "how things work" is system engineering. This aspect is essential, but it is not mentioned at all.

The key background question that this paper addresses is: "What is it that we (safety engineers) do that is different from those things done by other members of a project team?" I would like to offer a personal opinion. I view system safety as the pinnacle of system engineering. System
Engineering knowledge is used to design systems and their control algorithms. System safety takes an already-designed system and analyzes it to ensure that any failure will bring the system to a safe state. Before one can be a system safety engineer, one should be a good system designer. Safety engineering qualifies a system through analysis of a design as safe or not. Safety engineering field practitioners qualify an implemented system as safe to commence operation.

The paper goes on to express dissatisfaction with companies that justify a lack of safety engineers on a team by claiming that the company’s designers are safety conscious. Usually, the missing link is the fact that safety is not applied in a systematic way in such companies. Hence, each designer will apply safety based on his or her personal interpretation of the applicable regulation. This creates conditions for hazardous situations to remain unidentified at the design stage.

As a corollary to the key background question, the paper asks rhetorically another good question: “Do we (safety engineers) not bring anything special or important to the team?” In my view, the answer is a definite “Yes.” However, I believe that the key to respond to the posed questions within the ISSS framework is to discuss “system safety” rather than “safety professionals.” The basic skill required in safety is systems engineering that can be clearly defined. System safety in a given industry is the outcome of the applicable legislation or standards requirements, combined with the safety policy of the industry (or company). In my view, it is not possible to define an all-encompassing “need” for safety. It is industry-specific.

Ady Solomon, Ph.D., P. Eng.
Toronto, Ontario, Canada

Copyright © 2012 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.