Journal of Aviation/Aerospace Education & Research

Volume 8
Number 1 *JAAER Fall 1997*

Article 2

Fall 1997

Beyond the Classroom with System Safety

Donald E. Smith
smithdo@erau.edu

BEYOND THE CLASSROOM WITH SYSTEM SAFETY

Donald E. Smith

At the Daytona Beach, Fla., campus of Embry-Riddle Aeronautical University, a System Safety course is offered at the undergraduate and graduate levels. To enhance the techniques learned in the classroom, students work with local industries, applying classroom knowledge. The safety or efficiency surveys they perform provide a service to the participating firms, strengthen the university/industry partnership, and reinforce classroom concepts for the students.

System safety originated with the nuclear missile program (Stephenson, 1991), in which failure obviously was not an option. The philosophy was soon embraced by the military, NASA, and other industries such as mass travel whose first-time failures could be catastrophic. System safety, in a system-production context, is an upstream effort in which designers and engineers ask, What can break? What can go wrong? What is the probability? What are the consequences? A thorough upstream effort can provide management with detailed and prioritized information about problem areas and about where to apply limited resources. It didn't take general industry long to figure out that the same questions could be asked about product reliability, material selection, production efficiency, customer satisfaction, and freedom from litigation. System safety techniques also are used in the accident-investigation milieu.

On the first day of class, Embry-Riddle system-safety students are asked to provide inputs for a simple task that demonstrates the flexibility of system-safety concepts and their attendant deductive thinking. The students are asked, What did it take to get you to school on time today? The instructor constructs a tree on the blackboard, with the top event defined as *Get To School On Time*. The inputs for the next branch of the tree usually involve *get up on time*, *health okay*, *car okay*, *weather okay*, *traffic okay*, and other related items. The instructor usually concentrates on *getting up on time* and its subsequent layers of the tree.

Inputs for getting up involve an alarm clock. Was it set? Set correctly? Can you hear it? Did it work properly? Concentrating on the latter brings to focus the need to examine every component of that clock and how it was manufactured. Additionally, the competency, training, and mental attitudes of the workmen could be considered at a human-factors level. Even the processing of the metal for the spring in a windup alarm would be part of a thorough system-safety effort.

The lesson is vivid. System safety forces deductive thinking, and, addressed correctly, is extremely thorough. It is flexible. The same thought process could be applied to building a Titan missile, a skyscraper, or a baby doll. As the students reflect on how much detail could go into something so simple as the functioning of an alarm clock, the instructor reminds them they haven't addressed the car yet. Also not addressed was the probability of each event's occurrence and the consequences of failures.

Fault Tree construction and analysis, such as the drill just discussed, is only one of the techniques learned in the classroom. Other system-safety techniques are Failure Modes and Effects Analysis, Energy Trace and Barrier Analysis, Project Evaluation Tree (Stephenson, 1991), Management Oversight and Risk Tree, Change Analysis and Event and Causal Factors charts. The students are equipped with the knowledge to conduct safety and/or efficiency surveys on products, production lines, or procedures. Human-factors considerations in system safety also are examined. The students become familiar with the ABCs of setting up a companywide system-safety program. They are ready to apply their knowledge working with a local industry. Approximately one month of the term is devoted to the project.

The generous cooperation of several local industries allows the students to put into practice the concepts they have learned. A major automotive industry cam-producing company has benefited from several student-team visits. The teams usually consist of four to six students. This firm has had the students apply system-safety techniques to a milling operation to find potential sources of errors. Teams also have performed Energy Trace and Barrier Analyses on several workstations to improve production-line safety. These analyses involve determining the types and sources of energy involved in an operation, identifying the barriers protecting the "targets," and improving or recommending additional barriers.

Similar workstation studies were performed at a major pleasure-boat factory. The company had been experiencing many workers' compensation claims, and surveys suggested several steps to reduce these claims. Another project involved improving the efficiency of separating fiberglass hulls from their forms. Another team performed several analyses on a fiberglass process to reduce bubbling in the fiberglass compound.

A metals manufacturing firm with which student teams had previously worked unfortunately experienced a catastrophic fire in the plant. A team sat down with design engineers and helped incorporate a system-safety philosophy into the new facility and workstations. Perhaps this one won't burn.

A Project Evaluation Tree (Stephenson, 1991) study was conducted on an airborne cargo-delivery company. This analysis studied the organization's personnel, procedures, and equipment. Several good recommendations surfaced that improved the efficiency of the operation.

The students also worked with a metal-filter manufacturing firm. The president of this company had recently instituted a Failure Modes and Effects program after design-related recalls of a certain filter type. This analysis calls for design engineers to question how something could fail, then determine failure probability and also the fiscal consequences of failures. Ironically, the president did not want the probabilities and consequences as part of the analysis. When asked why, he responded that he did not want *anything* indicating they knew something might fail. He was, not surprisingly, afraid of litigation and the information that opposing attorneys might obtain in a legal action. This situation is unfortunate in that with a comprehensive system-safety program and *exactly* that type of information, one not only receives valuable management information about precisely how to improve the product but one can also significantly reduce exposure to litigation with the resultant better product.

Student teams also have conducted safety surveys of Embry-Riddle's flight line and flight operations. They have performed an analysis of the new aircraft maintenance facility. Taking advantage of the flexibility of system-safety concepts, teams have examined what it takes to successfully organize an intercollegiate basketball game at the fieldhouse and what steps are necessary for a successful freshman year.

These in-the-field experiences have greatly augmented the knowledge gained in the classroom and have provided valuable additions to the students' resumes. Although the prospect of performing these evaluations in a major manufacturing environment is usually daunting at first, student feedback is extremely positive. This cooperative effort is a win-win scenario for the students, the industries, and the university.□

Donald E. Smith is a graduate of the National War College. He has an M.S. in Aeronautical Engineering from the U.S. Naval Postgraduate School and a B.S. in Naval Engineering from the U.S. Naval Academy. He is an assistant professor in the Aeronautical Science Department at Embry-Riddle Aeronautical University.

REFERENCES

Stephenson, J. (1991). *System Safety 2000: A practical guide for planning, managing, and conducting system safety programs.* New York: Van Nostrand Reinhold.

https://commons.erau.edu/jaaer/vol8/iss1/2
DOI: https://doi.org/10.15394/jaaer.1997.1210