# Lessons Learned from Teaching System Safety

D.E. Strub; Embry-Riddle Aeronautical University; Vandenberg AFB, California, USA

Keywords: education, lessons learned, process improvement

## Abstract

Some universities and colleges teach system safety as part of a defined curriculum culminating in a specific degree, most often a Bachelor of Science (BS) or a Master of Science (MS) degree. While the specific subject matter can differ between institutions, the basic elements of hazard identification, the subsequent risk assessment, and risk mitigation comprise the basic building blocks of any system safety course of instruction. While these elements are the same, teaching a system safety class requires an instructor to convey a unique point of view to students. To educate, the instructor must employ specific techniques to ensure students leave the course with a basic understanding of how to best employ system safety. This paper discusses how to engage students in the basic elements of system safety and outlines methods that have the best overall chance of success in conveying the merits of system safety to the students. The paper will also address how measures of student satisfaction can be used as the basis for improvement in future system safety course content.

## Introduction

As a general proposition, teaching is rewarding but also extremely difficult. Of course, there are a number of variables associated with that proposition. At the college level, the student is the primary (and most important) variable. With the student, teaching would be a futile exercise at best. The attitude and background of the student are certainly key, but the open mindedness of the student is the most important characteristic. The support of the college is also an important component – characterized, at a minimum, by a directed program with specific educational goals, the resources to support these goals, and certifications by independent agencies to ensure standards are met and maintained to a high level. As a final addition, the instructor is an important element. The instructor provides the means by which the material is presented, discussed, and applied throughout the teaching process. All of us know a good instructor can make an important difference between a poor learning experience and an inspirational learning experience. While the role of the instructor has always been important, technology has multiplied the capability of the instructor. In addition to the traditional classroom environment, newer modalities have been added within the past few years that have challenged a lot of instructors. Online instruction is one modality, often necessitating a non real-time interaction between student and instructor. Also, video based teleconferencing has also become an increasingly available option for colleges to convey courses to students. All of these factors have presented instructors both with opportunities and challenges to teaching system safety.

## System Safety – The Basics

A number of excellent texts exist on the subject of system safety. However, this paper is not intended as a comparison on the different approaches to system safety. In order to simplify this paper, only one text will be used as the basis for what needs to be discussed for system safety. The text, "System Safety for the 21st Century" by Richard A. Stephens (ref. 1) provides a good overview of system safety and related topics.

The basis of the system safety process is the generation of specific products that support the identification of details to not only the practitioner of the process, but also the presenting of this information to key decision makers. The first of these products, according to Stephens, is the System Safety Program Plan (ref. 1). This product provides details of the system safety effort in terms of specific tasks, risk assessment methodology and risk acceptance criteria, milestones, and the system safety organization (ref 1.). After that point, the system safety process becomes involved with the system design process in terms of an incremental review, design, and assessment process. The final output of the system safety effort relative to the design process is the Operating Hazard Analysis, or OHA. This provides the basis for making an informed decision regarding the design risk inherent in a system.

Any system safety effort also includes the effects of the human in the operation of the system. Handled conceptually at first and dealt with increasing detail as the design of the system becomes firmer, the role of the human in terms of error rates and potential impacts to the system is constantly assessed (ref 1.). The role of the human is a key part of

system safety, which will be addressed in a later topic. Stephens also cites a number of analysis tools that assess human reliability (ref 1.).

To be practical, a system safety program must also consider operation of the system after implementation. Stephens cites the use of the Operating and Support Hazard Analysis, which he also refers to as the Operating Hazard Analysis (ref 1.). This analysis includes the operator as a part of the system safety process. In addition, Stephens also discusses use of the Change Analysis Report (ref 1.) within the context of a specific system safety product. Being able to assess a change and provide an assessment of the safety impact of the change provides a greater certainty of the safety of the system.

The core of any system safety process is the use of the system safety precedence. Since this paper is not meant as a system safety tutorial, the specific aspects of what constitutes the system safety precedence are left to the reader. Suffice it to say, the inclusion of the system safety precedence is a key part of any beginning discussion on system safety, and is addressed by Stephens (ref 1.).

System safety is based on risk assessment and risk acceptance. Stephens discusses these in detail (ref 1.) and provides a good overview of the constituent elements of these items. The topic of risk acceptance is very important, and serves as the main underpinning of system safety. The risk assessment provides management with the means by which the safe operation of the system can be judged.

The above provide the minimum of what needs to be addressed by any system safety course. Any system safety course that does not stress the need to assess the elements of design, operations, and humans that comprise a system will not be an effective system safety program. It is at this point the student needs to be aware of the unique aspects of system safety and how they differ from other courses.

## Students – What they bring and don't bring to the system safety class

As stated in the introduction, students bring a number of good qualities to class. Students that bring a desire to learn are especially important to the system safety class. In addition, students are well motivated and have advanced to a degree where discussion of concepts is easily accomplished. However, students might not be familiar with the concepts as presented in a system safety class. The concepts in a system safety class are process based and don't readily share the same tangible aspects of other courses of study. For example, mechanical engineering brings forth several discrete exemplars familiar to students – rotating wheels, forces on truss members, and materials composition are familiar to students, whereas items such as a preliminary hazard analysis, system hazard analysis, or human error prediction rate theory are conceptual aspects of a system. Another item is the interaction between the completed design, the human operator, and increasingly the software that comprise a completed and functional system. Depending on the specific context, these items will affect the safety of the system in different ways. A system employing automated control and robots in a manufacturing setting will have different levels of safe operation than a hydraulic crane operation. In short, the student might not be able to conceptualize the role of the system with regard to the contribution of a specific item when it comes to the safety of the overall system. The final aspect of this discussion is what can best be described as an aspect of critical thinking – the aspect of thinking of the system in terms of a failure situation. Most all courses take into consideration the success of the system being discussed – never the "other side" of the failure of the system or what causes the failure. The issue of not being able to understand the system from a "failure" point of view is the most critical shortcoming in terms of what students don't bring to class.

## What works (and doesn't work) to teach system safety to the student

As with any course, a number of items need to be done in order to ensure success at any level. The first of these is that the course has to be well organized. While this brings to mind a number of items, there are a few specific items that stand out. The course syllabus needs to specify course policies and college requirements in an unambiguous manner. The lessons for the upcoming term needs to be identified and presented in terms of specific course meeting dates and times. In addition, firm expectations need to be identified and presented to the student. This is especially true in terms of course assignments such as papers and class projects. Without these firm expectations, the student is often left to their own devices on how best to fulfill an assignment – thus making choices that don't fit the intent of the assignment at all. The use of a standardized format for course material at the college is essential – that way,

students know what is required in all classes. The last item is the use of references for class. Traditionally libraries have been used for this purpose, but that is changing. Students are increasingly turning to the Internet as a research tool. Citing a reference from the Internet needs to follow the same rigor and standards as a properly cited book reference. All formats in use today (MLA, APA, Chicago, etc.) have specific requirements for properly citing these references.

System safety brings a special need to have techniques that work to teach the student. One of these is the use of a study guide for exams and tests. Employing a study guide allows the instructor to guide the student's learning of system safety and allows greater retention of critical class material. The other aspect is the use of examples familiar to the student. All students are familiar with automobiles – using this technology as a basis for examining the design and operations analyses specific to system safety will yield much greater comprehension of these analytical techniques than items unfamiliar to students. In addition, the use of a properly selected example can also provide a basis for introducing more advanced topics such as software safety analysis and human factors analyses.

## What does all of this mean to the instructor?

As indicated in the introduction, the instructor is key to the educational process. Not only does the instructor provide an example to the student, the instructor also provides the basis by which the student enhances the understanding of system safety as a course topic. The instructor must be organized, well read, and ready to support the student in the understanding of the material. In addition, the instructor must also be flexible enough to present material to students in an interesting presentation style. But most importantly, the instructor must learn to now present materials and communicate on a number of different teaching methods, known as modalities. The classroom is increasingly being supplemented by the Internet and the real-time videoconference. A properly prepared instructor will be ready to teach at all times and in a variety of different methods.

## What's next?

System safety is a unique discipline and also a unique way of looking at the world. The system safety instructor must not only be able to teach system safety, but must also deal with an increasingly expanding set of delivery methods for educating the student. Being ready to take advantage of these opportunities, using the points identified in this paper, will greatly enhance the effectiveness of teaching system safety to the ultimate customer, the student.

## References

1. John Wiley & Sons, Inc. System Safety for the 21st Century. Hoboken, New Jersey, 2004.

## Biography

D.E. Strub, MS, CSP; Embry-Riddle Aeronautical University; Vandenberg AFB, California, USA, telephone – (805) 734-4076, facsimile – (805) 734-4076, e-mail – daniel.strub@erau.edu.

Mr. Strub is the Director of Academics and serves as adjunct faculty at the ERAU campus at Vandenberg AFB, CA. He has taught extensively in system safety, human factors, safety program management, and safety law.