Notes on Society History

by Rex B. Gordon
ISSS Historian

A Historical View of System Safety Orthodoxy

A Webster's definition of "orthodoxy" is "a belief or a way of thinking that is accepted as true or correct." The founding fathers of our Society were convinced that the System Safety Concept (SSC), as articulated by Chuck Miller and other visionaries of that time, was true and correct. Moreover, it provided a critical means for reducing the catastrophic aerospace mishaps so prevalent during our "Cold War" race for nuclear missile supremacy, a key to preventing World War III. At that time, system safety — the "new kid on the block" — was being challenged by the design, reliability, quality and traditional safety interests as being redundant to their activities and an unnecessary drain on available funding.

> "Any suggestions that system safety activities be limited to the design phase only or to any subset of the total system under consideration should be considered opposed to our Society's orthodoxy. Suggested new analytical techniques and other methodologies, on the other hand, should be *welcomed* and, if found valid, *encouraged* by the ISSS."

Our Society was formed not only to provide networking support to those entering the field, but also promote "system safety orthodoxy," and defend the concept against those wishing to modify or replace it. Throughout the history of the Society, we have countered these challenges successfully. Today, system safety is a well-established element of most highly hazardous endeavors worldwide. But we need to be aware of becoming overly complacent with our past success.

In today's rapidly expanding cyber-technology environment, there is an abundance of new publications focused on how better to minimize the risks inherent in our ever more software-driven and complex systems, activities and products. Some of these promote new analytical thinking and techniques and suggest many or most of the old traditional system safety engineering tools may be obsolete. Others proclaim a whole new paradigm for safety thinking. What then should be the position of the International System Safety Society (ISSS) relative to these ostensible attacks on our historic orthodoxy?

Ultimately, this is a matter for our officers to resolve. However, as Society Historian, I feel it appropriate to make a few observations on this matter. First and foremost, I feel we must establish just what system safety orthodoxy is — and what it is not. The earliest discussions by our members on this subject were remarkably consistent. We were opposed to any attempts to limit the scope or involvement of system safety by arbitrary restrictions. We eliminated the limiting term "aerospace" in our name. To be brief, our orthodoxy was essentially confined to the following:

The System Safety Concept holds that a holistic approach to hazard identification and controls is essential. It must address all significant accident risks, for all system activities, components, software and human interactions. It must be implemented from the conceptual through disposal phases. It must be embedded in all management, conceptual, design, engineering, testing and operational activities.

System Safety Methodology refers to the analytical tools and other techniques used to satisfy the system safety objectives of a project or hazardous undertaking.

System Safety Management refers to the organizational planning, funding and responsibilities required to implement a system safety activity.

System Safety is the general term that encompasses these interrelated aspects.

My purpose in this brief review of historical terminology is to point out that our initial orthodoxy did not ascribe to any particular methodology or analytical tool for conducting system safety. It was agreed that this was an area that had no obvious boundaries and was destined to continually evolve. Therefore, I suggest our response to challenges regarding the effectiveness of our traditional approaches to system safety should be aimed at assuring that the basic tenets of the System Safety Concept are not violated.

Any suggestions that system safety activities be limited to the design phase only or to any subset of the total system under consideration should be considered opposed to our Society's orthodoxy. Suggested new analytical techniques and other methodologies, on the other hand, should be *welcomed* and, if found valid, *encouraged* by the ISSS.

The theme for the 35th ISSC, "Pushing the Boundaries of System Safety," seems quite fitting in this context.