Gains from Losses

John Livingston

Getting Started in System Safety

This past year, I spent some time supporting an effort to develop a set of hazard report review guidelines to be used by engineers assigned to hazard report review teams. The subject reports were developed by contractors for a major program and the review was done by a government team. The engineers were selected for their engineering expertise and, in most cases, were getting their first experience in assessing hazard analysis reports. I was reminded of my own start in the field of system safety almost 40 years ago.

While I acknowledge that almost all readers of *Journal of System Safety* (*JSS*) are experienced system safety practitioners, we all had to start somewhere. In my case, it was with little guidance or formal training.

It takes both knowledge and communication of that knowledge to make a meaningful system safety contribution. Together, they support an initiative assessment process that is quite similar to the basic feedback concept of system control theory. Figure 1 depicts the application to a system safety effort.

In 2007, Bryan O'Connor identified 11 characteristics of good system safety engineers [Ref. 1]. For the purpose of this discussion (getting started in system safety), I will group the characteristics into three subsets: Knowledge, Philosophy and Temperament.

Knowledge

- Technically credible
- Experienced in design, testing and evaluating (T&E), and operations
- Knowledgeable in SMA requirements and tools
- Above average communication skills (both verbal and written)

Philosophy

- Systems engineering bent
- Energetic and creative ("yes, if")
- Persistent, yet pragmatic

Temperament

- Firm, but not hard headed
- Humble, but not reserved
- Skeptical, but not cynical
- Thick-skinned, with a sense of humor (necessary for longevity)

Most of my discussion will address the development of knowledge, with a few comments about my philosophy on communication and feedback. I acknowledge the importance of the right temperament for any system safety practitioner, but such discussion really deserves commentary from a more accomplished source.

Becoming Streetwise

While a few new members of the profession may be fresh from a college or university program, most new members will have a measure of technical expertise or experience in a particular technical discipline. The challenge for all "newcomers" is to develop the necessary knowledge to make their efforts effective and to add value. Becoming "streetwise" requires technical knowledge, knowledge of the tools and processes of the system safety profession, and program (or product) knowledge.

Technical Knowledge

It is important that a system safety practitioner develop contacts within the engineering community. Such contacts are important for identifying technical requirements and standards. They also provide technical expertise in the major systems of the program to which the analyst has been assigned (electrical, mechanical, pressure, material properties, etc.). Engineering sources should include those familiar with the product design and operational considerations, including testing and other verification activities. Such contacts are essential for understanding the elements of the basic product

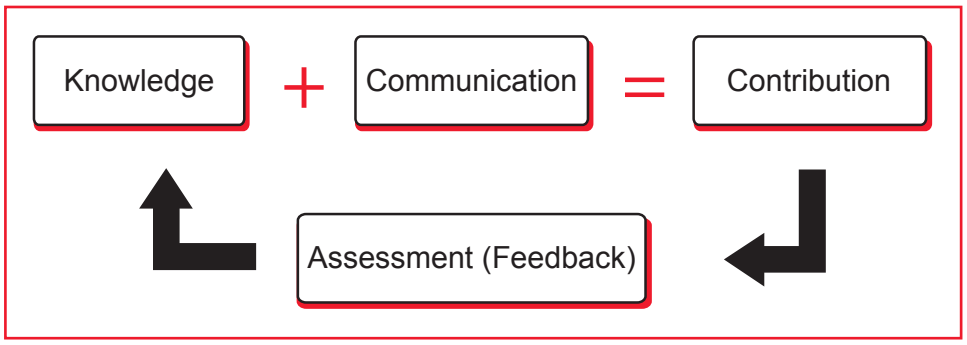

Figure 1 — The Basic Elements of a System Safety Effort.

and gaining knowledge of technical issues or concerns. Where the organizational engineering community may not possess a needed technical capability to address a specific issue or concern, they may be able to identify additional resources to contact. The Internet may also be a useful source of technical information, if used in an intelligent manner.

System Safety Knowledge

Undoubtedly, the most pressing challenge for a newcomer is to quickly gain knowledge of system safety concepts, tools and processes. While there are a variety of formal training options available, most organizations do not immediately send new system safety personnel off to formal training. For most, it is a matter of on-the-job training (OJT), with varying amounts of mentoring and tutoring by other members of the system safety organization. Unfortunately, the most knowledgeable team members are least likely to have time available for such activities.

A little initiative on the part of a new practitioner will speed up the learning process. This includes developing contacts within the local system safety community and related professional societies. I worked in system safety for 10 years before I developed an appreciation for such resources.

Several members of the International System Safety Society have contributed to my professional growth. Earl McNail encouraged me to join the Society in the summer of 1987 and offered advice drawn from his many years of experience. His analysis efforts on the NASA Skylab program provided insight to a broad range of safety-related design criteria with suggestions for their application [Ref. 2]. Pat Clemons provided direct support in the development of training of the members of my Marshall Space Flight Center system safety team. He was also an available resource for many of my system safety questions. Additionally, ideas from his System Safety Scrapbook were helpful in expanding my system safety horizon [Ref. 3]. Another one of my early Society contacts was Clif Ericson, who provided insight on Fault Tree Analysis (FTA) [Ref. 4] and a file of his Fault Tree Analysis tool, which was in an early development stage. There are a number of other authors within the Society (for example, Dev Raheja, Mike Allocco, Terry Hardy, Jeff McIntyre, Brian Moriarty and Nancy Leveson), and all of these authors have knowledge and experience that are invaluable to any system safety analyst. Society publications like the *System Safety Analysis Handbook* should be part of any system safety practitioner's reference collection [Ref. 5]. Not to be overlooked is the value of an active relationship with a local chapter or the Society's virtual chapter.

Program Knowledge

Each program phase has its own system safety aspects. System safety assessments are iterative processes that should start at the concept stage and evolve with the development of the product (hardware and software). Joining a program at the concept phase has many advantages, including a greater opportunity to achieve safety requirements by elimination of identified hazard or design options that greatly reduce their probability of occurrence. Even with this "freedom," the analyst must have technical knowledge and system safety knowledge. Joining a program in process offers the additional responsibility of making a critical assessment of the system safety efforts that preceded your assignment. In my case, I passed on an opportunity to do such a critical assessment, based on others' assurance of the quality of the established assessments and the "operational" nature of the program. It was a decision that I would later regret.

Programs are not created in a safety vacuum; they come with certain developer goals and different types of regulatory requirements. System safety requirements are generally a combination of specific safety requirements and derived requirements based on engineering technical requirements and standards. The evolving system safety assessment will probably add to the "specific" safety requirements needed to assure compliance with the developer and regulatory requirements. The first step is to establish the initial set to support the system safety assessment activities.

The new practitioner needs to understand that even the most structured program safety assessment process will require additional effort to support dialogues both internal and external to the program. While

analysis format and content requirements are important, they do not replace cognitive efforts by the system safety analyst. The analyst should also understand that his or her efforts are the first and primary contributions to the safety assessment process. While reviews of the assessments may be by a more "learned" group, these reviews will not be to the same depth or hold the same insight. Their role is generally one of oversight, which does not lessen the obligations of the system safety analyst.

The program phase is also a factor in the type and level of system safety assessment that is required. Program schedules may offer challenges, but they should never be used as excuses for failure to meet the program system safety assessment requirements.

Establishing (and maintaining) a knowledge database becomes increasingly important and challenging as the system safety practitioner's knowledge grows. Figure 2 illustrates several of the contributors to a system safety knowledge database.

One knowledge source (Lessons Learned) applies to all of the knowledge types. For the new practitioner or analyst, the source will be external and historical in nature. Real-time lessons will evolve as the program experience grows. Those with extensive subsystem design experience also need to adjust to a total system perspective, where combinations of failure sources must be identified and assessed.

> "Communication is important, both in terms of the original assessment and the continuing feedback process. To make a contribution, the system safety analyst must be familiar with program processes and the designated role of system safety assessments. More important, there must be an understanding of the program mentality. The nature of our profession requires good communication skills and a strong sense of situational awareness."

Philosophy

Bryan O'Connor noted several characteristics of good system safety engineers that I grouped under "philosophy." Since my discipline background was limited to the development of flight control systems for different space launch systems (real and proposed), I had little discipline inertia to overcome. My educational background in physics was varied, which was helpful in establishing a total system outlook. For those with specific engineering training and experience, acquiring a system perspective, it can be a more difficult task. Thinking with "top-down" (systems level) perspective is different from the bottom-up (component level) analysis focus of many subsystem designers. Unfortunately, many system safety orga-

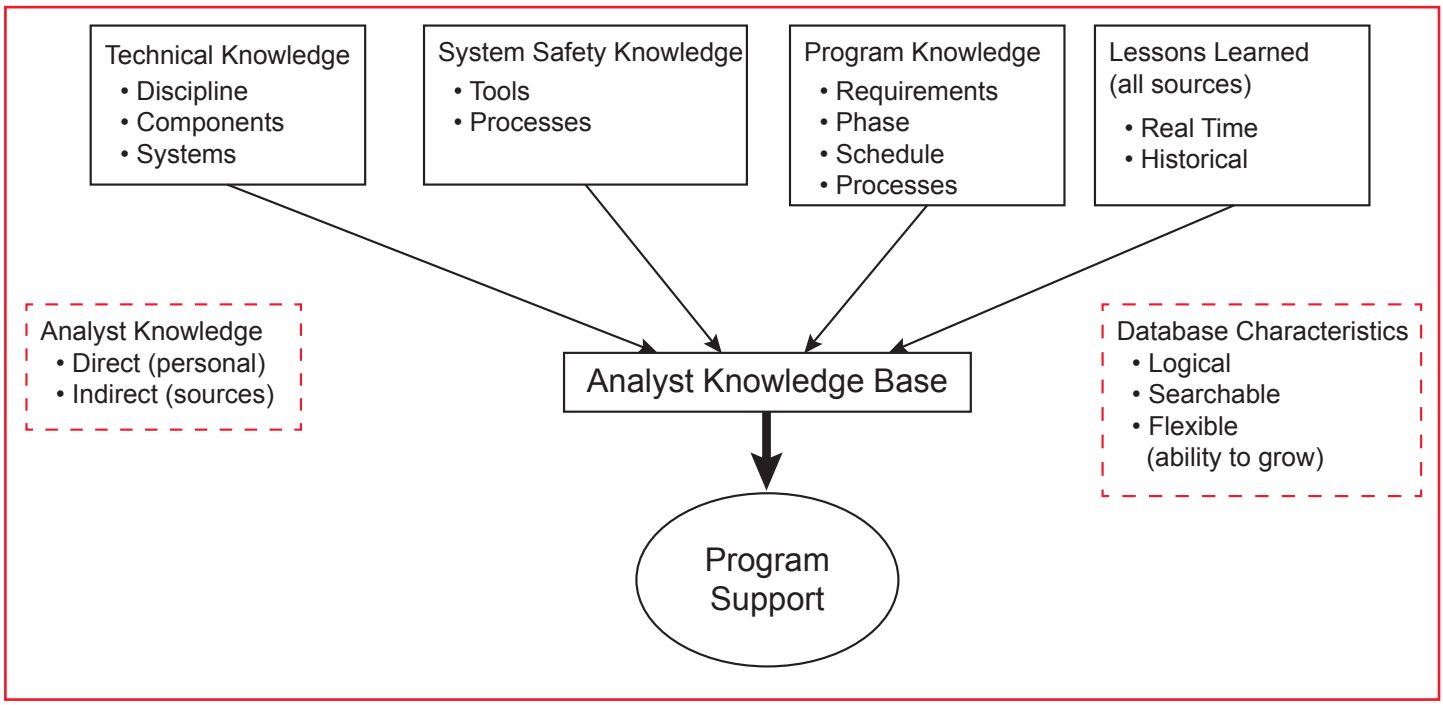

Figure 2 — Analyst/Practitioner Knowledge.

nizations lack the organizational clout of their engineering counterparts. A system safety practitioner needs to understand that a position or recommendation may require persistence to gain acceptance and the value of engineering allies. From a pragmatic perspective, there is a need to understand which positions are negotiable, and which are "throw your badge on the table" in character. The rules of engagement for "western gun fights" do apply.

Using Your Bullet(s)

- Never draw your gun until you are sure it is loaded (you have the right ammunition, both in content and logic)
- Selecting your target is critical
  - — Identify the "highest" threat (risk)
  - — Be careful about wasting your ammunition (there may be another "bad man" around the corner)

Communication

Communication is important, both in terms of the original assessment and the continuing feedback process. To make a contribution, the system safety analyst must be familiar with program processes and the designated role of system safety assessments. More important, there must be an understanding of the program mentality. The nature of our profession requires good communication skills and a strong sense of situational awareness.

Conclusion

As noted at the beginning of this article, my objective was to provide some insights for those getting started in a system safety career. I hope that I provided some useful information and ideas to share with new members of system safety organizations. If I provided any new insights for the reader, that would be an added dividend for my efforts.

References

1. O'Connor, Bryan. "NASA Chief of Safety and Mission Assurance, Characteristics of a Good System Safety Engineer," Group Discussion at the 25th ISSC, August 2007.
2. McNail, Earl. "System Safety Checklist Skylab Program Report" (NASA TM X 64850), May 30, 1974.
3. Clemons, Pat. *System Safety Scrapbook*, (Originally a publication of the Sverdrup Safety Office in the 1980s, currently available at http://www.apt-research.com/capabilities/systemSafety.html.
4. Ericson, Clifton A. *Hazard Analysis Primer*, CreateSpace Inc., 1999.
5. *System Safety Analysis Handbook (2nd Edition)*, System Safety Society, August 16, 1999.

Mark Your Calendar

33rd International System Safety Conference
August 24-27, 2015
Manchester Grand Hyatt San Diego
San Diego, California
issc2015.system-safety.org/

System Safety and Cyber Security 2015
October 20-22, 2015
London Savoy Place
London, England
http://www.theiet.org/events/

2015 International Annual Meeting of the Human Factors and Ergonomics Society (HFES)
October 26-30, 2015
JW Marriott Los Angeles
Los Angeles, California
www.hfes.org//Web/HFESMeetings/2015AnnualMeeting.html

53rd Annual SAFE Symposium
November 2-4, 2015
Caribe Royale Orlando
Orlando, Florida
http://www.safeassociation.com/index.cfm/page/symposium-overview

68th Annual International Air Safety Summit (IASS)
November 2-4, 2015
Eden Roc Hotel
Miami, Florida
http://flightsafety.org/meeting/iass-2015

62nd Reliability and Maintainability Symposium (RAMS)
January 25-28, 2016
Loews Ventana Canyon Resort
Tuscon, Arizona
http://rams.org/