# Journal of System Safety

Volume 50, No. 2
Spring/Summer 2014

# Selling the Need for Safety



**A publication of the International System Safety Society** —
Professionals dedicated to the safety of systems, products and services

# Journal of System Safety

*A publication of the International System Safety Society*

*Volume 50, No. 2*





*Journal of System Safety* is
produced by Panorama Creative Group
1770 N. Audubon Drive
New Albany, IN 47150-4937 USA
Tel.: 812-565-2880
Fax: 407-479-3472
email: journal@system-safety.org

Publisher: Dave Davis


# System Safety Society

**Professionals Dedicated to the Safety of Systems, Products and Services**

## Officers



## Directors



## Corporate Members

A-P-T RESEARCH, INC.
BASTION TECHNOLOGIES
DSTA Defence Science & Technology Agency
BCSP Board of Certified Safety Professionals
BOEING
L3
ST Kinetics
Atlantic Software TECHNOLOGIES
HCRQ
isograph
LOCKHEED MARTIN
LOCKHEED MARTIN AERONAUTICS COMPANY
UNIVERSITY OF MARYLAND
A. JAMES CLARK SCHOOL OF ENGINEERING
Shell
Sikorsky A United Technologies Company

**An official publication of the International System Safety Society, Inc., a non-profit corporation incorporated in the District of Columbia.**

*Journal of System Safety* is published three times a year by the International System Safety Society for the transmission of technical material and news of topical interest to those associated with the practice of system and product safety. Information, recommendations, statements and opinions expressed herein are those of the individual authors and advertisers and do not necessarily represent those of the International System Safety Society. Certain material is published for the purpose of stimulating independent thought on controversial matters or on problems of vital concern to safety professionals. Although caution is taken to ensure accuracy, the publishers or editors cannot accept responsibility for correctness or accuracy of the information presented.



**ARTICLE SUBMISSION**

*Journal of System Safety* welcomes article submissions from its readers. Technical manuscripts and news items of interest should be sent to Clifton Ericson, *JSS* Technical Editor, 6406 Medallion Drive, Fredericksburg, VA 22407 USA.
Email: cliftonericson@verizon.net.

Authors should include the following: (1) one printed copy of the manuscript, double spaced; (2) electronic file in Microsoft® Word™, Adobe® InDesign® or ASCII format; (3) a statement of copyright ownership; (4) a short (one paragraph) author profile; (5) the author's name, address, daytime phone and fax number, email address, affiliation and professional status. For more information on submissions, please email cliftonericson@verizon.net.

All submissions are subject to peer review. If authors wish to have their materials returned, they should send a specific request along with a self-addressed, stamped envelope.

**ADVERTISING POLICY**

*Journal of System Safety* welcomes advertising compatible with the objectives of the International System Safety Society, subject to the approval of the Technical Editor. The acceptance of advertising does not imply endorsement by the Society or *Journal of System Safety*.

For information on advertising rates and submission guidelines, please contact Clifton Ericson, *JSS* Technical Editor, 6406 Medallion Drive, Fredericksburg, VA 22407 USA. Tel.: 540-786-3777; email: journal@system-safety.org. For more information on advertising, please email cliftonericson@verizon.net.

**SUBSCRIPTION AND MEMBERSHIP INFORMATION**

For information on subscription rates and membership, contact the International System Safety Society, P.O. Box 70, Unionville, VA 22567-0070 USA. Tel: 540-854-8630; email: systemsafety@system-safety.org; Web site: www.system-safety.org.



(ISSN-0743-8826)

# Table of Contents

## In The Spotlight



## Features

# President's Message

*International System Safety Society President*
*Robert Schmedake*

## The Value of a Mentor

At the core of any professional society is the charge to aid the membership in its professional development. A few years ago, our Society created the position of director of mentoring, research and development. Currently, Steve Mattern serves that role. Steve took on the program initiated by Mike Allocco and has established the mentoring program. He is now seeking members interested in participating, including mentors, as well as mentees. I believe that participating in a mentoring program is a tremendous benefit to any person's professional development.

In my career, I have been blessed with a number of mentors. These were people who were senior to me in my company, in my profession, in my military organization or in my education. Some were technical experts, some were managers and some were experts in other areas, but understood the business environment in which I worked. Being mentored was an advantage — it meant I could learn from the experience and mistakes of others.

Sometimes, the mentor brought expertise on the product. When I worked on weapon programs, I had a mentor who had experience in getting weapons certified for use. He understood the issues related to getting board approvals, and my program and I greatly benefited from his advice. When I worked on fighter jets, I spoke with pilots to learn about how situations looked from their perspective. I also spent time with maintainers and discovered their unique perspective on keeping aircraft safe. Sometimes, someone who has been down a path before can be a real asset, and sometimes it is good to hear another point of view of a problem on which you have been working.

Another type of mentor has been the career mentor. Some managers have helped me identify my strengths and weaknesses. They helped me identify career opportunities, develop my skills and improve my value to my employer. In short, they helped me find my niche.

With 30 years behind me now, I might be tempted to say I no longer need a mentor, but that's just not true. There is always room for improvement, and there are always new challenges. Lately, I have gotten good advice on corporate survival. In the six months since I took office in the Society, I have struggled with budget issues and Conference legal issues, as well as with finding ways to encourage volunteers. I have come to rely on a number of good managers at my company, as well as a number of excellent members from our Society.

In any enterprise, seeing the dangers that lie ahead of an obstacle is a challenge. Mentors are the advance scouts who may have already traveled the route you are now taking. They illuminate the way forward and help us see the dangers and benefits of a particular path. I cannot imagine what my career would have been without the mentors I have had, and I want to encourage you to take advantage of the networks you are in to find the right mentor for the path you are taking.

Being a mentor also has benefits. As a Boeing Technical Fellow, I am expected to provide mentoring. I find that mentoring a less-experienced engineer sharpens my skills as much as theirs. For one thing, ideas I have come to accept as true get challenged. Questions from an engineer on why a particular path is a good path cause me to re-evaluate what I believe, and I often have a much better understanding of the topic after the time I spend discussing it with the mentee.

So, how does being a mentor benefit my value as a professional? One's career arc starts with the role of being a learner. We transition from learning the job to doing the job. Eventually, we get to a point where we imagine better ways of doing the job and create efficiencies in our work. When we move from creating better ways for ourselves to teaching others about these efficiencies, we begin to influence our employer's productivity and effectiveness at a much higher rate. When we transition from mentoring individuals to leveraging change at an organizational level, we are truly impacting our organization's effectiveness. Our value to the organization increases as we follow this arc.

So, contact Steve at smattern@bastiontechnologies.com and volunteer. Become a mentor, or get a mentor. This is an excellent way to develop within your profession.

# 32nd International System Safety Training Symposium

**August 4-8, 2014** **St. Louis, Missouri**

**Meet us in St. Louis at ISSTS 2014.** The goal of this training symposium is to bring practitioners and the foremost experts within the system safety discipline together to exchange ideas, knowledge, experiences and best practices.

There will be contributions from a variety of domains including aerospace, automotive, defense, health care, rail transportation, critical infrastructure systems, robotics, industrial control systems, and academia.

**Register Now** – Discounts are available for early registration and full-time students

**Reserve Your Room** – Guarantee a spot at the hotel while rooms are still available

**Earn CEUs** – Continuing Education Units (CEUs) will be issued for training tutorials

**We Need You** – Chair a session or workshop

**Become a Sponsor** – Show your company's support and receive many benefits

**Exhibitors Wanted** – Take advantage of a wonderful marketing opportunity

**Bring the Family or Extend Your Stay** – There is a lot to see and do in St. Louis

Additional information can be found at
**http://issc2014.system-safety.org**

# From the Editor's Desk...

*JSS Technical Editor*
*Clif Ericson*

## Habits

As editor of *Journal of System Safety*, I often do "extra-curricular" reading to keep up with events and technology. Recently, I read a book titled *The Power of Habit* by Charles Duhigg. The book is primarily about the power that habits hold over us, how to modify bad habits and how to create new, good habits. It was an interesting book, but what really caught my attention was one of the case studies described in its pages. This particular case study followed Paul O'Neill as he took over as CEO of Alcoa in 1987. He took the reins during a time of low profits and a poor accident record. But, as the new CEO, he did not make promises to lower costs, increase productivity and boost profits, as was expected. He stated that his goal was to make Alcoa the *safest* company in America — his objective was zero injuries. At that point, nearly everyone in the audience thought his selection as CEO was a mistake and many recommended selling their stock before the company fell into decline.

> "[Alcoa CEO Paul O'Neill's] philosophy was that if Alcoa could bring its injury rates down, it would happen because managers and employees would have agreed to become part of something important — they would have devoted themselves to creating a *habit* of excellence. Safety would become an indicator in changing bad habits across the entire company."

O'Neill believed that some habits have the power to start a chain reaction throughout a company. Safety was a *keystone* habit that influenced all other habits and processes in the company. His philosophy was that if Alcoa could bring its injury rates down, it would happen because managers and employees would have agreed to become part of something important — they would have devoted themselves to creating a *habit* of excellence. Safety would become an indicator in changing bad habits across the entire company.

O'Neill was serious about safety, and the book explained many of the detailed steps he took to instill this new keystone habit. Within a year, company profits reached a record high. By the year 2000, when O'Neill retired, someone who had invested a million dollars in the company when O'Neill was hired would have earned another million in dividends.

For me, the moral of this story is that, as safety engineers, we must never give up or concede to degraded levels of safety. We need to vigorously continue to "sell" safety to management and use stories such as this to show that it really works. This is a great example of where safety had an even greater pay-off than saving lives.

The first technical paper in this issue, "*Exxon Valdez*: Human Error, Plain and Simple" by Arthur Barondes, notes that the effects of the 1989 disaster continue to be felt to this day. Not surprisingly, various interests seized on the catastrophe to support their causes or improve their lots. While it is now clear that the ship went aground purely as a consequence of human errors — there were no mechanical or electrical failures — the event has been used to justify changes that, while desirable, would not have prevented the *Exxon Valdez* from going aground, or the subsequent oil spill. These changes include, among other things, a variety of improved navigational aids, expanded Coast Guard monitoring capabilities, increased requirements for harbor pilots and required crew rest. In looking back, one might be led to believe that the ship went aground in a sea of red herrings. This paper reviews what *really* happened on that night, and the incontrovertible evidence that supports the idea that human errors — and a failed safety culture — were solely responsible for the disaster.

The second technical paper in this issue contains the results of the two-day Safety Case Workshop that was conducted in January 2013. The workshop, under the sponsorship of the SAE International G-48 System Safety Committee, generated international participa-

tion from industry, government and academia. The United States has typically used a process-based approach in managing system safety programs, but there is a current movement to use the evidence-based Safety Case approach to validate the safety of systems. At the conclusion of the workshop, participants reached the consensus view that the Safety Case approach has merits worthy of being accepted among the best worldwide system safety practices.

The third technical paper in this issue, "Technical Safety or System Safety? Why Names Matter" by Sergio Oliva and Ricardo Lopez, discusses a challenge the authors faced from a customer who opined that technical safety was different from the other "safeties," such as system safety, functional safety or operational safety.

In his "System Safety in Healthcare" column, Dev Raheja discusses "The Challenges of Sign-offs." As healthcare has become more specialized, more clinicians are involved in patient care, which often leads to more complex patient sign-offs as compared to years past. Erroneous sign-offs can contribute to gaps in patient care and hazards in patient safety, including medication errors, wrong-site surgeries and patient deaths. Clinical environments are dynamic and complex, presenting many challenges for effective communication among healthcare providers, patients and families. This article presents an overview of sign-offs and hazards, as well as suggestions for quality improvement initiatives and recommendations for potential remedies.

In his "TBD" column, Charles Hoes discusses the leak of MCHM (4-Methylcyclohexanemethanol) into the drinking water supply for the city of Charleston, West Virginia. As it turns out, there was actually more than MCHM in the leak, but since the company failed to notify the authorities about the additional chemical(s), they weren't included in the initial tests for water safety.

In his "Unintended Consequences" column, Terry Hardy discusses the lessons learned from an aluminum dust explosion that occurred at the Hayes Lemmerz International-Huntington, Inc. facility in Huntington, Indiana on October 29, 2003. And, in his "Design-Based Safety" column, Dave MacCollum discusses the concept of "Selling Safety."

Remember, if you wish to opine send me an email at journal@system-safety.org.

Until next time,
Clif

## Mark Your Calendar

**12th Probabilistic Safety Assessment and Management (PSAM) Conference**
August 22-27, 2014
Sheraton Waikiki - Honolulu, Hawaii
http://www.psam12.org

**The 52nd Annual SAFE Symposium**
November 3-5, 2014
Caribe Royale - Orlando, Florida
http://www.safeassociation.com/index.cfm/page/symposium-overview

**Human Factors and Ergonomics Society (HFES) 2014 Annual Meeting**
October 27-31, 2014
Hyatt Regency Chicago - Chicago, Illinois
https://www.hfes.org/

**Safety in Autonomous Systems**
December 4, 2014
London, U.K.
http://www.safety-club.org.uk/e299

# TBD

*by Charles Hoes*

As you have likely heard by now, there was recently a leak of MCHM (4-Methylcyclohexanemethanol) into the drinking water supply in the city of Charleston, West Virginia. It turns out that there was actually more than MCHM involved in the leak, but since the company failed to notify the authorities about the additional chemical(s), they weren't included in the initial tests for water safety.

The leaking tank problem generated a lot of press because it caused such a large problem to the local community, shutting off the city's water supply for many days. A couple of interesting problems have been highlighted in the news discussions. One of these was the lack of understanding of the hazards associated with the leaked material. Apparently, the best information available to emergency response personnel was obtained from the material safety data sheets (MSDS). Unfortunately, almost all of the important safety information was listed as "unknown."

The next problem of note was the almost *complete lack of planning* by the company, the water district or anyone else concerning what to do in the event of a chemical leak into the drinking water. Then, there is the issue of reports that the storage facility hadn't been inspected for the last 20 years. Not only that, but the leak was reportedly only detected because neighbors complained about odors. The tank had apparently been leaking into the water supply for an unknown length of time.

I found one news article to be quite interesting because it pointed out that the planning activities for this sort of thing are done at the local level by local resources. We have a similar situation in my neighborhood. I live in a "rural" agricultural community that has several potential sources of significant chemical spills into local water supplies. We are located close to the Sacramento River, which is a major source of water for much of the state of California. Our fire department is located within a few feet of Interstate 5, which is the main north-south artery for the western United States. There is always a potential for large spills of a wide variety of chemicals from tanker trucks, rail cars on the railroad running adjacent to the highway or local storage facilities. There are a number of chemical storage and distribution centers in our small community, handling large amounts of pesticides and other chemicals important to the local agricultural and natural gas drilling industries.

Our fire department is charged with identifying chemical hazards and making plans to control them. However, as a member of the local volunteer fire department, I know that there is nobody in the department who is necessarily qualified to do any of this work (with the possible exception of myself). The department sends out a fire department member without any training or background in safety (who happens to be the chief) to look at new chemical facilities as part of the county permit process. He signs whatever needs to be signed to obtain the permit, and that is the end of it. There is no follow up. There are no verification inspections or periodic inspections. Nobody looks at or evaluates company safety plans, and the department has no internal plans, equipment or training in what to do in the event of a significant spill.

While it sounds extreme, it is the way it's done in every small town and city in northern California — and probably the other states, as well. Generally, there are no resources available to do this sort of planning, and most of the people who are charged with doing it have no training, ability or inclination to do so. In many cases, these people are the same people who would have to spend extra money if something was found needing to be fixed. The local folks who are in control also tend to be the local folks who have a financial stake in everything that happens locally. They are also usually convinced that they are being overly regulated by government agencies of all sorts in the first place.

In addition to a lack of qualifications to perform comprehensive emergency planning, a lack of chemical safety information makes effective planning almost impossible. It is my understanding that something close to a "Catch 22" cycle exists. The Toxic Substance Control Act

> “...there was recently a leak of MCHM (4-Methylcyclohexanemethanol) into the drinking water supply in the city of Charleston, West Virginia.... One of [the problems] was the lack of understanding of the hazards associated with the leaked material. Apparently, the best information available to emergency response personnel was obtained from the material safety data sheets (MSDS). Unfortunately, almost all of the important safety information was listed as ‘unknown.’”

(TSCA) of 1976 requires companies to perform safety studies on chemicals that the EPA has determined are hazardous. However, the EPA doesn't have the staffing or funding needed to determine which chemicals might fit into this category of requiring safety studies. Not only that, there are tens of thousands of chemicals, formulations and mixtures that are unknown to the EPA. The end result is that few chemicals are actually studied for safety. The main tool used to notify the EPA that a chemical is hazardous comes from epidemiological studies in which people have been found to have been injured by the materials.

MSDSs are required for chemicals placed into commerce, but these are often created by individuals lacking the necessary qualifications and based on questionable data and MSDSs for the materials that are used to make the new product. Even if the information for the raw materials was good (an extremely unlikely situation), the assumption that the risks of the final product can be predicted from the risks of the raw materials is fraught with uncertainty. For example, the risks of water are different from the risks of either of the constitute parts (hydrogen and oxygen). There are risks associated with water, but flammable and explosive hazards no longer apply once the materials have combined into a new form. It should also be noted that there are essentially no government or third-party reviews of the quality of MSDSs. The documents are assumed to be valid, complete and accurate without oversight or review.

Because of these (and many other) issues, it seems the system designed to protect people and the environment from potentially hazardous chemicals and materials is woefully inadequate. While the structure and framework for appropriate regulations and planning are in place, they are often ignored and not enforced because of limitations on funding, manpower and the will to do so.

There is constant pressure from the news media and politicians to deregulate and remove existing safety and environmental protections. The public seems to assume that we have a strong consumer and environmental safety culture, when we actually have a lax one. Examples of “overregulation” get front-page news coverage, but the positive impacts of appropriate regulations and the need for additional regulations with effective monitoring and oversight seldom get reported.

Most people that I talk to are shocked and appalled when I tell them that few products have been tested or evaluated for safety, and that the vast majority of chemicals have unknown safety characteristics. Most homeowners are equally ignorant about the lack of safety planning and site inspections for the chemicals stored in their neighborhoods and near their sources of water. They believe that the government is not only looking after their welfare in these areas, but that it is doing so in excess — causing harm to industry and the economy. I guess this is what is meant by “living in a fool's paradise.” I don't know what we can do to address these issues, but we can at least attempt to educate our friends and neighbors regarding the lack of regulation and scientific understanding of the safety implications of the chemicals that surround us on a daily basis. Unless the public is informed about the true nature of the regulatory situation, people will continue to believe that we are overregulated and are over-studying the issues — and will demand further cuts in funding to these efforts.

# Unintended Consequences

*by Terry Hardy*

## Dust Explosion in Indiana

On October 29, 2003, an aluminum dust explosion occurred at the Hayes Lemmerz International-Huntington, Inc. facility in Huntington, Indiana. One worker was killed and six others were injured in the explosion. The U.S. Chemical Safety and Hazard Investigation Board (CSB) investigated the accident and found that the explosion occurred in the scrap re-melting system, a system used to re-melt chips of aluminum scrap from wheel machining operations.

The CSB said in its report that the accident was the result of several factors. First, the chip feed system was releasing excess aluminum dust, but the company did not perform a review to examine why this was occurring. The company made temporary patches to the system to repair holes that had worn through ducts and pipes, but dust and chips still blew through unrepaired leaks. Second, the CSB stated that the company did not properly design its dust collection system. Third, the company did not ensure that the dust collection system and installation followed industry guidance. Finally, the company had experienced several fires, but did not have a formal root cause and corrective action system to investigate these incidents. For example, just hours before the accident, a duct fire had occurred that was extinguished. Employees told CSB investigators that such fires were frequent events.

The report also said that, while formal procedures existed, employees received no formal training on those procedures. According to the report, "The lack of formal training for the chip and dust collection systems' operators and maintenance personnel led to acceptance of abnormal conditions — the 'normalization of deviations,' such as flashes during chip feed startup and fires in the fume exhaust ducts."

"According to the [CSB] report, 'The lack of formal training for the chip and dust collection systems' operators and maintenance personnel led to acceptance of abnormal conditions — the 'normalization of deviations,' such as flashes during chip feed startup and fires in the fume exhaust ducts.'"

**Lessons Learned:** Analyses after accidents often show that clues existed before the mishap occurred. Such clues frequently take the form of anomalies observed during the lifecycle of a project. An anomaly is an apparent problem or failure that occurs during verification or operation and affects a system, subsystem, process, support equipment or facilities. Anomaly or problem reporting and corrective action, therefore, can play an important role in system safety analyses. An effective anomaly report and corrective action process not only allows for the reporting of problems, but also implements a closed-loop process for finding and fixing the root cause of a problem. In the case of this accident, if the near-misses had been properly reported and analyzed, it may have been prevented.

Readers are encouraged to review the full accident and mishap investigation reports referenced here to understand the often complex conditions and chains of events that led to each accident discussed here. Additional lessons learned are available at www.systemsafetyskeptic.com.

### References

U.S. Chemical Safety and Hazard Investigation Board, "Investigation Report: Aluminum Dust Explosion (1 Killed, 6 Injured), Hayes Lemmerz International-Huntington, Inc., Huntington, Indiana, October 29, 2003, Report No. 2004-01-I-IN, September 2005.

# Now Is the Time… To Upgrade Your Membership

*by Russell Mitchell, C.S.P.*
*Houston, Texas*

"May you live in interesting times" — so goes the curse. Lately, it seems there are interesting developments at every turn. The International System Safety Society (ISSS) has taken on the objectives of providing global system safety perspectives and improving member value in the midst of real flux in the profession. The policy and budget drivers shaping our key industries are not particularly supportive of our efforts. In this climate of "leaner and meaner" societal norms, each of us must put forth our best efforts and be seen in the best possible light to influence the projects and programs where we work, simply to survive. There is no substitute for sound system safety practice. We each need to do the right jobs, in the right way, to have the best influence on our work. In addition, it helps to have professional recognition. The ISSS has long asserted that members benefit from being recognized for their professional capabilities and professional service.

The ISSS recognizes members in various ways, including professional awards and a professional membership advancement track that includes Senior and Fellow membership designations. These credentials provide members with tangible evidence they can use to enhance their resumes and CVs, to hang in their offices and to support their advancement within their companies.

As a member, the real key to your membership advancement is your application. You'll need to download an application (available at http://www.system-safety.org/pdf/SSS_membership_application_form_rev41.pdf) to see if you meet advancement criteria.

Once you have the application handy, you can review the advancement criteria against your experience. The basic criteria for advancement to Senior Member include:

- Four years of System Safety Society Membership
- 35 points cumulative from:
  - o At least 12 points must be from the combined *educational, experience, and contributing achievement* areas
  - o At least 10 points from the *professional achievement* area.

The educational area credit is awarded based on your studies. The application provides you the opportunity to take credit for university or professional training.

The experience area credit is awarded based on your work experience. The application provides credit for full-time and part-time work on system safety-related tasks, at a rate of one point per year of full-time experience (or a half-point for a year of part-time experience).

The contributing achievement area credit is awarded based on your experiences serving in roles supporting either your local chapter or the Society internationally. The application presents an extensive list of opportunities to take credit for your efforts to support the International System Safety Society.

The professional achievement area credit is awarded based on your advancement in your professional career such as professional engineer, certifications, awards, publications and promotions. The application presents an extensive list of opportunities to take credit for your professional advancement.

Advancement to Fellow uses the same application and requires the following basic criteria:

- Minimum of five years of Senior membership
- Minimum of 70 points
  - o At least 35 points qualifying under the Senior Member criteria mentioned above.
  - o Another 35 points of which must come from the contributing achievement area.

Both Senior and Fellow applications require three letters of recommendation. For Senior members, the recommendations should come from either Senior members or Society Fellows. Recommendations supporting an upgrade to Fellow must come from Fellows of the Society. Have the letters sent directly to russmitchellcsp@yahoo.com.

Because the application must be submitted with copies of documentation that will be used to verify the application, contact headquarters prior to submitting your application. Also, email russmitchellcsp@yahoo.com to arrange for a discussion of the process and guidance about the application and qualified documents. Many applicants provide more information than required or procrastinate applying because they feel overwhelmed. My job is to make the process painless and straightforward.

The application process moves fairly quickly once all of the information has been received. All communications are now electronic, including the various approvals and voting, so there is no need to wait. If you would like to receive your certificate or plaque at the annual meeting in August, plan on submitting your application in April to avoid the year-end rush in June.

I am preparing my own paperwork right now; you should, too!

# System Safety in Healthcare

*Dev Raheja & Maria C. Escano, M.D.*

## The Challenges of Sign-offs

With increasing demand for efficiency and productivity from a clinical team that's often overworked and understaffed, provision of seamless patient care is challenging. Clinicians need to hand off — or sign off — essential information to the next provider to help transition care. An effective hand-off supports the transition of critical information, along with continuity of care and treatment. This article offers an overview of sign-offs, hazards and suggestions for quality improvement initiatives, as well as recommendations for potential remedies.

Healthcare has become more specialized, and more clinicians are involved in patient care, which often leads to more complex patient sign-offs compared to years ago. Erroneous sign-offs can contribute to gaps in patient care and hazards in patient safety, including medication errors, wrong-site surgeries and patient deaths. Clinical environments are dynamic and complex, presenting many challenges for effective communication among health care providers, patients and families.

Sign-offs are not free of human errors. Clinicians are overwhelmed with the volume of electronic notifications and may ignore them because of warnings and alerts fatigue. If clinicians do not check the messages, the EMR's safeguards are ineffective. Another risk occurs when a clinician uses the e-prescribing function of an EMR, but if the computer is temporarily unavailable, the clinician may prescribe on paper, which may not be entered into the system. The next prescriber may be totally unaware of the prescription.

Other hazards include:

- **System Crashes —** A clinician may fail to back up files and may end up losing patient records, which may also create problems for payers when it is time for an audit.

- **Automatic Orders —** Sometimes, a computer software program will order diagnostic tests automatically. This may result in overtreatment. A physician recently commented that "Doctors want to practice medicine the way it was intended to be practiced — individualized in care" [Ref. 1].

- **Usability Errors —** These errors, omissions and hazards can range from missing an important finding that is buried in a template charting and inadvertent selection of the wrong patient from the drop-down menu to computer glitches that result in a loss of unsaved data, and auto-population of incomplete or erroneous data from generic templates.

- **Distraction Oversights —** These oversights can include omission of vital information presented by the patient while the clinician is entering data. He or she may fail to hear everything the patient is saying or ignore the body language of the patient when the computer becomes a barrier instead of an adjunct to patient care [Ref. 2].

- **Computer Entry Errors —** Computer entry errors can range from clinicians clicking the wrong box to the system pulling incorrect data. In one survey, 75 percent of clinical staff indicated they have identified multiple errors on a weekly basis. One hundred forty-two nurses from Contra Costa County Hospital filed formal complaints alleging errors in the EHR, which resulted in medication dosing errors. The system also wouldn't allow them to document medication administration appropriately. Dosages recommended by the system would have been fatal had they been administered [Ref. 3].

“Computers, just like any other technology, have advanced health care in ways that were not possible generations ago. However, patient care is a dynamic and complex process. This challenge needs to be met and balanced with individual patient needs, staff/clinician resources, and technological limitations to minimize patient harm.”

## What are the Remedies?

The usual remedies (not always practiced) are to use risk analysis tools on the sign-off process, such as Preliminary Hazard Analysis and Fault Tree Analysis [Ref. 4 & 5]. These tools help predict harmful errors and provide guidelines for risk mitigation.

Dr. Mark Chassin, president of The Joint Commission, and Dr. Jerod M. Loeb, executive vice president for healthcare quality evaluation of The Joint Commission, suggest paying attention to reliability methods. They report that “too many hospitals and healthcare leaders currently experience serious safety failures as routine and inevitable parts of daily work” [Ref. 6]. To prevent the harm that results from these failures, which affect millions of Americans each year, the article specifies a framework for major changes involving leadership, safety culture and robust process improvement. This framework is designed to help hospitals make progress toward high reliability, which is the achievement of extremely high levels of safety that are maintained over long periods of time — safety comparable to that demonstrated by the commercial air travel, nuclear power and amusement park industries.”

Dr. Chassin further said that although no hospital has been able to achieve high reliability, there are some practical changes that can be made to improve safety and quality. “The time is now to start taking the steps needed to get from where we are today to where we want to be,” he said.

Computers, just like any other technology, have advanced health care in ways that were not possible generations ago. However, patient care is a dynamic and complex process. This challenge needs to be met and balanced with individual patient needs, staff/clinician resources, and technological limitations to minimize patient harm.

## References


1. Makary, Martin, M.D. “What Hospitals Won’t Tell You and How Transparency Can Revolutionize Healthcare,” March 24, 2013, http://articles.mercola.com/sites/articles/archive/2013/03/24/modern-medical-errors.aspx
2. Buppert, Carolyn. “Electronic Medical Records: 18 Ways to Reduce Legal Risks,” *Topics in Advanced Practice Nursing* eJournal, January 13, 2010, http://www.medscape.com/viewarticle/714812_1
3. Roberts, Laura and Amy Bailie Muckler. “Electronic Health Records – Auditing Quality and Compliance,” American Health Lawyers Association, http://www.healthlawyers.org/Events/Programs/Materials/Documents/FC12/205_muckler_roberts_slides.pdf, accessed on October 10, 2014.
4. Raheja, Dev. “System Safety in Healthcare: Preliminary Hazard Analysis for Minimizing Sentinel, Adverse and Never Event,” *Journal of System Safety*, July-August 2009.
5. Raheja, Dev, and Maria C. Escano, M.D. “Reducing Patient Healthcare Safety Risks Through Fault Tree Analysis,” *Journal of System Safety*, September-October 2009.
6. Zhani, Elizabeth Eaken. “Hospitals Still Far from Being Highly Reliable,” *The Milbank Quarterly*, September 17, 2013.

# Design-Based Safety

*David MacCollum*

## Selling Safety

Marketing safety can be compared to the Greek myth in which Sisyphus, the King of Corinth, was punished in Hades by having to roll a huge stone uphill, only to have it roll down repeatedly as soon as he had pushed it to the summit. A quick review of negative opinions that make selling safety a task like that of Sisyphus tells us that the introduction of alternate safer design is often greeted with the comment, *"Safety does not sell."* Many people have a built-in mindset that rejects design-based safety. They feel that *accidents can be avoided with simple common sense* and believe accidents are the result of bad luck and are the cost of progress. Few people are aware that accident prevention is a "Gemini function" with twin approaches:

"Developers of projects usually lack the expertise to ensure for safety and environmental hazard prevention. Safety by design is an invisible function. All enterprise needs the expertise of system safety engineers to overcome people and environmental hazards with green engineering."

- The first "twin" is the most-used concept in avoiding accidents: *All that is required is to modify human behavior.* As Sisyphus found, this twin relies on behavior modification to avoid a hazard, but discovers that the hazard, like the stone, can roll back down because it has not been eliminated.
- The second "twin" is usually overlooked; it requires the hazard to be eliminated by design.

"Selling" safety requires that the public be told that when a hazard is eliminated by design, the accident cannot be repeated. But there are a number of reasons why safety does not sell. Usually, management takes the easy way out and relies on insurance to pay for the loss. This allows speculation as to what the risk will be for the occurrence of unidentified hazards causing injury, death or damage. Management is now no longer troubled with the task of hazard identification and prevention. Those responsible for the purchase of equipment or machines are often uninformed about available safety appliances or safer designs. These should be specified in purchase contracts. Developers of projects usually lack the expertise to ensure safety and environmental hazard prevention. Safety by design is an invisible function. All enterprise needs the expertise of system safety engineers to overcome people and environmental hazards with green engineering.

The "Catch 22" is that a change of emphasis has evolved with the development of automation. This has given priority to design-based safety. The 21st century will bring workerless production, just as we hear today about driverless cars. The seeds of this change were planted in the 1960s, when the Department of Defense implemented MIL-STD-882 for system safety. The development of sophisticated electronics to guide drones, missiles and surveillance systems was a top-secret effort requiring military security clearances. Today, we are experiencing how, little by little, system safety is being incorporated into our economy. Our National Transportation Safety Board (NTSB) started with airline safety and then promoted legislation for Positive Train Control (PTC) to overcome inherent lapses in operating engineers' consciousness. The British are adopting Business Information Modeling (BIM), which copies the U.S. Army's civil districts' public works program called Construction Operations Information Exchange (COIE) and includes hazard identification and prevention at the time of planning and design. Building plans in three dimensions afford bigger, better and faster construction, as these plans show what the completed project will look like. This activity makes hazards visible.

“A hazard is always in one of three modes: dormant, armed or active.... A clear example of this is when a raised crane boom comes into contact with a power line. The ability to raise a crane boom so it can reach a power line is always present. When a crane is used in a location in which there are no power lines, the hazard is *dormant*; when it is used where a power line can be reached with its raised boom, the hazard is now *armed*; when the boom strikes a high-voltage overhead power line, it is *active*.”

Automation is liberating the workforce from monotonous and dangerous employment, and is providing opportunities in higher-paying installation, operation and maintenance of automated production positions. The public has little awareness of the nature of hazards, so they can be identified.

A hazard is always in one of three modes: dormant, armed or active. Many people believe it is only by chance that a hazard will become active, making prevention unnecessary. A significant concern is how much harm the hazard will cause when it becomes active. A clear example of this is when a raised crane boom comes into contact with a power line. The ability to raise a crane boom so it can reach a power line is always present. When a crane is used in a location in which there are no power lines, the hazard is *dormant*; when it is used where a power line can be reached with its raised boom, the hazard is now *armed*; when the boom strikes a high-voltage overhead power line, it is *active*. The prediction of the harm that the active hazard will cause is another uncertainty. It may only cause momentary sparks, but it can also cause severe injuries or even deaths, costly property damage or a huge electric power outage. Hazard avoidance training does nothing to eliminate this hazard.

Advocates of hazard avoidance rely primarily on modifying worker behavior, but this does not remove the overhead power lines from the crane’s work site, nor does it provide insulated links to guard the workers guiding the load from the flow of high voltage or provide workers with a proximity alarm device that would warn that the boom is near a power line. Sole reliance on worker behavior is not a reliable measure to prevent wrongful injuries or death from crane boom/power line contact. This illustration is one of countless examples of how sole reliance on personnel behavior modification is like repeatedly pushing a huge stone uphill and having it roll back down. When a hazard is avoided by worker training, even though it is obvious that the hazard could have been eliminated, the public loses confidence in safety in two ways:

- It knows that training alone isn’t the answer.
- It considers the safety profession ineffective, as the hazard was not discovered and removed.

The only reliable means of preventing costly occurrences is to use the second “twin”: requiring design-based safety. Because a hazard can be in one of the three modes described previously and because of the uncertainty of the consequences, the emphasis shifts from hazard identification and prevention to speculating that a loss is only by chance and may arise from unknown occurrences. Risk management focuses primarily on developing a safety culture that centers around behavior-based safety, with little emphasis on hazard prevention through design-based safety. It is at this point that some people become dissatisfied with the lack of emphasis on hazard removal or by not providing accessories that either warn of the hazard or intercede to prevent injury. Often, managers just hope that they can continue to be lucky.

With all the negative aspects around the functional administration of safety, most management leaders are totally blind to this shift to automation. The reduction of defense spending is curtailing opportunities in the development of military systems. Both business leaders and specialists who have experience in developing system safety now have a new challenge to transform their expertise in design-based safety from military applications to civil automation. Many steps can be taken by system safety specialists to tap the bonanza of the switch to automation with design-based safety. The old academic adage to "publish or perish" rings true for the system safety specialist. Trade publications are always looking for articles on how safety features reduce costs, injuries or death.

System safety specialists have unique knowledge that is marketable in teaching engineers in conventional disciplines how to expand their practice by identifying hazards at time of design and by providing alternate, safer designs. New career paths are opening for specialists to be retained by companies that are providing design-based automated systems. Even personal injury attorneys understand the need to inform courts and juries as to how design-based safety eliminates hazardous conditions and circumstances.

The marketing of safety to overcome the Sisyphus syndrome needs the expertise of public information specialists. Progressive business management either has this staff capability or can expand this effort by retaining nationally recognized authorities on public information. When public relations is funded to ensure publication in major radio, television, newspapers and magazines, a dramatic public interest can be developed. It is a well-documented fact that executives and top managers do read and improve their own activities and operations from what is in publications such as *The Wall Street Journal*, *Business Week*, *The Economist* and *Engineering News Record*. Members of the general public who want to stay current read *The Atlantic* and *The New Yorker*. Public relations experts know how to shape the public's awareness to benefit their clients. Public relations could include interviewing system safety specialists to develop their identity as individuals with special knowledge on how to protect people's lives with design-based safety, while improving the profit margin of the enterprise. Public relations professionals know where to target the placement of advertisements and text to motivate acceptance by those who should adopt design-based safety.

But public relations is not a do-it-yourself activity. In addition to providing a well-funded program, some of the large international design-and-build construction and mining firms have substantially increased their operations by first training all their engineering and construction management staff members in the basics of design-based safety. This method of "selling" safety to key staff engineers and construction managers provides them with the expertise to sell their safety to their clients. They are then able to expand the scope of their proposals and activities to include design-based safety. The growth of professional societies is becoming dependent on their choices to ensure members personal development and success, and on promoting educational opportunities and public awareness of their members' expertise in design-based safety. These organizations would do well to retain public relations firms to tell the business world and the public about the accomplishments and special skills of their members.

The task of selling design-based safety as a marketable enhancement of products, services and systems is unlimited. Every enterprise can benefit by selling design-based safety as a critical component of their activity. As every community becomes more dependent on technology, more and more people are becoming dependent on design-based safety. Public opinion can be like a huge rock being rolled uphill. When things go wrong because of hazardous design, the huge rock of public opinion rolls back down the hill. No longer will the public tolerate an absence of transparency and allow themselves to be the guinea pigs in identifying hazardous conditions or circumstances. Nor will blaming someone else as a scapegoat suffice as an excuse for not providing safe design. Selling design-based safety is rapidly becoming a marketable commodity. The recent poisoning of the water supply in Charleston, West Virginia is a great example of how toxic chemical storage tanks need to be placed within a watertight basin so that if a leak occurs in a tank, the toxic liquid cannot contaminate the soil and water table. The limited scope of safety professionals' being restricted to prevention of worker injury and death needs to be expanded to include the public, product safety and environmental safety. To sell safety effectively, we need to use examples of the second Gemini twin's ability to eliminate the hazard. The traditional method of behavior modification does not work, as it is vulnerable to the Sisyphus syndrome of the hazard repeatedly causing injury or death. Many safety heroes, whose work products have eliminated hazards by design, have never been recognized. Telling the world about these heroes who have developed safety features is the best method of selling safety.

# A Lifetime Dedicated to Making Workplaces Safe

*by Dana Cole*
*Sierra Vista, Arizona*

David V. MacCollum, known for visionary achievements as a safety engineer, is being recognized for a lifetime of contributions in the safety profession.

Recently, during a reception in his Sierra Vista home, the Board of Certified Safety Professionals (BCSP) recognized MacCollum by naming a $2,000 scholarship in his honor. In addition, he was presented with a plaque by Don Eshelby on behalf of the BCSP, a board dedicated to certifying practitioners in the safety profession. MacCollum's presentation was made before members of the Southern Arizona Chapter of the American Society of Safety Engineers (ASSE).

"The Certified Safety Professional Award of Excellence is given to one individual each year with the greatest contribution to the safety profession," Eshelby said. The $2,000 scholarship will be awarded to a student, safety educator, college professor or an individual who works in the safety field.

During a discussion about MacCollum's career and contributions, Eshelby said, "With around 10,000 Certified Safety Professional certifications throughout the world, David MacCollum holds the third certificate. He's one of the very few individuals who has achieved as much recognition and respect from safety professionals."

In addition to the BCSP scholarship, the Southern Arizona ASSE established and named a visionary scholarship after MacCollum, also honoring his extensive list of contributions to the safety profession, in recognition of a career that spans more than 60 years.

Shari DiPeso, Southern Arizona ASSE president, said, "We are very fortunate to have an individual like David as part of our chapter and part of the safety community. His contributions to the body of knowledge for the safety profession are legion. His energy, focus and intellect in so many areas have resulted in better designs, which have saved numerous lives. It is only fitting that our scholarship, which will support the next generation of safety professionals, be named in his honor."

The ASSE is currently building the fully funded $30,000 scholarship which will be administered through the ASSE National Foundation, said Mark Grushka, a health and safety consultant and ASSE member. "Once we reach the $30,000 goal, we are hoping this will become self-sustaining, so a deserving student in the health safety or environmental field will be given a $1,000 scholarship each year."

MacCollum, 90, is a past ASSE president and was a member of the first U.S. Secretary of Labor's Construction Safety Advisory Committee (1969-1972). In 1999 the ASSE named MacCollum a Fellow, the Society's most prestigious honor, recognizing a lifetime of commitment to the occupational safety and health profession.

"I've been a maverick, fighting the system forever," smiled MacCollum, whose interest in occupational safety dates back to 1946 during a time when he worked in the logging industry while attending college at Oregon State University. "I witnessed a lot of very serious accidents on that job, where one man a month was killed," he said. MacCollum's experiences in the logging industry served as a driving force behind rollover protection structures for tractors and other construction equipment, which he developed in the 1950s while working with the U.S. Army Corps of Engineers in Oregon.

Through his role as an occupational safety engineer, MacCollum fought for improved safety conditions for workers in a wide range of industries. "I have always believed you can prevent serious injuries by eliminating hazards, but there were many times when I had to fight to get my ideas accepted."

MacCollum has authored four industry-related books, along with a novel, *Murder by Electrocution*, published in 2010. In addition, he has published more than 400 articles and has written for numerous industry-related newsletters.

David MacCollum and his wife of 61 years, Nancy, are longtime Sierra Vista residents.

Founded in 1911, the ASSE is the oldest and largest professional safety organization in the world, said Grushka. As a global association of occupational safety professionals, it represents more than 35,000 members worldwide. Through its proactive efforts of creating safer work environments, its members record less lost time and lower workers' compensation costs, increased productivity and higher employee satisfaction.

The BCSP Scholarship Fund was established within with ASSEF to encourage entry into and advancement of the safety profession. For information, go to the American Society of Safety Engineers Foundation website at www.asse.org/foundation.

*Reprinted with permission from*
*The Sierra Vista Herald (http://www.svherald.com/)*

## Central California

The Central California Chapter is in the planning phase for CY '14 field trip options. In addition to its regular support for the Central Coast Science Fair, the Chapter has also been presented with mentoring opportunities through the local American Institute of Aeronautics and Astronautics (AIAA) Chapter, which will help students prepare their science fair projects. Several Chapter members have shown interest in this opportunity.

## Northeast Chapter

The Northeast Chapter held its Fall general meeting on Thursday, October 3, 2013. The topic was "UTAS Space Systems: Approach to Safety through Systems Architecture" by Ben Bishop. Ben is a UTAS Fellow in systems architecture/controls integration, with nearly 45 years of experience in the design and development of complex systems for fluid, power, thermal and data management for DoD, NASA, and the printing and publishing industry.

The Chapter's Winter general meeting was held on Thursday, January 30, 2014. The topic was "Identification of Safety-Critical System, Hardware and Software Requirements Using Fault Trees," by Wes Rainey, MSEE Life Cycle Engineering, General Dynamics Electric Boat. Both meetings were held at the Go Fish Restaurant in Mystic, Connecticut, and were also available virtually for those who couldn't attend in person.

## Sierra High Desert Chapter (SHDC)

Sierra High Desert Chapter members in good standing voted unanimously to approve a motion for the Chapter to fund ISSS membership dues for all of its members for one Society year. The Society year was SY14 for the 11 members who have not renewed their ISSS membership this year and SY15 for the nine members who had already renewed ISSS membership for SY14, which began on July 1, 2013. The motion was made by John Leipper, and was seconded by Ken Chirkis and Jerry Banister.

The Chapter's next meeting is scheduled for May. Membership renewal, Chapter goals and the challenges facing our Society and Chapter will be discussed.

## Tennessee Valley Chapter

On December 11, 2013, 13 members and 16 guests attended the lunch meeting at QinetiQ in Huntsville. Jason's Deli box lunches and drinks were provided by the Chapter. Chapter Vice President Ken Rose presided over the meeting. Brandon Daugherty of Sikorsky presented a paper he authored with Cliff Pariso, manager of system safety at Sikorsky. The presentation was titled "Safety is Not an Option — Sikorsky's Aviation Safety Equipment List (ASEL) Process." ASEL is a method for evaluating and classifying rotorcraft safety-enhancing equipment in terms of impact on safety and various equipment installation factors. Guidance from certifying agency policy and system safety standard practice were considered, resulting in a classification tool that can be used to determine if equipment should be marketed and sold as either mandatory or optional. The methodology that was developed may have applications for other products and industries.

On January 15, 2014, 20 members and nine guests attended the lunch meeting at A-P-T Research in Huntsville, Alabama. Pizza was provided by the Chapter and drinks were provided by A-P-T. Don Swallom opened the meeting by welcoming the attendees. Pam Kniess, chair for the International System Safety Training Symposium 2014 in St. Louis, Missouri, gave an update on planning efforts. Dr. John McDermid of the University of York, U.K., gave a repeat of his presentation to the G-48/A-P-T Research Safety Case Workshop conducted at A-P-T on January 14 and 15, 2014. The presentation was titled "Safety Cases: Purpose, Process and Prospects." This presentation, along with the other workshop presentations and the workshop findings, is located at http://www.apt-research.com/news/newsBlog2014.html.

On January 18, 2014, Don Swallom and Chris Trumble of the Tennessee Valley Chapter served as judges for the System Safety Award at the Alabama Regional Future City Competition at the University of Alabama Huntsville. The Future City Competition is a national, project-based learning experience where students in sixth, seventh and eighth grade imagine, design, and build cities of the future. Students work in teams with an educator and an engineer mentor to plan cities using SimCity™ software, research and write solutions to an engineering problem, build tabletop scale models with recycled materials, and present their ideas before judges at regional competitions. A total of 19 teams competed at the Alabama regional event. The winner of the System Safety Award was the team from the Academy of Science and Foreign Language in Huntsville, Alabama. The team also won the overall competition and will compete at the National Finals in Washington, DC in February.

| | | | |
|---|---|---|---|
| D | Z | N | L |
| A | V | Y | F |
| G | D | P | I |
| Q | N | E | N |
| W | O | R | D |
| R | S | F | M |

## "Name Your Terms"

| | |
|---|---|
| Cases | Marketing |
| Comparison | Names |
| Coverage | News |
| Define | Perspective |
| Education | Public |
| Emergency | Reports |
| Investigation | Terms |

**(Answers on page 43)**

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M | E | L | E | A | I | W | A | S | T | S | U | B | S | E | C | E | T | A | F | U | S | R |
| E | A | O | D | T | H | F | O | P | A | R | D | O | Z | T | L | B | D | E | F | T | J | U |
| R | W | R | B | C | A | T | I | E | N | A | M | E | S | K | A | A | W | S | L | S | U | O |
| E | T | Z | C | J | N | Z | A | L | S | K | F | L | A | H | S | C | E | O | I | G | F | H |
| F | F | B | W | A | C | L | A | S | P | A | S | R | E | M | E | E | O | T | E | R | M | S |
| R | S | U | Y | Y | E | T | Y | B | E | A | L | A | E | F | T | C | A | E | D | P | Y | T |
| E | N | E | C | S | I | X | N | E | T | I | N | I | N | U | T | E | N | I | F | E | D | H |
| A | T | C | N | E | M | N | O | A | O | O | U | T | T | K | O | U | T | G | K | L | I | N |
| R | T | O | E | T | R | E | I | P | I | M | N | I | F | A | H | C | A | N | T | F | O | G |
| P | E | A | G | S | O | V | T | T | E | R | E | O | U | L | F | A | T | I | E | N | N | O |
| N | O | D | R | S | S | E | A | P | R | N | E | W | S | S | N | M | E | T | G | Y | T | O |
| A | P | P | E | I | O | C | G | E | A | E | O | L | S | I | E | L | L | E | N | E | E | L |
| T | N | A | M | N | U | P | I | X | T | K | V | E | T | R | R | C | A | K | I | T | M | J |
| I | S | R | E | D | M | K | T | I | K | I | S | A | F | A | Z | A | T | R | U | T | E | K |
| H | I | T | E | P | R | A | S | T | S | A | E | L | D | S | P | E | P | A | N | I | M | G |
| C | K | O | I | M | A | Y | E | G | C | O | O | G | R | E | L | R | H | M | W | L | V | A |
| T | E | N | D | L | H | I | V | O | D | A | R | M | A | V | O | B | A | A | O | N | N | C |
| I | R | S | P | O | A | S | N | I | B | O | S | A | L | D | C | G | P | L | D | C | C | U |
| H | S | U | E | R | Y | S | I | E | R | B | T | A | O | A | O | N | F | L | I | E | I | F |
| N | E | P | N | S | T | S | K | A | K | O | Y | W | N | N | E | I | R | E | N | G | L | C |
| A | R | E | W | R | U | A | C | I | P | E | G | A | R | E | V | O | C | H | L | Y | B | S |
| M | L | L | O | U | D | I | E | S | O | N | A | D | F | R | F | I | H | E | K | R | U | A |
| S | D | P | P | N | F | B | L | R | T | G | E | R | N | E | E | N | S | D | B | E | P | I |
| F | E | R | J | O | I | M | N | H | V | Y | E | V | I | T | C | E | P | S | R | E | P | T |
| R | S | I | T | C | A | L | S | S | E | W | A | K | I | W | A | Y | E | A | S | M | E | E |

# System Safety Bookshelf

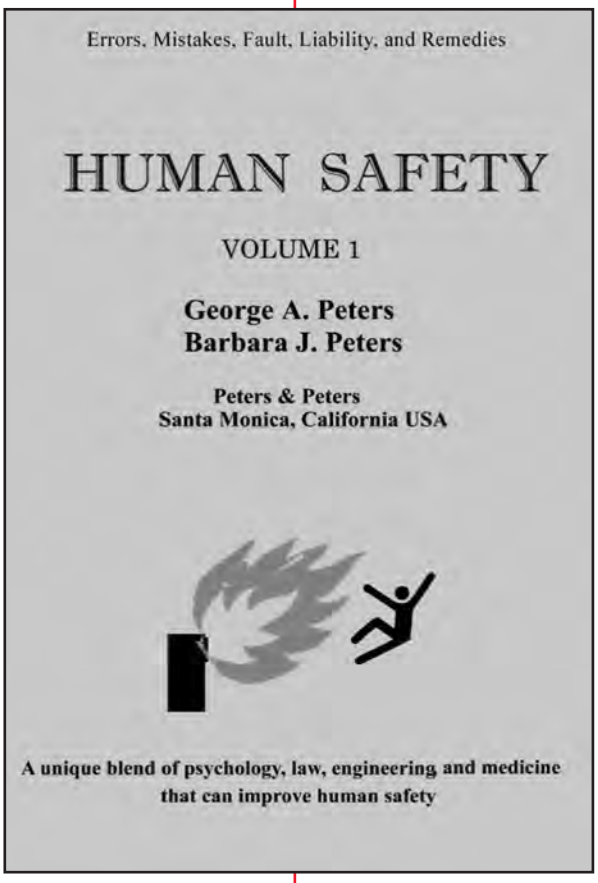
## A Deep Dive Into Safety Questions

***Human Safety (Vol. 1 & 2)***

**By George A. Peters and Barbara J. Peters**
**Publisher: CreateSpace**

**Volume 1**
**ISBN-10: 1490564454**
**ISBN-13: 978-1490564456**
**504 pages**
**Price: $36.00**

**Volume 2**
**ISBN-10: 1490567046**
**ISBN-13: 978-1490567044**
**498 pages**
**Price: $36.00**




George and Barbara Peters, the authors of *Human Safety*, have published a unique and useful system safety book. Their approach considers the entire realm of systems and industries, and serves as a reference guide that would fit nicely on your office bookshelf. This two-volume series also provides insight into the legal aspects of system and human factors engineering, hazard identification and mitigation, along with the human aspect to accidents that include human cognizance, memory, tiredness and communication.

The knowledge required to adequately perform system safety in our ever-evolving world is almost overwhelming. The authors provide pithy explanations of almost every safety and human factor topic, concern or hazard, with each and every reader of *Human Safety* coming away enriched and better prepared to meet their responsibilities as system safety professionals. The authors use accident examples to drive their respect points home in a succinct, unambiguous and useable manner. This book also provides checklists to ensure that every detail is considered in the performance of analyses. In summary, *Human Safety* is a must-read that will surely enrich your job and career. I believe *Human Safety* will earn a permanent and predominant position in your reference library.

**— Warren Naylor**

At last, a book has been written that addresses the many design safety questions that plague managers, designers and safety engineers. The latest book by George and Barbara Peters, titled *Human Safety*, contains a plethora of useful design safety information not found elsewhere. This book covers diverse topics, such as lasers, fatigue and toxic chemicals, along with many others. It analyzes and discusses past mishaps such as Bhopal, Deepwater Horizon and Fukushima.

The topics are so broad the book comes in two volumes. It has an extensive design safety checklist, healthcare safety checklist and a school safety checklist. This book not only addresses errors, faults and liability, but it also provides design safety remedies. And, the topics addressed are very diverse; for example, I had no idea that hair graft operations can result in brain damage if not properly performed. This book is highly recommended reading and should be on every designer's and safety engineer's bookshelf for reference. Don't be intimidated by the title; this book covers all aspects of the design safety of systems involving humans.

**— Clifton Ericson**

# Notes on Society History

*by Rex B. Gordon*
*ISSS Historian*

## Historical Note No. 1: The Founding of the Society

The event recognized as the founding of the Society occurred on December 4, 1963 in the main lecture hall at the School of Aviation Safety on the University of Southern California campus in Los Angeles. The gathering consisted of about 40 individuals, including many students and others from the USAF Aerospace Safety Center, some USC faculty members, along with system safety representatives of the numerous aerospace companies located in the area. They had been invited by current technical lead of the USC Aviation Safety School, C.O. (Chuck) Miller. He presented the current scope and purposes of the USC program, which had been contracted by the Air Force. It was designed for those currently in, or being assigned to, aerospace project safety positions, and was intended to better equip them to manage the implementation of the system safety engineering requirement of recently released MIL-S-38130 (now known as MIL-STD-882), stipulating implementation of system safety programs on Air Force aerospace/missile programs.

*Presentation of certificate of appreciation commemorating the 50th anniversary of the Charter Meeting of the Society. From left: Tom Anthony, Roger Lockwood, Francis McDougall, and Dr. Najm Meshkati*

Following Miller's presentation, Roger Lockwood, a member of the school's faculty, advised the gathering that he had obtained a state of California charter for a technical, non-profit organization to be known as the "Aerospace System Safety Society." With himself named as president, he invited any of those present who wished to pay a $2 member fee to become members. Lockwood maintained detailed records of those paying the initial and subsequent dues, thus identifying those 10 who both signed the charter member roll and paid the $2, and can be rightfully recognized as "Charter members of the Society." Within several months, a total of 30 members had paid their dues, (which had been quickly raised to $5 per year by a vote of the Charter members).

These 30 initial members noted here include 10 Charter members, nine past Society presidents and seven past chapter chairmen/presidents. As will be addressed in subsequent notes, the name of the Society has progressed from the Aerospace System Safety Society (ASSS) to the System Safety Society (SSS) to, currently, the International

Editor's Note — "Historical Notes" is a new series of articles that will be presented periodically in *Journal of System Safety*. These notes will provide members with a better appreciation of the Society's origins, trailblazing pioneers and critical events, as well as the opportunity for colleagues to critique and improve on the scope and historical accuracy of these notes. It is intended that when complete, these peer-reviewed notes will serve as a valid resource in the development of the *Official History of the Society*.

These notes will address the founding of the Society, and then cover its ever-expanding role in the promotion of the system safety concept, both in the U.S. and internationally. They will highlight key events and members who played critical roles in this expansion. These notes will further provide a timeline of key historical events — proceeding from the tenuous beginnings through to its current days.

System Safety Society (ISSS). These name changes offers an illustration of the expanding scope of the practice of system safety — from its aerospace origins in Los Angeles to a multitude of world-wide applications.

On December 7, 2013, in commemoration of the 50th anniversary of the Charter meeting of the Society, the Southern California Chapter presented a plaque to the current director of USC aviation safety programs, to be hung in the school's lobby. This presentation occurred during a Chapter luncheon held in Los Angeles. This "Declaration of Appreciation" identifies five key individuals who uniquely contributed the necessary elements leading to the Charter meeting of the Society. Subsequent "notes" will expand on the roles of these and other system safety pioneers, along with the necessary elements leading to the formation of the Society.

The honored guests at this 50th commemoration celebration were Founder and initial President Roger Lockwood and fellow Charter Member Rex Gordon. Joining Chapter President Francis McDougall and other Chapter members was Thomas Anthony, aviation safety program director and other USC faculty. The meeting culminated in the presentation of the Certificate of Appreciation by Francis McDougall and Roger Lockwood to USC's Tom Anthony and Dr. Najm Meshkati.

*Comments on the accuracy of these notes on the History of the Society should by addressed to Rex Gordon at rexbg@aol.com.*

| Original Members of the Society | |
|---|---|
| Sam Canale § | Edgar Mendenhall |
| • Edgar Cecawicz | • Chuck Miller ‡ § |
| Niel Classon ‡ § | Julius Morris |
| Gerald Couch | • George Peters ‡ |
| Alfred Dallman | Rolland Ratz |
| Saxe Dobrin | Herbert Robb |
| Elwood Driver ‡ § | Douglas Robinson |
| Gus Economy | • William Rogers |
| • Rex Gordon ‡ § | George Ruff § |
| • Willie Hammer | Leo Shroeder |
| • George Haviland ‡ | Albert Sternberger |
| Everett Hodapp | Lynn Stone |
| • Norman Horton | Gordon Willard ‡ § |
| Richard Kohlheyer ‡ | Ernest Zellerman |
| • Roger Lockwood ‡ | • James Zurn |

• - Charter Society Member
‡ - Past Society President
§ - Past Chapter President

## The System Safety Concept — Origins

*For almost any system, product or service, the most effective means of limiting product liability and accident risk is to implement an organized system safety function beginning in the conceptual design phase and continuing through to its development, fabrication, testing, production, use and ultimate disposal.*

While it can be argued that ancient and common laws, making the builder responsible for harm caused by faulty products, form the original basis of the SSC, addressed here in these notes is the direct antecedent of the current practice of system safety.

The initial formal documentations of what is generally recognized as the SSC are traditionally traced back to a technical paper presented by a Boeing engineering manager, Amos L. Wood, at the January, 1946 annual meeting of the Institute of Aeronautical Sciences (ISA) in New York. This paper addressed the importance of a manufacturer's organizational structure to incorporate a focus on safety from design through post-accident analysis. It was titled "The Organization of an Aircraft Manufacturer's Air Safety Program."

Some eight months later, in September 1946, a technical paper presented by William Stieglitz, an aeronautical engineer, at a special ISA meeting provided additional far-sighted views on the SSC. These included the following quotations:

> "Safety must be designed and built into airplanes, just as are performance, stability, and structural integrity."

> "Safety is a specialized subject just as are aerodynamics and structures."

> "A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or a weights group…"

Thus, we can see that while at least in the aviation industry, key elements of the SSC were being formally discussed by forward-thinking leaders as early as 1946, there was as yet little detectable change in the majority of traditional technical methods.

# *Exxon Valdez*: Human Error, Plain and Simple

*by Arthur D. Barondes, Alexandria, Virginia*

Much has been made of the *Exxon Valdez* going aground on Bligh Reef in Prince William Sound in 1989 — and rightfully so. The effects of the disaster continue to this day. Why the *Exxon Valdez* went aground is straightforward, although not widely well understood. As can be expected, various interests seized upon the catastrophe to support their causes or improve their lots. Whereas it is now clear that the ship went aground purely as a consequence of human errors — there were no mechanical or electrical failures — the event has been used to justify changes that, while desirable, would not have prevented the *Exxon Valdez* from going aground, or the subsequent oil spill. Those changes include, inter alia, a variety of improved navigational aids, expanded Coast Guard monitoring capabilities, increased requirements for harbor pilots and required crew rest. In looking back, one might be led to believe that the ship went aground in a sea of red herrings. This article reviews what really happened on that night and incontrovertible evidence that supports human errors — onboard the *Exxon Valdez* and thousands of miles away at the Exxon Shipping Company — in a failed safety culture as solely responsible for the disaster.

## Introduction

Most of you have at least heard of the *Exxon Valdez* disaster. You probably remember it as a tanker that went aground in Alaska and spilled 11 million gallons of crude oil into natural habitats. Some of you might even remember that the ship's captain was accused of being intoxicated and driving the ship aground. Those who followed the story of the *Exxon Valdez* might also recall some of the wide array of offered explanations, as well as the recommended corrective "fixes." There is some truth to such recollections. The *Exxon Valdez* certainly did go aground and spill a huge quantity of crude oil. But the story of why it went aground is now quite clear. Equally clear is the inability of those recommended fixes to have had any effect on preventing the accident. This is that story.

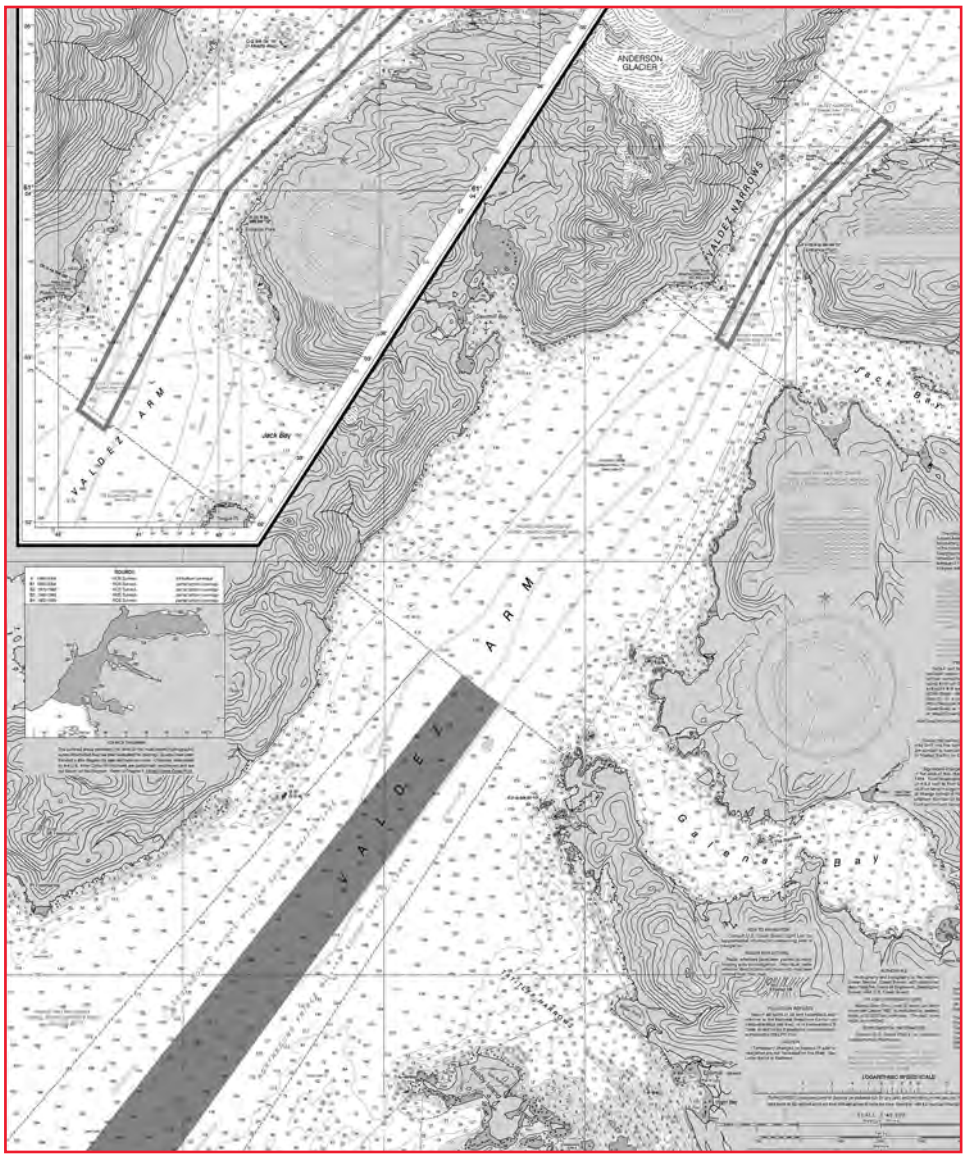
We begin with a brief description of what is supposed to happen, i.e., normal tanker operations in Valdez Bay and Prince William Sound. We follow that with a description of what *actually* happened on that fateful night in March, 1989. That description pinpoints the immediate causes of the ship going aground — all of them human failures. Then, we examine the array of recommended fixes and identify why each one would not have prevented the accident. Finally, we show that the accident was solely the consequence of human failures in an inadequate safety culture. We assert that the accident would not have occurred if the *Exxon Valdez* crew and Exxon Shipping Co. management had complied with established and published human performance procedures.


*Figure 1* — Exxon Valdez.

## Routine Valdez Tanker Operations

Valdez is a small town (population ~4,000) some 120 miles east of Anchorage, Alaska. As shown in the nautical charts in Figure 2, Valdez is located on the northeast side of Valdez Bay. It is the only cultural center on the Bay. On the south side of the Bay, the Alyeska Marine Terminal is used to store crude oil piped from the Alaska North Shore and transship it to seagoing tankers. On average, two loaded tankers sail from Valdez every day. In the 12 years before the *Exxon Valdez* accident, there had been nearly 9,000 tanker sailings without a single oil spill from going aground.

Tankers sailing from the Alyeska Terminal follow a controlled route. They proceed into Valdez Bay, navigate through the Valdez Narrows into the Valdez Arm of Prince William Sound (Figure 2), and then into sea lanes to their off-loading destinations: Panama, Los Angeles or San Francisco. The Coast Guard Vessel Tracking Center (VTC)/Marine Safety Office (MSO) controls and monitors traffic in the Bay, and controls the inbound and outbound traffic lanes in the Traffic Separation Scheme (TSS) in the Valdez Arm of Prince William Sound to




NOAA Graphic

*Figure 2 — Valdez Bay and Prince William Sound*

within about six miles of Valdez Narrows (the entrance to Valdez Bay and Port Valdez). The traffic lanes are almost a mile wide in most of the Sound, but gradually decrease to 3,000 feet approaching the Narrows. In 1989, a harbor pilot was required to steer ships in the Bay and through the Narrows. The ship's master is required to be on the bridge with the pilot, as well as when navigating in coastal waters, e.g., the Valdez Arm of Prince William Sound. By and large, such tanker operations are uneventful, with the primary hazard to navigation being small to moderate-size icebergs drifting south from Columbia Glacier into the outgoing lane, but also into the incoming lane of the TSS.

## What Happened on the Night of March 23, 1989

The sequence of events leading to *Exxon Valdez* going aground has been documented by the National Transportation Safety Board (NTSB) Marine Accident Report [Ref. 1]. The ship arrived at Valdez at 11:35 p.m. on March 22, docked at the Alyeska oil loading terminal and prepared to load 1.25 million barrels of crude oil [Ref. 1]. With the ship loaded on March 23, the third mate completed the testing of all required navigation equipment and found it operating properly. The ship departed the terminal at 9:12 p.m. that evening — an hour earlier than originally planned. The master was on the bridge with the chief mate, the helmsman and the required State harbor pilot. As the ship departed under the control of the harbor pilot, the third mate relieved the chief mate, and the master — contrary to regulations — left the bridge. The master did not re-appear until requested by the pilot after clearing the Narrows, putting the ship on its outbound course of 219° (all headings are True) and preparing to disembark. At 11:25 p.m., the master, in control of the ship, reported his position to the Coast Guard VTC. He advised that he was proceeding in the outbound lane of the Traffic Separation Scheme (TSS), with the ship's speed programmed to accelerate from the Narrows' speed limit of 6 knots (7 mph) to "sea speed" of 16.25 knots (18.8 mph) — a procedure that would take about 43 minutes, i.e., until about 1:08 a.m. on March 24.

As the *Exxon Valdez* continued into the Valdez Arm of Prince William Sound, this 45-minute critical chain of events evolved:

**11:25 p.m.:** The Coast Guard watchstander at the Valdez Marine Safety Office (MSO) requested a report on ice conditions in the channel. The master responded in a slurred voice, "Okay. I was just about to tell you that, ah, judging by our radar, I we'll probably divert from, ah, the TSS and end up in the, ah, inbound lane if there's no conflicting traffic." The watchstander confirmed that the inbound channel would be free of traffic, to which, the master responded, "That will be fine. Yeah. We may end up over in the, ah, inbound lane, outbound transit. Ah, we'll notify you when we leave the, ah,

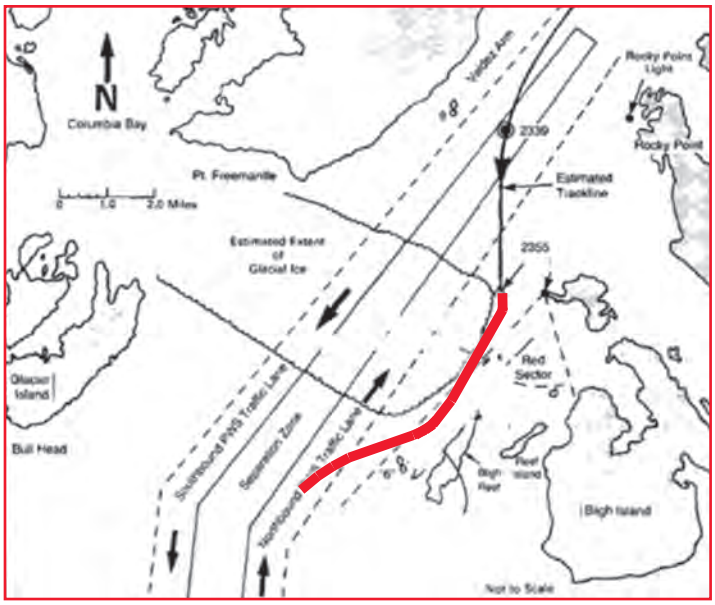



*Figure 3 — Master's Planned Course*

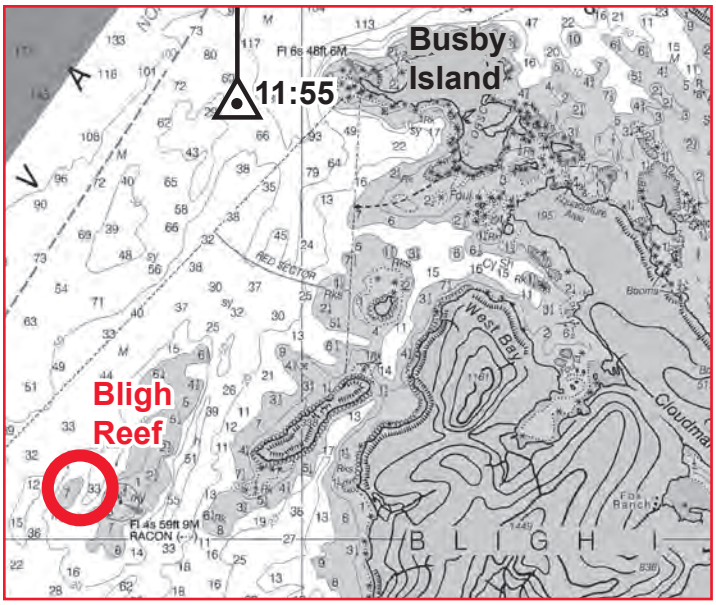



*Figure 4 —* Exxon Valdez *abeam.*

TSS and, and, ah cross over the separation zone." (Note: Coast Guard approved deviations from the established TSS lanes were common practice to avoid ice.)

**11:31 p.m.:** The master directs the helmsman to come port (left) to 200° and advises the Coast Guard watchstander, "I'm going to alter my course to 200° and reduce speed to about 12 knots to, ah, wind my way through the ice…." However, the master does not change the activated ship speed program to increase to sea speed (16.25 knots, 18.8 mph).

**11:36 p.m.:** The master directs the third mate, who has just returned from assisting the pilot off the ship, to take a fix of the ship's position. He tells the third mate that he will move the ship more quickly across the TSS by bringing it farther port (left) to 180° — due south — to skirt the ice (Figure 3). The third mate takes his fix with a visual bearing on Busby Light and radar range.

**11:39 p.m.:** The fix shows the ship to be in the separation channel.

**11:43 p.m.:** The ship is steady on a course of 180°. As directed by the master, the helmsman engages the autopilot. Changeover to the 0000-0400 watch is about to start with the master, the second mate and a new helmsman on the bridge. The master authorizes the oncoming forward lookout (who has a cold) to take her post on the starboard (right) wing of the bridge.

**11:50 p.m.:** The helm watch changes with the ship steady on 180° and on autopilot. (Note: Policy prohibits the use of the autopilot when navigating in the traffic lanes.) The master advises the third mate that he will be leaving the bridge "to do paperwork." He instructs the third mate to turn the ship back to the traffic lanes when abeam Busby Light and to advise him that he has started the turn. He asks the third mate if he feels "comfortable" with what he is to do. (Note: As shown in Figure 3, the master has the ship crossing the TSS inbound lane rather than entering it as approved by the Coast Guard.) The third mate, who is not certified to control the ship in coastal operations, decides to remain on watch until the vessel has cleared the ice and not call his relief, the second mate, who is scheduled to come on watch at 11:50.

**11:52 p.m.:** The master leaves the bridge. (Note: The Exxon Shipping Company "Bridge Organization Manual," requires that either the master or the chief mate be on the bridge in charge of the watch when arriving or leaving port or in congested waters.) The third mate, expecting to alter course, takes the ship off autopilot. This is observed by the helmsman.

**11:55 p.m.:** The ship is abeam Busby Light — three minutes after the unauthorized departure of the master. As the third mate is plotting the fix (Figure 4), the lookout advises him that the red light of Bligh Reef is to starboard (right). (Note: A red mark to starboard when leaving port is cause for concern, but with the ship deliberately heading due south across the TSS, the red light of Bligh Reef should have been to starboard.)

**11:56 p.m.:** One minute late, the third mate orders, "Ten degrees starboard (right) rudder." In a crucial oversight, he fails to check the rudder indicator on the bridge. After ordering the right rudder, he telephones the master as directed and informs him that he has started to turn the vessel back toward the traffic lanes. The master asks if the second mate is on the bridge. He tells him that the second mate has not been called. The ship is still building to "sea speed."

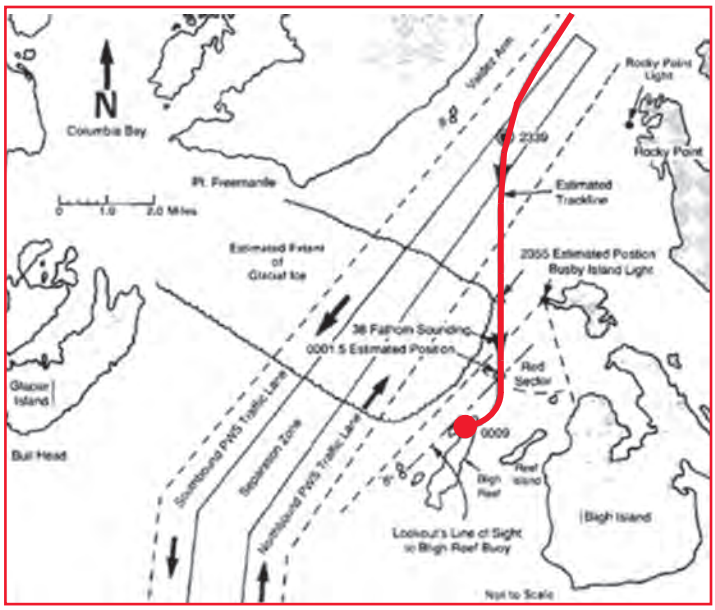



*Figure 5 — Track of the* Exxon Valdez.

**11:57 p.m.:** Off the phone, the third mate goes to the port radar and takes radar ranges from Bligh Reef buoy and Reef Island, which he has in sight, to determine the ship's change in course. There is none. (Note: Large ships, such as the 214,861-deadweight-ton *Exxon Valdez*, have large steering time constants, i.e., they respond slowly to rudder inputs.)

**11:59 p.m.:** Now four minutes late, the third mate orders, "20 degrees right rudder." He checks the ship's rudder indicator to confirm the change. He notes that the ship is not yet in the "red sector" of Busby Light (Figure 4).

**00:01½ a.m.:** The ship starts to turn.

**00:02 a.m.:** The third mate calls for "hard right rudder." The helmsman complies.

**00:04 a.m.:** The third mate telephones the master and says, "I think we are in serious trouble."

**00.05 a.m.:** As the telephone conversation is completed, the third mate feels the vessel contact the bottom. The ship speed is about 14 knots (~16 mph) with ~3E9 ft lb of kinetic energy being dissipated.

**00:09 a.m.:** The ship is aground on Bligh Reef (Figure 5).

**00:27 a.m.:** Eighteen minutes after going aground, the master advises the Coast Guard Vessel Traffic Control (VTC): "Yeah. Ah, it's *Valdez* back. Ah, we've — ah, should be on your radar there — we've fetched up, ah, hard aground north of, ah, Goose Island off Bligh Reef. And, ah, evidently, ah, leaking some oil, and, ah, we're gonna be here for a while. And, ah, if you want, ah, so you're notified."

The *Exxon Valdez* story continues to play out, surfacing important issues, such as containing the oil spill, getting the ship off the reef and minimizing the environmental impact. But those issues are irrelevant in determining why the ship went aground on Bligh Reef and what actions would prevent other ships from facing a similar fate. Those actions — recommended and adopted — are the subject of the next section. But, before addressing them, it is important to note from the foregoing description of events that:

- The *Exxon Valdez* had no mechanical or electrical failures
- The ship had a complete suite of navigational equipment (Table 1)
- There were no failures with Coast Guard navigational aids
- The ship responded properly to the orders it received
- The master and, subsequently, the third mate, knew exactly where the ship was at all times
- Failure to execute the rudder order at 11:55 sealed the fate of the *Exxon Valdez*.

*Table 1 — Navigation Suite.*

| |
|---|
| Ship Control Center<br>Sperry SRP-2000 |
| RADAR<br>Raytheon RAYCAS V S-band<br>(out of commission)<br>Raytheon X-band (2) |
| LORAN C |
| VLF Omega |
| NavSat (Transit) |
| GPS |

*Figure 6 —* Exxon Valdez *aground.*

## Explanations and Fixes

There has been no shortage of claims made to explain the *Exxon Valdez* going aground (Figure 6). Those claims — offered by various interests and sources ostensibly to prevent a recurrence of ships going aground in the Valdez Arm of Prince William Sound — have led to a variety of proposed, and oft-adopted, fixes. For the most part, these so-called fixes neglect to recognize that the *Exxon Valdez* went aground because of a series of strictly human failures. Worse, they were predominantly a failed safety culture that tolerated deliberate failures to adhere to established policies and procedures. It was not because of mechanical or electrical failures or shortcomings in Coast Guard navigational aids and supervision.

Some claims are based on assertions that are *demonstrably false*. As an example, "The captain was confirmed to be asleep when the ship crashed in Prince William Sound's reef" [Ref. 2]. Note that the third mate was on the phone with the master twice (11:56 p.m. and 00:04 a.m.) in the 10-minute period before the initial impact at 00:05 a.m. Many other offerings simply miss the point. In that context they are, in effect, red herrings in Prince William Sound. Specific examples include:

"There has been no shortage of claims made to explain the *Exxon Valdez* going aground.... Those claims — offered by various interests and sources ostensibly to prevent a recurrence of ships going aground in the Valdez Arm of Prince William Sound — have led to a variety of proposed, and oft-adopted, fixes. For the most part, these so-called fixes neglect to recognize that the *Exxon Valdez* went aground because of a series of strictly human failures."

**The RAYCAS V Radar —** Much has been made of the failure of the Exxon Shipping Co. to maintain the ship's advanced Raytheon Collision Avoidance System (RAYCAS) radar. One popular, but implausible, claim asserted that the radar "if functional, would have indicated to the third mate an impending collision with the Bligh Reef by detecting the 'radar reflector' placed on the next rock inland from Bligh Reef for the purpose of keeping boats on course via radar" [Ref. 3]. In another, "the radar system would have detected the 'radar reflector,' placed on the next rock inland from Bligh Reef for the purpose of keeping boats on course via radar" [Ref. 4]. In still another, "At the helm, the third mate would never have collided with Bligh Reef had he looked at his RAYCAS radar. But the radar was not turned on. In fact, the tanker's radar was left broken and disabled for more than a year before the disaster, and Exxon management knew it. It was just too expensive to fix and operate" [Ref. 5].

Whereas the RAYCAS V was a technologically advanced maritime radar system, it was not part of the suite of "minimum essential equipment" necessary to comply with the safety requirement for two operating radars. The RAYCAS V capability to "paint" the Bligh Reef corner reflector was not unique. As described earlier, at 11:57, the third mate had the light of the Bligh Reef mark in sight and was using a less-sophisticated RAYCAS radar (the port-side radar) to take range and bearing fixes. Whereas it could be argued that the RAYCAS V would have been more capable, that was not an issue: The position of the *Exxon Valdez* was never in doubt.

**The Coast Guard —** In a report addressing the Valdez accident, the Coast Guard enumerated the the changes required of it by the Oil Pollution Act (OPA) passed by Congress in 1990: "To strengthen (the Coast Guard's) regulations on oil tankers and their owners and operators. Today, tank hulls are specially designed to provide maximum protection against oil spills. Communications between vessel captains and vessel traffic centers have improved for safer sailing. In addition, the Coast Guard implemented stronger regulations on vessel traffic:

- The addition of three people at the Coast Guard's Vessel Traffic Service (VTS) to provide additional watchstanders round the clock
- The close monitoring of fully laden tankers by satellite as they pass through Valdez Narrows and exit Prince William Sound. In 1989, only Valdez Narrows and Valdez Arms were watched. [Note: The Coast Guard had two remote radar sites: one adjacent to its Valdez office and one at Potato Point (southwest end of the Narrows).]
- The continuous plotting of progress of all tankers in the Valdez channel
- The improvement of foul weather surveillance [sic] capability with the installation of an all-weather radar system….

- The erection of a major lighted aid to navigation at Bligh Reef" [Ref. 6].

Regarding the marker at Bligh Reef, one source [Ref. 7] went so far as to claim erroneously, "The *Exxon Valdez* ended up on Bligh Reef because they did not follow the correct route and did not see the warning markers."

While improved markers are desirable, they and the other improvements cited here — if present when the *Exxon Valdez* went aground — would not have prevented the accident. True, the position and course of the *Exxon Valdez* were not known to the Coast Guard VTC as the accident was playing out. But both the position and course were well known to the master until he left the bridge three minutes before the critical course alteration was to be made. As detailed in the NTSB Marine Accident Report [Ref. 8], the third mate, in control after the master departed, knew the position of the ship throughout its progress to Bligh Reef. In fact, the third mate was consumed with position fixing to the neglect of steering the ship and controlling its speed.

**The MIT Analysis —** A group at MIT examined the *Exxon Valdez* accident as part of "A New Approach to System Safety Engineering" [Ref. 9], wherein the thrust was to design safety into systems so as to preclude accidents. Whereas their approach is admirable, the use of the *Exxon Valdez* as a case in point — including questioning the culpability of the master — is not. Using the catch question, "Was he [the master] to 'blame'?" the "New Approach" identifies eight dubious causative factors that "spread the blame" and reduce the key role of human failures:

- "State-of-the-art iceberg monitoring equipment promised by oil industry, but never installed." This could be true, but it is not a causative factor unless the argument is made that the *Exxon Valdez* altered course on the basis of non-existent ice. But, there is no evidence to support that. Hazardous ice buildups from calving glaciers are common occurrences in Prince William Sound and, as on this occasion, appeared on ship's radar. A common practice, endorsed by the Coast Guard, was to steer around such build-ups, as was being done by the *Exxon Valdez* and other ships that day.
- "Radar station in city of Valdez, which was responsible for monitoring the location of tanker traffic in Prince William Sound, had replaced its radar with much less powerful equipment. Location of tankers near Bligh Reef could not be monitored with this equipment." The Coast Guard Valdez Marine Office of Safety (MOS) was primarily concerned with ships in the Valdez Arm near the Narrows, the Valdez Narrows and Valdez Bay. It provided tracking information out into the Valdez Arm and Prince William Sound as a service — not a requirement. That night, the Coast Guard watchstander had the Valdez Arm radar (at Potato Point) set on short range and was not tracking the *Exxon Valdez*. When the *Exxon Valdez* was reported aground, the watchstander set the radar to long range and immediately detected the ship (albeit now broadside to the radar). It could be argued that had the Coast Guard been tracking the *Exxon Valdez*, it could have warned that it was on a dangerous course, but the master knowingly set the ship on that course and the Coast Guard knew he had turned south. The ship's course became unrecoverable when the third mate failed to make the ordered turn. Again, it is important to note that the position of the *Exxon Valdez* was not in doubt.
- "Congressional approval of Alaska oil pipeline and tanker transport network included an agreement by oil corporations to build and use double-hulled tankers. *Exxon Valdez* did not have a double hull." Clearly, except to the extent that it affects the draft, the hull construction of the ship is irrelevant to going aground. Even so, the maximum vertical damage penetration measured…was 10.9 feet in two locations [with] transverse frames…deformed upward from 8 to 15 feet…. thus, minor leakage probably could still have occurred…. [But,] any outflow would have been expected to be considerably slower if the vessel had had a double bottom…" [Ref. 10]. The double-hull issue is another red herring when examining why the *Exxon Valdez* went aground.
- "Crew fatigue was typical on tankers. Crews routinely worked 12- to 14-hour shifts, plus extensive overtime." Although difficult to measure, various degrees of crew fatigue can be inferred from their on-duty time and sleep history. Long shifts for some crew members were characteristic of loading and unloading the ship, but not during the longer periods at sea. Normal watches underway were four hours on, eight hours off. There is no evidence that the master was suffering from overwork or sleep deprivation. Conversely, the *unqualified* third mate, who was in control of the ship by virtue of a human failure by the master, was judged by the

accident investigation board to have been impaired by "fatigue and excessive workload," even though he made the decision not to be relieved by the rested and qualified second mate. The malassignment of personnel on the bridge was magnified by the change in departure time (9:00 p.m. rather than 10:00 p.m.) that put the ship in the critical Bligh Reef region during watch changeover (11:50 p.m.) rather than an hour into the second mate's watch (00:00 a.m. to 04:00 a.m.).

- "Coast Guard at Valdez assigned to conduct safety inspection of tankers. It did not perform these inspections. Its staff had been cut by one-third." There is no evidence that the *Exxon Valdez*, before or after the accident, had any safety deficiencies. Another red herring: As attested by the harbor pilot, the third mate's inspection and the accident investigation, all required systems were functioning properly.
- "Tanker crews relied on the Coast Guard to plot their position continually. Coast Guard operating manual required this. Practice of tracking ships all the way out to Bligh Reef had been discontinued. Tanker crews were never informed of the change." This is simply a misconception. The crew of the *Exxon Valdez* did not rely on the Coast Guard to plot its position. The mate on watch had the responsibility of plotting the ship's position. Further, the position of the *Exxon Valdez* was never in doubt. (Note: The *Exxon Valdez* also had Global Positioning Satellite (GPS) capability, but there is no reference to it being used.)
- "Spill response teams and equipment were not readily available. Seriously impaired attempts to contain and recover spilled oil." Whereas this is true, it actually has no bearing on the *Exxon Valdez* going aground.
- "[The master] was tried for being drunk the night the *Exxon Valdez* went aground. He was found 'not guilty.'" This is true, but the implication that he was not impaired by alcohol is not. Through a series of glitches, the blood alcohol sample was not taken until some 10 hours after the accident. Although the alcohol content was unacceptably high, the master's lawyer successfully argued that those results could be attributable to alcohol consumed by the master after the traumatic accident — notwithstanding that alcohol was not permitted aboard the ship. An in-depth, but not conclusive, frequency analysis of the master's speech [Ref. 11], recorded by the Coast Guard *before* the accident (see previous examples at 11:25 p.m. and 11:31 p.m.), found it consistent with alcohol impairment. The accident investigation concluded the master was alcohol-impaired at the time of the accident.

## Human Failure, Plain and Simple

A careful review of the facts shows that the *Exxon Valdez* did not go aground because of any mechanical or electrical failures, the absence of Coast Guard oversight or inadequate navigational aids. Rather, it went aground solely because of a series of human failures — primarily failures to comply with established regulations, policies and procedures — starting well before the actual event. The number of human failures is sufficiently large as to require questioning the safety culture in the Exxon Shipping Co. and, in particular, the senior crew of the *Exxon Valdez*. Significant human failures include:

**Human Failure 1 —** Well before the accident, the Exxon Shipping Co. was aware that its master of the *Exxon Valdez* was an alcoholic with a record of "driving under the influence." In accordance with company policy, crew members with an alcoholic dependency are required to complete a rehabilitation program, followed by abstinence. The master did neither. This policy also "prohibits the use, possession, distribution, or sale of drugs and alcohol on company premises…[and forbids] being unfit for duty because of the use of drugs or alcohol…" [Ref. 12]. Further, crew members had reported to company management that the master was drinking and observed him openly drinking in Valdez the day the ship sailed. In effect, the company "looked the other way" and continued him as the master. Had the company human resources and medical departments complied with company policy, there would have been another master onboard the *Exxon Valdez*.

**Human Failure 2 —** Before the *Exxon Valdez* sailed for Valdez, an Exxon seaman reported to Exxon Shipping Co. management personnel that the master was using alcohol. No action was taken.

**Human Failure 3 —** The master is observed by other crew members to be drinking in Valdez before the *Exxon Valdez* sails. No action was taken.

**Human Failure 4 —** The master did not comply with the requirement to be on the bridge as the pilot takes the ship from the Alyeska Terminal into Valdez Bay and through the Valdez Narrows. He saw the pilot off only after the pilot requested his presence.

**Human Failure 5 —** Contrary to standard operating procedures, the master ordered the ship's programmed speed control to achieve Sea Speed (16

knots) in the coastal waters of Prince William Sound. A consequence of this human failure is a higher speed than allowed, greater turning radius and more damage when going aground.

**Human Failure 6 —** In response to Coast Guard approval to use the inbound traffic lane, the master told the Coast Guard that he was altering, heading to 200° to enter the inbound lane of the TSS. He subsequently steered 180° to expedite transit through the separation zone, through the inbound lane and into hazardous waters before his planned turn back onto the outbound heading. He failed to advise the Coast Guard of this change in heading.

**Human Failure 7 —** The master put an unqualified third mate in control of the ship.

**Human Failure 8 —** The master, required to be on the bridge, left the bridge "to do some paperwork" — a scant three minutes before the critical course alteration was to be made.

"Human failures in commission and omission of key actions by the master sealed the fate of the *Exxon Valdez*. Clearly, as required by company policy, he should have been replaced as master until successfully completing an approved rehabilitation program. Was anyone else to blame? Here again, the evidence supports a 'yes.'"

**Human Failure 9 —** The third mate decided he should stay in control of the ship rather than have the scheduled and qualified second mate take control. (Note: If the watch change to the second mate had started as scheduled at 11:50 p.m., the changeover briefing, with the master present, would have covered the rudder change to be made abeam Busby Light at an estimated time of 11:56 p.m.)

**Human Failure 10 —** The third mate and the helmsman, between them, failed to initiate the critical course alteration that would miss Bligh Reef. The third mate, in control, failed to monitor the ship's rudder position.

## Conclusion

To the MIT question, "Was he to blame?" we assert the evidence — as presented here — supports an unarguable "yes." Human failures in commission and omission of key actions by the master sealed the fate of the *Exxon Valdez*. Clearly, as required by company policy, he should have been replaced as master until successfully completing an approved rehabilitation program. Was anyone else to blame? Here again, the evidence supports a "yes." The omission of key actions by the Exxon Shipping Co. to execute its written policy on alcohol and drug use allowed the master to be in a position to make the decisions that led to the *Exxon Valdez* going aground.

As for the third mate, we assert that he bears some responsibility for the accident by not recognizing his limitations. Whereas he claimed to be "comfortable" following the master's orders, we picture him as a relatively inexperienced mate eager to gain experience in controlling the *Exxon Valdez* in coastal waters — a job both he and the master knew was above his "pay grade." We see him making three serious "rookie" mistakes:

First, he neglected to confirm his rudder order by observing the rudder indicator. Whereas it cannot be substantiated with evidence, we see the confusion between the third mate and the helmsman on the use of "hand steering" or autopilot as the key contributor. It appears that the helmsman used the autopilot to put in the 11:56 order for "10 degrees starboard rudder" when the ship was in hand steering mode.

Second, his navigation prowess is at issue. We would argue that considering the criticality of the turn abeam Busby Light, it was another "rookie" mistake to wait until the ship was "abeam Busby Light" to take his fix. A more experienced navigator would dead reckon (DR) ahead from the last fix to the turning point and use that estimated time of arrival (ETA) to have the helmsman put in 10 degrees starboard rudder, or alternatively order the turn on his "mark" when visually abeam Busby Light. This would have saved one or two critical minutes equating to a quarter or a half-mile — perhaps enough for subsequent unintended events to play out and still miss Bligh Reef.

Third, again related to his navigation prowess, at 11:59 p.m. he failed to recognize the potential catastrophic consequences of the ship not turning. He called for a modest "20 degrees starboard rudder" to make up for the missing 10 degrees starboard rudder. Had he called for "hard starboard rudder" as he did three minutes later at 00:02 a.m., the ship would clear Bligh Reef. Also, he failed to slow the ship as it continued its programmed increase in speed and associated growing turning radius.

Whatever the reasons for the accident, it is interesting to note that subsequent simulations showed that had the master's rudder order (10 degrees starboard rudder

when abeam Busby Light) been executed, the *Exxon Valdez* would have missed Bligh Reef and continued on an uneventful trip. The master would have continued his career and no one would have been the wiser — until his next cataclysmic human failure.

The recommended and actually implemented "fixes" have the appearance of enhancing the safety of maritime operations in Prince William Sound. But they would not have prevented what happened to the *Exxon Valdez*. Most of them relate to determining the accurate positions of ships — something not at issue with the *Exxon Valdez*. Hence, the fixes are largely red herrings. Only the use of a pilot all the way to Bligh Reef (essentially removing control from the master) offers any hope of having kept the *Exxon Valdez* off the reef — assuming the pilot does not make cataclysmic human errors.

"The recommended and actually implemented 'fixes' have the appearance of enhancing the safety of maritime operations in Prince William Sound. But they would not have prevented what happened to the *Exxon Valdez*."

As a post script, with all the attention on the *Exxon Valdez* and the host of subsequent fixes and "improvements," "a [136-ft] tugboat [drawing only 19 feet and scouting icebergs] …ripped open on Prince William Sound's Bligh Reef in 2009…. [The captain] was unaware of the boat's position when he put it on a crash course with the infamous and well-known navigational hazard…. [The captain] changed the tugboat *Pathfinder's* course, increased its speed and was playing a computer game just before it ran aground…" [Ref. 13]. We would say this was unarguably another human failure, plain and simple. Again, there were no mechanical or electrical failures. Also, there was no doubting the answer to the question: "Was the captain to blame?" Although sober, he and his mate were summarily fired.

So much for the many analyses of the infamous *Exxon Valdez* going aground and the so-called fixes subsequently introduced a decade ago.

## About the Author

Arthur Barondes, a principal at AIC, has developed, conducted and peer-reviewed probabilistic QRAs for 22 years. He worked on the "DoD/DOE Transportation Safety Study," developed the Weapon System Safety Assessment (WSSA) methodology for nuclear weapon systems, and led the peer-review teams for subsequent WSSAs and for the DDESB-requested SAFER program review. Earlier experience includes 11 years supporting the Defense Nuclear Agency "Theater Nuclear Forces Improvement Program" in Europe and 27 years in the Air Force, including command of a Minuteman III ICBM wing, and experimental flight test of Air Force and Navy air-to-air missile systems. He is a rated Master Navigator with 4,500 flying hours. He has a BS from the U.S. Military Academy, an MS(Aero) from the University of Michigan, an MBA from George Washington University and did his doctoral work at American University. He is a distinguished graduate of the National War College.

## References

1. National Transportation Safety Board (NTSB), Marine Accident Report: *Grounding of the U.S. Tankship* Exxon Valdez *on Bligh Reef, Prince William Sound near Valdez, Alaska March 24, 1989*, PB90-916405, NTSB/MAR-90/04, Washington, DC:, Office of Surface Transportation Safety, 1990.
2. http://www.solarnavigator.net/boats/exxon_valdez.htm
3. Ibid.
4. http://en.wikipedia.org/wiki/Greg_Palast#Exxon_Valdez
5. http://www.gregpalast.com/court-rewards-exxon-for-valdez-oil-spill/
6. Hq USCG, *The Coast Guard's Role in the* EXXON VALDEZ *Incident*, Historian Office, Washington, DC http://www.uscg.mil/history/articles/EV.pdf
7. http://answers.yahoo.com/question/index?qid=20080109150820AAyLbG3
8. NTSB, op. cit.
9. Levinson, N.G., *A New Approach to System Safety Engineering*, MIT, August 2006.
10. NTSB, op. cit., p. 163.
11. USCG, op. cit., Appendix J, "Speech Examination Information," pp. 219-255.
12. Ibid., p. 54.
13. Grove, C., "BLIGH REEF: Lack of crew communication about boat position, course is cited," *Anchorage Daily News*, May 10, 2011. http://www.adn.com/2011/05/10/1855776/report-faults-captain-in-tugboat.html

# Safety Case Workshop

*by Tom Pfitzer, Tom DeLong, Saralyn Dwyer, John Frost, Dave West*
*Huntsville, Alabama*

In January 2013, a two-day Safety Case Workshop was conducted in Huntsville, Alabama under the sponsorship of the SAE International G-48 System Safety Committee and A-P-T Research, Inc. (APT). Attendees from industry, government and academia participated, with several making formal presentations on various safety methods. Industry focus is turning to international pursuits, which involve a broader understanding of different approaches to ensuring safety. The United States has typically used a process-based approach in managing system safety programs, but there is a current movement to use the evidence-based Safety Case approach to validate the safety of systems. At the conclusion of the workshop, participants reached the consensus view that the Safety Case approach merits being accepted among the best world-wide system safety practices.

## Background

During the 2013 International System Safety Conference (ISSC), the SAE International G-48 System Safety Committee[1] accepted an action to investigate the utility of the Safety Case approach in relation to ANSI/GEIA-STD-0010-2009. The Safety Engineering and Analysis Center (SEAC) of A-P-T Research, Inc. (APT) offered to organize and host a workshop for that purpose. The SEAC was formed as a division of APT to support independent studies and risk assessments with special capabilities in safety. Leaders in the field were invited to present at the workshop, and a panel was selected. Moderated by John Frost, the panel's presenters included Dave West, SAIC; Don Swallom, U.S. Army Aviation and Missile Command (AMCOM); John McDermid, professor of software engineering at the University of York, U.K.; Barry Hendrix, Lockheed Martin; Dr. Homayoon Dezfuli, National Aeronautics and Space Administration (NASA); Robert Schmedake, Boeing; and Tom DeLong, APT. Representative members of industry, government and academia included AMCOM, APT, Boeing, NASA, Northrop Grumman, Missile Defense Agency (MDA), SAIC and the University of York.

## Scope

The purpose of the workshop was to identify the best relative approach to benefit the system safety discipline and make a recommendation to the G-48 Committee in an effort to define the best practices of system safety. The approaches reviewed and the findings of each are summarized here.

## Safety Cases: Purpose, Process and Prospects

The basic concepts and processes of the Safety Case approach were presented by John McDermid, University of York, U.K. In Ministry of Defence (MoD) practice, a Safety Case is defined as a structured argument supported by claims of why the system is adequately safe. The claims may initially be unfounded; during the course of the safety program, evidence is gathered to confirm

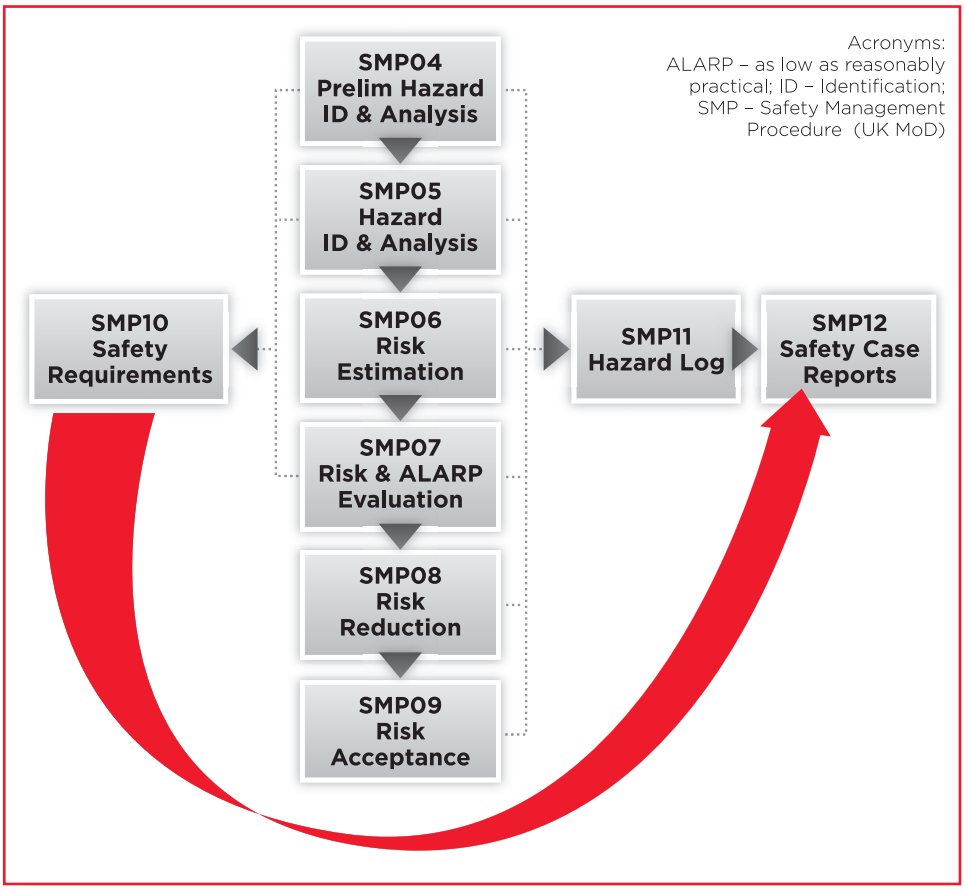



*Figure 1 — Role of (Final) Safety Case.*

[1] The charter of the G-48 Committee includes establishing national best practices in system safety.

or deny the claims. The focus of the program is on gathering evidence, which consists of analyses and data which correlate with the tasks in the ANSI/GEIA Standard and the MIL Standard. As shown in Figure 1, which reflects U.K. MoD practice, the final safety case offers evidence, which provides a comprehensive and compelling case that a system is safe to operate in a given scenario. Because these arguments are defined at the beginning of a program, they establish safety requirements that need evidentiary support to eventually conclude that the system is adequately safe. These claims and the supporting evidence must be independently reviewed prior to the risk acceptance decision.

## Other Approaches Presented for Comparison

### The ANSI/GEIA Process for System Safety Assurance

The background and principles of the ANSI/GEIA Standard (ANSI/GEIA-STD-0010-2009) developed by the G-48 were presented by Dave West, SAIC. The primary focus of this document is to simplify work elements and process flow, modernize the risk assessment matrix and introduce risk summing. The basic elements of an effective system safety program defined by the ANSI/GEIA Standard are shown in Figure 2.

### The MIL-STD-882 Process

The principles of MIL-STD-882E were presented by Don Swallom, AMCOM Safety. The basic elements of the standard were presented, as was background information on the standard. The basic elements of an effective system safety program, defined by MIL-STD-882E, are shown in Figure 3.

### SAE ARP 4761 Process

The SAE ARP 4761, SAE ARP 4754, IEEE STD 1228 and DO-178 process was presented by Barry Hendrix, Lockheed Martin. These documents focus on complex aircraft systems and the development of safety assessments that lead to certifications. The basic products include a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA). Residual risk is not part of the Aerospace Recommended Practice (ARP) process, as requirements must be met with few exceptions. The safety processes associated with aircraft systems are summarized in Figure 4.

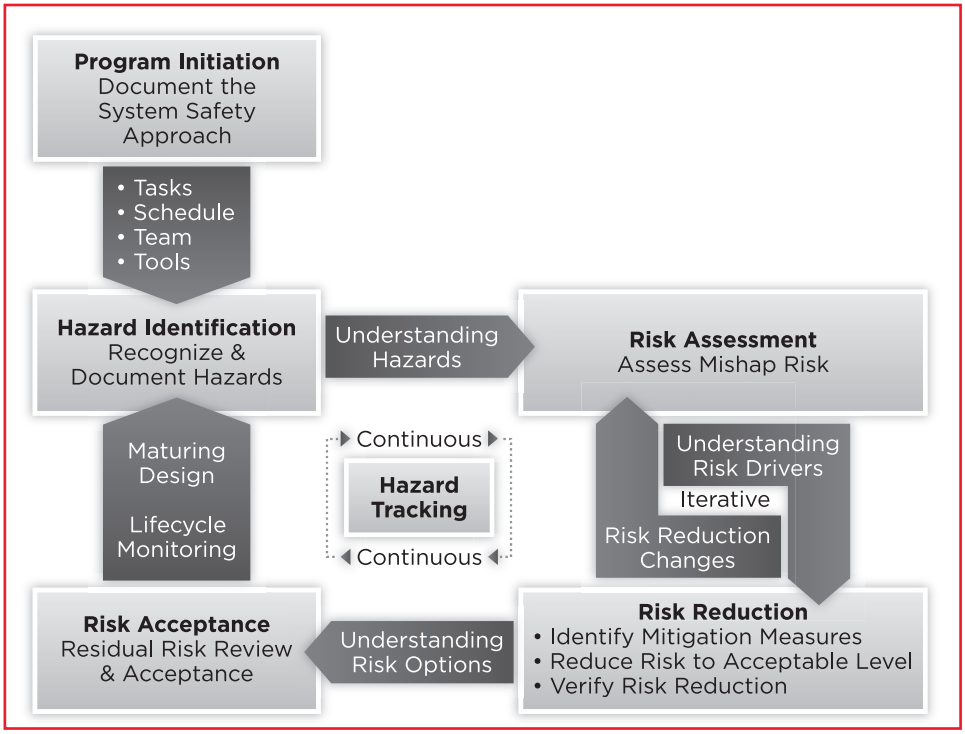



*Figure 2 — ANSI/GEIA-STD-0010-2009 System Safety Approach.*

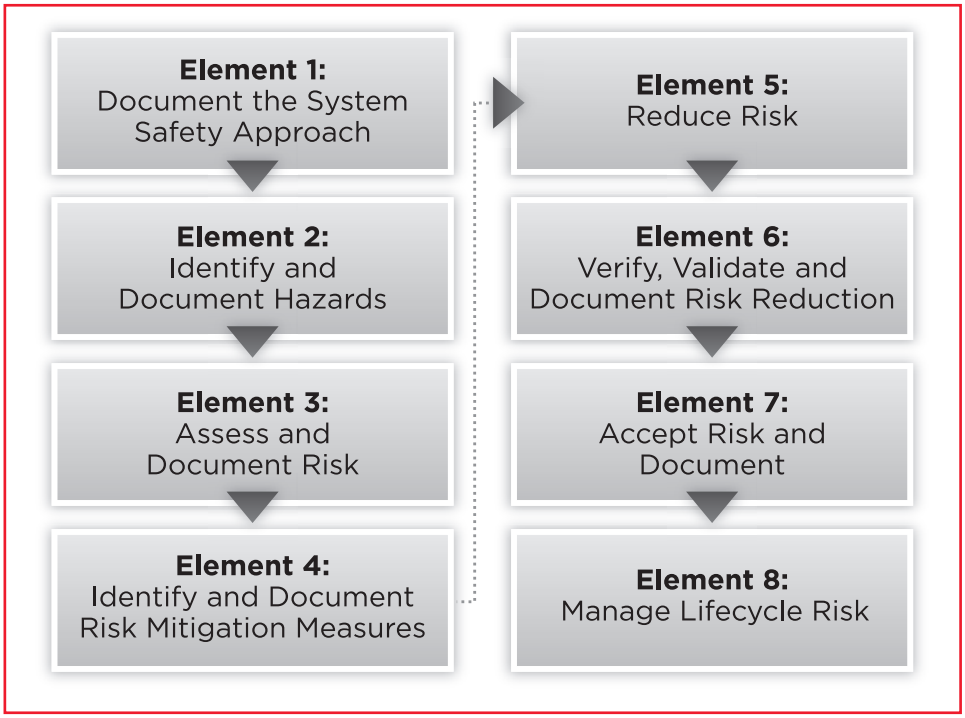



*Figure 3 — MIL-STD-882E System Safety Approach.*

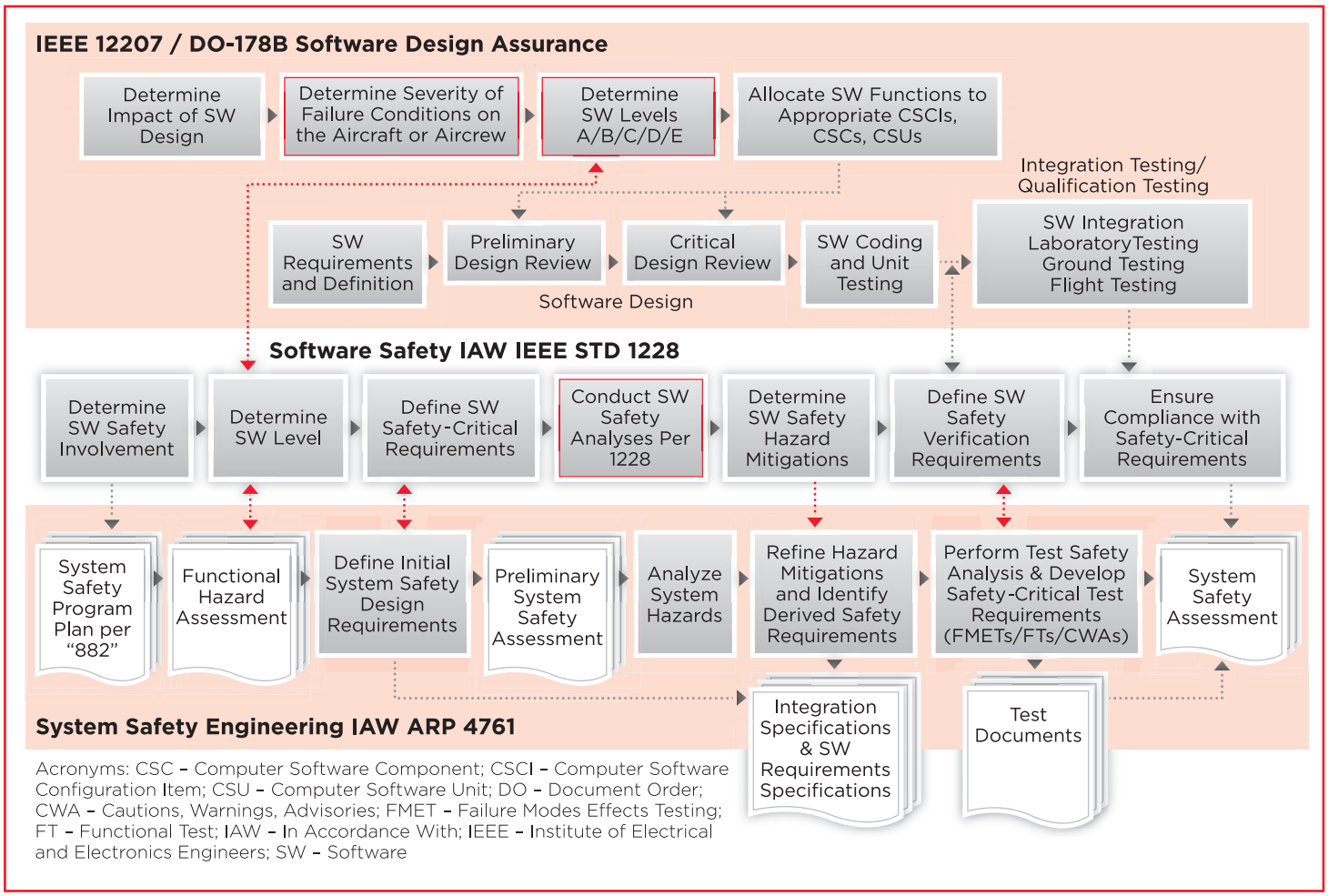



*Figure 4 — Top-Level System Safety Process Used by ARP.*

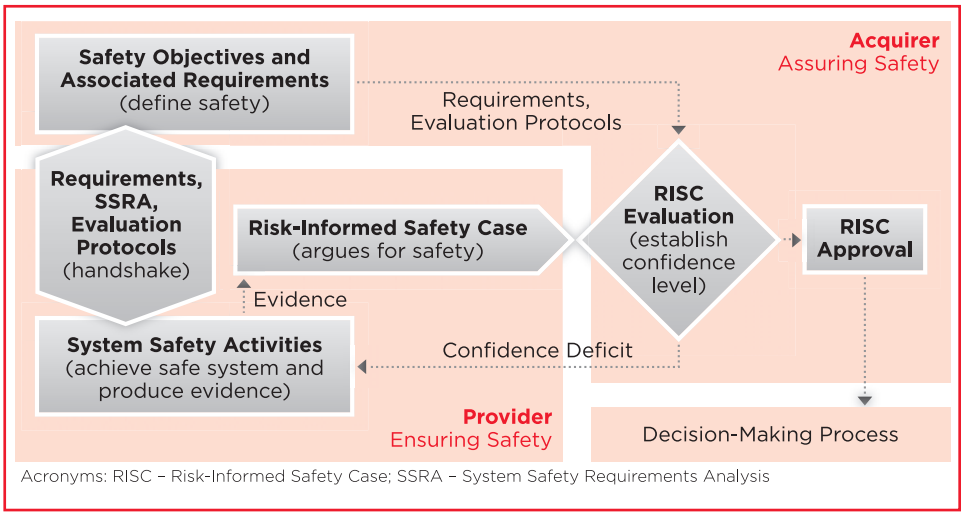



*Figure 5 — NASA System Safety Framework.*

## Application of Safety Case at NASA

Dr. Homayoon Dezfuli presented the NASA evolution of system safety and risk management, as well as the current thinking regarding system safety. The NASA system safety framework, documented in NASA/SP-2010-580, is shown in Figure 5.

Of note was a concept of how to account for Unknown/Underappreciated (UU) risks. NASA recognized the need to consider the gap between the known risk and actual risk when applying safety thresholds and goals. The concept of safety performance margin is used to account for UU risks. This provides a rational basis for deriving verifiable requirements on known risks.

## Safety Case and Software Development

Robert Schmedake, Boeing, discussed the Safety Case approach and how it can be used in software development. The current methods in the standards are not bad; however, there is room for improvement where software is concerned. The advantages of using the Safety Case approach include defining explicit claims for the safety design up front, giving safety claims to build an argument and providing evidence (analysis, inspection, demonstrations and tests) to support claims. The disadvantages include: a system-domain requirement for

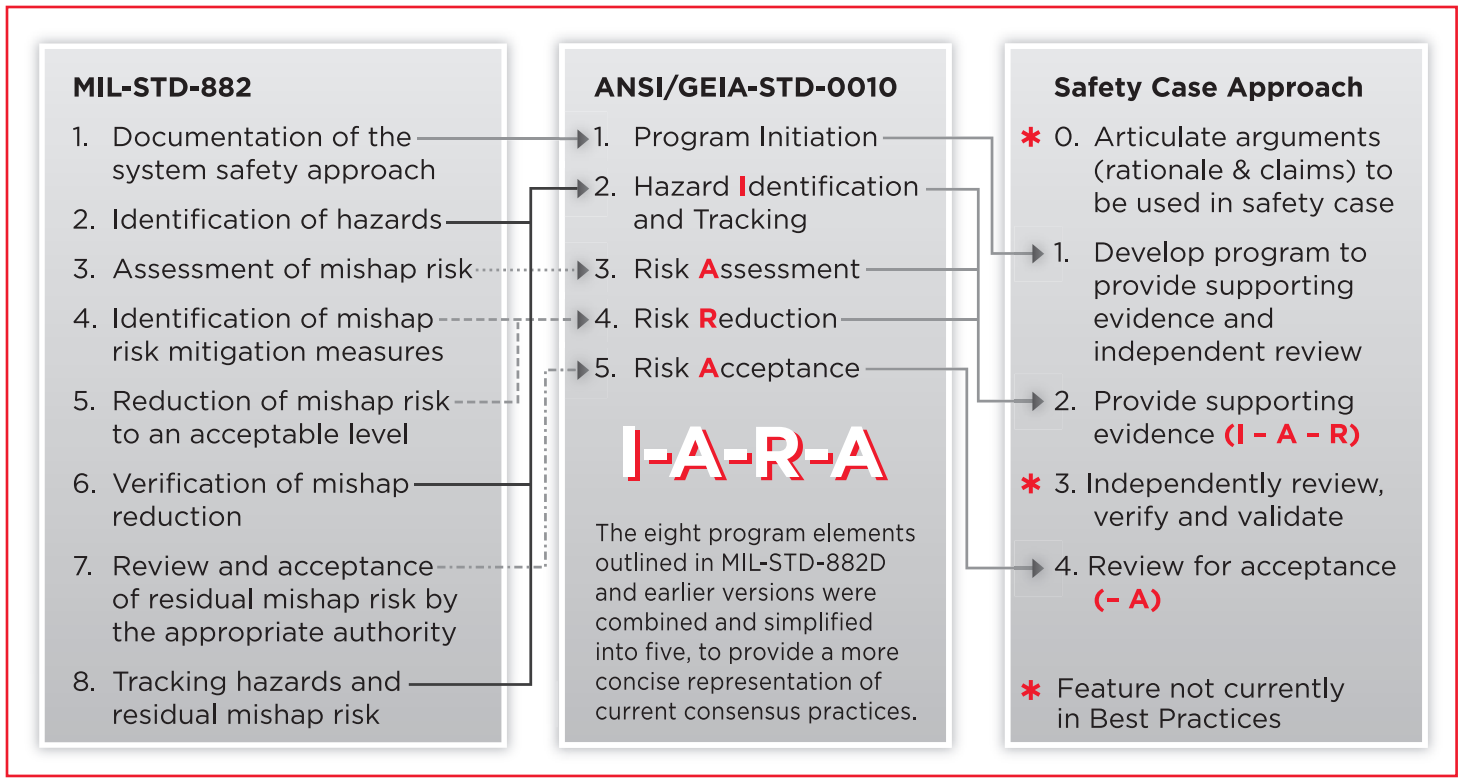



*Figure 6 — Mapping Between Standard Approaches — Traceability Has Been Defined Between ANSI/GEIA-STD, MIL-STD and Safety Case Approach.*

expertise of the developed system. Also, re-use of prior analysis can be problematic since the original case is specific to the original system context.

### Comparison of Methods

Tom DeLong, APT, summarized the various methods and led a group discussion on each. It was noted that in the U.S., NASA and the FAA are moving toward the Safety Case approach.

In the U.S., the safety assessment report (SAR) comes closest to the Safety Case approach; however, a Safety Case is broader in scope than the SAR. A Safety Case is a structured argument, supported by evidence, which provides a comprehensive and compelling case that a system is safe to operate in a given scenario. When compared to the SAR, the biggest difference is the use of arguments and associated evidence to justify them.

When looking at U.S. Army systems, safety processes that seem to be working best include fuzes, rocket motor ignition systems, insensitive munitions and similar items with the following common characteristics: detailed requirements that are included in contracts, well-defined processes to meet the requirements and demonstrate compliance, and a designated group of experts to validate compliance. The safety case approach can also provide the same benefits for a broader set of domains.

The Safety Case approach is a structured way of showing the work done on a safety program and highlights the importance of an independent evaluation group. By defining arguments at the beginning of a program, safety becomes the advocate rather than the protagonist. This approach could change the profession in profound ways by using a positive, front-loaded approach.

### Findings

Comparison of existing ANSI/GEIA-STD-0010 and MIL-STD-882 techniques found that the Safety Case approach includes the most critical elements of these techniques, as mapped in Figure 6. Strengths found in the Safety Case approach that are not included in the U.S. approaches include a beginning step that articulates the rationale, or requirements, to be used and an independent review of the safety approach.

A significant portion of the workshop was dedicated to investigating the strength of the Safety Case. It was noteworthy that with more than 1,000 person-years of safety experience in the room, there were few negative responses and a great many positives. The highlight of the second day of the workshop was reaching consensus on these strengths and observations, as shown in Table 1. The structured, evidence-based approach to satisfying the safety arguments established at the start of the program offers benefits that were not included in other techniques. The consensus of the workshop is summarized in Table 1.

*Table 1 — Strengths and Observations Concerning the Safety Case Approach.*

| Strengths | Observations |
|---|---|
| 1. Includes clear, early definition of most compelling issues | Not included in ANSI/GEIA or 882 |
| 2. Burden of proof is on the provider | |
| 3. Provides a baseline (normalcy map) for safety of the system | |
| 4. Explicit argument tying objective and robust evidence to support proof of claim | |
| 5. Essential narrative communicates effectively to decision makers, risk takers and other stakeholders | |
| 6. Requires robust evidence to support key decisions (e.g., to operate systems) | |
| 7. Explicitly addresses the needs of the decision maker in deciding whether to accept a system, permit a system to proceed to the next phase of development or go to operation | |
| 8. The approach is highly tailorable to fit the need for evidence and the complexity of the system | All safety processes are tailorable; however, this approach seems to be more so because the arguments are unique to the decision |
| 9. Inclusion of independence in review of the case (claims, arguments) | Not included in ANSI/GEIA or 882 |
| 10. Evidence and independent review can aid in risk acceptance phase | Review panels or experts will develop consistent rules |
| 11. Encourages multiple approaches to capture evidence/ facts vs. assumptions | Existing SARs may not include all supporting evidence |
| 12. Promotes a comprehensive assessment of the positive safety aspects of a design but does not overlook negative aspects of the design | Fills potential gaps in 882 |
| 13. Facilitates incorporation of methods, processes and tools from all existing sources | Freedom for broad tailoring |
| 14. Enables development of risk acceptance criteria in context of overall system risk | Enables focus on overall system level risk and does not mandate individual hazard risk assessment code |
| 15. Visibility of progress toward achieving and demonstrating safety objectives | Serves as a road map for the program manager |
| 16. Derived safety requirements from the statement of the arguments and hazard analysis can be put into systems engineering earlier than is currently being done | |
| 17. Earlier visibility of shortcomings (e.g., gaps in evidence) and understanding significance | |
| 18. International standardization of safety methodology | Saves costs on multi-national programs |
| 19. Facilitates a holistic view of complex systems, acknowledging that safety is an emergent property | |
| 20. Supports legal defense | List of hazards can impede legal defense |
| 21. Encourages system safety approach to become more evidence-based as opposed to product-or process-driven | |
| 22. Is compatible with and unifies otherwise potentially fragmented system safety processes and approaches | |
| 23. Encourages systematic attempt to identify where claims may not be satisfied | |
| | This method requires expertise in the system domain of the developed system |
| | Requires up-front work and may make reuse of prior analysis problematic |
| | Requires training and implementation strategies |
| | Requires extensive oversight by qualified practitioners |

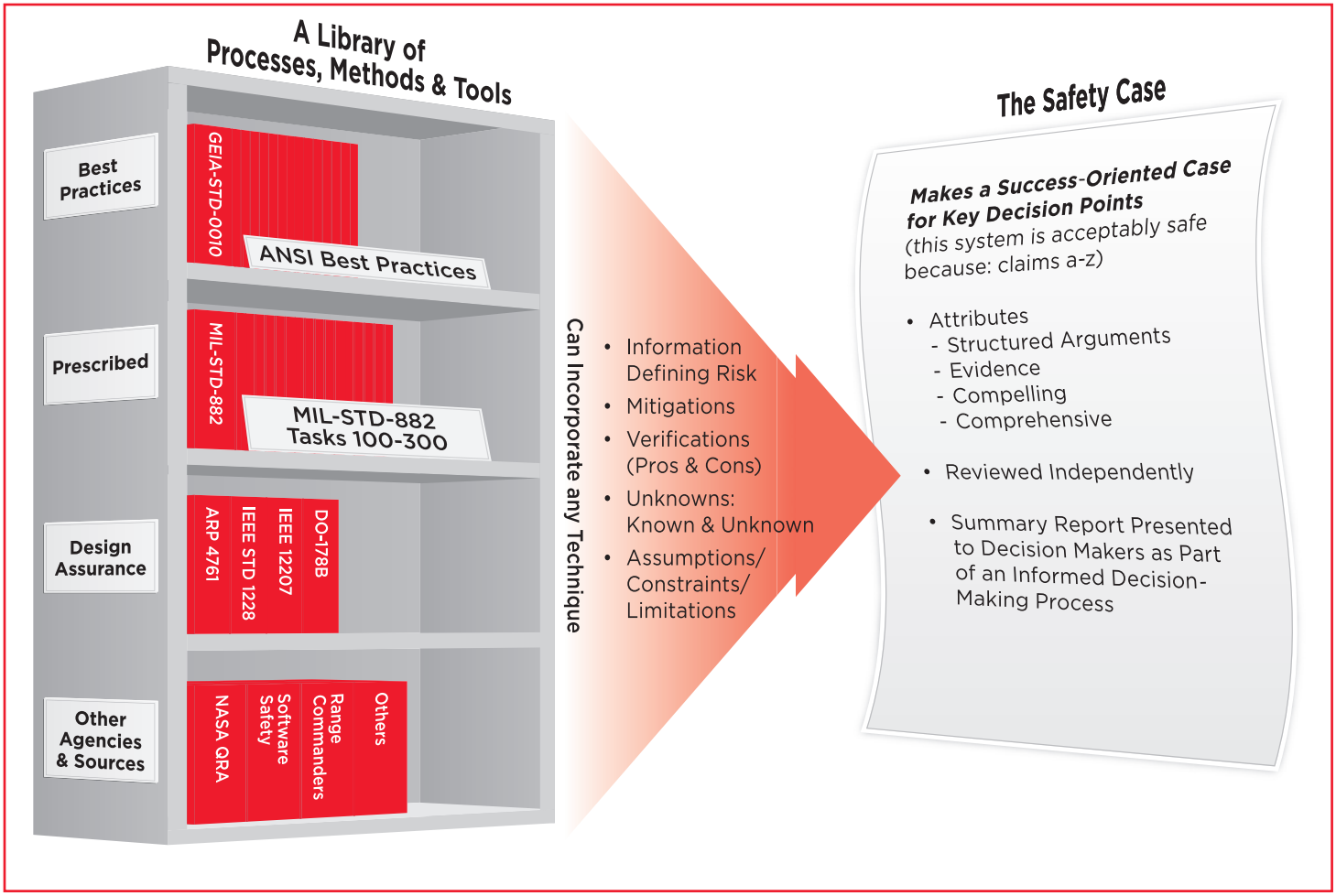



*Figure 7 — What is the Safety Case? An Evidence-Based Approach.*

A concept of what should be included in the Safety Case approach was developed, as shown in Figure 7. Ideally, a Safety Case makes success-oriented claims that, when combined, form the safety argument. After evidence is developed, the claims and evidence are reviewed independently, leading to risk-informed decisions.

## Recommendations Presented to the G-48

The workshop recommended that the G-48 Committee take steps to fully embrace the Safety Case approach as a recognized "best practice." It is also noted that multiple U.S. organizations, including NASA, major aerospace companies and the Chemical Safety Board, are already embracing the Safety Case approach.

Further, the workshop recommends that key features of the Safety Case approach be incorporated into existing approaches documented in ANSI/GEIA-STD-0010. These features include:

- Early identification of arguments required to demonstrate that a system is adequately safe
- Development of compelling and comprehensive evidence to underpin the claims of safety
- Independent review by qualified experts prior to risk acceptance decisions
- Incorporation of evidence that the claims have been substantiated in safety assessments of the system

## Actions Taken by the G-48 Committee

On the following day, January 16, the SAE International G-48 System Safety Committee convened a meeting, which included review of the previously outlined strengths and recommendations. During that meeting, the G-48 Committee endorsed the recommendations of the workshop and defined actions that would ultimately incorporate the Safety Case approach into documented "Best Practices." The actions assigned included developing a workshop paper documenting the findings of the group, developing a track/panel on this approach for the International System Safety Conference (ISSC), and planning the path forward for including the Safety Case approach in a future version of ANSI/GEIA-STD-0010-2009.

## Conclusion

For more than 40 years, the process-based approach has been used within the U.S. to manage system safety pro-

grams. These include the eight-step MIL-STD process and the IARA process used in the ANSI/GEIA Standard. During the past 15 years, a growing number of advocates have been using the evidence-based Safety Case approach to validate the safety of systems. A review and comparison of the methods show that the Safety Case approach includes strengths not found in the process-based approach. Therefore, it is concluded that the Safety Case approach has merits worthy of being accepted among the best world-wide system safety practices.

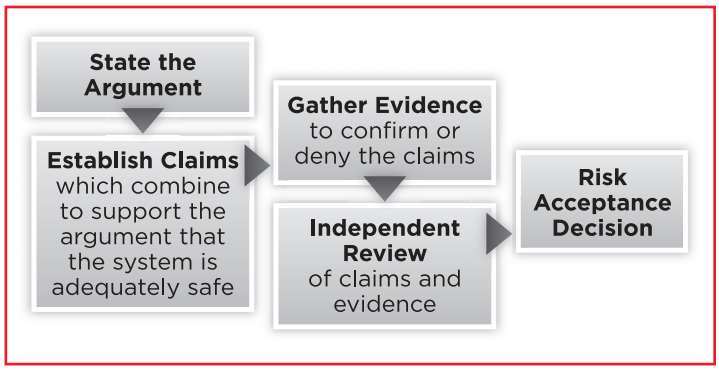



*Figure 8 — Safety Case Process.*

## About the Contributors

**John Frost,** moderator, is a current NASA Aerospace Safety Advisory Panel member who owns a successful safety consulting company. He is a Senior member of the International System Safety Society (ISSS), a professional member of the American Society of Safety Engineers and active in various system safety organizations and initiatives, including G-48. He is the former chief of safety for U.S. Army AMCOM, chaired the Army's Ignition Safety Review Board and served as an Army Explosive Hazard Classification authority.

**John McDermid,** OBE FREng, is professor of software engineering at the University of York, U.K. and was head of the Computer Science Department from 2006 to 2012. He set up the High Integrity Systems Engineering research group, and was instrumental in developing techniques for producing safety arguments and safety cases that are now used worldwide. He is a Fellow of the Royal Academy of Engineering, and an Officer of the Order of the British Empire (OBE).


*The Safety Case Workshop — Standing, left to right: Stephanie Wacenske, MDA; Tracy Conklin, Cargo Safety; Jim Gregoire, Northrop Grumman; Melissa Emery, A-P-T Research, Inc.; Ray Applebaum, A-P-T Research, Inc.; Willie Fitzpatrick, RDECOM, AMRDEC; Terrell Swindall, AMCOM Safety; Bob Youngblood, Idaho National Labs; Jason Kirkpatrick, PM UAS; Saralyn Dwyer, A-P-T Research, Inc.; Homayoon Dezfuli, NASA.*
*Seated, left to right: Tom DeLong, A-P-T Research, Inc.; Don Swallom, AMCOM; John McDermid, University of York; Tom Pfitzer, A-P-T Research, Inc.; John Frost, Moderator; Dave West, SAIC; Robert Schmedake, Boeing; Barry Hendrix, Northrop Grumman.*

**Dave West,** CSP, PE, CHMM, Fellow, is senior director and chief safety engineer of a 1,000-employee operation of SAIC, and is current chairman of the SAE International G-48 System Safety Committee. He is a former president of the ISSS Tennessee Valley Chapter, and has more than 25 years of experience performing safety work for Army aviation and weapon systems, chemical demilitarization, spaceflight programs, chemical plants, and nuclear facilities.

**Don Swallom** is a safety engineer for the U.S. Army AMCOM and a Fellow member of ISSS. He is a former president of the Tennessee Valley Chapter, former pilot, staff officer and developmental engineer in the U.S. Air Force, and former chief of safety for the Arnold Engineering Development Center.

**Barry Hendrix** is a Lockheed Martin Technical Fellow Emeritus for aviation safety and airworthiness and has more than 40 years of experience on various weapon systems. He is the IBCS System Safety Lead for Northrop Grumman and served 10 years in the U.S. Navy aboard aircraft carriers as an aviation fire control system specialist on fighter and attack aircraft.

**Homayoon Dezfuli,** Ph.D., is a NASA system safety technical fellow and the manager of system safety in the Office of Safety and Mission Assurance at NASA Headquarters. He led development of and co-authored several NASA procedures guides and handbooks, devised a safety goal implementation framework that has helped shape the NASA safety goal policy for human space flight, and is leading the development of the NASA System Safety and Mission Success Standard.

**Robert Schmedake** is a Boeing Technical Fellow, with more than 25 years of experience in system safety engineering. He is a Fellow member and current president of the ISSS, secretary of the G-48, U.S. co-chair of the S5000F Committee and a member of the joint Aerospace Industries of America & Aerospace and Defense Industries of Europe Integrated Logistic Support Specification Council. He served in the U.S. military from 1986 to 2012.

**Tom Delong** is the former lead systems safety engineer for SMDC, and has more than 35 years of safety experience. He chaired several missile anomaly investigations during a LAW alternative source selection and managed SETA contract and Range Safety Analysis contract at SMDC. He is lead instructor for APT's system safety training program, which provides instruction to more than 100 professionals annually.

## References*

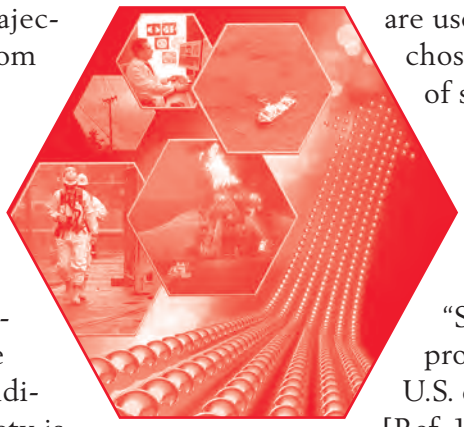

1. McDermid, John. "Safety Cases: Purpose, Process and Prospects," Safety Case Workshop, January 14-15, 2014.
2. West, Dave. "The 'ANSI' Process for System Safety Assurance," Safety Case Workshop, January 14-15, 2014.
3. ANSI/GEIA-STD-0010-2009, "Standard Best Practices for System Safety Program Development and Execution," February 12, 2009.
4. Swallom, Don. "The MIL-STD Process," Safety Case Workshop, January 14-15, 2014.
5. MIL-STD-882E, "Department of Defense Standard Practice System Safety," May 11, 2012.
6. Hendrix, Barry. "SAE ARP 4761 Process," Safety Case Workshop, January 14-15, 2014.
7. SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," December 1, 1996.
8. IEEE 12207, "Standard for Information Technology – Software Life Cycle Processes," May 1998.
9. DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," December 1, 1992.
10. IEEE STD 1228. "IEEE Standard for Software Safety Plans," March 17, 1994.
11. Dezfuli, Homayoon. "Application of 'Safety Case' at NASA," Safety Case Workshop, January 14-15, 2014.
12. Schmedake, Robert. "Safety Case and Software Development," Safety Case Workshop, January 14-15, 2014.
13. Delong, Tom. "Define & Compare Flowcharts of Each Method," Safety Case Workshop, January 14-15, 2014.


* Briefing available online at www.apt research.com/news/newsBlog2014.html#SafetyCase

# ‘Technical Safety’ or ‘System Safety’? Why Names Matter

*by Sergio Oliva and Ricardo Lopez*
*Houston, Texas*

By providing safety and risk management consulting services, we have the opportunity to be regularly involved with clients from a number of different industries. We often interact with professionals of varied trajectories and backgrounds, many of whom have never received comprehensive training in system safety. Those individuals are by no means less competent in their jobs; however, their schooling in system safety often comes from a senior colleague or mentor who held a safety-related position during a long career in a single industry. More often than not, the individual’s understanding of system safety is reduced to his or her limited exposure to this rich and diverse field.



A few months ago, we were involved in an offshore project for an oil and gas client. We visited the client’s office for a project presentation. The meeting was on a normal course until we brought up certain system safety issues that required our attendee’s review. These issues were under the label of “technical safety,” which in hindsight was a mistake. We were soon challenged to offer a definition of technical safety, which in our view was no different than system safety. This gentleman argued that technical safety was different from the other “safeties” such as system, functional or operational safety. Coincidentally, a few weeks later in a meeting with a different group of clients, we mentioned that our expertise included system safety. One of the meeting participants immediately asked: “What system?”

The preceding experiences made us consider how safety professionals may use tools, techniques or mental constructs that were developed in different industries, and originally labeled under different names. It is a matter of fact that familiarity with equipment, processes or activities in a technical field favors the use of unique terminology to the point of developing a professional jargon that is intelligible only to insiders. The constant repetition of a term by specialists in an industry without a clear definition of that term’s meaning creates a false sense of universality. The terminology used by industry experts frequently differs from the terms used by colleagues in other industries, despite the fact that similar, if not identical, methods, ideas and contraptions are used by all. This is extensive to our chosen profession and to the actual field of system safety.

## System Safety in All Its Flavors

After the previous experiences with our clients, we questioned our own understanding of the subject. “System safety” may be traced to the production of ballistic missiles in the U.S. during the decade after World War II [Ref. 1]. The first system safety practitioners developed methods to assess risks and controls of the hazards related to the rapidly changing technologies they were facing. Some of the new quantitative methods were highly favored by the emerging computerization taking place in military technology. Analyses were initially time consuming, limited and restricted to a few classified reports. In time, the proven success of the methodology became known worldwide. System safety as a professional field was thereafter established.

Variations of the concept of system safety have been offered by experts, but the almost 40-year-old definition remains up to date: *“The application of engineering and management principles, criteria and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle”* [Refs. 2 & 3]. The completeness and broad scope of system safety is manifest when the term “system” is subsequently defined [Ref. 4]: *“An integrated composite of people, products and processes that provide a capability to satisfy a stated need or objective. “*

We are personally aware that the aforementioned definition of system safety is accepted and in use in several industries, such as aerospace, defense, mass transit and medical device manufacturing. We are also aware that some areas of the body of knowledge of system safety have acquired their own specific names. Colleagues in various industries have attempted to define

*Table 1 — System Safety Under Different Names*

| Name | Most Accepted Definition | Industry | Reference |
|---|---|---|---|
| Functional Safety | Part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system, which depends on the correct functioning of the electric/electronic/programmable electronic safety-related systems, other technology safety-related systems and external risk reduction facilities | Electronics, Oil & Gas | [5] |
| Operational Safety (Management) | The systematic management of the risks associated with flight operations, related ground operations and aircraft engineering or maintenance activities to achieve high levels of safety performance | Civil Aviation, Railway, Nuclear, Oil & Gas* | [6] |
| Process Safety (Management) | The proactive identification, evaluation and mitigation or prevention of chemical releases that could occur as a result of failures in process, procedures or equipment. | Oil & Gas, Chemical | [7] |
| Technical Safety (Requirements) | The limits, controls and related actions that establish the specific parameters and requisite actions for the safe operation of a (nuclear) facility. | Nuclear, Oil & Gas Upstream** | [8] [9] |

* The use of "operational safety" has been adopted by these industries, civil aviation notwithstanding, without any formal definition. The reader may refer to [10] for more on the topic.

** No definition of "technical safety" for Oil & Gas is provided in [8], despite its title.

these safety areas, with limited success. Table 1 shows a list of definitions based on the authors' experience.

One may argue that since people have always been part of the system, occupational safety is therefore embedded in system safety. Perhaps for pragmatic reasons, the safety of workers in the workplace has been historically addressed by specialists with little experience in system safety. By the same token, system safety practitioners are often unaware of all the intricacies and requirements that compliance with workplace safety and labor laws demands from our occupational colleagues. This is especially true when the manufacturing, testing and deployment of a system imply managing people with different cultures and languages, and in compliance with laws in workplaces scattered around the globe.

Specialized scientific knowledge often spins off in time into a new field of science. The contributions of its practitioners propel the development of the new field with its ultimate acceptance by the scientific community and the general public. Process safety may be one of these cases as defined in Table 1. Any plant safety aspect related to a potential chemical release is now typically under the label of process safety. Its practitioners customized system safety methods in the 1980s, and even created new techniques to address the unique issues of the process industries, more specifically in petrochemical facilities. Layers of protection analysis (LOPA) and safety integrity levels (SIL) are examples of that effort. At best, these techniques match the capabilities of fault and event tree analysis. However, that does not change the fact that LOPA and SIL are central to process safety, and are often the first quantitative tools of choice for practitioners in that field.

The use of preceding modifiers to the term "safety" is customary in many industries and mostly useful to characterize a specialization within the broad professional field of safety. The modifier identifies the specialty to make a clear distinction from others. "Patient safety," "radiation safety" and even "system safety" are examples of that use. Therefore, the names in Table 1 suggest that those areas of safety are somehow different from system safety, and indeed perceived by many as disconnected from our chosen profession. Some may argue that the specialized knowledge required in those industry niches deserves specific designations within the safety profession. Time will tell, but a false sense of uniqueness is portrayed in the meantime. As long as no clear definition of those specialties is provided and the use of system safety methods continues, system safety practitioners are affected. Professionals and others with little exposure to system safety tend to believe that the meth-

odologies used in Table 1 specialties were developed within, or for, those industries alone. Managers and other decision-makers are often doubtful of methods and tools applied by outsiders, let alone of hiring system safety practitioners from a different industry. It may take years for a risk assessment technique to be tested and adopted outside its industry of origin [Ref. 11]. The frequent re-labeling of methods once they migrate to different industries compounds the detrimental effect. New practitioners are prevented from finding the original association, and often remain uninformed of concurrent breakthroughs by peers in other industries.

## Conclusion

Despite the issues discussed here, world-class organizations are working to close the gap among professionals on issues related to safety and risk assessment. In the Internet age, a professional forum is relatively inexpensive to create, and the benefits may be accessed by colleagues worldwide. The International System Safety Society is an example, for its outreach to foster communication among professionals of different industries across the globe.

As technologies and systems continue evolving, and capital projects remain fraught with risks, system safety will have an important place in project management. System safety practitioners will certainly have an important role in the optimization of all aspects of safety. This role will be fostered if it is derived from a cooperative effort among professionals in every industry — or it will likely be hindered by the atomization of our chosen profession.

## About the Authors

**Sergio Oliva** until recently was a senior safety and risk consultant at ERM in Houston, Texas. He currently works for Wild Well Control, Inc. Sergio has more than 17 years of multi-industry experience, and holds a master's degree in engineering from Texas A&M University at College Station. He is a certified safety professional (CSP) who is also experienced in system safety, reliability and quantitative risk assessment. He has authored reports and professional publications, including peer-reviewed technical papers in renowned scientific journals. He is a member of the International System Safety Society.

**Ricardo Lopez** is a principal consultant in safety and risk management within ERM's Houston office. He has more than 30 years of experience in civil engineering and a master's degree in environmental science from the University of Houston at Clear Lake. Ricardo has led efforts on reliability, availability and maintainability (RAM) analyses, financial risk, building site assessments and quantitative risk analyses of capital projects for major oil and gas companies.

## References

1. Vincoli, J. W. *Basic Guide to System Safety*, John Wiley & Sons, 1993.
2. Department of Defense Standard Practice for System Safety. "MIL-STD-882D," February 10, 2000.
3. "System Safety Links," International System Safety Society, accessed September 13, 2013, http://www.system-safety.org/links/
4. Air Force Safety Agency, Kirtland Air Force Base. "*Air Force System Safety Handbook* (AFB NM 87117-5670)," July 2000.
5. International Electrotechnical Commission. "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems," IEC 61508 International Standard, Part 4.
6. Civil Aviation Authority. "Safety management systems for commercial air transport operations," CAP 712, April 2002.
7. U.S. Department of Labor Occupational Safety and Health Administration. "29 CFR 1910.119 Federal Regulation, Process safety management of highly hazardous chemicals," July 2011.
8. Norwegian Oil Industry Association (OSL). "Technical Safety," NORSOK Standard S-001, Edition 4, February 2008.
9. U.S. Department of Energy Nuclear Regulatory Commission. "10 CFR Part 830 Federal Regulation, Nuclear Safety Management," January 2011.
10. Salter, M. "Managing the Operational Safety Case in High-Risk Systems," MS Thesis, University of York, Department of Computer Science, September 2006.
11. Stamatelatos, M. and H. Dezfuli. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (NASA/SP-2011-3421)," Second Edition, Office of Safety and Mission Assurance NASA Headquarters, December 2011.

# OSH Management Systems: Will They Hold Up in a Court of Law?

*by David Wise*
*Bethel, Pennsylvania*

The best occupational safety and health (OSH) management systems are "standards-based," i.e., they are grounded solely in the U.S. Code of Federal Regulations and other official statutory requirements. They employ standards based on the law and, consequently, provide significant liability protection.

Unfortunately, and often unknown to users, many OSH management systems are derived from "sources" that everyone assumes were developed from official regulatory guidance. This difference is important because derivations and assumptions may or may not hold up in a court of law. When it comes to protection from legal liability, only actual standards — to the "letter of the law" — really matter. (See Figure 1 for an example of a regulatory standard.)

Should a worksite death, accident or illness occur, the first questions that lawyers, prosecutors, judges, federal inspectors and others are likely to ask are these: "May we examine your OSH program records and documentation?" Or, "May we see the 'tangible evidences' of your OSH planning, training, self-inspection, review and other programs?"

When these types of documents are requested and these types of questions are asked, these individuals are checking to see if your company is employing standards-based programs, and that your company is effectively working those programs. They're also checking to see how accurately a company's OSH programs compare with the law. "Are they outdated? Are they incorrect or inaccurate?" Or, as required, "Are they based on current statutory law, and do they employ and/or direct users to valid statutory guidance?"

Also, for example, Occupational Safety and Health (OSHA) inspectors are going to ask similar questions at an "opening conference" of an on-site inspection. Inspectors are directed to immediately ask for injury and illness records. Then, they ask for "other OSHA programs and records … including hazard communication, lockout/tagout, emergency evacuation and personal protective equipment." In addition, "many standard-specific directives provide additional instruction to inspectors requesting certain records and documents at the opening conference" [Ref. 1].

29 U.S.C.
United States Code, 2011 Edition
Title 29 – LABOR
CHAPTER 15 - OCCUPATIONAL SAFETY AND HEALTH
Sec. 654. Duties of employers and employees
(a) Each employer—
(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
(2) shall comply with occupational safety and health standards promulgated under this chapter.
(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this chapter which are applicable to his own actions and conduct.
(Pub. L. 91–596, §5, Dec. 29, 1970, 84 Stat. 1593.)
From the U.S. Government Printing Office, www.gpo.gov

Also known as the General Duty Clause for Occupational Safety and Health
Cited as: 29 U.S.C. § 654, 5(a)(1)

*Figure 1 — Example of a Regulatory Standard.*

Editor's Note – This is the first of four articles in a series by David Wise. Be sure to watch for future articles on:

- Do your System Safety Approaches include multiple programs, including planning, training, inspecting, and reviewing? And, are those programs built on the Plan-Do-Check-Act cycle for "Continuous Quality Improvement?"
- Are your System Safety Approaches powered with Relational Database Management Technology (RDMT) or equivalent technology? That is, do your approaches share safety and health compliance management data relationally within and between multiple programs?
- Do you use your System Safety Approaches to Achieve Awards and Recognitions?

Again, inspectors are checking for similar things; namely, actively managed programs and systems based on the U. S. Code of Federal Regulations and other official statutory sources.

## Conclusion

Are your company's OSH management systems standards-based, i.e., are they based solely on statutory law? Said another way, will they hold up in a court of law?

Your company's management might as well ask these questions first, as they will likely be the first questions inspectors, lawyers and others will be asking should an OSH incident or on-site inspection occur at one of your company's worksites.

In the next two issues of *Journal of System Safety*, I will share two additional important components of a highly effective occupational safety and health management system:

- Multi-programmed and "quality"-driven: Built on the Plan-Do-Check-Act (or PDCA) cycle for "continuous improvement" (also known as the "quality" model). With this approach, multiple OSH programs are managed, including planning, training, inspection and review.
- Technologically-advanced: Powered with relational database management technology (RDMT) or equivalent technology, integrating compliance management data within and between each program, thereby eliminating redundant data and work efforts.

## About the Author

**David A. Wise** holds an MS in OSH/EM from Columbia Southern University and an undergraduate degree in health care management from the Community College of the Air Force. David is employed by the Department of Veterans Affairs as a CDL motor vehicle operator and bus driver, taking veterans to various morale, welfare and recreational activities, as well as medical appointments. He is also a chaplain's assistant with the U.S.A.F. Reserves. David Wise is the owner and developer of The Relational EHS™ Management System, a powerful, comprehensive relational database management system used by general industries to manage their environmental, health and safety (EHS) compliance requirements. David shares his application with companies as free shareware.

## Index of Advertisers



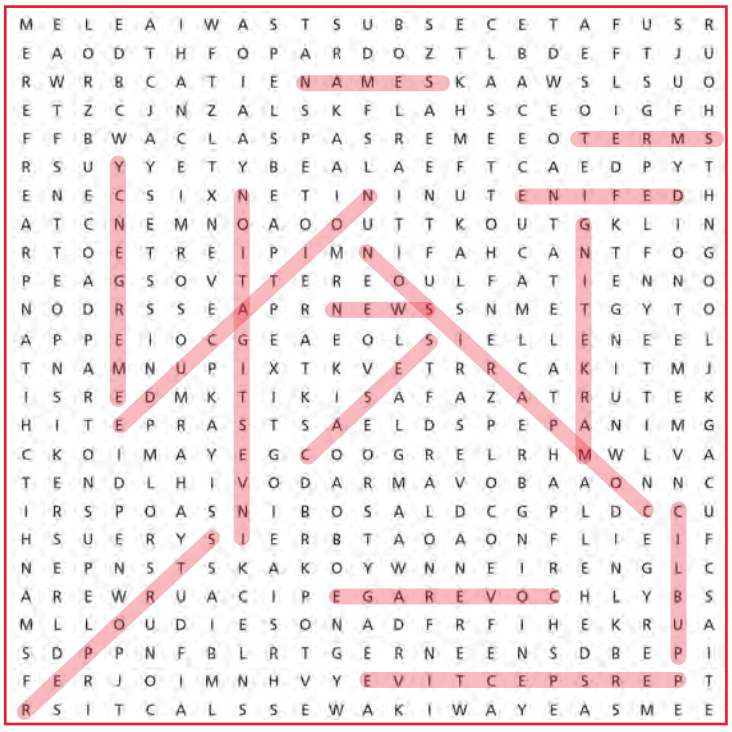
## We Want to Hear from You

*Journal of System Safety* is seeking papers and articles on topics including the following:

- Explosive Safety
- Nuclear Safety
- Hazardous Material Management
- Chemical Safety
- Biotech Safety
- Safety Management Issues
- Human Error
- Software Safety
- Safety-Critical Processes
- Lessons Learned

Please send summaries or abstracts to Clif Ericson, Technical Editor, at journal@system-safety.org.

## Word Find Solution (from page 18)



# System Safety Society Chapter Contacts

**ASIA PACIFIC**
**Singapore Chapter**
Ten Lin Mei
tlinmei@dso.org.sg

**AUSTRALIA**
Dr. Holger Becht
+61 (0)7 3102 9742
holger.becht@rgbassurance.com.au

**CANADA**
Maury Hill
613-220-0533
Mauryhill@rogers.com

**UNITED STATES OF AMERICA**
**ALABAMA/TENNESSEE/MISSISSIPPI**
**Tennessee Valley Chapter**
Don Swallom
256-842-8641
swallom@isss-tvc.org

**ARIZONA**
**Saguaro Chapter**
Amanda Boysun
520-794-5487
amanda.boysun@raytheon.com

**CALIFORNIA**
**Bay Area Chapter**
Graham Murray
408-756-2674
Graham.t.murray@lmco.com

**Central California Chapter**
Kathleen Brenna
805-606-2308
Kathleen.Brenna.1@us.af.mil

**Sierra High Desert Chapter**
Jerry Banister
760-377-4690
safety.citadel@earthlink.net

**Southern California Chapter**
Francis McDougall
310-653-1309
francis.mcdougall@us.af.mil

**GEORGIA**
Odell Ferrell
770-494-4814
odell.ferrell@lmco.com

**MAINE/NEW HAMPSHIRE/VERMONT/**
**MASSACHUSETTS/RHODE ISLAND/**
**CONNECTICUT/PENNSYLVANIA/NEW**
**YORK/NEW JERSEY**
**Northeast Chapter**
Scott Beecher
860-565-7022
Scott.Beecher@PW.utc.com

**MINNESOTA**
**Twin Cities Chapter**
Bill Blake
763-744-5086
bill.blake@atk.com

**NEW MEXICO**
William Harwood
505-853-4595
william.harwood@mda.mil

**TEXAS**
**Houston Chapter**
Derek Robins
281-820-8828
Derek.Robins@mwcc-usa.com

**North Texas Chapter**
Frank Rinaldo
817-762-3075
frank.r.rinaldo@lmco.com

**VIRGINIA/MARYLAND/DELAWARE**
**Washington DC Chapter**
Sean Peters
540-663-7369
sean.peters@urs.com

**VIRTUAL CHAPTER**
Doanna Weissgerber
408-289-4407
Doanna.Weissgerber@baesystems.com

**RVP Asia-Pacific**
Eng Ling Onn (Singapore)
011-65-9632-6256
onnel@stengg.com

**RVP Europe**
Gabriele Schedl (Austria)
43 (1)811-50-2758
gabriele.schedl@frequentis.com

**RVP North/South America**
Paul Kryska (USA)
408-953-4127
pkryska@yahoo.com

**International Director**
Robert Fletcher
613-837-4128
rwfletcher@sympatico.ca

**Director of Chapter Services**
Gerry Einarsson
613-824-2468
einargk@rogers.com

## Join the System Safety Society!

**Benefits of joining the System Safety Society include:**

- The System Safety Society is the only professional organization specifically dedicated to promotion of the system safety concept at the local, national and international level.
- Members benefit through contacts with other members and interfacing with persons in related disciplines at Chapter meetings, symposia and annual International System Safety Conferences.
- The Society promotes professionalism by establishing criteria and recognition for outstanding achievements.
- Recognizing the critical need for technical and philosophical communications on system safety at a professional level, it publishes the bimonthly *Journal of System Safety*.
- Members and employers receive assistance in finding and filling system safety positions.
- Society members are informed of new technology and advancements.

**For membership forms or more information, visit http://www.system-safety.org, call 540-854-8630 or email systemsafety@system-safety.org.**

## Activities

Through its local chapters, committees, executive council, publications and meetings, the Society provides many opportunities for interested members to participate in a variety of activities compatible with Society objectives. In addition to the basic operating committees, Society activities include several noteworthy publications and events.

## Publications

- ***Journal of System Safety*** is the official Society journal. Published three times a year, *JSS* keeps members informed of the latest developments in the field of system safety.
- Chapter newsletters are published periodically to disseminate news of chapter activities and items of interest to chapter members.
- Proceedings of Society-sponsored conferences and symposia are made available to members at a special discount.

## Meetings — Conferences — Symposia

- International System Safety Conferences are sponsored annually. These conferences have proven to be a very popular and effective means for highlighting the latest techniques, applications and social/legal aspects of system safety.
- Mini-symposia are sponsored by local chapters to provide an in-depth exploration of a specific system safety-related topic.
- Chapter dinner meetings, field trips and panel discussions are held at intervals throughout the year.
- The Society is a co-sponsor of various system safety-related symposia and conferences.

Membership in the Society is open to all persons having an interest in or currently involved in work related to system safety or an allied discipline. Professional membership grades are available for those able to demonstrate sufficient qualifications, experience and training. Annual dues are $100 (USD) for United States and Canada and $110 (USD) for international members. Student memberships are free. There is a one-time application fee of $20 (USD). Society members and subscribers are located in all areas of the United States and many countries around the world:

**Australia**
**Austria**
**Cameroon**
**Canada**
**Chile**
**China**
**France**
**Germany**
**Greece**
**Israel**
**Italy**
**Japan**
**Netherlands**
**Nigeria**
**Norway**
**Russia**
**Saudi Arabia**
**Singapore**
**South Africa**
**Spain**
**Sweden**
**Switzerland**
**United Kingdom (England, Northern Ireland, Scotland and Wales)**
**United States of America**

Requests for membership applications, subscription orders, requests for Conference Proceedings and other matters related to membership and services should be addressed to the **International System Safety Society**, P.O. Box 70, Unionville, VA 22567-0070. Tel: 540-854-8630; fax: 540-854-4561; email: systemsafety@system-safety.org. Visit our Web site at http://www.system-safety.org.

The **International System Safety Society** is a non-profit organization of professionals dedicated to the safety of systems, products and services through the effective implementation of the system safety concept. Under this concept, appropriate technical and managerial skills are applied so that a systematic, forward-looking hazard identification and control function becomes an integral part of a project, program or activity at the planning phase and continues through the design, production, testing, use and disposal phases.

## The Society's Objectives

- To advance the art and science of system safety
- To promote a meaningful management and technological understanding of system safety
- To disseminate advances in knowledge to all interested groups and individuals
- To further the development of the professionals engaged in system safety
- To improve public understanding of the system safety discipline
- To improve the communication of system safety principles to all levels of management, engineering and other professional groups

**International System Safety Society**
**Professionals Dedicated to the Safety of Systems, Products and Services**

**INTERNATIONAL SYSTEM SAFETY SOCIETY, INC.**
P.O. Box 70
Unionville, VA 22567-0070

Change Service Requested

World Wide Web: http://www.system-safety.org

Presorted Standard
U.S. POSTAGE PAID
Permit No. 1152
Louisville, KY