Journal of System Safety

Volume 50, No. 1
Winter 2014

Catching Safety Problems at the Planning Stage

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. 1

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
GENERAL DYNAMICS Electric Boat
Atlantic Software TECHNOLOGIES
HCRQ
isograph
LOCKHEED MARTIN
LOCKHEED MARTIN AERONAUTICS COMPANY
RCCSS: RESEARCH & CONSULTATION CENTER FOR SYSTEM SAFETY
UNIVERSITY OF MARYLAND 18 56
A. JAMES CLARK SCHOOL OF ENGINEERING
SoHaR Engineering Support for Critical Systems since 1978
Sikorsky A United Technologies Company
Shell
WWW.ARMY.MIL/AMCOM U.S. ARMY AVIATION AND MISSILE LIFE CYCLE MANAGEMENT COMMAND

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

On Recent Changes and Looking to the Future

A lot has been going on since our last *Journal of System Safety*. We had our International System Safety Conference in Boston with the constraints of the government sequestration affecting our profitability. The conference is a very important source of income for this Society — it amounts to at least half of our income in a normal year. While our conference offered excellent professional development and networking opportunities, 2013's conference operated at a financial loss. We have been responding to this loss by addressing the areas of the budget that we have control over. One of these is the frequency of *Journal of System Safety*. While we have every intention of providing the same quantity of material in *JSS*, we will only publish three journals this Society Year (July 2013 through June 2014). More information about this decision is posted on the Society's Website at http://www.system-safety.org/.

> "...I want to assure you that the Society is committed to providing its membership with an ever-improving quality of service, despite our economic challenges. We will be taking steps to ensure you receive all that we can give, and that at the end of the year, you feel you received the value you expected."

We have been very active renegotiating the conditions in our 2014 conference contract to ensure we do not operate at a loss. The problem we have with these contracts is that we commit at least one to two years in advance of the conference, and this leaves us vulnerable to the effects of drastic changes in the business environment. In last year's case, we had planned on the same attendance as we had experienced for the conferences of previous years, but we had committed to this in 2011. Between the time we committed and the time the conference actually took place, the sequestration rules on government participation in conferences resulted in reducing our attendance by more than 50 percent.

Fortunately for the society, our reserves were able to cover this year's losses, and we expect the cost-cutting efforts will help keep us operating within our income. We are also actively seeking alternative income sources that make sense for the Society.

The Job Target Website has been getting a lot of use lately, helping members find system safety positions and helping employers to find qualified applicants. This site is available at http://www.system-safety.org/jobs/. This service also has the benefit of generating a small amount of income for the Society each month.

We have made progress on the conference venue for 2014. Our conference will occur from August 4 through 8 at the Union Station DoubleTree Hotel in St. Louis, Missouri. The Website will be set up soon for registration, and we are currently signing up sponsors for the conference. The Boeing Company has signed up as the Corporate Sponsor for the conference, and we are now signing up Gold- and Silver-level sponsors, as well as exhibitors. Conference information will be available by a link from the Society's Web page at www.system-safety.org.

St. Louis offers a number of activities that should be of interest, which you can learn about at www.explorestlouis.com. St. Louis is a baseball town; few cities have such loyal fans or a team that so consistently makes it to the playoffs. As luck would have it, the Boston Red Sox and the St. Louis Cardinals will be playing at Busch Stadium during the conference week. Come and see the two teams that played in the 2013 World Series.

In closing, I want to assure you that the Society is committed to providing its membership with an ever-improving quality of service, despite our economic challenges. We will be taking steps to ensure you receive all that we can give, and that at the end of the year, you feel you received the value you expected.

Sponsor/Exhibitor Opportunity

32nd International System Safety Training Symposium

St. Louis, Missouri August 4-8, 2014

Sponsor

Cost: $3,500 and Includes:

- Two conference registrations (can rotate between company personnel; includes Awards Banquet tickets)
- 20% discount on up to three additional registrations
- "Plus" booth package (allows selection of booth location based on final payment)
- Two copies of proceedings
- One full-page advertisement in proceedings
- Company logo and hyper link on the conference web page
- Company literature in each attendee's welcome package
- One year System Safety Society Corporate membership and its benefits

Exhibitor

Cost: $2,200 and Includes:

- Limited conference registrations

(Two tickets to the luncheons Tuesday through Thursday, including the special exhibitors social event)

- Regular booth package
- One copy of proceedings
- One business card-size advertisement in proceedings

Contact

Barry Hendrix aviationgeek@bellsouth.net 470 422 9837	or	Melissa Emery memery@apt-research.com	or	Pam Kniess pamkniess@gmail.com 256.828 5467

Deadline for all registrations is July 15, 2014

Booth location selection will be offered by date of receipt of payment.

From the Editor's Desk...

JSS Technical Editor
Clif Ericson

Changes

At the last Executive Council meeting of the International System Safety Society (ISSS), a decision was made to temporarily reduce the number of *Journal of System Safety* issues to three hard copies per year. This measure was necessary in order to reduce expenses that are currently exceeding income. We'll continue to provide a high-quality journal by including a little more material in each issue to help make up for the loss. If more members would pay their dues and encourage non-members to join the ISSS, our income would increase enough to go back to the normal number of issues.

"...a decision was made to temporarily reduce the number of *Journal of System Safety* issues to three hard copies per year. This measure was necessary in order to reduce expenses that are currently exceeding income. We'll continue to provide a high-quality journal by including a little more material in each issue to help make up for the loss."

The first technical paper in this issue, "Using the Performance Specification Process in Hazard Elimination and Control" by Pamela Wilkinson, looks at performance specifications, which define the functional requirements for the product, the environment in which it must operate, and its interface and interchangeability characteristics. A performance specification states requirements in terms of the required results. However, a performance specification does not state the methods for achieving these required results. Performance specifications translate operational requirements into more technical language that tells the manufacturer what will be acceptable product performance and how that product acceptability is determined. System safety professionals can make use of the performance specification process to include those items that will verify the elimination or mitigation and control of a variety of hazards. This paper discusses the history and provides an overview of the Department of Defense performance specification process. It also provides guidance to the system safety professional in writing performance specifications and how to best use this process to verify that potential hazards have been eliminated or controlled.

The second technical paper in this issue, "Eliminating or Controlling System Risks via Effective System Safety Requirements and Standards" by Mike Allocco, looks at oversimplistic suppositions that occur when addressing system risks, when an analyst assumes that once single hazards are identified and hazard controls are applied, the job of a safety engineer is complete. Such a mindset is dangerous in that potential system accidents may not have been identified and mitigated. System accidents may be the result of many hazards that, under specific circumstances, form an adverse progression, resulting in harm. Consider that there may be systemic and synergistic risks associated with a system. Designers are generally concerned with meeting a customer's needs; however, in many situations, neither the customer nor the designer may be aware of systemic and synergistic risks related to a particular design. Experience shows that more than 50 percent of requirements are either not defined or not articulated clearly by the customer. Given that there may be non-apparent system hazards that present systemic and synergistic risks, how then are effective system safety requirements and standards developed to assure that system risks are eliminated or controlled to acceptable levels? This paper offers concepts, criteria and considerations to provide context and answer that question.

In his "System Safety in Healthcare" column, "Curing the Risk Management Process in Hospitals," Dev Raheja discusses the hospital risk management process, pointing out the simple fact that the risk management process itself in most hospitals is sick. The symptoms are clear, yet there are still more fatalities from medical mistakes than there would be if a jumbo jet crashed every week. Forty wrong surgeries occur each week, up to 30 percent of nurses have musculoskeletal injuries

from handling overweight patients, most hospitals are at a three-sigma level of quality, and there has been practically no reduction in the number of adverse events during the last 10 years. The medical system can be cured, but the system safety process needs to be applied.

In his "TBD" column, Charles Hoes presents three safety fairy tales. As with common fairy tales, they are based on factual events, but have muddled and incomplete descriptions of what happened and why. The purpose of fairy tales is not to frighten, but to point to universal safety messages that will hopefully keep us from future dangers. A common element of all three stories is a failure of human judgment and/or actions, which are ultimately likely the result of system design.

In the "Unintended Consequences" column, Terry Hardy discusses a fire that occurred on February 2, 2001, during which two employees of the Bethlehem Steel Corporation's Burns Harbor Mill in Chesterton, Indiana died. The accident occurred during work to remove a furnace that had been decommissioned in 1992, along with its associated piping. There are important lessons to learn from this mishap.

Dave MacCollum actually provides two "Design-Based Safety" columns for us: "Highjacking Shakedown" and "Scapegoats." As usual, both of these articles inform while delivering a touch of both prophecy and humor.

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

Until next time,
Clif

In Memoriam: Jimmy Keith Turner

We were saddened to learn of the passing of ISSS Member Jimmy Keith Turner. Turner was 64 and a resident of Tucson, Arizona.

The son of the late Jimmy E. Turner and Mary N. Turner, Jimmy is survived by his wife Atsumi and his younger siblings Gina Cummings of Memphis and brother, Glen Turner of Collierville. Jimmy, or "Keith" as he was known by family and friends, grew up in Memphis, Tennessee and graduated from high school there in 1967, attending Watkins S. Overton High School. He enlisted in the Navy in 1968 and was honorably discharged January 15, 1980 with the rank of Chief Petty Officer (E-7).

Jimmy held the position of chief fire control technician and was a leader in the field of system safety engineering, serving in many leadership roles within the International System Safety Society, and chaired the G-48 System Safety Standards Committee from 2005-2010. In lieu of flowers, the family requests a donation be made to the American Cancer Society (https://donate.cancer.org)

Mark Your Calendar

59th Annual Business Aviation Safety Summit (BASS) 2014
April 16-17, 2014
Sheraton San Diego Hotel & Marina
San Diego, California
http://flightsafety.org/aviation-safety-seminars

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

TBD

by Charles Hoes

This installment of my TBD column involves three safety fairy tales. As is common with fairy tales, they are based on factual events, but with muddled and incomplete descriptions of what happened and why. The purpose of fairy tales is not to frighten, but to point to universal safety messages that will hopefully keep us from future dangers. I doubt my thoughts will have the impact of a great Grimm's fairy tale, but maybe they can serve as stones on the path to improvement.

As I sit to write this, there are three big safety events sharing the front pages of current newspapers. While they are all different, I see important similarities. Because each of my fairy tales is based on current news, the descriptions and my guesses about the events are incomplete and almost certainly incorrect in many details — hence, the "fairy tale" nature of my stories. Still, even if it turns out that I am totally incorrect in all of the details, there may be some useful insights to be gleaned.

The first story is about a train, pulling many oil tankers, that ran away and crashed in a huge ball of flame in a small town in Canada. Apparently, the engineer had stopped for the night and gone to sleep in a nearby hotel. The train slowly started to roll back downhill, picking up speed until it derailed in the middle of a small town, bursting into flames, destroying a large part of the town and killing dozens of people. My first reaction when I saw the footage on the evening news was to turn to my wife and — half in jest — say that the engineer failed to set the parking brake before leaving the train for the night. After a couple of weeks, I am hearing stories in the news that, apparently, the engineer failed to set the parking brake. The reason given is that there was an earlier fire on the train, the fire department had messed with the brakes and the engineer failed to notice. Somehow, this led to his failure to properly set the brakes. This seems odd, but not knowing the details of the braking system, all I can do is wonder how that could occur.

The second story that has been given front-page coverage in California has to do with the broken bolts on the new section of the Bay Bridge designed to reduce earthquake risks. This is a slowly evolving story having to do with very large, very strong bolts snapping when tensioned. Of course, hydrogen embrittlement was the first thing that popped into my mind when I first heard about the snapping bolts. This seemed highly unlikely because of the well-known nature of the problem and the equally well-known solutions. Over the past couple of months since the initial event, much has been said about poor Chinese quality control, failure to perform proper testing/inspections on the bolts, etc. None of this made much sense to me, but lately the news has been getting a little more specific and it is starting to make more sense. The current story is that high-strength bolts were selected and that the bolts were galvanized to prevent corrosion. As we all know, galvanizing high-strength steel is a recipe for causing hydrogen embrittlement, which has now been identified as the cause of the bolt failures. A little bird whispered into my ear that once upon a time, a long time ago, an engineering study was performed on this aspect of the design with the recommendations that:

- High-strength bolts not be used in this application because of the propensity for hydrogen embrittlement failures
- Galvanizing not be used on high-strength steel (if used) because of the potential for hydrogen embrittlement
- Every item be individually tested and inspected if high-strength steel is used
- Bolts be protected with a specific type of epoxy material

Apparently, none of these recommendations was followed. By the way, that same little bird indicated that the current behind-closed-doors engineering meetings on the subject are deciding whether to open the bridge or tear it down because the same problem exists elsewhere in the structure in locations that cannot be fixed. As with

any good fairy tale, I have no validation of that last point — it is just a quiet rumor in the hallways. I assume the engineering review team will make the correct decisions.

The third story has to do with an airliner crashing upon approach at the San Francisco airport. Apparently, the plane came in a bit too low and slow, hitting the tail section on a breakwall and coming to a spectacular crash on the runway. "Luckily," only three people were killed (not so lucky, of course, for those three and their families and friends). The story in the news is that the plane was coming in above the glide slope, then it was below the glide slope. There was also a "stick shaker" event, warning the pilot of an impending stall. It appears that once it became clear that the plane was too low, the pilot "pulled" up, most likely right into a stall condition. It is my imagination that the maneuver not only caused the plane to stall and therefore lose more altitude, but it also changed the attitude of the plane, causing the tail section to drop even lower and allowing it to hit the wall. Of course, there is much more to be learned — such as what was going on to allow the plane to get into the incorrect orientation and speed in the first place.

"A common element of all three stories as I have related here is a failure of human judgment and/or actions. However, I doubt if any of the parties in these stories did anything 'wrong' or in 'error' in the sense that they *intended* to do one thing and did something else."

A common element of all three stories as I have related here is a failure of human judgment and/or actions. However, I doubt if any of the parties in these stories did anything "wrong" or in "error" in the sense that they *intended* to do one thing and did something else. My guess is that they were all highly qualified and experienced professionals who did exactly what they thought was the correct thing, and did it perfectly — with the intention of doing it safely. There were no "errors" in the sense of intending to do something but failing to pull it off, such as slipping on a rock when crossing a stream, and no errors from inattention, such as failing to notice the car next to you when changing lanes because of texting while driving. Rather, these all seem to be errors that were purposeful, thought out and intentional. In the first case, it may have been based on a mental model of the status of the train controls. The engineer almost certainly didn't "forget" to set the parking brake; he probably thought about it and was certain that it was set. In the second case, it wasn't that the management didn't notice the memos warning of the dangers of hydrogen embrittlement; it involved a reasoned decision that the memos were incorrect and that the danger did not exist. The third event seems to have involved a problem with the pilot's "mental model" of what would happen if he were to "pull up" at that particular moment. He undoubtedly thought that the plane would gain elevation so he could go around for a second try, rather than drop and rotate enough to cause the landing gear and tail to hit the wall.

It seems that we are faced with three more instances where the events immediately proximate to the accident point to "human error" of one kind or another, rather than to equipment design. With the possible exception of the bridge, the designs were "good" — the brakes would have held the train, the steel bolts had adequate strength, the flight control system did everything it was intended to do. Yet we still had huge economic and personal losses because of the failure of a person (or persons) to do the "right" thing. I contend that the design, the design process and the social pressures in existence during the design process led to these errors. They were not errors of judgment; they were errors evolving from the failure of the design team to fully anticipate the mental models of the people who make the ultimate decisions about which action to take.

As I sit and watch the news unfold on these events and "armchair quarterback" what could have been done to prevent these situations, it appears that we might be focusing too much on how things work (the mechanical and software side of safety) and too little on the mental models that we all use to successfully get through our days. A personal example might help clarify the point. When I was first learning to drive, I had one heck of a difficult time learning to shift smoothly. Finally, one day I saw a clutch assembly in my brother's shop and saw how it worked. It then was totally natural to shift smoothly — once I had the correct mental model, it was a piece of cake to do it right. Without that model, I was learning motions, but there were just too many variations for me to learn them all. It went from thousands of learned micro-actions to one consistent set of actions based on a complete mental model.

I think we need to spend more time considering and learning about the *psychology* of engineering. This includes the engineering processes themselves so that we avoid integrating bad ideas into designs because of group pressure or outdated understanding, as well as how people learn to acquire the correct mental models of how complex equipment works so that the "instinctual" reaction is the correct reaction.

Unintended Consequences

by Terry Hardy

Fire in Indiana

On February 2, 2001, two employees of the Bethlehem Steel Corporation's Burns Harbor Mill in Chesterton, Indiana died in a fire at the plant. The accident occurred during work to remove a furnace — and associated piping — that had been decommissioned in 1992. This batch furnace had been isolated from coke ovens through the use of a 10-inch valve. One month prior to the accident, a leak had been discovered in this valve, likely the result of water from the accumulation of coke oven gas condensate that had frozen and cracked the valve.

Two employees were assigned to remove the valve. They first installed a slip blind at the upper flange of the valve on January 5. However, this action allowed flammable condensate liquid from the coke-making process to collect in a deadleg upstream of the valve. On the day of the accident, the employees were to complete the job by replacing the blind and the cracked valve with a drain assembly. When they loosened the bolts around the blind, liquid began to seep out. Then, the liquid sprayed the employees when they further loosened the bolts. This liquid ignited, likely from an infrared heat lamp or a space heater being used in the maintenance operation. The two employees were engulfed in flames and died, while others in the area were burned from spraying liquid and the resulting fire.

The U.S. Chemical Safety and Hazard Investigation Board (CSB) found that the management systems for overseeing maintenance were inadequate, especially with regard to the decommissioning process. According to the CSB, the work should not have continued without a plan to control the hazards related to flammable materials. In addition, the employees who died had not been made aware of the hazards of this work, and they had not been informed of previous condensate incidents. The CSB also found that the employees could not easily evacuate the area once the emergency occurred because the escape routes had been blocked by demolition work. In addition, the company did not have a program to analyze hazards and implement safeguards related to decommissioning and demolition, according to the CSB.

"A majority of engineering efforts are focused on design, development and operation of systems. But at some point, systems will wear out, be damaged or become obsolete. Hazards related to the disposal of equipment are often different from those of nominal operation and must be evaluated."

Lesson Learned: A majority of engineering efforts are focused on design, development and operation of systems. But at some point, systems will wear out, be damaged or become obsolete. Hazards related to the disposal of equipment are often different from those of nominal operation and must be evaluated. Organizations should explicitly identify disposal and decommissioning hazards, plan for decommissioning early in the lifecycle and identify special procedures and equipment needed for handling and disposal.

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.system-safetyskeptic.com.

References

1. U.S. Chemical Safety and Hazard Investigation Board. "Investigation Report: Steel Manufacturing Incident (2 Killed, 4 Injured), Bethlehem Steel Corporation, Burns Harbor Division, Chesterton, Indiana, February 2, 2001," Report No. 2001-02-I-IN, January 2002.
2. Flint, L. "Chem Demil Plant Decommissioning & Closure System Safety Engineering Lessons Learned," *Proceedings of the 27th International System Safety Conference*, 2009.

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

Curing the Risk Management Process in Hospitals

The risk management process in most hospitals is sick. The symptoms are clear:

- There are more fatalities from medical mistakes than there would be if a jumbo jet crashed every week
- There are 40 incorrect surgeries performed a week
- Up to 30 percent of nurses have musculoskeletal injuries from handling overweight patients
- Most hospitals are at a three-sigma level of quality
- There has been practically no reduction in the number of adverse events in hospitals during the last 10 years

The system can be cured, but we need the right caregivers, including surgeons and physicians, who can cut out the non-value processes and replace them with high-value transplants.

Why is the Risk Management Process Broken?

Bad stuff happens; anticipated events don't unfold as planned and unanticipated events occur. Remarkable numbers of "near misses" still occur routinely. Most caregivers have neither the time nor the willingness to report on their own mistakes. Moreover, these near misses are typically invisible to patients and administrators. That is why hospital mistakes are 10 times the level that is reported [Ref 1]. The main function of risk management is to deal with this negative aspect of uncertainty.

Managers with no formal training in risk management seem to be largely responsible for many of the ad-hoc approaches to risk management. A particular favorite of these folks is ad-hoc scoring methods that involve the ordering of risks based on subjective criteria. The scores assigned to risks are thus subject to cognitive bias. Even worse, some of the tools used in scoring can end up ordering risks incorrectly. Bottom line: Many of the risk analysis techniques used have no justification.

The Process Can Be Fixed

Whether health care risk management "best practices" are outdated or not, we can fix the process. It is about looking outside the box to other industries. Even though hospitals have imported crew resource management from the aviation industry and the FMEA from the Department of Defense, there is a lot more to learn from the aerospace, nuclear, automotive and chemical industries. Best practices must be built and doubted at the same time. We use them not because they are perfect, but because we feel secure in the company of peers. If you simply ask, "Can anything go wrong with the best practice?" in an M&M conference, there will be more unresolved issues than the number of people attending. Brainstorming with a diverse group and looking for what can possibly go wrong is one of the best ways to identify risks. We need to re-think risk management. The sound principles of risk management, coupled with innovative solutions, can assure high return on investment. These principles are:

- Identify risks
- Assess risks
- Mitigate risks
- Orchestrate risk management
- Aim at high return on investment (ROI) without compromising safety

One topic in this list, "orchestrate risk management," is the least-discussed topic in risk management. Another topic, "aim at high ROI," is highly misunderstood. It is worth the time to explore them.

Orchestrating Risks

The statistics from The Joint Commission, The National Committee for Quality Assurance, National Quality Measures Clearinghouse and National Quality Forum show that patient safety and quality movement has been a great failure, according to Lucian Leape, the originator of the patient safety movement. They show that the current effectiveness of risk management functions has been, at best, marginal. Hospital managers often prevent mishaps after the damage is done. It is

not their fault, since most of them are never exposed to the best techniques used in aerospace. They rarely use formal and structured safety analyses, nor are most managers familiar with the tried-and-tested mitigation techniques used in aerospace. But what is missing in risk management is risk orchestration, which is making sure the right things are happening at the right time when a patient is in the path of the harm. In other words, the role of a risk manager should be like that of a symphony orchestra conductor who makes sure every musician plays his or her piece at the right time and in synergy with fellow musicians.

Take the situation of the 18-month-old baby Josie King, in which all the caregivers were too engrossed doing their own things while she was dying from dehydration [Ref. 2]. The staff administered wrong medication, even when the mother protested. She told them that Josie needs fluids, not methadone, a narcotic pain medication. The nurses and doctors both ignored her requests. One thing led to another and Josie wound up with cardiac arrest and two infections. This happened in the nation's No. 1 hospital. The question is, who was making sure that the doctors and nurses did the right things at the right time to manage the risk? The risk manager was only involved later, when the parents decided to take legal action. In our vision, the risk manager does not have to personally monitor all risks, but the risk manager should delegate this responsibility to a staff member trained in risk management for every patient in critical care. This is one way the nurses, physicians and support staff can orchestrate their work to play to the same music.

The orchestration process requires a sustainable structure for sound risk management. This structure should include the integration of support staff. Once the structure is there, rehearsals must also be there as evidence that the orchestra is prepared for the performance.

Creating a Sound Structure

"A structure represents the basic characteristics of physicians, hospitals, other professionals and other facilities," said Dr. Carolyn Clancy, head of the Agency for Healthcare Research and Quality (AHRQ), in her testimony before the U.S. Senate Committee on Finance, Subcommittee on Health Care [Ref. 3]. "It describes whether there are well-educated health professionals, appropriate hospitals, nursing homes, and clinics, as well as well-maintained medical records and good mechanisms for communication between clinicians. For example: Is the mammography equipment up to date and maintained properly? Are the cardiologists well trained and board certified? If the structure is solid, we can concern ourselves with the process of medical care. Concern for process suggests that quality is determined not just by having the right people and facilities available, but also by having the right things get done in the right way."

She defines health care quality as getting the right care to the right patient at the right time — every time. The implementation of this vision is a sound structure. In addition, there must be safeguards if an activity is not performed correctly. These are the core activities.

A structure should also include a "thank you" system to employees who are fully engaged and willing to walk an extra mile. The Gallup organization measures what percent of employees are engaged, what percent of employees are not engaged, and what percent of disengaged employees can harm the patient from carelessness. Most of the hospitals have less than 35 percent employees who are engaged. Teams should be rewarded for failure-free performance over time. Reward nurses who go out of their way to help families in grief. Seek peer opinions on decisions made with good understanding. Use this data to also improve the system.

Integrating Support Staff

Make sure that the support functions are well integrated. If the support staff is not integrated with mainstream activities, the music will not happen correctly. Imagine if a musician shows up, but because of a glitch in transportation, her piano does not. The same thing can happen when a device fails during surgery and nobody can locate the back-up device, or the back-up device is also not functioning. Someone needs to be in charge of making sure the support services are there when needed.

Support functions include the right medical technicians with an adequate supply of gowns, needles, sanitized wheelchairs and surgical instruments, as well as all emergency care providers. Make sure the housekeepers who disinfect patient rooms have a basic knowledge of infection control and know which chemical to use for which objects in the room. In a surprise visit by the Joint Commission, all of a hospital's housekeepers were questioned about their knowledge of infection and chemicals. No housekeeper had satisfactory knowledge.

Conducting Risk Management Rehearsals

There is no way to trust the outcome of a symphony without a rehearsal. The same strategy applies to health care. In aerospace and aviation, the rehearsals are called emergency drills. They can be used to verify that patient emergencies, such as cardiac arrests and strokes, can be handled flawlessly. In health care, we need to go the extra step of rehearsing for selected non-emergency situations also, such as listening to the patient's family, administer-

ing the right medication in a timely manner and making sure physicians are available in reasonable time, in spite of distractions and poor communications. These are precursors to a real emergency.

Some ideas for emergency drills are:

- Have a person pretend to have a heart attack and suffer from MRSA infection at the same time, and observe the events with a video that can be used as a training tool later
- Send in about 100 patients to the emergency department (ED) as if they were being transported from a train accident in the city and videotape the care
- Create an emergency where the surgeon is very busy and highly distracted
- Conduct drills on day-to-day tasks, such as taking a patient for an MRI from the emergency room
- Simulate a dummy fire in the ED and observe how the patients are protected from risks

Ideas for non-emergency, but relevant situations include:

- Send a wrong label on a medication to designated staff and observe how the defect is caught prior to administering
- Send a wrong dose, such as heparin 5000 instead of heparin 1000 to a pediatric ICU
- Send a defective ventilator that gives more respiration than indicated. Observe if this is noticed by the staff
- Follow a patient complaint with the patient. Same for a complaint from a patient's family member
- Put an epidermal solution instead of an injection solution in a surgery set-up to verify if the staff can reject the solution
- Follow the actions of the staff when a patient needs the doctor immediately, but the doctor is not available

A risk manager can choose to assign the risk management rehearsals to the quality assurance department or to the patient safety officer. The important thing is to make constant system improvements from this data. Occasionally, an independent outside team should audit how good the risk management strategy is, and how well it is implemented. This process is a formal process in aerospace. Another positive action is to take a look at adverse and never events. Find out the deficiencies in knowledge and execution. Then, make system changes.

Aiming at High Return on Investment Without Compromising Safety

Safety and high return on investment are not opposite goals, if you compare the total cost of doing the right thing versus not doing the right things over a period of at least five years. Sometimes, it is hard to put numbers on intangible benefits, such as getting more customers, avoiding negligence claims and avoiding patient harm. But a good manager can see them intuitively. Usually, employees already have a cheap and simple solution. Toyota Car Company calls such solutions "elegant solutions." Dr. Peter Pronovost's simple five-point checklist for preventing the central line-associated bloodstream infections at Johns Hopkins helped hundreds of hospitals. It saved thousands of lives and millions of dollars with hardly any investment.

Conclusion

It is a good practice for senior managers to ask the following questions:

1. Are the current best practices really the best?
2. If they are not the best practices, do the employees know that these methods are ineffective?
3. Do employees know the consequences if these practices don't work?
4. Are current practices good enough when a disaster, such as a tornado or an earthquake, strikes?
5. Do employees understand that humans will make mistakes and patients must be protected from the consequences of mistakes?

Answering these questions is a good place to reinvent your own risk management process. Let us also not forget the words of Thomas Edison, who said, "There is always a better way. If we all did the things we are capable of, we would astound ourselves!"

References

1. Kenen, Joanne. "Medical Errors Occur 10 Times More than Previously Thought," *AARP Bulletin*, April 7, 2011.
2. Pronovost, P., and E. Vohr. *Safe Patients, Smart Hospitals*, Hudson Street Press, 2010.
3. Clancy, Carolyn. "What is Health Care Quality and Who Decides?" Testimony before the U.S. Senate Committee on Finance, Subcommittee on Health Care, March 18, 2009, http://archive.ahrq.gov/news/speech/test031809.html.

Design-Based Safety

David MacCollum

Scapegoats

Rare tragedies with terrible unintended consequences are usually preceded by a history of denial of a past series of related hazardous conditions. Thomas Bayes was a minister better known for his mathematical doctrine of chance, in which a number of similar hazards can become active at the same time to produce disaster. Civic leaders are usually unable to perceive how similar hazards can combine and create a colossal danger to the public. When noted authorities warn of danger and the need for costly safety features, community leaders often try to avoid imposing such costs on the community. When a tragedy does occur, those who could have made a difference often welcome an excuse to avoid accountability. That's when a scapegoat becomes an acceptable choice.

Community leaders do not relish having to develop detailed engineering analyses of the specific hazards and appropriate alternate safer designs and/or provisions for safety accessories. The real truth that could absolve the alleged scapegoat of guilt may never be known, or may take years to expose.

A classic example of scapegoat syndrome is the 1970 Pioneer Hotel fire in Tucson, Arizona. A black teenager named Lewis Taylor was convicted after a seven-week trial on circumstantial speculation in a case of arson in which 28 people were killed. A scapegoat becomes an acceptable alternate. Since 2003, a voluntary Arizona Justice Project involving a former Arizona State Supreme Court justice and several prominent attorneys has been working to free Lewis Taylor from a wrongful conviction. This group has found no factual evidence that Lewis Taylor started the hotel fire. A current county prosecutor has issued a no-contest ruling freeing Lewis Taylor, who spent 42 years in prison for a crime he contends he did not commit. The prosecutor did not want an unwinnable trial presented by the Arizona Justice Project and made a no-contest ruling — which does not erase the alleged guilt of Lewis Taylor; it simply lets him out of prison.

But this article is not about the conduct of our justice system. It is a review of the related design hazards that allowed a fire to race at a devastating speed to the top of an 11-story hotel building. Newspaper articles and other reports list the following hazardous conditions in the hotel building before the fire in 1970:

- No sprinkler system
- No smoke detectors
- An open stairwell that served as a chimney that would flood the building hallways with smoke
- Flammable decorations and drapes in the assembly rooms, without flame-proofing treatment
- Twenty-two inches of walls from the floor up were covered with flammable carpeting, and the remainder of the walls were covered with a combustible vinyl material
- Poorly designed fire escape system accessible only through hall windows and hotel rooms

These conditions made the hotel building a veritable furnace that could be ignited from many sources of mechanical or electrical failure.

For instance, heat from a small fire of paper trash in a cigarette ashtray in a building hallway can generate enough heat to create flashover to ignite any nearby flammable materials, such as — in this case — the flammable wall carpet. The National Fire Protection Association (NFPA) has, since the early 1900s, developed fire life-safety codes for municipal, county and state agencies to adopt. The six hazards listed earlier are well-recognized hazards that can be overcome at the time of design or when remodeling an existing building.

The building's owners had two choices: rely on insurance if a fire occurs or spend money so the building would be in compliance with NFPA standards. In this case, the choice was made to opt for the lower annual insurance premium. However, an investment to ensure compliance with NFPA standards would have resulted in a much lower long-term annual insurance premium that, in time, would have paid off any investment in life-safety fire protection and ensured the safety of the hotel's occupants.

In addition to failing to comply with the NFPA's life-safety standards, hotel management appears to have given lip service to ensuring fire-safety practices when it:

- Locked the doors to the third floor to prevent exiting from the upper floors to the mezzanine (ballrooms) and down to the first floor (lobby)
- Provided iron grills for the Penthouse windows that *could not be opened from the inside* to allow escape to the open roof in the event of smoke or fire
- Refused to treat the drapes in the hall conference rooms with fire retardant
- Stored materials on the exit stairways
- Attempted to extinguish two previous fires before calling the fire department
- Made no effort after two attempted *arsons* occurred to conduct a follow-up investigation to locate the wrong-doer

"When inappropriate decisions are made by individuals who lack qualifications to rule on issues in which they have had no formal training and/or experience, a social environment in which serious error will occur is created. When those who are unqualified err and the loss of life and property occurs, the temptation to identify a scapegoat becomes apparent. The Catch 22 is that when a criminal action is called 'arson,' liability for gross negligence is eliminated. Then, no one is responsible for paying for the damage."

Analysis of the failure of the hotel owner and elected city officials to require compliance with NFPA standards and operational fire safety practices shows clearly that their misplaced management priorities created an inability to ensure public safety. It is criminal to rely on personnel with no engineering qualifications and no understanding of fire safety design criteria or operational safety to be the watchdogs to protect the public. The very reason that doctors, engineers, nurses and dentists are licensed is to prevent the unqualified from making decisions that are outside their expertise. When inappropriate decisions are made by individuals who lack qualifications to rule on issues in which they have had no formal training and/or experience, a social environment in which serious error will occur is created. When those who are unqualified err and the loss of life and property occurs, the temptation to identify a scapegoat becomes apparent. The Catch 22 is that when a criminal action is called "arson," liability for gross negligence is eliminated. Then, no one is responsible for paying for the damage.

Dodging these issues by incriminating a scapegoat after a disaster continues to occur. After the recent massive explosion at a Texas fertilizer plant, it was reported that an individual was arrested on charges that authorities stressed were not linked to the deadly blast. Is this the first step in placing blame on a scapegoat? Before a disaster, those who have a responsibility to ensure the safety of the public and do nothing are those who, after the disaster, look for scapegoats.

System safety analysis needs to become a standard that reaches far beyond the limited scope of MIL-STD-882. The design and construction of all new large facilities, such as skyscrapers, manufacturing plants, fast-rail passenger transportation, mining and many other enterprises, need to include a system safety engineering analysis that is made available to the public. The good news is that some progressive design-and-build construction firms have adopted system safety concepts, usually under other names. This approach removes the opportunity for unqualified organizations to make design-safety decisions, and with it, the temptation to find a scapegoat when they err.

Design-Based Safety

David MacCollum

Hijacking Shakedown

Are challenging new private-sector projects on environmental hazards becoming blood sports? Have environmental safety issues become a pervasive socially acceptable reason to confront and badger our federal, state and local authorizing agencies to delay, block or reject the development of huge new projects? Are public hearings on new pipelines, energy development and mining just tools to remove the welcome mat to private-sector industrial development? These three questions have led to my strong suspicion that our empire-building enterprises are being hijacked by a shakedown. This abusive politicizing of environmental and safety concerns appears to be highway robbery of our economy, reducing our middle class and contributing to growing poverty because there is a lack of well-paying employment.

It appears to me that a messenger is needed to overcome this unwarranted attack on private enterprise. The most likely envoy is a system safety engineer who can convey the fact that design-based safety was able to land people on the moon and ensure their safe return by eliminating monstrous hazards. This same design-based safety expertise can eliminate environmental hazards. Most people are totally unaware of the fact that the dramatic growth of green engineering provides environmentally friendly design. Several articles in the August 13, 2013 issue of *Engineering News Record* (ENG) tell how large contractors are benefiting from safety programs that focus on safe design. New multi-million dollar projects are really complex systems with many hazards arising from different priorities. Large international construction firms apply these same key principles of system safety by examining the proposed plans to identify each and every hazard, and provide a reliable, safer design, use safety appliances or adopt a safer method so that the entire system becomes hazard free. These system safety programs have demonstrated the effectiveness of reducing both environmental and human hazards. However, these positive results are concentrated among larger firms, with little input for the public.

During the last decade, green engineering services worldwide have grown from $30 billion to more than $50 billion [Ref. 1]. The reason for this amazing growth in design-based safety, construction safety management and lifecycle project safety management is that these large firms could not sustain the high cost of environmental damage and injuries to people with insurance. The losers are those proposed projects experiencing hijacking shakedowns from special interest groups that want to prevent them from starting. These anti-development fanatics display charismatic ignorance in their drive to delay or reject projects for environmental and safety reasons. With this no-go political ideology, a significant amount of new development never occurs and green system safety engineering has no chance to prove its worth.

The message to those who "cry wolf" is that they are the culprits who are preventing the green engineering market from reaching $100 billion a year and causing our country to endure a continuing poverty economy. Absent in the anti-development pronouncements is any cooperative participation or acceptance of design-based safety. Their intent is to kill pipelines, gas and oil development, and mining as they ignore the existence of technology that will protect the environment. These self-proclaimed environmentalists are like Gulliver's six-inch-tall Lilliputians, always at war or talking about how they will capture corporate America. Their strategy is to impose needless costs for every proposed project by calling for groundless reviews and investigations, and making speculative allegations to cause costly delay after delay. Their goal is to bankrupt their corporate victim so the project is discontinued.

The proliferation of not-for-profit special-interest groups has politicized new project approval so that reason and fact are often excluded. The opponents' battle cry is to cite environmental hazards created nearly a century ago and allege that these same hazards will start all over again with the new project. These special-interest groups ensure that environmental science is never relayed and is artfully concealed from the public.

The media are often the worst offenders. They rely on yellow journalism to report unsubstantiated speculation about the environmental damage that new pipelines, oil and gas wells, and mines will produce. It is said that the journalists who publicize the outlandishly biased statements of the opposition are favored for authoring this propaganda. One only needs to read newspapers to become aware of a senseless furor to prevent mining on land that is worthless for grazing and ill-suited for camping or recreation.

To become effective system safety messengers, we also need to become aware of how our tax system clouds the issues of design-based safety. Taxation appears to be an easy method to delay or stop the development of new private-sector projects. The traditional practice of giving corporations the same treatment as real living persons hinders design-based safety. When profits are taxed twice — first on the non-person corporations and again on the individual who is a real-person investor — an oxymoron is created. In my opinion, a two-class society of earned and unearned incomes is not working. We need a trade-off of taxing only real people's incomes regardless of how that income was acquired (by labor, investment, royalties, etc.). It becomes a joke to even tax non-person corporations, as most large firms avoid profit taxation with politically granted exemptions.

To develop middle-class participation in capital growth, our individual retirement account (IRA) programs that make savings for retirement tax free appear to be working, as they provide investment capital for new environmental-safety projects. When new projects use public lands, the public is entitled to a fair market-price royalty on (1) products mined, (2) use of land for grazing and (3) sales tax on products to pay for services (gas tax to fund roads and highways).

The reason for including the controversial subject of taxation in design-based safety is so that sustainable costs can be calculated on the design and management of private-sector project development. Bankers are the gatekeepers of investment capital. They are suspect of market manipulations of hoarding metals to drive up prices in the futures market. Civil lawsuits may occur, but they are slow in coming up with the facts. Meanwhile, uncertainty about the market price for raw materials prevails.

This is all just to say that good system safety engineering is not enough, as politics and economics are foreboding obstacles. For these reasons, the system safety engineer has an important role in coordinating the design-based safety features with employers or their clients. It is more important that the system safety engineer describe, in lay terms, how these features will reliably prevent environmental and people hazards. Facts showing how system safety will make the project safer need to be presented. Each hazard needs an explanation as to how a mechanical or other physical feature will eliminate that hazard. People need to know how sensors and detectors can automatically interrupt the activation of a hazardous condition. Further, the re-evaluation of a rare event's prevention needs to be included, as overlooking a rare event because it is low risk is contrary to basic reliability mathematics.

“...good system safety engineering is not enough, as politics and economics are foreboding obstacles. For these reasons, the system safety engineer has an important role in coordinating the design-based safety features with employers or their clients.”

The role of the system safety engineer is that of a messenger in defining — in simple language — how improved design reliably works. This critical information becomes the tool that management can use to counter wrongful statements publicized by the media. Industrial management cannot afford the proliferation of false propaganda that incites fear in the general public. Management must develop its own corps of journalists who, in their reporting, cross-examine those in opposition and reveal how their allegations are not factual.

Design-based safety is the vehicle that will advance the professional status of system safety engineers as they expand their role by being the messenger and key information person in stopping the senseless hijacking shake-down of new enterprises so our nation can return to its former prosperity. I believe the good news is that within the next decade, the international environmental marketplace will double. This will provide many new careers for system safety engineers who will become skilled messengers to the private sector.

References

1. Hickoc, Stephen. “Looking at Markets — Looking at Global Regions,” *Engineering News Record*, p. 36-52, August 13, 2013.

Northeast Chapter

The annual summer meeting of the Northeast Chapter of the International System Safety Society was held on June 20, 2013 at the Go-Fish restaurant in Mystic, Connecticut. The summer meeting facilitated the Society Year (SY) 2014 elections by a plurality vote of the membership. The newly elected Executive Council (EC) includes President Scott Beecher (Scott.Beecher@PW.utc.com), Vice President James Krodel, (James.Krodel@PW.utc.com), Treasurer Cliff Parizo (CParizo@Sikorsky.com), Secretary Pamela Alte (Pamela.Alte@Sikorsky.com) and Events Coordinator Charlene Huberdeau (Charlene_Huberdeau@Raytheon.com).

The past and present EC would like to express the Chapter's appreciation to Ron Bartos of Raytheon, Richard Anderson of Sikorsky and Alan Southwick of Raytheon for their service on the nominating committee.

The EC would also like to thank outgoing President Alan Southwick for all his hard work growing the Northeast Chapter and hopes he stays involved as the chapter president emeritus!

Summer General Chapter Meeting — An exceptional lecture on "ARP4754 Revision A – The Latest in Aircraft Systems Safety" was presented by Andrew Gagnon. Gagnon is manager of the Systems and Requirements Integration department at Pratt & Whitney and is formally trained in ARP-4754A. He has experience in both military and civil aircraft domains, and is currently Pratt & Whitney's Engineering Process Group leader.

Pratt & Whitney's Andrew Gagnon gave a lecture on "ARP4754 Revision A – The Latest in Aircraft Systems Safety" at the Chapter's summer general meeting.

The newly elected Northeast Chapter Executive Committee is, from left, Pam Alte, Cliff Parizo, Scott Beecher and Jim Krodel.

At the conclusion of the Chapter meeting, the Chapter Scientific Award — given to the Chapter member who has contributed significantly to the advancement of the system safety profession during the past year — was presented to Pamela Alte. Alte received the President's Award in recognition of her significant contributions to advancing the recognition of the International System Safety Society, the Northeast Chapter and the system safety profession.

The President's Award is given to the Chapter member who, during that Chapter year, has contributed the most to the Chapter's success. Charlene Huberdeau received the President's Award in recognition of her significant contributions to furthering and revitalizing the International System Safety Society's Northeast Chapter.

The Chapter is already working on its Fall general meeting. Topics are being reviewed now. Highlights from the 31st International System Safety Conference (ISSC) in Boston will be shared.

Central California Chapter

The ISSS Central California Chapter was pleased to support the 28th Annual Central Coast Science Fair on May 31 and June 1, 2013. The science fair is organized by the Endeavour Center, a Central Coast teacher's resource and student outreach center, and the American Institute of Aeronautics and Astronautics (AIAA) Vandenberg Section. More than 84 students from Lompoc Unified School District entered 100 projects. The Central California Chapter provided financial support, helped with

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

"Proper Processes"

Assurance	Identification
Concepts	Levels
Control	Performance
Design	Requirements
Developments	Review
Directive	Sequence
Dynamics	Standards

(Answers on page 35)

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

set up and judging, and presented awards consisting of Certificates of Recognition from the ISSS and special VIP bags generously provided by NASA. ISSS Certificates and NASA VIP bags were awarded to, sixth-grader from Miguelito Elementary School sixth-grader Kayla Thompson for "Which Wrap Traps," Vandenberg Middle School seventh graders Maggie Farrington and Tess McIntyre for "Are Cats Mostly Left or Right Pawed or Ambidextrous?" and Vandenberg Middle School seventh graders Tristin Fichtner and Graham Richards for "Does Age and Eye Color Affect the Speed of Adaptation to Dark Vision?"

The keynote speaker was Col. Shahnaz Punjani, 30th Launch Group commander at Vandenberg Air Force Base. Col. Punjani provided a presentation on how science touched her life and career path, a topic well-suited to the audience.

Singapore Chapter

The Singapore Chapter celebrated its 10th anniversary on Oct. 29, 2013 at the YMCA's Lee Kong Chian Auditorium. The celebration started with a system safety workshop held in the afternoon session, which was attended by 95 participants. During the workshop, Clifton Ericson gave a safety presentation and then joined the Chapter's EC members in a two-hour round table discussion with the participants.

The celebration concluded with an appreciation dinner event, where the supporters of the Chapter were invited to celebrate a decade of joint efforts in promoting system safety. Among the guests were former EC members and the working superiors of the EC members who have been supporting the Chapter's activities in one way or another. Chapter Founder Onn Eng Ling gave a reflection on the Chapter's progress and achievements. She was joined by Chapter President Ten Lin Mei, who gave an overview of the Chapter's goals for 2014-2015.

Sidney Dekker spoke to the Singapore Chapter about "Safety Culture."

The invited speaker, Sidney Dekker, also gave a light-hearted presentation on Safety Culture and he surprised everyone with a spontaneous piano-playing when he spotted a piano on the stage after the presentation. The Chapter is thankful to its presenters, volunteers, participants and all guests who have turned up for the events.

Gains from Losses

John Livingston

The Importance of an Active and Robust Working Relationship Between System Safety and Engineering

The next few columns will address the importance of an active and robust working relationship between system safety and engineering. While the importance of this relationship is an often-stated axiom, post-accident assessments continue to cite causes reflecting shortcomings in system safety and engineering efforts that are rooted in either a lack of the basic exchange of knowledge or in the mutual utilization of that knowledge for the identification and control of project hazards and safety risk assessments.

These columns will take an ephemeral look at the key relationships between engineering and system safety efforts during a project's lifecycle. The references cited provide more detailed insight into each discipline, and I welcome the contribution of additional sources. Because of the nature of my personal experience and the references that will be used for examples and source information, these columns will have a strong aerospace flavor. In general, it is not the nature of the enterprise, but the complexity of the individual projects that fuels the challenges to the system safety/engineering relationship.

Highly complex systems are becoming more common, which only increases the need for a truly integrated effort. Areas of specialized knowledge and discipline expertise must be molded into one joint effort that addresses all aspects of the project, its hardware and its operation.

These columns will be divided into three general project phases: concept development, design definition and program operations. This column on concept development will offer an overview of the respective roles of each discipline and suggest areas of mutual interest, as well as the advantages of coordinated efforts.

Concept Definition Goals and Objectives

There are many important goals and objectives for engineering and system safety during the concept definition phase. Engineering plays a key role in the development of the system architecture, defining technical requirements, leading the evaluation of design trade-offs, including associated technical risk of the different options, and the establishment of the roles and tasks that engineering will perform for the balance of the project lifecycle [Ref. 1]. Major tasks for system safety include the development of initial safety requirements and risk management criteria, the performance of trade studies that evaluate hazardous conditions or concept options with high risk sensitivities (with recommended alternatives) and the identification of safety tasks that will become the core of the system safety and risk management efforts during system definition, design, manufacture, test and operations [Ref. 2].

While each discipline's approach and specific objectives may vary, the commonality of the major tasks allows us to structure our discussion into three general topics: development of discipline requirements, discipline trade studies, and planning for the next stage of the project development.

Requirements Development

System Engineering — The initial engineering requirements based on the assigned project objectives should be part of the project lifecycle kick-off. These top-level engineering requirements lead to a set of baseline requirements, which include supporting derived requirements. For most efforts, the derived requirements will make up the great majority of the engineering requirements on the project. Project engineering requirements should address the total lifecycle and cover all design aspects. The details of the derived requirements closely interact with the development of the concept details. The "established" concept should be based on a "converged" set of engineering requirements that are both understandable and verifiable. It is also important that they are placed under program control and that traceability of their origin is maintained. It is not usual for conflicting project engineering requirements to occur, necessitating project -level trade studies to assure that resolutions provide the best possible balance between project goals and sound engineering principles [Ref. 3].

System Safety — The first step in developing project safety requirements is the definition of what

is an acceptable safety risk, along with the factors and conditions that present unacceptable accident/mishap risks. These definitions provide a program baseline for forming design criteria and assessing the suitability of proposed candidate solutions. Requirement sources include (but should not be bounded by) historical experience with similar systems, associated trade studies and related hazard analyses. Requirements may be inherited (or imposed) from outside sources, but all should be carefully evaluated for applicability to the concept under development.

The basic safety philosophy and associated design requirements should be established prior to initiation of any hazard analysis tasks. A lack of standard or benchmark safety requirements can lead to reactive (operational) controls, rather than design "corrections." Opportunities to develop solutions that offer the most productive reduction in potential risks are generally the greatest at the concept development stage with minimum impacts [Ref. 4]. As the project progresses, design options decline and costs increase.

It should be remembered that safety requirements include both deterministic and risk-informed requirements: "A deterministic safety requirement is the qualitative or quantitative definition of a threshold of action or performance that must be met by a mission-related design item, system, or activity in order for that item, system, or activity to be acceptably safe. A risk-informed requirement is a safety requirement that has been established, at least in part, on the basis of the consideration of a safety-related risk metric and its associated uncertainty" [Ref. 2].

Trade Studies

In this series of discussions, we will use the general definition that "a trade study is an objective comparison with respect to performance, cost, schedule, risk, and all other reasonable criteria of all realistic alternative requirements; architectures; baselines; or design, verification, manufacturing, deployment, training, operations, support, or disposal approaches" [Ref. 5] with the important caveat that "risk" evaluations include system safety trade assessments. The trade study effort is an important part of any project and evolves as the project moves through its lifecycle. As the details of the system emerge, the resolution of the trades becomes more specific and the linkage to the project more complex. At any stage of development, the quality of the trade studies is directly dependent on the knowledge, skill and range of expertise of the participants. Also important is the leadership of the trade study efforts and their role in the progress of the project toward an optimum system design.

Engineering — Design concept trade studies are an important part of the engineering process used to support the development of a concept that provides the best combination of effectiveness and cost.

In this discussion, we will use the following NASA definitions [Ref. 1]:

- **Effectiveness:** The effectiveness of a system is a quantitative measure of the degree to which the system's purpose is achieved. Effectiveness measures are usually dependent on system performance.
- **Cost:** The cost of a system is the value of the resources needed to design, build, operate and dispose of it.
- **Cost-effectiveness:** The cost-effectiveness of a system combines both the cost and the effectiveness of the system in the context of its objectives:
  - While it may be necessary to measure either or both of those in terms of several numbers, it is sometimes possible to combine the components into a meaningful, single-valued objective function for use in design optimization
  - Even without knowing how to trade effectiveness for cost, designs that have lower cost and higher effectiveness are always preferred

In the most favorable situation, the design trade studies will start within the project-acceptable cost/effectiveness envelope. There are design options that either reduce cost while still maintaining the project effectiveness requirements or improve the project effectiveness while staying within the cost boundaries. In the best of both worlds, there are design solutions that improve project effectiveness and reduce costs at the same time. Much more likely are project design alternatives that trade cost for effectiveness or effectiveness for cost. The most challenging outcomes are presented by trades that have only alternatives that fall outside the cost or effectiveness boundaries.

Additional factors that must be considered include the fact that for most complex systems, the total design effectiveness is composed of system, sub-system and component factors that may have conflicting attributes. With any option, the quality of the supporting knowledge must be considered. These potential uncertainties add another dimension to the trade studies. It should be no surprise that numerous trade studies are required for major projects.

System Safety — System safety trade studies should be a part of the process of concept development and a factor in concept selection. The objective of the safety concept trade studies is the evaluation of potential hazards associated with concept candidates both in terms of the hardware and the operational characteristics. This

evaluation should include associated risk sensitivities for the different options and the safety recommended alternatives. The evaluation also provides support for any formal concept hazard analyses and risk assessments that assess potentially hazardous systems. The trade studies provide insights that aid in the development of the initial safety requirements and risk management criteria. The effort should also identify any follow-on special safety studies and risk assessments that may be required during system definition or design.

Project Development Planning

Engineering — Engineering has a major role in planning the technical effort for the balance of the project, based on the results of the project concept definition phase and traditional engineering roles. Project activities that should be addressed in the planning for the continuing engineering support include [Ref. 1]:

- The identification and definition of the technical effort required to satisfy the project objectives and lifecycle-phase success criteria
- The engineering roles in the project technical reviews and technical issue assessments
- The validation of the project technical requirements
- Support for the development of any enabling new technology associated with the concept selected
- The engineering role in the project technical risk management activity, including risk tracking and control functions (risk mitigation actions)

While some of the activities are extensions of the concept definition phase engineering efforts, it is important that all engineering support efforts are addressed in terms of the project lifecycle effort. For example, the verification and validation (V&V) of project technical requirements is a fundamental part of the project technical integration that has roots in the concept development. The details of the process (test, analysis, demonstration, inspection or similarity engineering) will emerge as the project design matures. Proper planning is important because of the relationship with the selection of specific technical requirements and its role in other project aspects, including cost and schedule. Because V&V will be required at the component, sub-system and system levels, it is important that the systems engineering team develop a top-level verification plan early in the project development cycle [Ref. 3].

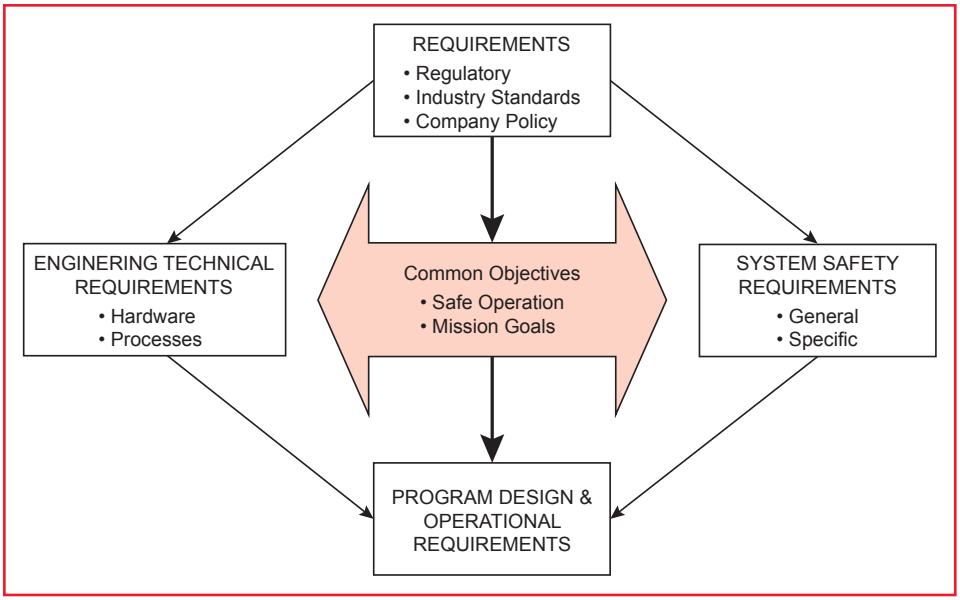


Figure 1 - Concept Requirements Development.

System Safety — System safety planning for the next stage is an important part of the concept development activity. Planning for the project development stage should reflect the project system safety program requirements that originate from many different sources. Government regulations, company policies and customer requirements all play a role. The knowledge gained from the concept definition activity should also be factored into the planning. Part of the planning activity should be the establishment of safety and risk goals and objectives that will be used to determine the safety and risk inputs for the overall program. The goals should be measurable, and the related safety tasks and risk management tasks should be clearly identified. Each task should be constructed in a manner that will demonstrate that its respective goals have been met. The development of the planned safety activities should also include estimates of the personnel requirements for the safety program for the balance of the project lifecycle [Ref. 2].

Common Interests

Early and direct involvement in any project or program is critical to the success of project support for the engineering and system safety disciplines. The three major concept development efforts discussed have activities that have strong parallels (and interfaces) between the two discipline efforts. These common interests offer the opportunity to improve each effort and the overall welfare of the client project.

Figure 1 illustrates the general flow of concept requirements development. While each discipline provides unique contributions to the requirements development, they share the common objectives of assuring

safe operation and the achievement of the project's mission goals.

Many of the project technical requirements are drivers for system safety requirements. It is important that system safety practitioners have knowledge and understanding of project technical requirements. This knowledge can be enhanced by direct contact with the engineering discipline experts and the project system engineering staff. It is also important that the project engineering side of the project has the appropriate understanding of the design requirements driven by system safety discipline sources.

Less obvious is the interrelationship of the respective quality for both efforts. For example, both disciplines face the challenge of providing the best products with the resources provided by the project. The general lack of communication about program design requirements (and implementation) between program engineering and system safety was one of the findings of the Space Shuttle Challenger accident investigation [Ref. 6]. One could argue that system engineering shortcomings in the establishment of technical requirements and their validation cited in the Mars Climate Orbiter Mishap Report [Ref. 7] and the Genesis Mishap Report [Ref. 8] might have been diminished by a strong interface with system safety (and quality assurance) requirements efforts.

Figure 2 illustrates some of the major objectives of the trade studies that support concept definition. Again, both disciplines have different focuses based on their assigned responsibilities; they share the common objective of assuring that the "best" concept is developed in terms of the candidate hardware and the associated operational characteristics.

For major projects, a number of technical trade studies will be conducted in parallel. While system safety should have insight into all of the trade studies, it is a must that system safety engineering personnel participate in all trade studies that have been identified as being safety related. This direct involvement ensures that safety impacts are addressed and technical risk assessments have system safety factors as part of the trade study decision drivers. From a system safety perspective, it is important that the trade study results show that the safety risks for the recommended solution are equal to or less than the other alternative being traded, or provide sufficient justification (safety margin) for the recommended option [Ref. 4].

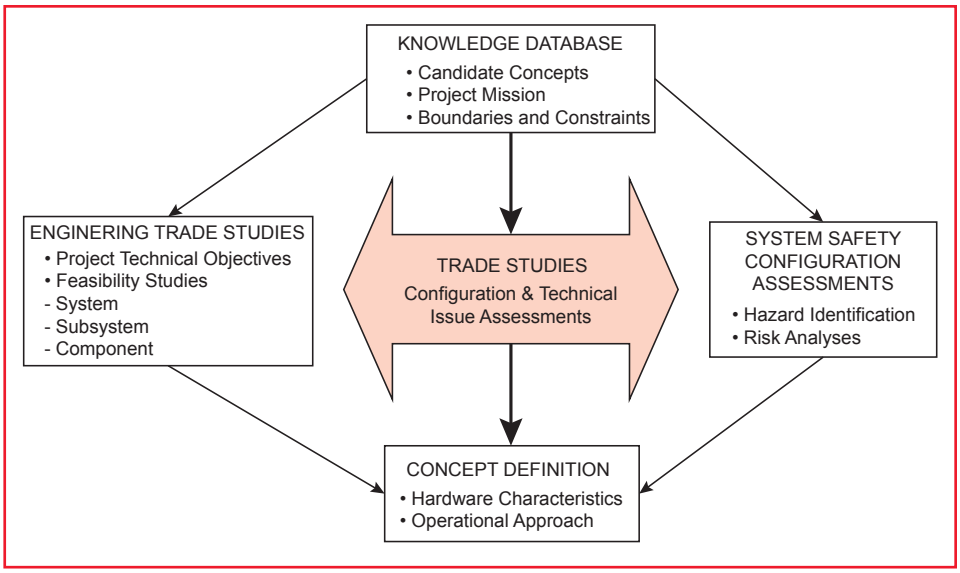


Figure 2 — Concept Trade Studies.

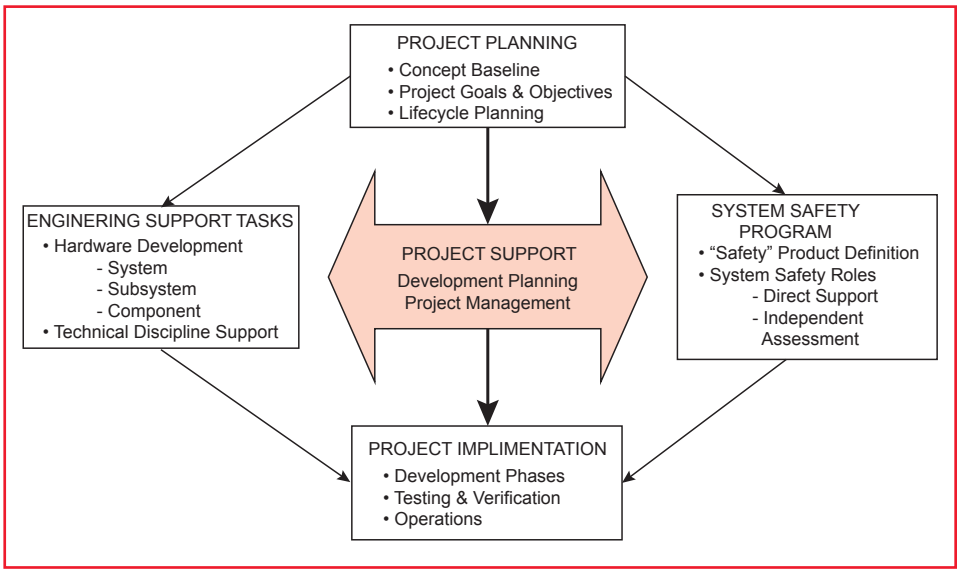


Figure 3 — Project Planning Tasks.

There should be linkage between the technical trade support activity and any related system safety trade analyses. This linkage provides support to the system safety team member's efforts to assure that there are optimum safety provisions developed for each option and inputs to the establishment of the system safety position on trade study recommendations. The effectiveness of this imbedded approach is driven by three factors: the ability to identify safety-related trade studies, the resources necessary to support trade studies, and the necessary system safety role in the project concept selection process.

Figure 3 illustrates the planning for the movement of the project from the concept definition stage into the project development stage. Each discipline has an important role in the planning of project implementation and management activities.

It is important to both disciplines that the proper "go forward" planning is done. Planning is based on the expected roles of each discipline in the project development stage and should utilize the experience gained during the concept definition stage. Each discipline should acknowledge the role of the other discipline in the development of project support activity plans. Acknowledgements that are not mutual or are not consistent should be subject to question and inquiry.

"It is important to both disciplines that the proper 'go forward' planning is done. Planning is based on the expected roles of each discipline in the project development stage and should utilize the experience gained during the concept definition stage. Each discipline should acknowledge the role of the other discipline in the development of project support activity plans. Acknowledgements that are not mutual or are not consistent should be subject to question and inquiry."

The benefit of mutual planning is illustrated by the following example. For any crewed launch vehicle, the provision of a launch pad escape system is of primary importance. Planning for the development of such systems requires the consideration of many factors (hardware and system characteristics procedures) and inputs from many contributors (vehicle designers, pad system developers, human factors experts, system safety engineering and system engineering). Even specialized analyses like the development of the minimum timeline for the flight crew to escape to a place of safety requires input from many sources to provide a complete assessment. Engineering studies that address only the quickest path in terms of the functions of the different subsystems (stairs, pathways, chutes, transporters, etc.) still need input from the human factors evaluations and system safety analyses to determine if the optimum technical system will meet the crew egress survival requirements. Conversely, the system risk analysis needs the inputs of the system engineering analyses and system safety assessments to determine the risks associated with the baseline system and potential alternative solutions. True mutual efforts are based on plans that address all information sources and their application to the system definition development. Such plans should describe an iterative approach that encourages interactions among the contributors to the different aspects of the system during its development.

In the next column, we will address engineering and system safety relationships during the project development phase. Attributes introduced in this article will be expanded and a few new "wrinkles" will be added.

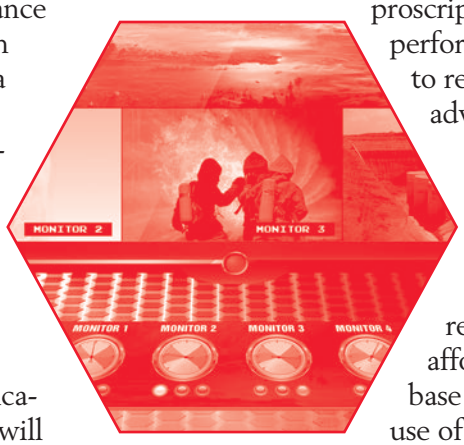
References

1. "Systems Engineering Handbook," National Aeronautics and Space Administration, NASA Headquarters, Washington DC, December, 2007, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20080008301_2008008500.pdf, accessed on July 31, 2013.
2. NPR 8715.3C, NASA Safety Manual, January 24, 2000. Change 6 as of February 3, 2011 Source: NASA Online Directives Information System (NODIS) Library, http://nodis3.gsfc.nasa.gov/, accessed on July 31, 2013.
3. Blair, J.C., R.S. Ryan and L.A. Schutzenhofer. "Engineering the System and Technical Integration," NASA/CR—2011–216472, NASA Scientific and Technical Information (STI) Program Office, http://www.sti.nasa.gov, accessed on July 14, 2013.
4. "Air Force System Safety Handbook," Air Force Safety Agency, Kirtland AFB NM, http://www.system-safety.org/Documents/AF_System-Safety-HNDBK.pdf, accessed on July 31, 2013.
5. "Space Systems Engineering Course: Chapter 12, Trade Studies," http://spacese.spacegrant.org/index.php?page=trade-studies, accessed on August 6, 2013.
6. Report of the Presidential Commission on the Space Shuttle Challenger Accident, National Aeronautics and Space Administration, Washington, DC, 1987, http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/table-of-contents.html, accessed on August 9, 2013.
7. Mars Climate Orbiter Mishap Investigation Board Phase I Report, National Aeronautics and Space Administration, Washington, DC, 1999, ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf, accessed on August 9, 2013.
8. GENESIS Mishap Report, Volume I, National Aeronautics and Space Administration, Washington, DC, 2005, http://www.nasa.gov/pdf/149414main_Genesis_MIB.pdf, accessed on August 9, 2013.

Using the Performance Specification Process in Hazard Elimination and Control

by Pamela K. Wilkinson, MS
Stafford, Virginia

Performance specifications define the functional requirements for the product, the environment in which it must operate, and interface and interchangeability characteristics. A performance specification states these requirements in terms of the required results. However, a performance specification does not state the methods used for achieving these required results. They translate operational requirements into more technical language that tells the manufacturer what acceptable product performance is and how that product acceptability is determined. System safety professionals can make use of the performance specification process to include those items that will verify the elimination or mitigation and control of a variety of hazards. This paper discusses the history and provides an overview of the Department of Defense's (DoD) Performance Specification process. It will also provide guidance to the system safety professional in writing related performance specifications and how to best use this process to verify that potential hazards have been eliminated or controlled.



Introduction

Since World War II, the U.S. federal government has used technical data packages (TDP) and detailed design data (DDD) to procure most of its materiel. This includes detailed military standards, specifications to drawings and detailed manufacturing process specifications [Ref. 1]. Basically, the government told the contractor exactly how to build a product. This helped ensure quality, but not innovation. This lasted until technology began to outstrip the DoD's ability to keep applicable requirement specifications and details current [Ref. 2]. It was determined that there must be "greater interaction between the defense and commercial industries" to keep the "U.S. military technology the best in the world." It was also noted that many commercial items of comparable or higher quality were being made substantially cheaper than those made according to existing military specifications [Ref. 2].

On June 29, 1994, the Secretary of Defense directed sweeping reform of military specifications and standards. The Secretary directed the DoD to make greater use of performance and commercial requirements in the acquisition process. Performance specifications are preferred over detail specifications [Ref. 3]. This was part of the DoD acquisition reform, in which all or most proscriptive requirements were replaced with performance-related requirements in an effort to reduce costs while increasing access to advanced technological improvements.

Performance specifications were crucial to acquisition reform. They permitted the contractor needed flexibility to develop innovative product solutions. The government could then receive quality products and services at affordable prices from a larger industrial base more responsive to DoD needs. The use of performance-based specifications resulted in cutting-edge products due to greater industry competition for government business, which significantly helped modernize today's military [Ref. 1].

Another law — the Federal Acquisition Streamlining Act of 1994 (FASA) — was signed by President Clinton on October 13, 1994. This law streamlined the federal government's acquisition system significantly by changing the way the government buys products. The government (1) put a heavier reliance on procuring commercial products and services (2) made the process for high-volume, low-value acquisitions easier (3) expanded opportunities for small businesses to sell to the government (4) improved the bid protest process and (5) extended the Truth in Negotiations Act to civilian agencies [Ref. 4].

William J. Perry, Secretary of Defense to President Clinton, on June 29, 1994 stated [Ref. 5],

> "I have repeatedly stated that moving to greater use of performance and commercial specifications and standards is one of the most important actions that DoD must take to ensure we are able to meet our military, economic and policy objectives in the future. Moreover, the Vice President's National Performance Review recommends that agencies avoid government-unique requirements and rely more on the commercial marketplace.... Performance specifications shall be used when purchasing new systems, major modifications, upgrades to current systems and non-developmental and commercial items, for programs in any acquisition category….

Table 1 — Common Requirement Categories.

Requirement	Definition
Operational Requirements	Statements that define the basic needs and expectations of the system in terms of mission objectives, environment, constraints and measures of effectiveness and suitability (MOE/MOS).
Functional Requirements	The necessary task, action or activity that must be accomplished.
Performance Requirements	How well the system must perform — generally measured in terms of reliability, quality and other performance-related goals.
Design Requirements	The actual "how to build or buy" types of requirement. Design requirements may include the types of coating to be used, etc.
Derived Requirements	Implied requirements or requirements that must be followed due to higher-level requirements.
Allocated Requirements	A requirement that is established by dividing or otherwise allocating a high-level requirement into multiple lower-level requirements.

Table adapted and quoted from *Systems Engineering Fundamentals [Ref. 6]*.

> To the extent practicable, the Government should maintain configuration control of the functional and performance requirements only, giving-contractors responsibility for the detailed design."

Thus, specifications moved from detailed specifications (how to build) to performance-based specifications (what it does).

Determine What Requirements Apply

To determine what the product should do, a program must first understand the needs of the user. Begin by reviewing the program's operational requirements. As stated in Reference 6, "Requirements relate directly to the performance characteristics of the system being designed. They are the stated lifecycle customer needs and objectives for the system, and they relate to how well the system will work in its intended environment."

Safety-critical design requirements and design criteria for a system under design/development and assessing existing requirements for safety impacts can be accomplished via a safety requirement/criteria analysis (SRCA). The system safety professional reviews or creates the systems preliminary hazard list (PHL) and analyzes the potential hazards to current system requirements, performance specifications, laws, standards and regulations to create a list of regulations or design requirements [Ref. 7].

The system safety profession will need to assess the operating environment, materiel handling and other issues that could potentially impact the safety of the operator or maintainer throughout the life of the system. Requirements can be categorized in various ways [Ref. 6]. See Table 1 for common requirement categories.

Review all of the operational, functional, performance and design requirements for any potential safety impacts and determine any related derived or allocated requirements. Thoroughly review the expected/required operational environments, as they may create additional safety impacts to operators and maintainers. The impacts likely will cause allocated safety requirements. Also, consider any safety-critical impacts that could be caused by software failures.

Many times system safety-related requirements may seem vague or missing. Requirements are rarely defined explicitly. Because MIL-STD-882 is required in accordance with DODI 5000.02, it is an automatic derived requirement. A thorough review of safety-related military and industry standards is important, as they likely contain other derived or allocated requirements. OSHA Standards, MIL-STD-1472, MIL-STD-1474 and various branch-specific standards such as OPNAVINST are excellent places to start. Also, consider researching industry standards such as ANSI, IEEE and SEC standards. Some other sources of requirements [Ref. 8] are:

- Architecture documentation
- Statements of work (from previous increments)
- Design documents from previous increments
- Documents from similar programs
- Lessons learned documentation
- Initial capabilities document
- Capability production document
- Capability development document

Key for system safety professionals is to understand all the stated and implied requirements, and how to best meet those requirements. This understanding is based on the use of integrated environment, safety and occupational health working groups (ESOH WG) composed of all engineers, test, logistics and human systems integration

personnel. The ESOH WG must ensure that the safety strategy and approach addresses the potential hazards and adequately demonstrates the safety of the design in the expected operational environment during test events. The safety professional must work closely with testing and evaluation (T&E) professionals to assist in the development of a requirements testability matrix (RTM) depicting how each safety requirement will be tested [Ref. 9].

Below are some basic questions to ask to help determine operational requirements [Ref. 6]:

- Where will the system be used?
- How will the system accomplish its mission objective?
- What are the critical system parameters to accomplish the mission?
- How are the various system components to be used?
- How effective or efficient must the system be in performing its mission?
- How long will the system be in use by the user?
- In what environments will the system be expected to operate in an effective manner?

Other areas to consider when analyzing requirements for potential safety issues are listed in Table 2 [Ref. 6].

As you review these requirements, develop or add to the system's preliminary hazard list. Keep in mind potential hazards that could happen in operations, maintenance, test and disposal phases. Depending on the complexity of the system, you may be able to begin a preliminary hazard assessment. Consider ways that proactively following the derived requirements you've found could mitigate or eliminate these potential hazards. From this point, you can begin to develop a performance specification to eliminate or mitigate the hazard while still in the design stage.

Coordinate with Systems Engineers and Test and Evaluation personnel to ensure that the requirement is added to the Requirements Traceability Matrix and addressed at the System Requirements Review.

Performance Specifications

According to MIL-STD-961E [Ref. 10], a performance specification is "a written requirement that describes the functional performance criteria required for a particular equipment, material, or product. The overall purpose of a

Table 2 — Considerations for Requirements Analysis.

Consideration	Description
Customer Expectations	(What the customer wants the system to accomplish)
Project and Enterprise Constraints	(Cost, schedule, available manpower, management decisions, etc.)
External Constraints	(Available technology, public and international law, external equipment)
Measures of Effectiveness	(Mission performance, safety, reliability, etc.)
Measures of Suitability	(Maintainability, ease of use, etc.)
System Boundaries	(What systems or components are under assessment, what falls outside of the area of control?)
Interfaces	(What other equipment is necessary for the component or system to operate? What tools are necessary for maintenance or test?)
Utilization Environments	(Weather, temperature extremes, vibration, noise, operational time of day, etc.)
Lifecycle	(Operations, maintenance, test, disposal, etc.)
Functional Requirements	(What the system must accomplish)
Performance Requirements	(How the system must perform)
Modes of Operation	(Types of operations and conditions under which they must operate)
Technical Performance Measures	(Thresholds and objectives)
Physical Characteristics	(Size, weight, type of coating, etc.)
Human Systems Integration	(Noise, lighting, reach, space limits, ergonomics, etc.)

specification is to provide a basis for obtaining a product or service that will satisfy a particular need at an economical cost and to invite maximum reasonable competition."

In 1908, the US Signal Corps drafted a general document to identify the required specifications of the Wright Brothers' heavier-than-air flying machine [Ref. 11]. The document included specifications such as:

- Be easily taken apart for transport in Army wagons
- Be capable of being re-assembled for operation in an hour
- Carry 350 pounds for 125 miles
- Maintain 40 miles per hour in still air

The Wright Brothers won the contract, awarded about two months after the announcement, at a cost of $25,000.

Performance specifications provide specific parameters that describe a product from the basis of how the end result will satisfy a particular need, so that industry, through a competitive environment, can provide the best solution at the most economical cost. According to MIL-STD-961E [Ref. 10], "A good specification should do four things: (1) identify minimum requirements, (2) list reproducible test methods to be used in testing for compliance with specifications, (3) allow for a competitive bid and (4) provide for an equitable award at the lowest possible cost."

As stated in SD-15 [Ref. 12], "Performance specifications define the complete performance required of the product, the intended use, service environmental conditions, maintainability, and necessary interface and interchangeability characteristics." Performance specifications must be quantitative (or measureable) rather than qualitative (or subjective). See Table 3 for additional guidance on qualities of a well-written performance specification.

System safety, environmental and human systems integration sections are generally included in the draft performance specification document that is part of the request for proposal. Typically, there may be two limits: a threshold limit (the specification that must be met) and an objective limit (the specification that is desired). However, some specifications list only one when the objective and the threshold are at the same level.

A general system safety performance specification may state something to the effect that:

> "The operation, maintenance, storage, transportation, or disposal of the system shall not present any hazards that are assessed as more severe than Serious risks as specified in MIL-STD-882E (Threshold). It is desired that the operation, maintenance, storage, transportation, or disposal of the system does not present any hazards that are assessed as more severe than Low risks as specified in MIL-STD-882E (Objective)."

For a system with lithium batteries, a performance specification may state:

> "If the system contains Lithium batteries, the system and the battery shall be capable of meeting all requirements needed for approval by the Navy Lithium Battery Review Board (Threshold); is already approved (Objective)."

For a system that might have the potential for hazardous noise levels, a performance specification may be,

> "In an operational state, the internal acoustic noise level shall not exceed an A-weighted steady state noise limit of 70 db(A)."

Table 3 — Qualities of a Well-written Performance Specification.

Clear	A performance specification is clear if it is written in plain English. Although most performance specifications are written in a positive sense, there is no need to do so if stating it in the negative sense improves its clarity.
Consistent	A performance specification is consistent if it does not conflict with any other specification.
Correct	A performance specification is correct if the users agree the performance specification reflects their need.
Not Redundant	A performance specification should not be redundant. It is redundant if there is another performance specification that means the same thing.
Unambiguous	A performance specification is unambiguous if it has only one interpretation.
Verifiable	A performance specification is verifiable if the specified behavior of the characteristic can be checked in a repeatable manner.

Adapted from "Requirements Document for System Approach for Safety Oversight (SASO)" [Ref. 13]

Table 4 — Specification/Verification Cross Reference Matrix.

METHOD OF VERIFICATION 1 – Analysis 2 – Demonstration 3 – Examination 4 – Test		CLASSES OF VERIFICATION A – Design Verification B – First Article Test C – Conformance						
Section 3 Performance Specification		Verification Methods				Verification Class		
		1	2	3	4	A	B	C
4.5.3.1	In an operational state, the internal acoustic noise level shall not exceed an A-weighted steady-state noise limit of 70 db(A).				x		x	x
4.5.3.2	Equipment requiring more than one (1) person to lift shall be clearly labeled to indicate the weight and the number of personnel required to lift.			x			x	x

Adapted from SD-15 [Ref. 14]

It is important to work with the systems engineering and test and evaluation team, as safety is a trade-off between cost, schedule and performance. Safety-related performance specifications can be a valuable way to proactively eliminate or mitigate hazards early while the system is in the design phase.

Verification Techniques

All specifications must be verified. The verification process allows the government to avoid unnecessary cost, schedule and performance risks while ensuring that the system or component under consideration meets the users' needs and performance requirements. There are four types of verification activities used to determine if a system or component meets the stated requirements [Ref. 10]:

- **Demonstration:** Involves the actual operation of an item to prove that the system functions as necessary during specified scenarios. The system or component may have instruments attached.
- **Examination or Inspection:** Generally, a non-destructive type of verification that includes the use of sight, hearing, smell, touch and/or taste, simple physical manipulation, and may include the use of mechanical or electrical gauging to verify the item performs as required.
- **Analysis:** Uses established technical or mathematical models or simulations, algorithms, charts, graphs, circuit diagrams or other scientific principles and procedures to provide evidence that stated requirements were met.
- **Test:** A verification method in which scientific principles and procedures are applied to determine the properties or functional capabilities of items.

As stated in SD-15 [Ref. 14]:

> "The type of verification techniques used in a performance specification and the amount of test and evaluation needed depends upon various risk factors, such as whether the item is used in critical applications, whether development is required or if acceptable non-developmental items exist, or whether the technology is well-understood and stable or if it is a rapidly changing technology."

Each requirement must be verified. If the requirement cannot be verified, it is not a valid requirement. More than one verification activity may be used to determine if a system or component meets the stated performance specification. It is important to work with the systems engineers and test and evaluations personnel to determine that the proper type of activity is applicable to verify each system safety performance specification.

Verification Events

System safety verification activities take place at various verification test events throughout the system lifecycle. Both the type of verification and the corresponding PVT event would, depending on the complexity of the system or component under consideration, be part of the system verification plan, test and evaluation master plan and/or system test evaluation strategy. System safety professionals must work closely with test personnel to coordinate the verification of safety performance specifications at the earliest applicable event.

Verification events are typically grouped into the following classes of events: design verification events, first article testing (FAT) and conformance events, Opera-

tor Evaluations (OE), performance article testing (PAT), post implementation evaluations (PIE), and independent logistic assessments (ILA). Scheduling the verification of safety-related performance specifications in earlier events such as FAT and OEs allows for changes to the system with a lower risk for cost, schedule and performance issues. Typically, most safety verifications will occur during FAT. However, there is a need to continue to ensure safety verifications during later events such as the PAT, PIE and ILA.

When determining what is needed to verify a performance specification, test and evaluation personnel may find it helpful to create a specification/verification cross reference matrix, such as the one in Table 4.

Conclusion

When system safety is properly integrated in the early acquisition process, many hazards can be eliminated or mitigated as contractors are considering solutions during the proposal stage. When potential safety issues are tied to performance, verification of a hazard's elimination or mitigation is given an earlier priority. The system safety professional will need to work closely with other systems engineers, test and evaluation personnel and acquisitions professionals to ensure an appropriate balance between safety, cost, schedule and performance.

About the Author

Pam Wilkinson is a Certified Safety Management Practitioner (CSPM) and has more than 24 years of experience in the areas of product safety, system safety, human systems integration (HSI), occupational health and industrial hygiene. Pam holds a Master of Science Degree in Safety Science from Indiana University of Pennsylvania. She has provided safety consulting to various branches of the Department of Defense on a number of acquisition programs.

Pam currently serves as Vice President of the Virtual Chapter of the International System Safety Society. She is also Conference & Seminars and Award & Honors Chairman for the Military Branch of the International Practice Specialty Council on Practices and Standards, and a member of the International Council on Systems Engineering (INCOSE).

Pam regularly writes for peer-reviewed publications, teaches and presents at both external and internal training sessions on various product safety, system safety, environmental, occupational health and Human Systems Integration (HSI).

References

1. *Procurement Guide for the Preparation and Use of Performance Specifications*, AMC-P 715-17, Headquarters, U.S. Army Materiel Command, Feburary 11, 1999.
2. Grasso, Valerie Bailey. "Defense Acquisition Reform: Status and Current Issues," CSR Issue Brief for Congress, November 8, 2001.
3. *Performance Specification Guide*. Standardization Program Division, Office of the Assistant Secretary of Defense (Economic Security), Falls Church, Virginia,1995.
4. Cohen Segias Pallas Greenhall & Furman P.C. *Federal Acquisiton Streamlining Act*, http://www.cohenseglias.com/government-contracts.php?action=view&id=331.
5. Perry, William J. "Specifications & Standards - A New Way of Doing Business." Secretary of Defense memo, June 29, 1994.
6. *Systems Engineering Fundamentals*, supplementary text. Fort Belvoir, Virginia: Defense Acquisition University Press, January 2001.
7. *Environment, Safety, and Occupational Health (ESOH) Handbook*. Marine Corps Systems Command, January 6, 2006.
8. Kies, Michael. "Creating the System Performance Specification," QinetiQ NA internal presentation. Stafford, Virginia, April 2011.
9. "Incorporating Test and Evaluation into Department of Defense Acquisition Contracts." Washington D.C.: Office of the Deputy Under Secretary of Defense for Acquisition and Technology, 2009.
10. "MIL-STD-961E with Change 1." Defense and Program-Unique Specifications Format and Content. Ft. Belvoir, Virginia, April 2, 2008.
11. Wright Brothers Aeroplane Company. *Signal Corps Specification No. 486*. http://www.wright-brothers.org/History_Wing/Wright_Story/Showing_the_World/Back_in_Air/Signal_Corps_Spec.htm, accessed October 18, 2011.
12. "SD-15," *Performance Specification Guide,* Office of the Assistant Secretary of Defense for Economic Security, June 29, 1995.
13. "Requirements Document for System Approach for Safety Oversight (SASO)." Federal Aviation Administration, Washington DC, May 23, 2003.
14. "Guide for Performance Specification," *SD-15*. Defense Standarization Program, August 24, 2009.

Eliminating or Controlling System Risks via Effective System Safety Requirements and Standards

by Mike Allocco, PE, CSP
Centreville, Virginia

When addressing system risks, an overly simplistic supposition exists when an analyst assumes that once single hazards are identified and hazard controls are applied, the job of the safety engineer is complete. Such a mindset is literally dangerous in that potential system accidents may not have been identified and mitigated. System accidents may be the result of many hazards that under specific circumstances form an adverse progression, resulting in harm. Consider that there may be systemic and synergistic risks associated with a system.

Designers are generally concerned with meeting a customer's needs; however, in many situations, neither the customer nor the designer may be aware of systemic and synergistic risks related to a particular design. Experience shows that more than 50 percent of requirements are either not defined or not articulated clearly by the customer.

Given that there may be non-apparent system hazards that present systemic and synergistic risks, how then are effective system safety requirements and standards developed to assure that system risks are eliminated or controlled to acceptable levels? The following discussion provides concepts, criteria and considerations to provide context and answer the proposed question.

System Risk Identification

When thinking in terms of system risks, obvious questions come to mind. How are system hazards identified and evaluated in terms of systemic or synergistic risks? Consider the application of interactive, interfacing and integrated hazard analyses and risk assessment methods, which address system risks, system of systems or families of systems (SOS/FOS) risks that can be identified, eliminated or controlled. The keys to such analyses are understanding hazardous actions, inactions or activities that can have an adverse effect on the system, SOS or FOS under evaluation, and applying scenario-driven hazard analysis. Since a system risk can be comprised of many hazardous actions, inactions or activities, a scenario is to be hypothesized and a model may be developed depicting the event sequencing. A number of worksheets or matrices may be designed to compile the details of the system risks under study. As an output of such system hazard analyses, risk controls are defined and further refined into system safety requirements that form overall standards.

Designing Hazard Controls Strategies

As a result of successful system hazard analyses, it is expected that a number of system risks have been hypothesized in some form, whether a narrative, worksheet sequence, diagram or particular model. There may be complicated sequences with many initiators (I), contributors (C) and primary hazards. Given the scenario in Figure 1, the analyst develops a so-called hazard control scheme, which includes many hazard (or risk) controls.

Hazard Control Concepts

Using a narrative, worksheet sequence, diagram or particular model, the analyst develops a hazard control plan to mitigate the system risk to an acceptable level. Within the strategy, many hazard control concepts can be applied — for example, using multi-level lifecycle hazard controls, multi-level system element controls, system assurance controls, applying inductive and deductive hazard controls, encapsulating, compartmentalizing, or segregating controls, implementing redundant hazard controls, designing dynamic hazard controls that will evolve to accommodate system dynamics, utilizing hazard control effectiveness in the design of the controls, implementing hazard control analyses methods, and considering complexity.

Multi-level lifecycle hazard controls — Many abstractions can be applied when addressing the design of hazard controls. For example, apply timelines that depict the lifecycle of the system — all of its various phases and operational sequences addressing development through life extension. Consider the risks associated with the lifecycle of a system accident, contingency, recovery, fail-active and passive modes, damage control

For initial discussions on controlling risks with effective system safety requirements, please refer to: Raheja, Dev G., Allocco, Michael, *Assurance Technologies Principles and Practices: A Product, Process, and System Safety Perspective*, Second Edition, pages 346 through 352, John Wiley & Sons, Inc., 2006. Additional materials may be found in: Allocco M., *Safety Analysis of Complex Systems*, pages 131 through 144, John Wiley & Sons, Inc., 2010.

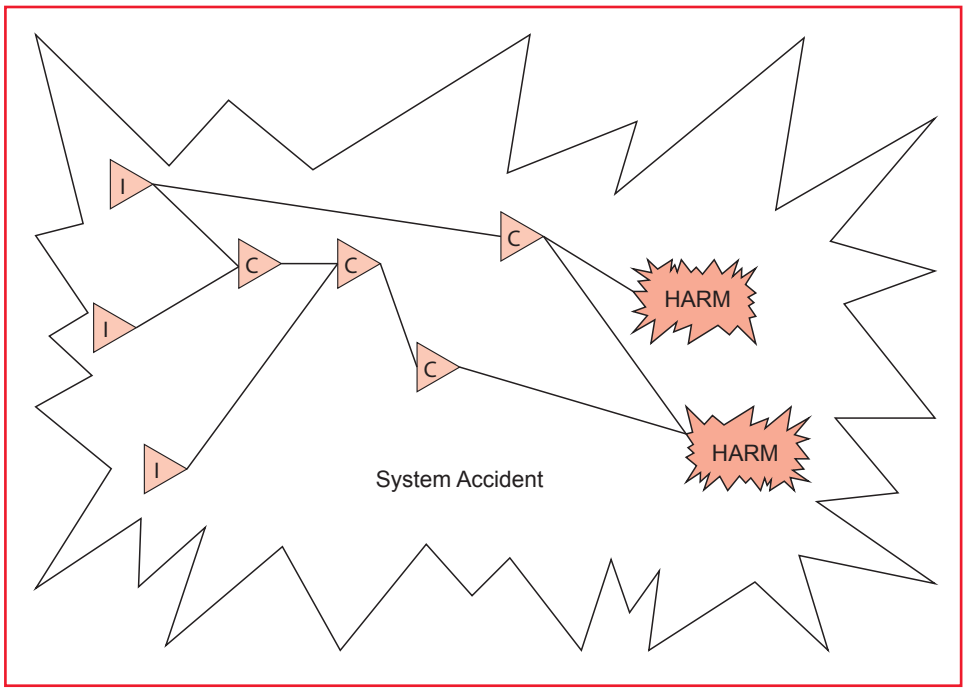


Figure 1 — An Example of a Potential System Accident.

and emergency action. A hazard control application timeline is established, depicting the state of hazard control activity.

Multi-level system elements controls — Apply distributed controls throughout the system elements: the human, hardware, environment, software design, firmware, algorithm, architecture and mathematical logic. Address interfaces, interactions and inactions. There may be manual, semi-automated and fully automated controls that should be integrated, and such controls may work in concert, or be independent, providing redundancy.

System assurance controls — Provide integrated system assurance controls for reliability, maintainability, availability, human factors, survivability, logistics, security, quality and system effectiveness. When considering system risk, it is important to evaluate all system-related requirements. If such specialty system engineering requirements are inadequate, system hazards may be the result. Apply holistic "systems thinking" and understand how specialty requirements interplay. There can be situations when hazard control effectiveness is degraded by inappropriate interaction between similar specialty requirements.

Inductive and deductive controls — Complex systems are decomposed into parts to enable analysis. Adverse sequences can be looked at inductively or deductively. Consequently, high-level, mid-level and low-level hazard controls may be applied at these various levels to abate adverse flow, prohibiting a lower-level hazard from propagating up to a top-level system hazard. Event trees, logic or fault trees can be used to depict adverse progression (cut sets).

Encapsulating, compartmentalizing or segregating controls — When energy inadvertently becomes uncontrolled, adverse propagation is enabled, and barriers must be provided to abate or hinder adverse progression (see Figure 2). Encapsulating, compartmentalization or segregating is a means to control abnormal energy release. The concept of exposure control also comes to mind, including the inadvertent exposure to dangerous energy, toxic or hazardous materials, ionizing or non-ionizing radiation, harmful temperature, failure propagation, synergistic reactions, inadvertent release of potential energy, rapid oxidation, etc.

Redundant hazard controls — In some designs, it becomes appropriate to "stack" hazard controls to inhibit adverse progression, making defeat of a number of hazard controls within the adverse progression necessary for harm to occur. This concept is also referred to as "defense in place." It is further advisable to provide N-version controls, in that the controls are of independent means or designs to eliminate common-cause events, which may defeat the stacking concept. Think of employing different human, hardware, firmware and software controls within the redundant schema.

Side note: A control can be considered less than adequate (LTA) when real-time validation of the control is not assured or affirmed. In other words, controls can be inadvertently deleted from the stack. So-called back-up, fail-safe or fail-operational designs have failed when needed.

Dynamic hazard controls — Risk is dynamic in that there may be system variation throughout the lifecycle due to many reasons: wear, degradation, unplanned automated operations, changing tolerances, inappropriate maintenance actions, inadvertent operations and unplanned environmental occurrences.

Independent system monitoring is designed to detect circumstances that are hazardous. There must be a capability for appropriate contingency, causality and recovery response. In some situations, it may be appropriate to enable a redundant independent monitoring capability, both with automated and manual responses. Consider trade-offs between automated and manual monitoring. Should an unplanned adverse situation occur, the automated design may not be able to accommodate unplanned contingencies. Conversely, the human may have the capability to deal with

unplanned contingencies. When there is reliance on the human, appropriate training and simulations in contingency variation, crises thinking and emergency diagnostic approaches are needed, which provide other supportive administrative controls. Consider the lifecycle of a system accident, knowing that additional harm can occur during chaotic situations.

Hazard control effectiveness — When dealing with large, complex systems, many controls may be designed. Many supportive analyses can be applied to evaluate hazard controls, including the concept of validation, to determine if the particular control mitigates risk associated with a specific control or set of controls. Several ways to rank controls and apply hazard control effectiveness remain, coming into play during resource allocation. Expenditures can be applied toward the controls that are most effective.

Side note: Risk (control) is the most important attribute when conducting trade-off studies associated with hazard controls. Care must be applied in the exchanging, re-designing or refining of hazard controls. The inappropriate exchanging of one control for another can induce additional risk. Control complexity is another important attribute. Developing overly complex control designs can introduce higher risk, as can making inappropriate decisions between manual, semi-automated, and automated controls. A careful balance must be maintained between all the attributes discussed here.

Hazard Control Effectiveness Analysis

Many supportive methods can be applied to determine hazard control effectiveness. These techniques employ decision analysis to assess different attribute weighting factors, and to attribute parameters and a score value range. Decision logic techniques can include analytic hierarchy process, fuzzy logic and utility analysis. Worksheets are designed to include attribute weighting factors, attribute parameter criteria and score value ranges. Attribute parameters may include:

- Hazard Control Coverage (HCC) — The control under evaluation may be applicable to none or many other hazard scenarios (risks) identified within the safety analysis.
- Hazard Control Association (HCA) — The control may directly eliminate the risk or reduce the risk associated with a particular contributor.
- Cost Effectiveness (CE) — The cost associated with the particular hazard control is at a particular budget range.
- Engineering of Control (EC) — The level of design work is considered in the implementation of the control.
- Applied Science (AS) — The degree of knowledge related to the science to be applied in the development and implementation of the control is considered.
- Codes, Standards and Law (CSL) — The control meets existing codes, standards and law, or new codes, standards or laws need to be developed.
- Adverse Associated Effects (AAE) — The control may or may not have an adverse effect on the system in the event of control malfunction or failure.
- Administrative Control Application (ACA) — The administrative control can be easily implemented, or there is a need for study, analysis or tests.
- Hazard Control Similarity (HSC) — The control is an existing implemented requirement, or there is no similarity.
- Hazard Control Verification (HCV) — The hazard control verification is accomplished by simple observation, inspection, interview or discussion, or the verification requires extensive study, analysis or testing.
- Risk Elimination and Reduction (RER) — It is apparent that a single hazard control will eliminate or reduce the risk to an acceptable level, or many controls are required to eliminate or reduce risk.
- Risk Likelihood Reduction (RLR) — The hazard control reduces the likelihood by a factor of X.

Barrier Analysis

Potential system accidents can be depicted in various conceptual models, where initiators (I), contributors (C) and primary hazards (Harm or HAR) are indicated within an adverse flow. A barrier analysis enhances the depiction by showing the barriers that will abate adverse flow within the sequence. Figure 2 shows a potential system accident, along with nine barriers, which are hazard controls to mitigate the system risk. Note that there are three initiators, four contributors and two possible outcomes. Consider that any combinations of the three initiations can occur, which will start the adverse sequence. An initiator can be a latent or real-time hazard that may trigger under certain circumstances. The real-time hazard may also act as a trigger. These triggering events may also be shown within the model.

Developing Hazard Control Requirements

The objective is acceptable risk via the appropriate application of hazard controls, which are the output of hazard analysis and risk assessment. Controls are transformed into an appropriate set of requirements forming a safety standard. In designing controls, there are many considerations, including:

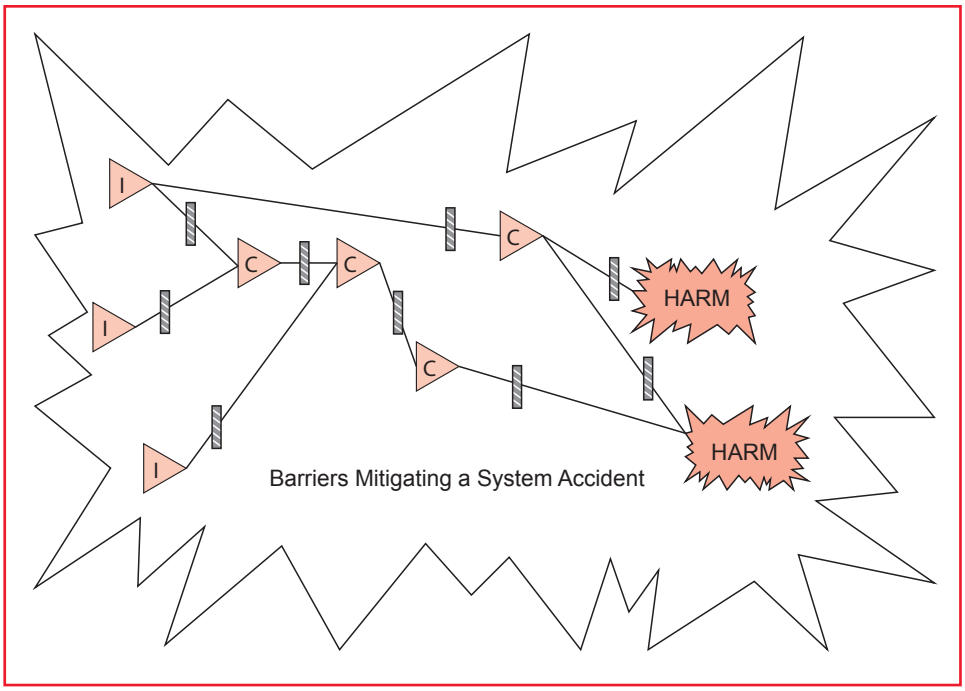


Figure 2 — An Example Depiction of Barriers Applied to Abate Adverse Progression.

- Conformance to existing safety-related standards is required to meet minimal levels of protection or risk mitigation. However, acceptable levels of risk may not be assured due to many reasons, including inappropriate decisions, poor consensus, biases, limited proactive safety assumptions, over-generalization or poor investigative and analysis work.
- When deriving requirements, the specific safety-related experience or issue — and/or the output of an unbiased accident analysis, system safety analysis, safety study, safety assessment or review, survey, observation, test, simulation or inspection — must be considered and addressed.
- Design requirements that will be validated and verified. Provide specific means to assure that the requirement will work as intended when needed by formal approaches, including tests, simulations, analysis, inspection or observation.
- Understand system dynamics and provide requirements to accommodate dynamic changes to assure continued acceptable levels of risk.
- Apply standardized language usage criteria in requirements development.
- Independently evaluate requirements development tools.
- Consider the real world when developing requirements. When addressing functions or operations, know what drives the function or operation, such as combinations of human, hardware and software actions.
- Understand requirement abstraction, semantics, context, terms and written tense. Minimize jargon. Define requirements within logic, depictions, illustrations and diagrams.
- Analyze requirements language; know conventions, stereotypes and the intended user.
- Independently define requirement intent and verify that intent.
- Define requirements to show consistency between high-level, mid-level and lower-level abstractions; provide tractability.
- Document requirements development processes and reviews.
- Provide configuration control during requirements development.
- Assure consistency between specialty engineering requirements.
- Define risk-based and contractual criteria for ranking, validating and verifying requirements.
- Independently evaluate the total system safety standard, and eliminate redundancy.

Conclusion

To assure continued acceptable (system) risk, system safety efforts must be ongoing. These efforts do not stop with the conclusion of an appropriate system hazard analysis and risk assessment. Hazard controls need to be developed and converted into safety requirements that form an appropriate system safety specification. This article addressed the various concepts, criteria and considerations needed in the development of hazard controls, as well as refining these controls into a requirement specification.

About the Author

Mike Allocco, PE, CSP, is a Fellow of the International System Safety Society and its former director of mentoring, research and development. He has been involved in system safety, safety engineering and safety management since 1976. He has conducted system safety engineering on diverse complex systems for DOT, DOD, DOE, NASA, and general industry. He is the author of *Safety Analyses of Complex Systems: Considerations of Software, Firmware, Hardware, Human, and the Environment*, Wiley, 2010 and is coauthor (with Dev Raheja) of *Assurance Technologies Principles and Practices: A Product, Process, and System Safety Perspective*, Second Edition, Wiley, 2006.

System Safety Bookshelf

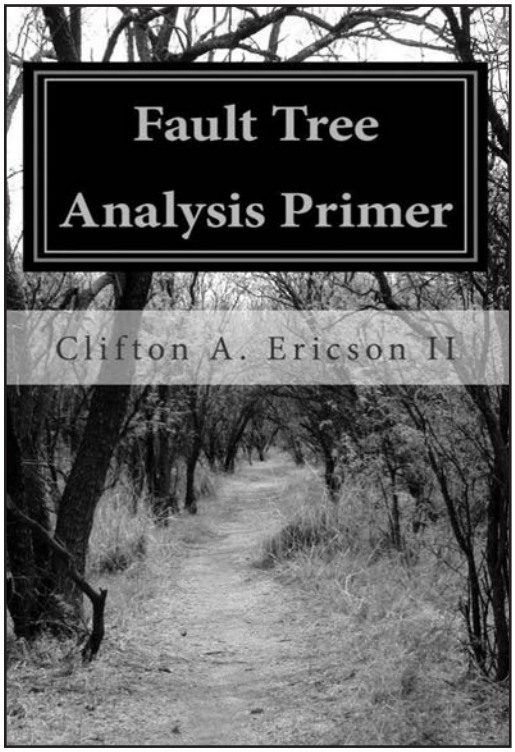
P.L. Clemens, P.E., CSP

A Kind Introduction to FTA

Fault Tree Analysis Primer

By Clifton A. Ericson II
Publisher: CreateSpace
135 pages
ISBN: 10:1466446102
ISBN–13:978–1466446106
Price: $27.00

A color photograph gracing the cover of this book depicts a path winding through a forest of many trees — quite appropriate, given the purpose of the book. It's an inviting path, criss-crossed by shadows that suggest there's a brightly sunlit meadow lying at the path's end. And so there must be! The meadow, in this case, is mastery of a system safety analysis technique that's both reviled and held sacred. But be wary: A clump of brush intrudes into the path. Does a *bête noir* with sharp fangs and a nasty disposition lurk within it? Yes — so stay alert!



Inject the three-word phrase "fault tree analysis" (FTA) into a discussion on any topic among a group of safety professionals. Do it with a flat, unemotional voice. Observe the reactions of others. It doesn't much matter whether fault tree analysis is at all appropriate to the topic under discussion by the group — reactions by your colleagues will be much the same. There will be those who shudder with woe, grimacing and shaking their heads at the mention of FTA. Too often, they make up a majority. But there'll be a few others smiling warmly.

Why do we see these polar opposite reactions? FTA is one of the several system safety analytical techniques that can be applied either subjectively (i.e., non-numerically) or quantitatively. (Couple that with the fact that neither with FTA nor any of the myriad other techniques do we ever actually analyze a system. We analyze only our personal conceptual models of systems — and there, now, is a recipe almost guaranteeing analytical mayhem!) A philosophy that serves in two realms can mistakenly come to be thought of as belonging to neither.

This book opens with an explanation of the function of FTA. Both text and diagrams clarify that identifying hazards is not a principal FTA function. An FTA explores a system to search out those sources and mechanisms that might lead to an already-identified undesirable event. FTA is described as a cause-effect probing of the system. The undesirable event may be a loss event that has, indeed, already occurred — in which case, the FTA then becomes an invaluable investigative tool. A bulleted list of 13 candidates suggests practical applications for which an FTA can be of valuable service. This is but one of this book's many such lists, each speaking silently of having served the author in decades of system safety service and now shared with us to enhance our own practice — each designed to protect against one *bête noir* or another.

This is a kind book, a gentle book. And given the topic, that is a pleasant surprise. Although it commences, as declared by its title, at a "primer" level, it proceeds well into graduate school, taking compassionately small steps as it goes. Its topic is recognized as lying fully across that prickly dividing boundary between the non-numerical system safety methods, i.e., those that might be thought of as almost exclusively "narrative" — e.g., preliminary hazard analysis — and those that are often wholly quantitative, e.g., Markov analysis. This is principally a "teaching" book, and is an excellent choice for classroom use. Nothing more than high school algebra should be needed for its reader to grasp even its most elegant points. And there's stealth and treachery in its di-

dactic methods! You'll read a small handful of paragraphs and discover that you've learned something altogether new to your understanding, or perhaps developed a new outlook toward something you've long understood. And so it is with all of this prolific author's books dealing with topics in system safety.

This book is a badly needed "lite" NUREG-0492, *Fault Tree Handbook* (N. H. Roberts, W. E. Vesely, et al, USNRC, 1981.)

There are valuable hidden lessons that emerge for the user of this book. Here, paraphrased, are two related gems:

- Unquantified fault tree structure alone will reveal much about system risk that might otherwise go undiscovered. A fault tree need not be slathered with statistics to be of value to the system analyst and the system designer.
- If the analyst can't sketch an accurate functional representation of the system, he is not prepared to fault tree it.

Fault tree analysis is not without its limitations and its detractors. Author Clifton Ericson has cataloged a fine "watch-out" chapter that, alone, is worth the price of admission. It is broken into two parts:

- **Common FTA Myths —** Ten myths are presented. Each is followed by a "truth" statement that unarguably sets the record straight. An example myth: If two FTAs for the same loss event and the same system are different in appearance, at least one is incorrect. A pair of differing FTAs is used to explode this myth quite neatly. Their cut sets are identical, but their graphic representations are vastly different from one another, although both of them are correctly drawn.
- **Common FTA Criticisms —** Each of 12 common complaints about FTA by its detractors is presented. A "reality" statement is then presented to correct the disparagement. Partial truths among them are also acknowledged.

And lastly, this book makes an excellent shelf mate to others with titles like these by the same author:

- *Concise Encyclopedia of System Safety*
- *Hazard Analysis Techniques for System Safety*
- *System Safety Primer*
- *Hazard Analysis Primer*
- *System Safety/Reliability Engineering*

Index of Advertisers

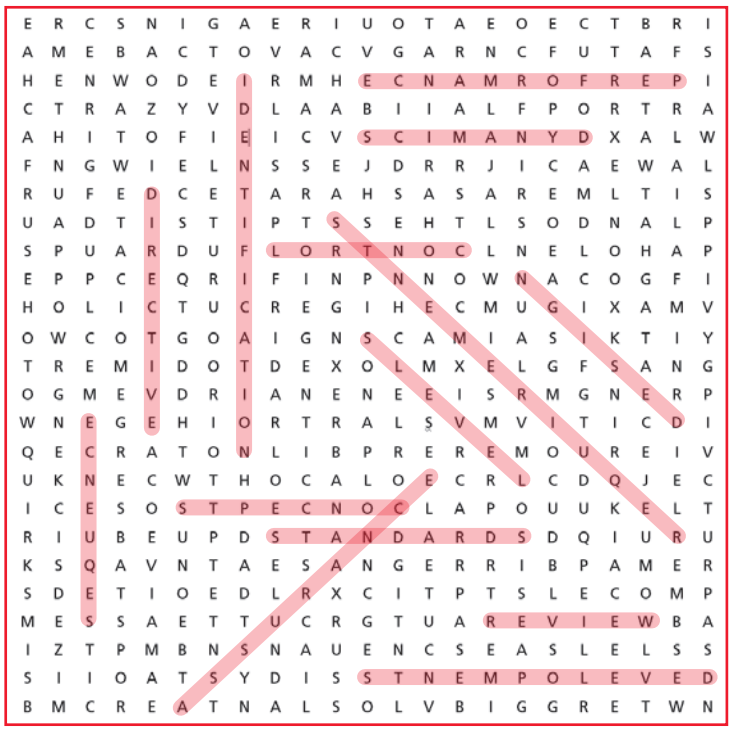
We Want to Hear from You

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 17)



Thank You

to all of the Sponsors & Exhibitors of

The 31st International System Safety Conference

From The International System Safety Society

Sikorsky
A United Technologies Company

A-P-T RESEARCH, INC.

BOEING

LOCKHEED MARTIN
We never forget who we're working for
Aeronautics Company & Space Systems Company

AST AEROSPACE
A DIVISION OF ATLANTIC SOFTWARE TECHNOLOGIES

BASTION TECHNOLOGIES

isograph

UNIVERSITY OF MARYLAND
A. JAMES CLARK SCHOOL OF ENGINEERING

A.L.D. Advanced Logistics Development Ltd.

BCSP | Board of Certified Safety Professionals

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

MathWorks®

Safety for the Long Run

The 31st International System Safety Conference

August 12-16, 2013

Boston, Massachusetts was the setting for the 31st International System Safety Conference, and in one of America's oldest cities, attendees heard from some of the leaders in the field to map out safer paths into the future. The theme of the ISSC 2013, "Safety in the Long Run," spoke of the challenges that changing demands can place on new and existing technology, and how new tools, findings and ways of thinking can help safety practitioners make the world a safer place.

Photos by Rod Simmons, John Hewitt and Alan Oliver

Speakers

ISSS Fellow Member Emeritus Rex B. Gordon was the opening ceremonies' 50th Celebration Speaker. Rex, a past president and editor of Journal of System Safety, *spoke about the origins of the Society and gave an overview of how far the ISSS — and the field of system safety in general — has come in the past 50 years to help renew the dedication and vision of current ISSS members.*

Rex B. Gordon and ISSS President Robert A. Schmedake

Keynote Speaker James P. Keller, vice president of Health Technology Evaluation and Safety at the ECRI Institute, spoke on "Health Technology-Related Patient Safety Perspectives." He delivered information on safety management in hospitals from both a professional standpoint and his personal experiences of "alarm fatigue" from his mother's stay in the hospital.

James P. Keller and ISSC 2013 Chair Pam Alte

Dr. Nancy Leveson, from the Massachusetts Institute of Technology's Aeronautics and Astronautics Department, presented "The Path to More Cost-Effective System Safety" at the Sponsor and Exhibitor Luncheon. She spoke on how using hazard analysis techniques created 40 to 50 years ago are not effective, and how the role of humans in systems, and accidents, has changed.

From left, ISSC 2013 Chair Pam Alte, ISSC President Robert A. Schmedake and Dr. Nancy Leveson

Dr. John McDermid, professor of software engineering at the University of York, presented "Autonomous, Adaptive and Safe?" at the International Luncheon, looking at automation in unmanned aircraft, examining issues including safety, certification and assessments.

ISSC 2013 Awards

Manager of the Year

Pam Kneiss

Scientific R&D Award

Bruce Partridge

International Award

Rod Simmons

Professional Development

Dave West

Educator of the Year

Steve Mattern

New International System Safety Society Fellows (Not pictured)
Bob Schmedake and Don Swallom

Awards presented by Chuck Muniak

Chapter of the Year

Virtual Chapter

President's Award

Cathy Carter (presented by Bob Schmedake)

Best Paper Award

Towards Automatic Verification of Safety Properties in AADL System Models" — from left, Rikard Land, Stefan Björnander and Patrick Graydon.

Best Paper Award (Not pictured)

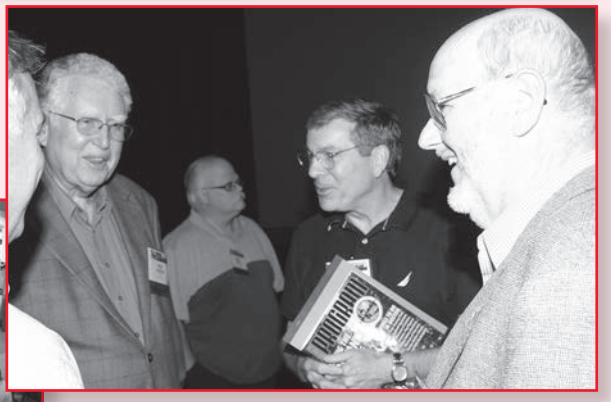
"Software Risk: The Third Rail of Safety Analysis" by Holly S. Hildreth, PhD, and Charles Greg Elcock, USN-R, Aviator.

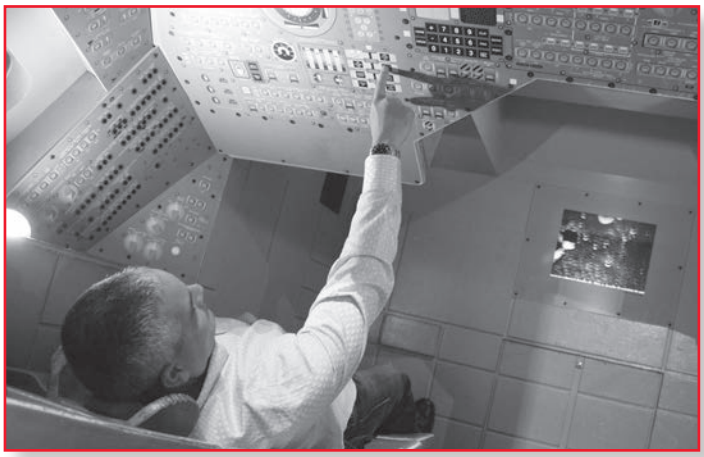
Northeast Chapter President Scott Beecher

ISSC 2013 Chair Pam Alte

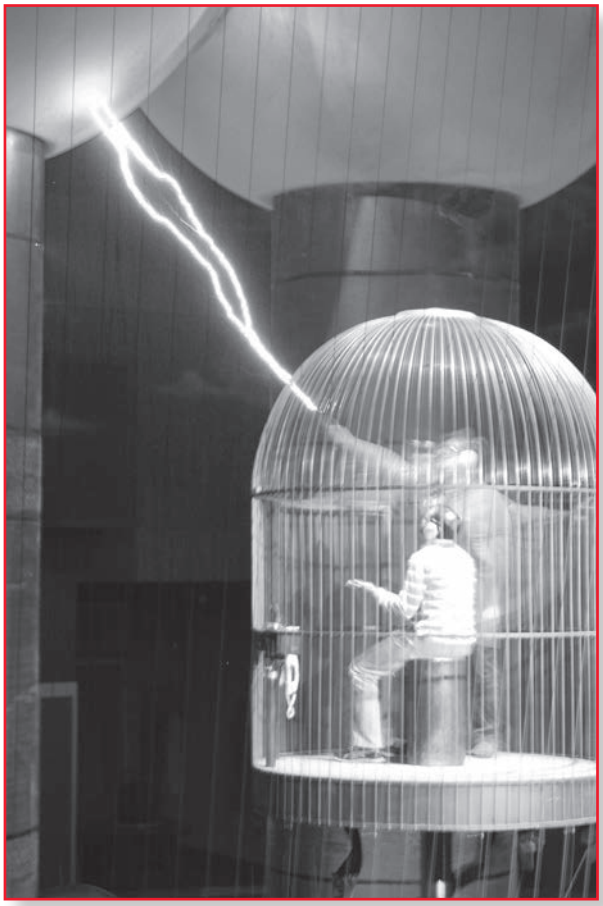
ISSS President Robert A. Schmedake

Attendees of the 2013 ISSC had the opportunity to meet in classroom settings, small group settings or network independently. The relationships built at conferences such as the ISSC can prove invaluable to careers and to the practice of system safety.





ISSC 2013 attendees also took a field trip to the Boston Museum of Science. Above, full-size models of the Apollo and Mercury capsules were available to explore.



A Van de Graaff generator (above) and displays of static electricity (left) were some of the sights to see — and feel — at the Boston Museum of Science's Theatre of Electrical Science.

The Boston Museum of Science also offers the exhibit "Mathematica," where the role of mathematics in science and post-modern design is explored.

Interview: Richard Hawkins
Doctoral Student

Richard Hawkins, a student in the software safety Ph.D. program at the University of York, attended the 2013 International System Safety Conference (ISSC). Journal of System Safety sat down with Richard and asked him about his views on the Conference, international cooperation and ways to move the field forward.

Richard Hawkins

Journal of System Safety: **How did you get started in the field?**
Richard Hawkins: When I graduated, I got a job as a safety advisor in the nuclear industry, but that was working more with occupational safety — it wasn't really involved with system safety. Then, I changed tack and did a master's degree in computing, and realized that there was actually cross-over between the two. When I found out about the opportunity to do a Ph.D. at York in system safety, I combined the safety and software aspects together and started working with John McDermott in the High Integrity Systems Group at York and earning my Ph.D. in software safety.

I'm extremely grateful that the Northeastern Chapter was good enough to fund my trip here. As part of John McDermott being the keynote speaker for the International Luncheon, they offered for one of his students to come across. Otherwise, the funding wouldn't have been available for me to come.

JSS: **What are your overall thoughts on the ISSC?**
RH: For me, the best thing about coming here is that there is such a large number of people from industry, and people with a lot of experience doing system safety over a long period of time. For someone like me who's trying to do research, it's good to be able to share in that knowledge and experience — particularly coming to the U.S. to get the views of people in the States, which are sometimes slightly different from the way we think about things in Europe. It's good to come here and get that different perspective that I wouldn't get necessarily from attending a conference in Europe.

In addition to the presentations, which are a good way of seeing what people are doing, the tutorials and workshops are very valuable. If there are specific things you want to know more about, you can get more information there than you would get from a presentation. So, I think that having a mix of the two is a really positive thing about the Conference.

JSS: **What will you be taking back home with you from the ISSC for your research?**
RH: One of the things that has really stood out for me is the increase in autonomous systems. A lot of people in their talks mentioned this increase in autonomy, such as with UAV and aircraft, and cars becoming more autonomous. Even in medicine, there are more autonomous systems. That's been a real eye-opener for me, how much more important those aspects are going to become. That's encouraging for me, since the focus of my research is software.

JSS: **What did you think of the ISSC's structure?**
RH: It's good that there's space in the Conference for social events. I think, in terms of talking to people, social events are good for that, and one of the great things about this conference is that you feel that there's time for the social things, as well. It's not all about the technical stuff.

JSS: **What are your future plans after you earn your degree?**
RH: Ideally, I'd like to carry on with research, since there are so many areas that still need to be looked into. A lot of the research that we do at York is closely linked to industry, so a lot of our research is funded by companies that have specific problems they want us to look at for them. I think with enough problems that these companies face from a system safety — and particularly a software — point of view, hopefully that money will carry on.

JSS: **Have you seen a big difference between Europe and the U.S. in the way that system safety is handled?**
RH: Fundamentally, it's the same, but there's an emphasis, especially in the U.K., on more of a safety case

approach — a more goal-based regulation — whereas things seem proscriptive over here, although I know that's a sweeping generalization. It does seem that more people here are getting interested in the safety case approach, though.

***JSS:* Did the ISSC stand up to conference standards in the U.K.?**
RH: Yes. It's slightly different, because a lot of the conferences in the U.K. are focused on academia, where this one seems more focused on industry. And I think that's a good thing, because you need both. There's a place for academic conferences, but there's a place for more industrial conferences. It provides an opportunity for people from academia, like myself, to link into that community and find out from a broad range of people what's actually happening — the current best practices in the industry. It feels like this conference is aimed more at the industrial side; I don't know if that was the intention, but that's how it feels to me.

***JSS:* Do you think we in the United States are too U.S.-oriented and not international enough?**
RH: I don't think so. All countries are focused on their own issues, but I think that's inevitable, really, because the industry is so highly regulated. Each country has its own regulators. Everyone gets a bit territorial because of that reason. It's almost a side effect, because you're regulated at a national level. For example, in Europe, the French, the Germans and the British all are a bit self-focused. The Americans are, too, but I don't think it's unusual. Maybe that's another reason we should be sharing across the community. No one has a perfect way of doing it.

***JSS:* Do you have any thoughts on improving the ISSC, or conferences in general?**
RH: One thing I've talked about this week is trying to bring the U.S. and European communities together, because clearly from this conference there is a big community here. There's a big community in Europe as well, but I don't see a lot of cross-over. I've been to conferences in Europe and now this conference. There are a small number of faces you see at both, but it's quite a small number. It would be nice to see more cross-over. I realize that it's difficult to achieve because of travel expenses, but I think that there's a lot that could be done by bringing the two communities together. Maybe there are virtual things we could do by using video conference facilities, where we could have presentations in Europe attended by people here, to get the sharing of ideas without having to move people across the Atlantic.

Thanks to the ISSC 2013 Sponsors and Exhibitors!

Gold Sponsors

A-P-T Research, Inc.

Boeing

Lockheed Martin

Lockheed Martin Aeronautics Company

Silver Sponsors

Atlantic Software Technologies, Inc.

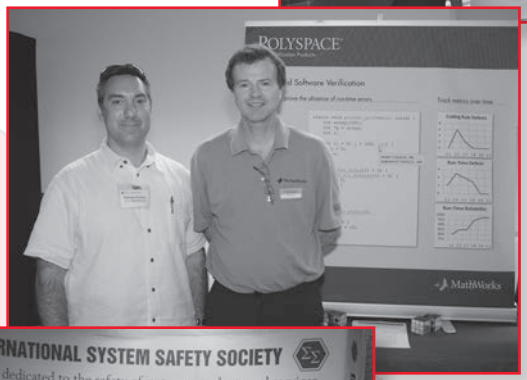
Bastion Technologies, Inc.

Isograph, Inc.

University of Maryland

Corporate Sponsor

Sikorsky Aircraft Corporation



Exhibitors

Advanced Logistics Development

Board of Certified Safety Professionals

Electric Power Research Institute

International System Safety Society

MathWorks, Inc.

Partner

The Institute of Engineering and Technology

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
Terry Gooch
770-494-3527
terryjgooch@gmail.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