President's Message

by Gary Braman

Two years ago, I and several others took on the task of updating the International System Safety Society's Strategic Plan. This was a daunting task, but one that I was sure would be rewarding when complete. When we initially started, we purchased a book about strategic planning since we weren't quite sure what a strategic plan was. Strategic planning is a tool for organizing the present on the basis of the projections of the desired future. That is, a strategic plan is a road map to lead an organization from where it is now to where it would like to be in five or 10 years. The strategic plan has three parts: Vision Statement, Mission Statement and Strategic Goals.

We began the process by reviewing and updating the Society's current Vision Statement (Be the recognized international leader in the system safety discipline) and Mission Statement (Advance the system safety discipline by creating an international, interdependent network of system safety professionals dedicated to the continuous improvement of the art, sciences and technology needed to provide the best total system safety solutions). The proposed updated Vision Statement is "To make the world a safer place through safer systems" and the proposed updated Mission Statement is "Advance the system safety discipline by creating an international, interdependent network of system safety professionals dedicated to the continuous improvement of the art, sciences and technology needed to provide the best total system safety solutions. Be the recognized international leader in the system safety discipline."

The next step was to develop the Strategic Goals necessary to accomplish the mission and attain the vision of the Society. In developing these goals, we began by looking at other organizations that are similar to ours and determining what these organizations were doing to accomplish their mission and attain their organization's vision. We looked at several similar private and professional organizations, including the American Society of Safety Engineers (ASSE), the American Society of Mechanical Engineers, the Human Factors and Ergonomics Society (HFES), the Institute of Electronic and Electrical Engineers (IEEE), the Society of Automotive Engineers (SAE), the United States Army Warrant Officer Association (USAWOA) and the Army Aviation Association of America (AAA). We found that these organizations had many things to offer to their members — some that we had, and some that we wanted to have. The things that we want and need include our own office space or building, multiple sources of income, certifications, leadership programs, mentorship programs, undergraduate and graduate degree programs, professional development programs and scholarship programs. After reviewing these organizations' strategies, we began to develop ours. We used a process called SMART in developing the Society's Strategic Goals: Specific, Measurable, Achievable, Relevant and Time Bound. The following are the eight Strategic Goals (SGs) that were developed, along with some of the metrics used to measure their success:

- **SG1**: Develop and sustain multiple income streams to fund achievement of the Society's Strategic Goals. Some of the metrics include developing Society memorabilia for sale to members and others; selling system safety and other safety-related standards and publications; establishing a Society "job board" on the Society Website; and increasing the number of corporate sponsors and their sponsorship of Society activities.

- **SG2**: Provide staff, facilities and automated processes that quickly and efficiently resolve the needs and requirements of Society members and chapters. These metrics may include augmenting the current staff at Society headquarters, leasing or building our own facility and automating many Society, chapter and member functions.

- **SG3**: Provide communication capability to facilitate worldwide communications between Society members, chapters, and the Executive Council (EC). We envision improved communications between the EC and the Society chapters and members through Society-
provided telephonic and Web-based communication systems, and an improved Society Website that incorporates new functionality.

- **SG4:** Provide educated, certified and competent system safety engineers to industry for resolution of their complex safety issues. We will continue the work of establishing a graduate-level system safety engineering and management program, along with a certification for system safety engineers and the establishment of system safety engineering competencies.

- **SG5:** Provide professional development opportunities for the members worldwide. In addition to the Society's annual Conference and regional conferences, we would like to provide online training opportunities to our membership.

- **SG6:** Provide an online information database with industry best practices and lessons learned. Metrics include a Web-based information system with lessons learned, safety-related publications and access to our Conference proceedings.

- **SG7:** Increase and sustain membership worldwide. We felt that the best way we could increase and sustain our membership is to automate the membership and membership upgrade processes.

- **SG8:** Provide cost-effective and efficient Society governance. Two of the metrics include streamlining or eliminating cumbersome Society processes (membership and membership upgrade), and eliminating overlapping duties of Society directors.

Hopefully, you will have gathered that these goals are tied together and must all be accomplished to attain our "vision" as a Society and to accomplish our Society's mission. As soon as the plan is complete, it will be forwarded to the EC Members for review, comment and a vote. Upon approval, we will begin the execution of our Strategic Plan. As always, I appreciate your time and your support of our Society. Please feel free to contact me with any ideas you may have on how we can improve our Society.

Thank you!

— Gary Braman
President
International System Safety Society

Copyright © 2011 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.
Vol. 47, No. 6 • November-December 2011

From the Executive Vice President

by Robert Schmedake

As the new Executive Vice President for the International System Safety Society, I do appreciate the opportunity to serve this Society. The role of the Executive Vice President is largely a lieutenant role to that of the Society's President. However, one key responsibility that I take seriously is the requirement to ensure that the Society abides by its bylaws, policies and procedures.

These are essentially a contract between Society officials and the Society membership. They commit a process for how we do business, and are available for all to see on our Society's Website. This command media is intended to ensure that all decisions are made openly, ethically and in keeping with the principles of this Society.

Within our Society, there are different tiers of documents. At the top are the bylaws. They document the organization's purpose and structure. They lay out the rules of how decisions are made. The next tier down is the Operating Manual. Within the scope of the bylaws, this manual describes the day-to-day operation of the Society. It details specific responsibilities for the elected and appointed officials that serve the Society.

Other documents that govern how we operate include the Strategic Plan, and the Fundamental Canons of Ethics. Our Strategic Plan outlines the goals of the Society and concrete actions to be taken to further those goals. It is revised regularly and reflects the current thinking of the Executive Council. In contrast, the Fundamental Canons of Ethics were written earlier in the life of the Society and remain relatively unchanged over the years. They describe the guiding principles of a system safety professional and represent the ideal.

Our command media has provisions for change and improvement. There are good reasons for periodically reviewing our documents to determine if they reflect the best way of doing business today. When inefficiencies that can be eliminated exist, then we should eliminate them. The key is to fix the process, not bypass it.

Officers and directors are expected to work within these rules, guidelines, principles and objectives. In this Society, as in our daily work lives, there are temptations by those with responsibility to streamline decisions at the expense of the process. My role is to ensure that we abide by our Bylaws and Operating Manual. I feel that if we were to do otherwise, we would not be keeping our commitment to our membership.

All of these documents are available on the Society Website at www.system-safety.org/ecdocs/.

— Robert Schmedake
To DAL or Not to DAL?

by Clif Ericson

As many readers know, DAL refers to "design assurance level" — or is it "development assurance level?" I have seen both. Either way, the DAL concept is a nifty idea whereby a system, subsystem or software item is built to a specified DAL. There are typically five DALs, where level one (or level A) requires the most stringent development rigor, while each lower level requires less rigor. This methodology presumes that the more rigor applied, the safer the resulting design; however, there does not seem to be evidence supporting this theory. ARP-4754A now has multiple DAL levels; there is the Functional DAL (FDAL) and the Item DAL (IDAL). Does this strike anyone else as confusing? My concern is: Do DALs replace or ignore the proven system safety process? ARP-4754A does not even call out or discuss hazard analysis, hazard risk or hazard elimination/mitigation. What am I missing here?

The first technical paper in this issue, "The Use of Safety Cases in Certification and Regulation" by Dr. Nancy Leveson, discusses the certification of safety-critical systems using safety assurance cases and global methods, including the impact of regulations. This paper uses the term "assurance cases" in general and limits the use of the term "safety case" to a specific definition as an argument for why the system is safe. It also examines the use of safety cases and some dangers associated with their use.

The second technical paper in this issue, "Safety Implications of Software in Safety-Critical Devices" by Amber Schauf, discusses three specific cases in which a software error was the culprit in a safety-critical device. While discussing software errors, this paper elucidates the relationship between electronics and software.

In his "System Safety in Healthcare" column, Dev Raheja discusses the "Swiss Cheese Model for Investigating the Causes of Adverse Events." He expands upon Reason's Swiss Cheese model for human error and describes how it is used in the healthcare industry.

In his "Gains from Losses" column, John Livingston delves into how the Tennessee Valley Authority (TVA) has made a significant impact on the Huntsville, Alabama area during the last 80 years. He discusses some myths, misperceptions and truths regarding commercial nuclear power safety.

In his "Unintended Consequences" column, Terry Hardy describes a past mishap and the lesson learned from that mishap. The mishap in this issue is the TWA Flight 800 accident, which occurred on July 17, 1996. In case you have forgotten, this is a significant lessons learned regarding ignition of fuel in the center wing fuel tank, where the tank was regarded as being ignition source-free.

In their Outside the Lines Column, Benner and Rimson discuss the state of the International System Safety Society. They suggest that the ISSS has never subjected itself to an analysis similar to those its members apply to the hazards and risks, and that perhaps we should. In their column, they present a system safety analysis of the ISSS. In order to understand concerns and challenges to the ISSS, they have developed a short questionnaire they would like readers to respond to. They will devote a future column to the results of this survey, so please participate.

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

Until next time,
Clif
**Outside the Lines**

"The ISSS at Half a Century"

by Ira J. Rimson and Ludwig Benner, Jr.

Where does the International System Safety Society stand today, and what is its future? As the ISSS approaches its 50th anniversary, we think it appropriate and useful to explore the Society's future service to its members and their professional needs. If members support this initiative, we'll try to prepare a system safety analysis (SSA) of the Society in next year's columns. We'll need your inputs, including your expectations of the Society and how well its activities fulfill your professional needs. We'll use your feedback to address questions like:

- Are the Society's activities valuable enough to keep old members and attract new ones?
- What risks might jeopardize its membership maintenance and growth?
- What can it do to reduce those risks and improve its value to its members?

Our goal is to stimulate constructive critiques of the Society's current "system state," with the objective of improving its value to its members, to potential members, and to their clients.

**QUO VADIS, ISSS?**

In the early 1960s, managers, scientists and engineers implemented a new approach to dealing with safety risks that could threaten the success of the U.S. Air Force's ICBM and NASA's major aerospace programs, which were more complex than any systems designed previously. In 1963, Roger Lockwood and others who shared a common investment in the potential for the new system safety process founded a new organization to support their long-range visions for more widespread system safety application. They called their new organization the Aerospace System Safety Society.

We know how far system safety and its professional practices have come in the Society's first 50 years. But what about the future? Can the ISSS meet the safety demands of all the systems whose complexities continue to multiply throughout our technological world? Will continuing the Society's current activities fulfill the future professional needs of its members? How can the Society support the needs of the profession and its members' goal of hazard and risk reduction?
Outside the Lines

"The ISSS at Half a Century"

by Ira J. Rimson and Ludwig Benner, Jr.

Page: 1 | 2 | 3 | 4

To our knowledge, the ISSS has never subjected itself to an analysis similar to those its members apply to the hazards and risks of others. What if we were to view the Society itself as a "system," and subject it to analysis? Could this analysis disclose hazards and risks that might adversely affect the Society's future? With the cooperation of the Society's management and membership, we propose to subject it to a system safety analysis.

First, we will attempt to define the Society as a system by using information posted on its Website. After that, we'll add data from inputs we get from both management and the members. After defining the "ISSS system," we'll try to identify and define both internal and external hazards and their resultant risks, using system safety hazard analysis tools and members' evaluations of current operations. In analyzing the Society's hazards and risks, we hope to be able to suggest actions that it could take to subdue those risks and increase its value in fulfilling member needs.

ISSS System's Objectives

At the outset, the Society's objectives must be robustly defined to be used as metrics against which to measure its accomplishments. We have begun by collecting information from the Society's Website\(^1\), where its objectives are reported, or can be inferred:

- Advancing the state of the art of system safety
- Contributing to a meaningful managerial and technological understanding of system safety
- Disseminating newly developed system safety knowledge to all interested groups and parties
- Improving the public understanding of the system safety process and discipline
- Promoting system safety to all levels of management, engineering and other professional groups
- Fostering communication within the system safety profession, and with other scientific, legal, public and professional groups
- Encouraging research into the development and application of new safety management, scientific or engineering techniques
- Encouraging system safety professional development and education

\(^1\) http://www.system-safety.org/about/
ISSS System Components

The ISSS system's components are Society-sponsored functions and activities by which it achieves its objectives, identified on its Website as:

1. Organizational management and administration, including administrative forms, records and reports:
   - The Society's organizational management and administration should achieve orderly operations, organizational sustainability and satisfaction of its legal responsibilities. These processes include selecting personnel who manage the Society and its activities, providing funding and staffing resources for the Society's operations, and establishing and evaluating its goals and professional policies.

2. Chapter meetings:
   - Members' professional development results principally from personal interactions and knowledge shared at meetings of local chapters.

3. Annual conferences:
   - Annual conferences are forums at which papers examining new and innovative progress in system safety are presented and discussed among attendees, contributing to members' professional development.

4. Bi-monthly Journal of System Safety:
   - The print and online Journal of System Safety adds to the professional development of members with discussions of provocative and useful system safety information and applications to a wide audience.

5. Online technical resources:
   - Online technical resources for members include system safety-related government documents, links to relevant Websites, papers from historic conferences and articles from the Journal of System Safety.

6. Providing professional position inputs to other entities:

These components generate outputs that benefit the membership. To analyze the system processes that produce these outputs, we need to decompose them:
The ISSS has contributed to rulemaking proceedings, and is represented on the Board of Certified Safety Professionals.

7. **ISSS Bulletin Board:**
   The ISSS Website contains a bulletin board accessible to members.

8. **Online employment opportunities:**
   Members may submit and access posting of job openings on the Website.

9. **The Tech Fellows' Corner:**
   Fellow members can share their knowledge and experience by posting articles or white papers, or engaging in dialogue in this section of the Website.

---

2 http://www.system-safety.org/jss/
3 http://www.system-safety.org/ — under “Products and Resources”
4 http://www.system-safety.org/techfellows/
"The ISSS at Half a Century"

by Ira J. Rimson and Ludwig Benner, Jr.

What Next?

To help the ISSS meet future challenges and flourish as it moves into its next 50 years, we need to hear members' thoughts about our Society:

- What did you expect of the Society when you joined?
- How well have those expectations been met?
- How has it helped you meet your professional needs?
- What do you expect your membership in the "ISSS system" to provide to you in the future?
- What ISSS system goals and components do we need to change or add to make it ready for a system safety analysis?

We'll use your feedback to improve the accuracy of the Society's model and report it in our next column. Please send your feedback to us at journal@system-safety.org by January 31, 2012.

Copyright © 2011 by Ira J. Rimson and Ludwig Benner, Jr. All rights reserved.
While in the past most assurance was prescriptive (either product or process), there has been interest in performance-based regulation and assurance by government agencies, starting in the U.S. during the Reagan administration, often spearheaded by pressure from those being certified.

### Types of Regulation

Safety assurance and certification methods differ greatly among industries and countries. Safety assurance methods commonly used can be broken into two general types, which determine the argument used in the assurance or certification process:

1. **Prescriptive**: Standards or guidelines for product features or development processes, which are used to determine whether a system should be certified, are provided.
   
   **A. Product**: Specific design features are required, which may be specific designs, as in electrical codes, or more general features, such as fail-safe design or the use of protection systems. Assurance is usually provided by inspection of the design features provided to determine if they are effective and implemented properly. In some industries, practitioners are licensed based on their knowledge of the standards or codes of practice. Assurance then becomes the responsibility of licensed practitioners, who can lose their license if they fail to follow the standards. Organizations may also be established that produce standards and provide certification, such as the UL rating.

   **B. Process**: Here, the standards specify the process to be used in producing the product or system, or in operating it (e.g., maintenance or change procedures), rather than the specific design features of the product or system itself. Assurance is based on whether the process was followed and, sometimes, on the quality of the process or its artifacts. The process requirements may specify:
   
   - General product or system development processes and their artifacts, such as requirements specifications, test plans, reviews, analyses to be performed and documentation produced
   - The process to be used in the safety engineering of the system and not the general development process used for the product.
Performance-based or goal-setting approaches focus on desired, measurable outcomes rather than required product features or prescriptive processes, techniques or procedures. The certification authority specifies a threshold of acceptable performance and a means for assuring that the threshold has been met. Basically, the standards set a goal, which may be a risk target, and it is usually up to the assurer to decide how to accomplish that goal. Performance-based regulation specifies defined results without specific direction regarding how those results are to be obtained. An example is a requirement that an aircraft navigation system must be able to estimate its position to within a circle with a radius of 10 nautical miles with some specified probability.

While in the past most assurance was prescriptive (either product or process), there has been interest in performance-based regulation and assurance by government agencies, starting in the U.S. during the Reagan administration, often spearheaded by pressure from those being certified. A similar, but much more successful, movement was started in Great Britain around the same time, some of it stemming from the Cullen report on the Piper Alpha accident [Ref. 2].

Certification in the U.S. primarily uses prescriptive methods, but mixes the two types (product and process). Commercial aircraft, for example, are certified based on airworthiness standards requiring specific features (e.g., oxygen systems and life preservers), and more general features such as fail-safe design. Certification also requires the use of various types of safety analysis techniques, such as Fault Hazard Analysis, and general engineering development standards. NASA also uses both product and process standards.

While the Nuclear Regulatory Commission requires prescriptive assurance for nuclear power plants, the American Nuclear Society in 2004 called for the use of risk-informed and performance-based regulations for the nuclear industry, arguing that,

"Risk-informed regulations use results and insights from probabilistic risk assessments to focus safety resources on the most risk-significant issues, thereby achieving an increase in safety while simultaneously reducing unnecessary regulatory burden produced by deterministic regulations." [Ref. 1]

Similar arguments have been made about FAA regulations and procedural handbooks being inflexible and inefficient, and about rule-making taking too long. Recommendations have been made to redesign the rulemaking process by moving to performance-based regulations where appropriate, but this type of certification is controversial, particularly with respect to how the performance goals are set and assured.

next page »
The Use of Safety Cases in Certification and Regulation

by Nancy Leveson, Aeronautics and Astronautics/Engineering Systems, MIT

Assurance Cases

Assurance Cases

Often, certification is a one-time activity that follows the development process and occurs before the product or system is allowed to be marketed or used. For complex systems, such as aircraft and nuclear power plants, certification may involve both initial approval and oversight of the operational use of the system. Changes to the original system design and certification basis may require re-certification activities.

All certification is based on "arguments" that the certification approach has been followed. Inspection and test may be used if the certification is based on following a product standard. If the certification is based on the process used, engineering artifacts or analyses may be required and reviewed. Performance-based regulation may require a particular type of analysis (such as the use of specific types of probabilistic risk assessment), or may allow any type of reasoning that supports having achieved a particular performance goal.

As an example, the U.S. Department of Defense (DoD) in MIL-STD-882 [Ref. 18] uses a prescriptive process that details the steps that must be taken in the development of safety-critical systems to ensure that they are safe. The purpose of the safety assessment report (SAR), which is used as the basis for certification, is to describe the results of the prescribed steps in the standard. The SAR contains the artifacts of the prescribed process, such as a Safety Plan (which must be approved by the DoD at the beginning of the development of the system), a Preliminary Hazard Analysis, a System Hazard Analysis, a Subsystem Hazard Analysis, an Operating System Hazard Analysis, etc. The DoD evaluates the quality of the process artifacts provided in the SAR as the basis for approving use of the system.

While NASA has recently been influenced by the nuclear power community emphasis on probabilistic risk analysis, traditionally it has taken — and continues to emphasize — an approach similar to that of the U.S. DoD. The U.S. Federal Aviation Authority (FAA) approach to civil aviation has also been overwhelmingly prescriptive, and the initial certification has been based on the quality of the prescribed process used to develop the aircraft and the implementation of various airworthiness standards in the aircraft's design. Operational oversight is based on inspection, as well as feedback about the safety of the operations process. Recently, the FAA has moved to create a requirement for a safety management system by those developing or operating aviation systems to shift more of the responsibility for safety to the airframe manufacturers and airlines.

The type of evidence required and assurance arguments used are straightforward with prescriptive regulation, but performance-based regulation requires a more complex argument and evaluation strategy. While the term "safety case" may be used in prescriptive regulation, it is more commonly used in a performance or goal-based regulatory regime.

Performance-Based Regulation and Safety Cases

Government oversight of safety in England started after the Flixborough explosion in 1974, but the term safety case seems to have emerged from a report by Lord Cullen on the Piper Alpha disaster in the offshore oil and gas industry in 1988, where 167 people died. The Cullen report on the Piper Alpha loss, published in 1990, was scathing in its assessment of the state of safety in the industry [Ref. 2]. The Cullen report concluded that safety assurance activities in the offshore oil industry were:
The type of evidence required and assurance arguments used are straightforward with prescriptive regulation, but performance-based regulation requires a more complex argument and evaluation strategy. The report suggested that regulation should be based around "goal setting," which would require that stated objectives be met, rather than prescribe detailed measures to be taken [Ref. 21], i.e., performance-based rather than prescriptive. In such a regime, responsibility for controlling risks shifted from the government to those who create and manage hazardous systems in the form of self-regulation. This approach has been adopted by the British Health and Safety Executive and has been applied widely to industries in that country.

The British safety case philosophy is based on three principles [Refs. 9 and 17]:

- Those who create risks are responsible for controlling those risks
- Safe operations are achieved by setting and achieving goals, rather than by following prescriptive rules. While the government sets goals, operators develop what they consider to be appropriate methods to achieve those goals. It is up to the managers, technical experts and operations/maintenance personnel to determine how accidents should be avoided
- All risks must be reduced so that they are below a specified threshold of acceptability

When performance-based or goal-based certification is used, there are differences in how the performance or goals are specified and how the evaluation will be performed. In 1974, the creation of the Health and Safety Executive (HSE) was based on the principle that safety management is a matter of balancing the benefits from undertaking an activity and protecting those who might be affected by it — essentially cost-benefit analysis (CBA). The HSE also instituted the related concept of ALARP or "as low as reasonably practicable," and widely used probabilistic risk analysis as the basis for these goals. Each of these is controversial.

The nuclear power industry was probably the first to use probabilistic risk analysis as a basis for certification. In the U.K., the Nuclear Installations Act of 1965 required covered facilities to create and maintain a safety case to obtain a license to operate. The nuclear industry has placed particular emphasis on the use of Probabilistic Risk Assessment (PRA) with the use of techniques such as Fault Tree and Event Tree Analysis. Because of the use of standard designs in the nuclear power community and slow introduction of new technology and innovation in designs, historical failure rates are often determinable.

Other potentially high-risk industries, such as the U.S. nuclear submarine community, take the opposite approach. For example, SUBSAFE does not allow the use of PRA [Ref. 12]. Instead, SUBSAFE requires Objective Quality Evidence (OQE), which may be qualitative or quantitative, but must be based on observations, measurements or tests that can be verified. Probabilistic risk assessments for most systems, particularly complex systems, cannot be verified.

A second unique aspect of the British approach to safety assurance required by the HSE is argumentation and approval based on whether risks have been reduced as low as is reasonably practicable (ALARP). Evaluating ALARP involves an assessment of the risk to be avoided, an assessment of the sacrifice (in money, time and trouble) involved in taking measures to avoid that risk, and a comparison of the two. The assumed level of risk in any activity or system determines how rigorous, exhaustive and transparent the risk analysis effort has been. "The greater the initial level of risk under consideration, the greater the degree of rigor required to demonstrate that risks have been reduced so far as is reasonably practicable." [Ref. 7].

The application of ALARP to new systems, where "reasonably practicable" has not yet been defined, is questionable. Not increasing the accident rate in civil aviation above what it is today seems like a reasonable goal, given the current low rate, for example, but it is not clear how such an evaluation could be performed for new technologies (such as satellite navigation and intensive use of computers), or the new and different procedures that are planned. There are also ethical and moral questions about the acceptance of the cost-benefit analysis underlying the ALARP principle.
While none of these more controversial aspects of assurance and certification need to be present when using a "safety case" approach, they are part and parcel of the history and foundation of safety cases and performance-based regulation.
An important component of mindset is the concept of confirmation bias. Confirmation bias is a tendency for people to favor information that confirms their preconceptions or hypotheses, regardless of whether the information is true. People will focus on and interpret evidence in a way that confirms the goal they have set for themselves. If the goal is to prove the system is safe, they will focus on the evidence that shows it is safe and create an argument for safety. If the goal is to show the system is unsafe, the evidence used and the interpretation of available evidence will be quite different. People also tend to interpret ambiguous evidence as supporting their existing position. Experiments have repeatedly found that people tend to test hypotheses in a one-sided way, by searching for evidence consistent with the hypothesis they hold at a given time. Rather than searching through all the relevant evidence, they ask questions that are phrased so that an affirmative answer supports their hypothesis. A related aspect is the tendency for people to focus on one possibility and ignore alternatives. In combination with other effects, this one-sided strategy can obviously bias the conclusions that are reached.

Confirmation biases are not limited to the collection of evidence. The specification of the information is also critical. Fischhoff, Slavin and Lichtenstein conducted an experiment in which information was left out of fault trees. Both novices and experts failed to use the omitted information in their arguments, even though the experts could be expected to be aware of this information. Fischhoff et al attributed the results to an "out of sight, out of mind" phenomenon. In related experiments, an incomplete problem representation actually impaired performance because the subjects tended to rely on it as a comprehensive and truthful representation — they failed to consider important factors omitted from the specification. Thus, being provided with an incomplete problem representation
Confirmation bias. Confirmation bias is a tendency for people to favor information that confirms their preconceptions or hypotheses, regardless of whether the information is true. People will focus on and interpret evidence in a way that confirms the goal they have set for themselves.

These problems are not easy to eliminate, but they can be reduced by changing the goal. The author's company was recently hired to conduct a non-advocate safety assessment of the new U.S. Missile Defense system for the hazard “inadvertent launch,” which was the major concern at the time [Ref. 15]. The system safety engineers conducting the independent safety assessment did not try to demonstrate that the system was safe; everyone was already convinced of that, and they were prepared to deploy the system based on that belief. The developers thought they had done everything they could to make it safe, and had constructed a “safety case” argument during development that justified their belief in its safety. By law, however, the government was required to perform an independent risk analysis before deployment and field testing would be allowed. The goal of the independent assessment was to show that there were scenarios in which inadvertent launch could occur, not to show that the system was safe. The analysis found numerous such scenarios that had to be fixed before the system could be deployed, resulting in a six-month delay for the Missile Defense Agency and expenditure of a large amount of money to fix the design flaws. The difference in results was partly due to the use of a new, more powerful analysis method, but also involved a different mindset and a different goal, which was to identify unrecognized hazards rather than to argue that the system was safe (that inadvertent launch could not occur).

Engineers always try to build safe systems and to verify to themselves that those systems will be safe. System safety engineering adds value by taking the opposite approach: to show that the system is unsafe. Otherwise, safety assurance becomes simply a paper exercise that repeats what the engineers are most likely to have already considered. It is for exactly this reason that Haddon-Cave recommended in the Nimrod accident report that safety cases should be relabeled “risk cases” and the goal should be “to demonstrate that the major hazards of the installation and the risks to personnel therein have been identified and appropriate controls provided” [Ref. 5] — not to argue that the system is safe.

A final potential problem with safety cases, which has been criticized in the offshore oil industry approach to safety cases and with respect to the Deepwater Horizon accident (and was also involved in the Fukushima Daichi nuclear power plant events), is not using worst-case analysis [Ref. 8]. The analysis is often limited to what is likely or expected, and doesn't include what could be catastrophic. Simply arguing that the most likely case will be safe is not adequate: Most accidents involve unlikely events, often because of wrong assumptions about what is likely to happen and about how the system will operate or be operated in practice. Effective safety analysis requires considering worst cases.

But while theoretical arguments against safety cases are interesting, the proof is really "in the pudding." How well have they worked in practice?
Unfortunately, careful evaluation and comparison between approaches has not been done. Most papers about safety cases express personal opinions or deal with how to prepare a safety case, but not whether it is effective. As a result, there is no real evidence that one type of regulation is better than another.

Experience with Safety Cases

The use of performance-based regulation has not necessarily proven to be better than the other approaches in use. One of the most effective safety programs ever established, SUBSAFE [Ref. 12] — which has had no losses in the past 48 years, despite operating under dangerous conditions — is the almost total opposite of the goal-based orientation of the British form of the safety case. The spectacular SUBSAFE record is in contrast to the U.S. experience prior to the initiation of SUBSAFE, when a submarine loss occurred on average every two to three years. SUBSAFE uses a prescriptive approach, as does the civil aviation community, which has also been able to reduce accident rates down to extremely low levels and keep them there.

The use, or at least poor use, of safety cases has been implicated in accident reports. The best known of these is the Nimrod aircraft crash in Afghanistan in 2006. A safety case had been prepared for the Nimrod, but the accident report concluded that the quality of that safety case was gravely inadequate [Ref. 5]:

"...the Nimrod safety case was a lamentable job from start to finish. It was riddled with errors... Its production is a story of incompetence, complacency, and cynicism... The Nimrod Safety Case process was fatally undermined by a general malaise: a widespread assumption by those involved that the Nimrod was 'safe anyway' (because it had successfully flown for 30 years) and the task of drawing up the Safety Case became essentially a paperwork and 'tickbox' exercise."

The criticisms of safety cases contained in the Nimrod report include:

- The Safety Case regime has lost its way. It has led to a culture of "paper safety" at the expense of real safety. It currently does not represent value for money.
- The current shortcomings of safety cases in the military environment include bureaucratic length, obscure language, a "failure to see the wood for the trees," archaeological documentary exercises, routine outsourcing to industry, lack of vital operator input, disproportionality, ignoring of age issues, compliance-only exercises, audits of process only and prior assumptions of safety and "shelf-ware".
- Safety cases were intended to be an aid to thinking about risk, but they have become an end in themselves.
- Safety cases for "legacy" aircraft are drawn up on an "as designed" basis, ignoring the real safety, deterioration, maintenance and other issues inherent in their age.
- Safety cases are compliance-driven, i.e., written in a manner driven by the need to comply...
with the requirements of the regulations, rather than being created as working documents to improve safety controls. Compliance becomes the overriding objective, and argumentation tends to follow the same, repetitive, mechanical format that amounts to no more than a secretarial exercise (and, in some cases, have actually been prepared by secretaries in outside consultant firms). Such safety cases also tend to give the answer that the customer or designer wants, i.e., that the platform is safe.

- Large amounts of money are spent on things that do not improve the safety of the system.

Haddon-Cave, the author of the Nimrod accident report, concluded that safety cases should be renamed "risk cases," and made the following recommendations (among others):

- Care should be taken when utilizing techniques such as Goal Structured Notation or "Claims-Arguments-Evidence" to avoid falling into the trap of assuming the conclusion ("the platform is safe"), or looking for supporting evidence for the conclusion instead of carrying out a proper analysis of risk. (Note the similarity to the concerns expressed earlier about mindset and confirmation bias.)
- Care should be taken when using quantitative probabilities, i.e., numerical probabilities such as $1 \times 10^{-6}$ equating to "remote." Such figures and their associated nomenclature give the illusion and comfort of accuracy and a well-honed scientific approach. Outside the world of structures, numbers are far from exact.
- Care should be taken when using historical or past statistical data. The fact that something has not happened in the past is no guarantee that it will not happen in the future. Piper Alpha was ostensibly "safe" on the day before the explosion. The better approach is to analyze the particular details of a hazard and make a decision on whether it represents a risk that needs to be addressed.
- Care needs to be taken to define the process in which new hazards can be added to the Risk Case, incorporated in the Hazard Log and dealt with in due course, as well as how original assumptions about hazards or zones are to be re-examined in light of new events.
- Once written, the safety case should be used as an ongoing operational and training tool. There are all too many situations where a comprehensive safety case is written, and then sits on a shelf, gathering dust, with no one paying attention to it. In such situations, there is a danger that operations personnel may take the attitude, "We know we are safe because we have a safety case."
The Use of Safety Cases in Certification and Regulation

by Nancy Leveson, Aeronautics and Astronautics/Engineering Systems, MIT

Vol. 47, No. 6 • November-December 2011

Conclusion

To avoid confirmation bias and compliance-only exercises, assurance cases should focus not on showing that the system is safe, but on attempting to show that it is unsafe. It is the emphasis and focus on identifying hazards and flaws in the system that provide the "value-added" of system safety engineering. System engineers have already created arguments for why their design is safe. The effectiveness in finding safety flaws by system safety engineers has usually resulted from the application of an opposite mindset from that of the developers.

Whatever is included in the assurance case, the following characteristics are important:

- The process should be started early. The assurance case is only useful if it can influence design decisions. That means it should not be done after a design is completed or prepared in isolation from the system engineering effort. If safety cases are created only to argue that what already exists is safe, then the effort will not improve safety and becomes simply a paper exercise to get a system certified. One result might be unjustified complacency by those operating and using the systems.
- The assumptions underlying the assurance case should be continually monitored during operations, and procedures should be established to accomplish this goal. The system may be working, but not the way it was designed, or the assumptions may turn out to be wrong, because of poor prediction or because the environment has changed. Changes to the system and its environment may have been made for all the right reasons, but the drift between the system as designed and the system as enacted is rarely if ever analyzed or understood as a whole, even when each particular deviation appears sensible or even helpful to the individuals involved.
- To make maintaining the assurance case practical, the analysis needs to be integrated into system engineering and system documentation so that it can be maintained and updated. Safety assurance is not just a one-time activity; it must continue through the lifetime of the system, including checking during operations that the assumptions made in the assurance argument remain true for the system components and the system environment. The problems in updating and maintaining safety assurance do not arise from the form of the assurance documentation or in updating the argument once the need for it is established; rather, problems arise in relating the assurance case to the detailed design decisions so that when a design is changed, it is possible to determine what assumptions in the safety analysis are involved.
- The analysis should consider worst cases, not just likely or expected cases (called a design basis accident in nuclear power plant regulation).
- The analysis needs to include all factors, and be comprehensive. It should include not just hardware failures and operator errors, but also management structure and decision-making. It must also consider operations, and the updating process must not be limited to development and certification, but must continue through the operational part of the system lifecycle.
- To be most useful, qualitative and verifiable quantitative information must be used, not just probabilistic models of the system.
- The integrated system must be considered, rather than considering each hazard or component in isolation.

References
There are multiple factors that lead to software failure. Companies are under extreme pressure to be the first entity to get a functioning product on the market. In addition, the pace at which technology is created continues to increase at an exponential rate. Because traditional safety methods do not work in a fast-paced development and acquisition market, this results in critical errors in products. Examples of these errors can be found across all engineering disciplines. This paper will discuss three specific cases in which a software error was the culprit in a safety critical device.

The Electronics Race

There are many aspects of creating a product intended for mainstream usage — the main factors in product development are the costs associated with designing the product and the time necessary to create a prototype for mass production purposes. These are the concerns that every company in both the private and government sectors take into consideration before funneling funds into a project. If the basic needs are not met, it could mean great financial loss for that company.

The consumer determines what new product is needed by the market. Corporations hire marketing and research companies to enter the field and assess what product should be targeted for production. Once a product is determined to be marketable, it is handed over to the design team to create a device that fits the specifications of that need. The average time for a product to make it to mainstream market is solely based on the product category and the market climate for that product. For instance, an aftermarket device designed to increase fuel efficiency in vehicles would be widely accepted in today's economic situation, whereas a device designed to heat a pool that doubles the energy consumption rate would be seen as interesting, but too costly for a consumer to justify using.

The consumer determines what new product is needed by the market. Corporations hire marketing and research companies to enter the field and assess what product should be targeted for production. Once a product is determined to be marketable, it is handed over to the design team to create a device that fits the specifications of that need. The average time for a product to make it to mainstream market is solely based on the product category and the market climate for that product. For instance, an aftermarket device designed to increase fuel efficiency in vehicles would be widely accepted in today's economic situation, whereas a device designed to heat a pool that doubles the energy consumption rate would be seen as interesting, but too costly for a consumer to justify using.

In addition to the design of the new product, there are also fees incurred through legal departments, the building of scaled prototypes, building real-sized test and the costs of testing those products. Contract bids are placed with companies to see who would like to buy the product. Consumer data-gathering studies are done to make the product more alluring to potential clients. Patents are acquired to protect designs from other companies trying to create the same product first. All of this is done without the guarantee that the creator will be successful in finding someone to purchase the product.

While safety is a highly regarded measure, companies are under great strain to beat the competition
to the mainstream marketplace. The supply and demand for newer, better consumer products, for a military weapon that is more efficient and more powerful than the enemy's, or for faster, more accurate healthcare equipment far exceeds the current wait period for necessary patents, rigid safety testing and complete data gathering. The economics of placing a competitive product on the market first creates an environment where shortcuts are taken at the expense of safety.
In the Spotlight

Safety Implications of Software in Safety-Critical Devices

by Amber D. Schauf

The Birth of Electronics

Electricity is a fundamental force of nature that is present in every aspect of daily life. It is defined as a "form of kinetic or potential energy created by the free or controlled movement of charged particles such as electrons, positrons and ions" [Ref. 1]. It consists of two charged particles, positive and negative; the positive charges will repel other positive charges, but attract negative charges. The same occurs for negative charges; a negatively charged particle attracts only positively charged particles. Only one negative and one positive particle can attract to each other, creating a net charge of zero. This is explained by the Law of the Conservation of Energy: electric charge is conserved; it cannot be created nor destroyed, and the sum of all charge in a system remains unchanged.

1. Early Devices

The study of electricity has been validated back to the writings of Thales of Miletus in 600 BCE. It was found that if you rubbed fossilized amber, the substance would become charged. One device that came to the attention of archeologists in 1938 was the Battery of Babylon, also known as the Battery of Baghdad, which is located in Iraq. The device is a six-inch high clay pot that contained a copper cylinder soldered shut with a lead-tin alloy.

![Battery of Babylon](Ref. 2)
When an acidic agent was poured into the pot, a chemical reaction occurred that produced a small, electric current. When several of these pots were placed in series, there was enough voltage created to allow for the electroplating of metals. Scientists also believe that this device could have been used for religious purposes.

Other than these two documented occurrences, there were no real advances until 1600 AD. An English scientist by the name of William Gilbert began documenting the electrical properties of several known substances and named the phenomenon electricity, derived from the Greek word for amber. It is through his work that he has been named the Father of Modern Electricity.

Following Gilbert’s work, a series of electrical experiments took place. In 1660, a German scientist, Otto von Guericke, invented the first electrostatic generator, the “Elektrisiermaschine” [Ref. 2]. This device (Figure 2) could produce static electricity (high voltage, continuous current) via friction.

Figure 2 — Elektrisiermaschine [Ref. 3].

Many electrical studies ensued after the invention of the electrostatic generator. In 1745, Pieter van Musschenbroek developed the Leyden (Leiden) Jar, the first electrical capacitor.
The glass jar had a metal coating on both its inside and outside, but the surfaces did not come in contact with each other. An electrode was connected to the inner foil and protruded out of the opening of the jar. The electrostatic generator was then connected to the electrode and the outer foil was connected to a grounded source. The inner surface would store the positive charge, while the outer surface stored the negative charge; the net charge of the entire system was equal to zero. These two inventions provided scientists with instant electrical current. This allowed for controlled experimentation with electrical devices. Much of the work of Nikola Tesla, Thomas Edison and Benjamin Franklin came from working with these two devices, and has led us to the modern world in which we now live.
Vol. 47, No. 6 • November-December 2011

In the Spotlight

Safety Implications of Software in Safety-Critical Devices
by Amber D. Schauf

Pages 1 | 2 | 3 | 4 | 5

2. Modern Development

Turning the clocks ahead to present day, we find that electric devices that were large and cumbersome to carry around have now been reduced in size to devices not capable of being seen by the naked eye. These products now exist in the majority of what we touch and use, and are an integral part of our lives. Instead of paper and pen to write letters, electronic messages are sent through invisible waves to international destinations in the blink of an eye. Modern warfare is now conducted from behind a computer screen, as opposed to lines of soldiers packed shoulder to shoulder on a front line. Medicine is delivered at the click of a button, and heartbeats are measured by blipping lines on a screen. All of these marvels take place on a micro- and nano-scale field.

Transistors were first patented in 1925, but did not come to fruition until 1947 by a couple of American physicists working for AT&T’s Bell Labs. The first silicon transistor was developed in 1954; in 1958, the first integrated circuit (in which a transistor is incorporated) was created and only two years later, the Metal Oxide-Semiconductor Field Effect Transistor (MOSFET) was invented.

Since the 1970s, the complexity of integrated circuits has doubled every two years, while the size decreases exponentially. Today, we are able to build circuits on the nanoscale (nanotechnology) that

Figure 4 — Transistor Schematic [Ref. 5].
are being used for various purposes — some examples are electronic products, cancer treatments and accelerometers. However, with all of these electrical advances we are still in need of a command system that tells the brain of the circuit what to do — i.e., software.

Software and Programming Development

The concept of programming a device can be traced to Greek Mythology; the Antikythera Mechanism is an ancient mechanical computer that was built around 150-100 BCE and was used to calculate astronomical positions. Programs have gone from analog/mechanical machinery to the lines of digital code used in today's products. Software programs are a necessary part of integrated circuits; without a set of explicit instructions, the circuit is unable to function as designed. While there are several tools designed to facilitate staying on task in developing a program, one of the most widely used methods is the waterfall method.

![Waterfall Model for Software Development](Ref. 6)

The waterfall model details the order that a software developer should follow to be able to complete a successful program:

- **Requirements**: Verify what the customer is asking for and what the expected end product is supposed to do.
- **Design**: Create a program around the general requirements and estimate the cost of the project based on the work effort needed to complete it. This is usually referred to as a scope document and can function as a legal contract between parties.
- **Implementation**: The code for the program is written. It is then tested for defects in the code line and documented for future usage.
- **Verification**: The software engineer double checks the scope document to verify that the program has been designed and developed to the required specifications.
- **Maintenance**: After the program has been tested and released to the client, it is important to supply software training and support to the client to make certain that the software is functioning properly. If any enhancements need to be made, they are done in this time period.

Safety Engineering and Software

Safety engineering must be an integral part of software design. Many of the safety-critical devices on the current market are dependent on reliable software. For example, almost all commercial airlines "fly by wire." Traditionally, aircraft control surfaces, throttle controls, landing gear, etc. were operated by a series of mechanical devices and cables but, due to the increase in size and weight of aircraft, it became necessary to replace these systems with more sophisticated electromechanical devices driven by software logic. When the controls are activated by the pilot, an electrical pulse runs through the wire and is translated by the software as a command to move the control surfaces, or increase or decrease acceleration. There are also several systems within the aircraft that run built-in tests to ensure that the onboard computer systems are functioning properly prior to take off.

Other systems that rely heavily on software are autonomous (and semi-autonomous) weapon
systems. They are a new and rapidly developing area of the warfare industry. The use of these systems requires a significant level of analysis and test to verify and validate that the system safety requirements are achieved to an acceptable level. Once operational, the systems typically run a "Built-In Test" (BIT) to ensure that the system startup has been successfully completed and that safety features are in place. After successful BIT and in an operational state, the weapon will autonomously follow whatever program has been placed within the system. One of the functions of the weapon is to use sensors to gather data from a target zone and an image processor, then to take that information and process it to identify potential targets. It then passes that information to a fire control system that calculates the data necessary to fire its payload at the potential target.

The healthcare industry also relies on safety-critical devices to monitor, medicate and save patients in the healthcare system. These devices range from IV infusion pumps and vital monitors to machines responsible for delivering accurate doses of medication for cancer treatment. As these devices directly interact with patients, it is paramount that the software that regulates the machinery be free from defect to avoid catastrophic results.
Hazard Assessment

There are two basic design considerations when developing a software system: performance and safety. Meeting performance requirements is normally measured during the test and validation verification phase and does not consider many safety aspects of the design. Consider an automobile with "accelerate by wire" capability. The simple Boolean matrix in Table 1 reflects the possible combinations of message traffic across the software interface for pressing the accelerator, and the importance of including safety considerations in the design.

Table 1 — Boolean Matrix.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Right Message, Right Time</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Right Message, Wrong Time</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Wrong Message, Right Time</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>Wrong Message, Wrong Time</td>
</tr>
</tbody>
</table>

The matrix indicates that other testing and analysis needs to be considered to fully characterize the implications of receiving erroneous messages that could potentially cause fatal accidents due to software errors within the "accelerate by wire" functionality. These errors could manifest as a result of either coding errors and/or timing and sequence problems associated with the hardware design.

There are several methods used to identify hazards and risks in a program. The two most commonly used forms, both private and government sector, are the Fault Tree Analysis (FTA) and the Failure Modes and Effects Analysis (FMEA).

- Fault Tree Analysis: This is an analytical method that starts from the complete system and funnels down through all possible errors the system could suffer. FTA starts with one well-defined, undesirable event and then models the combinations of events that will produce it. It consists of Boolean logic gates (AND, OR, NOT) that trace primary events that cover human error, system failures and outside influences on a system. A fault tree can be evaluated as a qualitative (cut sets and likelihood judgments) or a quantitative (probability of it happening) approach to failure assessment. FTA's are sometimes used in conjunction with an event tree.
Failure Modes and Effects Analysis: Initially developed by the military in the 1940s, FMEA is extensively used by a broad range of industry as a tool to study and reduce failure rates of products. There are three steps in assessing a product using FMEA. The first is severity, to determine all failure modes depending on the functional requirements of the system and their effects as a whole. The second step is occurrence; what is the cause of a failure mode and how many times is it reached. The third is detection. After examining the entire system and the self-detection measures built into the program, what is the level of risk that the failure will escape detection?

Each step has a value from 1 (no danger) to 10 (critical danger) assigned to it. The numbers are then tallied and the system is assigned a Risk Priority Number (RPN). Based on the value of the RPN, corrective measures are then taken to make the safety-critical device safer.
Safety Implications of Software in Safety-Critical Devices

by Amber D. Schauf

Case Study 1: Patriot Missile Defense Weapon Software Failure

On February 25, 1991, during Operation Desert Storm, a Patriot missile defense system operating in Dhahran, Saudi Arabia failed to track and destroy an incoming enemy Scud missile. Due to the failure of the equipment, the missile hit an Army barracks and killed 28 Americans. After a review of the system and the facts of the case, it was determined that the software in the system-critical device was faulty. Reviewers found that the longer the system was left on (operating), the capability of the system to accurately track and identify incoming missiles became unreliable. At the time of this incident, they found the system had been operating for more than 100 hours and was looking in the wrong place for enemy fire. It originally located the incoming missile; however, when it recalculated for the position, the clock timing in the sensor was off, and when it could not locate the missile again, it was looking in the wrong location, it took it off the radar [Ref. 9].

It was also noted in the official report that two weeks prior to the incident, there had been complaints from the Israeli Army (using the same technology) of inaccuracies with the Patriot system after only eight hours of operation. The Army had created a software modification to improve accuracy (not correct the actual problem) and the modification did not reach Dhahran until February 26, 1991 — one day after the catastrophic loss. After repairs to the software, the Patriot system was again deployed in Operation Iraqi Freedom in 2003. The system did not have the same failure.

Case Study 2: Therac-25

The Therac-25 was a radiation therapy machine produced by Atomic Energy of Canada Limited. Its purpose was to deliver predetermined doses of radiation therapy to cancer patients. The error was a software glitch that did not notify the radiation technician that a dose had been delivered to the patient. Instead, it gave an error message that the dose was not delivered when, in fact, it had been dispensed. The technician would then clear the error and hit the button again to deliver the dose. This caused the patient to receive up to 100 times the intended dose of radiation, having lethal results.

During a review of the Therac-25, it was found that AECL did not have an independent review of the software code used by the machine. The user manual did not address the error code displayed to the radiation technician and allowed him or her to override the system without clearing the code. There were also several engineering issues with the device. Used between 1985 and 1987, it was directly responsible for the deaths of six patients and the radiation injuries of several more. As a result of the procedural mitigations, AECL claimed to have achieved a solution but admitted they still didn’t have a known cause. All of the machines were recalled in 1987 [Ref. 10].

Case Study 3: Royal Air Force Chinook

The CH-47 Chinook is a twin-engine, tandem rotor helicopter used for troop movement, the placement of artillery and battlefield re-supply efforts. It is now produced by Boeing Integrated
Defense Systems, and is mainly used by the U.S. Army and the Royal Air Force. On June 2, 1994, a Royal Air Force Chinook helicopter crashed into the Mull of Kintyre, Scotland, killing all 29 people onboard. The first review that came out cited gross negligence on the part of the flight crew for flying in dense fog. However, after a second review in 1996 (in an attempt to clear the flight crew of wrongdoing), the software code responsible for controlling the fly-by-wire system was examined. After going through "only 18 percent of the code, they found 486 anomalies and stopped the review" [Ref. 11]. They also found intermittent engine failures of the Chinook helicopter in question.

**Similarity in Cases**

When reviewing the three case studies, it was found that regardless of whether it was in the government or private sector, software was a key problem in each accident. These problems point to the following possible pitfalls associated with the design and development of safety-critical software:

**Inadequate engineering rigor within the design:**
- Lack of understanding of the intended use of the system
- Inexperienced or no safety professionals involved
- Inappropriate system safety program definition

**Design and development issues:**
- Inadequate requirement definition
- Lack of coding standards or guidelines

**Test and analyses deficiencies:**
- Lack of necessary hazard analyses (PHA, SHA, SSHA, etc.)
- No peer-review code analyses process
- No fault insertion, boundary value, static or dynamic tests

**Configuration management issues:**
- Multiple versions of unregulated software released
- Inability to trace software changes between versions

**Conclusion**

Software intensive systems are becoming more pervasive in all segments of our society, and we rely on these products to provide for our needs in many areas of our lives. It is becoming increasingly necessary for us to consider the negative aspects of operating these systems in a safe manner. It is incumbent upon those producing the products to ensure that safety has been considered during the design and development of potentially dangerous systems.

**References**

One appealing approach to mitigating human errors is the one proposed by James Reason [Ref. 1]. Generally referred to as the "Swiss cheese" model of human error trapping, he describes four levels of human failure, with each level influencing the next (seen in Figure 1). These failures are likened to holes in a Swiss cheese. Working backwards in time from the adverse event, the first level depicts those "unsafe acts" that ultimately led to the mishap.

This level generates the most investigation and, consequently, is the level where most causal factors are uncovered. After all, it is typically the actions or lack thereof that are directly linked to the adverse event. For instance, failing to properly administer a medication may yield grave consequences, as in the recent death in a California hospital where a nurse gave a cancer patient an enteral solution intravenously instead of through a feeding tube [Ref. 2]. Represented as "holes" in the Swiss cheese model, these active failures are typically the last unsafe acts committed by caregivers.

What makes the "Swiss cheese" model particularly useful in investigating adverse events is that it forces investigators to address latent failures within the causal sequence of events. The latent failures are also "holes," but in different slices of cheese. As their name suggests, latent failures, unlike their active counterparts, may lie dormant or undetected for hours, days, weeks or even longer, until one day, they adversely affect the unsuspecting caregiver. Consequently, they may be overlooked by investigators — even those with the best intentions.

Within this concept of latent failures, Reason described three more levels of human failure. The first involves the condition of the caregiver as it affects performance. Referred to as preconditions for unsafe acts, this level involves conditions such as mental fatigue, poor communication and coordination practices, and frequent interruptions. Not surprising, if fatigued caregivers fail to communicate and coordinate their activities, poor decisions are made and errors often result.

![Figure 1 — The "Swiss Cheese" Model of Human Error Causation [Ref. 3].](image)
breakdown in good practices can be traced back to instances of unsafe supervision, the next level of human failure. If, for example, inexperienced caregivers are unfamiliar with certain tasks, such as medication delivery and dosing, or lack experience with utilizing medical equipment — from ventilators to laboratory machines — errors from lack of sufficient supervision are prone to happen. To make matters worse, the lack of quality assurance audits, support system, training and availability of qualified personnel can increase the potential for more errors. In a sense, these caregivers were “set up” for failure.

Reason’s model doesn’t stop at the supervisory level; the organization itself can impact performance at all levels. For instance, in times of fiscal austerity, funding is often cut and as a result, training is curtailed and work load becomes excessive. Not surprisingly, failures will begin to appear, all of which will affect performance and errors. Therefore, it makes sense that if the adverse events are to be prevented, they must be analyzed in entirety and foreseen beyond the caregiver. Ultimately, causal factors at all levels within the organization must be addressed if any prevention system is going to succeed. One needs to know what these system failures or “holes” are, so that they can be identified during investigations or, better yet, detected and corrected before an adverse event occurs.
Swiss Cheese Model for Investigating the Causes of Adverse Events

by Dev Raheja, Associate Editor, Maria C. Escano, MD

The FDA monitors these adverse events. In the case of adverse events secondary to medical devices, the FDA recommends three levels of follow-up. This model might prove useful if applied in a hospital setting. The first level involves damage control — "correction." It refers to recognizing the error and providing an immediate intervention to prevent further harm. The second level involves finding a permanent solution so that the same event never happens again. This level is called the "corrective action." The third level is called "prevention action." This involves looking for system-wide solutions so that similar events never happen in other areas of the hospital. The FDA guideline makes sense in light of the Swiss cheese model.

The Swiss cheese model in healthcare facilities can be applied in numerous ways. We can constantly monitor symptoms and causes of latent hazards in all three levels, namely the conditions of the caregiver, unsafe supervision and causal factors at the organizational level, and mitigate them before any patient safety issue arises. Below are some examples.

**Caregiver level factors:**
- Failure to prioritize; lost focus and attention
- Omission of a step in a procedure
- Inadequate procedure
- Omission of a checklist item
- Inadvertent use of medical device controls
- Use of improper procedure
- Inadequate ability or training
- Wrong response to emergency
- Insufficient safeguards in delivery of medications

**Unsafe supervision factors:**
- Inadequate sanitation habits
- Occasional ignoring of the checklist
- Lack of availability of caregiver support
- Inadequate training of staff and inadequate supervision
- Insufficient enforcement of policies
- Time pressure prevents a junior caregiver from speaking up
- Inadequate use of lessons learned to prevent mishaps
- Insufficient focus on system thinking
- Insufficient training

**Organization level factors:**
- No ongoing senior management reviews of risks and mitigations
- Lack of documented procedure on risk assessment
- Lack of regular review of prevention of adverse events
- Lack of policy for prevention of adverse events
- No measure of policy effectiveness
- Poor cross-functional teams to prevent latent hazards

**Conclusion**

The Swiss cheese model offers a highly effective approach in understanding and preventing adverse events.
events. It facilitates a multi-dimensional view of healthcare delivery, and offers preventive strategies and mitigation solutions in different levels.

References:

2. Woodall, Angela. "Woman who died at Alta Bates may be victim of medical error not medication mistake," Oakland Tribune, September 26, 2011.
Open Letter to Corporate Management about Unmitigated High Risk

The International System Safety Society (ISSS) will be developing a program plan in support of mentoring, research and development. We continue to be involved in many projects, such as developing white papers, developing software safety guides, and applying system safety techniques and methods for automated tools. We are also looking into forensics engineering and system safety applications. Should you have an interest in participation please contact me. If you are currently working on one of our projects, I stand by for your inputs.

Best regards,
— Mike Allocco

Special Offer

In order to reward authors of papers printed in the Journal of System Safety, a special promotion is being offered. For the entire year of 2012, all authors that have papers published in the JSS will receive a free copy of the new book System Safety Primer by C. Ericson. The contents of this book can be reviewed at Amazon.com. Submit a draft of your paper to journal@system-safety.org.
An EF-5 tornado, which passed within seven miles of the Browns Ferry Nuclear Plant, severely damaged transmission towers and lines in the area, cutting all of the lines to the plant except one. The plant went into a shutdown mode at 4:36 p.m. on April 27, which was reported to the NRC as an 'unusual event due to...
Two major sources of electrical energy were also impacted by the loss of transmission lines. The Widows Creek coal-fired plant and the Browns Ferry Nuclear Plant lost many of their connections to the TVA system power grid. The biggest impact was the consequence on the Browns Ferry plant.

An EF-5 tornado, which passed within seven miles of the Browns Ferry Nuclear Plant, severely damaged transmission towers and lines in the area, cutting all of the lines to the plant except one. The plant went into a shutdown mode at 4:36 p.m. on April 27, which was reported to the NRC as an "unusual event due to loss of offsite power." All three of the reactors at the plant were automatically scrambled ("A rapid emergency shutdown of a nuclear reactor"). [Ref. 3]

In a statement released the next day, TVA stated that the three reactors at the plant had shut down safely. Unit 2 and Unit 3 had achieved cold shutdown (less than 212 degrees Fahrenheit) by late the next afternoon. Unit 1 was shut down and cooling to the desired temperature.

The result of the shutdown was a loss of TVA power for 641,000 customers in North Alabama and Mississippi. By May 5, only about 14,000 in the hardest-hit areas were still without power. TVA estimates of the system damage had grown to 107 of its major transmission lines and 350 structures supporting those lines. In a major feat of reconfiguring its network, TVA had managed to restore power to the local power distributors with only about 25 percent of its structures restored.

Browns Ferry remained offline because of the extent of damage to the transmission lines from the plant. For example, the Huntsville Utilities — with 300,000 customers — had eight connection points for power from TVA, but the "restored" system had only two — one from the east, with a repaired 500,000-volt line connecting Huntsville to Widows Creek and Guntersville Dam, and one from the west, with power being supplied by the Sequoyah Nuclear Plant in Tennessee and other sources [Ref. 4].

The last two 500-kilovolt lines and three 161-kilovolt lines in north Alabama were back in service by early July. The TVA reported that in a 74-day, around-the-clock effort, 108 transmission lines had been repaired. The 353 transmission structures and transmission lines that were replaced required 1.4 million pounds of steel and 275 miles of new wire.

"What they've accomplished is truly amazing," said Rob Manning, TVA executive vice president for power system operations. "TVA strives to be among the nation's leaders in customer reliability" [Ref. 5]. In the midst of the successful effort to restore the electrical power system, the TVA received a "red" safety finding on its handling of a hardware problem in the 2008-2010 timeframe.

Browns Ferry Safety

On May 9, 2011, the Nuclear Regulatory Commission announced that a valve that failed (stuck) during the past year at the Browns Ferry plant posed a safety threat that fell into the "red" level category, the most serious on its four-color scale. It was only the fifth time, since the establishment of the ratings scale in 2001, that the NRC had placed a finding in that category.

The valve was located in the reactor's residual heat removal system, which enables the reactor to cool after it has shut down. The failure was discovered when the reactor was shut down for a periodic re-fueling. The system is also an important part of the emergency safing systems used if an accident required the reactor to shut down quickly.

The valve consists of a flat metal disk inside the pipe, which is positioned by a rod. The rod had become disconnected from the disk, apparently weeks or months earlier. The residual heat removal system consists of two separate sets of pumps, valves and piping. One set would not have worked if the valve could not be operated. In certain accident scenarios, loss of the total residual heat removal system could lead to core damage. In response to the finding, the TVC told the NRC that the valve had a manufacturing defect but that it would still have opened if needed. The NRC disagreed.

Specifically, the NRC finding cited a violation of technical specifications involving the failure to implement an inspection program in accordance with the American Society of Mechanical Engineers (ASME) Code for Operation and Maintenance of Nuclear Power Plants. This failure precluded the timely identification that the RHR loop II subsystem was unable to fulfill its safety function due to a failure of the LPCI Outboard Injection Valve. The finding noted that TVA was not able to verify operability and functionality of valves susceptible to stem and disc separations as required by the ASME code. Because the subject valve was inoperable from March 13, 2009 to October 23, 2010, the specification limit for functional outage time (seven days) was exceeded [Ref. 6].

The NRC was unmoved by TVA's response to the finding, rejecting the TVA position that the "red" level finding was not justified. The Commission notified TVA that additional inspections would be
made to provide the NRC with supplemental information on performance, as well as insights into the breadth and depth of safety, organizational and programmatic issues. The objective of the reviews was to aid the NRC in deciding whether additional regulatory actions would be necessary to assure public health and safety. The inspection would also include an assessment of the safety culture at the Browns Ferry Nuclear Plant. The review would center on the validation of TVA's third-party safety culture assessment and root cause evaluation program. The NRC did perform an "independent" review of the original findings and notified TVA in August, 2011 that the assessment by a branch of the NRC not involved in the original investigation confirmed the original finding.

1 Nuclear folklore attributes the term to Enrico Fermi, known for his nuclear "Pile" design, which obtained the first sustained nuclear chain reaction. Dr. Fermi had added two independent (manual) means of stopping the reaction in case of an emergency. One system was to have three "junior physicists" always ready to pour buckets of cadmium sulfate down through the pile if Fermi gave them a certain hand signal. The other system, which was the "primary" system, required a specialist (a logger skillful with an axe) to cut a heavy rope that restrained a poison cadmium rod freeing the weighted rod to fall into the pile. Since the logger needed to concentrate on the rope, Fermi was to holler "scram" as the signal to cut the rope. At the planning meeting, before the big event, the logger asked Fermi "just what does 'scram' mean? Fermi's reply was, "Safety Cut Rope Axe Man." Of course, it was also appropriate advice if both systems failed. See http://www.ornl.gov/info/reporter/no19/scram.htm (ORNL Reporter, September 2000).
Even more questionable is the use of 4,000 pounds for the maximum car mass. In TVA country, parking lots are full of SUVs and trucks which may weigh up to 6,000 pounds. Hopefully, the NRC will re-visit some of its analyses that support its confidence in the current plant design requirements.
A Few System Safety Observations

- To ensure availability when needed, all emergency safing systems should have the capability of periodic verification of operability.
- It is important that hardware performance be continually used to evaluate the effectiveness of proposed hazard controls, whether for operational systems or those used in emergency or contingency situations.
- Changing threats or environments should also be evaluated. For example, the warning coordination meteorologist in the NWS district office in Calera, Alabama has stated; “Seven of 10 significant tornado outbreaks in the state occurred in the last 10 years,” which might call for a review of probability of occurrence assumptions [Ref. 2].
- Changes in operational conditions should be evaluated for potential adverse effects on plant safety. Even though the NRC has approved the use of more dense storage configurations for spent fuel rods in the large storage pools, the presence of the additional rods increases the loads on heat dissipation systems. While the support structure may provide increased resistance to storm debris, the tolerance to debris in the pools may be reduced.
- Beware of “extenuating circumstances” — while the 1975 fire led to a new federal protection law for nuclear power stations, the three Browns Ferry units do not meet the law’s requirements for use of multiple manual safing systems in the same fire zone (fire barriers, smoke detectors and automated suppression; or a minimum separation of 20 feet between redundant circuitry with no intervening combustible materials). While the NRC accepted the TVA’s plan to use operator manual actions to accomplish a post-fire safe shut-down, manual actions (shut down or activation) would be difficult after an EF-5 tornado strike.

Conclusions

The NRC Website (www.nrc.gov) has extensive information on nuclear plants and nuclear materials. The information covers current events (Japan nuclear accident, Virginia earthquake, public meetings and news releases), federal regulations and enforcement, and the basic elements of the agency’s safety program. While issues (including the Browns Ferry Red finding) are identified, there is the general perception that the NRC is meeting its stated purpose “to enable the nation to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected.”

The Union of Concerned Scientists (UCS) is one of several “watchdog” organizations that have a different perception than the NRC on the state of the nuclear power industry in the United States. If you are curious about its views on the safety of your local reactor, log on to the UCS “Nuclear Power Information Tracker” (http://www.ucsusa.org/nuclear_power/reactor-map/embedded-flash-map.html). It is a “reactive” map that has key information links on all U.S. nuclear reactors, including licensing data and safety history. In the case of Browns Ferry Unit 1, five of six safety issue categories are checked (elevated spent fuel pool, fire protection problems, groundwater leaks reported, heightened NRC attention, year plus outages). Given the 1975 event, from an operational history perspective, the sixth category (near misses) would also get my check mark. On June 14, 2011, the UCS’s Nuclear Safety Project Director rated Browns Ferry Unit 1 as “the poorest performing reactor in the entire United States,” ranking 104 in the NRC’s list of 104 operating reactors [Ref. 10].

References:

Book Review

Murder by Electrocution
By David MacCollum

Reviewed by Clifton A. Ericson II

For more than 60 years, the hazard of boom equipment making contact with overhead power lines has been an ever-increasing source of wrongful injuries that maim for life or result in an extremely painful death. As engineers, we all know that to overcome predictable human error, we must implement design-based safety, rather than speculate that such behavior can be modified. For more than 50 years, power line proximity sensors and interlocks have been known to stop dangerous boom movement before the power line is struck, thereby eliminating the hazard. The use of insulation guards against the dangerous flow of electrical current should contact be made.

MacCollum's novel portrays how easily overhead contact accidents can happen and the devastating results that occur. This novel also shows how redundant elimination of the hazard and guarding against the flow of dangerous electrical current will reliably save lives. Strikingly vivid is how available engineering technology is aggressively rejected, while system safety comes to the rescue.

This book not only describes the boom hazard in great detail, but it also nicely weaves into the story much about liability cases and tort law. We tend to assume that liability cases are all excessive and simply about people trying to make money. This novel describes how the legal system is often abused in order to avoid implementing system safety.

In addition to being an interesting novel, I have to confess that I also learned quite a bit about electrical hazards, safety design features and how some parts of industry and society aggressively work at defeating safety.

The book is available for sale through the International System Safety Society, P.O. Box 70, Unionville, VA 22567-0070 USA Tel: 540-854-8630; email: systemsafety@system-safety.org; Website: www.system-safety.org.
Unintended Consequences

TWA Flight 800 Accident

by Terry Hardy

On July 17, 1996, Trans World Airlines (TWA) Flight 800, a Boeing 747, crashed into the Atlantic Ocean just after take-off from John F. Kennedy International Airport in New York. All 230 people onboard were killed. The National Transportation Safety Board (NTSB) determined that the probable cause of the accident was an explosion of the center wing tank. The tank likely exploded from a flammable fuel/air mixture ratio in the tank, probably ignited by a short circuit outside the tank, resulting in excessive voltage surging through the wiring of the fuel quantity indicator system inside the tank. The NTSB faulted the certification of the Boeing 747. This certification process allowed heat sources to be located beneath the tank, with no means to reduce the heat transferred into the tank or render the fuel tank vapor nonflammable. The NTSB also faulted the design and certification concept that assumed that tank explosions could be precluded solely by eliminating ignition sources.

The NTSB stated that experience has shown that all possible ignition sources cannot be predicted and reliably eliminated. In this case, the NTSB found that qualification testing had been performed on fuel quantity indicator system probes, and that testing showed that the probes were free of arcing up to 2000 volts. Therefore, the system was assumed to be "explosion proof." However, that testing had been performed in the 1960s, and the probes had been in use for more than 30 years, leading to deterioration and potential for arcing that invalidated this assumption. While conducting its investigation, Boeing provided the NTSB with a fault tree analysis of possible ignition mechanisms. The Boeing analysis concluded that the probability of wiring producing an ignition source in the tank as being 1x10^-6 events per hour. An independent review of that analysis by NASA showed that the Boeing analysis had relied on unrealistic inputs, and — had realistic numbers been used — a much higher probability of ignition would have been obtained for the fuel quantity indicator system wiring. In its evaluation, NASA stated that, "Many of the probabilities, failure rates, and/or exposure times were much lower than would reasonably be expected." As a result, NTSB stated that, "Failure modes and effects analyses and fault tree analyses should not be relied upon as the sole means of demonstrating that an airplane's fuel tank system is not likely to experience a catastrophic failure."

Lessons Learned: Risk assessment helps to understand significant problems, and to focus and prioritize resources to fix those problems. When risk assessment is not rigorous or is performed improperly, decision makers may not fully understand the potential for harm or the likelihood of a catastrophic event. Therefore, every attempt should be made to validate analysis inputs, and to allow for independent review of the results of any risk assessment. In addition, the assumptions we make in our analyses should be questioned, including both assumptions in our safety approach and assumptions in our quantitative analyses. Also, analyses alone should not be used for safety decisions. Analyses should be supported by testing, accepted industry standards, validated processes and sufficient design margin to ensure that the risk has been reduced.

Readers are encouraged to review the full accident and mishap investigation reports [Ref. 1] to understand the often complex conditions and chain of events that led to each accident discussed here. Additional lessons learned are available at www.systemsafety skeptic.com.

References


When risk assessment is not rigorous or is performed improperly, decision makers may not fully understand the potential for harm or the likelihood of a catastrophic event. Therefore, every attempt should be made to validate analysis inputs, and to allow for independent review of the results of any risk assessment.
"Safety" and "murder" are polar opposites. The compass of life provides a conscious choice of direction by protecting the public from harm or for the enhancement of wealth by endangering others. Safety points north toward social progress. Murder points south to social decline. As the sun rises in the east, it brings the light of day that will illuminate all of the physical laws of science that remain constant. As the sun sets in the west, it brings the darkness of night that hides all of the evils of human behavior that remain variable.

There is a difference when safety features are deleted for gain or profit, as now murder is in the process of being attempted. It is the dark side of the law when an uncontrolled hazard maims or kills, and is defended as a cost of enterprise. It is a sin to rationalize that when a product or facility has a history of life-threatening or life-taking experience, it is unnecessary to provide safety accessories or alternate safe design for any or all of the following excuses:

- To believe it is a matter
- To speculate that the safety feature is unreliable when experience shows otherwise
- To theorize that the cost of safety features exceeds the cost of possible harm
- To infer that the utility of the product or facility will be compromised
- To blame victims for being at fault because of their unsafe behavior
- To assume the provider of the product or facility had no duty to know of the hazard
- To abrogate responsibility to include safety features by pretending risk is acceptable

It is criminal to defend the absence of safety features that will eliminate, guard against, provide a safety factor or ensure for redundancy of features to prevent the hazard from causing harm. This is unconscionable and unreasonable logic that wrongfully endangers the public. The term "accident" is a grossly inappropriate description for a fatality that is the result of a failure to provide design-based safety; the word should be "murder."
Australian System Safety Conference Call for Papers and Presentations

The Australian System Safety Conference, to be held May 23-25, 2012 in Brisbane, QLD, Australia, is a joint conference between the Australian Safety Critical Systems Association (ASCSA) and the International Systems Safety Society (ISSS) Australian Chapter. This year the conference also incorporates the International System Safety Regional Conference.

The theme of this conference focuses on “System Safety... What's the Value-add?” System safety programs are always challenged by the availability of qualified resources, program budget, integration with and influence over the engineering development and planning. Yet liability protections — and regulation — require formal safety assessment of all complex systems with major hazard potential. Add-on safety programs are universally experienced to be least efficient and least effective. So, what are the successful strategies, methodologies, tools and experiences of implementing and adding value through a system safety program?

"Value," in this sense, can be viewed as increased safety or capability via "return on investment" of effort. Several seeds, or lines of enquiry, are indicative of likely interest for papers:

- Advances in methods/tools and automation
- How is safety valued?
- Software assurance "return on investment"
- Selling risk reduction and safety actions
- Communicating system safety risk
- Human factors analysis
- Budget for an ALARP safety program
- System safety program budgeting metrics
- Best skill-mix in the safety team
- Valuing system benefits against risk/cost

Call for Papers and Presentations:

The conference is accepting two types of papers:

1. Refereed Papers by the conference program committee
2. Industry Presentations (not subject to peer review)

For paper format details see www.crpit.com.

Key Dates:

- Abstracts — November 28, 2011
- Notification — December 19, 2011
- Submission — February 24, 2012
- Notification — March 29, 2012
- Final Paper — April 30, 2012

Disciplines of Interest:

- Safety Engineering
- Safety Management
- Software Engineering
- Software Assurance
- Software Safety
- Human Factors
- Systems Integration

Submit a Paper
All submissions can be made by using the online submission facility at www.assc2012.org. Alternatively, submissions can also be emailed to program@assc2012.org.

For more information: Visit www.assc2012.org

Registration for RAMS 2012 is now open.

RAMS 2012 will be held from January 23 to 26, 2012 in Reno, Nevada. If you are new to the reliability and maintainability field, RAMS 2012 will provide you with the core education you need to progress. If you are an experienced professional, RAMS 2012 will provide you with cutting-edge education to keep you on top of your field.

**RAMS Tutorial Certification**: a two-level program, based on attendance at five core tutorials and 10 elective tutorials. Enroll at the registration area for $75.

**ASQ Certifications**: by special arrangement with ASQ, RAMS offers on-site Reliability Engineer (CRE), Six Sigma Black Belt (SSBB), and Six Sigma Green Belt (SSGB) Examinations. Deadline for advance registration is December 22, 2011. Walk-in registration for the CRE and SSGB examinations is noon, Wednesday, January 25, 2012 on a space available basis.

**CEUs (Continuing Education Units) from IEEE**: CEUs can be earned by attendance at workshops and tutorials.

Tutorials, presentations, CEUs, certifications, and networking are combined into one symposium, delivering cutting-edge information to all technical industries.

For more information, go to [http://rams.org/](http://rams.org/)

---

Conference Speakers wanted for the Car Training Institute ISO 26262 Conference

Car Training Institute (CTI) is sponsoring a conference on the ISO 26262 safety standard on June 12 - 14, 2012 in Detroit, Michigan, and is accepting applications from proposed speakers until January 20, 2012.

The safety standard ISO 26262 (Road Vehicles - Functional Safety), parts 1-9, which applies to safety-related electrical and electronic systems in passenger cars, has been published. This standard applies to systems developed or changed after November 15, 2011. Those members involved in drawing up the standard already apply draft versions of ISO 26262 to some degree. The following countries participate in the ISO: Belgium, Canada, France, Germany, Italy, Japan, Sweden, the UK and the USA.

The standard is relevant worldwide.

ISO 26262 consists of ten sections covering the following themes:

1. Vocabulary
2. Management of functional safety
3. Concept phase
4. Product development: system level
5. Product development: hardware level
6. Product development: software level
7. Production, operation and decommissioning
8. Supporting processes
9. ASIL and safety-oriented analyses
10. Guideline (now approaching FDIS) ISO 26262 leaves plenty of room for interpretation and the conference will provide an opportunity for delegates to present and compare their own interpretations and concepts in the company of like-minded experts.

**Appropriate conference themes**

The aim of the CTI conference ISO 26262 is to present the fundamental aspects and initial implementations of the requirements for compliance to all ASILs. This will focus particularly on:

- Proposals for the introduction day
- Concept, basics and content of ISO 26262
- Methodical approach to ISO 26262
- Successful implementation of ISO 26262 in practice
| Identified challenges to the introduction and implementation of ISO 26262 |
| "Lessons learned" (dos and don'ts) in the application of ISO 26262 |
| Parallel implementation of ISO 26262 and other standards |
| Questions that ISO 26262 has still not addressed |

Field reports are also welcome from other sectors that already have specific standards on functional safety, such as medical technology and avionics.

For more information, go to [http://www.car-training-institute.com/iso26262-usa](http://www.car-training-institute.com/iso26262-usa)
Bay Area Chapter

The Bay Area Chapter conducted an Executive Council meeting on August 29, 2011 at Pedro's restaurant in Santa Clara, California.

Discussions on upcoming events, Brown Bag topics and potential field trips were held. Other topics of discussion included the Bay Area Chapter Website, which is tentatively scheduled to hit the World Wide Web prior to the end of this year. Some ideas for the Website include a Chapter calendar, job posting board, photo album and contact list — more info will be forthcoming. The Bay Area Chapter is also on LinkedIn — please add it to your professional network (Bay Area Chapter International System Safety Society).

On October 25, the Bay Area Chapter celebrated Oktoberfest and toured the Gordon Biersch facility in San Jose, California. The tour was tailored to focus on the safety of brewing and free samples were provided throughout the tour.

Plans are also in the works for a possible field trip to the SLAC National Accelerator Laboratory in November, as well as a Brown Bag presentation, scheduled to take place on December 1, 2011 at Lockheed Martin in Sunnyvale, California.

Canada Chapter

The Canada Chapter recently presented a noontime talk on “Root Cause Analysis and Human and Organizational Factors — Experience in the Nuclear Power Plant Industry” by Suzanne Dolecki, senior human factors specialist, Canadian Nuclear Safety Commission. This presentation addressed some common human-factors lessons common to other safety-critical industries. The Canada Chapter programs up to four noontime presentations during the year, culminating with a half day seminar in the spring as a yearly wrap-up. The spring seminar usually has four speakers addressing a common theme, followed by a group discussion.

At the Society year 2011 Awards Banquet in Las Vegas, Robert Fletcher (Past President Canada Chapter, Director of International Development) received the International Award for his contribution to the international advancement of the System Safety Society during the 2010-11 year. Gerry Einarsson (Chapter Treasurer, Director of Chapter Services, past Executive Secretary) received the President's Award for outstanding service to the society — his second President's Award since 2000.

Note: Photos of the Chapter award winners were printed in the September-October 2011 issue of the JSS.

Sierra High Desert Chapter (SHDC)

Chapter Treasurer Ken Chirkis gave an outstanding Risk Acceptance Process presentation to a joint SHDC and Washington DC Chapter meeting on July 13 at URS in Dahlgren, Virginia. After teaching his excellent Fault Tree Analysis course to many chapter members, Cill Ericson II, JSS Technical Editor and Director of Publicity and Media, joined Jim Zdzik, NAVAIR National Division Head for System Safety Engineering, as distinguished guests for the chapter meeting at the Ridgecrest Pizza Factory on July 19.
The Sierra High Desert Chapter held a joint chapter meeting with the Saguaro and Washington DC Chapters at the 29th International System Safety Conference held at the MGM Grand Hotel in Las Vegas, Nevada in August 2011. At the Society Year 2011 awards banquet, the Sierra High Desert Chapter won the Chapter of the Year Award. In addition, Mark Buffum received the Engineer of the Year Award, and Jerry Banister received the President's Award for outstanding service as director of chapter services. This was the Chapter's SHDC founder, president and membership chair's second President's Award. The Sierra High Desert Chapter of the International System Safety Society had a great showing at this year's Conference in Las Vegas, with 20 members in attendance.

John Leipper, Fellow, continued his long and invaluable support to the ISSCs, and Ken Chirkis volunteered for many tasks as ISSC 29 planning committee members. SHDC's Chapter president appointed John Alves as Chapter Webmaster.

Note: Photos of the Chapter award winners were printed in the September-October 2011 issue of the JSS.

Singapore Chapter

The Singapore Chapter participated actively in the 2011 ISSC. There were about 15 participants and two papers presented from Singapore. The papers were "Applying System Safety Methodology and Related Tools for a Public-Private Partnership Programme," presented by Mr. Heah Minyi and Mr. Chua Boon Heng (DSTA,) and "Adaption of Software Risk Assessment," by Ms. Ng Suk Fen and Ms. Mok Boon Eang (ST Electronics, Info-Software).

The Singapore Chapter saw the hand-over of the Chapter presidency from Ms. Siow Seet Ting (ST Kinetics) to Mr. Yap Kwee Seng (Land Transport Authority). The Singapore Chapter held a meeting on September 16, 2011 at the Land Transport Authority (LTA) Hampshire Office. The Chapter Executive Committee (EC) welcomed two new officers, Mr. Rodney Tan Kheng Eng and Mr. Teo Yeow Keong from Defence Science & Technology Agency (DSTA).

The Singapore Chapter would like to take this opportunity to thank Mr. Michael Tan (DSTA) for his valuable contribution to the Chapter EC since its inauguration in 2002. Mr. Michael Tan decided to step down from the Chapter EC in August 2011. The Chapter EC meeting discussed the work plan for this Society work-year and aligned the proposed activities with the ISSS's strategic objectives. The Chapter EC also introduced two new office positions — Publicity & Media to be headed by Mr. Oei Su Cheok, the Chapter's current Webmaster, and Professional Education & Development to be headed by Ms. Onn Eng Ling. The Chapter has created a new Past President Council, which the current president can tap for resources. In addition, the council can also advise the Executive Committee and safeguard the Chapter's reserves.

Washington DC (WDC) Chapter

After a great multi-chapter meeting in Las Vegas (co-hosted by the Sierra High Desert, New Mexico and Saguaro Chapters), members of the WDC area returned to their respective workplaces.
revitalized from the 2011 ISSC and all the knowledge gained there. The WDC Chapter would like to express its congratulations to the Sierra High Desert Chapter on its successful win of the Chapter of the Year Award!

On August 24, James Spencer gave an engaging presentation on “Practical Applications of Weibull Analysis including New Methods and Lessons Learned.” This meeting was held in Leonardtown, Maryland.

Next, the WDC Chapter hosted a monthly meeting at the Booz Allen Hamilton offices, located in Crystal City, Virginia, on September 21. Sherman Forbes, Jeff Walker and Bob Smith gave a fantastic brief on the status of MIL-STD 882E and its pending release. The New Mexico Chapter joined the meeting via teleconference.

On September 30, the WDC awarded two engineering students the WDC Engineering Scholarship. One recipient is a 24-year-old man (3.9 GPA) who is about to receive his two-year degree in general engineering, and the other is a 31-year-old veteran (4.0 GPA) who is a year away from obtaining his two-year degree as well. Both recipients are transferring to a four-year institution to complete their engineering educations. A formal awards ceremony is scheduled to take place in October, 2011.

On October 5, the WDC hosted its annual Oktoberfest at the Oak Crest Winery. The guest of honor was Michael Demmick, past president of the WDC Chapter and co-founder of the WDC Engineering Scholarship Program. Mike left in mid-October 2011 for a one-year temporary duty assignment abroad. Additionally, Mike’s son, Robert Demmick, is also back from the Navy on leave and is en-route to his first tour in the Navy to Guam as an explosive ordnance disposal technician. The WDC Chapter wishes them both a safe journey and a speedy return.

Upcoming events for the WDC Chapter are the monthly meeting in November 2011 (to be held in Dahlgren, Virginia) and the annual Christmas Party to be held on December 2 in Fredericksburg, Virginia.

As always, the WDC Chapter welcomes all ISSS members to its meetings and functions. If ISSS members are interested in attending WDC events and would like to be on the distribution list, please forward your email address to Amber Schauf, Chapter president.

Virtual Chapter

During the past few months the Virtual Chapter has held its annual face-to-face meeting at the System Safety Society Conference. At that meeting, the Chapter took nominations for the various Chapter offices and held an election on September 12. New officers include:

Jimmy Turner — President
Steve Mattern — Vice President
Lee Flint — Treasurer
Matt Johnson — Secretary

Our chapter has a group located on LinkedIn (http://www.linkedin.com/). Search for Virtual Chapter of the System Safety Society.

The Chapter typically meets on the second Monday of the month at 6 p.m. Central Time. In the past, discussions have included topics such as hazard tracking databases, integrating system safety into defense acquisition, hazard lessons learned and more. In the future, the Chapter will have a presentation on virtual meeting and collaboration opportunities and data exchange standards. Join the Virtual Chapter as a primary member or, if you are already affiliated with another chapter, you can attend as an associate. It costs nothing to participate, and you gain the opportunity to network and learn what others in the profession are doing.

For more information about the chapter, visit its LinkedIn page or contact Jimmy Turner at ts41930@yahoo.com.
Vol. 47, No. 6 • November-December 2011

Mark Your Calendar

20th Safety-Critical Systems Symposium (SSS '12)
February 7-9, 2012
Bristol Marriott Royal Hotel
Bristol, U.K.
http://www.safety-club.org.uk

2012 Symposium on Human Factors and Ergonomics in Health Care: Bridging the Gap
March 12-14, 2012
Baltimore Marriott Waterfront Hotel
Baltimore, Maryland
http://www.hfes.org/

57th Annual Corporate Aviation Safety Seminar (CASS) 2012
April 17-19, 2012
Grand Hyatt San Antonio,
San Antonio, Texas
http://flightsafety.org/aviation-safety-seminars

Australian System Safety Conference
May 23-25, 2012
Mercure Hotel
Brisbane, QLD, Australia
http://www.assc2012.org

30th International System Safety Conference
August 6-10, 2012
Loews Atlanta Hotel
Atlanta, Georgia
http://issc2012.system-safety.org/
Journal of System Safety, eEdition


Article Submission | Advertising | Subscriptions & Membership | Copyright

Journal of System Safety is published six times a year (four print and two electronic editions) by the 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 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.

All articles and papers published in Journal of System Safety remain the property of the original authors, and are protected under U.S. and international law. For copying and republishing permission, please see http://copyright.gov/.

ARTICLE SUBMISSION

Journal of System Safety welcomes article submissions from its readers. Technical manuscripts, "Opinion" and other submissions should be sent to:
Clifton Ericson, JSS Technical Editor
6406 Medallion Drive
Fredericksburg, VA 22407
USA
540-786-3777
Email: journal@system-safety.org

Authors should include the following:
(1) one typewritten copy of the manuscript, double spaced; (2) electronic file in Microsoft Word, Adobe InDesign or ASCII (plain text) 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 journal@system-safety.org.

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 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.

Ad prices in the printed JSS are as follows:
Full-page ad — $800
Half-page ad — $400
Quarter-page ad — $225

For electronic ads:
Small ad = 150 x 75 pixels = $20
Medium ad = 150 x 350 pixels = $110
Large ad = 150 x 600 pixels = $210

For information on advertising rates and submission guidelines, please contact:
Clifton Ericson, JSS Technical Editor
6406 Medallion Drive
Fredericksburg, VA 22407
USA.
540-786-3777
Email: journal@system-safety.org

SUBSCRIPTION AND MEMBERSHIP INFORMATION

For information on subscription rates and membership, contact:
System Safety Society
P.O. Box 70
Unionville, VA 22567-0070 USA
Tel: 540-854-8630
Fax: 540-854-4561
Email: systemsafety@system-safety.org
Web: http://www.system-safety.org

Copyright © 2011 by the System Safety Society. All rights reserved. The double-sigma logo is a registered service mark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.

(iSSN-0743-8826)
DIRECTORS:
Chuck Muniak
Education and Professional Development
Syracuse Safety Research
cmuniak@stevens.edu
315-663-7606

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

Dave Shampine
Conferences
URS
dave.shampine@urs.com
540-663-9588

Bob Fletcher
International Development
rwfletcher@sym pathetic.ca
613-837-4128

Clifton A. Ericson Publicity and Media
EG&G Technical Services
cliftonericson@cs.com
540-663-9591

Saralyn Dwyer Member Services
APT Research, Inc.
sdwyer@apt-research.com
256-327-3377

Mark Geiger
Govt. and Inter-Society Services
OPNAV Safety Liaison Office
mark.geiger1@navy.mil
703-695-4703

Michael Allocco
Mentoring and R&D
michael.allocco@faa.gov
202-385-4714

CHAPTER POINTS OF CONTACT:

Go to complete listing on the Society web site.

Copyright © 2011 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.