President's Message

Society Elections

by Gary Braman

As I have noted many times, being a member of the International System Safety Society (ISSS) is both a privilege and an honor. But that membership also brings with it many responsibilities, one of which is involvement in the organization. A great way to get involved with the Society is to serve as an officer or director at the Society level. Serving as a Society officer or director is an educational and rewarding experience. Those who serve in any of these positions play a key role in developing policies and procedures that advance our profession and grow our Society.

Each position has a host of responsibilities: representing the organization at professional development functions, representing Society members, communicating with members, leading the Society forward, mentoring new members, coordinating and overseeing meetings and voting on issues affecting the Society and its operations. It is important to keep in mind that performing these duties requires time and commitment. Your actions and leadership influence almost 1,000 system safety professionals and the operation of our organization.

The opportunity to really get involved is now at hand. All Society officers and several of our Society directors are up for election next year, but the process begins now. The following positions are up for election; the duties associated with each can be found in Section 4 of the Society's Operations Manual (OM) found on the Society's Website:

- President
- Executive Vice President
- Executive Secretary
- Treasurer
- Director of Inter-Society Services
- Director of Member Services
- Director of Mentorship, Research and Development
- Director of Publicity and Media

I urge you to consider serving in one of these positions. Run for election if you can commit the time and effort required. If you cannot serve now, talk to others who can and are willing to serve. Please note that to seek and hold office, candidates must be professional members in good standing. A list of candidates will be submitted to the Executive Committee (EC) for approval and then to the executive secretary for preparation of the ballots. Each candidate is required to submit biographical information and a photograph for publication in the Journal of System Safety and on the ballot form.

Please submit your nomination for office, along with the required biographical information and photograph, to me, as I will serve as the Nominating Committee chairman. Nominations must be received by December 31, 2012. Please consider serving your profession and Society.

Thanks for your support, and I hope to see you at next year's International System Safety Conference in Boston!

— Gary Braman
President
International System Safety Society
Elections and Transitions

by Clif Ericson

It's that time of year again — time for elections. However, I am not referring to the recent national, state and local elections. I am referring to our International System Safety Society elections. The first step in our Society election process is to nominate a slate of officers for the next term. Read the President's Message for additional information on the nomination process.

It is with sadness that I announce the retirement of Ludwig Benner and Ira Rimson as regular contributing authors in JSS. Ira and Ludi have been writing the "Outside the Lines" column for quite a few years and are long-time members of the ISSS. They have made considerable contributions to system safety and to JSS. I would like to personally thank them for everything they have done.

The first technical paper in this issue, "ESOH Considerations in the Selection of Alternative Energy Sources" by Adam Gambriell, presents the various safety implications of alternative energy sources, such as wind, solar and biofuels. While these alternative energy sources may seem benign in comparison to nuclear power, their effects on safety and the environment should be thoroughly explored for hazards and hazard risk.

The second technical paper in this issue, "Common Statements...Trouncing Safety" by Mike Allocco, is an interesting look at statements commonly heard within industry that show a lack of understanding of system safety. He specifically identifies 60 misconceptions, and presents a valid view on these topics. It's worth reading this paper to determine if one of these items is on your hot list, and if you agree with Mike.

In his "System Safety in Healthcare" column, Dev Raheja discusses the hazards of patient-controlled pain medication pumps. There are serious safety issues involved with these devices, and with patients controlling their amount of medication, which Dev discusses in this article.

In his "Unintended Consequences" column, Terry Hardy discusses a communication breakdown that occurred, causing the crash of Avianca Airlines flight 52 while it attempted to land at John F. Kennedy International Airport. This mishap occurred on January 25, 1990. The NTSB determined that the probable cause of the accident was the failure of the flight crew to manage the airplane's fuel load; however, communications and standard terminology were also major factors.

In his "Design-Based Safety" column, Dave MacCollum discusses how leadership in a design-based safety process brings order out of chaos. He also provides seven leadership skills that can be employed to enhance the safety process.

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

Until next time,
Clif
From a policy perspective, it makes sense to examine the most popular current options. Wind, solar, geothermal, wave energy, tidal currents, nuclear energy, agricultural residues, bio fuels and algae are all popular sources of alternative energy.

**Alternative Energy Sources**

From a policy perspective, it makes sense to examine the most popular current options. Wind, solar, geothermal, wave energy, tidal currents, nuclear energy, agricultural residues, bio fuels and algae are all popular sources of alternative energy. Now take into account the hazards presented by just one of these alternative energy sources — nuclear energy. Nuclear energy grew popular when it became a vastly viable source of electricity; however, due to the long-term risks of radioactive waste on the environment — which still have no long-term solutions in place — and the ill effects on human exposure, this source of energy appears to have been scaled back long before its full potential could be realized.

Assuming that nuclear power is the exception to the rule with regard to potential ill effects on humans and the environment,
energy, agricultural residues, bio fuels and algae are all popular sources of alternative energy.

When considering primary fuel sources used by DoD and the federal government, for example, it is important to understand some of the basic properties of alternative fuels. The most common alternative fuel sources are bio fuels, of which there are two widely used types: ethanol and biodiesel. To better understand two simple properties of fossil fuels and these alternative bio-based fuel sources, see Table 1.

Table 1 — Comparison of Conventional and Bio-Based Fuels.

<table>
<thead>
<tr>
<th></th>
<th>Gasoline</th>
<th>Ethanol (E85)</th>
<th>No. 2 Diesel</th>
<th>Biodiesel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight (lbs)</td>
<td>6.3 lbs.</td>
<td>~6.6 lbs.</td>
<td>7.15 lbs.</td>
<td>7.34 lbs.</td>
</tr>
<tr>
<td>BTU</td>
<td>109,000 — 129,000</td>
<td>80,000</td>
<td>128,000 — 130,000</td>
<td>117,000 — 120,000</td>
</tr>
</tbody>
</table>

Note: This table identifies weights and the energy contained in 1 U.S. gallon of each fuel to give the reader a comparison of each of the two primary fuels (gasoline and diesel) and their current alternatives.
Clearly, the argument in this case shows that if biofuels are to be used as a 1-for-1 substitute for fossil fuels, there is not enough cultivated land area to support biofuel production and sustain the world’s future food production needs. This extends beyond the realized environmental impacts of such heavy cultivation of soils, and resulting erosion, greenhouse gas emissions related to cultivation, transport and manufacture of biofuels, along with other negative effects. These effects clearly show that there would be huge impacts to the human environment. People, especially the poor, may lose out on nutrition in the global race for biofuel production. This is clearly not a winning scenario within the big picture of human sustainability.

Any benefit from the use of biofuels would have to be realized at a limited capacity, such as today’s common blended fuels like
there is not enough cultivated land area to support biofuel production and sustain the world's future food production needs.

Puzzle E10 and B20, where 10 percent of ethanol is blended with regular gasoline, and 20 percent of biodiesel is blended with diesel No. 2, respectively. Today's use only offsets our dependence on fossil fuels by a marginal amount. There is an obvious trade space in the pursuit of clean alternative energy, and higher blends of biofuels on a global scale simply cannot be sustained while feeding the world's growing populations.

With respect to energy conversions, it is important to note that some studies provide no net gain when it comes to the energy produced by biofuels, and the energy used to produce biofuels. This is called net energy return, or "the ratio of energy in the final product to the energy required to produce the commodity" [Ref. 3]. When considering the net energy to produce ethanol, for example, and taking into account that "the direct energy costs of corn cultivation but also for the energy costs of field machinery and irrigation…the ratio of energy contained in ethanol to energy used in corn production and fermentation is just 0.77, which is a significant energy loss" [Ref. 3]. Clearly this is not a winning scenario when considering cost or environmental effects.

Ethanol production takes a step backward and uses more energy to produce than what is actually created — not to mention there are ill-effects, such as soil erosion, mineral depletion, etc. when cultivating crops for this purpose. It is noteworthy that since this paper was written, the only gas station dispensing E85 for public use within a 50-mile radius of the author's house was shut down, likely for the reasons highlighted above — that E85 costs more to produce and is not cost effective for the common consumer.

Some other considerations regarding biofuels include:

- **Weight**: Ethanol weighs more than gasoline and provides less BTUs per gallon. Increased weight and fuel volumes should stand out as a key factor when considering lightening military supply lines, transportability, fuel handling, etc.
- **Flammability**: Flammability concerns vary, according to the following table, when considered alongside conventional fuels. Flammability is most commonly measured in terms of the highest (Upper Explosive Limit) and lowest (Lower Explosive Limit) concentrations of gas mixed in air that can produce a flash of fire when exposed to an ignition source. Auto-ignition temperature is also considered, as this is the temperature at which the fuel will ignite on its own. As indicated in Table 2, E85 has a higher flammability range than conventional gasoline; however, its auto-ignition temperature typically ranges higher.

Table 2 — Flammability Comparison.

<table>
<thead>
<tr>
<th>Flammability</th>
<th>Gasoline</th>
<th>Ethanol (E85)</th>
<th>No. 2 Diesel</th>
<th>Biodiesel (No. 2 Biodiesel)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper Explosive Limit (UEL)</td>
<td>7.7%</td>
<td>19%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Lower Explosive Limit (LEL)</td>
<td>1.4%</td>
<td>1.4%</td>
<td>3%</td>
<td>.3%</td>
</tr>
<tr>
<td>Auto-ignition Temp.</td>
<td>536°F</td>
<td>833°F</td>
<td>500°F</td>
<td>1131°F</td>
</tr>
</tbody>
</table>

Note: Items in this table were taken from various Material Safety Data Sheets and some numbers may vary, depending on distributor.

- **Human health effects due to contact/exposure**: While ethanol and biodiesel are less toxic than traditional fossil fuels, they still present significant health effects through various methods of exposure.
- **Environmental contamination due to spill/release into environment**: Biofuels clearly provide more positive effects than conventional fossil fuels, but may still locally degrade the environment surrounding a spill or contamination.

The trade space when considering biofuels must take into account the effects of over-farming, the offset to vegetable consumption, energy use and energy conversions to create the fuels. Clearly, advertising and political lobbying have made biofuels appear to be a winning choice for the environment, but as pointed out earlier, there is a great amount of energy loss and potential negative environmental effects that go into the production of biofuels. Policy makers and program managers need to know the facts about this alternative energy source before committing to programs that appear to benefit human health and the environment, when, in fact, they do not.
While most wind turbines are located in sparsely populated areas and the probability of a blade injuring someone or causing property damage is likely to be minimal, this scenario certainly poses a valid hazard. Other concerns relate to navigation of aircraft where tall windmills pose a collision hazard. If adequately controlled through the use of beacons and markings on maps and other navigation aids, however, the probability of an aircraft collision is likely reduced.

According to a presentation by Hart Aviation [Ref. 5], the international Civil Aviation Organization (ICAO) identified the following measures that should be taken with regard to wind farms:

A wind turbine shall be marked and/or lighted if it is determined to be an obstacle. The rotor blades, nacelle and upper 2/3 of the supporting mast of wind turbines should be painted white, unless otherwise indicated by an aeronautical study. When lighting is deemed necessary, medium intensity lights should be used. In the case of a wind farm, lights should be installed as follows: the perimeter of the wind farm should be identified; the spacing of lights should be in accordance with the recommendations of any other widely spaced obstacles, unless an assessment determines otherwise; flashing lights, when used, should flash simultaneously; and the tallest wind turbines should be identified, regardless. Obstacle lights should be installed on the nacelle in such a manner as to provide an unobstructed view for aircraft.
approaching from any direction [Ref. 5].

The wind turbines themselves create significant amounts of electricity as "wind turbines with ratings of 1-2 MW are now concentrated in large groupings" [Ref. 3]. While standards for the control and isolation of electricity are well established, hazardous levels of electricity exist in these systems and must be controlled appropriately. Aside from direct hazards to humans and property, windmills have also been found to come with some negative environmental effects. Such effects include inevitable bird kills, blade noise pollution and visual pollution [Ref. 3].

Additionally, the following hazard sources should be explored further to determine the extent that each plays in contributing to a hazard:

- Electricity
- Momentum (energy)
- Environmental effects due to installation of and digging for footings, migratory bird impacts, aircraft, eyesore (public disdain)
- Ice and other weather phenomena
- Falls (worker-related)
- Low-frequency noise vibrations
ESOH Considerations in the Selection of Alternative Energy Sources

by Adam Gambriell

Solar Power

Solar energy is another alternative energy source presenting some potential environmental and human health hazards. Solar energy drives the food chain here on Earth. Without it, plants would not be able to undergo photosynthesis, animals would starve, and the world would be a rather gloomy place. It wasn’t until recently that scientists were able to harness solar energy or photons, and convert this energy to electricity. The energy is often stored as DC power in batteries and converted to AC when needed for use.

This brings us to our first hazard source with solar power: electricity. As we all know, contact with electricity can cause electric shock and burns to humans. Given that solar power is typically stored in DC and at low voltage, the effects of electric shock at the source of collection may be limited, but the risk is present nonetheless. Some lesser-known effects of solar power may include environmental degradation to soil and habitats, as vast solar arrays require much real estate. To minimize the effects on the environment, solar panels can be installed on rooftops, where the environmental impacts are mostly absorbed by the existing structure. Because most solar panels store electricity in batteries, a vast amount of batteries (typically, lead acid) are required to hold the energy until needed for use. Lead-acid batteries come with their own set of safety and environmental concerns. Aside from the potential exposure to lead, sulfuric acid and hydrogen gas, batteries are somewhat of a disposal concern, especially on a grand scale. They also require proper storage, handling and disposal methods. The more batteries are produced to store solar electricity, the more cumulative environmental effects may be felt due to their use and disposal.

Solar panels are also somewhat susceptible to high winds, sand and dust, as well as large hail. Because most panels are encased in glass, they are prone to breakage. Aligning panels at the appropriate solar inclination angle helps to lessen the effect of a hailstone, as opposed to laying panels horizontally, but this mitigation proves to have a minimal effect, especially at the lower latitudes and equator as the panels are aligned more closely to the horizontal plane.

Solar panels may also degrade a building’s structural integrity because of the added weight. Some regions that stand to benefit from solar electricity are also prone to high winds and heavy snowfalls. The weight of snow resting on a heavy solar array atop a structure not suited for the additional weight may lead to structural damage and potential collapse, injuring the occupants and causing property damage. It is vital that a thorough analysis of the structure be conducted prior to the installation of any solar array on top of a building.

Aside from these safety, health and environmental concerns, solar power is a generally safe and effective way to gather electricity. With the initial purchase and routine maintenance costs aside, the trade-offs for “free” electricity seem to be worth the potential ESOH effects, especially if solar
arrays are thoroughly planned and take into account considerations for human health, safety and the environment.
ESOH Considerations in the Selection of Alternative Energy Sources

by Adam Gambriell

Pages 1 | 2 | 3 | 4 | 5

ESOH Implications

ESOH implications for DoD and the federal government with regard to alternative energy sources are not as clear as one may initially assume. Biofuels often require more energy to develop than the energy contained within the product. Biofuels production essentially removes vital crops from the food chain. These crops could be used to feed hungry populations, but are instead trending toward fuel production. In some instances, such as with E85, the fuel weighs more per gallon than its conventional counterpart, and provides less energy. This is clearly not a winning scenario when battlefield tactics require an advantage focused on lighter weight and enhanced mobility.

Aside from the relative permanent infrastructure required by wind power, today’s windmills offer little to DoD and the federal government with regard to strategic military operations. Wind power may be of use at fixed bases where the average wind speed provides an incentive for its use, but this alternative energy option is not without its own safety and ESHO considerations as well. While not outside the ordinary, visual and noise pollution, the possibility of falls, electrocution, mid-air collisions and catastrophic failure lead the reader to understand that wind power comes with its own set of limiting factors that must be weighed by decision-makers before fully embracing this approach to significantly off-setting our dependence on foreign supplies and improving our overall energy efficiency.

Solar power could be a more viable option if real estate was available to support a measurable solar infrastructure. Solar power has been proven to work in small-scale tactical operations where systems such as the Marine Corps’ Solar Portable Alternative Communications Energy System (SPACES) are used to power small-scale electronics, batteries and firing systems [Ref. 6]. Notwithstanding the limited ESHO considerations outlined here, solar power could be the best option for the DoD and federal government to promote alternative energy sources. Thoroughly planned and combined with base infrastructure, and installed atop existing structures, solar power may be the most promising alternative energy source with the most controllable ESHO considerations.

Conclusion

The federal government and DoD have taken on a tough and necessary challenge to become less dependent on traditional energy sources, such as fossil fuels. To become more effective, new technologies must be developed and tested alongside existing capabilities so that the most balanced approach can be achieved. However, any promising new technology will not be without its own set of trade-offs. We owe it to ourselves and the environment to promote more effective and less harmful energy sources and supplies. As we progress toward higher efficiency and less foreign dependence, we cannot forget Newton’s Third Law: With any action, there is always an equal and opposite reaction. This

To become more effective, new technologies must be developed and tested alongside existing capabilities so that the most balanced approach can be achieved. However, any promising new technology will not be without its own set of trade-offs. We owe it to ourselves and the environment to promote more effective and less harmful energy sources and supplies.
applies in the case of energy. With nuclear energy as a prime example, along with its multitude of benefits, we still have not conquered the ill effects of its use and the resulting waste. More promising technologies must take into account this relationship, even more so when the promise appears to the public and policy makers as a "silver bullet" solution.

About the Author

Adam M. Gambriell has nearly five years of experience in systems safety, environment safety and occupational health. He spent two years supporting the Joint MRAP Vehicle Program as a systems safety engineer and another two years supporting USMC communications systems in systems safety as the safety team lead. Prior to igniting his professional career, he earned a bachelor of science degree in aerospace studies and a graduate studies certificate in aeronautical science with a focus on aviation safety systems, both from Embry-Riddle Aeronautical University. Adam’s interests include technology and advanced power systems, systems engineering, flying, aviation safety, outdoor recreation and working as a youth leader. He is a member of the International System Safety Society.

References

Common Statements...Trouncing Safety

by Mike Allocco, Fellow

Safety Avoidance Logic

Through a lack of understanding of system safety axioms, poor decisions that hinder system safety and increase risk are often made. Common statements support safety avoidance logic, and these statements are often made in the context of safety, which may be inappropriate. These statements may reflect limited background, knowledge, experience, attitude, perception, misguidance or maybe simply arrogance.

It seems that many people do not understand the axioms of system safety, yet the base of all our efforts in system safety depend on knowing these axioms. There is frustration when the system safety practice is not properly applied, as well as more risk to the system if there is deviation from practice. Note that actual circumstances will vary and good judgment has to be used when applying the axioms.

Legal Ramifications

There are legal ramifications concerning the use of safety-related "terms of art." These terms may or may not be appropriate and will vary depending on the particular legal entity (state, country or jurisdiction). This discussion excludes particular legal ramifications.

It is the reader's responsibility to know and understand all legal ramifications associated with the practice of system safety, safety engineering and safety management.

Common Statements Applied

What follows is a discussion of some common statements that may reflect a limited background, knowledge, experience, attitude, perception, misguidance or arrogance, along with counter statements that support a more logical safety-related argument. It is recommended that these limiting statements be abated or challenged when necessary.

• “Quantitative analysis is more vigorous and appropriate than qualitative analysis.”

Quantitative analysis is rigorous and laborious, and it takes time. However, quantification is needed to develop design requirements, evaluate simulations to determine distributions composed of random variables and test system response. Probabilities may be helpful in determining availability or reliability. Probabilities actually indicate that an event is possible. Considering randomness and regardless of the high confidence level, the event can still occur tomorrow.

If all safety resources are allocated toward laborious quantification, consider all the system risks that may not have been identified because an inclusive hazard analysis was not conducted. For complex systems, there may be hundreds of risks and thousands of hazards throughout the lifecycle that may not be addressed. It is important that system safety resources are appropriately applied and that, depending on the circumstances, both quantitative and qualitative analyses be conducted. Qualitative analysis may be more appropriate, considering it is important to identify, eliminate and control risks.

• “Accidents, hazards, risks, and outcomes, it's all the same thing...there is only one
It seems that many people do not understand the axioms of system safety, yet the base of all our efforts in system safety depend on knowing these axioms. There is frustration when the system safety practice is not properly applied, as well as more risk to the system if there is deviation from practice.

- "Operators don't make errors and when the system fails it will be detected."

Novice analysts may assume best-case situations within hazard analyses and, as a result, only consider three or four hazards of low risk. If the analysis was conducted and all the risks are low, the effort is completed. Depending on contingency response, worst-, mid- and best-case situations must be considered. Different hazards and mitigations may be determined or identified when all possible sequences are addressed. People are imperfect; there will always be errors and, since people create systems, there will be latent errors and real-time hazards to address.

- "These are two independent events and the probability of these events occurring is EE-9. We can exclude these events from the analysis."

A probability alone is not a hazard control. Consider all risks and their associated hazards, regardless of what the estimated probability is. All hazards must be fixed. Rare events can result in catastrophic outcomes. Seemingly incredible independent events do line up and form adverse sequences. Consider that system safety analyses may not have been conducted adequately, since common-cause events were not investigated, or hazards were excluded because of an estimated probability.

- "The Military Standard 882 Z method is good or bad."

There is no one particular safety standard that contains all the appropriate axioms of system safety, safety engineering or safety management. It is important to fully understand all the principles and practices (axioms) within the safety disciplines. There are common threads that are axioms throughout safety practices.

Once the level of protection has been applied, the safety bar has been raised. There is now an obligation to meet that level of protection, regardless of any new or revised safety standard or specific revised term within the standard. For example, consider the typical safety term of "hazard;" it has been re-defined multiple times, perhaps as the result of a new expert safety engineer. In some entities, a hazard may be considered a threat. A "threat" is a security term. A "hazard" remains the potential for harm, including unsafe acts and/or conditions within an adverse sequence.

- "It is more important to have specific industry experience rather than system safety experience."

Yes, specific experience needs to be accessed while conducting system safety analyses; however, the safety professional is just as important. It is vital that system safety axioms be appropriately applied. A cursory or inappropriate safety analysis may introduce additional risks, there may be many risks that have not been addressed, and/or mitigation may be inadequate. False confidence can be established regardless of the result, leading to an inadequate, incomplete or inappropriate analysis.

- "We need a team of people to do hazard analysis."

Depending on the analysis or system, a team of people may hinder or adversely affect the analysis. In some situations, it may be more appropriate for a qualified safety professional to initially conduct the analysis and then invite particular people into the process as the analysis progresses. If the analysis team is not properly trained and the meetings not properly facilitated,
wheel spinning will occur and resources may be wasted.

- "You need a specific credential to do system safety."

Almost anyone with the capability to learn the axioms can practice system safety. On the other hand, there is no such thing as too much knowledge of science, physics, human factors, health, medicine, engineering, technology, mathematics and statistics. An experienced safety professional is constantly learning and has the capability to extract the information needed from other professionals.

- "We must apply this particular safety model while conducting analysis."

In the literature, there are many safety models that can be useful. Depending on the analysis and system, some specific safety models may be more appropriate than others. It is often helpful to use many different models to evaluate the system from different points of view. Additional risks, hazards and/or mitigations may be identified. Consider that some models may be abstractions and may or may not be accurate depictions. Models may represent theories or hypotheses that may or may not be true.

- "(Abstracted) models of the system are accurate."

Any depiction of the system can be inaccurate. Accuracy can be judged by physical reality, applied physics, measurements, true observations, experimentation and testing.

- "It's redundant so it's safe."

Unfortunately, people still make this statement. Considering complex automated systems, it is a challenge to prove redundancy of software, firmware, hardware and human elements. There can be a common connection point or a common event that can defeat redundancy.

As you would expect, "safety" is a relative term. Nothing is totally safe. Safety implies freedom from all forms of harm, which is not possible. However, safety can imply that the identified risks are acceptable, given the mitigations.

- "We do safety better than that group. We know the best way of doing safety."

"Not invented here" syndrome often occurs. People become experts in their fields and automatically consider themselves experts in system safety. They may have even developed some form of system safety application. Again, a false sense of security is established. It is advisable to keep an open mind and gain knowledge of system safety axioms throughout various applications and industries.
Common Statements...Trouncing Safety

by Mike Allocco, Fellow

Never assume that a hazard has been mitigated, unless there is formal and current validation and verification. When evaluating a change to an existing system, there may be mitigation in place. The change may introduce new risks that may or may not be adequately mitigated by existing controls. The interfaces and interactions between the change and the existing system must be evaluated, as well as the existing mitigations. An integrated hazard analysis addresses the change as it is integrated into the existing system. The analyses should identify and mitigate all new and existing risks throughout the lifecycle. It is also important to re-validate and re-verify any existing controls that will mitigate new and existing risks associated with the interfaces and interactions.

There have been examples of poorly done or non-existent integrated hazard analysis. Analysts have attempted to evaluate change only at some arbitrary boundary, and have failed to consider all interfaces and interactions. Consequently, changes were incorporated and there were risks and hazards not eliminated or controlled.

A similar problem occurs when an existing redundancy, back-up or contingency is assumed. Consider that the redundancy, back-up or contingency has failed and the situation is not known, or that the redundancy, back-up or contingency will fail when these controls are needed. Formal and real-time validation and verification should be required for redundant, back-up or contingency controls. Consider that these controls can include automation, semi-automation or manual action and involve elements of firmware, software, hardware, human and/or the environment.

Incredible or rare accidents do occur when ostensibly incredible hazards line up within the adverse sequence. Once hazards are identified, they must be mitigated. The credibility of the potential accident should be assessed with two tests:

- Can the accident occur physically, conforming to physics or physics of failure, and considering the natural order of the system?
- Is the adverse sequence logical?

When system anomalies occur, it may not be possible to determine exactly what failed. Consider a system that is re-booted and the anomaly goes away. This is definitely a problem from a system safety view. Sometimes, duplicated line replaceable unites (LRUs) have been replaced and the anomaly has cleared. Further, consider that such an anomaly could have been caused by a transient environmental problem, such as electromagnetic interference, static discharge, logic error, single bit upset or flip, temperature change, humidity, water intrusion, debris, dust, degradation within a micro-substrate semi-conductor, physical shock and/or vibration.
System accidents are rare events; they do not occur frequently. Rare events are hard to predict statistically. A particular statistical probability is not a single-point estimate (a single number), but a distribution of probabilities. Within the risk engineering disciplines, there are continuous debates concerning statistical concepts associated with quantitative risk, particularly as to the validity of placing a number (probability) on a complex rare accident (system risk). In some cases, when dealing with large numbers, it may be possible to estimate prior distributions of risk generally. The more frequently an accident occurs, the less rare it is. It may become possible to estimate future probability distributions when previous probability distributions are known. The process of combining prior and future distributions and estimating future risk is known as Bayesian analysis.

No attempt should be made to place a single number on an actual potential system accident. In conducting risk assessment, the analyst estimates the likelihood of a potential accident, given the mitigations. This is more of a ballpark estimate with a bandwidth (distribution) of possible probabilities. Such an estimate is to be used to compare or rank similar risks.

Another important aspect of probability, other than randomness, is the consideration of independence. There are additional complications, such as determining independence within a complex system, as well as some discussion of the relationship between randomness and independence when addressing human errors, coding errors, design errors, decision errors and consequent malfunction of complex systems. In many situations, it is hard to prove that particular random events within an adverse process were independent. Generally, hazards can be interconnected within a complex system. When addressing complex system accidents, working the mathematics can become a big problem.

Many additional complexities associated with quantitative risk analysis, human factors and decision-making must also be addressed.

Environmental monitoring may be a control to limit human exposure to toxic gases, fumes or vapors. Monitoring can be automated, semi-automated or manual. Considering system safety precedence, the system should be designed to eliminate inadvertent human exposure to toxic gases, fumes and vapors. This may be accomplished through isolation, encapsulation, containment, venting or the use of scrubbers or flares. If possible, all steps to assure leakage or seepage containment should be taken. In some situations, there is over-reliance on manual monitoring as a control to limit human exposure, other engineering mitigations not initially considered within the design.

Automation can be used as a control to remove the human from a hazardous, monotonous or repetitive operation. Depending on task analysis or link analysis, automation may be an appropriate means to conduct an operation. However, there are usually trade-offs. Automation can introduce complexity, increase human exposure to risk and add complex risk to be assessed and controlled. Now, further complications have to be addressed: software error, logic error, environmental effects to firmware or hardware, maintenance, computer-human interaction, etc.

Almost every year, there is a new and improved so-called hazard model, along with a new definition of what a hazard is or is not. Hazards are unsafe acts and/or unsafe conditions; there are initiating, contributory and primary hazards. Hazards provide the potential for harm. Hazards can be latent or real time.

The system is safe because we tested it.
A complex system can be tested for years, but still not verify all logic. The key is to conduct an appropriate hazard analysis and risk assessment to derive safety-related tests. Specific testing should be conducted to validate and verify mitigations.

Test engineering is an extensive discipline, and books have been written on testing methods: prototyping, mock-up, bread boarding, "go, no-go" testing, built-in testing, simulation, statistical analysis and trending. All of these aspects have system safety ramifications, especially if the testing is conducted specifically for safety.

The bottom line: If system risks are not identified, extensive testing will not help from a safety point of view. The most important action is to conduct an inclusive hazard analysis and risk assessment. The output of such an analysis will drive safety-related testing requirements.

Conducting test safety analysis is another important consideration. There can be real-time hazards and risks during or as a result of testing. The test may also introduce real-time or latent hazards within the actual design. If the test plan is not adequately designed, additional hazards and risks may also be introduced. Decision errors made in the plan can also introduce risks. A poorly constructed or incomplete test will also introduce more risks.

• "The use of this safety standard is only for guidance."

There is a problem with the concept of "only for guidance," especially if a particular safety standard has increased the level of protection or control. Consider that a new innovation is mitigation against a fatal risk, and the state of the art or best practices have improved. The new protective concept has been published and it has been applied. Consequently, poor judgment is applied, and the new protective concept is not adapted since the standard is "only of guidance." From a system safety view, the state of the art in protection must take precedence over all other logic.

• "This system has been grandfathered and we don't have to apply the new safety requirement."

This statement applies poor logic to avoid the improvement in safety. Naturally, cost and resources are always involved in a decision. The point here is that if a hazard has been identified, it must be fixed. There may be other cost-effective methods of mitigation that can be applied.

• "I am the management authority and I will assume the risk."

A person may assume a risk, but may or may not have the actual authority and accountability to assume the particular risk — especially if the risk is involuntary and the general public is involved. A question comes to mind: What gives this person the right to assume a risk when other people are exposed? The person making the inappropriate decision may not be aware of all the existing axioms. Again, the risk must be mitigated.

• "Concentrate on design requirements to make the system safe."

It is important that safety is designed into the system. However, there are many risks that cannot be designed away. Consider the lifecycle of the system and the lifecycle of a system accident. Any poor decisions throughout the lifecycles that will have an effect on the system can have an adverse effect on system safety. To mitigate poor decisions, there is a need for safety programming, which supports the lifecycles. There are many administrative controls within safety programs needed to mitigate risks introduced by people interfacing and interacting with the system. Unfortunately, because of adverse human dynamics, it is not possible to design out all risks. An analyst must keep an open mind and try to holistically address all system risks.
Common Statements...Trouncing Safety

by Mike Allocco, Fellow

In the Spotlight:

• "Our approach to safety is the best way to go."

There is no best way of applying safety. It is a good idea to have broad experience and knowledge of system safety, safety engineering and safety management. Maintain a diverse tool box of methods and techniques that have been applied in other safety-related disciplines.

• "These people don't understand system safety.... or x safety"

Some safety people do not do a good job of communicating their safety expertise. They tend to practice or stay in one particular safety area or industry. Safety specialty disciplines have had a decentralized evolution, and integration with cross-communication is limited. Keep an open mind and you will find that there are commonalities and new ways of applying techniques and methods. Good cross-communication will increase understanding and improve knowledge.

• "I need to do this or that analysis."

There are many system safety analysis methods, and some of the methods may be redundant or similar. Some of the techniques can be integrated together to conduct a more comprehensive safety analysis. An analyst may favor a particular method and may develop an expertise in applying a particular technique. But an inappropriate method can be selected and applied with little benefit. A particular method may be selected simply because it is common or known, like fault tree analysis or failure modes and effects analysis.

There should be a specific reason or requirement as to why a particular method is being used. It is essential that system risks throughout the lifecycle have been identified and the overall analysis must be as inclusive as possible. A most significant aspect of system safety is conducting a good hazard analysis.

• "This element of the system is more important than that element."

A complex system may include hardware, software, firmware, and human and environmental elements. Some analysts may concentrate on one or two particular elements of the system, and may exclude other elements of the system. Within a complex automated system, analysts may concentrate on software or firmware, resulting in extensive resources expended. There may be laborious efforts in two out of the five elements. Unfortunately, minimal work may have been conducted for hardware evaluation, and the human and environmental areas and hazards may not have been identified. This is why inclusive system hazard analysis is emphasized, where system risks — and the interactions and interfaces between all the elements — are evaluated.

There is always a trade-off between resources and safety benefits gained. It may be more important to conduct analysis with breadth rather then depth, in that lifecycle risks are considered. Good safety planning is needed before analysis tasks are allocated. Planning should also consider the discovery of complex system risks that may require in-depth detailed analysis.

• "System hazard analysis will not work for this complex system."
System safety has accepted and adapted to cutting-edge, known and initially unknown engineering challenges and highly complex technical risks. A main premise or axiom of system safety is to support cutting-edge and exploratory efforts. If the entity can be described and understood, it can be analyzed from a system perspective. System hazard analysis addresses the total system, from inception through disposal, and, in some cases, extended use. The analysis considers system, systemic and synergistic risks.

- "That intended use was not addressed and the system was misused."

Intended use considers the criteria as to how the system is to be used. Foreseeable misuse must also be evaluated when addressing system safety. It is important to determine how a system can be intentionally or inadvertently misused. There have been situations when the reinvented intentional misuse has become customary use and, consequently, the so-called misuse must be evaluated from a system safety view.

Loosely coupled distributed systems may evolve over time and the evolution may not have been part of the original design. This evolution needs to be evaluated from a system safety view.

Also, the extended life of a system may change its intended use. Systems may last longer than expected, or a new application may become apparent. Bottom line: Any change to the system must be evaluated from a system safety perspective.

- "Safety engineering is more important than safety management."

It is imperative to apply diverse knowledge of system safety, safety engineering and safety management practices. These disciplines are integrated via some common principles and axioms and, depending on the specific safety-related need, a particular method within system safety, safety engineering and safety management may be applied.

- "We have met the rules, criteria, and assumptions defined in the analysis (safety report), so we are safe and the analysis is complete."

An analysis can be easily negated by inappropriate statements, poor assumptions, illogical caveats, mistakes in methods applied, missing information, misjudgments, oversights, errors and omissions, cursory efforts, inappropriate definitions, deviations from practices, poor criteria and inappropriate terms.

- "The following (important elements) are excluded from the system analysis."

It is inappropriate to exclude important elements that affect system risks: hardware, software, firmware, and human and environmental factors. However, in conducting subsystem analysis, elements may have to be excluded, since, for example, software or firmware may be the subject of the specific analysis. It is expected that subsystem hazards are to be included within potential adverse sequences when addressing potential accident scenarios and system risks.

- "This safety problem does not come under system safety or x safety."

Unfortunately, system safety may not have been applied within a complex entity, and different conventional safety approaches may have been adapted. In some situations, concepts of system safety may have been implemented within safety management systems. It remains a challenge to attempt to manage the safety of a large complex entity while excluding system safety axioms that address system thinking, integration, interaction and system risks.

- "We must use this particular worksheet to conduct hazard analysis."

Some management authorities may insist on the use of particular types of worksheets to conduct system safety analyses, hazard analysis, accident investigation or particular safety studies. Highly experienced analysts may be hindered in their efforts when particular formats are dictated. There is a need for flexibility so that experienced safety professionals can create and adapt many
methods and techniques applied within analysis. In some situations, a number of techniques may be used in an integrated manner to meet a particular objective.

• "The probability of this risk is EE -X based upon past accidents."

Past history and loss analysis may or may not be applicable when estimating future risk. When there is a frequent type of accident (not a rare event), applying appropriate statistics can be helpful. Keep in mind that the system may be dynamic and in constant change, and prior distributions of random variables may not be the same for future distributions containing random variables. The past will not repeat itself statically, especially if the previous accidents were adequately investigated and changes were made to mitigate risk.

• "This event can't happen because of how many failures that have to occur."

Time and again, people are dumfounded, confounded and mystified when catastrophic events occur. How could all the unusual events line up to form this accident? The accident was incredible! Unfortunately, incredible accidents do occur. But many accidents are preventable, and this is why system hazard analysis is so vital. Potential accidents in the form of system risks must be hypothesized, considering physics and the natural order of adverse progression.

• "We can only analyze the system to a single failure."

There may be some confusion between reliability and system safety, when this statement is made. There is an antiquated assumption that systems should only be analyzed considering a single failure, and that two failures are unlikely. In a robust appropriate design, one can argue that two failures are unlikely only when common-cause events have been eliminated.

• "Our personnel are trained and they will not make errors or mistakes."

The answer for all human deviation is not training. There are extensive methods in behavioral-based safety, human reliability, human cognitive science and human factor engineering, which identify, study and mitigate the risks associated with human error. The human remains the most complicated part of the system.

• "That hazard is fixed because of this mitigation."

A particular hazard may or may not be fixed by a single mitigation. Consider the concepts of hazard control analysis, validation and verification of controls, as well as monitoring the system to assure continued control. Mitigation can fail, validation and verification of control can be inadequate, and monitoring can also fail. All of these failures can be latent or real-time hazards.
Common Statements...Trouncing Safety

by Mike Allocco, Fellow

Pages 1 | 2 | 3 | 4 | 5

- “These safety people don’t understand the operation.”

Actual experience can be invaluable; however, not everyone can acquire a particular type of experience. A safety analyst needs to have the capability to acquire operational knowledge through facilitation, communication, discussion and interview. An analyst must be able to gain information from experienced professionals. Analytical work can be conducted via team effort, including experienced operational professionals and experienced safety professionals.

- “We only address X number of hazards.”

It is not appropriate to confine an analysis to identifying only a particular number of hazards. The analysis activity must be as inclusive as possible and lifecycle risks must be addressed. An analysis is complete when no other risks are identified. The lifecycle of a system accident must also be considered.

- “This is not a hazard.”

If the circumstance, condition or act presents the potential for harm, it is a hazard and it must be mitigated.

- “The risk is within this cell of the risk matrix.”

Risk has many attributes. Risks can be point estimates or they can be characterized as distributions. Risk can also be static or dynamic. As the system changes, so does its risks. It is advisable to define risk by its attribute of concern and understand that risk will vary by many factors or circumstances. Risk is an estimation to be used for comparison or risk-ranking purposes.

- “Simulation is good or bad; it proves or disproves safety.”

Simulations and models can provide important information about the potential performance of a complex system, process or procedure. These methods can be used to acquire data to develop design requirements, and provide visual or virtual views of the system. Simulations or models can be useful in identifying hazards and acquiring safety-related information associated with the integration of various elements of a system. Simulations or models can aid designers in predicting how the system will perform, given particular situations or events. From a safety perspective, simulations and models must reflect circumstances, situations or conditions, and be as close to reality as possible. Depending on the importance (level of risk), there is a need to be able to judge how close the simulation or modeling is to reality. Additional hazards and risks can be introduced if simulations and models do not
define risk by its attribute of concern and understand that risk will vary by many factors or circumstances. Risk is an estimation to be used for comparison or risk-ranking purposes.

- "We are only evaluating the change in the system."

It is not easy to confine a safety analysis to a particular change within a complex system. The change itself may be bounded as if it were a black or white box that has been integrated into the complex system. There are lifecycle risks associated with the change, as well as interactions and interfaces to consider. It is advisable to understand all the potential accidents that can occur as a result of the change. It may be inappropriate to assume that existing controls will mitigate system risks that may be introduced as a result of the change. Errors can be made by excluding elements of the existing system. For example, with complex automated systems, a seemingly minor software patch may introduce latent hazards elsewhere in the existing system.

- "You must use this accident model."

There are favorite accident or hazard models within particular industries. A precise model may be referenced from time to time so it may become a custom. There are many so-called accident and hazard models that vary by points of view, theory and custom. It may be helpful to study the particular model to understand the principle it is trying to convey. It can also be useful to use different models to look at a particular safety problem from a different point of view. After studying various models, common concepts may be identified. These common concepts or axioms may be adapted, considering the human, machine and environment.

- "The automated system will get better with age."

An automated system will not get better with age. Consider systems with extensive software; it may take many years to verify all logic, if that is even possible. There may be a point of view that the system will fail and be repaired and eventually all problems will be fixed. This attitude will contribute to risk, not mitigate it. This is the old "fly fix fly" concept used prior to system safety implementation at the end of World War II.

There is no easy solution when evaluating a complex system. The details remain important and must be evaluated from a system safety view. These details include evaluating all the elements of the system: software, algorithms, associated logic, architecture, firmware, micro-devices, hardware, human interaction and environment. There are, however, ways of mitigating lower-level hazards by applying higher-level controls. There are always opportunities to apply system safety analyses to existing systems, as long as the design information is accessible or can be reconstructed or re-engineered.

- "The system has been in the field for x years, so it must be safe."

There may be false trust in that the system has been in operation for a period of time without a failure or malfunction. However, a latent hazard can sit dormant until a particular circumstance occurs and that latent hazard is triggered. This situation may be more likely if detailed system safety analyses have not been conducted.

There is a "performance paradox" to address when the system is stable and there are no accidents — safety efforts may decrease and resources may be re-allocated. This is another form of false trust in the system. When considering complex systems, system safety efforts should involve a continuous process of improvement. Because of extensive complexity, it may take a continuous process of monitoring, on-going hazard analysis and risk assessment.

- "The system was just inspected, so it must be safe."

Nothing is perfectly safe and no single inspection can guarantee safety. As you may expect, safety-related inspection is another extensive topic. Depending on the inspection objective, there will be an inter-relation, interaction or interface with system safety. Expensive loss-control audits can enable the evaluation of most safety-related programs and associated hazard controls. Specific inspections may pinpoint latent catastrophic hazards. Cursory or inadequate inspections can introduce risk and create additional hazards. Inspectors have inadvertently damaged systems and introduced latent or real-time hazards. A false sense of security has also been established as a result of an inadequate inspection. There are also lag times between inspections in which hazards can exist, develop or manifest. Adequate inspections can be a source of hazard identification, and real-time hazards can be mitigated.
“There have been no catastrophic accidents in x time, so our safety efforts are working.”

System safety is not stagnant; it is a dynamic set of processes. There is also variability in systems; they are dynamic. Because of dynamics, new risks can be introduced at any time throughout the system lifecycle. A so-called simple mistake, human error or physical degradation in the system can introduce new hazards. When there is over-trust or over-confidence in the system, complacency may develop, and accidents will happen.

“We will fix this hazard by applying this new method of behavioral modification and re-training.”

The human is the most complex and dynamic element of the system. Poor decisions and almost any human action can have an adverse effect on the system; hazards and additional risks may be introduced. Consequently, human engineering is vital. However, there are poorly engineered systems that do not accommodate human dynamics. The human or system, therefore, may be exposed to risk as a result of minor errors, deviations, mistakes or inappropriate actions. Behavioral-based safety and human reliability techniques, when appropriately applied, can eliminate or control risk.

It may be more appropriate to initially design the system to accommodate the human, since humans are dynamic and mistakes will happen. An existing system may be re-engineered and re-designed so that the hazards are eliminated or controlled to an acceptable level. In some situations, a simple modification can be made to the system, rather than attempting to change human behavior or applying additional training. Some human factor-related risks may present more challenges — way beyond attempting behavior modification and training. Changing a so-called mindset is not easily accomplished.

“Our safety culture is excellent, so we must be safe.”

Safety culture gained notice as a result of a report of the same name by the International Nuclear Safety Advisory Group of the International Atomic Energy Agency (1991).\(^1\) Culture describes a set of shared attitudes, beliefs and habitual practices: “the way we do things around here.” The so-called safety culture in an organization is dynamic and variable. Safety culture is affected by internal and external influences: subcultures, internal strife, economics, various physical and emotional stressors, motivation, attitudes, social norms, and conventions and politics.

In the real world, there may never be a perfectly balanced system with a particularly good safety culture. In many situations, the safety professional must effectively practice in entities with no specific safety culture. It becomes a laborious effort to implement a good safety culture. All the elements of an effective safety program come into play: positive self-motivation, open communication, continuous improvement, knowledge of risk and hazards, proactive thinking, contingency planning, human reliability, monitoring of behavior and appropriate training.

One can consider the Safety Culture Maturity Model\(^2\). To improve safety culture, there is a need to:

- Develop management commitment
- Realize the importance of frontline staff and develop personal responsibility
- Engage all staff in developing cooperation and commitment to improving safety
- Develop consistency and fight complacency

“We re-started the system and the anomaly (safety problem) went away.”

Unfortunately, this is typical when considering complex automated systems with extensive software. The operator re-boots the system and the problem goes away. This situation can be a result of a systemic abnormality, and it may not be possible to replicate the anomaly. It can be expected that there is a latent hazard if the situation repeats itself. System safety evaluation and investigation is required.

---

\(^1\) For an excellent reference source that addresses safety culture and error avoidance techniques, see: Electric Power Research Institute (EPRI), Report, Approaches to Error Avoidance, December 2006.

**In the Spotlight**

**Common Statements...Trouncing Safety**

by Mike Allocco, Fellow

Keep your eye on your sources, keep your eye on your system. To make a decision, you must know what you’re working with. You can’t lean on the data you have, you have to lean on what the system is capable of. You can’t assume that the system will do what you think it will do, you have to assume that it will do what it will do. You can’t trust the system to do what you think it will do, you have to trust the system to do what it will do. You can’t rely on the system to do what you think it will do, you have to rely on the system to do what it will do.

---

*We conducted a lean safety analysis.*

Lean production and manufacturing techniques are in vogue. But it can be dangerous when lean techniques are applied to safety. Lean safety analysis can introduce risks in that false confidence may be established, and there may be many unidentified risks. Nothing is more disheartening then a cursory safety analysis. In system safety, the details are vital. An innocuous latent hazard can have catastrophic results.

However, there are exceptions involving detailed analysis — when safety analysis is applied in real time by the people who may be directly exposed to the apparent risk. From a human factors or behavioral-based safety perspective, it may be prudent to train front-line people to recognize hazards and know how to mitigate them. Job safety analysis, contingency and procedure analysis come to mind. It is advisable that the safety professional participate, train, review and provide guidance. The safety analyst may develop a generic analysis template (GAT), which is a detailed analysis of typical exposure that is likely to exist — typical hazards and controls. The GAT can be used as a checklist and guide for conducting similar analyses.

*We will stand by for instruction from the safety manager during this contingency.*

The concept of proactive thinking supports contingency planning. It is important to anticipate what can happen during an accident, as well as after harm has occurred. The concept of the lifecycle of an accident addresses the adverse process from the initiating hazard through to the outcome. Contingency action can start during the initiating event to abate or hinder adverse flow. Further, the harm can be decreased by containment and causality response.

Within contingency analysis, potential accidents are addressed and particular contingency actions are planned for the total accident lifecycle. Administrative controls in the form of procedure response, instruction, training, mock-ups, dry runs, simulations and drills are conducted. Specific emergency response equipment may be needed. Real-time contingency response can be hindered without proper planning. There have been past catastrophic and major accidents with delayed or hindered contingency response. For any system, contingency analysis and planning is vital.

During an emergency situation, it is inappropriate to start an evaluation or analysis to determine what is happening. Understanding how complex systems fail and propagate is an important part of contingency analysis and planning. Appropriate simulations and modeling can help in the understanding of failure, error and hazard propagation. The simulation and model must be as close to the design and reality as possible.

*System safety is rocket science: hard to understand, complex, laborious, and it is used by aerospace and defense industries only.*

Unfortunately, some people may be intimidated by system safety. Properly explained and communicated system safety axioms can and have been applied to almost any safety-related problem, entity or system. However, note that if the axioms are not appropriately applied, more risks can be introduced.
During an emergency situation, it is inappropriate to start an evaluation or analysis to determine what is happening. Understanding how complex systems fail and propagate is an important part of contingency analysis and planning. Appropriate simulations and modeling can help in the understanding of failure, error and hazard propagation. The simulation and model must be as close to the design and reality as possible.

• "The functional hazard analysis is complete and no other analyses are required."

A functional analysis can be important, depending on circumstances. However, the analyst must understand what drives the function, considering that a function is an abstraction of the system. Actual physics and energy interaction are involved with the particular physical action within the system. There is hardware, software, firmware, human factors and the environment to address, and many other system safety analyses, techniques and methods to be applied. 4

• "We can't make everything safe, so accidents will happen."

Accidents are preventable and by proactively hypothesizing potential accidents, associated risks can be mitigated to an acceptable level. The key is to aggressively identify and mitigate risks throughout the lifecycle. Consider that humans will make errors and mistakes, and will deviate. These situations can be initiators within the adverse process. The system should be designed to accommodate errors, mistakes and human deviations.

• "We met this safety standard, so we must be safe."

Meeting a particular standard is no assurance of a safe system. Standards may be the result of a general consensus associated with a generic risk. The standard may not accommodate the particular exposure, system state or specific design, or mitigate a particular hazard. This is why inclusive hazard analysis and risk assessment is vital. Safety is a relative term. It can only be indicated that the identified risks have been eliminated or controlled to an acceptable level. Should there be deviation, failures or errors related to the controls, hazards will manifest and risk will increase.

• "The inspector just approved this system so we must be safe."

The inspection criteria applied may or may not mitigate a particular risk. There can be errors associated with the inspection process, procedure, checklist, related equipment and devices, as well as with the inspector's background, training and experience. These errors are considered hazards that must be mitigated.

However, an appropriate inspection may verify a particular hazard control. Real-time inspection may also uncover additional hazards, scenarios and risks. Inspection techniques can be considered hazard controls in that real-time circumstances may be verified. Random observational inspections are part of behavioral-based safety in that unsafe acts and/or unsafe conditions can be noted. Experienced inspectors are also important participants within the hazard analysis efforts.

• "The system is listed and certified so it must be safe."

Listing and certification services may only address a small subset of particular hazards, and those hazards may not be mitigated to an acceptable level. Listing and certification criteria will vary and may involve particular generic tests and analyses. It may be possible via evaluation of the particular criteria that the hazards considered are appropriate. General industry standards may have been met, again only to mitigate obvious apparent hazards. It remains important to conduct an inclusive hazard analysis and risk assessment.

About the Author

The concept of the Generic Analysis Template was initially discussed within the following:

See the following references for further information on analyses methods and techniques:
The Pennsylvania Patient Safety Authority has received 4,230 event reports associated with PCA pumps. Many of the reports showed confusion about the medication order. Their analysts researched the U.S. Food and Drug Administration's Manufacturer and User Device Experience (MAUDE) database as of January 31, 2011. They found that out of the reports of events using PCA pumps, 826 (19.5%) resulted in injury or death.

PCA pumps are filled with Morphine, Fentanyl or Dilaudid. They are strong narcotics that effectively and rapidly diminish pain. The standard of care [Ref. 2] requires an order for a PCA pump, which includes the name of the medication, the dose that can be delivered when the patient pushes a button, the interval between doses, the lockout interval (how much medication the patient can receive in an hour), possibly a basal rate (continuous infusion of the narcotic), the frequency of monitoring of the patient, and orders for a rescue drug (Narcan) in the event of over-sedation.

Hazards Associated with PCA Pumps

According to FDA, the most common types of reported problems have been associated with software defects, user interface issues and mechanical or electrical failures, including [Ref. 3]:

**Software defects:** Many of the problems that have been reported are related to software malfunctions. For example, some pumps fail to activate pre-programmed alarms when problems occur, while others activate an alarm in the absence of a problem. Other software errors can lead to over- or under-infusion. In one case, a software problem called a "key bounce" caused an infusion pump to occasionally register one keystroke (e.g., a single zero, "0") as multiple keystrokes (e.g., a double zero, "00").

**User interface issues:** There have also been numerous reports of confusing or unclear on-screen user instructions, which may lead to improper programming of medication doses or infusion rates. For example, the design of the infusion pump screen may not make clear which units of measurement (e.g., pounds versus kilograms) should be used to enter patient data, leading to inappropriate dosing.

**Mechanical or electrical failures:** Other problems that have been reported include components, such as pump housings that break under routine use, premature battery failures, and sparks or
pump fires. Each of these types of incidents can create risks to patients, including the potential for over- or under-administration of critical fluids.
Infusion pumps empower patients to control pain, but they remain a serious risk. Just as with any medication, frequent re-evaluation and monitoring should be performed in a consistent and judicious fashion.

What is being done to mitigate hazards?

The FDA plans three major initiatives:

- **Establish additional requirements for infusion pump manufacturers.** To provide greater assurance that design deficiencies are identified and corrected before they lead to safety problems, the FDA is moving to require that manufacturers of infusion pumps include additional design and engineering information as part of their pre-market submissions and conduct additional testing of their devices. It recommends that each infusion pump pre-market submission include a comprehensive discussion of steps the manufacturer has taken to mitigate risks at each stage of the device’s lifecycle — including design, manufacture, servicing, and maintenance and use. In addition, it recommends that manufacturers conduct design validation testing in the setting where the device is intended to be used (e.g., a hospital or the home), to account for real-life environmental or user interface issues.

- **Proactively facilitate device improvements.** The FDA is actively working with manufacturers, members of the academic community and others to address identified infusion pump problems. The agency is also collaborating with its foreign regulatory counterparts to confront infusion pump safety issues. It is currently engaged in a number of cooperative efforts to facilitate the development of safer and more effective infusion pumps. It is also using its in-house expertise to help prevent malfunctions in infusion pump software.

- **Increase user awareness.** The FDA is launching a new infusion pump Website, which features basic information about infusion pumps and commonly seen problems. The site also describes actions that patients and professionals who interact with infusion pumps — including hospital staff and administrators, as well as home users — could take to help prevent safety problems. The FDA encourages all users to report infusion pump problems to help the agency develop a better understanding of the risk-benefit profile of these devices and to take appropriate actions to enhance patient safety.

The Pennsylvania Patient Safety Authority has yet another approach. It seeks to empower patients and caregivers to avoid medical errors and protect patients, and has issued the following guidelines:

- Since the patient must deliver each dose of medication to him- or herself from the PCA pump, it is important that the patient is mentally alert and able to understand how the PCA pump should work. The PCA pump patient should also be able to communicate his or her pain level to the caregiver. Therefore, children and confused older patients are not ideal candidates for the PCA pump.

- Over-sedation has also occurred in PCA pump patients who have health problems prior to their hospital stay. For example, obese patients, asthma patients, patients with sleep apnea or patients taking prescription drugs that may increase the effect of stronger pain-relieving medications are questionable candidates for using the PCA pump. Basal rates should be avoided and, if added, patients should be closely monitored.

- Patient caregivers should be aware of any changes in the patient that do not seem right. For example, if the patient is still experiencing pain after dosing, a healthcare worker should double-check the pump’s programming.

- Caregivers should not push the button for their patients. It increases the risk of the patient overdosing if more than one person is administering the medication.

- Patients should be able to understand what is expected of them if they are put on a PCA pump. Caregivers must make sure the patient understands what is expected when using a PCA pump. This PCA pump education should be done before the operation or hospital stay.

Some monitoring recommendations

As part of the current state assessment, the San Diego Patient Safety Council conducted a failure mode and effects analysis (FMEA) for PCA usage. The Council attempted to address all of the failure modes in recommendations provided in a tool kit [Ref. 4], providing ways to prevent harm by a redundant system. Such systems are:

- **Pulse oximetry monitoring.** This is primarily useful for assessing changes in oxygenation. While it is not an early indicator of ventilatory failure, this measure eventually falls as the patient stops breathing. If an intervention is given right away, a patient has a chance to survive.

- **Capnography monitoring.** This measures the presence of carbon dioxide continuously and is a more sensitive indicator of hypercapnia. It is more effective than pulse oximetry in providing early warning. It is capable of significantly clarifying the respiratory picture with regard to over-sedation.

Conclusion
Infusion pumps empower patients to control pain, but they remain a serious risk. The FDA is using a good approach from the system safety point of view. It is proactively looking at the risks and seeking risk mitigation prior to the release of new pumps. Meanwhile, the Pennsylvania Patient Safety Authority is offering ways to protect patients. Just as with any medication, frequent re-evaluation and monitoring should be performed in a consistent and judicious fashion.

References

Design-based Safety

by David MacCollum

Leadership in design-based safety is a process that brings order out of chaos. Safety appliances or alternate safer designs often never see the light of day. Why? Because the traditional economic, political and operational priorities have not been satisfied. Before design-based safety can be accepted, the engineer must show how the new design effectively overcomes the traditional priorities.

In most cases, economic barriers are easily overcome, as injuries usually cost more than safety features. The injury-preventing table saw technology developed by Dr. Stephen Gass, called "Saw Stop," prevents injury as the fast-spinning saw blade is instantly arrested in one-quarter of a turn. Yet manufacturers and sales trade associations are actively opposing this safety feature, as they allege that it eliminates the sale of low-cost table saws. Their real reason is to avoid liability. It would seem that their goal is short-term profit from the sale of unsafe table saws rather than reducing the number of severe table saw injuries that cost the public billions. (See "Table-Saw Safety Bill Advances in California Over Objection of Power-Tool Industry," Engineering News Record, page 14, August 27, 2012). Proposals for inherently safer features need to include an explanation of the long-term injury and liability costs that can be reduced by design-based safety.

Today's news media reveal countless examples of hazards that never meet the public eye until the cumulative injury occurrence becomes a scandal. The reason for this oversight of hazardous design is that traditional priorities create strong incentives for covering up repetitive injury occurrences from the same hazard on the same type of machine. I have observed the same hazard in building design. On a flat roof, a 42-inch parapet wall instead of an 18-inch wall becomes a safety railing and prevents falls off the building. When life-threatening hazards are deliberately covered up so that the public is unaware of multiple occurrences from the same hazard, this anti-safety tradition becomes a disgustingly shameful disgrace. Another factor is that some people consider a hazard an acceptable risk. There are also those who feel that buying insurance to spread the risk among many is cheaper than paying for safer design to eliminate the hazard.

Political excuses may also serve as a reason to avoid safe design. In the 1930s, the passenger dirigible Hindenburg burned when docking in New Jersey, and is an example of how highly flammable hydrogen gas was used on this lighter-than-air-ship rather than unburnable helium. It was feared by some that Nazi Germany would use helium for military purposes. The memory of dirigible bombings in London during World War I led to a decision to enact an embargo on helium sales to German firms. The decision to ban the sale of helium did not include an analysis that the zeppelin was a large, slow-moving target that could be shot down easily. A different decision would have allowed the development of this type of air travel.

Operational traditions are notoriously continued for avoiding safe design. Most notable were three NASA disasters:

- The incineration of three astronauts in a space capsule, caused by its oxygen-rich atmosphere (Apollo I)
- A faulty fuel pipe gasket that was not resistant to cold weather (Space Shuttle Challenger)
- The Styrofoam insulation that broke loose and was propelled at a high velocity into a wing (Space Shuttle Columbia)

All of these were hazards deemed by management as "acceptable risks." The reason for these decisions was management's blind devotion to these activities going forward to show the public that NASA was making newsworthy progress. An urgent requirement for immediate results creates strong incentives to avoid any safety delays. To stop an activity because a hazard could possibly cause a failure creates a conflict with management's goals for immediate results. Management then considers the hazard only as a possible chance of failure or a risk. Then,
management speculates on the degree of risk, and the need for safe design becomes no longer relevant. Management's authority to take risks needs to be curtailed. We, as system safety engineers, need to develop for ourselves a broader public exposure. We need to speak out on safe design issues. Somehow, a public record needs to be available so that design-based safety features are made known to the public before a disaster occurs. Unfortunately, after a disaster, when the facts become available showing that design-based safety would have easily prevented the hazard, the person who makes this revelation is labeled a "whistle blower," a term used to change the subject so the need for safer design is put on the back burner and forgotten.

The current role of the system safety engineer as an advisor to management is a step in the right direction. This is not enough, however, as it only puts the ball in the manager's court where there is often little accountability. What is missing is the absence of public awareness of a specific hazard and how to control it by design. The system safety function needs access to independent funding to conduct tests so the hazard can be validated as fact, not nebulous risk. An independent test would have shown that ignition in an oxygen-rich capsule would result in complete incineration. A test would have shown how a gasket can become inflexible in cold weather and not function properly. A test also would have shown that Styrofoam propelled at high velocity could pierce a shuttle's wing. With system safety testing done during development, the opportunity would be reduced for management to engage in speculative risk-taking at a time of "go or no go" decision making.

Planning documents should first be reviewed by a safety engineer, who would list each hazard. Test results always need to be available to the public and the press. Safety engineering leadership based on fact will then become a protector of both management and the public.

I have always been amazed by how Frank Lloyd Wright, the famous architect, was able to project himself to the public as the ultimate visionary leader of his profession. He stated, "Architecture is man's great sense of himself embodied in a world of his own making. It may rise as high in quality only as its source because great art is great life."

Design-based safety is an even greater calling than art, since it is a protector of life! To become a leader, one must serve an apprenticeship to learn the basics. Wright began his career by studying civil engineering, and then he became a draftsman for a leading architect. In 1893, after learning the basics, he opened his own office to pursue an independent practice. On his own, he designed and supervised the construction of the first air-conditioned building. In 1922, after 19 years of practice, he was ridiculed for building the Imperial Hotel in Tokyo on a big flat reinforced concrete saucer rather than on conventional pilings. Frank Lloyd Wright understood why the buildings built on fill in San Francisco collapsed during the 1906 earthquake. When the 1923 earthquake leveled Tokyo, his building was undamaged. Now, he had worldwide fame. In 1938, he founded his western headquarters at Taliesin outside Phoenix, Arizona, which soon became a mecca for those who wanted to become architects. During the last years of his life, he designed the famous Guggenheim Museum in New York. The lesson Frank Lloyd Wright taught is to have enough confidence to stand up to traditional ideology and push to develop safer designs.

Another famed leader, Lee Iacocca, when president of Ford Motor Company, installed an interlock to prevent the driver from starting a car until the seatbelt was attached. The public rejected this approach, and Ford's car sales dropped dramatically. Later, as president of Chrysler Motor Company, Iacocca met with President Richard Nixon and objected to a mandatory federal regulation for airbags, coining the phrase "Safety does not sell!" Design-based safety needs to be scoped to create no conflicts with user priorities. Ultimately, the driver just wants to start the car. The seatbelt interlock was a barrier to this objective. Seatbelts are a voluntary safety feature and user acceptance requires time to develop. Today, voluntary seatbelt usage is generally between 80 to 90 percent. Airbags are not barriers to starting or driving a car, and have been an outstanding success in reducing injuries and deaths in the event of an automobile crash.

Another exemplary function of safety engineering leadership is community stewardship. Washington Group, a large international design-and-build construction company and now part of URS, knows the value of investing in its immediate community. It gave the gift of a Saw Stop table saw to Idaho school districts' manual training shops. These table saws have been designed with a patented safety feature that stops its spinning circular saw blade in a millisecond, making it safer than a cumbersome guard. Students using this saw learn how design overcomes hazards. This gift to the public schools gained Washington Group much community good will.

System safety practitioners grow in professional leadership by using each of these seven skills or
functions:

- In all presentations, studies or recommendations, tell how the proposed alternate safer design or safety feature will meet or surpass traditional economic, political and operational priorities.
- Always review engineering plans and specifications, product prototypes or existing machines to identify hazardous conditions or circumstances of use. Our duty is to identify hazards and eliminate them by design. This sets our profession apart from the marketplace priorities.
- Enhance your competency through continuing education, training, experience, professional license or certification to develop alternate safer designs, and apply technology transfer or select appropriate safe appliances to ensure for reliable hazard prevention by design. This function identifies our professional life-protecting skills.
- Have professional independence from peer pressures that favor anti-safety economic, political and operational biases.
- Gain community support and goodwill wherever possible.
- Develop the ability to show the public design-based safety features that you have had a hand in developing.
- Become a spokesperson for our profession. The public needs to hear about safety from us, not groundless speculation from self-proclaimed publicists. Design is the Holy Grail of safety.

Focusing on the seven key issues will help ensure that your system safety engineering will bring "order out of chaos" and be welcomed by management and the public.
The Conference is Over...Everyone Back in the Box!

by Steven Mattern, Society Fellow Member

Historically, I have had concerns whenever someone suggests that it is a really good thing to "think outside the box." As this thought was the theme of our latest International System Safety Conference (ISSC) in Atlanta, I would like to address some of the issues that I have with this type of thinking from a system safety engineering perspective. Do not get me wrong; I am not against thinking outside the box — some problems may take a non-standardized approach to solve. However, it appears to me that the way this theme is used today, it almost implies that standardized and well-accepted approaches just do not apply in the modern and complex technological environment in which we live and operate. Personally, I do not think this theme should ever drive us to forget the solid foundations of science, math, physics and engineering that have become our foundational and best practices today.

To consider what is "outside the box," one should first consider what is in the box. From the perspective of system safety as an engineering discipline, there are both positive and negative elements inside the box. It should be noted that the lists provided here represent a portion of the system safety paradigm within which I personally work. Your paradigm may look and feel different.

Some Negative Elements in the System Safety Box

- Insufficient resources (money, personnel and schedule)
- Insufficient management support
- Insufficient training and mentoring
- Lack of in-depth engineering analysis
- Stagnation of ideas
- Individuals (some) who have lost their desire and passion

Some Positive Elements in the System Safety Box

- Standards and guidelines
- Best practices
- Lessons learned
- Accepted tools, techniques and methods
- Defined processes
- Defined tasks
- Defined products
- Individuals (some) who have not lost their desire and passion

So, what is outside the system safety box? Personally, I am not really sure. Is it possible that I am getting old and I am not comfortable "outside the box," so I do not want to know? Well, I know for a fact that one of those statements is definitely true! However, I do not want this to sound like an old man's rant about the "good ole days." There is a bottom line to my thinking.

From my perspective, there is a lot of room to work and be successful from within the traditional "box." Consider that the box is full of the basics of sound, fundamental system safety engineering. Many of today's safety engineers have not been taught the basics — or, worse, they have ignored the basics. What is worse yet are scenarios where the basics of sound safety engineering principles are not allowed or implemented due to managerial or contractual constraints. Failure to successfully implement a system safety program in today's environment happens most frequently when the basic principles, techniques and methods are ignored. I do not have to think outside of the box to conjure this opinion.

Bottom Line: Maybe it is time to clean up the inside of the box instead of looking outside the box. I think my box contains nearly everything I need to remain pertinent and successful. However, a
good cleaning is definitely warranted.
Comments and Observations on "The Science and Superstition of Quantitative Risk Assessment"

by Arthur Barondes

(Editor's Note: The following is a critique of the article "The Science and Superstition of Quantitative Risk Assessment" by Andrew Rae, John McDermid and Rob Alexander, which ran in the July-August 2012 issue of Journal of System Safety)

QRA Superstition. Not fit for purpose. Really? The article by our Yorkshire colleagues goes back and forth in describing various pros and mostly cons of Quantitative Risk Assessments (QRAs) before settling on: safety practitioners’ time “may be better spent on activities other than QRA,” such as “thinking about how to make a system safer.” One is left to ponder whether “thinking about safety” is more “fit for purpose” than QRAs. More important, one wonders why “thinking” and QRAs are offered as either-or alternatives when QRAs entail extensive thought processes and are not the sole basis for risk-informed safety decisions. Based on our extensive experience with QRAs for engineered systems, we challenge many of the authors assertions and research, and make some counter observations on QRA limitations.

Clarification

Before examining the authors’ arguments, some clarification is needed on how the authors structured their case against QRA fit for purpose (defined as: “good enough to do the job it was designed to do”). They describe three forms of QRA applications that vary in scope, and then proceed to attack the use of QRAs on the basis of their broadest (and most unlikely) application, viz., assessing all system safety risks, “the ‘top number’ — the aggregated measure of total system risk” as in “determining total risk [for]…all [emphasis added] of the real world consequences.” They generalize their “fit for purpose” arguments on the basis of that broadest application — one that, in our view, is largely impracticable and unreasonable for engineered systems. Indeed, we would agree that as a practical matter, QRAs are not fit for — nor, as far as we know, used for — such far-reaching assessments. But we question the logic of generalizing from that unrealistic application to an all-encompassing denigration of QRA “fit for purpose.” In particular, we find QRAs to be applicable and fit for purpose for assessing risks of specific high consequence, rare events that warrant their high costs in time and money, as in the Nuclear Regulatory Commission (NRC) WASH-1400 that took four years and cost $4M (1975 dollars). The authors give that type of QRA a qualified “free pass.” They concede that such focused QRAs may be “sufficiently accurate and precise…for specific outcomes arising through specific mechanisms, as many of the challenges to QRA [generated by the authors] do not apply in these cases [emphasis added].” But the damage is done. We are left to conclude — perhaps erroneously — that the authors are presenting a “stalking horse” to stimulate debate on the “fit for purpose” of QRAs. Unfortunately, in the process of generalizing on impracticable applications, they have cast unwarranted aspersions on what others see as “tremendous progress toward rational decision making.”

Observations

Recognizing that the authors may be seeking a solution to a non-problem, we make a number of selected observations to set the record straight. To begin, we applaud their skepticism and some of the issues they raise. However, we find it important to note that their attacks on QRA “fit for purpose” are based, for the most part, on examples of shortcomings not in the QRA methodology, but in the execution. They present an overview of the QRA methodology from the “30-year-old 1983 "Red Book" (tailored to adverse health effects, e.g., cancer, rather than engineered systems) with the authors’ closing critical observation: “very little information exists on the validity...
We do not find that dearth of information. As an example, the 34-year old (1978) NRC-chartered Lewis Review Group (LRG)\(^5\) of WASH-1400 (cited by the authors) — an in-depth peer review — includes an entire page (p. 45) of examples of techniques and their use in the regulatory process. A few are quoted here:

Use of the techniques was anticipated in several applications made before the Study was completed. A probabilistic study of aircraft crashes has led to a criterion limiting acceptability of sites for nuclear power plants to areas far enough from airports. The earlier reviews (1972-73) of anticipated transients without scram (ATWS) started from a requirement that these events have a probability of less than \(10^{-6}\) and assessed the ability of reactor designs to meet this. Other uses of probabilistic methods have been made with varying success in increasing numbers since issuance of the Reactor Safety Study. A few examples are: more refined methods of seismic analysis based on probability of occurrence of earthquakes and probability that structures can withstand assumed earthquake stresses, performance of backup power systems, the effects of overpressure and other transients on reactor pressure vessels, the probability of piping failure, and the effects of missiles generated by breakup of a turbine.

That aside, we argue against the authors' defined "primary claim" for QRAs, viz., that they must have sufficient accuracy and precision for "aggregated…total system risk." As described earlier, each QRA should have sufficient accuracy for its specific purpose. That is rarely, if ever, assessing aggregated risk. Rather, it is assessing the risk of a single specific end state (mishap), e.g., core meltdown, and often ordering risk contributors to support risk management. The use of a single end state is exemplified with the authors' use of WASH-1400. That pioneering 1975 QRA examined two reactors to assess a specific end state: core meltdown and consequent health effects — not "aggregated…total system risk."

Looking more closely at WASH-1400 and the LRG report, we form a different picture than the authors do. Whereas the LRG severely criticized parts of that QRA's execution, it endorsed the methodology and advocated its wider use. The LRG report states (p. vii):

> We do find that the methodology, which was an important advance over earlier methodologies applied to reactor risks, is sound, and should be developed and used more widely under circumstances in which there is an adequate data base or sufficient technical expertise to insert credible subjective probabilities into the calculations.

As for the values of the risk estimators and their uncertainty bands, the LRG said, "We are unable to determine whether the absolute probabilities of accident sequences in WASH-1400 are high or low, but we believe that the [stated] error bounds on those estimates are, in general, greatly understated," — i.e., optimistic. However, with the benefit of hindsight, we note that subsequent years of real-world U.S. reactor experience that includes the Three Mile Island accident — "extant evidence" — shows core meltdown frequency within the WASH-1400 upper uncertainty bound. (Note: The authors erroneously claim that "uncertainty ranges were not provided" in WASH-1400, and that the LRG "raised concern...that the uncertainty...was unstated...[and] unknown." They also refer to claims that the probability estimates were pessimistic.)

The authors also cast doubt on the QRA methodology by citing that "one of the [seven LRG] authors...questioned whether the methods could ever provide estimates with sufficient confidence." But that is not an accurate interpretation of Dr. Frank von Hippel's reservation. As stated in the LRG report, he "...questions whether, for a system as complex as a nuclear power plant, the methodology can be implemented to give such a high level of confidence, that the summed probability of many known and unknown accident sequences leading to an end point such as a core melt is well below the limit set by experience [emphasis added]." Note that the reservation is for accepting probabilities that are not consistent with experience — not for the QRA methodology, per se. The NRC translated Dr. von Hippel's concern into "quantitative risk assessment techniques...should not be used to estimate absolute values of probabilities of failure of subsystems unless an adequate data base exists, and it is possible either to quantify the uncertainties or to support a conservative analysis."\(^2\) That was in the late 1970s, in the typewriter days, before the widespread use of computers and, in particular, bench-marked fast-running simulation codes to fill data voids.

Next, we examine the authors' arguments on causal models. Whereas comprehensive hazard identification is part of the QRA methodology and essential for executing the methodology, we would argue that hazards are most apt to be identified using a methodology that actively seeks them in a structured program. The QRA methodology includes overarching qualitative fault trees that have the specific purpose of identifying all hazards and initiating events that might lead to the undesired end state (top event). These Rasmussen-inspired Master Logic Diagrams (MLDs) are peer reviewed and updated for newly discovered hazards. This is a "process of systematically...and good reason to view the results...with skepticism."
We also take issue with the question-and-answer sequence on the utility of a QRA that produces an inaccurate "top number" (a loaded question to begin with). In something of a non sequitur, the authors cite a paper by Apostolakis\(^6\) (now a NRC Commissioner), saying he "chose specifically not to defend the quantification of aggregate risk." In our reading of his paper, we do not find any substantiation for that observation. Indeed, the paper does not contain the phrase "aggregate risk" — perhaps because QRAs are not suited to that purpose. However, the paper does contain numerous references to the productive use of Quantitative Risk Assessments for high-consequence, rare events.

Continuing with the Apostolakis paper, the authors mistakenly state that he "concentrates on identifying opportunities for design improvements or further assurance." In fact, he concentrates on safety programs that exhibit "defense-in-depth," as in, "It is my thesis that QRAs should be viewed as an additional tool in safety analysis that improves safety-related decision making... [although the tool is not perfect] it represents tremendous progress toward rational decision making." And, "I wish to make one thing very clear: QRA results are never the sole basis for decision making by responsible groups... safety-related decision making is risk-informed, not risk-based. The requirements of the traditional safety analysis...are largely intact." Since we might be viewed as biased in our reading, we strongly recommend that those interested in the subject read the Apostolakis paper for themselves (see link in footnote 2).

Next, the authors identify a number of potential problem areas that, although real and worthy of serious consideration, are extraneous to the issue of QRA methodology "fit for purpose." They deal with analyst and reviewer bias, competence, integrity and the like, as well as management considerations, such as effective communication, separation of risk assessment and risk management. The "reviewer" issues are interesting, not because they are germane to evaluating QRA methodology, but because they introduce the reader to the otherwise neglected quality assurance role of structured peer involvement and review by independent experts embedded in the methodology. Whereas peer review poses its own problems in execution, it has long been accepted in the scientific community as "the best method of assuring the technical credibility of such a complex undertaking."\(^7\)

### QRA Limitations

We could go on with more comments and observations, but we find these sufficient to question the QRA "fit for purpose" paper — or, in the authors' words, "good reason to view the results...with skepticism." Instead, accepting that QRAs are not perfect, we offer what we see as some real programmatic limitations — as in cost, schedule and performance — in the execution of what we see as a fit for purpose QRA methodology.

First, QRA execution is time-consuming and expensive. Again, WASH-1400 was a four-year, $4M effort in the 1970s. This limits the application of QRAs to risks that are commensurate with the QRA costs. This usually means risks of high-consequence, rare events.

Second, QRA execution must get the physics and statistics right. This is easier said than done. This can require material properties outside the range of empirical data and extreme environments not normally encountered. The statistics must produce risk estimators based on a host of random variables expressed as distributions with confidence intervals and correlations in events. The statistics must also accommodate uncertainties as they apply to the risk estimators.

Third, QRA execution can face critical data voids and uncertainties. These can be "show stoppers" or expensive "show extenders." Accommodating them can involve test programs and structured expert elicitations that add cost and can affect schedule. Worse, aleatory and epistemic uncertainties can be too great to order risk contributors with statistical significance.

Fourth, required peer involvement during the course of QRA requires disinterested peers. These can be hard to find. Further, their reviews can lead to extensive and expensive re-work.

Fifth, QRAs are not intended to answer the question, "How safe is safe enough?" They provide quantitative risks estimators (usually central values from risk distributions) and their uncertainty bands. "How safe is safe enough?" is answered by management in terms of willingness to accept risk. QRAs can also identify risk mitigation actions for consideration by management.

### About the Author

Arthur Barondes is a principal at Analytics International Corp., based in Alexandria, Virginia.
Safer Hospital Care
By Dev Raheja
CRC Press, Taylor & Francis Group, 2011

Book Review by Clif Ericson

It's somewhat disconcerting to learn that more people die each year from medical errors than from auto accidents and cancer. This fact has been documented by the medical industry. Is there anything that can be done to change this? It appears that in addition to lethargy in making recommended safety changes, the medical industry has not yet quite discovered system safety and the benefits it provides.

Author and engineer Dev Raheja has addressed this problem and has written this book on how system safety can be effectively applied and integrated into the medical field. In it, he has taken a unique approach — rather than attempting to directly translate aerospace safety to medical safety, he has nicely woven safety around the concepts of continuous improvement and human error design. For me, this eliminates the mental bias of "just do it the aerospace way," which can put many people off right from the start.

Raheja stresses the idea that medical safety is about implementing management methods to both address safety and to work on continuous improvement in healthcare processes. His realistic mantra throughout the book is: It may not always be possible to eliminate human error, but accepting mishaps resulting from human error is a choice. Accepting the mishaps resulting from human error is an obvious poor choice; the better choice is to prevent these mishaps by applying the methods described in this book.

Raheja has more than 30 years of experience in the safety field, and has written several books on safety. He is well recognized in both the safety and reliability fields, and is well known for his expertise in human error and how to protect against human error mishaps. He has been a leader in advancing professional safety methods by understanding the errors that occur in hospitals and how these errors can be reduced in order to save lives. He writes a regular column on healthcare safety in Journal of System Safety.

I highly recommend this book for those individuals interested in improving medical and hospital safety. I would also recommend this book for current system safety engineers who would like to
learn more on how to improve on human error safety.
Unintended Consequences

Communication Breakdown

by Terry Hardy

On January 25, 1990, Avianca Airlines Flight 52 crashed while making an attempt to land at John F. Kennedy International Airport in New York. A total of 71 people died in the crash, while 74 people survived — many seriously injured. The National Transportation Safety Board (NTSB) determined that the probable cause of the accident was the failure of the flight crew to manage the airplane's fuel load. The airplane ran out of fuel before it could land, and the NTSB determined that the crew did not communicate an emergency fuel situation to air traffic control before the airplane ran out of fuel.

The NTSB also stated that the lack of standardized, understandable terminology for pilots and controllers for minimum and emergency fuel states contributed to the accident. The crew apparently asked for a "priority" landing, which had different meanings to the Spanish-speaking pilots and the English-speaking controllers. A priority landing could be interpreted as an "emergency" to the Spanish-speaking pilots, but the controllers did not draw that conclusion.

The report also noted that there was a breakdown in communications among the crew members. The second officer, for example, never provided the captain with important fuel burn calculations, and was not asked to do so. The captain relied on the first officer for communications and clearance information, but did not cross-check that information. Training, specifically with regard to managing events during emergencies, could have also been a key factor in this accident. The NTSB noted, "The Safety Board believes that the AVA052 flight crew's ability to perform their duties on the accident flight could have been improved significantly if they had received CRM [Crew Resource Management] and LOFT [Line Oriented Flight Training] training as part of their initial and recurrent qualification for line operations."

Lessons Learned: Our complex technologies all involve some sort of human interaction to operate and maintain those systems. Therefore, communications is a critical part of those operations. Accidents can result because people may not be told what they need to know, may not understand critical information or may misunderstand what is being told to them. Therefore, system safety efforts must consider those human interactions in evaluating the potential for accidents. In addition, training is a critical aspect of safe operations. This training should include both nominal and emergency conditions, and should focus on the actions and roles of each team member during a crisis.

References:


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

by Mike Allocco

We have received feedback on the DRAFT Director's Mentoring, Research and Development Plan, and we plan on making minor revisions. Other recent projects include the research and review of safe design concepts for complex systems and “getting back to basics” in safe design. Consider the importance of developing good concept designs based on system safety axioms. A new white paper on this topic is under development. We are also in discussion with a major university to develop joint research and development projects.

Please contact me if you would like to participate in one of our projects, or if you would like to develop a mentoring agreement. We are available for mentoring and training support.

Regards,

Mike Allocco
Director, Mentoring, Research and Development
(571) 232-7960
HCRQ, Inc. specializes in system safety and software safety, providing both consulting services and courseware. HCRQ targets the aviation; defense; light, heavy and high-speed rail transportation; nuclear power; and medical device sectors.

HCRQ dates back to 1986. Its head office is located in Williamsburg, Virginia. The company entered the software safety arena when it analyzed the safety of the THERAC-25 cancer therapy machine following accidents involving patient injury and death due to severe radiation overdoses.

For the past 20 years, HCRQ has been teaching courses in system safety and software safety. In addition, during the last four years, the company has also taught Webinars on focused topics.

Contact information: info@hcrq.com (email), 757-564-7703 (office), 757-564-7704 (fax).

More information regarding HCRQ can be obtained at http://www.hcrq.com.
**Announcements**

**International Award**

The International System Safety Society (ISSS) International Award is presented to a person, group or organization for outstanding achievement or special service in the advancement of the system safety discipline in a country other than the United States of America.

Dr. Carl Sandom is the 2012 recipient of the International System Safety Award for his many accomplishments in the field of system safety engineering. He is a recognized global subject matter expert in the fields of system safety, software safety and human factors engineering, as well as a world-renowned instructor. Additionally, Dr. Sandom has been the chairman of the Institution of Engineering and Technology (IET) International System Safety Conference since its inception in 2006, actively promoting international cooperation between other safety organizations including, but not limited to, the IET, ISSS and the Australian Safety Critical Systems Association (aSCSAs). As IET System Safety and Cyber Security Chairperson, Dr. Sandom has promoted cooperation and collaboration among system safety professionals from many countries and continents.

Since Dr. Sandom was not present to receive the award at the 2012 ISSC, he was presented the award at the 2012 IET Conference by Warren Naylor, past president of the ISSS.
David V. MacCollum Scholarship

Southern Arizona Chapter of the American Society of Safety Engineers Names Visionary Scholarship after David V. MacCollum

The Southern Arizona Chapter of the American Society of Safety Engineers recently announced that it will honor David V. MacCollum with its new visionary scholarship.

David's many contributions to the safety profession span more than 60 years and include:

- Developing design criteria for roll-over protection structures for tractors and other construction equipment in the 1950s as part of the U.S. Army Corps of Engineers
- Serving as safety director for U.S. Army STRATCOM's worldwide communication command
- Serving on the U.S. Department of Labor's Construction Safety Advisory Committee
- Serving as principal reviewer of MIL-STD-882 during development of the landmark system safety standard
- Being elected national president of ASSE in 1975
- Receiving the highest ASSE honor by being named Fellow in 1999
- Authoring more than 400 published articles on safety
- Authoring three textbooks, including *Crane Hazards and Their Prevention*, *Construction Safety Planning* and *Construction Safety Engineering Principles*
- Frequently contributing to *Journal of System Safety* with his "Design-Based Safety" column
- Being named to the 2010 Construction Safety Group Hall of Fame

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

To make a donation to the David V. MacCollum Scholarship, visit [http://www.asse.org/foundation/contribute/donation.php](http://www.asse.org/foundation/contribute/donation.php), select "Other" and indicate the name of the fund in the text field.
Call for Papers 31st International System Safety Conference

by Steven Mattern, Society Fellow Member

August 11-16, 2013
Boston Marriott Copley Place
Boston, Massachusetts

Welcome to the 31st International System Safety Conference! The Conference theme for 2013, "Safety in the Long Run," will explore the long-term benefits of integrating safety into a system. This year's Conference is a joint venture with the Joint Weapons Safety Conference (JWSC). We hope you will share your knowledge, attend and learn. We would also invite you to provide a presentation on any safety process, method or technique that you believe contributes to the goals and objectives of system safety.

We want this Conference to bring practitioners and the foremost thinkers of the system safety discipline together for an exchange of ideas, knowledge and experience. Contributions will come from many different industries, including the automotive, aviation, defense, healthcare, oil and gas, power generation, rail, robotics and transportation industries.

The Conference is accepting four types of presentations:

Technical Papers: Two types of technical papers will be accepted: peer reviewed and Conference papers. Peer-reviewed papers will be reviewed by a committee composed of system safety experts — required by many in the world of academia. Both types of papers are generally compositions between six and 10 pages, written by one or more authors, dealing with a subject related to system safety. Technical papers are published in the Conference proceedings and are presented to Conference attendees.

Panels/roundtables: Discussion-oriented forums in which either a series of related presentations are delivered by a small number of experts (panelists), or a general topic is discussed informally by any or all participants. Discussions are led by a facilitator.

Tutorials: Educational presentations delivered by one or more instructors, intended to give practical information.

Workshops: Conference forums conducted in an interactive setting, intended to give participants problem-solving experience.

Key Submission Dates

March 29: Paper abstracts
April 5: Panel, roundtable, tutorial and workshop proposals
May 10: Draft papers
June 28: Final Paper
July 12: Draft presentations
July 26: Final presentations

Domains of Interest

Aviation
Explosives safety
Ground transportation
Hazard/risk management
Georgia Chapter

The Georgia Chapter contributed immensely to the success of the 30th International System Safety Conference (ISSC), held in Atlanta, Georgia August 6 - 10, 2012. The following Georgia Chapter members were on the Conference organizing and planning committee and worked tirelessly for almost two years in their respective areas: Barry Hendrix, chair; Terry Gooch, co-chair and sponsors/exhibitors; Terry Hall, conference operations chair; Dennis J. Beard, audio visuals/computers; Steve Lee, logistics/equipment; Colleen Sadeski, purchases, bags and gifts; Odell Ferrell, offsite events; Tom Lewis and James Harris, Security and Integrity; Dr. Coleen Thornton, menus; Bhavin Patel, flags; Clyde Watson, photography; Rich Campolmi, electrical equipment; and David Alberico, support. The Georgia Chapter would like to thank several others from different chapters who supported the Conference, especially Registration Chair Bob Cade, Webmaster and Publicity Chair Don Swallom and Technical Chair Dave West (and others in nearby Huntsville, such as John Livingston, Saralyn Dwyer and Heather French), as well as the Protocol Chair Lynce Pfledderer from North Texas, who interfaced with our four high-profile guest speakers. The Georgia Chapter has increased its membership substantially, and is highly engaged and committed to serving the ISSS in the future. We are in the process of welcoming back Georgia Chapter Secretary Don Morgan, who is in the last phase of completing Army helicopter training at Ft. Rucker, Alabama in the fall of 2012.

Saguaro Chapter

The Saguaro Chapter continues to hold phone meetings on a monthly basis. The Executive Council of the Chapter is planning numerous upcoming events. We expect to hold a meeting in the next few months at the Pima Air and Space Museum, to visit and tour Davis-Monthan Air Force Base, and to possibly hold a learning workshop in the Spring. If anyone has any interest in conducting a workshop in Arizona, contact Chapter President Amanda Boysun.

Singapore Chapter

The Singapore Chapter held a meeting on Sept. 28, 2012 at the Land Transport Authority (LTA) Campus. The Executive Council discussed and agreed on the creation of a Consultative Committee. This committee would be composed of individuals affiliated with the Singapore Chapter or past presidents of the Chapter. The main function of this committee will be to approve the nomination of the Executive Council and to provide advice on the use of Chapter funds.

The Singapore Chapter will celebrate its 10th anniversary in September 2013. Several activities will be held to celebrate this event.

Virtual Chapter

Nearly all of the members of the Chapter were able to leave their virtual worlds and attend the ISSC in Atlanta. Given this face-to-face opportunity, the Virtual Chapter held its August meeting during an evening session. There were 10 members and 27 associates in attendance, making the meeting our largest of the year. Steven Mattern chaired the meeting and presented the recommended goals and objectives for the new Society year.
In addition, the Virtual Chapter gave those in attendance the rationale behind membership in a "virtual" context. The Chapter affords Society members who are not normally active in either chapter or Society functions because of geographical (or other) constraints, the opportunity to participate in the virtual space. The Virtual Chapter continues to gain membership and has become a dynamic and functioning chapter within the Society.

The Virtual Chapter is also growing its membership communication capabilities. Chapter Secretary Matt Johnson continues to work to establish a Virtual Chapter Website, as well as a document and information repository on a Google site. While both sites are a work in progress, they are a great help to members in remaining current in Chapter activities.

Chapter officer elections will be held in June 2013. Officer nominations will begin in April. Questions regarding the Virtual Chapter should be sent to Steven Mattern at smattern@bastiontechnologies.com.

---

**Washington, DC (WDC) Chapter**

The WDC Chapter would like to welcome home Michael Demmick from his tour in Afghanistan working in the field of system safety. We wish safe travels to his successor, Peggy Rogers.

The WDC Chapter would like to thank Dev Raheja, ISSS Fellow Member, for his presentation, "What Every System Safety Engineer Must Know About Design for Reliability" at the WDC Chapter meeting held on September 12, 2012. The WDC Chapter truly appreciates his continued support.

Future events include the annual Christmas scholarship fundraiser, the WDC Wounded Warrior Golf Tournament and the WDC American Heart Association 5k Run.

As always, the WDC Chapter welcomes all ISSS members to its meetings and functions. Those who would like to be on the Chapter distribution list should forward their email address to Amber Schauf, Chapter president, at amber.schauf@urs.com. Note: To participate in Webcasting events, you must be a U.S. citizen.
Vol. 48, No. 6 • Nov-Dec 2012

Mark Your Calendar

21st Safety-Critical Systems Symposium
February 5-7, 2013
Bristol Marriott Royal Hotel
Bristol, U.K.
http://www.safety-club.org.uk/e210

2013 Symposium on Human Factors and Ergonomics in Health Care
March 11-13, 2013
Baltimore Marriott Waterfront Hotel
Baltimore, Maryland
https://www.hfes.org/Web/HFESMeetings/2013healthcaresymposium.html

2013 Business Aviation Safety Seminar (BASS)
(previously known as the Corporate Aviation Safety Seminar — CASS)
April 10-11, 2013
Fairmont Queen Elizabeth Hotel
Montreal, Ontario, Canada

31st International System Safety Conference (ISSC)
August 12-16, 2013
Boston Marriott Copley Place
Boston, Massachusetts
http://issc2013.system-safety.org
In his "TBD" article in the May/June 2012 edition of JSS, Charles Hoes raised a few professional questions of introspective nature that indirectly invited a forum for discussion. With this understanding in mind, I am writing this letter to provide an opinion to some of his posed questions.

There is a subtle difference between "competency" and "qualification." Competence means "the ability to do something successfully or efficiently," which implies accumulated knowledge. Qualification means "pass of an examination or an official completion of a course, especially one conferring status as a recognized practitioner of a profession or activity." In the absence of an accredited organization that could administer an examination to qualify a safety professional, we are left with an assessment of "competency."

As an example of such an assessment, the article mentions NASA's view on system safety competencies. I believe that the five categories identified in the NASA chart are correct. They mirror the development lifecycle of a safe product. Here is the reasoning:

- **System Safety Analytical Methods.** Safety must be embedded in the design and safety must be predictable; hence, the need for analytical methods. Since safety is often the result of vertical and horizontal interactions within a system, the safety is designed and analyzed primarily from a system perspective.
- **Mathematical Skills.** These skills are required to be able to describe a system. System engineering and applied math have had a long history of cross-fertilization. A system that has a validated mathematical model is likely to have most of its safety issues resolved at the design phase. It is noted that as systems become more complex, a validated system model is becoming the exception rather than the norm.
- **System Safety in Operational Management.** This refers to contributions made by safety practitioners that test the system in the field. This is a safety "hands on" field of knowledge that encompasses operations.
- **System Safety in Acquisition.** Since this view is coming from NASA, which is known to integrate many smaller subsystems, it is important that when a specification is issued, the safety requirements are specified at the acquisition level.
- **System Safety Rationale.** The rationale must be available during the integration of a complex system to ensure proper system validation.

Thus, I believe that the NASA categorization is the most complete one. When applied to engineering domains other than NASA, these categories should be tailored as applicable. As far as I know, we do not have in safety engineering a situation of "one size fits all."

The work done by the International System Safety Society's "Competency Committee" is valuable. It shows the complexity of the subject and the difficulty of defining a "system safety competencies chart." I notice that if safety management is left to specific industries and associated standards, education and training is left to universities — with the ISSS potentially providing curricula guidance — and certification is left to accredited organizations, then ISSS could be in a better position to define safety engineering as a profession in the realm of safe product development. This appears to be a goal that could lead to practical classifications of competencies.

The paper goes on to describe with professional passion "… one of the most important areas of (safety) competency is having a solid technical and scientific background concerning how things work." Without engaging in the semantics of "solid technical and scientific background," I would like to point out that what glues together the knowledge of "how things work" is system engineering. This aspect is essential, but it is not mentioned at all.

The key background question that this paper addresses is: "What is it that we (safety engineers) do that is different from those things done by other members of a project team?" I would like to offer a personal opinion. I view system safety as the pinnacle of system engineering. System
engineering knowledge is used to design systems and their control algorithms. System safety takes an already-designed system and analyzes it to ensure that any failure will bring the system to a safe state. Before one can be a system safety engineer, one should be a good system designer. Safety engineering qualifies a system through analysis of a design as safe or not. Safety engineering field practitioners qualify an implemented system as safe to commence operation.

The paper goes on to express dissatisfaction with companies that justify a lack of safety engineers on a team by claiming that the company’s designers are safety conscious. Usually, the missing link is the fact that safety is not applied in a systematic way in such companies. Hence, each designer will apply safety based on his or her personal interpretation of the applicable regulation. This creates conditions for hazardous situations to remain unidentified at the design stage.

As a corollary to the key background question, the paper asks rhetorically another good question: “Do we (safety engineers) not bring anything special or important to the team?” In my view, the answer is a definite “Yes.” However, I believe that the key to respond to the posed questions within the ISSS framework is to discuss “system safety” rather than “safety professionals.” The basic skill required in safety is systems engineering that can be clearly defined. System safety in a given industry is the outcome of the applicable legislation or standards requirements, combined with the safety policy of the industry (or company). In my view, it is not possible to define an all-encompassing “need” for safety. It is industry-specific.

Ady Solomon, Ph.D., P. Eng.
Toronto, Ontario, Canada
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. 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.

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 printed 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 © 2012 by the System Safety Society. All rights reserved. The double-sigma logo is a registered service mark of the System Safety Society. Journal of System Safety and the System Safety Society name are registered service marks of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.

(ISSN-0743-8826)
Contact Us

Puzzle

520-419-6918
jean_sauerman@raytheon.com

Warren Naylor, Past President
Northrop Grumman Electronic Systems
410-765-6910
warren.naylor@ngc.com

Office Manager: Cathy Carter
systemsafety@system-safety.org
540-854-8630

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@sympatico.ca
619-837-4128

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.