In the Spotlight

Common Statements...Trouncing Safety

by Mike Allocco, Fellow

Pages 1 | 2 | 3 | 4 | 5

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 then 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

Pages 1 | 2 | 3 | 4 | 5

• "We assume that this hazard is mitigated."

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.

• "This hazard is not credible."

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?

• "The hardware, software or firmware caused the anomaly."

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.
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.

“We must meet 10 EE – X.”

An important safety axiom addresses the objective that accidents are preventable. In understanding potential accidents, system risks can then be estimated and consequently mitigated. By investigating and studying past accidents, knowledge can be acquired that may help predict future potential accidents (system risks). However, caution should be applied.

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.

“Monitor the system to assure this level of exposure.”

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.

“Automating the task will make it safer.”

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.

“Hazards are defined as this...not that.”

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.
In the Spotlight

Common Statements...Trouncing Safety
by Mike Allocco, Fellow

"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 than 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 dumbfounded, 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.
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.

• “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. The principles of risk may be applied to almost any safety analysis.

- "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. Curious 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 Model2. 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.

Common Statements...Trouncing Safety

by Mike Allocco, Fellow

"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


See the following references for further information on analyses methods and techniques: