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

by Mike Allocco, PE, CSP
Centreville, Virginia

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

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

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

System Risk Identification

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

Designing Hazard Controls Strategies

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

Hazard Control Concepts

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

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

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

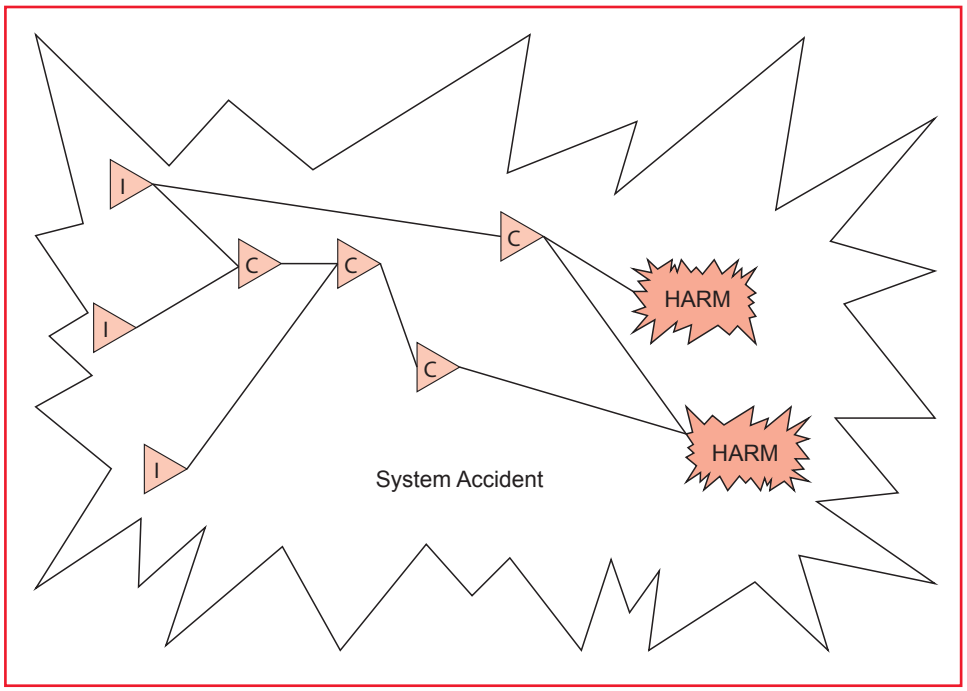

Figure 1 — An Example of a Potential System Accident.

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

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

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

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

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

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

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

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

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

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

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

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

Hazard Control Effectiveness Analysis

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

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

Barrier Analysis

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

Developing Hazard Control Requirements

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

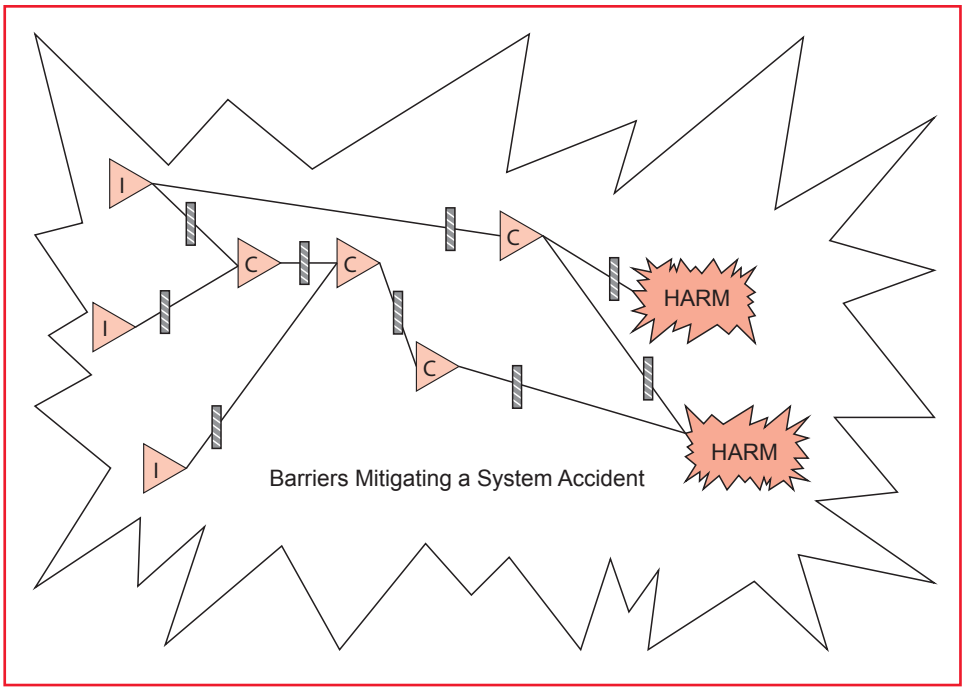

Figure 2 — An Example Depiction of Barriers Applied to Abate Adverse Progression.

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

Conclusion

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

About the Author

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