In the Spotlight

Considering System Risks
by Michael Allocco, PE, CSP
Washington, DC, USA

Introduction: A Review of System Accident Criteria

Understanding the concept of a system accident is important. System accidents may not be the result of a simple single failure, a behavior deviation or a single error, although simple adverse events still do occur. System accidents are the result of many initiators, contributors and combinations of errors, failures and malfunctions. It is not easy to see the system picture or to connect the dots while evaluating multi-contributors within adverse events, and identifying initial events and subsequent events to the final outcome. System risks can be unique, undetectable, not perceived, not apparent and unusual. A novice investigator, analyst or outside party can question the credibility of such diverse events.

When investigating system accidents, a typical question comes to mind: Why was the accident not anticipated? Thinking past simple linear logic is needed, such as a single failure and effect, or cause, single hazard and effect. System accidents can be predicted by inverting design logic, and by considering "what if" logic. Anything that can have an adverse effect on the system must be considered: a poor decision, poor assumption, error in design, calculation error, specification development problem, procedure development error, deviation, management oversight, poor resource planning, cultural influences, behavior, attitude, analysis error or poor judgment.

Designing Accidents

Determining potential event propagation through a complex system can involve extensive analysis. Specific system safety methods, such as software hazard analysis, human interface analysis, scenario analysis and modeling techniques, can be applied to determine system risks, which are the inappropriate interaction of software, human, machine and environment. All of these factors should be addressed when conducting hazard analysis and accident investigation. Consider that hazard analysis is the inverse of accident investigation. An analyst should be able to design prospective accidents, which are potential system accidents and system risks. In order to design a robust system, all the potential accidents associated with the system must be determined.

The objective is to understand the risks associated with the system. Risk knowledge can be gained reactively by conducting accident or incident investigations. It can also be gained proactively by conducting hazard recognition, by considering that hazards, or groups of hazards that define risk, can be identified by inspection, observation, safety review and hazard analysis. A so-called "safe system" is one in which all risks have been identified, eliminated or controlled to an acceptable level throughout the system's life-cycle.

To apply best practices in system safety, the analyst has to be able to identify all potential safety-related risks (system accidents). Thinking is not confined to the logic of a single hazard and linear cause and effect, but extends to multi-causal progression. The analysts should think in terms of being able to design potential accidents, which are unplanned dynamic adverse processes.
Considering System Risks

by Michael Allocco, PE, CSP
Washington, DC, USA

Pages 1 | 2 | 3 | 4 | 5

Hammer Model:

To further enhance and illustrate the discussion of the system accident, we will use the "Hammer Model." The hazard scenario concept first came to mind after study of Willie Hammer's books and material on system safety and in later discussions with Hammer. Hammer initially discussed concepts of initiators, contributors and primary hazards in the context of hazard analysis. Hammer noted that determining exactly which hazard is or has been directly responsible for an accident is not as simple as it seems.

To show the relationship between initiators, contributors and primary hazards, the "Hammer Model" is presented in Figure 1.

WHERE IS THE SINGLE HAZARD?

The model illustrates a simple accident: a compressed gas tank ruptures and causes harm. Note that there is no single hazard highlighted, but many hazards forming an adverse process: a scenario. Many things have to go wrong for the accident to occur. Hazard controls that can reduce the risk are also indicated. The specific system risk is only for this particular model: adverse sequence, the particular cutset. Each precise set of hazards will comprise a particular system risk. The terms "system risk," "system accident" or just "scenario" can be used the same way.

The system risk must be in a context, which is a specific system state or exposure. The system
state completes the picture of the potential accident by providing additional detail as to what is happening within the system during the adverse progression. Depending on the adverse progression and system state, worst-, mid-, and best-case situations are to be considered.

**Modeling Accidents:**

In analyzing complex potential accidents, or in reconstructing actual accidents, it is helpful to provide a model, graphic or picture of the accident. The presentation of a logical sequence is important in hazard analysis and accident investigation.

Models will vary in complexity, depending on the tools used, the type of model selected and the skills of the modeler. Some modeling techniques are extensive, laborious and time consuming. Decisions have to be made regarding the applicability of the modeling effort. People have spent extensive resources to construct fault trees on complex systems, and the so-called benefits gained did not justify these extensive efforts.

In applying formal hazard analysis and accident investigation, particular modeling techniques are used, such as cause-and-effect charts, flow charts, event trees, logic/fault trees, digraphs and fishbone diagrams. A model provides a means to show connectivity between initiators and contributors toward the final outcome.

**Comprehensive Picture of Risk**

In risk assessment, a model can indicate the possible events within an adverse flow. A more concise estimate of likelihood can be acquired. A so-called true picture of what can happen is presented, especially when conducting an evaluation of a very complex system.

More inclusive detail can also be indicated concerning risk management or risk control. The controls to mitigate identified hazards can also be provided within the model. The model then becomes a risk management tool by providing a more comprehensive picture of risk that considers all the controls within the adverse sequence. It can be shown that effective risk controls can act as barriers, buffers or safeguards in hindering or preventing adverse flow.
In the Spotlight: Considering System Risks

by Michael Allocco, PE, CSP
Washington, DC, USA

Models to Enhance Training and Contingency Planning

Models can also be applied in safety training and in formalizing contingency procedures. Models can be adapted to present simulations in order to train personnel in emergency protocols. With the advent of the laptop computer, complex models can be accessed for many safety-related purposes. A real-time depiction of the system can be provided, indicating system states. Failures or malfunctions can be indicated, and step-by-step troubleshooting procedures provided. Complex checklists can also be simplified and referenced when required. Additional detailed information can be accessed, including design details, schematics and calculations.

Such active real-time depictions must be evaluated from a human-factors perspective. These interactive models, if inappropriately designed, can introduce additional risks. Consider hazards such as undetected hazardous misleading information, the loss of information when required, errors made in designing procedures, missing information or masking important information, as well as overly complex information. Real-time safety-related information should be easy to interpret and access.

System Accidents

System accidents can be complex or simple. Initiators could be the result of latent hazards, such as software design errors, specification errors or oversights involving inappropriate assumptions. If hazard controls are not adequate, they become initiators or contributory hazards. If the control is not verified, it may not function when required. Validation considers the adequacy of the control. Is the control appropriately designed or applied?

Safety Integration:

With the understanding of potential system accidents, a form of safety integration is conducted. A system risk can be represented by a thread comprising an adverse dynamic process that can progress through complex systems, with various interactions. Within this depiction, mitigations are to be identified for all the identified hazards within the thread. Safety integration is accomplished by the grouping of the mitigations within the sequence — the potential system risk.

Accident Life-Cycle:

A system accident has a life-cycle associated with it. Accidents are initiated, they progress, and harm can result. In conducting scenario-driven system hazard analysis, the analyst should consider this concept. A system is in dynamic equilibrium when it is appropriately designed. The system is operating within specification and within design parameters; the system is operating within the envelope. When something goes wrong and an initiator occurs, however, the system is no longer in balance. The adverse sequence progresses, and the imbalance worsens until a point of no return, and harm results.

When conducting analysis, consider the accident life-cycle and how these adverse sequences...
With the application of hazard control, the adverse flow can be stopped. It is important that any imbalance is detected and the system is stabilized. Further, should the adverse sequence progress past the point of no return, the resultant harm may be minimized or decreased by the application of hazard control. Should harm result, the system should be brought back to a normal stable state. Consider that additional harm can occur during casualty or contingency. During hazard control application, not only are all the initiators, contributors and primary hazards controlled or eliminated, but contingency, recovery, damage and loss control are also applied toward the system life-cycle.

Errors in Logic Development

As discussed, thinking in terms of a single hazard (or failure) and cause (or failure mode or functional failure) with linear logic may not be totally appropriate. The system safety analyst should think in terms of the dynamics that can occur associated with the potential accident. If failures occur, these failures may or may not be hazards — thinking in terms of reliability and system safety simultaneously is not a good idea.

In the U.S., these two disciplines have evolved with different objectives. Failures are hazards when they are unsafe conditions within the potential accident. Confining the thought process is also not good when scenarios are being developed. A classic consideration is to think in terms of system functions, and that a functional analysis is required prior to any initial hazard analysis. An assumption is made that, in order to do hazard analysis, functions have to fail to identify hazards. Analysts should avoid a single mindset. Accidents could still occur during so-called normal functions. Functions can be inappropriately defined, or incompletely defined. To avoid single approaches, develop potential system accidents from different points of view. For example, consider abnormal energy interaction, oversight, omission, error, anomaly, malfunction and any deviation associated with the system under study. Develop the adverse logic throughout the accident life-cycle.
Determining Hazards

Most accidents are the result of human error, and it could be argued that many unsafe conditions associated with a design are the result of human error, oversight, omission or poor assumption. Keeping this human interface in mind, to determine hazards, a separation designation is required between the physical condition and an apparent human error. This being the case, a criterion was needed. A line of logic was defined which provides separation between physical unsafe conditions and non-physical unsafe human acts. The line was drawn where the human assumes control, assumes interaction or interfaces with the system — when the human is directly in the loop, such as a pilot manually landing an aircraft. Since the human is directly in the loop, if the human deviates, there can be an accident as a direct result, such as a controlled flight into terrain. Considering this separation, within the hazard analysis process, initial and contributory hazards are identified as unsafe acts or unsafe conditions. The determination of unsafe acts is the result of human factor analysis, and the determination of unsafe conditions is the result of abnormal energy analysis, for example. Because of the designation between unsafe acts and unsafe conditions, multi-linear analysis can be applied to assess and address the possibility of combinations of initiating and contributory events, both unsafe acts and/or unsafe conditions, that is part of the accident scenario.

Unsafe conditions consider any physical deviation, which is the result of uncontrolled energy forms. Singles bit upsets, bit flip, electromagnetic environmental effect, sneak path and wear are all considered hazards associated with unsafe conditions.

Integrating Concepts and Conducting Hazard Analysis

This scenario-driven process involves the identification of initiator, contributory, primary hazards and scenario themes. A preliminary hazard list is developed by formal or informal methods. The analyst studies concepts, designs or supportive analysis, such as Failure Modes and Effects Analysis (FMEA) or Fault Hazard Analysis (FHA). Hazards are not listed in any particular order or type. When a large list is developed, then it is possible to start constructing scenarios. Initially, it is best to start with developing scenario themes. The analyst lists the potential accidents that are possible. The next step is to equate the initiators to the scenario theme. Once this has been done, then contributory and primary hazards are also associated. To compile the analysis scenarios, worksheets are developed and used.

A scenario theme is a short, concise statement describing the potential accident. Consider safety problem statements that may include main initiators, contributors and outcome — the primary hazard.

Deductive and Inductive Approaches to Scenario Development

Depending on training, background and style of thinking, an analyst may approach scenario development in three ways: deductively, inductively or from the middle of the model or sequence.

Typically, a Fault Tree Analysis is considered a deductive top-down approach, where a scenario theme is considered the top event. The analyst starts the process with the theme and then conducts an investigation to determine what the contributors and initiators are that will support this scenario logic.

Some system safety engineers may approach scenario development inductively from the bottom
up. This is a more conventional approach. Conducting a Fault Hazard Analysis or Failure Modes and Effects Analysis can provide failure logic that includes initiators and contributors — the unsafe conditions.

After thinking in terms of accident scenarios, it is quite possible to construct logic starting from mid-level contributors and develop sequential logic in both directions toward the top event, scenario theme or the initiators.

**The Potential Accident**

Consider a simplified scenario sequence of a spacecraft colliding with a space station due to what is called “hazardous misleading information” being displayed during a manual procedure. The event sequence considers an initial failure, malfunction or error in a particular subsystem (named “Alpha”) that may be providing safety-critical information to a display. A pilot is relying on the display for information concerning the location, direction and speed of spacecraft, to enable manual control. Further, consider that we are developing a subsystem that provides all safety-critical information to the pilot's display. As a result of an initial failure, malfunction or error within the design, safety-critical information is inadvertently altered and hazardous misleading information displayed. In order to conduct an appropriate analysis of the particular subsystem, the analyst must fully understand the total potential system accident. All the dots must be connected. In constructing scenarios associated with the subsystem “Alpha,” initiators that can inadvertently alter information are considered. The analyst would “break” Alpha and evaluate the downstream effects. Initiators could be software malfunctions, design errors or anomalies that can affect the firmware or hardware. Data can be slightly altered, or numerical information can be changed.

![Figure 2 — Breaks in the Sequence are Hazards.](Click to enlarge)

Note that in Figure 2, there are breaks in the system that are considered hazards, and there is a specific progression, which forms the potential system accident. Potential accidents must conform to physics and the natural order or progression provided by the system, process or procedure analyzed.
In the Spotlight

Considering System Risks
by Michael Allocco, PE, CSP
Washington, DC, USA

Developing Scenarios and Risk Mitigation

Why develop an extensive list of scenarios? Each scenario will present a different system risk. Consider that likelihood and outcome will change; depending on the adverse sequence, some initiators and contributors may be more likely than others. Further, by developing additional scenarios, the effectiveness of mitigation can also be assessed. Some hazard controls may be more effective than others. In addition, consider that there is no automatic one-to-one relationship between a particular hazard and a hazard control. Depending on the scenario, it may take many controls to mitigate a particular hazard, or it can take one control to mitigate many hazards. Some controls may be effective as generic requirements. On the other hand, other controls may be very specific, such as a particular engineering or design control.

When addressing scenarios and adverse sequences, a more detailed mitigation picture can be seen. There is a hierarchy of hazard control to consider. Hazard controls can act as barriers within the sequence. Controls at a system level may mitigate many lower-level hazards within subsystems or components. For example, an automated safety monitor may be designed to conduct real-time, built-in-testing (BIT) to detect, isolate and correct failures within the system.

In considering scenarios and adverse sequences, it becomes apparent that some controls may be redundant, which adds to the hazard control effectiveness. The reliability and availability requirements, along with the requirements for an automated safety monitor, all provide mitigation against failures, which present hazards. There are also redundant controls against human error, such as quality control, supervision, training, formal methods and behavioral approaches.

Conclusion

Hammer indicated that determining exactly which hazard is or has been directly responsible for an accident is not quite as simple as it seems. Consequently, Hammer introduced the concepts of initiating, contributory and primary hazards — hazards within an adverse event sequence forming an accident or comprising a scenario. Further consider multi-event logic addressed within many industries, where hazards are considered unsafe acts or unsafe conditions that have the potential for harm. Initiating and contributory hazards may be equated to causes.

This paper has addressed the application of Hammer’s concepts of hazards in context with system risks and conducting scenario-driven hazard analyses. Consideration should be given to the concepts discussed.

The opinions expressed within this paper are strictly those of the author.

References

About the Author

Mike Allocco, PE, CSP, has been employed in safety management, system safety and safety engineering since 1976. He has conducted hazard analysis and risk assessments of nuclear and conventional weapon systems, the International Space Station, various aircrafts, aircraft ground
systems, medical devices, railroad systems, tunnel boring machines, complex processes and facilities. Allocco is coauthor (with Dev Raheja) of *Assurance Technologies Principles and Practices: A Product, Process, and System Safety Perspective, Second Edition*. He has conducted system safety engineering on diverse complex systems for the general industry, DOT, DoD, DOE and NASA. He is a Fellow and a former Executive Vice President of the System Safety Society. He is currently employed by the FAA.
WHERE IS THE SINGLE HAZARD?

Initiating Hazard

Contributory Hazards

Operating Pressure

Reduce pressure as tank ages

Catastrophic Events (Primary Hazards)

Equipment Damaged

Locate tank away from equipment susceptible to damage

Moisture → Corrosion → Weakened Metal → Tank Rupture → Fragments Projected → Personnel Injured

Use desiccant to keep moisture out of tank.

Use stainless steel or coat or plate carbon steel to prevent contact with moisture.

Overdesign metal thickness so corrosion will not reduce strength to failure point during foreseeable lifetime.

Use burst diaphragm to rupture before tank does, preventing more extensive damage and fragmentation.

Provide mesh screen to contain possible fragments.

Keep personnel from vicinity of tank while it is pressurized.
Breaks

What can break in the system?

Breaks

What can cause break in the system?

Breaks

What has to occur next in the sequence leading to the harm?

What are the other events or situations just before harm occurs?

What can happen next in the accident sequence?

Harm/ Damage/ Injury