Chapter 7:
Integrated System Hazard Analysis

7.0 Integrated System Hazard Analysis

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures, based on the system safety Order of Precedence (See Table 3.2-1 in Chapter 3.) Hazard analysis is the process of examining a system throughout its life cycle to identify inherent safety related risks.

7.1 Integrated Approach

An integrated approach is not simple, i.e., one does not simply combine many different techniques or methods in a single report and expect a logical evaluation of system risks and hazards. The logical combining of hazard analyses is called Integrated System Hazard Analysis. To accomplish integrated system hazard analysis many related concepts about system risks should be understood. These are discussed below.

In capsulated form, to accomplish Integrated System Hazard Analysis, system risks are identified as potential system accident scenarios and the associated contributory hazards. Controls are then designed to eliminate or control the risks to an acceptable level. The ISSWG may conduct this activity during safety reviews and Integrated Risk/Hazard Tracking and Risk Resolution.

7.1.1 Analysis Concepts

A scenario becomes more credible or more appropriate as the hypothesized scenario is developed to reflect reality, for example, an actual similar accident. Consistency and coherence are important during the composition of a scenario. Scenario descriptions will vary from the general to the specific. Scenarios will tend to be more specific as detailed knowledge is acquired. The completeness of the analysis also relates to how scenarios are constructed and presented. Some specific examples of scenarios are discussed in the next section.

The analyst should be concerned with machine/environment interactions resulting from change/deviation stresses as they occur in time/space, physical harm to persons; functional damage and system degradation.

The interaction consideration evaluates the interrelations between the human (including procedures), the machine and the environment: the elements of a system. The human parameter relates to appropriate human factors engineering and associated elements: biomechanics, ergonomics, and human performance variables. The machine equates to the physical hardware, firmware, and software. The human and machine are within a specific environment. Adverse effects due to the environment are to be studied. One model used for this analysis has been described earlier as the 5M model. See Chapter 3 for further elaboration.

Specific integrated analyses are appropriate at a minimum to evaluate interactions:

- Human - Human Interface Analysis
- Machine - Abnormal Energy Exchange, Software Hazard Analysis, Fault Hazard Analysis
- Environment - Abnormal Energy Exchange, Fault Hazard Analysis

The interactions and interfaces between the human, machine and the environment are to be evaluated by application of the above techniques, also with the inclusion of Hazard Control Analysis; the possibility of insufficient control of the system is analyzed.

Adverse deviations will affect system safety. The purpose of analysis is to identify possible deviations that can contribute to scenarios. Deviations are malfunctions, degradation, errors, failures, faults, and system anomalies. They are unsafe conditions and/or acts with the potential for harm. These are termed *contributory hazards* in this System Safety Handbook.

7.1.2 Hazards Identification and Risk Assessment

Throughout this handbook, reference is made to *hazards* and their associated *risks*. Hazards are the potential for harm. They are unsafe acts and/or unsafe conditions that can result in an accident. An accident is usually the result of many contributors (or causes) and these contributors are referred to as either initiating or contributory hazards. Depending on the context of the discussion, either hazards or their associated risks are referred to. Figures 7-1 through 7-4 provide examples of previous accident scenarios that have occurred. Note that many things had to go wrong for a particular accident to occur. Each of these accident scenarios has their associated risk. It should be noted that every contributory event has to be considered, as well as its event likelihood, when determining a specific risk. Consider that a risk is made up of a number of hazards and that each hazard has its own likelihood of occurrence. Further note that the potential worst case harm, which may be aircraft damage, injury or other property damage represents the consequence, or the severity of the accident scenario. Likelihood is determined based on an estimate of a potential accident occurring. That accident has a specific credible worst case severity. If the hypothesized accident's outcome changes, the scenario changes, and as a result, a different risk must be considered. The steps in a risk assessment are:

- Hypothesize the scenario.
- Identify the associated hazards.
- Estimate the credible worst case harm that can occur.
- Estimate the likelihood of the hypothesized scenario occurring at the level of harm (severity).

Figure 7-1 shows the sequence of events that could cause an accident from a fuel tank rupture on board an aircraft. There are a number of contributory hazards associated with this event: fuel vapor present, ignition spark, ignition and tank overpressurization, tank rupture and fragments projected. The contributors associated with this potential accident involve exposed conductors within the fuel tank due to wire insulation degradation, and the adequate ignition energy present. The outcome could be any combination of aircraft damage, and/ or injury, and/or property damage.

Figure 7-2 shows the sequence of events that could cause an accident due to a hydraulic brake failure and aircraft runway run-off. Note in this case there are again, many contributors to this event: failure of the primary hydraulic brake system, inappropriate attempt to activate emergency brake system, loss of aircraft braking capability, aircraft runs off end of runway and contacts obstructions. The outcomes could also vary from aircraft damage to injury and/or property damage. Note that the initiating events relate to the failure of the primary hydraulic brake system. This failure in and of itself is the outcome of many other contributors that caused the hydraulic brake system to fail. Further note that the improper operation of the emergency brake system is also considered an initiating event.

Figure 7-3 indicates the sequences of events that could cause an accident due to an unsecured cabin door and the aircraft captain suffers Hypoxia. Note that this event is not necessarily due to a particular failure.

As previously indicated, there are many contributors: the aircraft is airborne without proper cabin pressure indication, and the captain enters the unpressurized cabin without the proper personal protective equipment. The initiators in this scenario involve the cabin door not being properly secured, inadequate preflight checks, and less than adequate indication of cabin pressure loss in the cockpit. The outcome of this accident is that the captain suffers Hypoxia. Note that if both crew members investigated the anomaly, it would be possible that both pilots could have experienced Hypoxia and loss of aircraft could have occurred.

The safeguards that would either eliminate the specific hazards or control the risk to an acceptable level have also been indicated in the figures. Keep in mind that if a safeguard does not function, that in itself is a hazard. In summary, it is not easy to identify the single hazard that is the most important within the scenario sequence. As discussed, the initiating hazards, the contributory hazards, and the primary hazard must all be considered in determining the risk. The analyst must understand the differences between hazards, the potential for harm and their associated risks. As stated, a risk is comprised of the hazards within the logical sequence. In some cases, analysts may interchange terminology and refer to a hazard as a risk, or vice versa. Caution must be exercised in the use of these terms. When conducting risk assessment, the analyst must consider all possible combinations of hazards that may constitute one particular risk, which is the severity and likelihood of a potential accident.

Figure 7-1: Engine Covers Scenario

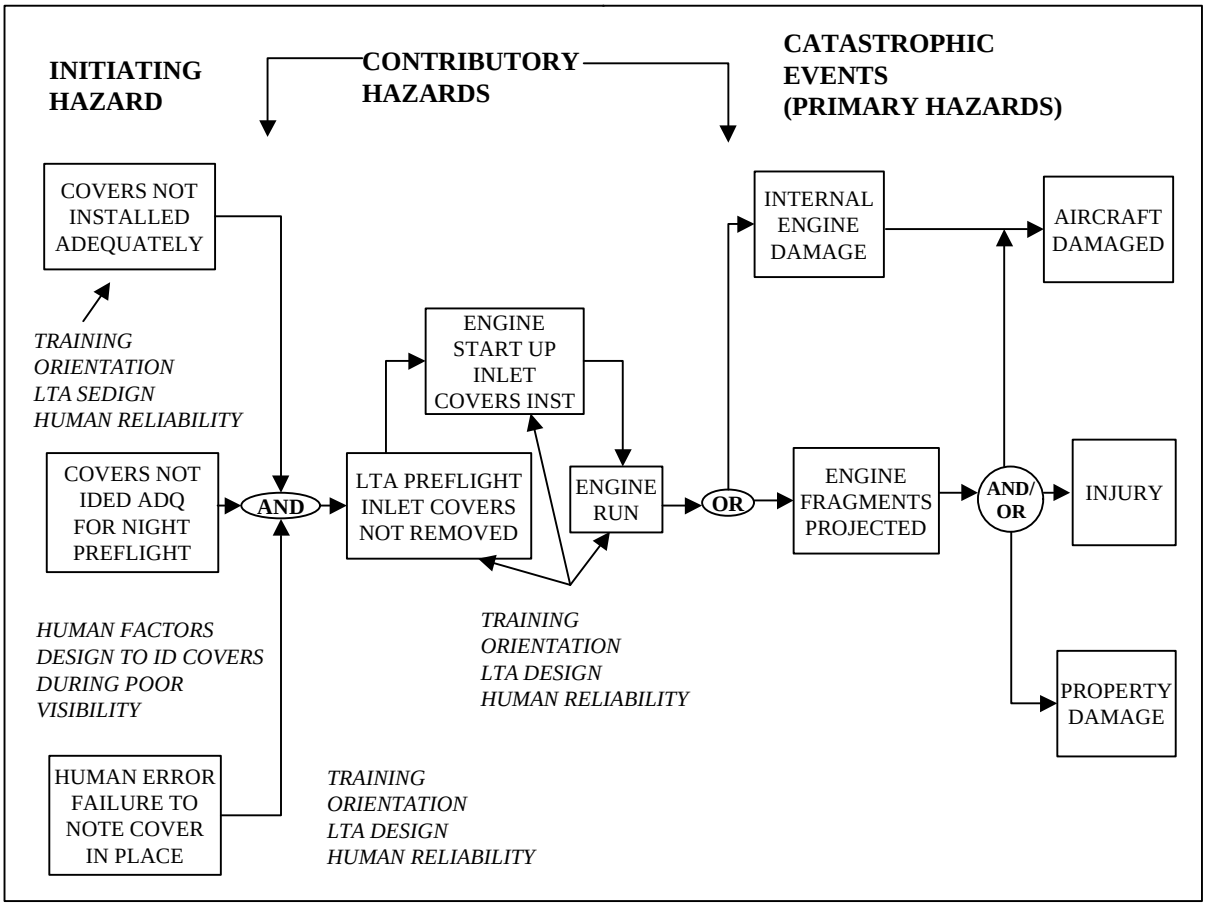


Figure 7-2: Fuel Tank Rupture Scenario

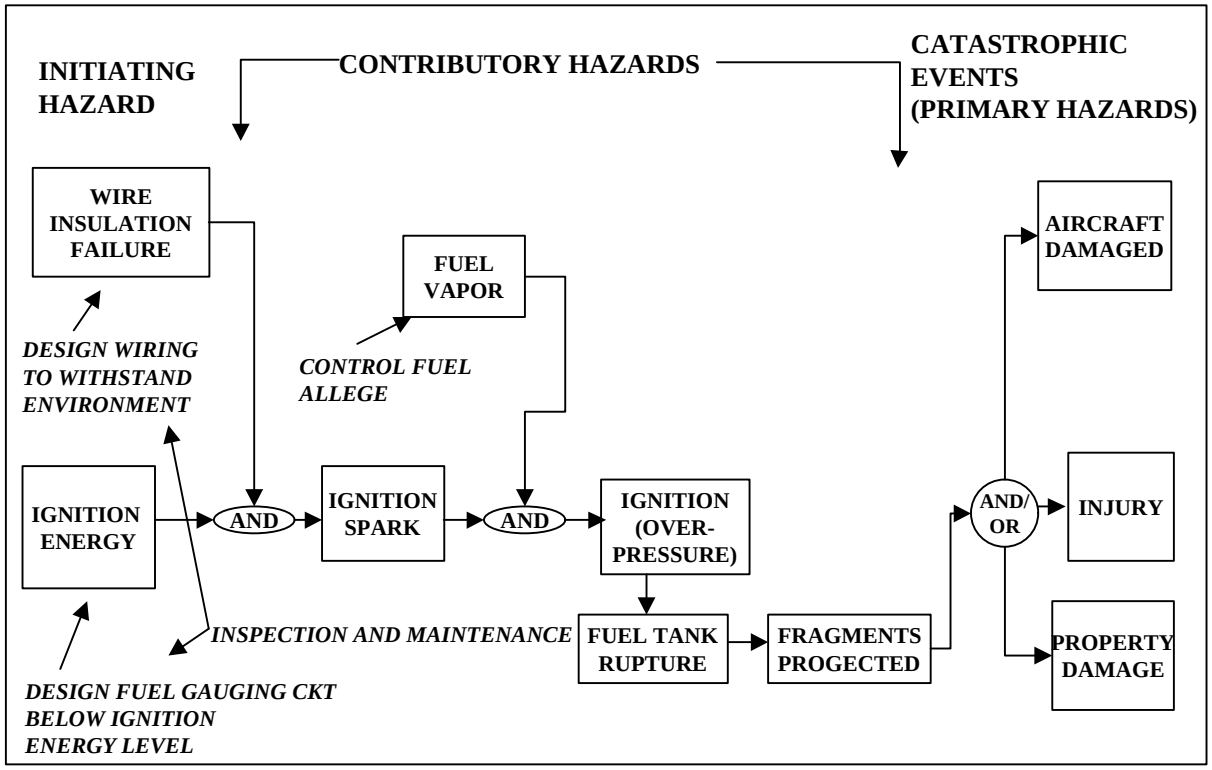


Figure 7-3: Hydraulic Brake Scenario

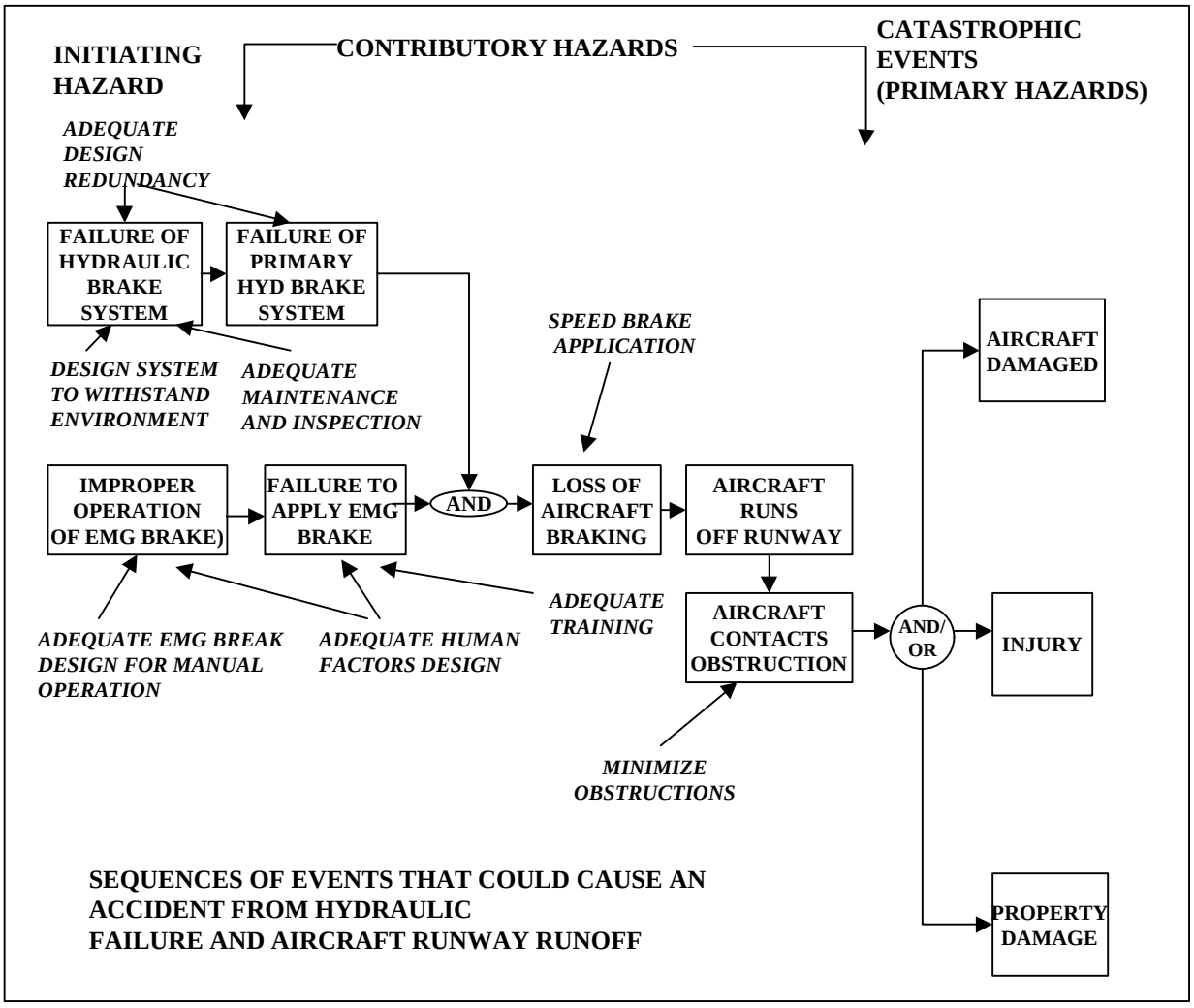
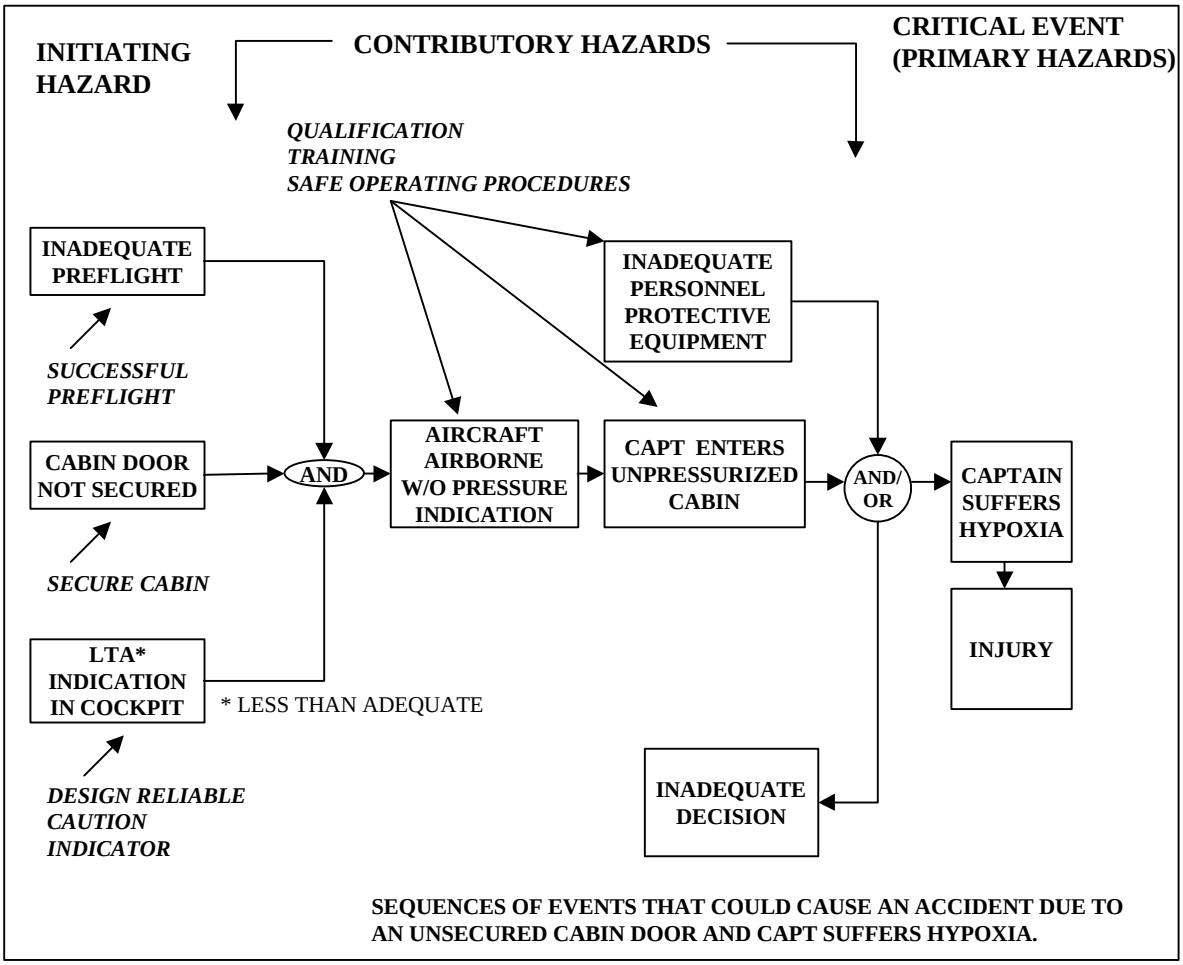


Figure 7-4: Unsecured Cabin Door Scenario



7.1.3 Common System Risks

At first exposure, to the lay person, there apparently is very little difference between the disciplines of reliability and system safety, or any other system engineering practice like quality assurance, maintainability, survivability, security, logistics, human factors, and systems management. They all use similar techniques and methods, such as Failure Modes and Effects Analysis and Fault Tree Analysis. However, from the system engineering specialist's viewpoint there are many different objectives to consider and these must be in concert with the overall system objective of designing a complex system with acceptable risks.

An important system objective should include technical risk management or operational risk management. Further consideration should be given to the identification of system risks and how system risks equate within specialty engineering. Risk is an expression of probable loss over a specific period of time or over a number of operational cycles. There are situations where reliability and system safety risks are in concert and in some other cases tradeoffs must be made.

A common consideration between reliability and system safety equates to the potential unreliability of the system and associated adverse events. Adverse events can be analogous to potential system accidents. Reliability is the probability that a system will perform its intended function satisfactorily for a prescribed time under stipulated environmental conditions. The system safety objective equates to "the optimum degree of safety…" and since nothing is perfectly safe the objective is to eliminate or control known system risk to an acceptable level.

When evaluating risk, contributory hazards are important. Contributory hazards are *unsafe acts* and *unsafe conditions* with the potential for harm. Unsafe acts are human errors that can occur at any time throughout the system life cycle. Human reliability addresses human error or human failure. Unsafe conditions can be failures, malfunctions, faults, and anomalies that are contributory hazards. An unreliable system is not automatically hazardous; systems can be designed to fail-safe. Procedures and administrative controls can be developed to accommodate human error or unreliable humans, to assure that harm will not result.

The model below (Figure 7-5) shows the relationship between contributory hazards and adverse events, which are potential accidents under study.

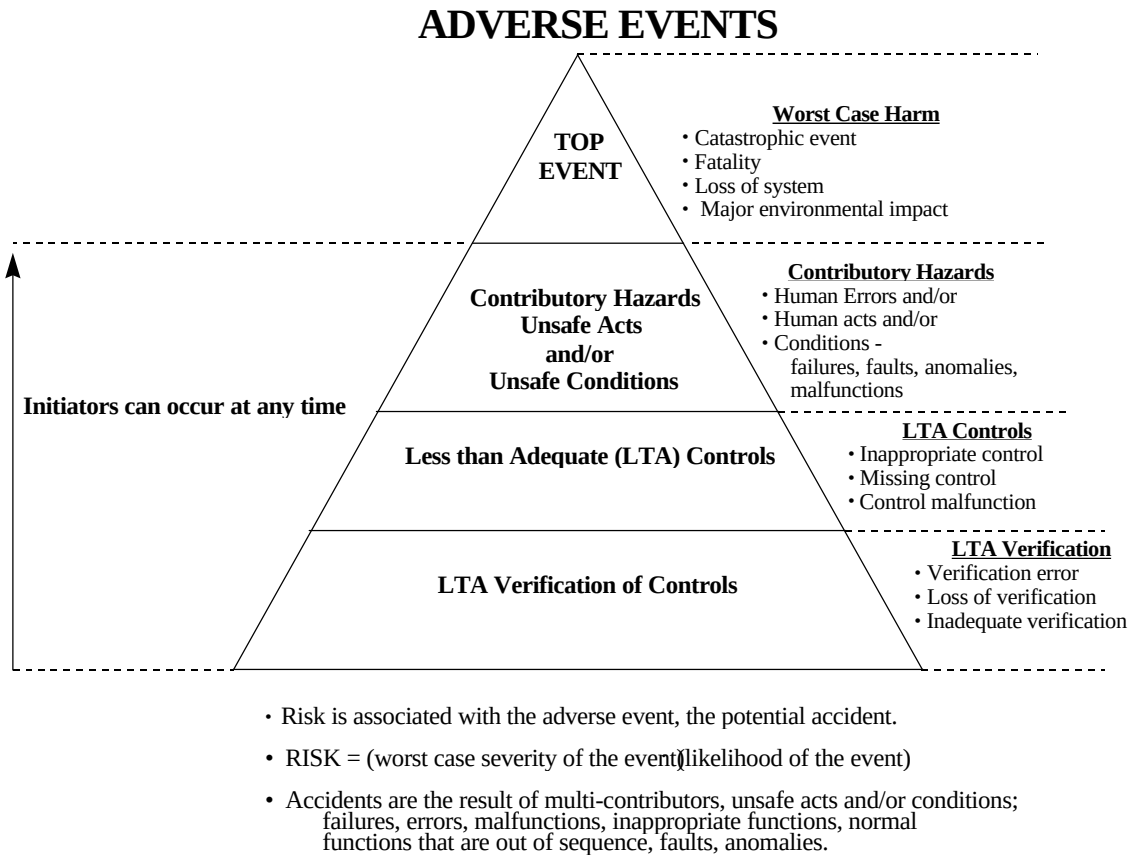


Figure 7-5: Relationship Between Contributory Hazards & Adverse Events

7.1.4 System Risks

Consider a system as a composite, at any level of complexity. The elements of this composite entity are used together in an intended environment to perform a specific objective. There can be risks associated with any system and complex technical systems are everywhere within today's modern industrial society. They are part of every day life, in transportation, medical science, utilities, general industry, military, and aerospace. These systems may have extensive human interaction, complicated machines, and environmental exposures. Humans have to monitor systems, pilot aircraft, operate complex devices, and conduct design, maintenance, assembly and installation efforts. The automation can be comprised of extensive hardware, software and firmware. There are monitors, instruments, and controls. Environmental considerations can be extreme, from harsh climates, outer space, and ambient radiation. If automation is not appropriately designed considering potential risks, system accidents can result.

7.1.5 System Accidents[i]

System accidents may not be the result of a simple single failure, or a deviation, or a single error. Although simple adverse events still do occur, system accidents are usually the result of many contributors, 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, identifying initial events, and subsequent events to the final outcome. System risks can be unique, undetectable, not perceived, not apparent, and very unusual.

Determining potential event propagation through a complex system can involve extensive analysis. Specific reliability and system safety methods such as software hazard analysis, failure modes and effects analysis, human interface analysis, scenario analysis, and modeling techniques can be applied to determine system risks, e.g., the inappropriate interaction of software, human (including procedures), machine, and environment.

7.1.6 System Risk Identification

The overall system objective should be to design a complex system with acceptable risks. Since reliability is the probability that a system will perform its intended function satisfactorily, this criteria should also address the safety-related risks that directly equate to failures or the unreliability of the system. This consideration includes hardware, firmware, software, humans, and environmental conditions.

Dr. Perrow in 1984 further indicated and enhanced the multi-linear logic discussion with the definition of a system accident: "system accidents involve the unanticipated interaction of multiple failures."

From a system safety viewpoint, the problem of risk identification becomes even more complex, in that the dynamics of a potential system accident are also evaluated. When considering multi-event logic, determining quantitative probability of an event becomes extensive, laborious, and possibly inconclusive. The above model of the adverse event represents a convention (an estimation) of a potential system accident with the associated top event: the harm expected, contributory hazards, less than adequate controls, and possibly less than adequate verification. The particular potential accident has a specific initial risk and residual risk.

Since risk is an expression of probable loss over a specific period of time or over a number of operational cycles, risk is comprised of two major potential accident variables, loss and likelihood. The loss relates to harm, or severity of consequence. Likelihood is more of a qualitative estimate of loss. Quantitative likelihood estimates can be inappropriate since specific quantitative methods are questionable considering the lack of relative appropriate data. Statistics can be misunderstood or manipulated to provide erroneous

information. There are further contradictions, which add to complexity when multi-event logic is considered. This logic includes event flow, initiation, verification/control/hazard interaction, human response, and software error.

The overall intent of system safety is to prevent potential system accidents by the elimination of associated risk, or by controlling the risk to an acceptable level. The point is that reliance on probability as the total means of controlling risk can be inappropriate. Figures 7-1 through 7-3 provided examples of undesired events that require multiple conditions to exist simultaneously and in a specific sequence. Figure 7-6 summarizes multi-event logic.

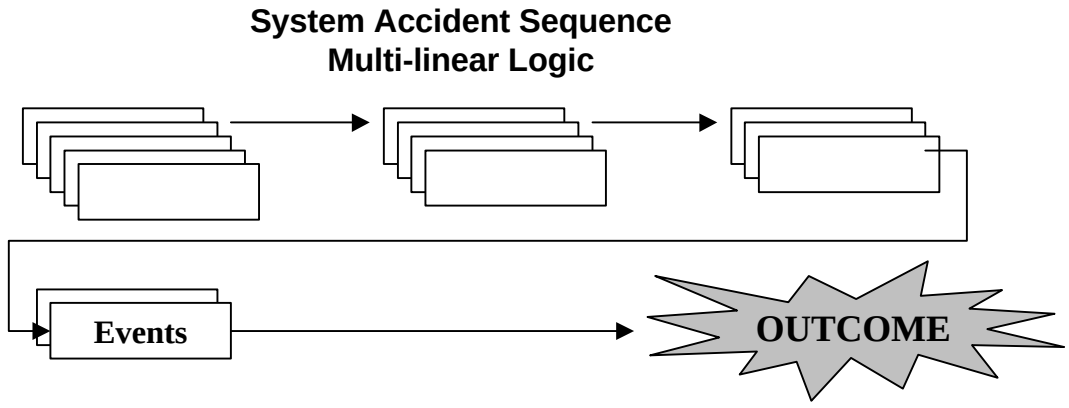


Figure 7-6: Multi-Event Logic

7.2 Risk Control

The concept of controlling risk is not new. Lowrance[1] in 1945 had discussed the topic. It has been stated that "a thing is safe if the risks are judged to be acceptable." The discussion recently has been expanded to the risk associated with potential system accidents: system risks. Since risk is an expression of probable loss over a specific period of time, two potential accident variables, loss and likelihood can be considered the parameters of control. To control risk either the potential loss (severity or consequence) or its likelihood is controlled. A reduction of severity or likelihood will reduce associated risk. Both variables can be reduced or either variable can be reduced, thereby resulting in a reduction of risk.

The model of an adverse event above is used to illustrate the concept of risk control. For example, consider a potential system accident where reliability and system safety design and administrative controls are applied to reduce system risk. There is a top event, contributory hazards, less than adequate controls, and less than adequate verification. The controls can reduce the severity and/or likelihood of the adverse event.

Consider the potential loss of a single engine aircraft due to engine failure. Simple linear logic would indicate that a failure of the aircraft's engine during flight would result in a forced landing possibly into unsuitable terrain. Further multi-event logic which can define a potential system accident would indicate additional complexities, e.g., loss of aircraft control due to inappropriate human reaction, deviation from emergency landing procedures, less than adequate altitude, and/or less than adequate glide ratio. The reliability related engineering controls in this situation would be appropriate to system safety and would

[1] Lowrance, William W., Of Acceptable Risk --- Science and the Determination of Safety, 1945, Copyright 1976 by William Kaufmann, Inc.

consider the overall reliability of the engine, fuel sub-systems, and the aerodynamics of the aircraft. The system safety related controls would further consider other contributory hazards such as inappropriate human reaction, and deviation from emergency procedures. The additional controls are administrative in nature and involve design of emergency procedures, training, human response, communication procedures, and recovery procedures.

In this example, the controls above would decrease the likelihood of the event and possibly the severity. The severity would decrease as a result of a successful emergency landing procedure, where the pilot walks away and there is minimal damage to the aircraft. The analyst must consider worst case credible scenarios as well as any other credible scenarios that could result in less harm.

This has been a review of a somewhat complex potential system accident in which the hardware, the human, and the environment were evaluated. There would be additional complexity if software were included in the example. The aircraft could have been equipped with a fly-by-wire flight control system, or an automated fuel system.

Software does not fail, but hardware and firmware can fail. Humans can make software-related errors. Design requirements can be inappropriate. Humans can make errors in coding. The complexity or extensive software design could add to the error potential. There could be other design anomalies, sneak paths, and inappropriate do-loops. The sources of software error can be extensive according to Raheja, "Studies show that about 60 percent of software errors are logic and design errors; the remainder are coding -and service-related errors." [2] There are specific software analysis and control methods that can be successfully applied to contributory hazards, which are related to software.

Again referring to the adverse event model above, note that software errors can result in unsafe conditions or they could contribute to unsafe acts. Software controls can be inappropriate. The verification of controls could be less than adequate.

7.2.1 Risk Control Tradeoffs

What appears to be a design enhancement from a reliability standpoint will not inherently improve system safety in all cases. In some cases risk can increase. In situations where such assumptions are made it may be concluded that safety will be improved by application of a reliability control, for example, redundancy may have been added within a design. The assumption may be that since it is a redundant system, it must be safe. Be wary of such assumptions. The following paragraphs present an argument that an apparent enhancement from a reliability view will not necessarily improve safety. Risk controls in the form of design and administrative enhancements are discussed along with associated tradeoffs, in support of this position.

7.2.2 Failure Elimination

A common misconception that has been known in the system safety community for many years was discussed by Hammer[3]. It is that by eliminating failures, a product will not be automatically safe. A product may have high reliability but it may be affected by a dangerous characteristic. A Final Report of the National Commission of Product Safety (June 1970) discussed numerous products that have been injurious because of such deficiencies.

[2] Raheja, Dev G., Assurance Technologies --- Principles and Practices, McGraw-Hill, 1991, page 269.
[3] Hammer, Willie, Handbook of System and Product Safety, Prentice - Hall, Inc., 1972 page 21.

Consider that deficiencies are contributory hazards, unsafe acts and/or conditions that can cause harm. Without appropriate hazard analysis how would it be possible to identify the contributors?

7.2.3 Conformance to Codes, Standards, and Requirements

Another misconception to be considered by a reliability engineer is that conformance to codes standards and requirements provides assurance of acceptable risk. As indicated, appropriate system hazard analysis is needed to identify system hazards, so that the associated risk can be eliminated or controlled to an acceptable level.

Codes, standards, and requirements may not be appropriate, or they may be inadequate for the particular design. Therefore, risk control may be inadequate. The documents may be the result of many efforts, which may or may not be appropriately related to system safety objectives. For example, activities of committees may result in consensus, but the assumptions may not address specific hazards. The extensive analysis that has been conducted in support of document development may not have considered the appropriate risks. Also, the document may be out dated by rapid technological advancement.

As pointed out in the Final Report of the National Commission on Product Safety, industrial standards are based on the desire to promote maximum acceptance within industry. To achieve this goal, the standards are frequently innocuous and ineffective.[4]

Good engineering practice is required in all design fields. Certain basic practices can be utilized, but a careful analysis must be conducted to ensure that the design is suitable for its intended use.

7.2.4 Independent Redundancy and Monitoring

Consider another inappropriate assumption; that the system is redundant and monitored, so it must be safe. Unfortunately this may not be true. Proving that each redundant subsystem, or string, or leg is truly redundant may not be totally possible. Proving that the system will work as intended is also a concern.

Take for example a complex microprocessor and its associated software. These complex systems are never perfect according to Jones:

> (response to all inputs not fully characterized), there may be remnant faults in hardware/software and the system will become unpredictable in its response when exposed to abnormal (unscheduled) conditions e.g. excess thermal, mechanical, chemical, radiation environments.[5]

This being the case, what can the system safety engineer do to assure acceptable risk? How does one prove independence and appropriate monitoring?

Defining acceptable risk is dependent on the specific entity under analysis, i.e., the project, process, procedure, subsystem, or system. Judgment has to be made to determine what can be tolerated should a loss occur. What is an acceptable catastrophic event likelihood? Is a single fatality acceptable, if the event can occur once in a million chances? This risk assessment activity can be conducted during a system safety working group effort within a safety review process. The point to be made here is that a simplistic assumption, which is based upon a single hazard or risk control (redundancy and monitoring), may be over simplistic.

---

[4] Ibid. Hammer page26.

[5] Jones, Malcolm, The Role of Microelectronics and Software in a Very High Consequence System, Proceedings of the 15th International System Safety Conference - 1997, page 336.

Proving true redundancy is not cut-and-dried in complex systems. It may be possible to design a hardware subsystem and show redundancy, i.e. redundant flight control cables, redundant hydraulic lines, or redundant piping. When there are complex load paths, complex microprocessors, and software, true independence can be questioned. The load paths, microprocessors, and software must also be independent. Ideally, different independent designs should be developed for each redundant leg. However, even independent designs produced by different manufacturers may share a common failure mode if the requirements given the software programmers is wrong.

The concepts of redundancy management should be appropriately applied.[6] Separate microprocessors and software should be independently developed. Single point failures should be eliminated if there are common connections between redundant lags. The switch over control to accommodate redundancy transfer should also be redundant. System safety would be concerned with the potential loss of transfer capability due to a single common event.

Common events can eliminate redundancy. The use of similar hardware and software presents additional risks, which can result in loss of redundancy. A less than adequate process, material selection, common error in assembly, material degradation, quality control, inappropriate stress testing, or calculation assumption; all can present latent risks which can result in common events. A general rule in system safety states that the system is not redundant unless the state of the backup leg is known and the transfer is truly independent.

Physical location is another important element when evaluating independence and redundancy. Appropriate techniques of separation, protection, and isolation are important. In conducting Common Cause Analysis, a technique described in the System Safety Analysis Handbook,[7] as well as this handbook, not only is the failure state evaluated, but possible common contributory events are also part of the equation. The analyst identifies the accident sequence in which common contributory events are possible due to physical relationships.

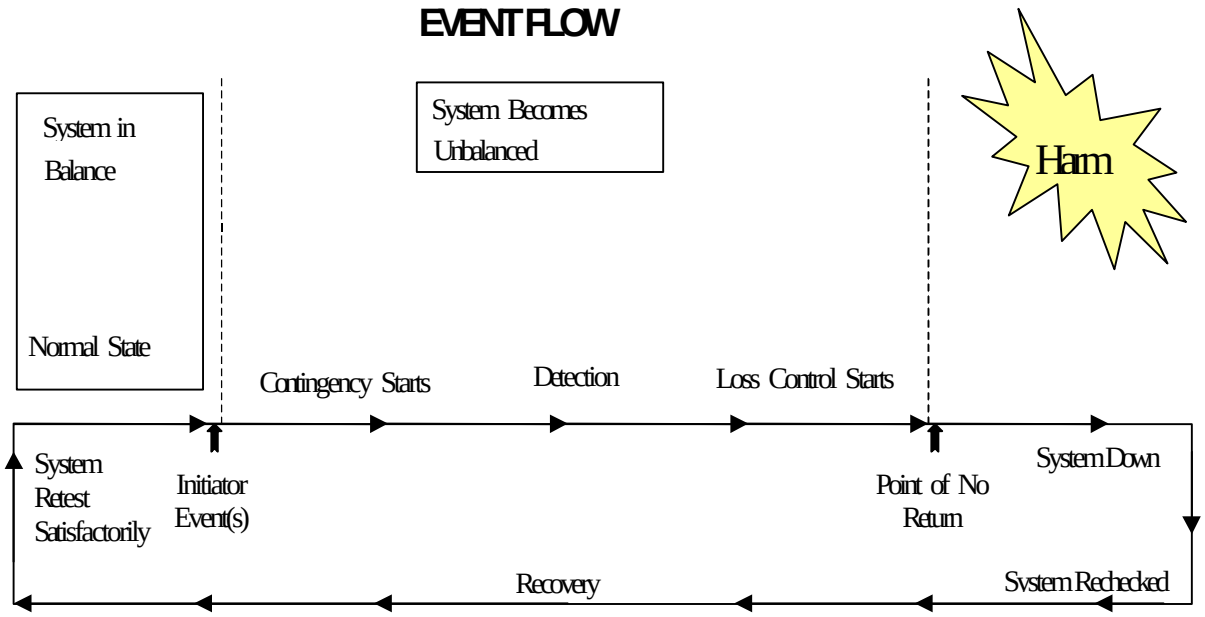
Other analysis techniques also address location relationships, for example, vicinity analysis, and zonal analysis. One must determine the possible outcome should a common event occur that can affect all legs of redundancy simultaneously, e.g., a major fire within a particular fire division, an earthquake causing common damage, fuel leakage in an equipment bay of an aircraft, or an aircraft strike into a hazardous location.

Keep in mind that the designers of the *Titanic* considered compartmentalization for watertight construction. However, they failed to consider latent common design flaws, such as defects in the steel plating, the state of knowledge of the steel manufacturing process, or the affects of cold water on steel.

Another misconception relates to monitoring; i.e., that the system is safe because it is monitored. Safety monitoring should be designed appropriately to assure that there is confidence in the knowledge of the System State. The system is said to be *balanced* when it is functioning within appropriate design parameters. Should the system become unbalanced, the condition must be recognized in order to stabilize the system before the point of no return. This concept is illustrated in Figure 7-5. The "point of no return" is the point beyond which damage or an accident may occur.

[6] Redundancy Management requirements were developed for initial Space Station designs.
[7] System Safety Society, System Safety Analysis Handbook, 2nd Edition, 1997. Pages 3-37 and 3-38.

Figure 7-7: Event Flow



Monitoring devices can be incorporated into the design to check that conditions do not reach dangerous levels (or imbalance) to ensure that no contingency exists or is imminent. Monitors[8] can be used to indicate:

- Whether or not a specific condition exists. If indication is erroneous, contributory hazards can result.
- Whether the system is ready for operation or is operating satisfactorily as programmed. An inappropriate ready indication or inappropriate satisfactory indication can be a problem from a safety point of view.
- If a required input has been provided. An erroneous input indication can cause errors and contributory hazards.
- Whether or not the output is being generated

7.2.5 Probability as a Risk Control

Probability is the expectancy that an event can take place a certain number of times in a specific number of trials. Probabilities provide the foundations for numerous disciplines, scientific methodologies, and risk evaluations. Probability is appropriate in reliability, statistical analysis, maintainability, and system effectiveness.

Over time, the need for numerical evaluations of safety has generated an increase in the use of probabilities for this purpose. In 1972, Hammer expressed concerns and objections about the use of quantitative

[8] Ibid. Hammer, page 262.

analysis to determine probability of an accident[9]. These concerns and objections are based on the following reasons:

- A probability, such as reliability, guarantees nothing. Actually, a probability indicates that a failure, error, or mishap is possible, even though it may occur rarely over a period of time or during a considerable number of operations. Unfortunately, a probability cannot indicate exactly when, during which operation, or to which person a mishap will occur. It may occur during the first, last, or any intermediate operation in a series. For example, a solid propellant rocket motor developed as the propulsion unit for a missile had an overall reliability indicating that two motors of every 100,000 fired would probably fail. The first one tested blew up.
- Probabilities are projections determined from statistics obtained from past experience. Although equipment to be used in actual operations may be exactly the same as the equipment for which the statistics were obtained, the conditions under which it will be operated may be different. In addition, variations in production, maintenance, handling, and similar processes generally preclude two or more pieces of equipment being exactly alike. There are numerous instances in which minor changes in methods to produce a component with the same or improved design characteristics as previous items have instead caused failures and accidents. If an accident has occurred, correction of the cause by change in the design, material, code, procedures, or production process may immediately nullify certain statistical data.
- Generalized probabilities do not serve well for specific, localized situations. In other situations, data may be valid but only in special circumstances. Statistics derived from military or commercial aviation sources may indicate that a specific number of aircraft accidents due to bird strikes take place every 100,000 or million flight hours. On a broad basis involving all aircraft flight time, the probability of a bird strike is comparatively low. However, at certain airports near coastal areas where birds abound, the probability of a bird-strike accident is much higher.
- Human error can have damaging effects even when equipment or system reliability has not been lessened. A common example is the loaded rifle. It is highly reliable, but people have been killed or wounded when cleaning or carrying them.
- Probabilities are usually predicated on an infinite or large number of trials. Probabilities, such as reliabilities for complex systems, are of necessity based upon very small samples, and therefore have relatively low confidence levels.

7.2.6 Human in the Loop[10]

Fortunately humans usually try to acclimate themselves to automation prior to its use. Depending on the complexity of the system acclimation will take resources, time, experience, training, and knowledge. Automation has become so complex that acclimation has become an “integration-by-committee” activity. Specialists are needed in operations, systems engineering, human factors, system design, training, maintainability, reliability, quality, automation, electronics, software, network communication, avionics, and hardware. Detailed instruction manuals, usually with cautions and warnings, in appropriate language, are required. Simulation training may also be required.

[9] Ibid. Hammer, page 91 and 92.
[10] Allocco, Michael, ***Automation, System Risks and System Accidents, 18th International System safety Society Conference***

The interaction of the human, and machine if inappropriate, can also introduce additional risks. The human can become overloaded and stressed due inappropriately displayed data, an inappropriate control input, or similar erroneous interface. The operator may not fully understand the automation, due to its complexity. It may not be possible to understand a particular system state. The human may not be able to determine if the system is operating properly, or if malfunctions have occurred.

Imagine relying on an automated system and due to malfunction or inappropriate function, artificial indications are displayed and the system is inappropriately communicating. In this case the human may react to an artificial situation. The condition can be compounded during an emergency and the end result can be catastrophic. Consider an automated reality providing an artificial world and the human reacts to such an environment. Should we trust what the machines tell us in all cases?

The integration parameters concerning acclimation further complicate the picture when evaluating contingency, backup, damage control, or loss control. It is not easy to determine the System State; when something goes wrong, reality can become artificial. The trust in the system can be questioned. Determining what broke could be a big problem. When automation fails, the system could have a mind of its own. The human may be forced to take back control of the malfunctioning system. To accomplish such a contingency may require the system committee. These sorts of contingencies can be addressed within appropriate system safety analysis.

7.2.7 Software as a Risk Control

Software reliability is the probability that software will perform its assigned function under specified conditions for a given period of time[11]. The following axioms are offered for consideration by the system safety specialist:

- Software does not degrade over time.
- Since software executes its program *as written*, it does not fail.
- Testing of software is not an all-inclusive answer to solve all potential software-related risks.
- Software will not get better over time.
- Software can be very complex.
- Systems can be very complex.
- Humans are the least predictable links in complex systems since they may make unpredictable errors.
- Faulty design and implementation of such systems will cause them to deviate.
- Deviations can cause contributory hazards and system accidents.
- Cookbook and generic approaches do not work when there are system accidents and system risks to consider.
- It is not possible to segregate software, hardware, humans, and the environment, in the system.

[11] Ibid. Reheja, page 262.

- It may not be possible to determine what went wrong, what failed, or what broke.
- The system does not have to break to contribute to the system accident.
- Planned functions can be contributory hazards.
- Software functions can be inadequate or inappropriate.
- It is unlikely that a change in part of the software does not affect system risk.
- A change in the application may change the risk.
- Software is not generic and is not necessarily reusable.
- The system can be "spoofed".
- A single error can propagate throughout a complex system.
- Any software error, no matter how apparently inconsequential can cause contributory events. Consider a process tool, automated calculations, automated design tools and safety systems.
- It is very hard to appropriately segregate safety-critical software in open loosely coupled systems.
- Combinations of contributory events can have catastrophic results.

Considering the many concerns and observations listed in these axioms, software-complex systems can be successfully designed to accommodate acceptable risk through the implementation of appropriately integrated specialty engineering programs that will identify, eliminate or control system risks.

7.3 Use of Historical Data

Pertinent historical system safety related data and specific lessons learned information is to be used to enhance analysis efforts. For example, specific reliability data on non-developmental items (NDI) and related equipment are appropriate. Specific operational and functional information on commercial-off-the-shelf (COTS) software and hardware to be used will also be appropriate. The suitability of NDI and COTS is determined from historical data. Specific knowledge concerning past contingencies, incidents, and accidents can also be used to refine analysis activities.