Analyzing Distributed Functions in an Integrated Hazard Analysis

A. Terry Morris[*]
NASA Langley Research Center, Hampton, Virginia 23681

Michael J. Massie[†]
ARES Corporation, Houston, Texas 77058

Large scale integration of today's aerospace systems is achievable through the use of distributed systems. Validating the safety of distributed systems is significantly more difficult as compared to centralized systems because of the complexity of the interactions between simultaneously active components. Integrated hazard analysis (IHA), a process used to identify unacceptable risks and to provide a means of controlling them, can be applied to either centralized or distributed systems. IHA, though, must be tailored to fit the particular system being analyzed. Distributed systems, for instance, must be analyzed for hazards in terms of the functions that rely on them. This paper will describe systems-oriented IHA techniques (as opposed to traditional failure-event or reliability techniques) that should be employed for distributed systems in aerospace environments. Special considerations will be addressed when dealing with specific distributed systems such as active thermal control, electrical power, command and data handling, and software systems (including the interaction with fault management systems). Because of the significance of second-order effects in large scale distributed systems, the paper will also describe how to analyze secondary functions to secondary functions through the use of channelization.

Nomenclature

CEV	=	Crew Exploration Vehicle
FHA	=	Functional Hazard Analysis
FMEA	=	Failure Modes and Effects Analysis
FTA	=	Fault Tree Analysis
GNC	=	Guidance, Navigation and Control
IHA	=	Integrated Hazard Analysis
ISS	=	International Space Station
MNWF	=	must not work function
MWF	=	must work function
NASA	=	National Aeronautics and Space Administration
Primary Hazard Effect	=	worst case effect of hazard which manifests itself
Primary System	=	system under assessment whose hazards directly result in undesired events
SAVIO	=	Software and Avionics Integration Office
Secondary Hazard Effect	=	additional effects of hazard which manifests itself
Secondary System	=	a supporting system whose failures can induce undesired affects in the system it supports

I. Introduction

Many in the safety community have noticed the preponderance of techniques focused on reliability and fault/failure analysis in the literature. These techniques can generally be called fault-event techniques and are powerful tools to aid safety personnel in reducing unwanted risks due to faults. All risk-reduction techniques,

[*] Safety-Critical Avionics Systems Branch, Mail Stop 130, SAVIO IHA Lead, AIAA Lifetime Associate Fellow.
[†] Lead for NASA's Constellation Integrated Hazard Analysis, ARES Corporation, Johnson Space Center.

Error Type	*Meaning in Hazard Analysis*
Type I (false positive)	Reporting risks higher than they actually are
Type II (false negative)	Omitting hazards or reporting risks lower than they really are
Type III (solving wrong problem)	Focusing analysis on faults or reliability versus on system safety

Table 1. Decision Errors in Hazard Analyses

however, are not created equal. Each risk-reduction technique must be chosen commensurate with the goal of the analysis, the structure and interactions of the organizations involved in the system and the constraints of the system being analyzed. The inappropriate use of risk-reduction techniques for large scale systems contributes significantly to miscommunication, schedule overruns, cost overruns and a false sense of confidence in understanding and controlling unwanted system behavior. Distributed systems, for example, form the infrastructure that enables other system must-work (MWF) and must-not-work functions (MNWF) to operate and be managed. Because of this, distributed systems must be analyzed using top-down, system-oriented techniques. The authors advocate the primary use of system-oriented techniques like integrated hazard analysis (IHA) for distributed systems in conjunction with secondary bottom-up failure-oriented subsystem techniques in this order. We believe this combination is appropriate to minimize errors of decision in reducing system-level risks for large scale distributed systems. The types of decision errors that will be reduced with the approach described in this paper include type II errors (false negatives, that is, overlooking hazards when hazards indeed exist) and type III errors (the error of having solved the wrong problem) (see table 1).

One of the primary underlying questions program and project managers want answered for large scale distributed systems is “Is the system safe?” Complete and absolute safety is a condition that is free from risk or harm. Some might even say that absolute safety appears to reside where there is perfect knowledge and complete control. This implies that all variables, parameters, factors, influences and interactions are known, delineated and controlled. This condition is far from true in present day real world large scale integrated systems. Since absolute safety is not attainable, particularly for inherently complex or hazardous systems, realistic system safety objectives are to develop a system with acceptable risk. This involves establishing a systematic approach that identifies potential hazards, analyzes their risks and then implements corrective actions to either eliminate or mitigate the hazards throughout the system lifecycle. From this perspective, system safety can be viewed as a relative or optimized level of acceptable risk for a given system and its resource constraints. The goal of system safety is to detect hazards as exhaustively as resources permit and to provide protective measures early in the system development to avoid costly design changes late in the program. Each step of this process involves a sequence of decisions that collectively guide the analyst toward the set of identified hazards, toward the set of hazard causes, toward the set of possible mitigations which generally leads to the identification of analyzed risk. A subsequent set of decisions generally identifies whether the analyzed risks are acceptable or not.

In order for analyzed risks to be accepted by a program manager or an independent safety panel, there must be some level of confidence in the safety process which produced the results. Without this confidence in the overall safety process, many will view the effort as “cosmetic only” with no real teeth to integrate safety into the actual design. In order to have an effective system safety program, a systematic process should be designed to minimize both systematic and uncertainty errors in judgment because each wrong decision in the sequences of decisions biases (to some degree) the risk results. Table 1 describes the three types of decision errors that should be minimized in a hazard analysis. Type I errors, false positives, are obtained when the hazard analysis reports there is a hazard, a cause or an increased level of risk when the real level of risk is significantly lower. Type I errors can be viewed as errors of excessive credulity. Type II errors, false negatives, are obtained when the hazard analysis omits a hazard, a cause or reports a decreased level of risk when, in reality, a hazard does exist, a hazard cause is valid or the real level of risk is significantly larger. Type II errors can be viewed as errors of oversight and result from information being overlooked, under analyzed or not communicated. For hazard analysis, the goal is to provide balance and context to the types of errors encountered. In some cases, type I errors may be more serious. In other cases, type II errors may be considered more serious.

In 1957, Allyn W. Kimball, a statistician with the Oak Ridge National Laboratory, proposed a different kind of error to exist with the first and second type of errors. Kimball defined this “error of the third kind[1]” as being “the error committed by giving the right answer to the wrong problem.” In 1974, Mitroff and Featheringham extended

Kimball's definition, arguing that "one of the most important determinants of a problem's solution is how that problem has been represented or formulated in the first place." They defined type III errors as "the error of having solved the wrong problem...when one should have solved the right problem[2]." For hazard analysis, this error occurs when the hazard analyst employs the use of failure-oriented or reliability-oriented techniques to solve system safety problems. Since hazards encompass more than faults and failures, the application of failure-oriented or reliability-oriented techniques to system safety problems produces a grave and serious type III error that provides a false sense of confidence in the results. For this reason, type III errors from a hazard analysis perspective may be considered more serious than type I and type II errors. This statement is not absolute, it is a heuristic. It is conditioned on the resources (financial, personnel and schedule) allotted to the task and the ultimate goal of the risk analysis.

An appropriate response to the question, "Is the system safe?" involves minimizing the decision errors that hazard analysts perform in their duties. This can be decomposed into two complementary processes. First, the response to what is "safe enough" must be addressed in the context of the endeavor. Second, the response to what is "not safe enough" must be identified with a process to address these findings. The approach outlined in this paper will attempt to minimize these errors in a hazard analysis by focusing on a subset of the decisions that must be made.

II. Background

To provide greater clarity to this discussion, background will be provided on the subset of decisions that must be made to answer the safety question. The major decisions involve selecting appropriate safety personnel with systems perspectives, understanding the differences in failure-oriented versus system-oriented tools and the limitations of each, recognizing the need to tailor the hazard analysis based on the structure of the organization and the type of system being developed (centralized versus distributed) and iterating the hazard analysis throughout the system life cycle to reduce uncertainty in the risk results.

A. System Safety Personnel Requirements

Of all the major decisions that have a profound effect on the end product, no problem is more important than the "who" problem. Questions like "Who will lead the system safety process?" and "Who will be the contributing members of the hazard analysis team, the safety assurance team, the safety panel, etc.?" are all who-type questions that require who-type decisions. In order for a program manager or safety panel to have confidence in the output of a hazard analysis, there must be some level of confidence in the person/team leading the analysis. Geoff Smart and Randy Street identify the impact of decision errors in personnel selection in their book titled, "*Who*[3]."

What are some of the general requirements for system safety personnel? Allen Long, Senior System Safety Engineer with Hernandez Engineering states that an analyst must have "...sufficient understanding of the details of a wide variety of systems and subsystems[4]." He continues by saying "the analyst must understand the system as an integrated interaction of subsystems." Simply stated, it is in the complex relationships and interaction of systems and components that reveal hidden discoveries. System safety personnel should have this perspective and mindset. Morris and Massie reveal requirements for IHA integrators[5] by analyzing necessary and sufficient requirements related to cognitive ability, expertise, emotional competence and big picture thinking. Their analysis reveals the need for interactive collaborators. These leaders as described by Michael Maccoby, in his book "The Leaders We Need[6]" focus on teamwork and self-development. Their strengths include their independence, their readiness for change and their quick ability to connect with others and work in a self-managed team. They are natural communicators and collaborators. They tend to be aware of their own transferences and generally rely on others (usually an outsider) to provide reality checks. In short, the *Interactive Collaborator* combines multiple capacities (emotional, strategic, big-picture thinking, etc.) into a cohesive whole in order to provide leadership to organizations. Organizations that employ personnel with these characteristics for large scale system safety applications prevent many of the type I, II and III decision errors in the end product because the personnel have the proper systems perspective throughout their analyses. Brad Cohen, from Boeing Information, Space and Defense Systems, provided lessons learned that described how to improve complex integration tasks related to the International Space Station (ISS), arguably the most complex large scale integration program developed during the 1990s. The number one lesson learned from ISS development was, "Hardware and software must naturally integrate by working the integration task from day one. This is solved by education, working together, and removing barriers[7]." In other words, the number one lesson learned from ISS development dealt with people, their perspectives and their mindsets.

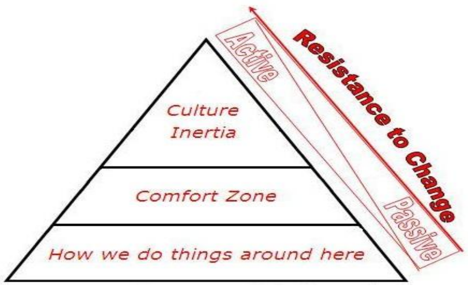

Figure 1. Resistance to Change Pyramid[8]

It is humorous to note that some organizations inadvertently sabotage the safety of their large scale systems by employing personnel who do not have or utilize a systems perspective. Reasons for this include an established organizational culture, a legacy of solving problems in pre-defined manners and a general resistance to change as depicted in the resistance to change pyramid[8] (figure 1). In general, safety analysts tend to experience more difficulty when there is a mismatch between their system safety perspective and a failure oriented perspective adopted by either a program manager or a safety panel. This clash of perspectives can be viewed as pushing a boulder up the resistance to change pyramid. Much energy is expended and wasted when consistent system safety perspectives are not employed (type III errors).

B. Knowledge of Failure-Oriented versus Systems-Oriented Safety Techniques and Their Limitations

Every practitioner utilizes, to some extent, a set of tools associated with a particular discipline. In the world of risk-based or risk-informed decision analysis, this is particularly true. In order to reduce type III errors (solving the wrong problem), organizations not only have to select appropriate personnel but also need to ensure system safety personnel know how to apply risk-based tools. This necessarily includes the limitations of such tools and techniques. Some techniques are appropriate for identifying hazards while others are appropriate in analyzing or identifying failures. System safety analysis, in particular, requires the use of techniques that consider the system as a whole and identifies how the system operates, identifies the interfaces and interactions between subsystems, identifies the interactions between the system and operators, and identifies both normally correct behavior as well as component failures. Techniques such as system hazard analysis, integrated hazard analysis and hazard causal analysis are examples of appropriate tools for identifying hazards for system safety. These techniques involve the use of functional decomposition and allocation to individual subsystem components. In some cases, the functions are refined further into must work and must not work function partitions. This decomposition and refinement helps to distinguish between actions that contribute to correct and incorrect system behavior as well as critical and noncritical behavior.

Some organizations improperly apply failure/fault or reliability-oriented techniques like fault tree analysis (FTA) and failure modes and effects analysis (FMEA) to do the job of a system level hazard analysis not fully understanding the intent and limitations of such tools. This misapplication takes several forms. Fault tree analysis, for instance, though performed from a top-down perspective, is generally a means of analyzing hazards, not identifying them. FTA, however, with a skilled practitioner can reveal problems with a system or “eurekas” as explained by Allen Long[4]. Long advocates the use of FTA in a much broader sense than is generally used. Many of his arguments are coupled with the use of personnel that have logical minds and the ability to visualize the structure and interactions between systems and subsystems. In order to utilize FTA for system safety, he also stresses the analyst to not define the tree branches in terms of failures. In summary, without a skilled practitioner, FTA alone is not appropriate for system safety.

FMEA techniques are generally used to predict equipment or component reliability. This technique is not appropriate for system safety because it was not designed particularly for identifying hazards. Hazards, from a system perspective, are more than faults. Hazards can stem from problems related to human error, design flaws, malfunctions or undesirable interactions which may occur when there is no faulty behavior. FMEA techniques are based on the assumptions that inputs into the component are correct, the operational environment is proper (and does not contribute to component failures), and human error (in terms of assembly, maintenance and other operations) is not a factor. Though FMEA techniques provide an excellent detailed examination of each internal component, organizations that utilize FMEA techniques for system safety inadvertently increase type III errors in their risk analysis.

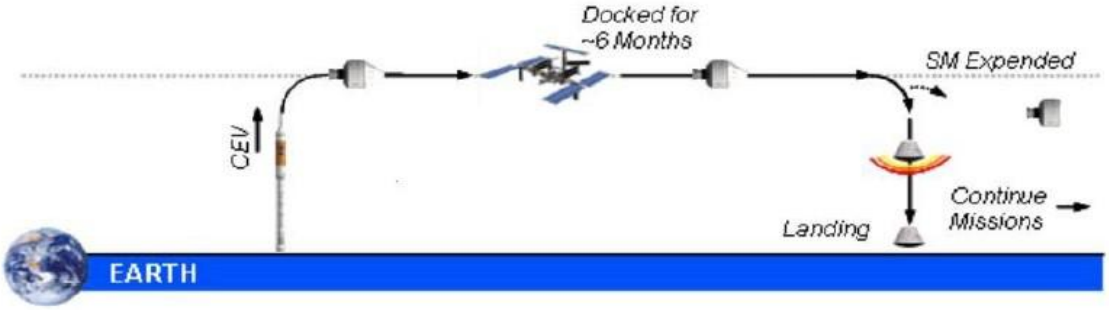

Figure 2. Constellation's ISS Design Reference Mission[9]

C. The Need to Tailor the IHA for the System being Analyzed

In addition to selecting appropriate personnel with system perspectives and knowledge of when and where to utilize analysis tools, organizations also need to understand that the hazard analysis needs to be tailored for the system being developed. This tailoring needs to incorporate the structure of the organization, the roles between engineering and safety organizations, the functional responsibilities and interactions between sub-organizations, the timing of the hazard analysis products for major milestone reviews, the type of system being designed, etc.. While the need to tailor a hazard analysis is a broad subject, this paper focuses on how to tailor a hazard analysis for a large scale distributed system.

D. Centralized versus Distributed Systems

One of the major decisions a systems analyst must perform is to determine how to appropriately tailor a hazard analysis for the type of system being developed. We will confine our descriptions to either centralized or distributed classifications. A centralized system is one that allows certain functions to be concentrated in the system's hubs. Benefits of centralization include the accessibility of resources and the power to make decisions for the whole system. Centralized systems also have limitations with data management and security; not to mention adaptability to new issues and environments. Single point of control and single point of failure are major issues with centralized systems. On the other hand, a distributed system consists of a collection of subsystems or components connected through a network which enables the subsystems to coordinate their activities and to share some resources so that users perceive the end product as a single, integrated system. Advantages of distributed systems include the ability of subsystems to execute concurrently, the option of increased adaptability to new technologies and the combination of heterogeneous components. Disadvantages include multiple points of control, multiple points of failure, a lack of system integrity if concurrent processes are not coordinated properly, and the increased need for organizational structure and agreement. Despite the disadvantages, many of today's large scale integrated systems are distributed by design.

In short, the collection of system requirements embodies the needs, goals and objectives of the end users. In effect, system requirements exist to describe the needs and the purpose of the system. System requirements are further decomposed into functions that help achieve either system performance objectives or system-level constraints. Functions, from the system perspective, delineate the operations the system must perform to satisfy the requirements and to achieve the system objectives. In many systems, only a subset of system functions contributes directly or indirectly to system level hazards. For distributed systems, it is generally the subsystems that perform the system functions. Distributed systems, in particular, form the infrastructure that enables system must-work (MWF) and must-not-work functions (MNWF) to operate and be managed. This is done by determining which set of subsystems are required to perform the system level function. For instance, a generic distributed communication system permits each subsystem to coordinate sub-function behavior to achieve each integrated system level function. From a hazard analysis perspective, most system or functional hazards have primary and secondary effects. An example of a large scale distributed aerospace system is NASA's Constellation program whose mission is to take humans back to the moon and onto Mars. The first phase of the mission is to launch an Orion crew exploration vehicle (CEV), dock the Orion vehicle with the ISS and then return to earth[9] (see figure 2). For the majority of large

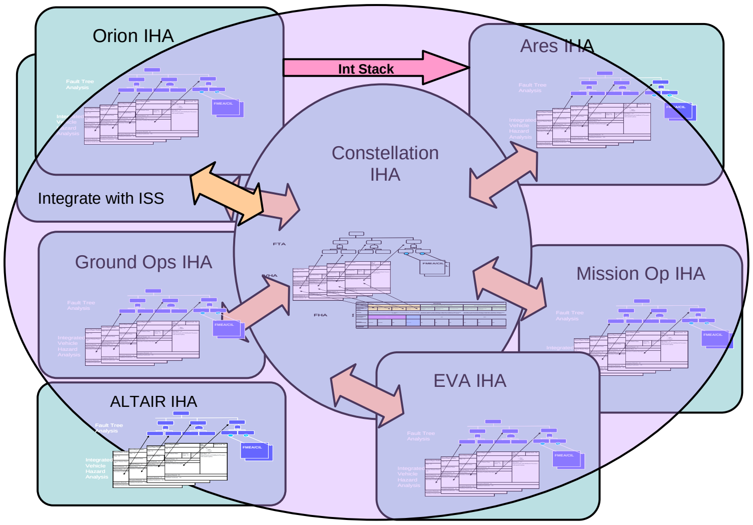

Figure 3. Constellation's Integrated Hazard Analysis Structure

scale systems like this one, the hazards related to the primary effects are of most concern. Some examples include "loss of CO_2 removal results in toxic atmosphere to crew" and "failure of docking attachment mechanisms to fully engage results in inadequate structural integrity." For many of the distributed systems, it is the secondary effects that are generally of most concern. For example, loss of power is a vehicle architecture configuration issue, but the loss of attitude control that is created by the loss of power is a primary hazard of the guidance, navigation and control (GNC) subsystem and therefore is a secondary hazard of the power subsystem. In summary, distributed systems must be analyzed for hazards in terms of the functions that rely on them. It should be noted that distributed system primary hazards must also be included in the hazard analysis, but these are often limited to the box or component level hazards. Examples include electric shock, fluid leakage, etc.

E. The Iterative Integrated Hazard Analysis Process

To be effective, the system safety process should employ an iterative hazard analysis process so that all available data are analyzed for potential hazards throughout the design cycle. Only in this way can safety be designed into the product and insights into potential hazardous behavior be revealed early enough to prevent the hazardous behavior or to mitigate the hazardous behavior by way of effective redesign. The hazard analysis process specifically iterates between the hazard causes and the hazard control story in such a way as to realize a system with acceptable risk. This is a defining difference between failure based analysis and true hazard analysis. The importance of the iterative nature of the hazard analysis throughout the system lifecycle has been stressed by DoD in MIL-STD-882D[10]. Massie, IHA lead for NASA's Constellation program, has prescribed four keys to success that if adopted will lead a system safety analyst to accomplish the enormous task of integrating various systems iteratively in a large scale distributed system[11]. These keys reveal strategic, operational and organizational lessons learned from previous IHA experiences including the International Space Station. The four keys are: 1) define the analysis structure, 2) provide a good IHA plan, 3) provide for good and reliable communications and 4) select and utilize the right personnel for the job. The first key tailors the hazard analysis for the type of system being analyzed and establishes the appropriate tools used to produce the risk declarations. Good adherence to this key significantly reduces type III errors (solving the wrong problem). The second key effectively tailors the analysis to the organizational structure and the processes defined for the system. The third key describes the lifeblood of how information is transmitted, communicated and received across various organizations to produce the risk assessment. The final key elaborates on the importance of selecting the right personnel for the task (previously described in section II. A). These steps were applied to NASA's Constellation program where multiple subsystems (Orion crew exploration vehicle, Ares I crew launch vehicle, mission operations, EVA astronaut suits and ground operations) were integrated across a mission timeline to dock the Orion crew exploration vehicle with the Space Station and safely return the crew to earth (see figure 2). The structure of Constellation's IHA involved analyzing the undesirable interactions between the subsystems that could lead to a hazard (see figure 3). The IHA process involved identifying all hazards in this system-of-subsystems

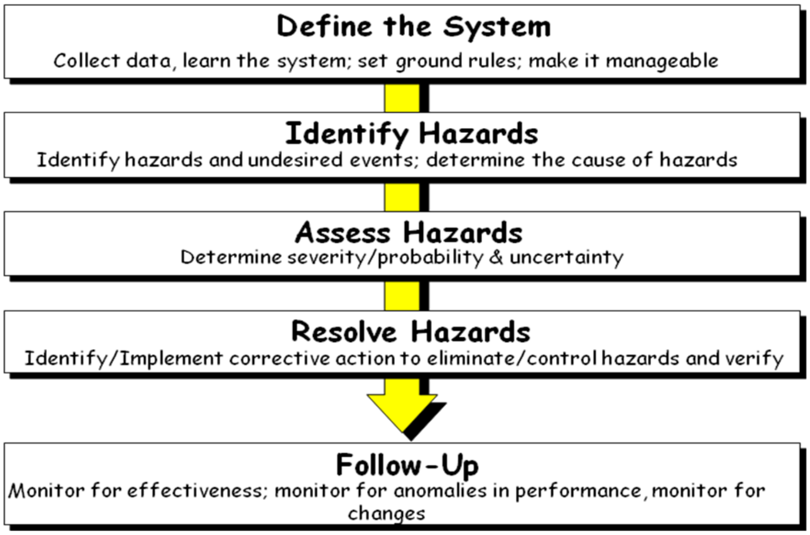
Define the System
Collect data, learn the system; set ground rules; make it manageable
Identify Hazards
Identify hazards and undesired events; determine the cause of hazards
Assess Hazards
Determine severity/probability & uncertainty
Resolve Hazards
Identify/Implement corrective action to eliminate/control hazards and verify
Follow-Up
Monitor for effectiveness; monitor for anomalies in performance, monitor for changes

Figure 4. Systematic Hazard Analysis Process

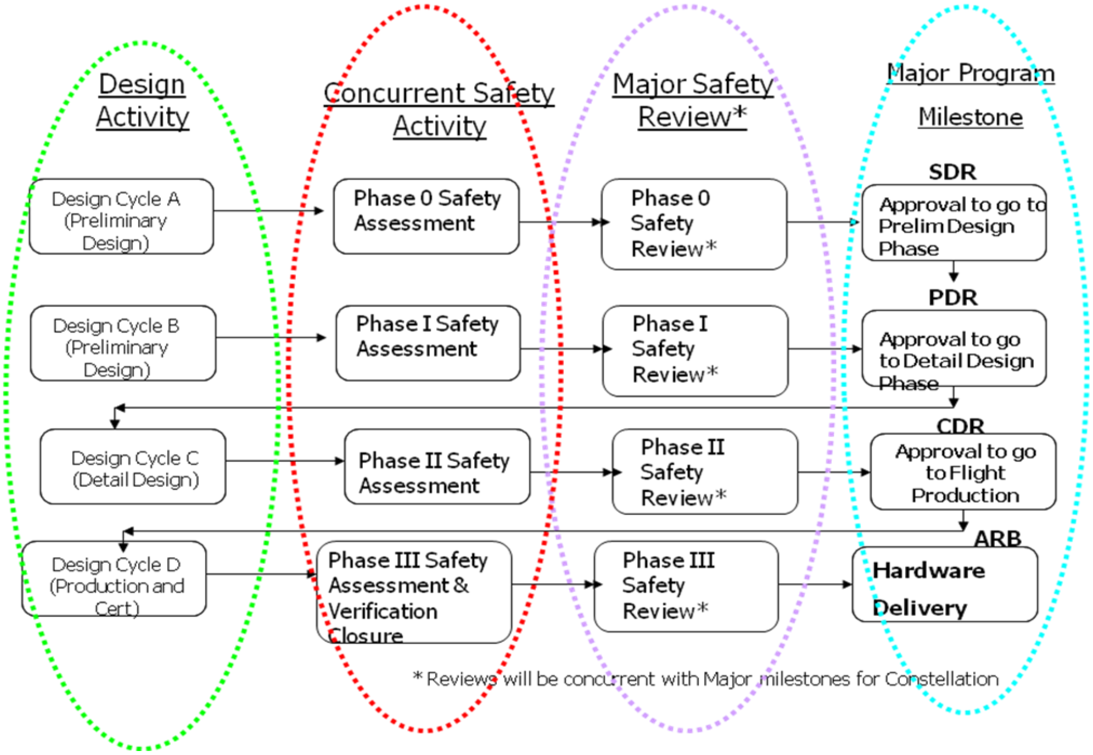
Design Activity
Concurrent Safety Activity
Major Safety Review*
Major Program Milestone
Design Cycle A (Preliminary Design)
Phase 0 Safety Assessment
Phase 0 Safety Review*
SDR
Approval to go to Prelim Design Phase
Design Cycle B (Preliminary Design)
Phase I Safety Assessment
Phase I Safety Review*
PDR
Approval to go to Detail Design Phase
Design Cycle C (Detail Design)
Phase II Safety Assessment
Phase II Safety Review*
CDR
Approval to go to Flight Production
Design Cycle D (Production and Cert)
Phase III Safety Assessment & Verification Closure
Phase III Safety Review*
ARB
Hardware Delivery
* Reviews will be concurrent with Major milestones for Constellation

Figure 5. The Hazard Analysis Phased Review Process

context, identifying all causes to each hazard, revealing the control story (while subsequently determining the risk associated with the control story) and providing verification of the controls in a systematic and iterative fashion (see figure 4). According to Constellation guidelines, hazard-related risks are to be identified during phased safety reviews which occur around major program milestones. Hazards, for instance, are identified during the program's initial design cycle, causal contributors are identified during the system definition review, controls are identified and analyzed during the preliminary design review with the verifications outlined during the critical design review (see figure 5). At each major review, the goal of the iterative hazard analysis is to ensure that the system stays in a known

Hazard Cause	Hazard Type	Primary Effect(s)	Secondary Effect(s)
Plate Tectonics[12]	Volcanoes	Lava flow, pyroclastic flow, tephra (volcanic bombs & ash falls), volcanic gases	Lahars (debris flows/mud flows) and tsunami
Plate Tectonics[12]	Earthquakes	Release of seismic energy (shaking), shifting of the land surface	Building collapse, fires, tsunami, landslides and soil liquefaction

Table 2. Primary and Secondary Effects for Specific Natural Hazards (Volcanoes and Earthquakes)

safe state regardless of the mission timeline or the state transitions. Wherever possible, the hazard analysis also attempts to update system requirements or system-level functions to ensure that the system remains in a known safe state according to the program's level of acceptable risk.

III. Analysis Techniques for Distributed Systems

A hazard is defined as a condition which if unmitigated could result in a mishap. It may also be viewed as a state or set of conditions, internal or external to a system, which has the potential to cause harm. Because distributed systems must be analyzed for hazards in terms of the functions that rely on them, care must be taken to ensure that both the primary and secondary hazards effects are analyzed with respect to both the primary and secondary systems. This section describes generic IHA processes to employ for system safety in order to analyze system hazards associated with both primary and secondary systems. The procedures outlined are intended to be generically prescriptive in intent targeted for use on large scale distributed aerospace systems. Special considerations, however, will be described for specific distributed systems such as active thermal control, electrical power, command and data handling and software subsystems. Because of the significance of second-order effects in large scale distributed systems, a process will also be described to analyze the interaction between secondary functions.

The following definitions are provided to establish common understanding between potentially confusing (and similar sounding) terms. The primary system is the system under assessment whose hazards directly result in undesired events. In like manner, the secondary system is a supporting system whose anomalous behavior can induce undesired effects in the system it supports. Technically, primary hazards refer to direct, potentially threatening results to targets (in aerospace contexts, targets refer to the crew, the vehicle, ground personnel, etc.). The primary hazard effect is generally the worst case effect of the hazard on the target. Secondary hazards, in contrast, may be viewed as indirect threats to targets. These hazards are sometimes called generic hazards since they stem from distributed system infrastructures and usually affect multiple primary hazards. Secondary hazard effects are additional worst case undesired effects separate and distinct from the primary hazard effects. Separate and distinct in this context does not necessarily imply the lack of causality or dependence.

To aid the discussion of hazard effects, a brief description of primary and secondary hazards associated with volcanoes and earthquakes is provided in table 2. Since these types of natural hazards are widely known, let's discuss two interesting points that may not be readily understood. First, volcanoes and earthquakes are both considered natural geological processes (systems) in and of themselves. But, when they affect human beings (as targets) in the environment, they are classified as hazards. Second, both volcanoes and earthquakes share the same underlying cause, that is, plate tectonics[12]. It is the interaction of the plates (subsystems) that allow major geological processes to take place such as volcanoes, earthquakes and the formation of mountain belts. Thus, the same underlying cause (plate tectonics) can produce different behavioral results depending on the details of the interaction between the plates (the subsystems) and the environment (chemicals, temperature, timing, etc.). Though distinct from hazards typically present in the aerospace industry, table 2 should provide a general understanding of the cause effect relationships by describing phenomena associated with primary and secondary hazard effects. In like manner, we will endeavor to explain and to simplify, as much as possible, how to identify and to analyze potential hazard effects associated with large scale distributed aerospace systems.

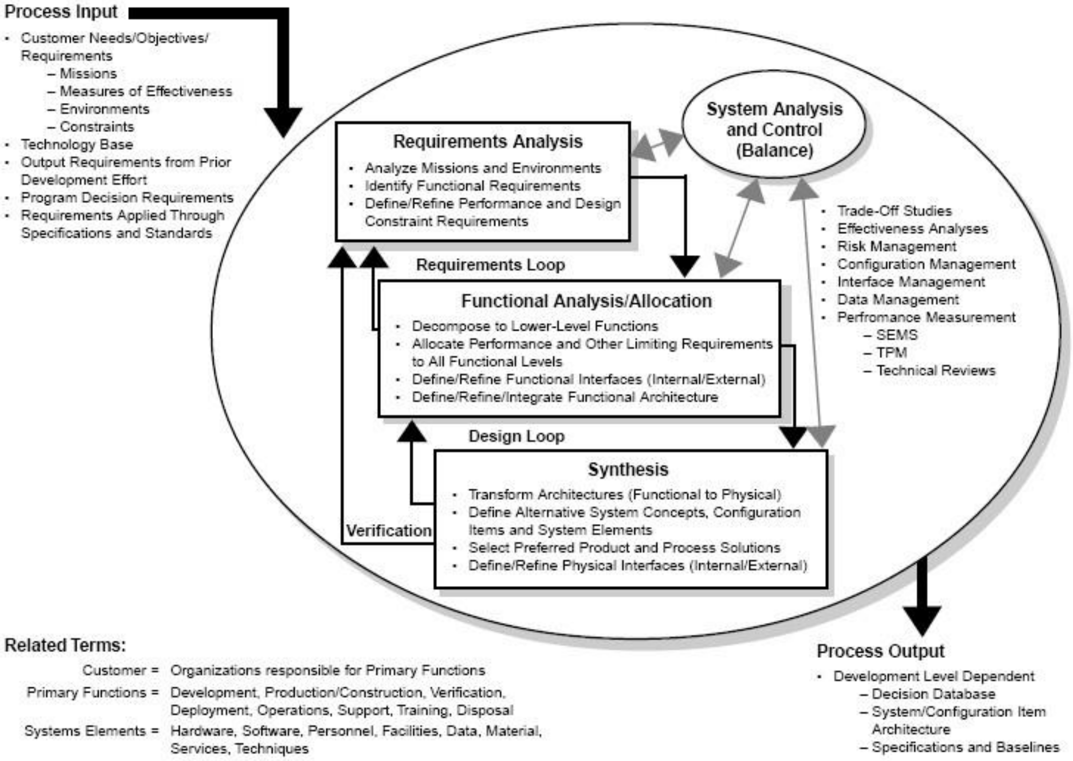
Process Input
• Customer Needs/Objectives/ Requirements
– Missions
– Measures of Effectiveness
– Environments
– Constraints
• Technology Base
• Output Requirements from Prior Development Effort
• Program Decision Requirements
• Requirements Applied Through Specifications and Standards
Requirements Analysis
• Analyze Missions and Environments
• Identify Functional Requirements
• Define/Refine Performance and Design Constraint Requirements
System Analysis and Control (Balance)
• Trade-Off Studies
• Effectiveness Analyses
• Risk Management
• Configuration Management
• Interface Management
• Data Management
• Perfromance Measurement
– SEMS
– TPM
– Technical Reviews
Requirements Loop
Functional Analysis/Allocation
• Decompose to Lower-Level Functions
• Allocate Performance and Other Limiting Requirements to All Functional Levels
• Define/Refine Functional Interfaces (Internal/External)
• Define/Refine/Integrate Functional Architecture
Design Loop
Synthesis
• Transform Architectures (Functional to Physical)
• Define Alternative System Concepts, Configuration Items and System Elements
• Select Preferred Product and Process Solutions
• Define/Refine Physical Interfaces (Internal/External)
Verification
Related Terms:
Customer = Organizations responsible for Primary Functions
Primary Functions = Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
Systems Elements = Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques
Process Output
• Development Level Dependent
– Decision Database
– System/Configuration Item Architecture
– Specifications and Baselines

Figure 6. Overview of System Engineering Process[13]

A. Validate the redundancy and independence of the primary system hazards controls

An overview of a generic system engineering process[13] is shown in figure 6. In order to assess the hazards associated with primary and secondary systems, the system level functions must first be identified along with their allocation to lower level subsystems. Functional analysis is the process that assigns, maps and traces high level functional requirements to subsystems or components of the physical design. It is in the iterative requirements and design feedback loops that IHA benefits the system. In common large scale distributed aerospace systems, the top level system functions can generally be clustered into power, avionics, environmental controls & life support, structural/mechanical, propulsion, GNC, communications, command & data handling and software system categories (to name a few). Depending on the purpose of the design, the requirements and the constraints, some of these systems can be considered primary systems while others can be considered secondary systems. To add to the complexity, these are not generally considered static relationships because primary and secondary systems are classified relative to the role they play in achieving the function. In other words, primary and secondary system classifications depend on the function the system is designed to perform. This, in turn, depends on how the sub-functions are allocated in the distributed system. Early in most standard hazard analyses, a proper system level functional analysis and a functional hazard analysis (FHA) resolves many of these issues by determining the system level function and their allocation to the lower level sub-functions. This functional allocation helps identify primary systems associated with system level functions which, in turn, help provide definition to the distributed system architecture.

Much of the iterative IHA process involves assessing and reassessing the control story in order to resolve prescient hazards (see figure 4). Let's call this particular system the primary system being assessed. The goal is to validate the redundancy and independence of the primary system hazard controls and to ensure that these controls are maintained as they are processed through the distributed system. This is accomplished by assembling a complete list of MWFs and MNWFs that depend on the distributed system. Next, itemize the hazard controls for each MWF/MNWF that relies on the distributed system for the primary function being assessed. Finally, analyze the distributed system architecture in terms of its ability to maintain the redundancy and independence of the hazard controls for each primary function that relies on the distributed system architecture. This is accomplished by creating

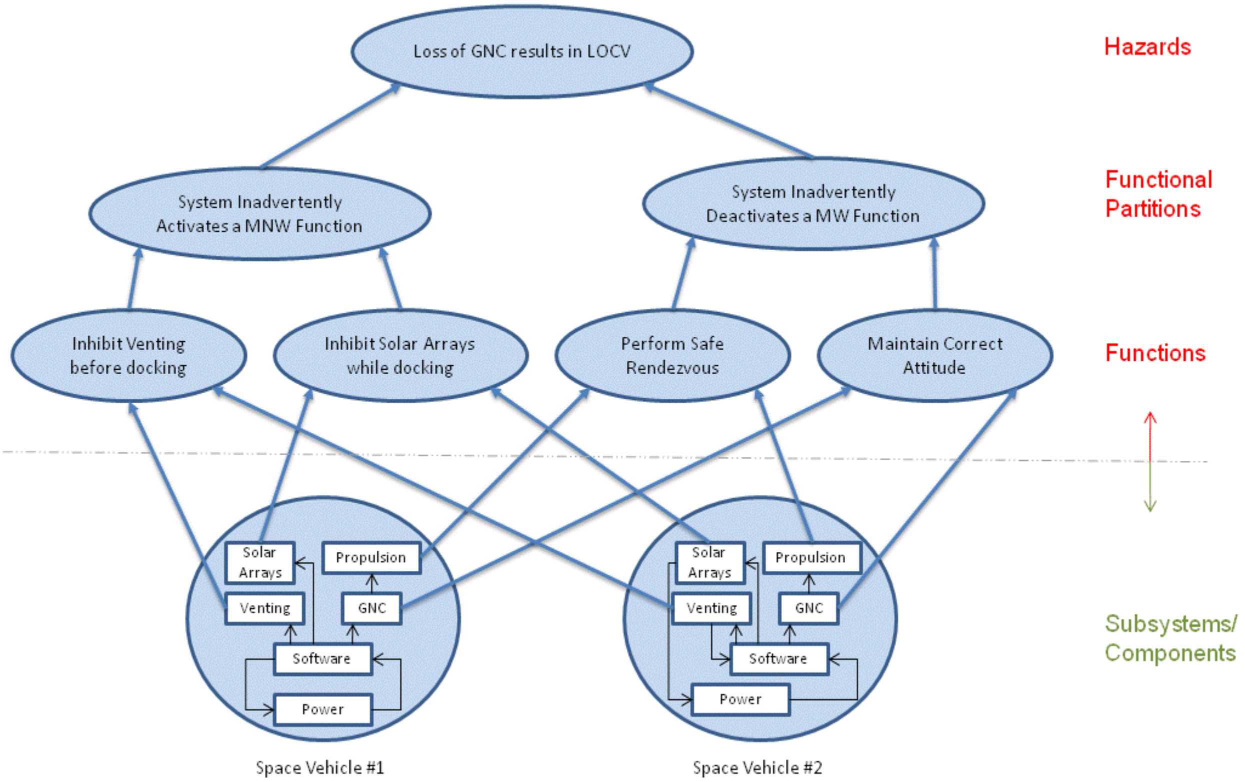
Loss of GNC results in LOCV
Hazards
System Inadvertently Activates a MNW Function
System Inadvertently Deactivates a MW Function
Functional Partitions
Inhibit Venting before docking
Inhibit Solar Arrays while docking
Perform Safe Rendezvous
Maintain Correct Attitude
Functions
Solar Arrays
Propulsion
Venting
GNC
Software
Power
Solar Arrays
Propulsion
Venting
GNC
Software
Power
Subsystems/ Components
Space Vehicle #1
Space Vehicle #2

Figure 7. Distributed Allocation of Functions for GNC-related hazards (notional)

tables, matrices and diagrams that track each primary function control through the distributed system and then validating that the redundancy and independence of the hazard controls are maintained. This process is repeated for each primary system being assessed in the hazard analysis process.

A brief example of this process is seen in the causal directed graph in figure 7. This generalized graph analyzes the hazards associated with the GNC system while docking two different vehicles in space. The top oval (or first layer) represents what is being analyzed, that is, hazards of the GNC system before and during docking. The FHA will generally reveal all events where GNC functionality is required. The second layer is used to partition the set of system level functions into MWF and MNWF categories. The third layer describes four functions that must be accomplished by the integrated system in order to avoid GNC hazards. The last layer generalizes the implementation of the distributed architecture where each space system can be considered a subsystem of the integrated system. Each space system has its own collection of subsystems (GNC, power, software, propulsion, etc.) instantiated and constrained by the space system architecture on the vehicle. It is the goal of each space system to perform the sub-functions (not shown) allocated to it. Time/event synchronization and time-to-effect conditions must also be coordinated between the two space vehicles. From a systems perspective, it is the interaction between the subsystems on both space vehicles that constitute the distributed system.

B. Assess distributed system for undesired events which will affect all or most primary system hazard controls

The distributed system must now be assessed for undesired events which will affect all or most primary system hazard controls it handles. This is accomplished by looking for the conditions which will set up the integrated system to lose the ability to function. The features of the distributed system that mitigate the set of conditions should be documented in a hazard report or a whitepaper. This document should be referenced from the primary system hazard reports. Finally, validate that the distributed system features provide mitigations within time to effect of each primary hazard being addressed.

C. Special Considerations for Specific Distributed Systems

Though the procedures identified thus far are applicable to many large scale distributed aerospace systems, the process needs to be tailored even more to handle certain types of distributed systems. Here are some special hazard assessment considerations for specific distributed systems.

1. Active Thermal Control (pressurized fluid system)

In order to analyze hazards associated with active thermal control systems, recovery procedures for fluid loop leakages' ability to be accomplished prior to time to effect need to be assessed for hazards by boxes that have lost cooling support. The partitioning of primary functions needs to be assessed between the active fluid loops for independence of hazard controls. Finally, the impact of single loop operations (if utilized) on the required redundancy and independence of the primary system hazard controls need to be assessed due to single loop operations.

2. Electrical Power

Electrical power is a classic secondary system in many applications since most avionic, control, communication and software systems require electrical power in order to perform their own functions. To analyze electrical power hazards, first assess the partitioning of primary functions between power channels for independence of primary system hazard controls. Second, assess power system capacity to provide minimum power required to support minimum vehicle primary functions to get the crew to safety in an emergency. This is achieved by assessing multi-battery configurations for the ability to tolerate multiple battery failures and still maintain minimum channel capacity needed for hazard controls. Next, validate to ensure the power overload response architecture is cascaded so that it removes user loads before the whole power system fails. Then, validate that the power system architecture ensures that the instabilities cannot cross power channel domains. Finally, validate that load shed functions do not simultaneously remove multiple legs of hazard control from primary systems.

3. Command and Data Handling

Command and data handling is a system used for situational awareness and control of critical functions. These hazards are in many large scale distributed systems. First, assess the partitioning of primary functions between command and data handling channels for independence of primary system hazard controls. Next, there should be a validation that command and data handling box fault detection isolation and recovery does not defeat primary system hazard control architecture. Finally, validate that the command and data handling fault detection isolation and recovery sub-process provides response within time to effect for all primary hazard controls handled by te command and data handling system.

4. Software Safety

Software systems are another classic secondary system on which many other systems depend (GNC, propulsion, control, aborts, communications, etc.). For boxes which handle all hazard controls or multiple legs of must work or must not work functions, a verification needs to be performed to ensure that software safety standards are met (e.g., command and data handling boxes initialize to known safe state, separate control paths, etc.). This should be included as part of the command and data handling assessment previously described. Next, there needs to be assurance that the caution and warning information for each primary function is provided in time to allow for crew responses. This is done by validating out of limit detection algorithms and timing delays to ensure that command and data processing tasks do not exceed time to effect of hazards (crew response times must be included in calculations).

5. Secondary Functions to Secondary Functions

Analysis of secondary functions to secondary functions addresses the impact of second order interactions in large scale distributed systems. In addition to supporting the primary vehicle functions, distributed systems support each other. A classic example of this type of analysis is the bidirectional dependence between the electrical power system and the software system (see fictional architecture for space vehicle #1 in figure 7). The software system requires electrical power in order to function and operate. The electrical power system, in turn, utilizes the software system to identify and manage power system faults. This cyclic dependence needs to be analyzed and controlled to prevent system level hazards. Channelization is the process used to assess the risks associated with each primary function across all supporting systems. This is accomplished by validating the redundancy and independence of primary hazard controls and ensuring that they are maintained. Finally, the analyst needs to validate that redundancy management responds properly to the loss of the primary hazard control independent of the control loss source (e.g., whether control lost was due to primary or secondary system failures). This information needs to be documented in the primary system hazard report.

IV. Conclusion

Validating the safety of large scale distributed systems is difficult because of the complexity of the interactions between simultaneous active components. Several processes have been provided to identify and to assess the risk of both primary and secondary systems in an integrated hazard analysis using systems-oriented system safety techniques. Special considerations were also provided. The net result of these system level IHA techniques is to reduce decision errors in a hazard analysis. Significant error reductions can be achieved by selecting personnel with system safety perspectives, by being cognizant of the difference between failure-oriented versus system-oriented risk reduction techniques, by understanding the fundamental difference between centralized and distributed systems and by iterating the prescribed hazard analysis processes throughout the system lifecycle.

References

[1]Kimball, A.W., "Errors of the Third Kind in Statistical Consulting", *Journal of the American Statistical Association*, Vol.52, No.278, (June 1957), pp.133-142.

[2]Mitroff, I.I. & Featheringham, T.R., "On Systemic Problem Solving and the Error of the Third Kind", *Behavioral Science*, Vol.19, No.6, (November 1974), pp.383-393.

[3]Smart, G. and Street, R., *Who: The A Method for Hiring,* Ballantine Books, New York, NY, September 2008.

[4]Long, A., *Beauty & the Beast – Use and Abuse of Fault Tree as a Tool,* source: http://*www.fault-tree.net/papers/*

[5]Morris, A. T., and Massie, M. J., "The Integrated Hazard Analysis Integrator," *AIAA Infotech@Aerospace Conference,* Seattle, Washington, April 6-9, 2009.

[6]Maccoby, Michael, *The Leaders We Need: and What Makes Us Follow,* Harvard Business School Press, Publishing, Boston, MA, 2007.

[7]Cohen, B., International space station. Large scale integration approach, *Acta Astronautica*, Volume 41, Issues 4-10, Developing Business, August-November 1997, Pages 361-368, ISSN 0094-5765, DOI: 10.1016/S0094-5765(98)00078-2.

[8]Frenette, N., KnowledgeTech Solutions Inc., Resistance to Change Pyramid, source: www.ktsprocess.com/highperformance.

[9]CxP 70007, Constellation Design Reference Missions and Operational Concepts, National Aeronautics and Space Administration, Washington, DC., January 2008.

[10]MIL-STD-882D, Standard Practice for System Safety, Department of Defense, Washington, DC., February 2000.

[11]Massie, M. J., "Constellation Integrated Hazard Analysis – Overcoming the Challenges," *Third IAASS Conference,* Rome, Italy, October 2008.

[12]The Regents of the University of Michigan, Global Change Program, Evolving Earth: Plate Tectonics, Univ. of Michigan, AnnArbor, Michigan, source: www.globalchange.umich.edu/globalchange1/current/lectures/evolving_earth/evolving_earth.html

[13]*Systems Engineering Fundamentals,* source: http://en.wikipedia.org/wiki/File:Systems_Engineering_Process.jpg, Defense Acquisition University Press, 2001.