Application of a Systems-Theoretic Safety Modeling Technique for Complex System Mishap Etiology

by

John Stealey
Master of Science in Engineering Management
University of Central Florida, 1994

Bachelor of Science in Engineering Mechanics
Southern Illinois University at Carbondale, 1987

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2003

Signature of Author______ ____________________
John Stealey
System Design and Management Program

Certified by_____ ____________________
Nancy Leveson
Thesis Supervisor
Professor of Aeronautics and Astronautics and Engineering Systems

Accepted by____________________ ____________________
Steven D. Eppinger
Co-Director, LFM/SDM
GM LFM Professor of Management Science and Engineering Systems

Accepted by________________ ____________________
Paul A. Lagace
Co-Director, LFM/SDM
Professor of Aeronautics & Astronautics and Engineering Systems

Application of a Systems-Theoretic Safety Modeling Technique for Complex System Mishap Etiology

by

John Stealey

Submitted to the System Design and Management Program
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

Abstract

Systems under development have grown ever more complex as time has passed. The introduction of automation and the increased tight coupling interactions between system components have produced emergent properties in system operation that were not anticipated in system design. The capability of current system safety analysis techniques is no longer adequate to assess the causality of accidents in systems being created with today's technology.

This thesis assesses the viability of using a new systems-theoretic safety analysis technique to understand complex system accident causality. A model was first tailored for the systems to be analyzed and then applied to sample accidents. The technique proved viable when applied as a framework for classifying causal factors that led to accidents in complex aerospace propulsion systems. The analysis raised many questions that should have been addressed in the official accident investigations but apparently were not. The causal factors were then examined for trends. The results of this examination could produce management intervention and recurrence control recommendations that focus on the most prevalent trends — conserving considerable resources and providing better effectiveness. Focusing on the systemic conditions rather than the isolated actions that led to accidents also displayed promise in enhancing organizational learning.

Thesis Supervisor:	Nancy G. Leveson
Title:	Professor, Aeronautics and Astronautics and Engineering Systems, MIT

Acknowledgements

I wish to thank; NASA and MIT for the opportunity to become part of the SDM community, my thesis advisor, Nancy G. Leveson for guidance, the SDM community for putting up with me, and above all — my family for their love, support and getting along without me.

Table of Contents

Chapter-1: Introduction

1.1 Motivation

The increased capability of systems being developed today is coming at the cost of increased complexity. Automation allows operators to control higher energy systems at great distance with increased precision by relieving them of having to physically manipulate controls. Accidents occur when properly functioning components interact in dysfunctional ways resulting in situations that the automation is not designed to control and operators may not understand. Traditional accident investigation techniques concentrate on component failure and "operator error." A new method of accident investigation is required to assess why an accident occurred when there are dysfunctional interactions as well as component failures.

The Systems-Theoretic Accident Modeling Process (STAMP) framework proposed by Leveson[1] provided the basis for the analysis of accidents involving mid-sized aerospace propulsion systems performed in this thesis. The hypothesis is that the STAMP framework provides a superior assessment of why an accident occurred by considering dysfunctional interactions as opposed to just describing what happened, as does the application of current techniques. The analysis produced a classification of the causal factors leading to each accident. Causal factor trend analysis in turn provided an explanation for why each accident occurred as well as a means for management to concentrate limited resources on correcting the most critical and prevalent causal factors. The applicability of utilizing the STAMP technique to enhance organizational learning, prevent accidents, perform risk assessment, and monitor performance were highlighted but their in-depth analysis was left for other researchers.

1.2 Terminology

The terminology used in this thesis is based on the terminology used by Leveson in "Safeware"[2] and is consistent with that used by Ackoff in "Towards a system of systems[3]." Key terms are listed in the glossary. It is critical that the system-safety terms be defined within this thesis since there is no single reference for system safety terminology. Both the first and most recent second editions of the System Safety Society's System Safety Analysis Handbook lament that there are no universally accepted definitions for important concepts in the system safety field[4]. Where possible terms are used consistent with those found in NASA documentation. Pertinent systems theory and control theory terminology is introduced in chapter 2.

1.3 Data Collection

Accidents happen every day. Most accident investigations are closed when a cause is found after being subjected to a cursory investigation into what happened. It is interesting to note that the availability of accident reports does not match the incidence of accidents. Some industries are better at making their accident reports available. NASA has a mixed record. It is very open about large-scale losses but not so open for smaller scale accidents.

1.4 Data Utilized

Three accidents from the aerospace industry were selected. The three examples ranged from small-scale research testing to large scale acceptance testing. They also ranged in time from the late 1960's to more recent. The impacts ranged from impact to commercial development work to a large-scale national initiative. Each of the accidents involved propulsion systems that were themselves elements of larger systems. None of them resulted in a loss of life nor did they have major financial impacts to their associated programs. The official reports contained findings that explained in lucid detail exactly what happened to the hardware involved in each accident. Corporate and organizational identification information is masked to prevent divulging proprietary information.

1.5 Hypothesis

The hypothesis is that a systems-theoretic feedback control loop can be used to identify what went wrong and provide categories of problems to be addressed by management. The STAMP technique provides a superior assessment of "why" an accident occurred as well as "what" exactly happened to the hardware, than usually produced by traditional techniques. It focuses on the big-picture systematic view rather than assigning blame to the operators of the hardware that failed.

1.6 Scope

There was a wide range of accidents that could have been chosen. The scope of this thesis will be constrained to aerospace projects propulsion test projects. The application of the STAMP framework contained in this thesis was developed for the limited area of rocket propulsion system developmental testing. It could also be used in other similar situations that are organized in a similar way. One potential application area is manned spaceflight operations.

Complexity is an ever-present theme throughout any accident investigation. The utility of the STAMP technique is that it enables the resolution of complexity through the use of systems theory. It also uses simple control theory principles to provide a framework for synthesizing the reasons for accident causality. Because they are central principles to the application of the STAMP framework, complexity, systems theory, and control theory are described in chapter 2. Systems theory was used extensively in the development of the framework applied in this thesis. It was used specifically to deal with the complexity of creating the system model of the organizational structure in the use of the STAMP technique.

1.7 Perspective

This thesis is based on a system operations perspective rather than a safety professional perspective. As organizations downsize and become leaner, they often concentrate more duties and responsibilities on the system operators. The concentration of greater responsibilities produces an ever-increasing chance for accidents.

1.8 Outline

Chapter 2 provides a brief overview of key concepts used in this thesis. Complexity of systems is increasing rapidly in today's environment and manifests itself in many forms. The chapter builds the systems framework for addressing that complexity. Also included is the necessary control theory that the rest of the thesis is based on. The control theory contained is tailored specifically to this thesis. The chapter starts with a fundamental control system and builds to a multi-controller multilevel hierarchical organizational structure.

Chapter 3 starts by outlining some of the current accident investigation models. It covers the ones utilized in NPG 8621.1, NASA Procedures and Guidelines for Mishap Reporting, Investigating and Recordkeeping. It next outlines the STAMP framework. It concludes with a comparison between the classical and STAMP techniques.

Chapter 4 summarizes the results obtained when using the STAMP framework to investigate the three accidents.

Chapter 5 provides a summary of the observations that the STAMP investigations produced and outlines some of the aspects that need to be changed in NASA's current accident investigation system. It concludes with a brief introduction to follow-on activities that can be pursued.

Chapter-2: Systems-Theoretic Foundation

2.1 Background

Devices being designed and constructed today are far more capable and flexible than devices built in the past and they are becoming more externally "user friendly." Most of the advances have been created at the cost of increasing the internal complexity of the device. In most cases, this internal complexity does not affect the operator. In some very critical instances, the operator must fully understand how the device works and how it will react in certain circumstances. The added internal complexity of the device makes this understanding more difficult. The organizations that design and operate today's devices are getting more complicated as well.

This thesis is concerned with the complex interactions involved with operating systems in hazardous environments. This chapter provides a very brief and high level introduction to the concept of complexity, the means used to address it, and the necessary control theory concepts to implement a systems-theoretic accident investigation model.

2.2 Complexity

Something is considered complex if it takes substantial knowledge, study, and effort to analyze, solve, and understand it. Complexity is at the root of most accidents today and probably always has been to some extent. Complexity itself is poorly understood. Complexity is not necessarily a tangible thing — in some cases it is the perception of complexity that causes problems. Hitchins suggests that there are three facets to complexity[5]: variety, connectedness, and disorder.

Variety is a commodity that can be measured. There is either more or less. Variety can be categorized as minimum, useful, and excess. In the case of minimum variety it is important to contain enough variation to survive environmental threats. Useful variety pertains to being able to respond to unanticipated needs. An excess of variety can lead to overburdening the available resources and cause the demise of the system.

A device does not require a large amount of variety to be considered complex. An item with only a small number of components can be extremely complex based on the connection between the components and the non-linear interactions between those components. Connectedness has to do with the ability of components to communicate with each other. As the number of components increases - the number of possible connections increases at a much faster rate. There are various ways that connectedness can be addressed.

Control is exercised through connectedness. In the typical hierarchical line organization, the complexity of managing large numbers of people is handled by establishing a hierarchical organizational structure that functionally breaks down the number of connections required by each individual person. A flat team structure is based on an entirely different approach that encourages participation and coordination of efforts rather than command and control.

Disorder relates to the concepts of confusion and disarray. Hutchins uses the concept of configuration entropy. He maintains that configuration entropy is the degree of disorder in pattern, organization, and structure. The greater the lack of order, the more complex something is and the more energy required maintaining stability. It is easier to comprehend something if it has an order to it.

There are two reasons that complex interacting systems do not degrade spontaneously into disorder. The first is that while there may be an extremely large set of possible ways for elements to interact, there are only a relative few that are likely to survive and be self-sustaining. The second deals with the amount of energy required to maintain the current configuration. Nature may prefer things that require less interaction energy.

Others have attempted to characterize levels of system complexity. Boppe characterizes levels of complexity as shown in Table 2-1[6]. A system may require a certain level of complexity based on its mission. Complexity typically increases when multiple facets or situations exist simultaneously.

Miller, in "The Magic Number Seven, Plus or Minus Two[7]," argued that complexity is tightly linked to human perception. In a now famous experiment, he quickly displayed cards with various numbers of dots. The subject was instructed to count the number of dots and report what they saw. The results were that when the number of dots was increased above seven per card, the subjects resorted to reporting that there were a "bunch" of dots. Miller concluded that there is a limit to the processing power of humans. The higher the complexity, the more difficulty humans have in comprehending it.

Level	Description
0	A part with a small number of features/attributes
1	A part with a large number of features/attributes
2	A system with a large number of parts
3	A system with a large number of different parts
4	A system with a large number of different parts connected in different ways.
5	A system with a large number of different parts connected in different ways where the state of the parts and connections changes over time.
6	A system with a large number of different parts connected in different ways where the state of the parts and connections changes over time and the people developing, building, and using the system have different cognitive abilities.

Table 2-1. Levels of Increasing Complexity

Steward maintains that the growth in technology has been primarily in the dimension of complexity[8] in how elements are assembled rather than by the application of previously unknown laws. The new laws that have been discovered have been discovered as a result of the ability to analyze more complex systems.

2.3 Systems Theory

Systems theory is the engineering solution for reducing complexity to manageable levels. This section first defines what a system is and then builds the case for using systems theory to address the complexity in the solving of complex problems. Simply taking apart or decomposing the overall problem into manageable tasks and then solving the individual tasks can be used to solve simple problems. The overall solution is simply the summation of the individual solutions. Complex problems, on the other hand, are not so easily decomposed. The solution is in the interaction among the individual tasks is a greater factor in the solution than the individual tasks themselves. The concepts of systems theory assists in resolving the problems associated with task interaction.

Russell Ackoff defines a system as a set of two or more elements that satisfies the following three conditions:

1. The behavior of each element has an effect on the behavior of the whole.
2. The behavior of the elements and their effects on the whole are interdependent.
3. However subgroups of the elements are formed, each has an effect on the behavior of the whole and none has an independent effect on it[9].

A system cannot be decomposed into independent parts. The two most important properties of a system are:

1. Every element of a system has properties that it loses when taken out of the system.
2. Every system has some properties that none of the parts do[10].

True understanding of a system is gained through synthesis. Synthesis is the converse of analysis. Where analysis looks to decompose systems into their elements, synthesis looks at the systems as an element of a larger containing system. The systems approach is a three step process:

1. Identify a containing whole (system) of which the thing to be explained is a part.
2. Explain the behavior or properties of the containing whole.
3. Then explain the behavior or properties of the thing to be explained in terms of its role(s) or function(s) within its containing whole[11].

It is important to note that in systems thinking analysis is performed last and from the viewpoint of the super-system in the next level of the hierarchy.

The same concept is presented as completeness by Hutchins — the set must be complete for the overall characteristics of the set to emerge[12]. Emergent properties are those properties of a system that are displayed by the whole collectively and are not due to any single element of the set. The interaction between the elements is of importance rather than just the sum of the actions of the individual elements. Another term for the same concept is Holism. Holism is the concept that there are properties of the whole that cannot be decomposed.

Systems theory also entails the concept of hierarchy of systems. Emergent properties emanate from each level of the system into the realm of a higher level system. A hierarchical model can be developed starting from a simple model. Each level of the hierarchy contains the system or groups of sub-systems contained in the level below. The concept of moving up and down the hierarchy is referred to as zooming. Zooming can be used to view sub-systems as a whole in themselves. The concept of aggregation refers to which elements are assigned to sub-systems. Aggregation is used to structure the elements into systems or sub-systems that in turn are contained by higher level systems. There is also the concept of multi-containment, which conveys that a system may reside within several higher level systems at once. In this case two or more super-systems "own" a sub-system. This leads to the potential for combinatorial explosion of interactions. It also leads to the possibility of conflicts between the objectives of the containing systems.

As systems are zoomed into smaller and smaller elements, the elements usually become easier to comprehend. As the number of elements grows the number of interrelationships grows even faster making it more difficult to assemble an understanding of the system as a whole. The choice of system model can have various consequences on how hard it will be to study the elements and the interactions of those elements. Care must be taken to do the zooming such that the interactions are not lost but also to minimize the number of elements. The drive towards minimization of elements has been apparent for a very long time as demonstrated by:

> Occam's Razor: entia non sunt multiplicanda praetar necessitatum
> (beings ought not to be multiplied, except out of necessity)
> William of Occam (c. 1280 - 1349)[13]

The previous discussion has provided a view of the world that allows for reducing complexity by organizing our perceptions into a hierarchy of systems. The complexity of the lower levels being masked by viewing them from a higher level in the hierarchy. Systems theory facilitates cutting through the real and perceived complexity to the essence of what is to be addressed[14].

One way of doing this is building models. A model is a simplified view of a more complex thing. Useful models provide a simplified representation of important aspects of complex systems. People use mental models to cope with complex systems. They form their mental models through training or trial and error. It is important that the operator's mental model is congruent with the designer's model used during the development of the system.

2.4 System Safety Theory

The systems safety concept was brought about by the lack of adequate attention to hazards in the design and operations of complex systems. The US Air Force initiated efforts to ensure that hazards were identified early in their weapons acquisitions during the advent of the intercontinental ballistic missile program. Other industries have started to adopt system safety concepts because of the exposure to liability faced from accidents .

The basic function of the system safety process is to make the hazards known and understood so they can be eliminated or controlled. The basis for system safety according to the System Safety Society is ensuring that systems do what they are supposed to and don't do what they are not. It maintains that accidents in complex systems are frequently caused by multiple factors. The Society's System Safety Analysis Handbook outlines a six step process for analyzing systems for hazards that lead to accidents. The steps are:

1. Understand the system of interest.
2. Identify and evaluate the potential hazards associated with the system.
3. Develop the means of sufficiently controlling the identified hazards.
4. Resolve identified hazards.
5. Verify the effectiveness of the implemented hazard controls.
6. Repeat the process at varying levels of detail[15].

The System Safety Society maintains that the systems approach is applied while using the above steps beginning with breaking down the complex system into understandable elements. The elements are then analyzed and any hazards are resolved. A holistic perspective of the system is to be used to ensure that there are no unintended consequences. They recognize that the process is open ended and that there is no predefined way to apply the six steps to provide a consistent solution.

The U.S. military has used MIL-STD-882 System Safety Program Requirements document, to define the tasks involved with system safety. Establishing the requirements for a system safety program is a start but it does not provide instructions on how to implement them.

It is interesting to note that the system safety concept is consistent with systems theory and its techniques but stops short of implementing them. Implementation of system safety concepts generally provide better investigation techniques for classic component-failure-induced accidents. The complex interactions involved in today's systems has led to what have been called systems failures. Systems failures are characterized by all of the elements of the system working as intended but their interaction produces hazardous conditions that lead to accidents. A new accident investigation model is required — one that is based on and implemented through true systems principles.

2.5 Control Theory

This thesis is about applying the concepts of an adaptive feedback control system to accident investigation. Control of dynamic systems is maintained through applying an adaptive feedback process. The adaptive feedback process consists of providing control action to the process being controlled, receiving feedback from the results of those actions, assessing the current system status provided by the feedback with the desired state, and then formulating a new control action based on the desired result and the constraints imposed on the system. All of the preceding actions take place in the presence of disturbances from the system's environment. The various elementary aspects of control theory relevant to this thesis are graphically depicted in figure 2-1 and are further defined below.

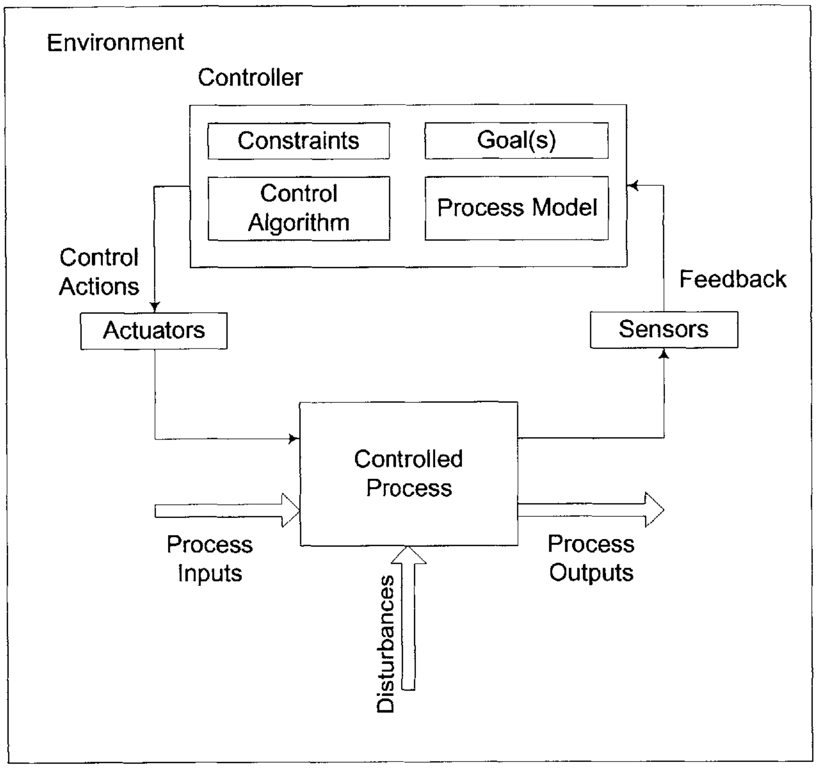

Figure 2-1. Simple Control Model

The controlled process in this simple case is the sub-system element that transforms the process inputs to process outputs. The transformation occurs in the presence of disturbances from the system's environment. The process is the system (or subsystem) that is responsible for producing the desired product. The product may be either physical or conceptual and either a product or a service. It takes inputs and produces outputs in the presence of disturbances.

The simple model above is of a goal-seeking system. Its function is to either achieve or maintain the controlled process in a desired state. The ultimate goal may not in fact be achievable. The system may strive to achieve a possibly unachievable state by continually setting and adjusting intermediate goals. Each goal is chosen for its progress towards the ultimate goal.

A clear understanding of the controlled process is required and is maintained in the process model. The control system must have an internal model of the process being controlled. The model must be detailed enough to accurately reflect the actions of the process. It contains the required set of parameters (controlled variables) required to actively control the system.

In order to affect change in the controlled process the system contains a control algorithm that describes a systematic set of actions based on the process model that are used to bring about the desired change in the process being controlled.

Control actions are the physical manipulation of the process to bring about the desired change. In a physical system, these would include things such as electrical and hydraulic actuators. They are the command directives in the case of non-physical or services systems. The feedback sub-system contains a sensor that is used to ascertain values of predefined variables. The data from the sensors is transmitted to the controller.

During operation, the control system first assesses the current state of the process using feedback data from the process. It then compares the current state with the goal. Using its understanding of the process contained in its process model, it enacts the appropriate control algorithm to decide on what set of control actions to take to bring about the desired change. The intent is for the system to continually assess the current state of the process and make corresponding adjustments that take the system toward its goal while at the same time not deviating outside of the established constraints.

The concepts for setting up a control system are relatively straightforward. First, the control system must have a goal to achieve or maintain. It can be a homeostasis system that is responsible for maintaining set point or it can be an goal-seeking system that has a sense of interim goals on the way to an overall goal. The ideal condition is for the control system to have a simplified yet complete understanding of key performance factors in the controlled process and to have an accurate internal process model of it. The creation of the process model is critical to the success of the control system. The control algorithm is developed from and is based on the process model. Control actions are designed to bring about a desired change in the controlled process. Feedback is also critical to the successful operation of the system. The system must be able to accurately measure, accept and understand the full range of feedback information. A control system that is working without feedback is known as an open-loop system.

Control systems can be flawed in several various ways. Goals may be flawed by being illegal, immoral, unethical, misguided, unaligned. This thesis assumes that the overarching goal is established and that it is understood.

Process models may be flawed in that they do not accurately reflect the actual process being controlled. The process model may have been formed incorrectly when it was designed. It may have drifted with respect to the controlled process. It may also not accurately account for time lags and measurement inaccuracies in the controlled process. A flawed process model will lead to the generation of a flawed control algorithm that will result in implementation of improper control actions.

The control algorithm may have been formed incorrectly when it was initially created. Control algorithms may drift with respect to the controlled process. Control algorithms may also not be accurate due to being modified themselves or the controlled process being modified without the proper changes being made to the control algorithm.

Control actions can involve miscommunication or no communication at all. The controlling function may itself be ineffective. There may also be unaccounted for time lags.

Feedback is critical to the successful operation of the control system. It may not have been provided for in the initial design. There may be communications problems. There may be unaccounted for time lags. The sensors responsible for obtaining the system's parameters may be broken or ineffective.

Investigation into control system problems starts with an assessment of the accuracy and completeness of the process model. Next, the control algorithm and control actions are assessed for adequacy. Finally, it must be determined if the feedback was adequate and that it truly reflected the state of the controlled process in a timely manner.

2.6 Multi-Controller Systems

This section expands the simplified single controller model to one containing multiple controllers at the same level. The possible breakdowns in operation that can develop because of multiple controller interaction are also discussed. In this example there are two controllers directing the activities of the process. There are two levels of detail in the hierarchy. The controlled process is at the bottom while the controllers form the higher level. Figure 2-2 depicts graphically the configuration of multiple controllers. The controllers can be automated or human. Both controllers must have the ability to control the actions of the actuators and to gain feedback from the controlled processes' sensors. Each controller must have a process model of the other controller as well as a model of the controlled process and of the interaction of the two. Malfunctions can develop from various sources. They are largely the result of flawed coordination between the controllers (human and automated). There can be instances where each controller believes that the other will take the appropriate action. There can also be instances where both controllers believe that they are in control but give conflicting command actions.

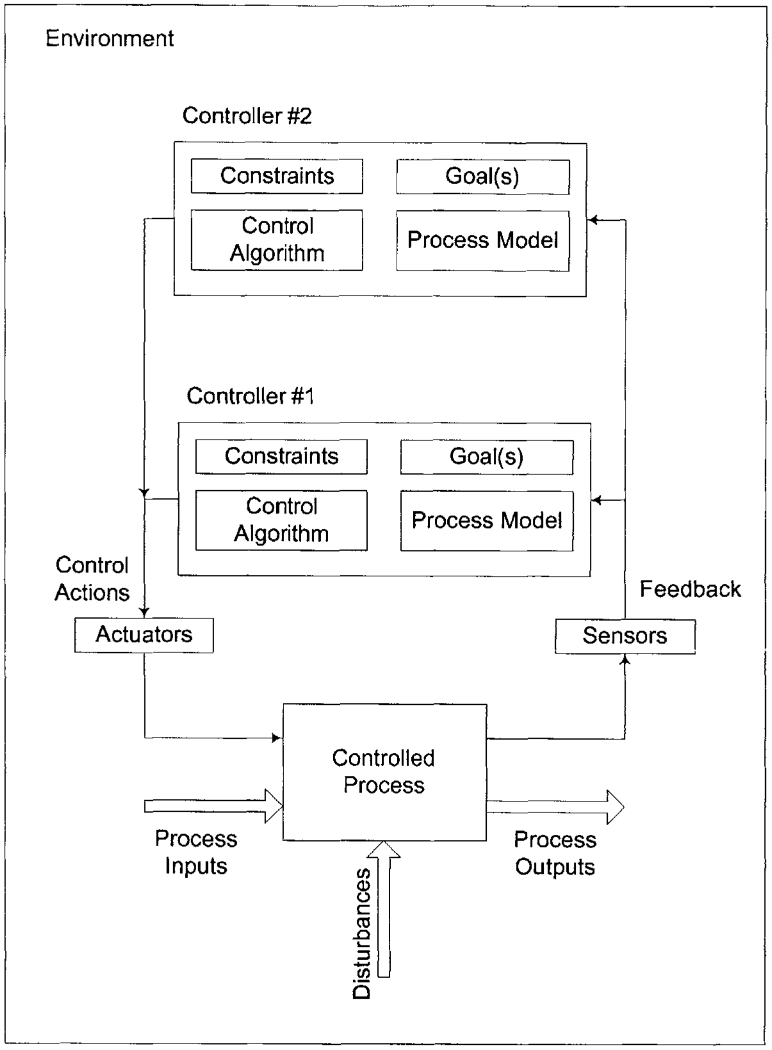

Figure 2-2. Dual Control System

2.7 Hierarchical Levels

This section builds on the previous dual controller case by adding resolution to the hierarchies of control. Each level of the hierarchy is in itself a contained system that is composed of elements. These elements interact with each other and are coordinated by the actions of at least one of the elements internal to that level of the hierarchy. Interactions between the elements that make up each of the levels produce the emergent properties that must be controlled by the level above it.

The controlled process usually contains many physical elements that must be coordinated. In this example it is done by a human controller. At the human controller (operator) level there may be many elements (people and/or whole organizations) that must interact in order to control the behavior of the controlled process. The actions of these elements may or may not be coordinated at this level. The level above must constrain the emergent properties of the levels below. A way of doing this would be to have a controlling or at least coordinating element within each level that interfaces with the levels above and below.

The key here is that the system can be decomposed into levels of control that enforce constraints on the level below it. The controlled process is controlled by the next level up and the process continues up the hierarchy. Within each level there should be a mechanism for coordinating the interactions between the elements. There can be a significant amount of interaction in larger systems. If the interactions are not constrained within the level, the emergent behavior of the level must be controlled by the level above. The goal of the overall system flows down from the top and the progress towards that goal is communicated up from the bottom in response.

2.8 Organizational Hierarchies

This thesis is geared towards organizational systems responsible for operating physical equipment. The following is a description of a general hierarchical structure for this case. The concepts presented in this section are graphically depicted in figure 2-3. At the lowest level (Level 0) is the physical hardware composed of many elements (components). In this case the physical hardware includes an automated controller that coordinates the actions of

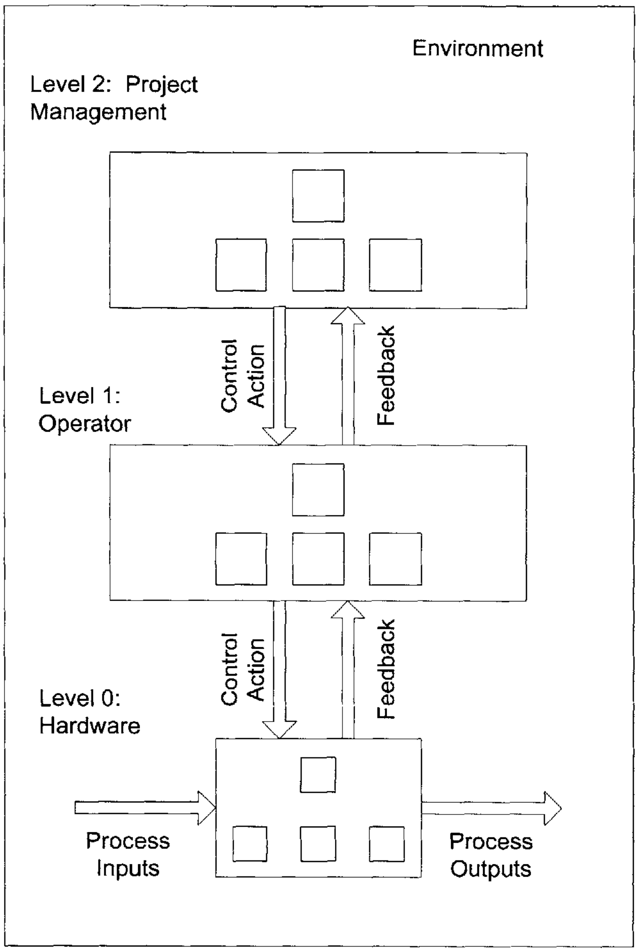

Figure 2-3. Generic Hierarchy Containing Sub-Hierarchies

the components — usually this is done for time-critical processes. Level 0 receives input and produces output in the presence of disturbances from its environment. Actions and interactions in level 0 are constrained by and cannot violate the physical laws of nature. The next level up the hierarchy (Level 1) is responsible for operating the physical system. Level 1 ensures that the hardware is not directed to violate the physical laws of nature and that it does not violate the constraints applied upon it from higher in the hierarchy. The next level up in the hierarchy Level 2: agency/company management — imposes company-level constraints while supplying direction. Level 3 consists of corporate management that is responsible for providing direction, guidance, and resources to the levels below it. Level 4 consists of regulatory agencies and legal systems of the Federal government (in the United States). Personnel at this level are public servants of the government and lawyers for the legal system. Level 5 consists of the Federal Government (in the United States). They create laws that constrain the actions of the regulatory agencies to act in the public good.

This chapter has provided a brief introduction to the concepts that are used in the rest of the thesis. Classic methods of investigating and explaining accidents falter as systems become more complex. Understanding and using systems theory is fundamental to understanding and utilizing the systems-theoretic accident investigation model introduced in the next chapter and used in chapter 4.

Chapter 3: Accident Investigation Models

3.1 Background

Chapter 2 outlined facets of complexity and briefly described systems theory used to address it. This chapter's goal is to outline classical accident investigation models and introduce a systems-theoretic modeling concept for accident investigation. This chapter will outline an approach based on systems-theoretic modeling that is capable of handling and describing the complex interactions caused by an evolving system that cause systems failures. This chapter first describes the models on which current mishap investigations are based.

In current industrial safety, a cause of an accident is composed of the set of conditions, each of which is necessary and which together are sufficient for the accident to occur. The individual conditions are causal factors. The set of causal factors make up the cause. Depending on the model that the investigation is based, the causal factor identification may involve much subjectivity and need to be interpreted with care. The most common causal factor used is that of operator error. There are legal ramifications when establishing guilt and liability — this thesis aims to determine causality for the sake of technological improvement.

For this thesis, a cause of an accident is the result of a lack of adequate constraints on behavior at each level of a socio-technical system. Flawed processes involving the interactions of the system's elements cause accidents in this model. The process leading up to an accident is described in terms of an adaptive feedback process that fails to maintain safety as performance changes over time to meet a complex set of goals and values[17].

3.2 Classic Mishap Investigation Models

As demonstrated earlier, models provide a way of grasping complex phenomena and communicating it to others. Models are abstractions that simplify reality by abstracting away irrelevant details and concentrate on the aspects that are most relevant. There have been many models created that attempt to describe an accident as a set of events and conditions that account for the outcome. Models are used to organize data and set priorities in the accident investigation. Their main goals are to understand past accidents and to learn how to prevent future ones. The following is only a sampling of the various types currently in use.

3.2.1 Energy Models

Energy models are the oldest and most ubiquitous in mishap investigation. They view accidents as the result of an uncontrolled and undesired release of energy. The most obvious way to eliminate accidents is to utilize barriers or other energy flow mechanisms. At least one energy model divides accidents into two types: energy transformation and energy deficiency. Energy transformation accidents occur when one form of controlled energy is transformed into another destroying property or injuring people. The absence of required energy needed to perform crucial functions brings about energy deficiency accidents. Another energy model also divides system into two types: action systems that produce energy and non-action systems that constrain energy. Action systems deliver energy or are responsible for operation of the system and non-action elements support or contain energy. This model does allow for complex systems that contain both action and non-action elements. Limitations on the operation of the system are used to control hazards in action elements and fixed standards, design constraints, and minimum safety factors are used to control non-action elements. The major drawback in energy models is that they do not include the mission assurance portion of safety. Non-physical losses caused by logic errors are not within their scope.

3.2.2 Domino and Single Events Models

It was realized early on in accident investigation that hazardous conditions were causing accidents. Industrial safety concentrated on unsafe conditions. The emphasis evolved from unsafe conditions to unsafe acts. Accidents were viewed as someone's fault because of the performance of an unsafe act.

Henirich proposed a "domino theory" of accidents where people and not things were the cause of accidents. The dominoes are labeled[18]:

1. Ancestry or social environment, leading to
2. Fault or a person, which is the proximate reason for
3. An unsafe act or condition (mechanical or physical hazard), which results in
4. An accident, which leads to
5. An injury

In theory when the first domino falls, it automatically knocks down the next and so on until the accident occurs. He argued that the third (an unsafe act or condition) was the most effective domino to remove. The drawbacks to this model are that symptoms may be removed while the causal factors remain and that when the identification of causal factors is limited so will be the potential solution. Some investigators suggested looking past the identification of an unsafe act and ask why the defect existed.

Others suggested modifications are to make the domino theory more general and to include management actions. Adams suggested the following dominoes[19]:

1. Management structure (objectives, organization, and operations)
2. Operational errors (management or supervisor behavior)
3. Tactical errors (caused by employee behavior and work conditions)
4. Accident or incident
5. Injury or damage to persons or property

Epidemiological models describe accidents in terms of an agent, the environment, and the host. Accidents are the result of complex and random interactions between the three elements. They can not be explained by addressing any less than all three. There are two types of epidemiological modes. The first is a descriptive epidemiology model that utilizes the general descriptive statistics of a population to describe the general distribution of injuries in that population. The second is an investigative epidemiology model that looks at specific injury data in order to design countermeasures. Several of the drawbacks to epidemiological models are that the approach assumes that statistical evaluation of the accident data is applicable, that common factors are assumed present, and the validity of the conclusions is dependent on the quality of the information database. Another significant drawback is that sequencing and timing relationships between events and conditions are not captured.

3.2.3 Chain-of-Events Models

Chain-of-events models organize causal factors into chains of events. An accident cannot happen if the chain is broken. Events are chained together into chronological sequence and events are labeled as proximate, primary, basic, contributory, systemic, or root. The unsafe events are used as a starting point in the search for why they were allowed to occur. One drawback to this method is that there is no hard stopping point when tracing back the events from the accident.

There are many expansions to the chain-of-events model. Some include the relationships among events and conditions in the accident sequence. They may use converging logic trees connected using AND/OR relationships to describe the accident process. Reoccurrence control measures involve either removing the events or conditions in the chain or by adding required simultaneous conditions or events that decrease the chance of all of the factors required for an accident being present.

Factors other than simple events and conditions are difficult to incorporate into basic chain-of-events models. Some of the difficult factors include organizational deficiencies and those related to the safety culture of the organization. The National Transportation Safety Board (NTSB) introduced a sequencing model in the 1970s. The NTSB's model described accidents as patterns of events and causal factors arising from contributory factors. The contributory factors in turn arise from systemic factors. The NTSB's model is similar to one proposed by Lewycky[20]. Lewycky proposed a three-level model for understanding accidents. The lowest level describes the chain of events. The next level up describes the conditions or lack of conditions that allowed the chain of events to occur in the first level. In the third level are weaknesses that not only contributed to the accident being investigated but also can affect future accidents. Factors in the third level are called the "root" causes of the accident and they affect general classes of accidents[21]. The root causes are divided into three categories: (1) deficiencies in the safety culture of the organization, (2) flawed organizational structures, and (3) ineffective technical activities. Flaws in the safety culture are seen as arising from: (1) overconfidence and complacency, (2) a disregard or low priority for safety, or (3) flawed resolution of conflicting goals. The priority for safety must be maintained by the formal and informal rules of the organization.

The Management Oversight and Risk Tree (MORT) model also is an expansion of the basic chain-of-events model. MORT was developed by Johnson[22]. He argued that simple chain-of-event models failed to recognize the role of purpose, goal, performance, and supervisory control and intervention. MORT is based on fault trees and is essentially a detailed accident investigation checklist. The factors involved in the accident are arranged in a tree diagram and accompanied by lists of criteria used to evaluate the performance of the steps necessary to complete a process. MORT is also based on the belief that unwanted transfers of energy due to a lack of barriers or controls cause accidents. In MORT accidents can come from two sources (1) specific job oversights and omissions and (2) the management system that controls the job. MORT is one of most comprehensive chain-of-events models in that it provides a method of breaking down the accident scenario, it adds change factors to the basic energy model, and it includes non-simplistic causal factors such as actions of the management system.

3.2.4 Current Models Based on Systems Theory

In systems safety accidents are seen as resulting from the interactions among humans, machines, and the environment. Each element of the system is an interrelated part that affects the others directly or indirectly. Safety is seen as an emergent property that arises when the elements of the system interact with its environment. Accidents are seen as resulting from the coincidence of factors related to each other in the system and stemming from multiple independent events. Safety is maintained by constraining the emergent properties of the interaction of the elements. System safety models concentrate on the operation and organization of the system to establish the set of causal factors while the industrial safety models usually concentrate on unsafe acts or conditions in the system. Accidents are described in terms of dysfunctional interactions, control theory, or deviations and determining factors.

Dysfunctional interactions occur when the elements in the system interact in such a way as to violate a system safety constraint. Leplat[23] divided the dysfunctional interactions into two types (1) deficiencies in the articulation of subsystems and (2) lack of linkup between elements of a system. He asserts that accidents arise from flaws in articulating and coordinating the elements of the system. The operation of the entire system not only depends on the successful action of the elements but also the successful results of the interactions of the elements. He points out three problem areas: (1) boundary areas - where the functions of the boundary areas are poorly defined, (2) zones of overlap - where two or more elements exert influence on the same element, and (3) asynchronous evolution of elements - where changes in one element are made without an assessment of the resulting interactions with other elements. The other type of problem involves the lack of linkup between elements. Lack of linkup involves two or more elements of the system performing actions that are consistent with their own frame of reference but dysfunctional from a system perspective because the individual frames of reference diverge.

In control theory models, systems are seen as interrelated elements that are kept in a state of dynamic equilibrium with feedback loops of control and information. Accidents result when disturbances are not handled adequately by the control system. Control theory models concentrate on changes rather than energy flows. Changes in complex systems can produce unforeseen consequences because of a flawed understanding of the system. Since safety is not directly measurable, control theory models infer the level of safety by a systematic and analytic prediction based on indirect evidence.

Deviations are emphasized in system theory models. A deviation is when a measured value of a system registers outside of a norm that was planned, expected, or intended. According to Kjellan[24] accidents occur as a result of maladaptive responses to deviations. Determining factors are properties of the systems from when it was created and tend to be stable over time.

The main drawbacks of current systems theoretic models are in their implementation. While the models themselves are based on systems theory, the techniques used to implement them are based on analytical versus synthetic investigative processes.

3.3 Classic Model Based Techniques

The current accident investigation models based on systems theory are the most comprehensive but are also the least well developed and understood. Current system-theoretic models still concentrate on analysis of causality rather than synthesis. They usually miss the factors that involve the interaction of the system's elements. Classic models can provide a reasonable explanation for what happened during and leading up to an accident but they don't necessarily provide the reasons why causal factors were allowed to emerge. Classic models tend to concentrate on a single phase of the system's life cycle and usually ignore the management and organizational factors that bring about the various causal factors. The following section introduces an enhanced systems-theoretic model to be used in accident investigation. It excels in the two major areas that classic models are deficient. First, it utilizes a system-theoretic context that explains accidents in terms of violating system safety constraints by utilizing synthesis rather than analysis. Secondly, it provides a framework to categorize the process failures and dysfunctional interactions that ultimately lead to an accident. The categorization will enhance the efficiency and effectiveness of reoccurrence actions.

3.4 STAMP Model Overview

In the STAMP framework, accidents occur when the safety control structure, which includes management functions fails to adequately handle external disturbances, component failures, and dysfunctional interactions among system components. Constraints imposed on the reactions of the system to the external disturbances, component failures, and dysfunctional interactions rather than events become the most basic concept in accident investigation. The system is required to achieve or maintain its goals and values while staying within the imposed safety constraints.

Accidents are viewed with respect to the failure of the system to properly impose safety constraints during design, development, operations, and maintenance of the system. The causal factors leading to an accident are described in the context of an adaptive feedback function. The control flaws leading to hazards are: (1) inadequate control actions, (2) inadequate execution of control action, (3) inadequate or missing feedback. Accidents occur when the system violates a safety constraint or the system finds itself in an unsafe state not addressed by the established safety constraints[26].

3.4.1 STAMP Implementation

The process starts with the system and subsystem model definition. It is first defined temporally by phase and then hierarchically according to the systems-theoretic structure. Then by phase, each level of the hierarchy is examined for physical component or process failures as well as dysfunctional interactions among components or personnel. The examination is done with respect to whether the failures or dysfunctional interactions were the result of inadequate enforcement of safety constraints, inadequate execution of processes that maintain the system within the safety constraints, or inadequate or missing feedback. Synthesis of the reasons for the accident proceeds from the output of the analysis of the causal factors that were the result of flawed control actions.

The generic procedure consists of:

1. Construct a system-theoretic model of the hierarchical control structure
2. Identify command and response carriers
3. Identify system hazards and the system safety constraints that were violated

4. Identify component and process failures as well as dysfunctional interactions

5. Categorize the control flaws as: (1) inadequate control actions, (2) inadequate execution of control actions, (3) inadequate or missing feedback.

6. Summarize and draw conclusions as to why the accident happened and propose corrective actions to prevent reoccurrence.

3.4.2 System-Theoretic Model for the Loss

Construction of the system-theoretic model is the most fundamental step. The definition of the system depends on the level and type of analysis being performed. The system in this case consists of both the hardware and organizational components as they progress through their entire life cycle. The overall system modeled consists of two fundamental structures. The first is the life cycle phases. The second is the hierarchical control structure. Each structure is specific to the situation being studied. It makes sense to aggregate elements of the overall system into functionally related groups within a hierarchy. The model can be developed to any level of detail desired. It is important to go to the depth for which there is control of the interactions. To go further would unnecessarily increase the combinatorial complexity of the investigation. The model of each system developed in this thesis used for accident investigation provides a multi-dimensional representation of the systems under investigation.

The phases used in the model developed for this thesis consist of design, fabrication, operations, and maintenance. The phases are defined below and a generic model illustrating the relationships between phases and levels is contained in figure 3-1.

Design includes all of the activities that precede physical construction of end product hardware (i.e. physical mockups and models used in feasibility studies). Chief among these activities is that of defining the purpose, gathering support, architecting and detailed design. The design phase does not necessarily end before the fabrication phase starts. In fact the design function may continue until the end system is removed from service.

Fabrication consists mainly of those tasks that are associated with construction and development (which includes verification and validation testing activities) and can proceed after the designers specify the components or elements to either build or buy. The tasks can be for one specific product or for mass production.

The operations phase consists of all the activities associated with operating the overall system.

Maintenance includes those activities that keep the overall system working nominally or that upgrade some facet of the system's performance.

The hierarchical decomposition is somewhat more difficult to do and is just as critical than the phase decomposition.

Aerospace hardware systems are known for being complex. The organizational complexity that surrounds the hardware is less well understood and far greater than for the hardware. In general, the hardware can be separated into facility, interface, and test article elements. In any case, there are multiple organizations involved with each hardware component as well as with the testing services performed. Each organization contains its own management structure. Some companies contract out most of their hardware development projects. Some companies act as the organization that integrates the components into the final system and in other cases they also contract out the hardware integration function. This functional division of duties is at times driven by political alliances rather than actual functionality of the hardware. The resultant organizational structure could become unwieldy to model without system theory principles that allow for more desirable system boundary definitions. For this thesis the hierarchical sub-system boundaries were chosen to minimize the complexities involved with contracted relationships. The relationships above are modeled in figure 3-1. The block labeled "P" is the prime control organization within each specific element of the system. The "X" and "Y" blocks represent other organizations within the same phase and level.

Level 0 consists of test article hardware. In most cases the majority of the time sensitive hardware actions and interactions are coordinated by an automated controller. The level 0 actions and interactions are coordinated internally and constrained by nature and the level 1 (operators) in the hierarchy above it. Level 0 and subsequent levels all interact with their environment. They both affect and are affected by it.

Level 1 consists of the organizations (across all of the phases) that are responsible for manipulating the physical hardware and its designs. It is the first level of personnel involved in the system. Their actions and interactions produce the designs and hardware as well as operate and maintain the system. The actions and interactions are coordinated internally by individuals in lead roles within the system and are constrained by the requirements of the system and the level 2 (managers) in the hierarchical level above. Level 1 implements control actions on level 0 and gets resultant emergent property response (or indications of it) from level 0 via the feedback system. The commands given are generally related to manipulation of the physical system (design or hardware) and the responses are related to the system's performance (or lack thereof).

Level 2 consists of the managers and supervisors. In this thesis, the project manager is responsible for overseeing the project. In some smaller projects, that project manager may be responsible for all phases of the system life cycle. The actions and interactions in level 2 are coordinated by individuals that are responsible for performing the various tasks in level 1. Level 2 implements control actions and receives feedback from level 1. Commands given are related to physical system, service, or operational requirements. The responses are generally system status and problem reports as well as inputs to project planning (design) documentation.

Level 3 consists of corporate management responsible for providing direction, guidance, and resources to the levels below it. Usually managers oversee multiple projects in various phases at any one time. Corporate management must deal with the emergent properties resulting from the interactions of personnel in level 2. Control actions implemented at level 3 on level 2 are related to direction and authority to proceed. The responses are generally system status and inputs for programmatic documentation.

Level 4 consists of regulatory agencies and legal systems of the Federal government (in the United States). Personnel at this level are public servants of the government and lawyers for the legal system. They enforce the laws enacted above them and the procedures developed at their level. Control actions are implemented from this level by the implementation of regulatory requirements and responses are compliance documentation.

Level 5 consists of the Federal Government (in the United States). They create laws that constrain the actions of the regulatory agencies to act in the public good. This thesis does not cover aspects of levels 4 and 5. The Federal Government is responsible for setting the agenda for public causes. It issues control actions by executive action and legislative constraints by laws. The responses are provided by level 4 as non-compliance audits.

The hierarchy obviously extends to the Agency, Regulatory, and Federal Government levels. They are not included here because of lack of information provided in the accident reports used. A more thorough investigation would include the upper levels.

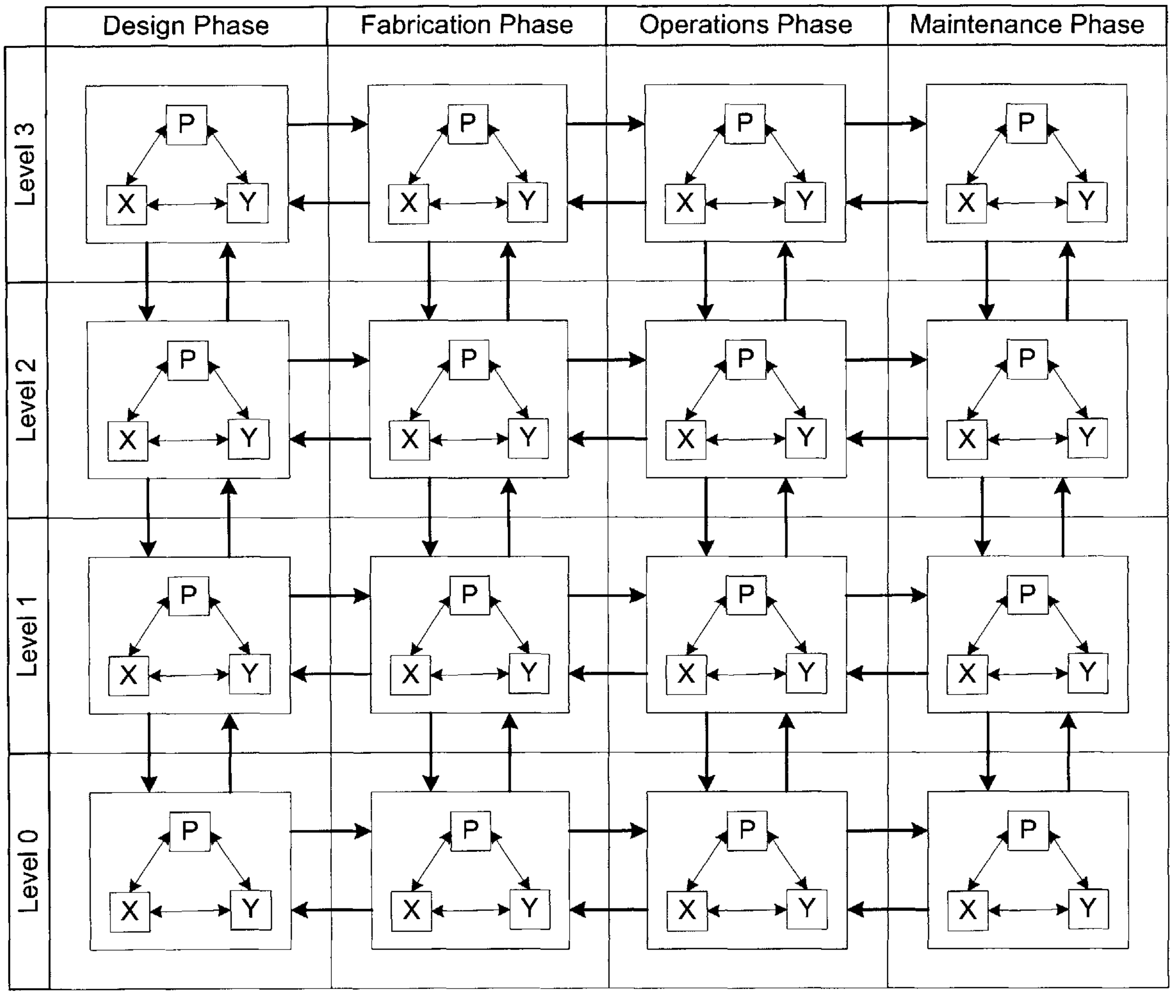

Figure 3-1. Generic Level and Phase Illustration

3.4.3 Hierarchical Interactions

Identification of the command and response carriers starts with describing the interactions between the levels of the hierarchical system-theoretic structure. Command carriers are those devices or processes that are used to transmit commands from a higher to a lower level in the hierarchy. Response carriers are the devices used to transmit feedback response to an upper level in the hierarchy. The same devices may be used internal to each level of the hierarchy also depending on the system model structure. The number of possible interactions between and among levels and phases will rise at an ever-increasing rate as the number of organizations involved increases. Luckily, the number of organizations involved in most projects is usually limited and their number further decreases at the upper levels of the hierarchy.

3.4.4 Identification of System Hazards

It is important to identify all the system safety hazards. Finding all of the hazards in a system requires a great deal of effort. The following hazard identification heuristics are a partial listing from P.L. Clements System Safety Scrapbook[27]:

- Conduct physical inspections / examinations
- Conduct real or simulated operational walkthroughs
- Consult with / interview current or intended system operators and maintainers
- Review historical evidence.

Leveson developed an extensive list of heuristics in Safeware[2]. Two of the accidents investigated in this thesis were the result of a contamination hazard when Foreign Object Debris (FOD) was inadvertently trapped in the test hardware.

3.4.5 Identification of System Safety Constraints

System safety constraints specify those relationships between system variables that constitute the non-hazardous system states[1]. The system safety constraints are based on the hazards faced by the system being investigated. In general they are related to the physical laws of nature, organizational implementation policy, operations policy, corporate policy, presidential policy, and laws. An example of a physical constraint is; tubing, lines, and duct connections must not leak.

3.4.6 Flawed Action and Dysfunctional Interaction Investigation

The following section describes an approach to finding the component and process failures as well as dysfunctional interactions involved in an accident from a systems-theoretical perspective. The actions and interactions are investigated in and between each level (Hardware, Controller, Management), with respect to each phase (Design, Fabrication, Operations, and Maintenance)[28]. A graphical depiction that also implements a numeric categorization of flawed action and dysfunctional interactions is contained in figure 3-2.

Inadequate implementation of safety constraints can occur because hazards are not identified (therefore constraints not identified) or because the control actions do not adequately enforce the constraints. Control actions may not adequately constrain system behavior due to flawed control algorithms, inconsistent or incorrect process models used by the control algorithms, or by inadequate coordination among multiple controllers and decision makers. Control algorithms may not enforce constraints because of flaws in the control algorithm when it was designed, one or more processes change without an appropriate change in the control algorithm, or one or more processes are changed incorrectly. There may be an inconsistency between the process models used by controllers and the actual process state. The process model (mental or software model) could have been created incorrectly, the process or the model can drift, or there can be time lags and measurement inaccuracies that were not accounted for. Multiple controllers can produce control actions that are inadequately coordinated or even conflicting.

Inadequate execution of control action can occur because there is a failure or an inadequate transmission of control commands or in their execution. A flaw in the communication, inadequate actuator operation, or a time lag that is not accounted for can cause the failure or inadequacy.

Inadequate or missing feedback can occur because there is a failure or inadequacy in the transmission of feedback information. The failure or inadequacy can be caused by failing to provide for it in the initial design, a flaw in communication, a time lag that is not accounted for, or inadequate sensor operation. A basic principle of systems theory is that no control system can perform better than its feedback channel.

3.4.7 Reasons for the flawed control actions and/or dysfunctional interactions

Very few projects suffer from all the possible failures explored above. Reasons for the dysfunctional interactions and flawed control actions within and between levels are described by the category they fall into. The system-theoretic control loop categories are: (1) inadequate control actions, (2) inadequate execution of control action, (3) inadequate or missing feedback. The specific categories utilized in this thesis are as follows:

1. Inadequate control actions

    1.1 Unidentified constraints

    1.2 Inappropriate, ineffective, or missing control actions for the identified constraints

        1.2.1 The design of the control algorithm does not enforce the constraints

            1.2.1.1 Flaw(s) in the creation process

            1.2.1.2 Asynchronous evolution between the control algorithm and the physical process

            1.2.1.3 Incorrect modification or adaptation of the control algorithm

1.2.2 The process model(s) are inconsistent, incomplete, or incorrect

1.2.2.1 Flaw(s) in the creation process

1.2.2.2 Asynchronous evolution between the process model and the physical process

1.2.2.3 There are time lags and measurement inaccuracies that are not accounted for

1.2.3 There is inadequate coordination among controllers and decision makers

1.2.3.1 Boundary coordination

1.2.3.2 Overlap coordination

2. Inadequate execution of control action

2.1 There is a communication flaw

2.2 There is ineffective actuator operation

2.3 There are unaccounted for time lags

3. Inadequate or missing feedback

3.1 Feedback is not provided for in the system design

3.2 There is a communication flaw

3.3 There are unaccounted for time lags

3.4 There is inadequate sensor operation

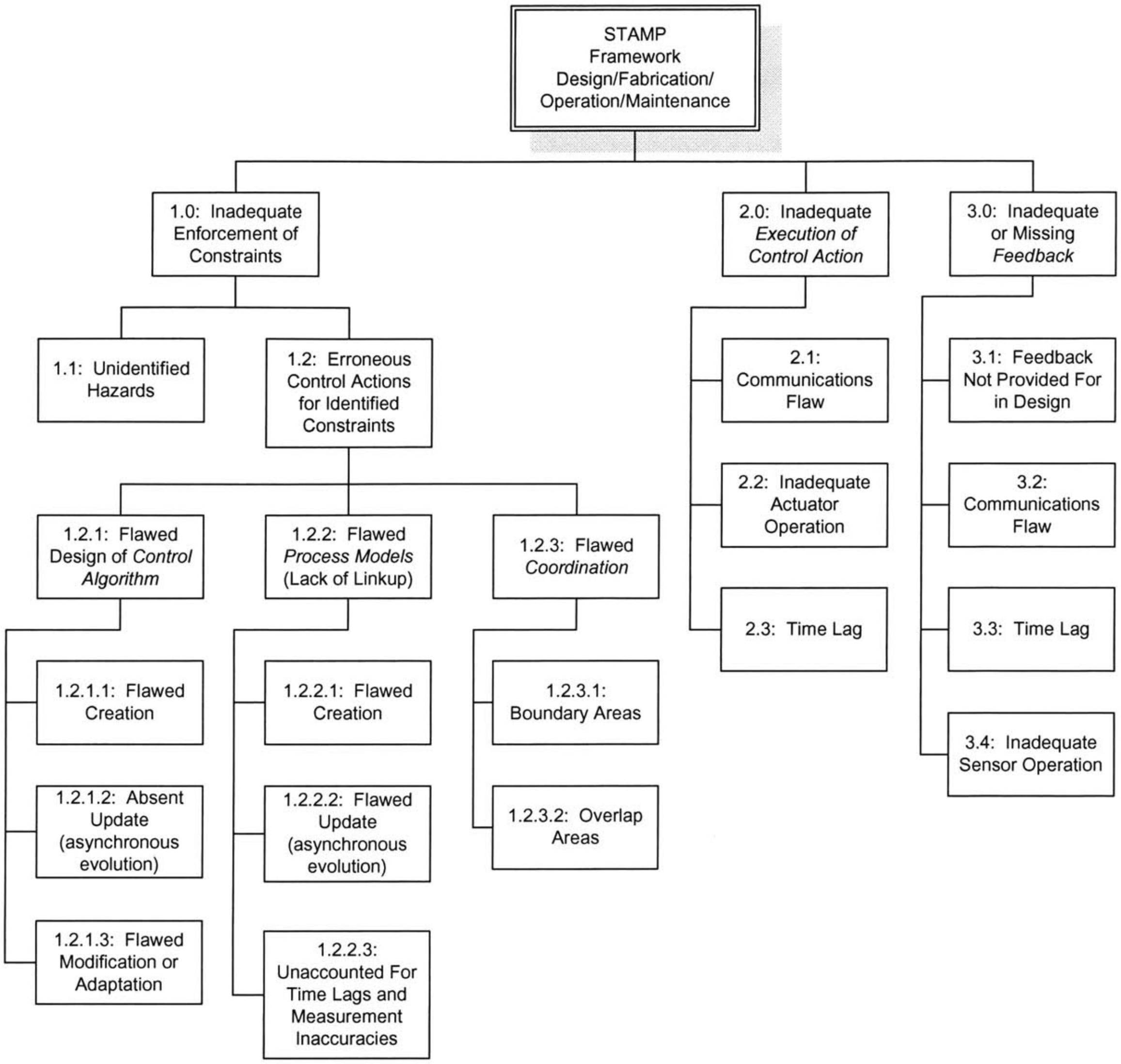
STAMP Framework Design/Fabrication/ Operation/Maintenance
1.0: Inadequate Enforcement of Constraints
2.0: Inadequate *Execution of Control Action*
3.0: Inadequate or Missing *Feedback*
1.1: Unidentified Hazards
1.2: Erroneous Control Actions for Identified Constraints
1.2.1: Flawed Design of *Control Algorithm*
1.2.2: Flawed *Process Models* (Lack of Linkup)
1.2.3: Flawed *Coordination*
1.2.1.1: Flawed Creation
1.2.1.2: Absent Update (asynchronous evolution)
1.2.1.3: Flawed Modification or Adaptation
1.2.2.1: Flawed Creation
1.2.2.2: Flawed Update (asynchronous evolution)
1.2.2.3: Unaccounted For Time Lags and Measurement Inaccuracies
1.2.3.1: Boundary Areas
1.2.3.2: Overlap Areas
2.1: Communications Flaw
2.2: Inadequate Actuator Operation
2.3: Time Lag
3.1: Feedback Not Provided For in Design
3.2: Communications Flaw
3.3: Time Lag
3.4: Inadequate Sensor Operation

Figure 3-2. System-Theoretic Flaw Categories

3.5 STAMP Comparison

STAMP is more of a radical new way of combining existing ideas than a radically new idea in itself. Most if not all of the elements of STAMP are contained in current accident investigation methods. The major difference is that STAMP is a true application of systems thinking. Some of the current methods are based on systems theory but fall short of implementing the concept of constraining emergent properties. They tend to concentrate on analysis — the decomposition of the system rather than on synthesis — the combining of the actions and interactions of the system elements that create the emergent properties. Current methods do not lend themselves to systemic improvement by providing categorization of causal factors as STAMP does. The STAMP technique assists in actively and systematically finding defects in materials as current methods do but also is effective in finding defects in actions as well. The defects are investigated using a systems-theoretic based process at each level of the control hierarchy. A defect is where a system attribute has drifted past a constraint or the constraint has shifted leaving the system attribute outside the limits of the constraint.

3.6 STAMP Implementation Utilized

The STAMP framework can be utilized in different ways. It can be used "bottom-up" to address a failure from all relevant information available and then used to draw conclusions. Due to time, resource, and space restrictions, this paper utilizes the STAMP framework from the perspective of the conclusions in the official mishap reports. Each conclusion is addressed relative to why the failure or dysfunctional interaction was allowed to occur from the perspective of the STAMP framework.

Ch-4: STAMP Accident Investigation

4.1 Introduction

This chapter implements the new systems-theoretic safety analysis technique for determining complex system mishap causality outlined in the previous chapter. It starts by first creating a generic systems-theoretic model for all three systems to be investigated. The generic model developed in the first part of this chapter is tailored to each individual accident investigation performed. The chapter then provides a summary of the findings from the three accidents where the technique was applied.

4.2 NASA Organizational Structure

NASA is a Federal agency that provides Americans with the science, technology, and operations needed to understand and explore the furthest reaches of space and to use the vantage point of space to understand and improve life on Earth. It provides data and information to scientists and engineers; advanced software and hardware concepts and systems to governmental, academic, and commercial endeavors; and educational expertise and materials for all levels of formal and informal learning communities worldwide. The Agency's primary areas of endeavor are space science, Earth science, biological and physical research, human exploration and development of space, and aerospace technology[29].

NASA is entrusted with tremendous public assets in the form of earth and space research infrastructure. High-risk missions have the potential for harming personnel and damaging high-value assets. Some missions take many years and can make up a significant portion of a researchers overall career. NASA has a responsibility to all of its stakeholders in supplying safe and reliable services.

NASA's core structure consists of a headquarters in Washington, DC; 10 Field Centers located in Maryland, Virginia, West Virginia, Florida, Ohio, Alabama, Mississippi, Texas, and California; and various facilities across the Nation. The Agency has a workforce of approximately 18,000 full time civil service employees, supplemented by academic and commercial contractors, and has a budget of approximately $14 billion[30].

4.2.1 General System-Theoretic Model

The following is a description of the general model structure. It includes the elements involved, their relationship to each other, and the interactions within and between each level. The composition of each level is somewhat arbitrary as with any systems definition. The structure is aggregated on a functional basis where like functions are placed in the same level. It is broken into design, fabrication and operations phases.

4.2.2 Hierarchical System Model

The first major complication in the hierarchical system model structure is the contract relationship that NASA maintains with academia and industry. NASA has contracted out a significant portion of all of its programs almost from its origin. Contracting enabled them to complete the Apollo Program given the strict time constraints. Relying on outside researchers and technicians to complete the Apollo program was a key and controversial decision. Some within NASA believed that relying on contractors would result in a loss of control. Others believed that it was the only way to quickly achieve the goal[31]. The numbers of personnel involved has decreased significantly from their peak but the inter and intra organizational complexities still remain.

Using a program management concept, NASA successfully demonstrated a way to manage complex elements in a multifarious task to successfully achieve a goal. There are three critical factors in conventional program management. The three factors are cost, schedule, and performance. These factors are interrelated and must be managed as a group. It was traditionally believed that if the program manager held one factor constant that at least one or both of the others would be adversely affected[32]. NASA is in the midst of a change to a Faster, Better, Cheaper (FBC) paradigm that maintains that cost, schedule, and technical performance can all be improved simultaneously. This change has added a new dimension of complexity as organizations have asynchronously adapted to the new paradigm.

A hierarchical system model based on the generic one developed in chapter 3 is shown in figure 4-1. The following labels were applied to each level of the hierarchy:

Level 0: Hardware
Level 1: Operator
Level 2: Project/Product Management
Level 3: Program/Corporate Management

Level 0

The physical hardware is at the lowest level. In this case, it is comprised of the test facility (TF), special test equipment (STE), and a test article (TA).

Design

The design consists of drawings, models, and other design documentation used to describe the hardware. The design is developed with the intent to be specific enough for the fabrication engineers to procure parts and assemble it, operations engineers to operate it, and maintenance engineers to maintain and upgrade it.

Fabrication

Buildup consisted of receiving parts shipped from vendors, assembling them into a completed stage, performing post manufacturing checkout tests, and then shipping the hardware to the test site.

Operations

Operations consisted mainly of providing propellant to the hardware to be tested and then operating the test article in a simulated operational environment.

Maintenance

Maintenance includes those activities that keep the overall system hardware working nominally or that upgrade some facet of the system's performance.

Level 1

The next level up in the hierarchy contains the "operators" of the hardware. They are the personnel that create the designs, assemble the hardware, and operate the physical system. It is their function to control the physical actions and interactions of the hardware in level 0.

Design

Architects and engineers in the first level of the organizational control hierarchy carry out the design function. The output of this function resides in the level 0 design package. It is created within the constraints levied from level 2 and usually with input from other functions residing in level 1.

Fabrication

Organizations responsible for procuring and assembling components can begin their functions once the designs have stabilized.

Operations

Operational use of the system can begin once the product is assembled and checked out.

Maintenance

Maintenance personnel perform those activities that keep the overall system working nominally or that upgrade some facet of the system's performance.

Level 2

The next level up the hierarchy is that of project management. It consists of the personnel that are responsible for directly supervising personnel or managing portions of the project. It includes project management, functional management, supervisors in matrix organizations as well as managers of support functions like finance and personnel.

Design

Design management ensures designs are created within budget, schedule, and technical requirements. They also ensure that the designs do not violate established and accepted management practices.

Fabrication

Fabrication management ensures that the hardware is assembled within budget, schedule, and technical requirements. They ensure that assembly of the hardware is performed according to established management practices.

Operations

Operations management ensures that test projects are executed within budget, schedule, and technical requirements. They also ensure that operations do not violate established management practices.

Maintenance

Maintenance management ensures that maintenance tasks that keep the overall system working nominally or that upgrade some facet of the system's performance are executed within budget, schedule, and technical requirements. They also ensure that maintenance tasks do not conflict with operational and other tasks.

Level 3

The next level up on the hierarchy is that of program, center, and corporate management. It consists of personnel that are responsible for ensuring that projects are selected and executed within the strategic framework of their respective domains.

4.2.3 Hierarchical Interactions

The complexity of the relationship between NASA and its contractors is further increased due to the difference in their organizational control structures. The contractors maintain a management structure that oversees the work that is directed by NASA. This hybrid matrix organization is also prevalent within NASA where workers are directed by a project manager but report functionally to a supervisor. These complexities can be modeled but are not for this thesis. The models in this thesis only consider the resultant interactions between these organizations and their environments.

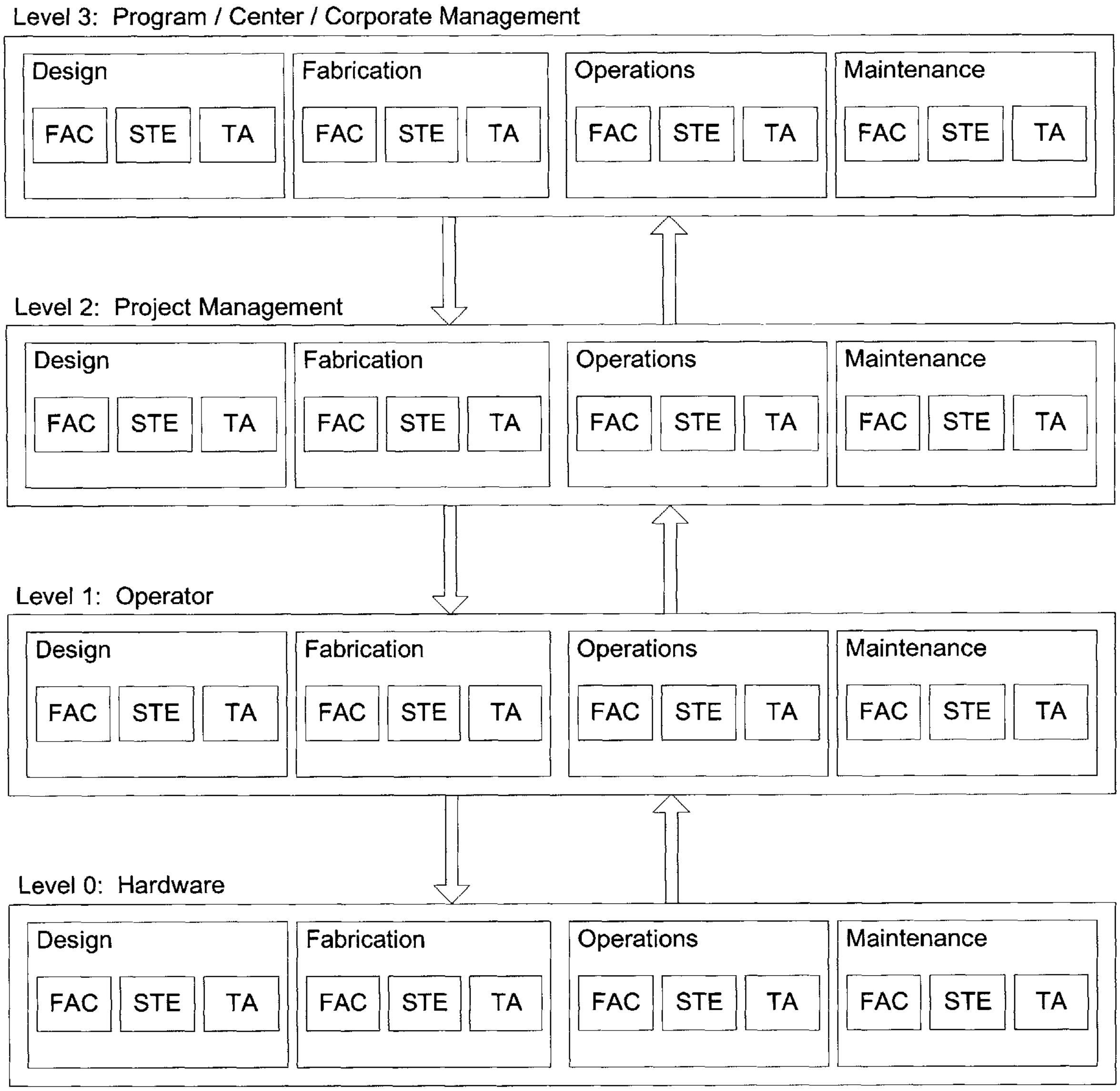

Figure 4-1. Generic System-Theoretic Model Diagram

4.2.3.1 Interactions between levels

The following is a description of the interactions between levels via "command" and "response" carriers. The interactions included in tables 4-1 through 4-4.

Design

Designs are validated and verified by the designers in coordination with other organizations in level 1 and are subject to the constraints emplaced by level 2 and above. Problems arise when designs are not adequately reviewed by other level 1 organizations or level 2 management.

Fabrication

Components of the system are procured and the fabricators construct the system. Buildup is validated and verified by the fabricators in coordination with other organizations in level 1 and subject to the constraints emplaced by level 2. Post buildup checks are performed to verify satisfaction of requirements. Problems arise when the hardware is not adequately reviewed by other level 1 organizations or level 2 management.

Operations

The hardware is operated within its environment and in coordination with organizations in level 1 and subject to the constraints emplaced by level 2 and above.

Maintenance

Maintenance includes those activities that keep the overall system working nominally or that upgrade some facet of the system's performance. The hardware is maintained within its environment and in coordination with organizations in level 1 and subject to the constraints emplaced by level 2.

Command and Response Carriers between the Environment and Level 0

Between Levels	Carriers	
	Command	Response
Level 0 & Environment	From: Level 0 To: Environment Physical Environmental Impact	From: Environment To: Level 0 Physical Environmental Impact

Table 4-1. Command/Response Carriers Between Levels 0 and its Environment

Command and Response Carriers between Levels 0 & 1

Between Levels	Carriers	
	Command	Response
Level 1 & Level 0	From: Level 1 To: Level 0 - Work Authorization Documentation including Emergency Response Procedures - Pre-Test Briefings	From: Level 0 To: Level 1 - Performance Data - Validation Data - Verification Data - As Built Configuration - Problems / Discrepancies

Table 4-2. Command/Response Carriers Between Levels 0 & 1

Command and Response Carriers between Levels 1 & 2

Between Levels	Carriers	
	Command	Response
Level 2 & Level 1	From: Level 2 To: Level 1 - Work Authorization Documentation Approval - Project Planning Documentation - Requirements Documentation - Management Instructions	From: Level 1 To: Level 2 - Open Item Status Report - Test Reports - Problem Reports

Table 4-3. Command/Response Carriers Between Levels 1 & 2

Command and Response Carriers between Levels 2 & 3

Between Levels	Carriers	
	Command	Response
Level 3 & Level 2	From: Level 3 To: Level 2 - Contract Documentation - Program Documentation - Strategic Direction	From: Level 2 To: Level 3 - Open Item Status Report - Test Reports - Problem Reports

Table 4-4. Command/Response Carriers Between Levels 2 & 3

4.2.3.2 Intra-Level Interactions

The difference in control structures between NASA and its contractors also affects the interactions within levels. The contractor operators in level 1 are an example of the systems engineering multi-containment principle. They are contained within and report to multiple systems. One is the NASA system and the other is the corporate system. Accounting for these interactions could lead to combinatorial explosion of interactions to be tracked. These complexities can be modeled but are not for this thesis. The models in this thesis only consider the resultant interactions between these organizations.

4.2.4 STAMP Investigation

The hierarchical model of the organizational structure developed above is specific to NASA programs. It is general enough that it applies to all three of the accidents investigated in this thesis. The zooming of the levels and the aggregation of the elements within each level was performed in such a way as to minimize the number and types of complex interactions that had to be addressed. The following section outlines the procedure and report format used in this thesis to investigate the three accidents.

4.3 Findings

Each mishap description is based on the generic model developed in the first part of this chapter. The hierarchical structure and interactions were basically identical for all three. There is a specific model tailored for each accident in the sections that follow. Other differences are noted in the each section below as required. Corporate and organizational identification information is masked to prevent divulging proprietary or information.

4.4 Mishap A

Mishap A occurred during a static test firing of a developmental component to be used in future rocket propulsion systems. The test series objective was to assess material performance properties. Post-test inspections revealed significant damage to the test article, special test interface hardware, and the test facility. There were no injuries. Based on the value of the hardware damaged, the mishap was identified as a Type C Mishap. The most significant aspects of this accident were that there were multiple organizations involved with hardware development and the operating organization failed to notice subtle clues from the system indicating that there was a problem. The project involved was a small scale, research oriented, short life cycle time, straightforward hardware development project.

The facility, equipment, and documentation used during this test project were not entirely new. Another hardware developer had just completed a very similar material test project using the same equipment. There were no major anomalous events during the earlier test project. The only major change since the previous test series was the test article. The new test article was developed by one organization to fit into the test rig of another per detailed design drawings.

The test article explosion occurred on the 12th test of the night. There was an abort during the first test of the night at 3 seconds due to an unrelated problem. The test before the incident lasted 120 seconds. Test durations for the night ranged from 10 seconds to 120 seconds. The planned duration of the 12th test was 120 seconds. The explosion occurred roughly 1 second into the test. The test facility and all related documentation and equipment were impounded immediately after the system was "safed" and secured.

The official report generally states that the incident was caused by detonation of the propellant that had leaked through the main facility propellant valve. It suggests that the conditions for that detonation were brought about by a failure of the designers and test crew to understand the physical and chemical properties of the propellant as well as the test crew either ignoring or missing the signs of a leak. The following STAMP investigation provides added insight as to why the accident occurred.

4.4.1 Hierarchical System Model

The hierarchical system model is shown in figure 4-2. The descriptions of the levels and interactions are consistent with the general case described earlier. The phases of interest for this investigation were the design and operations phases.

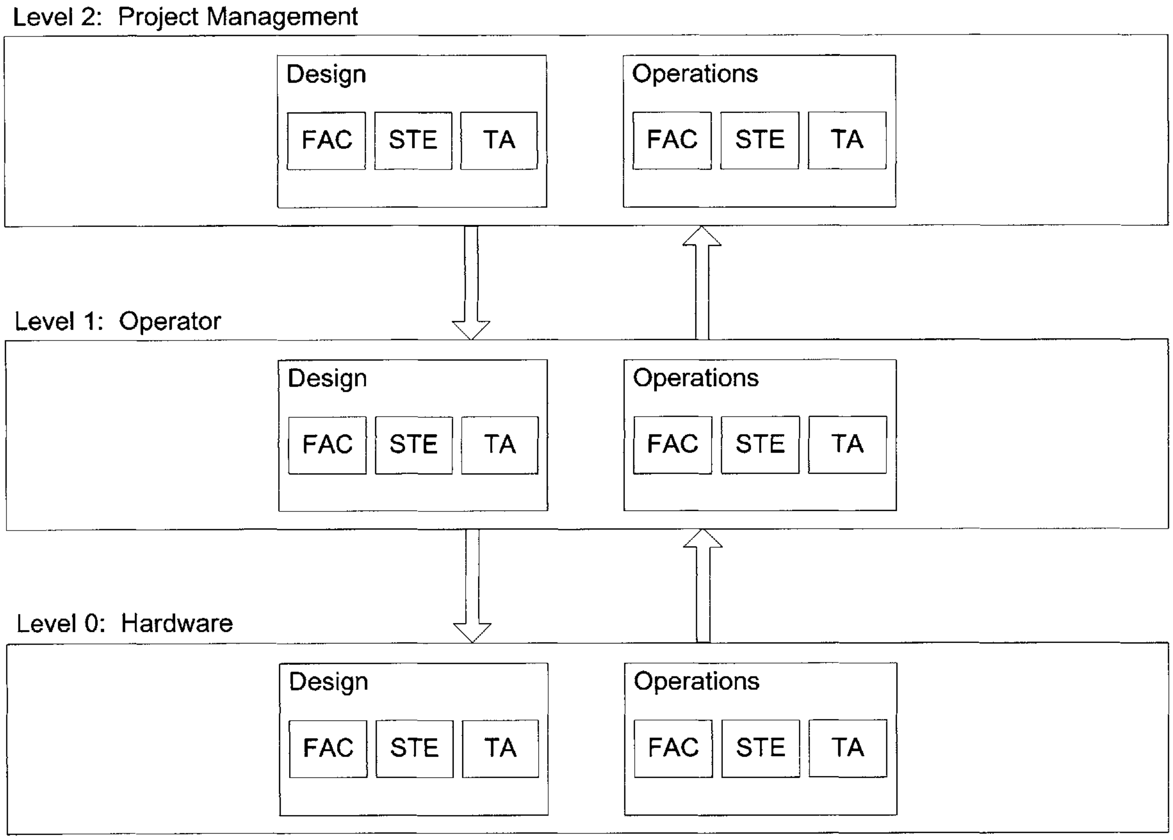

Figure 4-2. Mishap A Systems-Theoretic Model Diagram

4.4.2 System Safety Hazard

The system safety hazard that precipitated the accident:

> The uncontrolled exposure of propellant to a heat source while in a confined space — that resulted in an explosion.

4.4.3 System Safety Constraints

The specific system safety constraints that were involved with the accident are as follows:

1. Temperature of H2O2 must not exceed 212 deg F upstream of the catalyst bed.
2. Temperature of H2O2 upstream of the catalyst bed must be accurately measured.

3. Propellant valves must not leak.
4. Propellant valves that indicate leakage must be replaced promptly.
5. Tests must not be allowed to start given less than adequate system state parameters.
6. Test data gathered during emergencies and contingencies must be adequate to determine causality.

4.4.4 Flawed Action(s) or Dysfunctional Interaction(s)

The flawed actions and dysfunctional interactions are listed below by level within each phase. The numbering system from section 3.4.7 of chapter 3 is used to categorize each flawed action and dysfunctional interaction.

Design

Level 0:

1.2.2.3: The facility control and data systems used temperature probes located upstream of the test article mounted in the propellant flow stream instead of temperature probes mounted directly on the test article or its interface to the test rig for critical test readiness decision analysis.

Level 1:

1.1: The designers (and subsequently the test crew) were apparently not cognizant of the auto detonation characteristics of the propellant and hence did not hold test start for a test article temperature constraint.

3.1: Physical valve actuation sensing was not provided for the main facility control valve.

3.1: High-speed video or film records were not used for testing by the facility organization.

Operations

Level 0:

2.2: The main facility control valve developed a leak.

3.4: Pressure reading at time of incident pegged at 9,500 psig (was most likely much higher).

Level 1:

1.2.2.3: The test crew did not take into account that the temperature readings read high but were in fact higher due to the positioning of the temperature probes.

3.1: Video from facility camera indicated an internal leak of the main facility control valve either the test crew ignored or did not see it as a problem.

4.4.5 Flawed Control Actions

The following is a summary of the flawed control actions by level.

Level 0:

A facility valve developed a leak and did not adequately control the flow of propellant. Pressure sensors in the system went off scale and did not accurately measure the pressure spike during the explosion.

An explosion occurred and the hardware was damaged when the system did not keep the temperature of the propellant below the 212 deg F limit.

Level 1:

Designers of the system did not place the temperature probe for the test article in a position to accurately measure the test article temperature. The system also did not provide the test crew and facility control system with the sensor information that it did have.

Designers and operators of the system did not fully understand the physical properties of the propellant.

Designers of the system designed it to utilize the valve actuation command as an indication that the valve had opened rather than utilizing a physical valve position indication.

Valuable feedback data was not obtained due to the lack of adequate video or film recording of the event.

The bursting of the test article was the result of the valve containing propellant flow in conjunction with the test crew's lack of either noticing or taking action on the video and temperature data that indicated a problem.

4.4.6 Mishap A Summary

The STAMP investigation performed in this report corroborates the official report. The area that clearly needs attention is the development of adequate process models of the system by both designers and operations personnel in level 1 of the hierarchy. Hazards were overlooked and feedback was not received because either it was not looked for or it was ignored due to faulty process models. The managers in level 2 (project and line managers) failed to recognize the signs that the level 1 personnel were violating safety constraints. An example is that the lack of true valve position indication should have been resolved in design reviews. Management should concentrate on synchronously updating the process models with an added concentration in the identification of hazards as well as the fostering and accepting feedback. Level 3 managers did not provide facility assets that would have assisted greatly in the investigation of the mishap.

4.5 Mishap B

Mishap B occurred during a static test firing of one of the main propulsion units of a current launch vehicle. The propulsion unit was a unique developmental engine assembled for a specific series of tests. The test series objective was to demonstrate safe operation of the engine while a component underwent temperature variations. The objective of the first test of the series where the failure occurred was to characterize the engine's response to the throttling of a coolant control valve. Post-test inspections revealed significant hardware damage to the component under test. There were no injuries and the facility sustained no damage. Based on the value of the hardware damaged, the mishap was identified as a Type A Mishap. The most interesting aspect of this accident is that it was prompted by circumstances beyond the control of the operators. The emergency test termination actions were largely automated and performed as designed. The damage would have been reduced if the automation design had been updated. The project involved was a relatively large scale project, it is in operational mode, the hardware system was very complex, the system resides in a larger system which is more complex, and there were diverse organizations involved.

It is assumed that the facility preparations for the test proceeded nominally since the official mishap report did not go into great detail about them. The preparation for and the execution of a hot fire test are almost as complex as the engine itself. It takes many highly trained personnel to conduct a test. The test project is mature and stable. Along with the maturity have been process improvements and budget cuts. The process improvements have resulted in less personnel being required and the budget cuts have resulted in layoffs that reduce the number of personnel available. It is a continual struggle not to let the results of the budget cuts get ahead of the gains in efficiency from the process improvements. An imbalance as the result of a workforce reduction may have been present during engine fabrication.

The official report concludes that there was FOD in the propellant system, which caused hot gas to melt portions of the test article hardware, which then fell into the flow stream causing the destruction downstream. The FOD could have come from several different components. It was determined to be a piece of hardware that was supposed to be removed before the engine was assembled.

The STAMP analysis performed in this report corroborates the official report. The area that clearly needs attention is the development and maintenance of adequate control algorithms for the system by both buildup (fabrication) and operations personnel in level 1 of the hierarchy. The official report totally neglected the interactions at the project management level (level 2) and above. Their actions (or lack of action) are inferred from the flawed and dysfunctional actions that were allowed to occur in lower levels of the hierarchy.

4.5.1 Hierarchical System Model

The hierarchical system model is shown in figure 4-3. The descriptions of the levels and interactions are consistent with the general case described earlier. The phases of interest for this investigation were the fabrication and operations phases.

4.5.2 System Safety Hazard

The system safety hazard that precipitated the accident:

> Obstruction in the propellant system — that resulted in hardware damage.

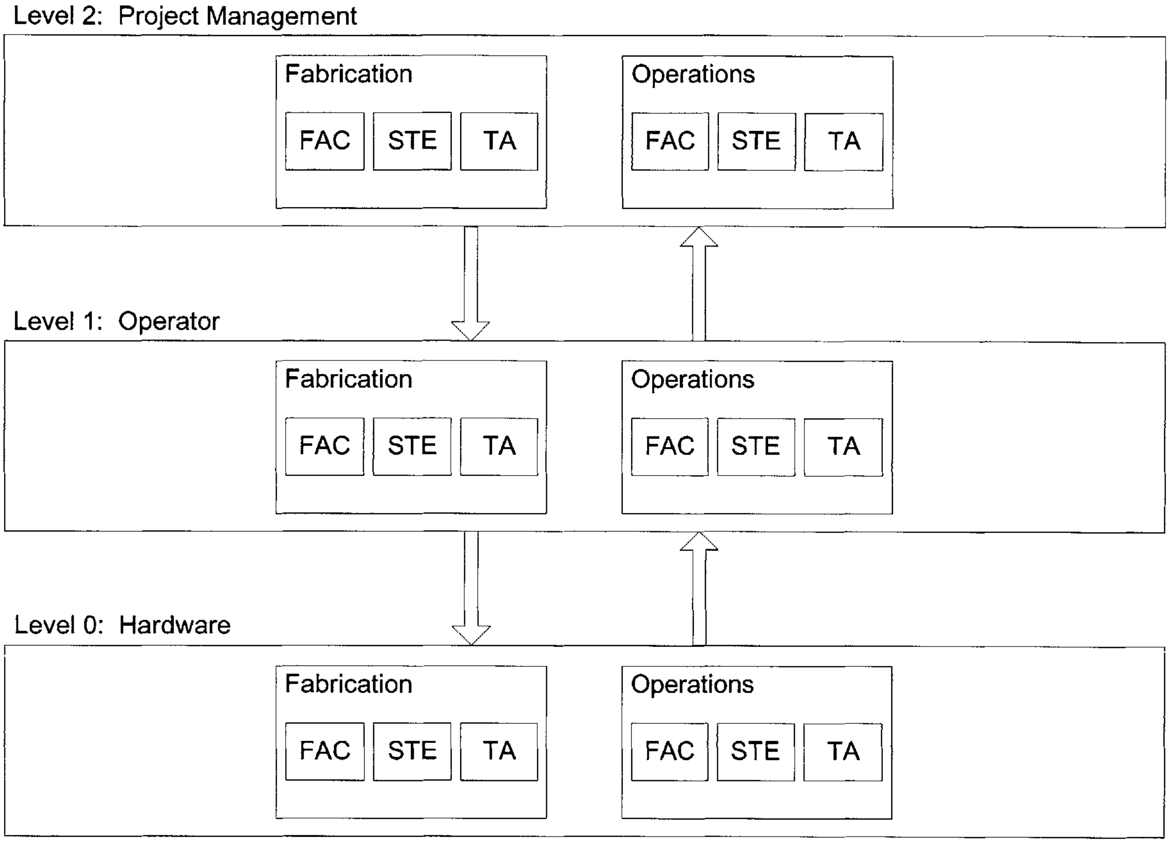

Figure 4-3. Mishap B Systems-Theoretic Model Diagram

4.5.3 System Safety Constraints

The specific system safety constraints that were involved with the accident are as follows:

1 Obstructions must not be allowed to enter or be trapped in tubing, lines, or ducts.

2: Acceptance testing must be capable of detecting if tubing, lines, or ducts are obstructed.

3 Acceptance testing must be capable of detecting if tubing, lines, or ducts are obstructed.

4. The intent of work authorization documentation must be unambiguous.

5. Configuration of all work authorization documentation changes must be maintained.

6. Constraints must be adapted as development progresses.
7. Components must be manufactured in accordance with design specifications.

4.5.4 Flawed Action(s) or Dysfunctional Interaction(s)

The flawed actions and dysfunctional interactions are listed below by level within each phase. The numbering system from section 3.4.7 of chapter 3 is used to categorize each flawed action and dysfunctional interaction.

Fabrication

Level 1:

1.2.3.1: Several organizations (within and between companies) were responsible for verifying that the debris dams were removed.

2.3: There was a time delay between when each of the suspect joints was inspected and when installation took place.

1.2.1.1: The serialization system for handling loose materials was not adequate.

1.2.1.1: Serialized debris dams were not used.

1.2.1.1: The assembly work authorization documentation could not have reflected loose material serialization due to the lack of loose parts being included in the serialization process.

1.2.2.1: There are incongruent mental models between those writing assembly procedures and discrepancy reports and those working to them.

1.2.1.3: Planning took an extended period of time which necessitated modification to the assembly sequence.

1.2.2.3: Planning took an extended period of time which left less time for assembly.

Operations

Level 0:

1.2.1.1: Debris in hardware caused localized high mixture ratio resulting in high temperatures, the localized high temperatures caused melting of hardware melting causing further damage downstream.

Level 1:

1.2.1.1: Pre-test checkouts were not designed to find blockage (they were designed as leak checks).

1.2.2.1: There are incongruent process (mental) models between those writing test procedures and discrepancy reports and those working to them.

1.2.2.2: A documented problem report was changed and record of the change was not recorded.

1.2.1.1: The test termination conditions were set during development and there was apparently no process put in place to readdress the timing.

1.2.1.2: The test termination timing should have been addressed as the start sequence got more predictable.

Level 2:

1.2.1.2: Management missed an opportunity to achieve an efficiency gain as the startup sequence became more predictable. Note: There is a balance between setting cut limits too close (which results in more unwarranted cuts - alpha error) and too loose (which results in not cutting when warranted - beta error)

4.5.5 Flawed Control Actions

The following is a summary of the flawed control actions by level within each phase.

Level 0:

The hardware did not safely absorb the induction of the protective hardware in the propellant system. It was not designed to do so and the condition was an accepted risk. Process controls had been in place to prevent FOD from entering the system.

Level 1:

The system allowed retention of FOD. This is an indication that the process controls did not work. It is likely that a boundary area emerged between shifts when there were time lags between when the joints were inspected and when they were mated.

Work authorization documentation lacked clarity in both the fabrication and operations phases.

Configuration control of work authorization documentation was not maintained.

The redline cut criteria were not updated as the program matured.

The system did not adapt to the perturbation in the planning timeline.

Level 2:

FOD related damage has been induced in tightly coupled rocket engine systems since their inception. Management in level 2 (and above) did not constrain the activities of the engineers, technicians, and quality inspectors in level 1.

Management did not take advantage of an opportunity for gains in efficiency by reducing the redline cut criteria.

4.5.6 Mishap B Summary

The majority of the improper actions in this system were the result of various aspects of inadequate control actions not enforcing constraints for known hazards. There were very few problems noted outside the lack of inadequate control actions. This seems inconsistent with the maturity of the program involved. It is likely that it is due to the lack of data in the official mishap report. If it is due to the maturity of the program, it could mean that there have been new or different personnel performing the work. New personnel could have less developed mental models of the task at hand. One possible explanation for having different personnel performing tasks is that downsizing had gotten ahead of process improvement gains. This thesis only stays within the scope of the official report, which only captures a small percentage of the possible problems in and with the project.

The only flawed action in the hardware was its inability to absorb the protective hardware that was left in the propellant duct. A hardware solution to this problem is unlikely given the unwillingness to invest funding to develop more robust hardware at a late stage in the programs life cycle. FOD is a known problem that has been addressed through process control from the beginning.

By far the most flawed actions were reported in level 1 of the operations phase and were the result of erroneous control actions for the identified constraints. The large percentage of flawed actions in level 1 were the result of the official mishap report concentrating its attention to the personnel and processes that constitute level 1. The apparent dysfunctional nature of level 1 must be controlled by level 2 which is not mentioned nearly as often as level 1. The improper formation of the control algorithm is one of the more significant aspects of the actions taken in level 1. This also seems inconsistent with the maturity of the program. New or different personnel performing standard tasks having inappropriate mental models rather than the established system being flawed can explain this observation. Next and related to the improper formation of control algorithms is that of the asynchronous evolution of the control algorithms. This may be another indication that downsizing has gotten ahead of efficiencies gained by process improvements. The one inadequate execution of control action within level 1 had to do with multiple operators believing that the others were going to ensure that the protective hardware was removed. The affects of the poor coordination were further exacerbated by a time lag in the system.

The lone noted flawed action in level two related to management's complacency in updating the emergency test termination requirements to take advantage of processes efficiencies gained through enhanced stability of the start sequence. If the test termination requirements had been tightened a majority of the down stream damage would not have occurred.

4.6 Mishap C

Mishap C occurred during a static test firing of one of the stages of a large launch vehicle. It occurred after there was substantial experience with testing the stage. The objective of the test was to satisfy flight acceptance testing requirements for the stage. Post-test inspections revealed significant hardware damage to the stage and the test facility. There were no injuries. The interesting aspects of this accident are that it was prompted by circumstances beyond the control of the operators and the response of the operators increased the damage. The project involved was a relatively large scale, was in an operational mode, the hardware system was very complex, and the stage project resided in a program which was tremendously complex.

The official mishap report concludes that the stage static firing incident was caused by the presence of a blockage in a fuel line to one of the engines. The presence of the blockage caused a fuel leak resulting in a fire that was ignited by the hot surfaces of the engine. The report established that the blockage was present from when the stage was originally assembled. The personnel responsible were aware that the blockage was not meant to be left in place. The official report concluded that the installation was not intentional. There was also significant damage done to the test article and the test facility as a result of the tests crew's response to the fire and subsequent automated cutoff. The majority of the report covers the severe breakdown in operational discipline. There were several instances where operations personnel did not react to the fire in an appropriate manner to terminate the test, suppress the fire, and properly safe the stage after the test was terminated. The official report does mention that the management of the operators bore responsibility for the actions of the operators.

4.6.1 Hierarchical System Model

The hierarchical system model is shown in figure 4-4. The descriptions of the levels and interactions are consistent with the general case described earlier. The phases of interest for this investigation were the design, fabrication, and operations phases.

4.6.2 System Safety Hazards

The system safety hazards that precipitated the accident:

An obstructed propellant line — that resulted in a leak.

The uncontrolled exposure of propellant to a heat source — that resulted in a fire.

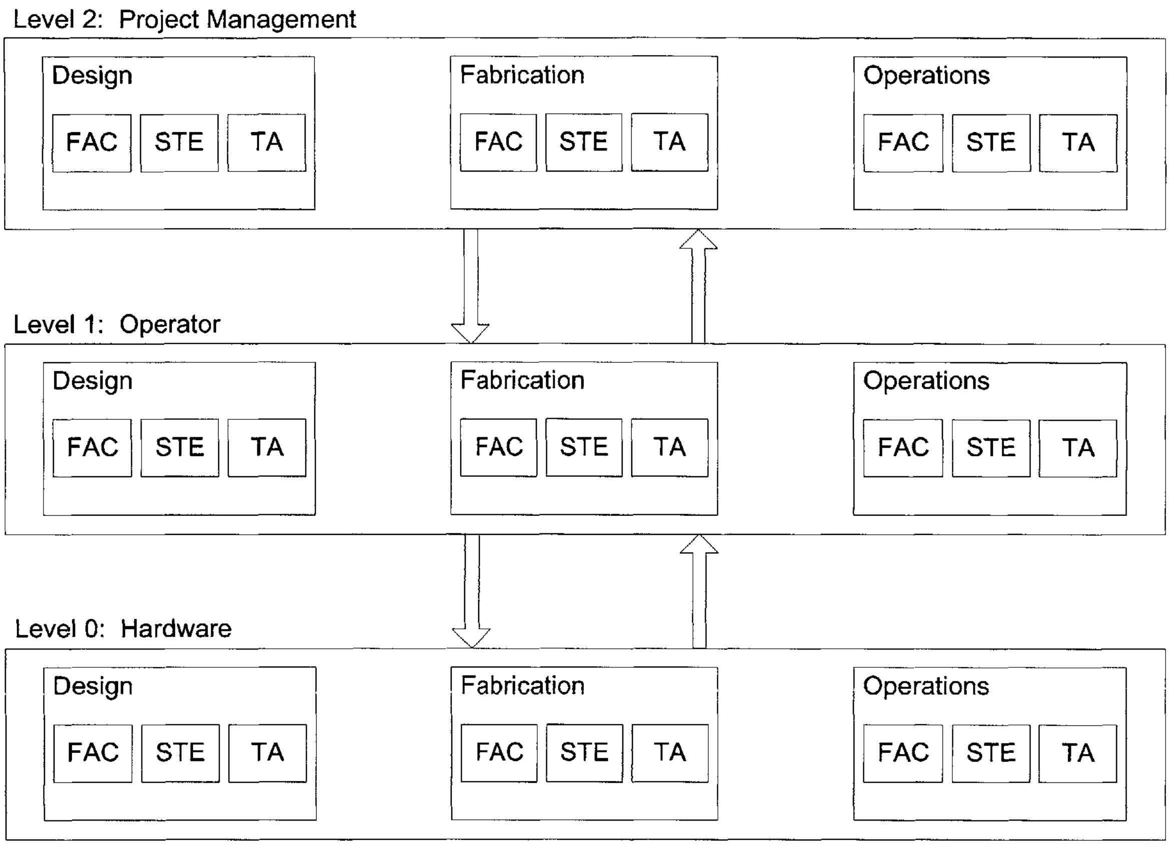

Figure 4-4. Mishap C Systems-Theoretic Model Diagram

4.6.3 System Safety Constraints

The specific system safety constraints that were involved with the accident are as follows:

1. Obstructions must not be allowed to enter or be trapped in tubing, lines, and ducts.
2. Acceptance testing must be capable of detecting if tubing, lines, and ducts are obstructed.
3. Tubing, lines, and duct connections must not leak.
4. Test crew must have immediate access to preplanned contingency procedures.
5. Test crew must have a preplanned process for handling unplanned contingencies for which there are no procedures.

6. System must not be configured such that conditions conducive to hardware damage are allowed to occur.

7. Personnel must be experienced and properly trained to control the system.

8. Corrective action (reaction) on the part of test crew must be accomplished in a timely manner.

9. There must be proper communication between organizations.

10. There must be continual oversight of organizations.

11. Management must understand the organizational capability and dynamics when transferring work from one organization to another.

12. Test crew personnel must be cognizant of the risks involved in high-energy systems.

4.6.4 Flawed Action(s) or Dysfunctional Interaction(s)

The flawed actions and dysfunctional interactions are listed below by level within each phase. The numbering system from section 3.4.7 of chapter 3 is used to categorize each flawed action and dysfunctional interaction.

Design

Level 1:

1.1: Blockage that results in a leak at an otherwise tight joint was an unidentified hazard.

1.2.1.1 Leak test was not designed to detect blockage.

1.2.3.1 Action of designers indicates that they thought the installation personnel were going to ensure removal of the flange protection hardware.

3.1 There is no indication that fabrication personnel tried to inform designers that installation of the protective hardware was even a possibility.

2.1: The design engineers did not fully update the test operations crew (via test engineering) what specific situations to avoid due to the possibility of geysering.

2.2: The design engineers did not make it impossible to configure the propellant system to keep it from geysering.

Fabrication

Level 1:

1.2.1.1: The flange protective disk remained in place when the duct was installed.

1.2.2.1: The procedure writer had never seen the physical work that he was planning.

1.2.2.2: Technicians were allowed latitude in the installation process allowing personnel to develop their own installation procedure.

1.2.3.1: The procedure writer left it up to the technicians and inspectors to ensure removal of protective hardware.

1.2.3.2: The technician, contractor inspector, and government inspector all relied on each other to catch missteps in hardware installation.

3.1: There was no logistical parts control for the shipping hardware following installation of the flight hardware.

1.2.2.1: The procedure writer wrote the procedures based on misconceptions of on how his procedures would be performed.

1.2.2.2: Technicians and inspectors were obviously interpreting the installation procedures differently.

3.1: There was no indication of a procedure update process (such as the one alluded to for the test procedures).

Level 2:

1.2.2.3: There was a time lag between the time the contractor inspector reported that he was overloaded and the assignment of additional inspectors.

2.2: Management didn't ensure that all personnel involved with assembly shared a common process model of how it should be performed.

Operations

Level 0:

1.2.1.1: The fuel line joint failed to contain the fuel.

Level 1:

1.2.1.1: The emergency test termination criteria allowed tremendous latitude in interpretation by observers.

1.2.1.3: The emergency test termination criteria were incorporated outside the normal change process for this test - they had not been contained within the procedure prior.

1.2.2.2: There was no sign from the test crew that they were concerned about the fire.

1.2.3.1: Observers with cut switches did not actively pursue cutting the test.

2.3: The test conductor did not appear to appreciate the time sensitivity of the conditions caused by the fire.

3.4: Test termination observers did not make calls indicating the fire was indeed causing a problem in their sub-systems.

1.2.2.2: Test operations had fully understood the basic geyser producing system configurations but did not utilize the knowledge during the incident.

1.2.3.1: Test engineering did not update or correct test operations during the test.

2.2: Test conductor assigned or allowed inexperienced personnel to operate in critical test positions.

2.2: Test conductor reassigned (and relocated himself) to critical positions in the terminal count phase of the countdown.

1.2.2.1: The test conductor (as well as the entire test crew) appeared to have a flawed mental model of what to do and how quickly to do it going into the test.

3.1: Lack of feedback to the test crew resulted in their mental models being flawed.

1.2.2.2: The test crew's perception of the risk involved with each test had degraded.

2.1: Test engineering did not communicate a concern about geysering.

Level 2:

1.2.1.2: Management allowed the test crew's overall experience level to decline.

1.2.1.2: Management lowed personnel to change positions late in the countdown.

2.2: There was no indication that management was enforcing procedural discipline with regards to emergency procedure preparation.

2.2: Test management did not ensure that test operations and test engineering actively integrated each other's process models.

1.2.2.2: Management had a flawed process (mental) model of how the test crew was performing.

2.2: Management did not adequately control the training of inexperienced personnel. This caused the test crew to assign whoever was available.

1.2.2.2: Management did not perceive the need to ensure that engineering and operations shared a common mental model.

2.2: Management clearly did not adequately control the process (mental) model generation process of the test crew.

1.2.3.1: Operations and engineering personnel had conflicting perceptions of who was in charge (of the procedure creation and update).

1.2.3.2: Operations and engineering personnel were both trying to control what was going on and their combined actions "confused" or misdirected the system.

3.2: There was evidence of poor communication between engineering and operations.

1.1: Management did not appear to understand that complacency could be a problem.

3.1: It is unclear if management was looking for or accepting feedback.

3.4: Observers of the test crew apparently did not communicate concern concerning complacency.

1.2.2.2: Management clearly had a flawed mental model of how the process was operating.

1.2.2.3: Management did not appear to understand that it took time for inexperienced personnel to come up to speed.

1.2.2.3: Management was unaware of the time scale in which low to medium probability evens can manifest themselves.

2.2: Management did not exercise adequate control over the test crew and its relationship with the test engineering group.

4.6.5 Flawed Control Actions

The following is a summary of the flawed control actions by level within each phase.

Design

Level 1:

Design engineers did not understand that a leak could develop in an otherwise tight joint if the joint is obstructed. They subsequently developed a leak test that was not designed to detect blockage.

The designers did not design the packaging and joints to prevent its installation within the mated joint. They also believed the installation personnel were going to ensure removal of the flange protection hardware.

The buildup personnel did not inform designers that installation of the protective hardware was possible.

The design engineers did not fully communicate to the test operations crew (via test engineering) what specific situations to avoid to prevent the possibility of hardware damage.

Fabrication

Level 1:

The buildup technicians did not remove the temporary flange protection hardware when the duct was installed.

The procedure writer did not obtain a true understanding of how assembly was carried out. He had never seen the physical work that he was planning. He allowed technicians latitude in the installation process allowing personnel to develop their own installation procedure. He also left it up to the technicians and inspectors to ensure removal of protective hardware.

There was no coordination among the technician, contractor inspector, and government inspector to ensure that at least one of them had performed their function.

Level 1 of the fabrication phase did not provide for a logistical parts control process for the shipping hardware following installation of the flight hardware.

Technicians and inspectors were obviously interpreting the installation procedures differently.

There was no indication of a procedure update process.

Level 2:

Fabrication management did not act quickly in giving the contractor inspector relief from being overtaxed.

Management did not ensure that all personnel involved with assembly shared a common process model of how it should be performed.

Operations

Level 0:

The duct joint did not contain the fuel.

Level 1:

The test operations did not clearly define and carry out the emergency test termination. There was no sign from the test crew that they were concerned about the fire. Observers with cut switches did not actively pursue cutting the test. The test conductor did not appear to appreciate the time sensitivity of the conditions caused by the fire. Redline cut observers did not make calls indicating the fire was indeed causing a problem in their sub-systems.

The emergency cut criteria were incorporated outside the normal change process for this test — they had not been formally contained within the procedure prior to this time.

Test operations had fully understood the basic geyser producing system configurations but did not use the knowledge during the incident.

Test engineering did not update or correct test operations during the test.

The test conductor assigned or allowed inexperienced personnel to operate in critical test positions and reassigned (and relocated himself also) to critical positions in the terminal count phase of the countdown.

The test conductor (as well as the entire test crew) appeared to have a flawed mental model of what to do and how quickly to do it going into the test. The lack of feedback resulted in a mental model that was flawed.

The test crew's perception of the risk involved with each test had degraded.

Test engineering did not communicate a concern about hardware damage.

Level 2:

Management was unaware of the time scale in which low to medium probability hazards can manifest themselves.

Management did not exercise adequate control over the test crew and its relationship with the test engineering group. Test management did not ensure that test operations and test engineering actively integrated each other's process models.

Management clearly had a flawed mental model of how the process was operating and did not appear to understand that it took time for inexperienced personnel to come up to speed.

Management did not understand that complacency could be a problem.

NASA observers of the test crew apparently did not communicate concern concerning complacency.

Operations and engineering personnel had conflicting perceptions of who was in charge (of the procedure creation and update). They were both trying to control what was going on and their combined actions "confused" or misdirected the system.

There was poor communication between engineering and operations.

Management clearly did not adequately control the process (mental) model generation process of the test crew. Management didn't perceive the need to ensure that engineering and operations shared a common mental model.

Management had a flawed process (mental) model of how the test crew was performing and did not adequately control the training of inexperienced personnel. This allowed the test crew to assign whoever was available.

Management allowed the test crew's overall experience level to decline and allowed personnel to change positions late in the countdown.

There was no indication that management was enforcing procedural discipline with regards to emergency procedure preparation.

4.6.6 Mishap C Summary

The level 1 designers of the propellant duct and its packaging did not fully understand the circumstances and conditions of how their hardware was going to be handled and installed. It is apparent from their not fully identifying all of the hazards involved. There is very little data in the official report concerning the design. The conclusions reached here are the results of the interactions of the level 1 fabricators during buildup.

The fabrication personnel in level 1 of the hierarchy did not form process models consistent with the physical process or the process models of others in level 1. The lack of an accurate process model led to inadequate boundary and overlap coordination conditions. There were cases of feedback problems that further exacerbated the process model problems.

There is not a great amount of detail on the actions of the level 2 fabrication personnel in the official report. There is an indication that the problems with the process models continued in this level of the hierarchy. Problems with the unaccounted time lags in assigning additional quality inspectors accentuated the problems with the flawed process models and may indicate that there were schedule pressure problems.

Most of the details in the official report concern the operations phase. While the official report concentrates on the actions of the personnel in level 1 it also includes data on the actions of the management personnel in level 2.

The initiating hardware failure that led to the fire was caused by the joint hardware not safely absorbing the presence of the protective hardware in the propellant system. The controllers in the next level higher did not notice that the leak check that they performed on the affected joint was incapable of detecting a blockage.

The most significant problem within level 1 of the hierarchy was the asynchronous evolution of the controller's process models. The next most significant was related to inadequate boundary coordination among controllers. These two problems are related in that personnel had differing mental models of the process that also affected the coordination between the controllers. Both of these problems were demonstrated in the fabrication and operations phases. In the fabrication phase they were demonstrated by how the procedure allowed for varying the assembly process and that 3 people missed removing the protective hardware thinking the others must have done or verified it. There were also communication flaws that resulted in the hardware to be configured inappropriately. Time lags were present in several instances. The most critical was the late action taken by the test crew to react to the fire. The test controllers in level 1 of operators that were supposed to monitor instrumentation for test termination constraints were acting as "sensors." As sensors they either did not understand that they were supposed to report the off-nominal conditions that their instrumentation was displaying or they chose not to report it for some other reason. One reason is that their understanding of what to report was different than the rest of the test crew's.

The level 2 managers in the operations phase faced many of the same problems as the personnel in level 1 below them. One of the two most significant problems at this level is with erroneous control actions for the identified constraints. Asynchronous evolution of management's mental models of the process in the hierarchy below them played a significant part in the accident. In the operations phase the managers appeared to believe that the test crew was gaining knowledge as they progressed from test to test when in fact new personnel were being introduced into the team and the experienced personnel were becoming complacent to the hazards they faced. The flawed process models on the part of management combined with unaccounted time lags in those models calls into question the assertion in the official report that schedule pressure was not a significant factor in the accident. There were also instances of inadequate boundary and overlap coordination. There were more instances of erroneous control actions for the identified constraints within this level than any other single factor in all levels. Most were related to the coordination actions of management such as allowing critical test crew personnel to change roles in time critical portions of the countdown.

At both the management and controller levels in each of the phases, it is readily apparent that personnel were forming poor process models (mental models) of the system (hardware and organization combined), which resulted in them not identifying hazards that led to flawed designs for enforcement of constraints. The flawed execution of control actions was more likely caused by trying to implement flawed actions than the actual control process being flawed. Unaccounted for time lags were a persistent problem throughout the overall process. The time lags and the feedback problems (which existed in all phases and in almost every level of each phase) were most likely the cause for the numerous incidences of asynchronous development of process models.

4.7 Investigation Summary

This chapter first established the general framework for investigating NASA propulsion test project accidents. The framework created is applicable to a wide variety of projects and programs within NASA with only minor adjustments in the system-theoretic model. Almost half of the problems in mishap A were the result of inadequate feedback. In mishap B, virtually all of the identified problems dealt with the inadequate control actions for the identified hazards. In mishap C, the vast majority of the flaws were also inadequate control actions for the identified hazards. The mishaps investigated were spread over several decades but demonstrated problems with the formation and development of process models and the control algorithms based on them. The encouragement and receptiveness of feedback needs to be addressed also. The next chapter provides a summary of the findings of this thesis as well as an overview of areas were a systems-theoretic framework may also be applied.

Chapter 5: Conclusion

5.1 Introduction

The objective of this thesis is to determine if applying the Systems-Theoretic Accident Modeling Process (STAMP) technique to accidents can provide better insight as to the reasons why the accidents occurred. This thesis assesses the viability in the use of a new technique in determining complex system mishap causality. First tailoring a systems-theoretic model for the system to be investigated and then applying the technique with the information available for the accidents accomplished the assessment. The technique proved viable when applied as a framework for classifying causal factors that led to accidents in complex aerospace propulsion systems. The analysis raised many questions that should have been addressed in the official accident investigations but apparently were not. The causal factors were then examined for trends. The results of this examination enable management intervention and recurrence control recommendations that focus on the most prevalent trends – conserving considerable resources and increasing effectiveness.

The STAMP framework is based on the hypothesis that a systems-theoretic feedback control loop can be used to identify what went wrong and provide categories of problems to be addressed by management. The STAMP technique provides a superior assessment of "why" an accident occurred as well as "what" exactly happened to the hardware. It focuses on the big-picture systematic view rather than assigning blame to the operators of the hardware that failed.

Follow on activities could include utilizing the information generated by STAMP investigation to provide a structured framework to enable and even enhance the learning from past mishaps. It can also be utilized to provide information for preventing mishaps, performing risk assessments, and monitoring performance.

5.2 Accident Etiology

Current accident investigation models based on systems theory are the most comprehensive but are the least well developed and understood. Current system-theoretic models still concentrate on analysis rather than synthesis of causality. They usually miss the factors that involve the interaction of the system's elements. Classic models can provide a reasonable explanation for what happened during and leading up to an accident but they don't necessarily provide the reasons why causal factors were allowed to emerge. Classic models tend to concentrate on a single phase of the system's life cycle and usually ignore the management and organizational factors that bring about the various causal factors.

The System Safety Scrapbook[34] presents a classification system for system safety tools. It splits the frameworks into two categories: (1) types of analysis that address what is analyzed or where within the system or when the analysis is carried out and (2) techniques of analysis, addressing how the analysis is performed. The techniques are further broken down into: (1) top-down, (2) bottom-up, (3) hazard inventory methods, (4) logic tree methods, (5) forward, and (6) backward. STAMP would be classified as: a technique that is a top-down, hazard inventory method that can be used as either forward or backward looking.

The following section provides a brief summary of the three accident investigations using the STAMP framework. The summaries show that accident investigation based on the STAMP framework excels in the two major areas that classic frameworks are deficient. First, it utilizes a system-theoretic context that explains accidents in terms of violating system safety constraints by utilizing synthesis rather than analysis. Secondly, it provides a framework to categorize the process failures and dysfunctional interactions that ultimately lead to an accident. The categorization will enhance the efficiency and effectiveness of reoccurrence control actions.

5.2.1 Report A

The official report totally neglected the interactions at the project management level (level 2) and above. Their actions (or lack of action) are inferred from the flawed and dysfunctional actions that were allowed to occur in lower levels of the hierarchy. It is not surprising that the STAMP investigation came to the same conclusion as the official report because the analysis done was limited to the data available in the official report. It is surprising that the official report came to the conclusions that it did from the information provided in the report. The official report gave an adequate description of what happened during the incident and gave good recommendations for how to correct the situation. It did not necessarily build the entire case as to what systemic changes were required to keep a similar incident from reoccurring. Nor did it go high enough in the organizational structure to identify the programmatic control actions that did not control the system at the "operator level" (level 1).

5.2.2 Report B

The majority of the improper actions in this system were the result of various aspects of inadequate control actions not enforcing constraints for known hazards. There were very few problems noted outside the lack of inadequate control actions. This seems inconsistent with the maturity of the program involved. It is likely that it is due to the lack of data in the official mishap report. If it is due to the maturity of the program, it could mean that there have been new or different personnel performing the work. New personnel likely have less developed mental models of the task at hand. One possible explanation for having different personnel performing tasks is that downsizing had gotten ahead of process improvement gains. Process improvement gains are realized, as the process becomes better understood over time. The problem arises when management counts on efficiency gains before they are realized and then reduces the labor force.

It is interesting to note that the official mishap report reported that 15 incidents of contamination problem reports were generated since 1980 that were the results of similar circumstances. The report goes on to state that 4 of the occurrences did not require recurrence control since the source of the contamination could not be identified or the contamination could not be retrieved for analysis. The discrepancy reports should have been used as feedback.

5.2.3 Report C

At both the management and controller levels in each of the phases, it is readily apparent that personnel were forming poor process models (mental models) of the system (hardware and organization combined), which resulted in them not identifying hazards that led to flawed designs for enforcement of constraints. The flawed execution of control actions was more likely caused by trying to implement flawed actions than the actual control process being flawed. Unaccounted for time lags were a persistent problem throughout the overall process. The time lags and the feedback problems (which existed in all phases and in almost every level of each phase) were most likely the cause for the numerous incidences of asynchronous development of process models.

The official mishap report describes what happened. It attempts to explain why it happened but only goes as far as to say that the controllers and their management were complacent and not effectively controlling the process. The STAMP analysis goes further by elucidating why the controllers and mangers were not in control. The official report's recommendations do effectively address the major issues as presented in the STAMP analysis. It is interesting that the mishap board was able to jump from what happened to how to fix it without fully explaining why it happened. By skipping over the analysis of why it occurred, it became very difficult to obtain true learning from the mishap personnel outside of those directly involved. The official mishap report concentrated on the level 1 operators but did expand their recommendations to include management.

The controllers and managers developed flawed individual mental models of the process that also asynchronously developed (degraded) over time. The official mishap report goes into detail on ways that the control actions were inadequate (at each level but mostly for the controllers and managers of the operations phase). This thesis points out that the flawed control actions on the part of management had more to do with the formulation and updating of the controller's mental models than on controlling the process. Feedback was inadequately used to assess the accuracy and consistency of individual mental models. The presences of time lags and their impact in the personal development of controller and management level personnel clearly contradict the official mishap report's assertion that schedule pressure did not play a significant role in the mishap.

5.3 STAMP Investigation Summary

The technique proved viable when applied as a framework for classifying causal factors that led to accidents in complex aerospace propulsion systems. The analysis raised many questions that should have been addressed in the official accident investigations but apparently were not. The causal factors were then examined for trends. The results of this examination could produce management intervention and recurrence control recommendations that focus on the most prevalent trends — conserving considerable resources and providing better effectiveness. Focusing on addressing the causal factors rather than isolated actions that led to the accidents also displayed promise in enhancing organizational learning.

The STAMP framework is based on the hypothesis that a systems-theoretic feedback control loop can be used to identify what went wrong and provide categories of problems to be addressed by management. Reasons for the dysfunctional interactions and flawed control actions within and between levels are described by the category and sub-category into which they fall. The system-theoretic control loop categories are: (1) inadequate control actions, (2) inadequate execution of control action, (3) inadequate or missing feedback. The sub-categories are graphically summarized in figure 4-2. The categorization allows for reducing the vast number of individual findings and observations generated by traditional accident reports to a manageable number of types of problems. Without the reduction in complexity that the categorization provides, there can not be a serious advance in the effectiveness of accident investigation given the complexity of systems developed today.

The utility of the categorization of the causal factors generated by the STAMP framework is demonstrated by the observation of the three accidents investigated for this thesis. In two of the investigations there are instances where the causal factors can be tracked from the lowest levels to the higher levels.

Further insight would be gained from utilizing the STAMP framework in an investigation where more information is available than was for this thesis. Several types of information were lacking from the investigation. The types of useful information lacking included a detailed description of the organizational structure of each of the projects, a more specific and detailed description of the interactions within and between levels, and detailed description of the system safety constraints. More time and resources in conjunction with the additional detail above would provide even richer and deeper insights to the causal factors involved in the three accidents.

5.4 STAMP Implementation Concerns

The STAMP framework suffers from some of the same problems that traditional accident investigation methods suffer. Terminology in the system safety community remains diverse between sources. The fundamental concept of a hazard is not consistent across or within industries. Another problem with terminology stems from implementation. Many system safety practitioners can agree on a definition but follow divergent implementations. Safety is often confused with reliability in hazard analysis and accident investigation. The STAMP framework implemented without well defined terminology will give similar results to traditional methods.

The most significant problem that implementation of the STAMP framework suffers is that systems theory is not widespread. System theory concepts are fundamental to the proper implementation of STAMP. Proper system model creation requires zooming to the correct level and aggregating the correct functions within those levels. Improper system model creation can lead to combinatorial explosion of interactions. Another problem concerns implementation. The interpretation of what constitutes a failure, flaw, or dysfunctional interaction may result in it being put it in multiple categories or lead to a disparity between two or more different reviewers among multiple accident investigations. This problem could be classified as an asynchronous usage problem. Due to multi-containment and organizational structure inconsistencies, the interactions within levels and between levels are extremely complex and varied — making the construction of a system-theoretic model more difficult.

5.5 Follow-On Activities

NASA's mishap investigation system can be modified to utilize the STAMP concept. The modifications would be minimal to the documentation but challenging in implementation. There are also many other opportunities to apply a systems-theoretic feedback control loop. Follow on research could include areas like learning from mishaps, developing performance metrics, assessing risk, and preventing accidents.

5.5.1 Use of STAMP In NASA Mishap Investigation

NASA uses chain of events model investigation techniques almost exclusively. MORT is recommended by the NASA's accident investigation documentation but doesn't seem to be used extensively. MORT is comprehensive for a classical non-systems-theoretic based technique. The official reports for the three accidents investigated in this thesis nominally followed the NASA documentation. It is not clear if the implementation of the recommended investigation techniques were followed during the official investigation of the accidents. There is a suggestion to utilize MORT but there was no sign in the reports that the investigation teams had done so. STAMP can easily replace or be recommended as a substitute for MORT as the recommended accident model. There is a requirement for the findings and observations from each investigation be incorporated into NASA's Lessons Learned Information System. The assessment of the STAMP framework in this thesis stopped short of investigating the actual utility of STAMP in organizational learning but the findings from its utility in accident investigation should apply to enhancing it. The next section will briefly outline how the STAMP framework can assist in organizing the information into a format conducive for use in learning.

5.5.2 Learning

NASA's current lessons learned system does not facilitate memory in a general sense — only specific "data points". The STAMP model can provide a conceptual framework to guide in categorizing causal factors to assist in "corporate memory." The STAMP framework addresses the aspect of complexity due to variety by providing simple but mutually exclusive categories for sorting accident causal factors. A learning system must be able to remember, assess, and change goals[35]. STAMP assists in reducing the complexity of memory. It provides a numerical system that is conducive to graphical depictions that abstract the data into knowledge.

Based on the observations of chapter 4, there are several reoccurring themes in the accidents investigated. One of them has to do with hardware: Materials or physical problems are addressed rather well in the traditional reports. The others have to do with dysfunctional interactions and poor control (oversight) actions. These have been traditionally ignored. The current method of "learning" in the LLIS cannot provide that kind of insight.

5.5.3 Preventing Mishaps

The STAMP framework can be used to help prevent accidents by providing developers and operators a common structured process (mental) model of how the system is to function. If developers and operators know the questions that will be asked during an accident investigation, they are more likely to prepare responses in advance — these responses would form the rationale for acceptance (or rejection) of the identified risks. The inquiry before an accident can be an open book test: by taking the time to prepare ahead of time the risks will have been addressed. If the accident does occur, its effects will likely be less devastating (to careers, personnel, and hardware).

5.5.4 Assessing Risk

The systems-theoretic modeling technique can provide a framework for assessing project risk by providing developers and operators with a common and structured mental model of the systems risks. This is actually a continuation of prevention of accident section above and is related to the following section on monitoring performance. Once the risks are "framed" within the systems-theoretic model, the state of the system can be assessed as to whether key system safety factors have (or are about to) violate system safety constraints. Also the constraints can be assessed as to whether they have drifted — leaving the current state of the system outside the now current constraints.

5.5.5 Monitoring Performance

The systems-theoretic modeling technique can provide a framework for assessing system performance by providing developers and operators with a common and structured mental model of the systems performance requirements. The performance requirements would be the system safety constraints. This is probably the most intuitive of the follow on activities. It can be used to assess whether the system's current performance level has drifted (or been driven) out of the bounds defined by the performance constraints or if the performance constraints have drifted leaving the current performance level inadequate.

The STAMP framework can be utilized to assess candidate projects for applicability to NASA's paradigm shift from its traditional large program focus to the concept of Faster, Better, Cheaper (FBC). Projects that have minimal time lags, internally and externally aligned goals, and enabling technology will make good candidates for FBC implementation. Forcing project execution faster than the slowest lag times in the control action and feedback loops will lead to a control algorithm that is out of sync with the process. An out of sync control algorithm will lead to temporally incorrect control action inputs resulting in haphazard progress in the project. Coordinated and aligned process models among controllers will naturally lead to "better" and higher performing systems. Projects completed faster will cost less if they do not violate system constraints. They will also cost less if new technology is available and its implementation is coordinated and all process models and control algorithms are synchronously updated.

5.6 Conclusion

The framework and the process for its application developed in this thesis provide a tool for identifying and categorizing the various causal factors associated with complex system accidents. It does so by providing a holistic systems view between the engineers and managers responsible for the design and construction of a system as well as between and with their counterparts that will utilize and maintain the system in operation.

System engineering tools are used to expose the dysfunctional interactions causing failures in complex systems. To apply these tools it is necessary to understand the process involved in the development of complex aerospace propulsion and ground systems as well as the associated product development decision-making process. Utilization of the framework requires systems theory to decompose the system under investigation into a hierarchical system-theoretic model that addresses the technical, managerial, and regulatory aspects of the system. Accidents are the result of inadequately constrained or controlled dysfunctional interactions among the various components of the system. The utility of the developed framework is in the synthesis of causal factors using control theory concepts.

The developed framework can be used stand-alone or in conjunction with current techniques. The application of this framework is competency enhancing when applied in conjunction with current accident modeling techniques. A major benefit from utilization of this framework is that it enhances the understanding of the reasons why an accident happened and assists in building the overall technical and business case for efficiently selecting controls to be put in place to prevent recurrence. Controls put in place can be physical, managerial, or regulatory. It also provides a common framework by which organizational learning can take place.

NASA's current organizational perception of safety is that it only applies to personal protection from hazards. It is an industrial safety view that is restricted largely to office and production personnel injury prevention. NASA's approach to the mission success side of safety has focused on the reliability of the hardware that makes up aeronautic and space missions. Safety should be defined with respect to both personal protection and mission success aspects.

In the recent past NASA has gone from a big program to a small project paradigm. That paradigm shift disrupted many established practices, causing asynchronous evolution of mental and process models as different organizations adopted or adapted to this new paradigm. The tools that NASA uses to investigate accidents must make the shift from a linear chain of events model to a new systems theoretic model in order to keep pace with the ever-increasing levels of complexity.

"He that will not apply new remedies
must expect new evils,
for Time is the greatest innovator."
Bacon Essays, 1625[36].

Glossary

It is tremendously important to establish a consistent set of nomenclature. Both the first and most recent second editions of the System Safety Society's System Safety Analysis Handbook lament that there are no universally accepted definitions for important concepts in the system safety field. Basic terms such as "hazard" and "risk" vary from source to source[37]. All terms used in this thesis are used consistent with the definitions established in Safeware[38]. Important differences and omissions in NASA and system safety documentation are noted in this glossary. Terms are defined here in an order conducive to building on each other first to define hazard then risk, and finally safety. The first definition following the term is the one used in this thesis.

Reliability

Reliability is the probability that a piece of equipment or component will perform its specified function satisfactorily for a prescribed time and under stipulated environmental conditions[39].

Failure

Failure is the nonperformance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions. Failure is an event (a behavior) that occurs at a particular instant in time. Failures are basic abnormal occurrences.

Two causes of failure:

1. Design flaw (systemic failure)
2. Deviation from the originally designed behavior[40].

Types of equipment failures:

1. Early failures occur during the "burn-in" period and are due to poor assemblies or to weak, substandard components that fail soon after system startup.
2. Random (or chance) failures result from complex, uncontrollable, and sometimes unknown causes primarily within the useful life of the component or system.
3. Wear out failures begin when the components are past their useful life[41].

Error

Error is a design flaw or deviation from a desired or intended state. An error is a static condition (a state) that remains until removed. The term human error is too ingrained in common language and in psychology to try to make it match the engineering definition[42].

Fault

Faults are higher-order events (than failures) that result from the improper functioning of some upstream component. In general, all failures are faults, but not all faults are failures.

There are several type of faults:

1. Primary Fault: a component fails within the design envelope or environment.
2. Secondary Fault: component fails because of excessive environmental stresses that exceed the requirements specification or design environment.
3. Command Fault: involve the inadvertent operation of the component because of a failure of a control element - the component operates correctly, but at the wrong time or place[43].

Accident and Mishap

An accident is an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

There are several aspects to this definition of an accident:

1. An accident is undesired, and because it is undesired, it also unplanned or unintentional, although it may or may not be foreseen.
2. Accidents result in a specified level of loss, which implies that there must be some sort of damage to life, property, or the environment. The damage may be immediate or manifest itself in the long term.
3. An accident is defined as a loss event, without placing limits on the type of event[44].

The Department of Defense and NASA both use the term mishap in place of accident. The Department of Defense defines mishap: an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment[45].

To NASA a mishap is an unplanned event that results in injury to non-NASA personnel caused by NASA operations; damage to public or private property (including foreign property) caused by NASA operations; occupational injury or occupational illness to NASA personnel; damage to NASA property caused by NASA operations; or mission failure. NASA mishap are categorized as Type A, B, or C mishaps, Mission Failures, or Incidents depending on the level of the loss[46].

It is interesting to note that the NASA Safety Manual (NPG 8715.3 dated 24 January 2000) does not include definitions for accident, incident, or mishap in its glossary.

Incident

An incident is an event that involves no loss (or only minor loss) but with the potential for loss under different circumstances[47].

Incident is not defined in MIL-STD-882C or the NASA Safety Manual. NASA does define incident in 8621.1. An incident is a mishap consisting of personal injury of less than a Type C mishap severity but more than first-aid severity, and/or property damage equal to or greater than $1,000, but less than $25,000[48]. The above definition is also known as a "close call" within NASA.

Hazard

A hazard is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event). A hazard is defined with respect to the environment of the system or component. What constitutes a hazard depends upon where the boundaries of the system are drawn. A system is an abstraction, and therefore the boundaries of the system can be drawn anywhere the person who is defining the system wants. The boundaries, in turn, determine which conditions are considered part of the hazard and which are considered part of the environment. One of the first steps in designing a system is to decide the conditions that will be considered to be hazards that need to be eliminated or controlled.

Hazards have two important characteristics:

1. Severity (also called damage), defined as the worst possible accident that could result from the hazard given the environment in its most unfavorable state.
2. Likelihood of occurrence, which can be specified either qualitatively or quantitatively[49].

Hazard Level: is the combination of severity and likelihood of occurrence[50].

The Department of Defense defines hazard as: a condition that is prerequisite to a mishap[51]. NASA defines hazard as: the existing or potential condition that can result in or contribute to a mishap[52]. The term hazard is not defined in the glossary of NASA's Guidelines For Mishap Investigating[53]. The Sverdrup System Safety Scrapbook [54] defines hazard as: a threat of harm.

Risk

Risk is the hazard level combined with (1) the likelihood of the hazard leading to an accident given the current state of the environment (sometimes called danger) and (2) hazard exposure or duration (sometimes called latency). Exposure or duration of a hazard is a component of risk: Because an accident almost always involves a coincidence of conditions, including the system hazards and events or states outside the system boundaries to the system, the longer the hazardous state exists, the greater the chance that the other prerequisite conditions will occur[55].

The System Safety Analysis Handbook defines risk as an expression of the probability of a hazardous state occurring; the probability of the hazard causing a mishap, and the perceived severity of the worst potential mishap that could result[56].

The Department of Defense defines risk as an expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability[57].

The NASA Safety Manual defines risk as the combination of (1) the probability (qualitative or quantitative) that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, or failure to achieve a needed technological breakthrough; and (2) the consequences, impact, or severity of the undesired event were it to occur.

A definition for risk was not found in NASA's Mishap Investigation Guidelines.

Safety

Safety is freedom from accidents or loss[58].

The System Safety Analysis Handbook defines safety similarly as: the freedom from exposure to the occurrence of mishaps[59].

The Department of Defense and NASA defines safety as: the freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment[60] [61].

The NASA Mishap Investigation Guidelines do not define safety[62].

Root Cause / Causal Factors

The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the system design and on operations, that is, by inadequate enforcement of constraints on behavior at each level of the socio-technical system. Flawed processes involving interactions among people, societal and organizational structures, engineering activities, and physical system components cause accidents in this model. The process leading up to an accident (loss event) can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values[63].

NASA documentation separates causality into dominant root cause, contributing root cause, and significant observation.

Dominant Root Cause: Along a chain of events leading to a mishap, the first causal action or failure to act that could have been controlled systemically either by policy/practice/procedure or individual adherence to policy/practice/procedure.

Contributing Root Cause: A factor, event, or circumstance that led, directly or indirectly, to the dominant root cause or that contributed to the severity of the mishap or close call.

Significant Observation: A factor, event, or circumstance identified during the investigation that did not contribute to the mishap or close call, but if left uncorrected has the potential to cause a mishap, injury, or increase the severity should a mishap occur[64] [65].

Bibliography

1 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

2 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995.

3 Russell L. Ackoff. *Ackoff's Best: His Classic Writings On Management.* John Wiley & Sons, Inc., New York, NY, 1999.

4 Richard A. Stephans, P.E.,CSP, Warner W. TalsoSystem Co-Editors. *Safety Society: System Safety Analysis Handbook 2nd Edition.* System Safety Society, New Mexico Chapter, Albuquerque, NM, 1997.

5 Derek Hitchins. *Getting To Grips With Complexity: Or A Theory of Everything Else.* http://www.hitchins.co.uk/ASE_Book.htm, 2000.

6 Charles Boppe. ESD.33J Systems Engineering: Complexity I. July 2001.

7 George A. Miller. *The Magical Number Seven: Problems of Perception.* The Psychological Series, Harvard Vol. 63, No. 2.

8 Donald V. Steward. Systems Analysis and Management: Structure, Strategy and Design. Problematics, 1995.

9 Russell L. Ackoff. *Ackoff's Best: His Classic Writings On Management.* John Wiley & Sons, Inc., New York, NY, 1999. Page 15.

10 Russell L. Ackoff. *Ackoff's Best: His Classic Writings On Management.* John Wiley & Sons, Inc., New York, NY, 1999. Page 16.

11 Russell L. Ackoff. *Ackoff's Best: His Classic Writings On Management.* John Wiley & Sons, Inc., New York, NY, 1999. Page 17.

12 Derek Hitchins. *Getting To Grips With Complexity: Or A Theory of Everything Else.* http://www.hitchins.co.uk/ASE_Book.htm, 2000. Part 2, Page 4.

13 Derek Hitchins. *Getting To Grips With Complexity: Or A Theory of Everything Else.* http://www.hitchins.co.uk/ASE_Book.htm, 2000. Part 2, Page 25.

14 Derek Hitchins. *Getting To Grips With Complexity: Or A Theory of Everything Else.* http://www.hitchins.co.uk/ASE_Book.htm, 2000. Part 2, Page 2.

15 Richard A. Stephans, P.E.,CSP, Warner W. TalsoSystem Co-Editors. *Safety Society: System Safety Analysis Handbook 2nd Edition.* System Safety Society, New Mexico Chapter, Albuquerque, NM, 1997.

16 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 17.

17 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

18 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 189.

19 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 190.

20 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 48.

21 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 53.

22 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 198.

23 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 199.

24 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 203.

25 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

26 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

27 P.L. Clemens. *System Safety Scrapbook*, 8th Edition. JE Jacobs Sverdrup, 2001. Sheet 87-2.

28 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

29 NASA. FY 2001 Performance Report. ftp://ftp.hq.nasa.gov/pub/pao/reports/2002/fy01_performancereport/overview.pdf

30 NASA. FY 2001 Performance Report. ftp://ftp.hq.nasa.gov/pub/pao/reports/2002/fy01_performancereport/overview.pdf

31 Roger D. Launius, NASA Chief Historian. *Apollo: A Retrospective Analysis.* NASA History Office, Updated 1999. The Program Management Concept. http://www.hq.nasa.gov/office/pao/History/Apollomon/Apollo.htm

32 Roger D. Launius, NASA Chief Historian. *Apollo: A Retrospective Analysis.* NASA History Office, Updated 1999. The Program Management Concept. http://www.hq.nasa.gov/office/pao/History/Apollomon/Apollo.htm

33 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

34 P.L. Clemens. *System Safety Scrapbook,* 8th Edition. JE Jacobs Sverdrup, 2001. Sheet 99-1.

35 Russell L. Ackoff. *Ackoff's Best: His Classic Writings On Management.* John Wiley & Sons, Inc., New York, NY, 1999. Page 58.

36 Derek Hitchins. *Getting To Grips With Complexity: Or A Theory of Everything Else.* http://www.hitchins.co.uk/ASE_Book.htm, 2000. Part 4, Page 2.

37 Richard A. Stephans, P.E.,CSP, Warner W. TalsoSystem Co-Editors. *Safety Society: System Safety Analysis Handbook 2nd Edition.* System Safety Society, New Mexico Chapter, Albuquerque, NM, 1997.

38 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Chapter 9.

39 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 172

40 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 172

41 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 174

42 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 172

43 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 173

44 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 175

45 DOD. MIL-STD-882C: System Safety Program Requirements. 19 January 1993.

46 NASA. NPG 8621.1: NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping. Effective Date: June 02, 2000

47 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 176

48 NASA. NPG 8621.1: NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping. Effective Date: June 02, 2000. Glossary.

49 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 177

50 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 179

51 DOD. MIL-STD-882C: System Safety Program Requirements. 19 January 1993.

52 NASA. NPG 8715.3: NASA Safety Manual. Effective Date: 24 January 2000. Appendix B.

53 NASA. NPG 8621.1: NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping. Effective Date: June 02, 2000

54 P.L. Clemens. *System Safety Scrapbook*, 8th Edition. JE Jacobs Sverdrup, 2001.

55 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 179

56 Richard A. Stephans, P.E.,CSP, Warner W. TalsoSystem Co-Editors. *Safety Society: System Safety Analysis Handbook 2nd Edition.* System Safety Society, New Mexico Chapter, Albuquerque, NM, 1997.

57 DOD. MIL-STD-882C: System Safety Program Requirements. 19 January 1993.

58 Leveson, Nancy. *Safeware: System Safety and Computers.* Addison-Wesley Publishing Company, Reading Massachusetts, 1995. Page 181

59 Richard A. Stephans, P.E.,CSP, Warner W. TalsoSystem Co-Editors. *Safety Society: System Safety Analysis Handbook 2nd Edition.* System Safety Society, New Mexico Chapter, Albuquerque, NM, 1997.

60 DOD. MIL-STD-882C: System Safety Program Requirements. 19 January 1993.

61 NASA. NPG 8715.3: NASA Safety Manual. Effective Date: 24 January 2000. Appendix B.

62 NASA. NPG 8621.1: NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping. Effective Date: June 02, 2000

63 Nancy Leveson. A Systems Approach to Safety Engineering, book in preparation.

64 NASA. NPG 8621.1: NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping. Effective Date: June 02, 2000

65 NASA. NPG 8715.3: NASA Safety Manual. Effective Date: 24 January 2000. Appendix B.