ACCIDENT ANALYSIS AND HAZARD ANALYSIS FOR HUMAN AND ORGANIZATIONAL FACTORS

by

MARGARET V. STRINGFELLOW

S.B. Aeronautics and Astronautics, Massachusetts Institute of Technology, 2004
S.B. Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2004

S.M. Aeronautics and Astronautics, Massachusetts Institute of Technology, 2008

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

October 2010

Signature of Author:_____
Department of Aeronautics and Astronautics
October 28, 2010

Certified by:_____
Nancy G. Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Certified by:_____
Joel Moses
Professor of Computer Science and Engineering and Engineering Systems
Committee Member

Certified by:_____
Meghan M. Dierks
Assistant Professor of Medicine at Harvard Medical School
Committee Member

Certified by:_____
James K. Kuchar
Leader, Weather Sensing Group, Lincoln Laboratory
Committee Member

Accepted by:_____
Eytan H. Modiano
Associate Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

[Page intentionally left blank]

ACCIDENT ANALYSIS AND HAZARD ANALYSIS FOR HUMAN AND ORGANIZATIONAL FACTORS

by

Margaret V. Stringfellow

Submitted to the Department of Aeronautics and Astronautics on 10/29/2010 in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Aeronautics and Astronautics

ABSTRACT

Pressures and incentives to operate complex socio-technical aerospace systems in a high-risk state are ever present. Without consideration of the role humans and organizations play in system safety during the development of these systems, accidents will occur. Safe design of the "socio" parts of the socio-technical system is challenging. Even if the system, including the human and organizational aspects of the system, are designed to be safe for anticipated system needs and operating environments, without consideration of pressures for increased performance and efficiency and shifting system goals, the system will migrate to a high-risk operating regime and safety can be compromised.

Accident analysis is conducted to discover the reasons why an accident occurred and to prevent future accidents. Safety professionals have attributed 70-80% of aviation accidents to human error. Investigators have long known that the human and organizational aspects of systems are key contributors to accidents, yet they lack a rigorous approach for analyzing their impacts. Many safety engineers strive for blame-free reports that will foster reflection and learning from the accident, but struggle with methods that require direct technical causality, do not consider systemic factors, and seem to leave individuals looking culpable. An accident analysis method is needed that will guide the work, aid in the analysis of the role of human and organizations in accidents and promote blame-free accounting of accidents that will support learning from the events.

Current hazard analysis methods, adapted from traditional accident models, are not able to evaluate the potential for risk migration, or comprehensively identify accident scenarios involving humans and organizations. Thus, system engineers are not able to design systems that prevent loss events related to human error or organizational factors. State of the art methods for human and organization hazard analysis are, at best, elaborate event-based classification schemes for potential errors. Current human and organization hazard analysis methods are not suitable for use as part of the system engineering process.

Systems must be analyzed with methods that identify *all* human and organization related hazards during the design process, so that this information can be used to change the design so that human error and organization errors do not occur. Errors must be more than classified and categorized, errors must be prevented in design. A new type of hazard analysis method that identifies hazardous scenarios involving humans and organizations is needed for both systems in conception and those already in the field.

This thesis contains novel new approaches to accident analysis and hazard analysis. Both methods are based on principles found in the Human Factors, Organizational Safety and System Safety literature. It is hoped that the accident analysis method should aid engineers in understanding how human actions and decisions are connected to the accident and aid in the development of blame-free reports that encourage learning from accidents. The goal for the hazard analysis method is that it will be useful in: 1) designing systems to be safe; 2) diagnosing policies or pressures and identifying design flaws that contribute to high-risk operations; 3) identifying designs that are resistant to pressures that increase risk; and 4) allowing system decision-makers to predict how proposed or current policies will affect safety. To assess the accident analysis method, a comparison with state of the art methods is conducted. To demonstrate the feasibility of the method applied to hazard analysis; it is applied to several systems in various domains.

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

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to my advisor Nancy Leveson. She took my interest in quirky software problems and showed me how they were related to an entirely new field (to me)—System Safety. Starting from the stories of disastrous endings of once-thought engineering marvels, she introduced me to the fundamentals of safety engineering and innovative new ways to think about design, software, and human behavior. Nancy, thank you for guiding me in my graduate work, providing critical feedback to improve my research (and writing!) and initiating me to systems thinking.

Meghan Dierks also deserves my utmost appreciation. Her enthusiastic support, candid attitude, and willingness to collaborate with an *aero/astro* student in the field of patient safety and risk allowed me to do the research in this thesis.

I would also like to thank Jim Kuchar, my Boss at Lincoln Labs and a committee member for this dissertation. He took me from theoretical solutions to testing practical implementations on real systems. He also let me play with Matlab code on >100 computers at once—which in the days before cloud computing was a Big Deal!

Joel Moses, thank you for taking the time to be a part of my thesis committee. I have thoroughly enjoyed our conversations about research and other topics.

Qi Van Eikema Hommes, a member of my defense committee, was a critical part of my learning process in my finals weeks at MIT. Her insights and probing questions were critical to communicating my research.

I also am sincerely grateful for the help of Sidney Dekker. It was an honor to have you sit on my defense committee. Your work was the inspiration for this research.

I would also like to thank John Sterman and Paulo Goncalves for exponentially accelerating my passion for system dynamics. Through their work and conversations with me, I discovered the joy of modeling complex feedback systems.

My CSRL colleagues deserve a Shout Out: Thank you for the conversations, debate, and insights. The discussion in 33-407 indelibly shaped this research from its earliest stages. I could not hope for a better set of colleagues: Katie Weiss, Nic Dulac, Brandon Owens, John Thomas, Matthieu Couturier, Blandine Antoine, and the new students just starting out.

Thanks also to Kathryn Fischer and Barbara Lechner for their help, assistance, and warm smiles over the past ten years.

To the denizens of Senior Haus: Thank you for giving me a home and being an exhilarating place to live.

And of course no thesis is complete without a little help from one's friends: Thank you to Edgar for everything, Zoe for telling it like it is—with charm, to Rebecca for B&H, Indy for keys, Carrie for the Pink, Yves for five-fingered feet, Astrid, Marguerite, Lindsey, Sawyer, Beeson, Carla, Ben, Star, Sari, Jasso, the Orc painters, the weight lifters, Tortles, the Yoshimi makers, the LB group, the Bramblebarbarians, Foodies, sh-grt, and everyone on eit (?!).

My biggest appreciation goes to my family: Papa, Mommie, Sara, Leigh, Charlie, and Keith. Charlie, thank you for being so cute. Mommie and Papa thank you for giving me perspective. Sara and Leigh-

leigh, I am debt for your Comments. Boyfriend, thank you for being the best husband on the planet. I could not have done any of this without you. Also, thank you for making dinner every day—I owe you a few!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ATC	Air Traffic Control
BBS	Behavior-based Safety
CBP	Customs and Border Patrol
CLD	Causal Loop Diagram
COA	Certificate of Authorization
CRM	Crew Resource Management
DER	Designated Engineering Representative
ECF	Events and Causal Factors
FAA	Federal Aviation Administration
FMEA	Failure Modes and Effects Analysis
FRAM	Functional Resonance Accident Model
FTA	Fault Tree Analysis
GA-ASI	General Atomics Aeronautical Systems Inc.
GCS	Ground Control Station
H	Hazard
HAZOP	Hazard and Operability Method
HFACS	Human Factors Analysis and Classification System
HRO	High Reliability Organizations
ICA	Inadequate Control Action
LOS	Line of Sight
NAT	Normal Accident Theory
OSHA	Occupational Safety and Health Administration
PIC	Pilot in Command
PPO	Pilot Payload Operator
PRA	Probabilistic Risk Assessment
NAS	National Airspace System
SAM	System Action Management
SC	Safety Constraint
SD	System Dynamics
SHOW	STAMP extension for Humans and Organizations using guideWords
SMS	Safety Management System
SOAM	Safety Occurrence Analysis Methodology

SRM	Safety Risk Management
STAMP	System-theoretic Accident Model and Processes
STPA	STAMP-based Analysis
TFR	Temporary Traffic Restriction
UAV	Unmanned Aerial Vehicle
UV	Unmanned Vehicle
WPAM	Work Process Analysis Model

CHAPTER 1 INTRODUCTION

Human and organizational factors are an important cause of accidents. As the design of electro-mechanical equipment becomes more and more safe, the causes of accidents are more likely to be attributed to human and organizational factors. Recent accidents and mishaps in aviation [89] and energy [70] have left the public wondering how such a dysfunctional organization could have been operating a system with such potential to harm the operators and the public. New technologies that hold the promise of autonomous UAV operations in the national airspace system have researchers and regulators struggling to define the correct role for humans to play in a robotized sky [22][90][91]. The field of safety engineering does not have suitable tools for answering these questions. There is no hazard analysis that can be used during the design phase of a complex system to identify and evaluate hazardous scenarios involving humans and organizational flaws. The engineering field lacks a method to design the *whole* system, including the human and organizational aspects to be safe.

As an example, an Unmanned Aerial Vehicle (UAV) crash in Nogales, Arizona was due in large part to flaws in the organizational structure controlling UAV operations in the national airspace system (NAS). UAV operators "lost link[1]" with the UAV during border control operations. In this case, the FAA, serving as the role of regulator, had no evidence to support that the vehicle was air-worthy, and air traffic control (ATC) had no observability into the state of the UAV as they performed their responsibility for air-traffic separation. Both of these conditions were due to the lack of feedback between the UAV operators and other controllers in the system (ATC and the FAA). Without any ability to issue commands to the UAV (the operating process) or receive communications about its whereabouts (process state information and feedback), the FAA and ATC were unable to control the UAV and therefore unable to maintain the safety of the airspace as the UAV pilots lost contact. This accident occurred due to technical failures that are reflections of organizational problems and the inadequate design of the human role as operator and regulator.

The Nogales accident does not stand alone. Despite the engineer's familiar canon of accident reports (including Bhopal, Uberlingen, and Zeebrugge), system engineers have struggled to incorporate the

[1] Link loss occurs when the UAV is out of communications with pilots or other operators. When this occurs, UAVs are programmed to fly a predetermined flight plan called a "lost link profile." The UAV will attempt to regain datalink communications with ground control at predetermined time intervals. If communications are not restored, the fuel on board the UAV will be exhausted and the UAV will crash to the ground.

lessons learned regarding human and organizational factors into the design of new engineering systems, and the same kind of accidents continue to occur [80] [81]. Accident investigators, with their post-mortem view of safety, have long known the importance of the "socio" parts of the system; engineers, at the other end of the system lifecycle, are at a loss as to how to create comprehensive organization and human factors design. While the human factors revolution has been successful at improving human-machine interfaces and ergonomic task design, it has been less successful with the design of the human role in organizations and complex socio-technical systems. Organization structures that support safety must be carefully designed to ensure system resilience and robustness to risk-increasing pressures.

Safety-driven design in a new concept in safety engineering [110], and currently state-of-the-art solutions for examining the impact of humans on safety are mostly limited to analyses performed after a system has been developed. Furthermore, these methods tend to focus their recommendations for safety improvements on operator behavior changes. Typical solutions focus on influencing operator decision-making through the issuance of directives to "work safer" or increase "situational awareness" [19][18] or "be mindful of weak signals" [82]. However, the imperative to "be safe" is already clear, and in many cases, indications of high risk are glaring—yet ignored. For complex systems to be operated in a low-risk state, the system must be designed to be safe from the beginning, and the system design must support and encourage safe human decision-making.

1.1 Limitations in Current Hazard Analyses

A hazard analysis is the process by which a design is analyzed for safety. Hazard analysis is used to identify hazardous states in a system and scenarios in which they can occur. When integrated with a design process, a hazard analysis allows engineers and designers to consider the safety-related design aspects during system development. Engineers can then make intelligent trade-offs between safety and other aspects of the design (e.g., performance, cost, schedule, robustness, etc.). As Willie Hammer states in the *Handbook of System and Product Safety* [40], "The system safety (and product safety) concept is predicated on this principle: 'The most effective means to avoid accidents during system operation is by eliminating or reducing hazards and dangers during design and development.'"

Hazard analysis methods in use today on socio-technical systems [27][28][83][88], do not call for safety engineers to analyze and plan for the impact of human operators, the organizations controlling and influencing the system, or the social context and community in which it operates. Although engineers devote considerable attention to technical processes and even to human-machine interfaces, engineers pay little attention to prospectively analyzing or planning the complete human and social levels of a system's

design for safety. The result is systems that have adequate technical specifications but contain flaws in the design of the technical process supporting the human operator(s), in addition to flaws in the human and organizational architecture supporting the operator and technical processes. Current hazard analysis methods, adapted from traditional accident models, do not address risk migration and they cannot be used to comprehensively identify hazardous scenarios involving humans and organizations. Without such scenarios, critical information for the design of systems to prevent loss events related to human error and organizational factors is missing.

1.2 Design For Safety

Because safety is an emergent property of systems, it must be designed into a system, rather than added-on to an otherwise complete design. To create a system-wide property such as "safety", engineers must intentionally design interactions within the system to be safe— "safety" should not be an emergent property that is achieved by accident. Furthermore, consideration of the technical process is not enough to ensure safety. Engineers must also design safety into the organizational structure and the individual human roles. This includes the design of, for example, command and control structures, communication structures, procedures, job processes, team makeup, and incentives shaping business unit and operator behavior. In order to design safety *into* a system, the design process must include a hazard analysis that considers the role of people *and* organizations in potential losses.

Understanding of complex systems can be increased through considering the effects of feedback and delays. One of the basic tenets of management science is that managers are not adept at predicting or understanding systems with long delays or feedbacks [24][25][26]. In any situation in which the cause and effect are not in the same medium or closely related in time and space, managers are bound to miss the interactions and effects of their policies on safety. Given this, the organizational structure must be designed such that delays are lessened and consequences may be more easily forecasted and understood.

In socio-technical systems, the human element itself cannot be designed. Humans are not the same as technical system components. They do not have a probability of "failure" like a component does (unless we consider physical mortality). Engineers cannot assign the personality, risk tolerance, or continued high level of motivation needed by an operator. They can, however, design a system to support humans, by modifying the operating context, managing workload, changing the priorities of operators and management through incentives, and managing risk tolerances through transparent and accurate risk assessments and decision support.

Regarding the human element, engineers may fall subject to the "fix it with the most flexible component" trap. If systems have flaws that can be overcome with new operating procedures, managers may feel that tweaking an operating procedure is a cheap solution. However, while rewriting an operating manual may be inexpensive—and even training sessions can be affordable—if the procedures are not followed [134][135][136][137][138] (whether due to conflicting priorities, boredom, or confusion), the system may be operated in a state of high risk. If the task is ill suited to human operations, accidents *will* occur.

There is a trend to designing humans out of the system (through automation), which creates a vicious cycle. The more human error, the more engineers design humans out of system, which reduces system robustness and squeezes the problem solver role, eventually leading to more human error [117]. The answer is not to design the human out of the system, but to design the human into the system fabric.

1.3 Limitations in Accident Analysis Practices

Accident analysts also lack a method for framing and connecting human and organizational factors to the technical system failure or loss event [77]. Accident analysis is used to examine the safety of a deployed system after it has failed. Safety professionals have attributed 70 to 80% of aviation accidents to human error [75]. Recently, accident analysts have also begun to cite organizational factors as contributory causes of accidents. While analysts have long known that the human and organizational aspects of systems are key contributors to accidents, they lack a rigorous approach for analyzing their impacts.

In particular, accident analysts justify blaming operators based on confusion between data availability and data observability [19]. Data availability is information that was present at the time of an accident but could have been buried deep in a hierarchical user interface or obscure dial, for instance. Data observability is data that could actually be observed given all of the pressures and tasks that were actually occurring. Without being inside the mind of an operator, it is impossible for analysts to know which data was available but not observable. It is common in accident reports to blame the operator for missing important information. For example, in a recent oil company accident, the operator had two level gauges available to him. The operator used one of the gauges to make control decisions but did not know that it was broken. The second, redundant gauge information was obscured within the user interface. Nevertheless, the operator was deemed negligent [85].

Many accident analysts strive for blame-free reports that will foster reflection and learning from accidents but struggle with methods that require direct causality, do not consider systemic factors, and seem to leave individuals looking culpable [77] [79] [80]. Safety professionals make do with ad hoc methods that

do not help guide investigations or help them determine which human and organizational data is relevant and which is not. In particular, investigators are not sure which people to interview or what questions to ask [62]. An accident investigation method is needed that will guide investigations, aid in the analysis of the role of humans and organizations in accidents, and promote blame-free accounting of accidents.

1.4 Challenges that Need to be Addressed

A unique challenge to the evaluation of hazards, the design of safe systems, and the investigation of accidents is the dynamic nature of socio-technical systems. Pressures and incentives to operate complex socio-technical aerospace systems in a high-risk state are ever present. For example, as new customer needs are identified, new environmental requirements levied, and stakeholder expectations raised, the needs of organizations change and the system is pressured to change. Even if the system, including the human and organizational aspects, is designed to be safe, given its preplanned operating requirements and conditions, without consideration of the system's evolving goals, risk migration will occur. Consideration of human and organizational impacts on safety must be considered both in the development and operation of socio-technical systems throughout the system lifecycle to prevent accidents.

Knowingly or unknowingly, complex systems are often operated in high-risk states, which can lead to unacceptable loss events or accidents [52][71]. System actors (including management and operators) are often unable to 1) recognize which designs, processes and procedures will lead to high-risk operations; 2) understand the causal factors and pressures that encourage high-risk operations; or 3) find design solutions to allow, enforce, or encourage safer operations. The challenges to safe operations are insurmountable without consideration of safety in the development of a system. Unsafely designed systems cannot be operated safely over a long period of time, so hazard analysis must make plain the conditions and design flaws that will foster risky operations and guide designers to safe alternatives. A useful hazard analysis technique must fulfill several goals:

1) Hazard analysis must consider how systems are pushed to high-risk states and the boundary of safe operations. A hazard analysis method should be useful in a) exposure of hazardous designs that will be susceptible to risk migration; b) identification of high-risk operations; c) diagnosis of policies or pressures that contribute to high-risk operations; and d) prediction of the impact on safety by proposed policies. It must also guide system developers to consider measures for pushing back against risk-increasing pressures while still allowing the system to change over time as its environment or mission changes. In essence, the hazard analysis must aid engineers in the design of resilient systems.

2) A new hazard analysis technique must be of use in the design of new systems as well as those already deployed. In new systems, the hazard analysis will be integrated into the design process to ensure the creation of a safe design. In existing systems, it will be used to analyze and then propose changes to re-engineer a system. In the re-engineering of a power generation facility, for example, the hazard analysis could be used to analyze the integration of new technology into an existing system and identify hazards and changes to ensure safe operations of the new whole.

3) The hazard analysis should also be adaptable to the analysis of accidents that have already occurred.

No hazard analysis for use on organizations and human system aspects currently exists. This thesis proposal presents the motivation, development, and demonstration of feasibility for such a new hazard analysis.

1.5 Research Goals, Hypothesis, and Approach

1.5.1 Research Goals and Hypothesis

The goal of the research presented in this thesis is to create a method for the inclusion of human and organizational factors and social context into safety engineering processes. My first research goal was to create a method that uses a rational framework. I would rather provide a rational safety engineering method that lacks completeness, than to identify all human and organization-related causal factors, but categorize them in an ad hoc manner. The research goal is that my method 1) enables the discovery and exposure of conditions leading to hazards; 2) identify and include human and organizational factors that contribute to inadequate control in safety analysis; and 3) assists engineers in finding new solutions, policies, and design changes to improve system safety. To that end, I sought to develop a novel method for accident analysis and hazard analysis suitable for human and organizational factors for socio-technical systems.

The hypothesis of this research is:

> *"The STAMP [5] accident analysis method and the STPA hazard analysis [8] can be extended to include structure for the discovery of human and organizational factors. This new method can be applied to the analysis of accidents so that additional insight is gained, and system recommendations created, for system redesign of the human context and the organizational design. Furthermore, the method is applicable to the analysis of complex systems prospectively,*

before an accident has occurred, and can be used to discover design flaws involving human and organizational factors."

1.5.2 Research Approach

To develop a new accident analysis and hazard analysis method for human and organizational factors, I sought to understand the human and organizational factors that contribute to accidents. Next, I tried to understand how to identify social factors and human and organizational design that could contribute to high-risk operations before an accident has occurred. In so doing, I took the following research approach:

1. Employed a grounded theory qualitative research approach [170] [171]using accident reports and analyses for data. Reviewed accident reports and accident analyses from the fields of aviation, energy, manufacturing, and medicine and identified inadequate control actions[2] [5] by both individual controllers and organizations.
2. Identified the context (the system design) that permitted or encouraged inadequate control.
3. Highlighted key words or phrases in the human and organization context and grouped key words into categories.
4. Distilled contextual factors from each category into essential guidewords. The process of contextual factor distillation was finished as each category reached theoretical saturation [170] [171].
5. Using a new set of four accidents, I identified inadequate control actions and then applied the guidewords to identify relevant context that contributed to the accident.
    a. No new guidewords were needed, and each guideword was used, giving confidence that the set of guidewords identified had reached theoretical saturation as a whole, and that the set spanned the set of contextual factors that may contribute to inadequate control.
6. The next step was to build the foundation of the method. In particular, I chose to use a control-theoretic basis, and identify what requirements must be in place for accident-free control by humans and organizations. Using concepts from control theory, I indentified requirements for controllability that must be met to ensure adequate control by human and organizations.
7. The identified control requirements help to bridge the gap between identifying the causes of "human and organizational error" and using principles from control theory and systems

[2] Those actions that violate safety constraints and safety responsibilities and may allow hazards to occur.

thinking to designing safe socio-technical systems. I then attempted to classify inadequate control actions using an engineering framework.

   a. The control requirements were used to create a human error taxonomy that describes and classifies sources of inadequate control for humans and organizations.

8. Using the control requirements and the guidewords, I created a structured approach to accident analysis and hazard analysis.
   a. I applied the accident analysis method to a well-known accident to demonstrate its feasibility.
   b. I assessed and compared my method to other state-of-the-art accident analysis methods.
      i. As part of the accident analysis method development, I identified dimensions to make a between-method comparison possible.
9. I then applied the hazard analysis method to several complex systems from several industries.
   a. I assessed and compared the hazard analysis method with a leading hazard analysis method for humans [27].

CHAPTER 2 LITERATURE REVIEW AND SURVEY OF THE STATE OF THE ART

2.1 Chapter Overview

The purpose of this chapter is to convey the foundations for system safety and safety engineering and show how they are used to support the methods, processes and techniques in the field. Each relevant safety engineering technique is briefly reviewed and assessed. In the field of safety engineering, all techniques are predicated on a view of the nature of accidents. The three major accident models used in practice are presented and assessed. The assumptions and tenets of an accident model for complex systems are in turn informed by a view of how humans and organizational decision-making contribute to accidents. The strengths and limitations of the views discussed in this chapter will motivate the development of the accident and hazard analysis method presented in this thesis. This chapter concludes with a statement of the motivating research goal, the author's research approach, and thesis outline.

2.2 Contributions from Systems Thinking

The need for systems thinking arose when traditional linear decomposition methods failed to provide insight into the behavior of complex systems. Previously, it was thought that by decomposing a system into its parts, the functioning of the system could be deduced by "adding up" its parts. This method, know as "reductionism", first described by Descartes in the 1600s, was employed successfully for many technical systems, but is not useful for complex systems such as those that are controlled by software or composed of social elements [8][19].

Systems thinking, pioneered by Ludwig von Bertalanffy [94][97][95], tells us complex systems can only be understood at the system-level, examining the system as a whole. Systems thinking suggested that many key system characteristics or behaviors are emergent and can only be analyzed from a system perspective [96]. The term "emergent" was defined George Henry Lewes, who wrote:

"Every resultant is either a sum or a difference of the co-operant forces; their sum, when their directions are the same—their difference, when their directions are contrary. Further, every resultant is clearly traceable in its components, because these are homogeneous and commensurable. It is otherwise with emergents, when, instead of adding measurable motion to measurable motion, or things of one kind to other individuals of their kind, there is a co-operation of things of unlike kinds. The emergent is unlike its

components insofar as these are incommensurable, and it cannot be reduced to their sum or their difference." (Lewes 1875, p. 412, [98])

For complex systems, the dynamic interactions and *relationships* between parts may be more important for the system behavior than the part itself [97]. For example, the functioning of a successful organization, cannot be predicted by surveying the talents of the engineers in isolation, but can only be seen in the interactions between managers, engineers and others within the organization. The success of the organization is an emergent property of the system. Safety, too, is an emergent property of systems, and so systems thinking provides a good foundation for system safety engineering theory and methods [5].

Modern system thinkers, such as Senge, Sterman, and others, have highlighted another challenge in complex socio-technical systems, that of *dynamic complexity* [26] [63]. Dynamic complexity is exhibited by systems that experience the relationship between cause and effect as obscured, either because the "effect" occurs after a long time delay in a different part of the system, is viewed by different system actors, or changes form. Dynamic complexity is a different beast from *detail complexity*. A system that is simply composed of many parts may be characterized by detail complexity. For example, a Rube Goldberg machine is a good example of a system exhibiting detail complexity. There are several parts, but each action in the system begins and ends with a movement directly linked to the subsequent action in the system until the final outcome of the system is observed. A Rube Goldberg machine may be successful analyzed with reductionist techniques, and is not considered to be complex from a systems perspective.

In another example, a simple supply chain, studied in the Beer Game [63][26], is characterized by dynamic complexity. Due to time delays in the system, participants in the game over order as supply runs low, with greater shortages leading to greater incidence of over ordering. Participants are surprised when midway through the game, after a period of great shortage, huge quantities of beer arrive. Participants are not able to see that the beer delivered is just what was ordered. This effect happens due to a time delay between beer orders and beer deliveries. When cause and effect are not closely related in time, space, and form, people have trouble predicting the dynamic behavior of systems [25][26][46][63][64]. In safety-related decision-making, the effects of the decision are often hidden, unobvious, or delayed. Safety engineering methods that do not take dynamic complexity into account are not suitable for use in complex systems.

Another great challenge to the development and operation of safe complex socio-technical systems identified by system thinkers is that of risk migration. Because systems are always moving—largely unseen—to states of high risk, safety is never a static quality that can be achieved; it must be strived for continually, or be lost [1]. As Rasmussen says, systems always move to the boundary of acceptable behavior and the limits of what is considered safe [1]. If an effort to build safety slackens, risk migration is all but certain as the obvious pressures of other system goals (e.g., financial goals) prevail over safety. The biggest threats to safety are slow, gradual, and often invisible processes—for example, boredom, breakdowns in reporting structure, quality erosion in reporting, time pressures that impacts learning from incident reports, and maintenance programs where funding does not keep pace with increasing maintenance needs. One of the challenges facing safety professionals and system safety engineering is building recognition and awareness of the safety boundary into the design of systems. An even more challenging situation is the design of system features that push back [26] and resist creep to riskier states.

Along with the identification of both critical properties of complex systems and challenges to the design and operation of complex systems, system thinkers have identified archetypical problematic behaviors of complex systems. These classical problematic behaviors must be avoided in the design and operations to ensure safety. One archetypical behavior in particular is the treatment of symptoms rather than problems. Due to the effects of dynamic complexity, policy makers often implement solutions that treat the symptoms of the problem rather than the problem itself, particularly when the cause of the problem is not immediately obvious [26] [64] [65] [58].

Created in the 1950s by Forrester, system dynamics is a method used to model complex systems. Causality in complex systems is often misunderstood due to feedback relationships and delays. System dynamics explicitly models feedback relationships and delays so that the dynamics of complex systems can be understood and manipulated. System dynamics models can be expressed with casual loop diagrams that show the influences between system state variables, or they can be made executable to show the influence of policies on system outcomes. Causal loop diagrams are built from two basic loops: reinforcing loops and balancing (or goal-seeking) loops. These two loops are shown in Figure 1.

In a reinforcing loop (or positive feedback loop), a change in the value in ‘‘variable 1’’ leads to a subsequent change in the value of ‘variable 2’. As indicated by the ‘+’ sign, a change in ‘variable 1’ leads to a change in variable 2 with the same polarity, i.e. an increase in ‘‘variable 1’’ will lead to an increase in ‘variable 2’ and similarly, a decrease in ‘‘variable 1’’ will lead to a decrease in ‘variable 2’. If made executable, reinforcing loops can express exponential growth or decay. The other loop building

block, balancing loops, are used to represent goal-seeking behavior. As shown in Figure 1, a difference between the value of 'variable' and the goal value will generate a corrective control action. If the value of 'variable' is less than the goal value, a control action will produce an increase in 'variable' that in turn decreases the value of the 'gap'. This behavior produce control actions that seek to minimize the value of the 'gap' variable.

The third element used in causal loop diagrams is a delay marking. Shown in Figure 2, the marking indicates a delay between the execution of the control action and when it affects the value of 'Variable'. Delays can adversely affect system stability: controllers are often unable to predict the delayed effect of a control action, and generate new control actions without taking the full effect of the delay, and the previous control action, into account.

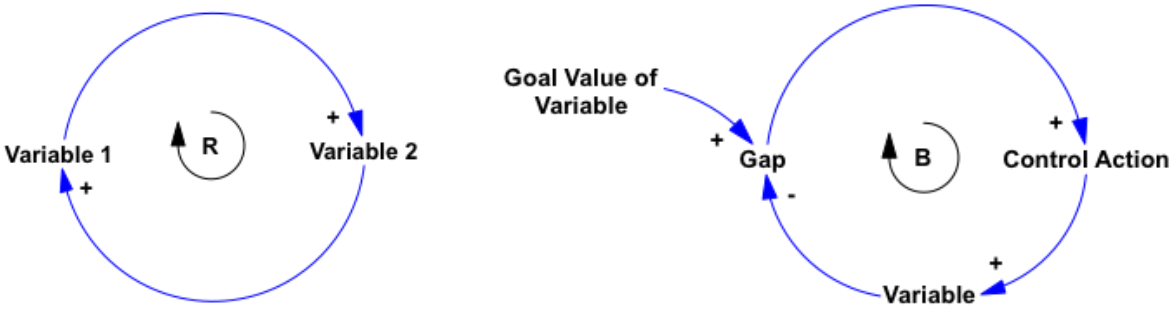

Figure 1 System Dynamics Causal Loop Diagrams: Reinforcing and Balancing Loops

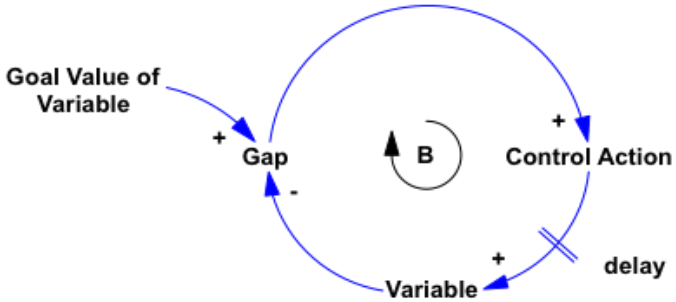

Figure 2 Balancing Loop with a Delay

System behavior archetypes may be represented using system dynamics Causal Loop Diagrams. For example, in the *Burning the Midnight Oil* Loop, shown in Figure 3, the solution to a common project

management problem, being behind schedule, is solved by increasing overtime. For a short while, productivity is improved and the factor makes up some schedule slip. However, after a time delay, the overtime leads to exhaustion and an increased number of mistakes, diminishing productivity. The company falls further behind than when it started due to an increased amount of rework. Rather than attempt to make up schedule by changing due dates, hiring additional workers or increasing worker efficiency through process innovations, management increased its problem by not correcting subtle issues in the company. The generic archetype exhibited by this loop is the *out of control* archetype, shown in Figure 4. The archetypical problematic situation is typified by short-term improvement followed by long-term ruin.

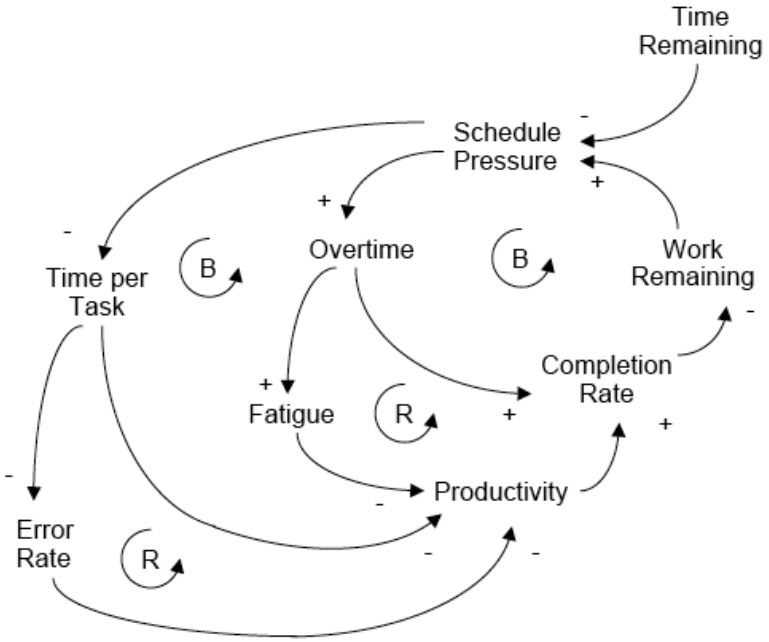

Figure 3 Burning the Midnight Oil [63]

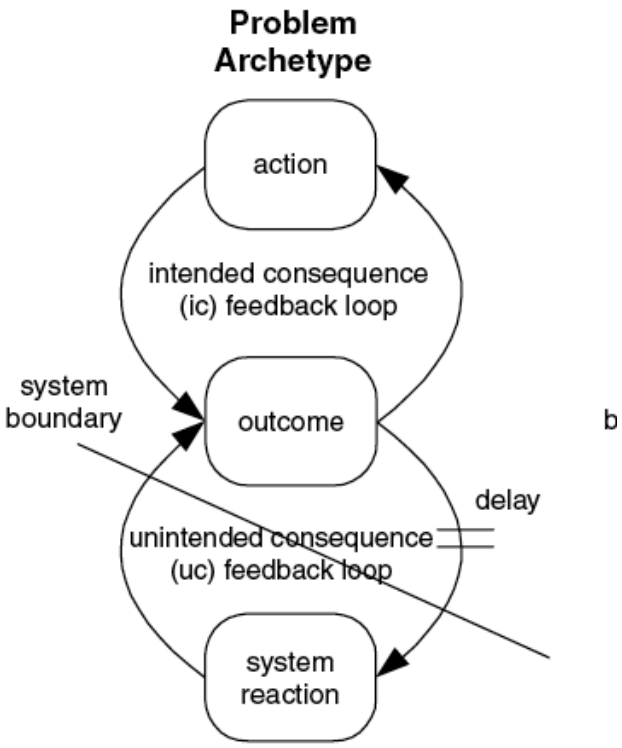

Figure 4 Generic Problem Archetype: Out of Control [278]

Marais et al. extended these problem archetypes to safety and identified key instances of these archetypes within NASA. For example, in Figure 5, Marais identified a typical safety archetype: Failed reward schemes to improve safety. Managers attempt to improve safety awareness through incident reporting. Initially incident rewarding goes up and safety is improved, however, after a time, employees with the cleanest safety records are rewarded and the incentive to report goes down. In Marais research [65], the safety at NASA was lower after this reporting scheme was put into place. For safety to be improved, all parts of the organization that affect it must be analyzed, from the reporting schemes to promotion policies.

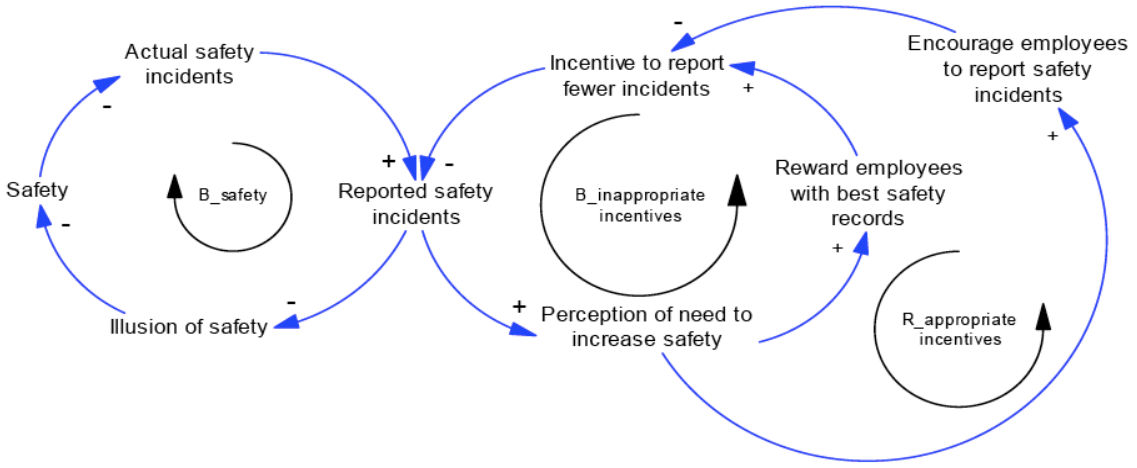

Figure 5 Safety Archetype: Ineffective Reward System For Safety

An example of treating symptoms rather than problems can be found in healthcare. A hospital was experiencing severe delays in the discharge of patients and sought to correct the problem by eliminating the bottleneck and hired additional full-time blood sample takers. While discharge times briefly improved, the hospital continued to experience long discharge times, and bottlenecks appeared elsewhere in the system. Discussion amongst members of the hospital problem-solving team did not yield insights. It was not until system dynamics experts and hospital operations experts together created a systemic model did they realize that resident decision-making time was the highest leverage variable for improving patient discharge time. The biggest contributor to hospital discharge time was masked by complex decision-making processes within the hospital. A model of the hospital system, rather than just the patient processing chain, was necessary to ferret out solutions that would improve discharge times [50].

A systemic view should not imply that systemic solutions necessarily come in the form of broad, sweeping reforms. The best solutions are those high leverage policies that provide small and focused solutions producing large and lasting improvements [26]. These high-leverage solutions are usually not obvious to system participants; otherwise, they would have been found and implemented. High leverage points are not closely related in time, space, and form, so a systems approach is needed to find them.

Event-based approaches are inadequate, as they lend themselves to treatment of symptoms rather than causes and to not encourage systemic understanding of the systems. In safety, the treatment of the symptoms can hide the existence of crucial safety problems and even improve safety for a short period of time before the system becomes less safe than before [76]. In another example, if an aircraft crashes due to a poorly maintained jackscrew, the recommendations may include the termination of the experienced

maintenance technician or improved maintenance procedures. Broad-reaching, systemic issues within the system may be ignored, such as the effect of company financial difficulties on the maintenance division's budget and technician training. In the short-term, everyone in the maintenance program may devote extra time and attention to their work, resulting in improved safety. However in the long-term, firing an experienced maintenance technician lowers the average experience within the team, and budget shortfalls will continue to adversely effect the division. Marais and Dekker have both cited the treatment of symptoms rather than finding systemic solutions as a common, unfortunate problem in safety management [76][65][17][18].

A successful hazard analysis method must be capable of moving beyond analysis of events and must be able to address systems that are dynamically complex, not just detail complex. As Senge says, focusing on events leads to "event" explanations and obscures the long-term patterns of change and the systemic factors behind those patterns [26]. The hazard analysis method must also leverage the dynamics' problematic archetypes identified by systems thinkers to avoid instances of these behaviors in new systems. Without systemic understanding of systems, systems that exhibit dynamic complexity will be subject to policies where overshoots and undershoots are common and treating symptoms of problems is the rule.

2.3 Management Approaches to Organizational Safety

Researchers in management and organizations have developed two popular theories of accidents and the role of organizations in safety: Normal Accident Theory (NAT) and High Reliability Organizations (HRO). Both are discussed in detail below.

2.3.1 NAT

One major theory behind the impact of organization on safety is that of Normal Accident Theory (NAT). The basic idea behind Charles Perrow's NAT [53] is that accidents occur in complex socio-technical systems because of tight coupling and interactive complexity. Prevention of normal (system) accidents cannot be prevented with redundancy techniques commonly used in electro-mechanical systems. Perrow notes that the addition of redundancy to tightly coupled, interactively complex systems adds further complexity and increases the risk of accidents [53].

Perrow considers all system accidents to be the result of unanticipated component failures. He further states that not all component failures can be anticipated due to the interactively complexity and tightly coupled nature of complex systems. Perrow contends that many systems are necessarily interactively

complex and tightly coupled and that the occurrence of accidents in these systems is normal in that they can be expected. He takes the pessimistic viewpoint that they are unavoidable. While Perrow's definitions and classifications of complex systems along the dimensions of interactively complex and tightly coupled have been criticized elsewhere [52], it is worth noting that accidents can occur when all components and subsystem work as intended and designed, that is, accidents can result from unintended interactions between subsystems and components [7][5][8].

2.3.2 HRO

Another theory of the relationship between organizations and safety is articulated by High Reliability Organization[3] (HRO). HRO maintains that some tightly coupled, interactively complex organizations achieve high levels of safety and have been free from accidents because they are highly reliable. The trademark of an HRO organization, as noted by La Porte and Roberts [36][55] [68][69], is that they have expert-level people, a strong commitment to safety, stable technical processes, and a commitment to being a learning organization. While not every complex system has the luxury of a stable technical process, the other noted facets that exemplify an HRO are desirable for any organization [26]. However, the above listed organizational facets are not enough to ensure safety of the system, and it is not clear how to achieve them. For example, without an understanding of how managerial policies will affect system safety, a 'commitment to safety' is not enough to achieve safety. The struggle to become a learning organization is constant and extremely challenging, as noted by Senge [26].

Aside from the HRO authors' uncertainty regarding the definition of reliability (which has been highlighted elsewhere [52]), the biggest definition problem with HRO is the rebuttal to NAT by noting organizations that are "high reliability" (which is never really defined) in spite of the highly coupled nature of the system. But the examples they cited in the HRO literature, which include the air traffic control (ATC) system, are in fact highly *de*coupled. ATC planes are routed in non-overlapping, mutually exclusive, and collectively exhaustive sectors across the country, and handoffs between them are tightly controlled. Each of these sectors, which are further divided into flight levels, includes regulations for aircraft type and flight patterns allowable for each level to promote safety. Moreover, temporal decomposition into phases of flight (landing, cruise, take-off) adds levels of safety. ATC was purposefully designed to be loosely coupled and non-interactively complex.

[3] The term "HRO" is widely used as both the name of a body of safety and organizational theory, and to characterize companies and organizations that achieve goals and conditions set by HRO theorists.

In an HRO organization, it is claimed that the operators know the technical process well, and due to the stability of the process, operators are able to predict the system's behavior over time. However, such a level of stability, observability, and knowledge of the technical process cannot be achieved in complex systems. For example, in health care, complete patients histories are not always known, yet surgeons must operate without them. In another example, an elderly patient taking a dozen medications, for which the drug interactions are not known, is still prescribed medicine in the face of great uncertainty by doctors. In other ways, the health care system exhibits HRO features like high technical expertise, preoccupation with failure, and continual striving to learn from accidents. Yet despite these positive features, the healthcare system is far from achieving the safety records claimed to be associated with HRO systems.

HROs strive to maximize learning from accidents, incidents, and near-misses [36]. While this is a solid idea and, certainly, learning from accidents is why investigators bother to analyze accidents and write insightful reports, investigators 1) often don't understand the full scope of problems within an organization and simply blame people for accidents and 2) are not very good at implementing lessons learned from accidents. Furthermore, in the development of many safety-critical systems, there may not be the luxury of learning from low-cost incidents or near misses. In these systems, accidents must be prevented before they occur.

Weick [54] claims that HROs are successful because of their successes in creating the right behaviors and attitudes. Shrivastava cites the following management failures of "poor training" and "motivation" for operators, and cuts in staffing (manning) leads to accidents [73]. In order to protect against cultural problems and organizational failures, Shrivastava recommends improving organization culture through, for example, the continuity of top management. While the value of a strong culture (see "just culture" and "safety culture" [19][17][8]) is important for all organizations, culture is not separate from the rest of the system and cannot be strengthened without consideration for the whole. HRO theory would be better served to recognize that the whole system must be considered to ensure safety.

Another facet of HROs is that they empower decision-making on the lowest levels of the organization [68]. While micromanagement is inefficient, safety-related decision-making should be in the hands of those that have a systems view because safety is a system property. Putting safety-related decision-making authority in the hands of low-level operators is dangerous, because operators only have a local view of the system and so may make decisions to achieve their personal goals at the expensive of system safety goals. However, HRO theory further claims that decision-making at low levels of the organization empowers operators in times of stress. But there is a difference between empowerment during times of stress and lack of guidance. In a recent oil refinery accident, all operators

were empowered to evacuate the plant, as they were the closest to chemical process and would quickly notice if a toxic release occurred. However, the operators did not evacuate the plant, as they were operating in an environment where false alarms were high and the personal cost of sounding an evacuation high [85]. More than just being used as an excuse to blame low-level operators, safety decision making at the low levels of the organization is dangerous. Policies and organization design must exist to support operator decision-making at all levels of an organization, putting low-level operators on the hook for safety is not effective.

HRO also claims that operator training is an essential feature of safety systems. [68]. For instance, in a particular nuclear power plant cited by Roberts [68], operators spend 25% of their work time on accident-preparedness training, and she claims that this training ensures safety. This claim is invalid for two reasons: first, training on this level is unsustainable and ineffective for the assurance of safety, and second, there is no scientific data supporting the claim. The lack of scientific rigor will be discussed later in this section.

Extremely high training levels are financially unsustainable for most organizations. In organizations where accidents have high public visibility, and operator training is heavily emphasized, such as in commercial aviation, pilots undergo "continuation training" once or twice a year. Furthermore, training is often inadequate. Systems are constantly evolving, and training usually only accounts for a set of conditions based on an outdated model of the real system and will not be useful for the real-life situations operators face. In commercial aviation, as in all industries, safety must be achieved in systems without relying exclusively on operator training. The system must be designed to be safe in the beginning, and safety flaws cannot be "fixed" with training. In the Three Mile Island accident operators were trained at the levels required by the Nuclear Regulatory commission [7][9]. While their training procedures were inadequate and did not convey basic understanding of reactor physics, the system had numerous, systemic safety problems, and better training could not have eliminated these issues. The amount of time spent in training does not correlate with safety in a system.

Roberts [68] suggests aligning pay for operators and managers with safety. In fee-for-service health care practice, financial incentives for delivery of care are tied to production, not safety [71]. However, it is easy to find bad example of unsafe system with poorly designed compensation policies, but it is also true that incentives are always conflicting. Complex systems are usually attempting to satisfy many goals at once. Safe organizations have conflicting incentives as well.

In a similar vein, many HROs glibly report that communication of the big (safety-related) pictures is important. Another concept related to HROs is that of heedful mind and collective interrelating. These

concepts basically illustrate the challenge of sustaining an accurate mental model for each person in an organization. The other feature of heedful mind and collective interrelating is that it aids organizations in resisting inertia and complacency [59]. These concepts are a "Zen goal" for organizations but do not give much guidance in achieving them.

Considering that communication is one of the most important jobs of management [26], it is hard to argue that communication is unimportant. The challenge is designing successful communication into the organization that ensures safety. In operations, the communication of safety is typically made using static signs and is ineffective. For example, signs imploring physicians to wash their hands have been ineffective at increasing hand-washing compliance [109] [132]. Operators become complacent or form mental models that they are not at risk of spreading disease. A new way to maintain safe operations is needed.

One of the primary solutions advocated by HROs is that of redundancy. Redundancy is not effective when used to duplicate non-hardware parts of systems. Redundancy cannot prevent accidents caused by design errors or flawed decision making. If a surgeon has a heart attack (the closest thing to a component failure), then having other surgeons available to operate on patients makes sense. A team of doctors treating a patient may be helpful, as they should all be able to diagnose complex pathologies more easily than a single doctor. But that is not necessarily so and it is NOT redundancy—the doctors on the team all have different expertise and play different roles. Redundancy is "the ability to provide for the execution of a task if the primary unit fails or falters [55]." Cogent teamwork and team diagnostics cannot be described as an implementation of redundancy.

A major flaw with the above HRO claims is the lack of insight. HRO has claimed that basic management features, such as communication, proper incentives, motivation, and "Big Idea" thinking are essential to safety. However, these claims are empty and superficial. No one will argue that communication within the organization is *bad,* however, HRO has not defined implementable communication requirements that have been shown to improve safety. Furthermore, HRO researchers have not shown that organizations without the features listed above do not have good safety records. Substantive and logical methods for designing and shaping safe organizations are needed, not vague statements about "big idea thinking."

2.3.3 Organization and Safety: Deviance

Vaughan defines organizational deviance as an "event, activity or circumstance, occurring in and/or produced by a formal organization, that deviates from both formal organizational design goals and

normative standards or expectations, either in the fact of its occurrence or in its consequences and produces an unanticipated suboptimal outcome“ [58]. There are several factors that influence deviance, including the organizational setting (networks and relationships) and the social context (political, technological, economic, legal, demographics, ecological, and cultural). Instances of organizational deviance include mistakes, misconduct, and disaster, but these occurrences of deviation are hard to classify, as Vaughan notes, because classification is relative to the social norms of the group doing the analysis. Furthermore, these events are classified after an accident has occurred, and this is problematic, as discussed previously.

Vaughan presents a key insight into organizations. She notes the tension between the level of central and decentralization in organization structure. Structures that promote rapid, effective decision-making in a crisis may stall and stagnate routine decision-making. Organizational design that exhibits a high degree of centralization may provide great coordination but less flexibility in system-wide decision-making [58].

Vaughan has cited trends in disaster research. Organizational factors that contribute to organizational misconduct and can lead to accidents include “conflicting goals, performance pressure, deadlines, escalating commitment, reward systems that reinforce productivity and undermine safety, and [the] decline of resource slack.” [58]. Competition and scarcity increase the risk of accidents in cases where management has made safety tradeoffs to save money. Safety however, does not need to come at the expense of other resources [7]. If safety is considered early enough in the design process, it can be designed into the system synergistically with other design goals [12]. Vaughan states “preventive strategies must go beyond individuals to institutional and organizational factors that shape individual cognition and action” [58]. Consideration of organizational design to avoid negative safety effects related to the factors listed above is a key factor for the safety of an engineering system.

2.4 Other approaches to Organizational Safety

Some researchers have tackled organizational safety from a culture approach. A key body of work for the design of safety in human-operated systems is that of “Safety Culture” [105][106][107] and “Just Culture” [17][108]. Safety culture is defined as “The product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization’s health and safety management” [106]. Just culture is defined as “an environment in which the reporting and sharing of information is encouraged and facilitated” [108]. Changes to an organization to achieve a healthy safety and just culture have been implemented in several industries, including aviation and healthcare [16][17].

Safety Culture and Just Culture are key aspects of any socio-technical system that hopes to operate safely. Leveson claims “blame is the enemy of safety” [9]. Building accountability into a system without blame is key for recognizing dangerous situations and learning from past incidents or accidents. However, accountability must not come at the expense of a blame culture.

Until recently, the human factors literature and accident investigators have centered analysis of the role of humans in accidents on factors contributing to human error, such as fatigue and “loss of situational awareness” [56][30][15]. At times reports have left their analysis of human factors with accounts of actions without understanding of contextual factors that account for human “errors”. New work by Dekker has refuted the “blame the operator” mentality in an effort to move past blame and into a non-normative understanding of human decision-making. From an operator’s mental model to an organization’s culture, this new work has contextualized human decision-making and explained behavior with an eye to local operators’ incentives and pressures [16][17][18][19][20].

Safety Culture and Just Culture help organizations and investigators move past blame. However, creating and fostering a healthy safety culture and a just culture is challenging. As Simon [41] reports:

> "Culture change is a distinct model for the continuous improvement of safety performance. Whereas behavior modification is an individual-based training method in behavioral observation analysis and feedback, culture change is a system-wide change effort, and the ‘organizational culture’ is the client system. A behavior modification project would increase the number of safety behaviors while stopping short of changing the organization’s core values. Culture change requires analysis of systems that hold norm assumptions and beliefs in place. It is strategy development carried out by leadership.”

Schein has noted that culture is not homogenous within an organization, and subcultures must be considered in order to design and maintain a safe organization. These subcultures are operator culture, engineering culture, and CEO culture. The operator culture is centered around people whose success is dependent upon trusting relationships within the company and whose system view is that of intra-organization connections among operators. The engineering culture consists of individuals whose bonds stem from common education in engineering disciplines. Schein states that many engineers wish to solve problems and resolve operational uncertainties by designing humans out of a system. Similar to the engineering culture, the CEO culture is comprised of individuals with bonds external to the companies

and forged by common education. CEOs are very concerned about the financial "bottom line," as their success depends on shareholder and board approval. CEOs are also far removed from the operating process and often feel like they cannot trust information they receive about the operating state [74].

Dekker has identified key ingredients to promoting a healthy safety culture, including management commitment to safety, understanding of operational safety and risk, employee empowerment to influence operational policies, connection of incentive structures to safety and safety reporting, effective flow of safety-related information, and learning from incident reports [18]. Unlike HRO theory, Dekker ties his work to numerous examples and industries, more judiciously relates management principles to safety, and does not claim these organizational facets will guarantee safety, or that systems without these cannot be safe. For example, "employee empowerment to influence operational policies" is far different from HRO's "employee empowerment to make safety-related decisions at the lowest levels of the organization" [68]. The latter organizational feature is used in HROs to fix system safety problems through operations, which is problematic, as discussed previously. In contrast, Dekker states that organizations that value and act upon operator suggestions and identifications of safety problems, have a better safety culture. A safety culture (an emergent feature of an organization) is helpful to ensure safety.

2.5 Accident Models

Hazard analysis methods and other safety engineering techniques are always based on an accident causality model. Linear-event chain models, such as those that can be represented by fault trees (e.g. Heinrich's Domino Theory [99]) and Reason's Swiss Cheese Model [2][3], are most commonly used. Control-based accident models such as Hollnagel's Functional Resonance Accident Model (FRAM) [4] and Leveson's System-theoretic Accident Model and Processes (STAMP) [5] are more relevant to the safety of complex systems.

2.5.1 Linear Accident Models

Linear accident models view the occurrence of accidents as the result of a chain of events or linear sequences of failures. If one event in the proximate causal chain is prevented from occurring, the accident will not occur. Thus, hazard analyses based on linear accident models are geared towards finding sequences of failures that can lead to accidents.

The first model of accidents, developed by Heinrich in the 1920s, stated that accidents were the result of a chain of events, each represented by a domino. If the first "domino" fell, the next domino would fall, eventually resulting in an accident. The solution then was to remove a "domino" to prevent accidents.

The first domino, Social Environment and Ancestry covered personal flaws such as greed and recklessness. The second domino, Fault of Person, also cover personality flaws, but those that are induced by flaws in the operator's family. The third domino is unsafe act or unsafe condition, such as starting up machinery without calling out a warning. The fourth domino is the accident itself, and the fifth domino is the resultant injury.

This accident model is grossly inadequate. The first two dominos (largely similar) are arbitrary labels assigned to individuals to aid in the assignment of blame. The model implies that accidents are initiated by bad or flawed people and then proceeds in a linear fashion. Even within an event-based framework, the domino model only examines one cause or event for each link in the event chain. No systemic or management issues or issues are examined.

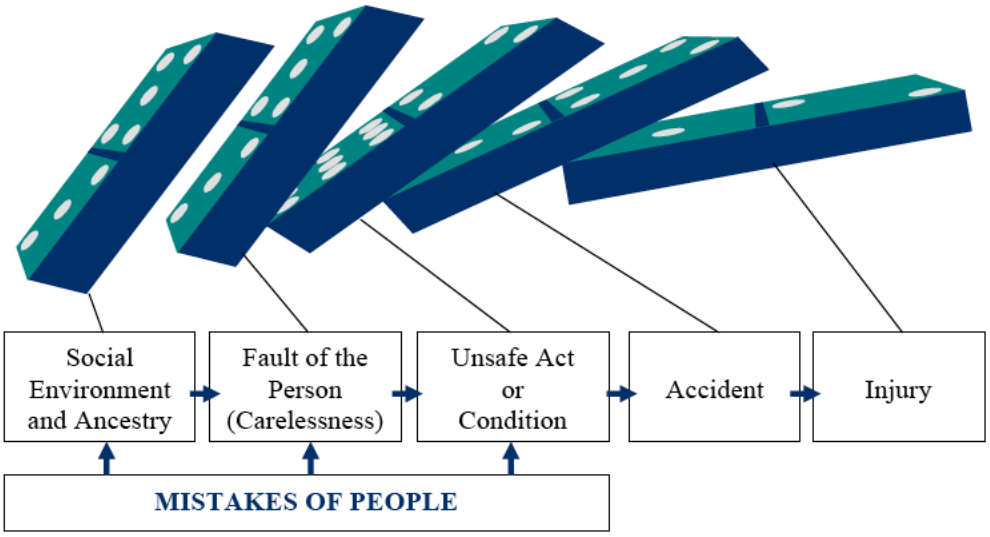

Figure 6 Heinrich Domino Theory Source: [100]

In 1976, Bird and Loftus updated Domino Theory to consider managerial issues and property loss [101]. The updated dominos were now labeled, Management: Loss of Control, Origins: Basic Causes, Symptoms: Immediate Causes. Contact: Incident and Loss: People-Property. The first domino is failure of management to plan, organize, lead and control. The second domino continues to include personal flaws, such as bad attitude, but also covers job factors, such as inadequate equipment. The third domino represents the symptoms caused by factors identified in domino 1 and domino 2. The fourth domino

represents the loss-creating event. Finally, the fifth domino is the loss, which can include property damage as well as injury.

The updated Domino theory is still as flawed as the original. While stepping slightly away from laying all the blame at the foot of the operator, it includes potential to blame managers as well, yet still does not uncover systemic organizational factors.

One of the most widely used modern linear models is Reason's Swiss Cheese. The Swiss Cheese model [2], [3] views the occurrence of accidents as the result of failures within each layer of the system "lining up." In Reason's model, the layers consist of active failures, preconditions for unsafe acts, unsafe supervision, and organizational influences. The latter three categories are considered to be latent. Active failures are those actions and events that are causally related to the loss and occur during operations.

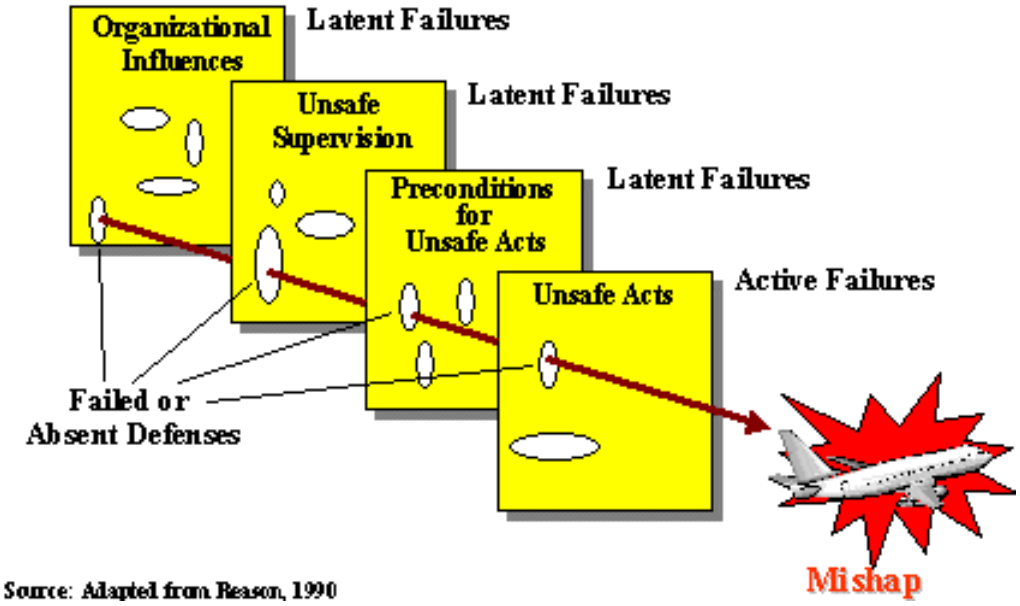

Figure 7 Reason's Swiss Cheese Model of Accidents

Preconditions for unsafe acts are conditions that exist during operations and lead to the unsafe acts, such as operator fatigue or poor communication. This category also covers design errors. For example, a design that places a power switch next to a control switch in a safety-critical system in such a way that leads to mode confusion may be described as a "precondition for an unsafe act."

Reason's next level is unsafe supervision. Unsafe supervision implies that someone is to blame and that he or she did not fulfill the role and responsibilities that were assigned to him or her. In an example, Reason suggests that pairing two inexperienced pilots together in the cockpit is an act of unsafe supervision. If two pilots are both inexperienced, their communication could be poor (a precondition for an unsafe act), which could lead to the failure of the pilot to command the first officer to lower the landing gear (an active failure).

Finally, Reason considers organizational influences. Organizational influences affect all decision-making. For example, productivity pressure can lead to high workload conditions for operators, which in turn can cause to fatigue and lead to active failures.

Reason's Swiss Cheese model is flawed for several reasons: by categorizing three categories as *latent,* the model masquerades as a system model, when in fact all of the categories require direct causality and may accurately be labeled as an event-chain model. The only difference between the latent and active failures seems to be that latent events take place well before an accident. The distinction between unsafe acts and conditions is arbitrary and classification of "active failures" and "latent failures" will vary between safety experts performing the analysis. Reason's Swiss Cheese model is simply an obfuscated domino model.

For example, one latent failure is *inadequate supervision*. Inadequate supervision, however, could be considered an active failure. For example, in an aircraft accident, we can trace events back from the accident-initiating event in the following manner:

> Maintenance technician did not adequately grease screw. -> Maintenance technician was in a rush, and manager did not check logs to make sure that all safety-critical tasks were performed. -> Maintenance turn-around time was compressed. -> Airline management was under financial pressures.

Was the maintenance manager's failure to check the logs an active failure or a latent failure? Furthermore, is a state of financial duress an event or a condition? Reason labels both events and conditions as "failures."

In complex accidents, it may be instructive to continue the analysis and discover why and how latent failures came to be. In other words, the analysis should not start from a causal event chain, examine "why" issues three times (or five times, as in the "5 Whys" approach [139]), and then stop. The analysis

should focus on instances of inadequate control for each of the relevant actors (controllers) in the system and the systemic factors that led to this inadequate control.

2.5.2 Non-linear Accident Models

FRAM

The Functional Resonance Accident Model (FRAM) [4] is a systemic accident model based on the notion that accidents occur as the result of unanticipated resonances between systems and typical noise in the system environment. Accident prevention methods using this model focus on the design of systems that are robust to disturbances and noise. Furthermore the system is analyzed for resonance modes, which may be triggered in operations. This accident model moves away from the linear-event chain and recognizes that safety is an emergent system property. Furthermore, it places emphasis on the very real problem of the unanticipated effects of disturbances on system operation [4]. However, FRAM does not provide any guidance for how to discover resonance modes within the system or address system migration to high-risk operations.

STAMP

STAMP is an accident causality model in which accidents stem from inadequate control or inadequate enforcement of safety-related constraints on the design, development, and operation of the system. Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interactions among components that result in a violation of system safety constraints [5]. STAMP treats safety as a control problem; accidents occur when component interactions and disturbances are not controlled, when components fail or when feedback is corrupted or missing. If a system is adequately controlled, no unsafe states exist and no safety constraints are violated.

Figure 8 shows generic example hierarchical control structure is shown. Each level in the structure imposes control on the level below it and receives feedback from it. Both system operations and system development are shown as they are both responsible for the enforcement of safe system behavior. Figure 9 shows the how the inadequate enforcement of safety constraints can lead to hazardous system states.

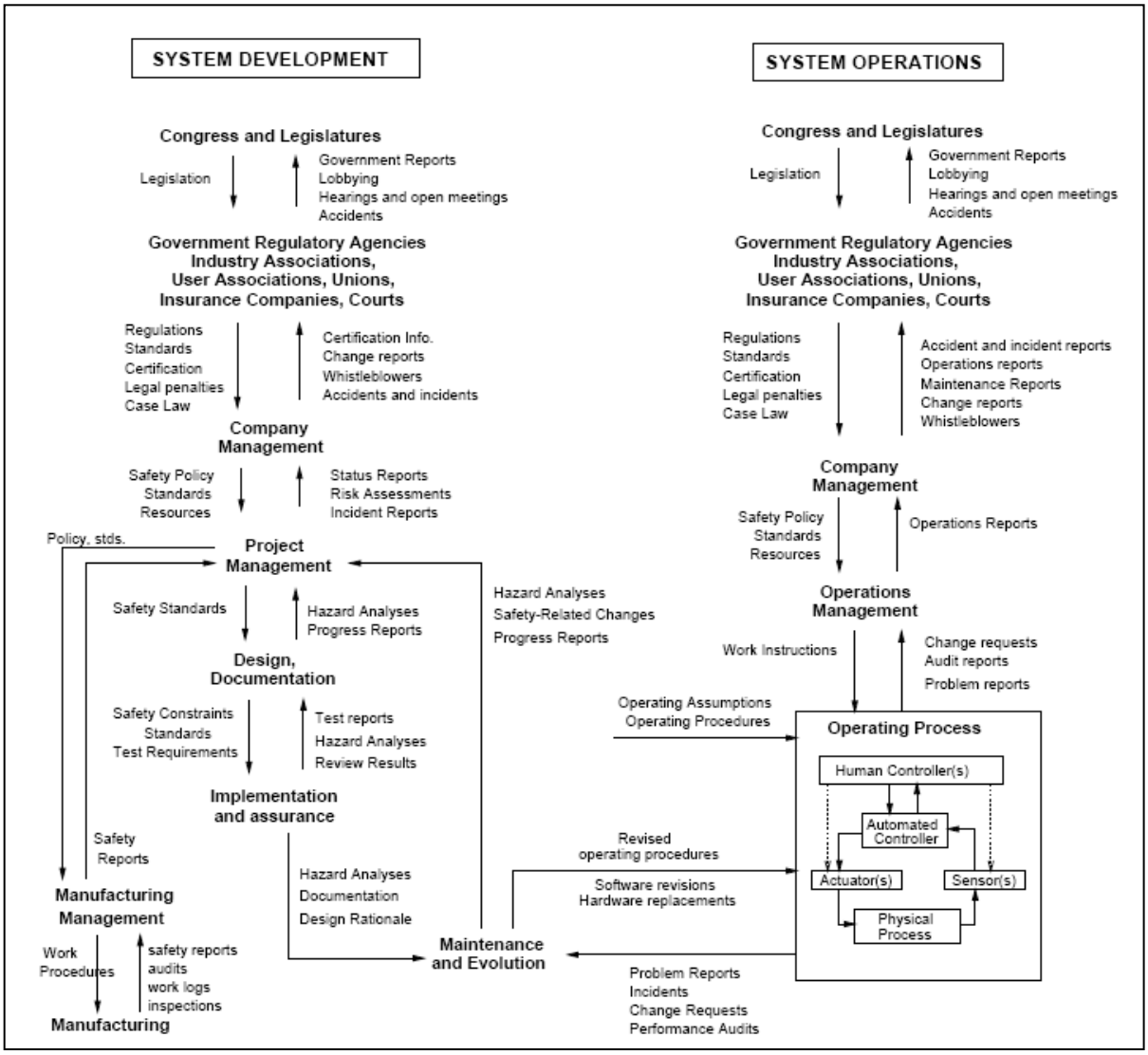

Figure 8 Generic Control Structure Source: [5]

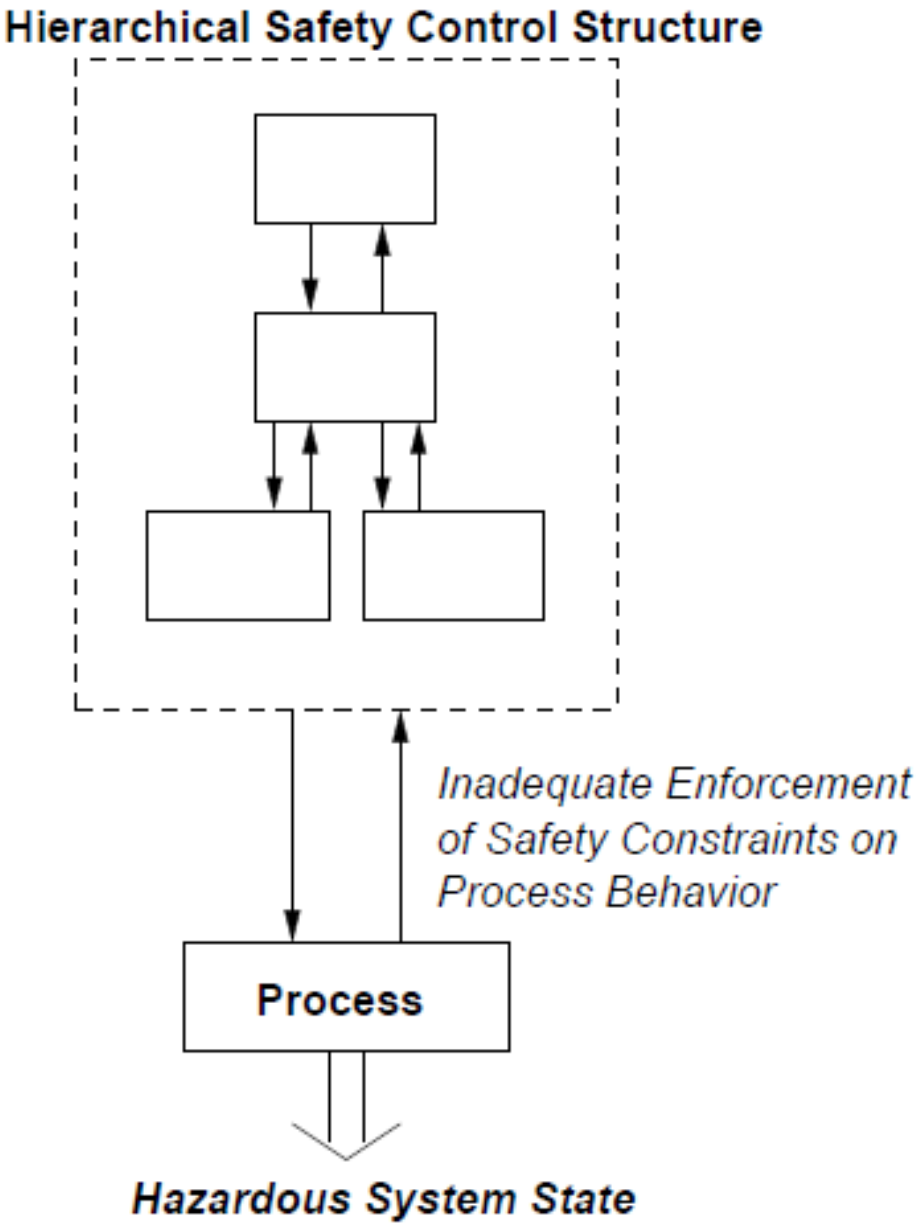

Figure 9 STAMP Causality Model Source: [8]

Any controller in the hierarchy must contain a model of the system being controlled. The model of the process may contain only a few state variables (such as can be found in a thermostat) or hundreds of state variables and transitions (such as that required for a spacecraft). For proper control, the process model must contain: the current state (the current values of the system variables), the ways the process can change state (the system dynamics), and the target values and relationship between system state variables

(the control laws). This process model is used by the controller (human or automated) to select control actions. The process model is updated through feedback from the process.

Accidents result when the process model does not adequately match the controlled process and unsafe control actions are provided (or safe ones not provided) as a result. The mismatch between the controller's model of reality and reality itself is called a mental model flaw [5]. As Dekker [18] states, the loss of situational awareness is equivalent to the difference between "what you now know the situation was actually like" and "what people understood it to be at the time." Situational awareness has also been defined as the ability to understand the operating environment and predict future system state and control actions [86], or in STAMP parlance, the ability to select the correct control actions. In many modern accident reports, analysts have cited "loss of situational awareness" as a cause of the accident. The labeling is not informative; as the occurrence of a mental model flaw (loss of situational awareness) is indeed the reason for inadequate control, but it does not point to the causes of the mental model flaw itself.

A link between STAMP and system dynamics exists. Dulac [158] created control structures in the normal STAMP manner, but made each controller an executable system dynamics model. Since both methodologies are based on systems theory and control theory, they can be integrated and used synergistically.

Comparison of STAMP to Linear Accident Models

Event-chain model based accident analysis often overlooks system factors and the existence of complex feedbacks are ignored [8] [76]. Without consideration of systemic solutions, engineers are left to design for the reduced likelihood of particular events, rather than for the elimination of hazardous states throughout a system. The specifications based on event-chain models focus on end-states (accidents) and preventing the failures that lead to them, rather than the hazards or conditions leading up to them [6][7]. Furthermore, linear models often assume independence of failure events and are not able to address systemic factors that push systems into high-risk states or create dependent proximate causal factors [5] [7] [8][9][10].

In particular, use of the event-chain model leads to a "defense in depth" engineering strategy common in the nuclear industry. The tenet underlying this technique is that, with the correct design of barriers, the propagation of failures will be limited, and accidents will not occur. For example, to limit the probability of an accident, engineers design high pressure-resistant reactor vessels, explosion containment buildings

and air filters to prevent the release of toxins to the surrounding area. One problem with this approach is that independence of failure of the barriers is assumed, but systemic factors can affect the operation of multiple barriers. Another feature of defense in depth is to "[assure] that ultimate safety does not depend on correct personnel conduct in case of an accident" [7]. Said more plainly, humans should be designed out of safety defenses. The defense in depth approach is limited, though, because the barriers are intended to break apart linear event chains and cannot prevent systemic factors. Furthermore, people are excellent problem solvers, and minimizing their role in troubleshooting safety problem is a wasted opportunity.

Rather than examine accidents through an event-filtered lens, it may be more helpful to examine accidents with a systemic control-theoretic view. Organizational actions, decisions, or goals can be analyzed in context: why did these actions, decision or goal states make sense to decision-makers at the time? For example, if an aviation accident involves inexperienced pilots paired together in the cockpit, due to "inadequate supervision", the analysis should not end with just a classification. In order to learn more from the accident, other questions should be investigated: If sufficient resources for staffing planes with expert-level pilots were unavailable, what other goals were important to the organization at the time, and what mental model flaws existed so that inadequate staffing was considered safe? Systems must be designed so that mental models more accurately reflect reality.

2.6 Hazard, Risk and Accident Analysis Methods

2.6.1 Linear Accident Model based Methods

There are several risk and hazard analysis methods based on linear accident models, such as Failure Modes and Effects Analysis (FMEA) [140], Fault Tree Analysis (FTA) [141], Probabilistic Risk Assessment (PRA) [142], and Hazard and Operability (HAZOP) Method [11]. These methods all rely on principles of linear-event chain models and are ill suited to assessing risk in complex socio-technical systems [7]. These techniques are useful for non-software-controlled electro-mechanical systems, where failure rate data is available, and redundancy can be added to reduce the probability of an accident. FMEA, FTA, PRA, and HAZOP focus on failure events and failure-event probabilities to calculate the probability of system failure.

Quantitative Risk Assessment for Human Factors

For many traditional approaches, human error is considered to be a deviation from the correct or normal behavior [57][32][54][58][59] and should be minimized. However, classification of a human act as a deviation requires that we know what the "correct" action should have been. The distinction of deviation

versus correct action is typically made after an accident has occurred and is subject to hindsight bias and outcome bias [19]. For the human operator involved, safety-related decisions seemed to be correct at the time. If the operator knew the decision would result in a catastrophe, he or she would have made another choice.[4]

Four techniques for human error probability calculation are the Technique for Human Error Rate Prediction [32], Accident Sequence Evaluation Programme [33], PRA [142], and Human Reliability Assessment [56]. These human reliability assessments refer to "failure" as a "mistake" or "error" and seem to consider people to be roughly interchangeable with fan belts, gauges, or reinforced tank cladding. This class of techniques output human error probabilities or the number of observed errors compared to the number of opportunities for error [30].

When humans are involved, these approaches assume a specific likelihood of human error in the calculation of failure. Research in the nuclear industry has compiled a large database of human actions, deviations from procedures, errors, mistakes, and slips. From this database [56], human error events are drawn to calculate human failure probability. It is impossible to identify all human deviation events in all systems. Quantitative risk assessment techniques were created for conventional electro-mechanical systems, where the relationship between failures and components are clear. For example, the failure rate data for motors is widely available. So while databases for the failure of materials and motors can be used to calculate electro-mechanical system failure, the same is not true for human error in complex systems.

Furthermore, it is impossible even to identify which actions are truly "wrong" without analysis of context—which includes the very thoughts of the operators themselves. Other areas of concern for these methods include deviation identification and generalizability. If the actions are labeled deviations *after* the result of an accident rather than *during* routine operations, they may be subject to hindsight bias. Often, so-called deviations are often encouraged by management, during times of high production pressure and only after an accident occurs are they labeled errors. In addition, the results from human error quantitative assessments are not generalizable to systems outside of the system that was used to collect the data at the time of collection. There are so many factors that impact human operational decision-making that a single probability cannot capture the underlying decision-making context and the dynamic organizational structure motivating the decision-making.

[4]I am assuming the humans in question are not sociopaths or otherwise intend to harm.

The same limitation applies to organizational aspects of safety management. Traditional hazard analysis techniques and quantitative probabilistic safety assessment techniques are inappropriate for the analysis of human and organizational aspects of socio-technical systems for four reasons: 1) It is unlikely that the system structure is known well enough in advance to predict all the types of events that could lead to an accident; 2) Their application requires a complete system design; 3) They do not capture dynamic behavior; and 4) The probabilities of human and organizational decisions are not calculable [5][7]. Rather than calculate the probability of human error, infrastructure supporting human operations should be analyzed for safety with a system-based hazard analysis.

Quantitative Risk Assessment for Organizational Factors:

It is hard to imagine the application of quantitative probability assessment to organizational "failures" or flawed management decision-making. Is there a comprehensive database for calculating the probability that management does not hire sufficiently experienced safety personnel? Several such quantitative risk assessment techniques have been proposed for organizational factors, however, including SAM, WPAM, and system dynamics + PRA.

The System Action Management framework (SAM) developed by Murphy and Paté-Cornell [102] is an attempt to include human and organizational factors in quantitative risk assessment. The basic concept underlying SAM is to use typical quantitative risk assessment techniques to find the probability of an accident given certain initiating states. The probability of an initiating state is conditioned on human decisions that can lead to those states. The probability of a particular human decision is calculated by conditioning on identified organizational influences (e.g. incentives, training, policies, procedures, selection criteria). The probability of all combinations of states, human decisions and organizational factors are evaluated to determine the eventual probability of an accident. The abstraction from the technical process to unsafe acts (human decisions) and organizational influences is drawn from Reason's model of accidents.

The SAM method is flawed for several reasons. First, it is impossible to identify mutually exclusive organizational influences on human behavior that lead to accident initiating states. SAM requires that all human decisions that can lead to an accident initiating state are known, and that the probability of a state given a particular decision can be calculated. Furthermore it requires that all organizational factors can be identified and included to determine the probability of a particular human decision. An example in one

paper [102] applies SAM to find the probability of driving accidents and only considers two human factors: whether or not the driver is fatigued and whether or not the driver is experienced. It is hard to imagine how the SAM method could scale to the complex decision-making processes inherent in an oil-refinery or airline. Not every human decision could be identified that could lead to an accident-initiating event. Nor could all organizational influences that bring about individual decisions be identified and calculated.

Another flaw is the assumption that accidents proceed like that of a Rube Goldberg machine. A single organizational influence is not responsible for a single human decision that initiates a chain of events that leads to an accident. The bottom-up approach of SAM would explode in complexity if applied to the real-life multitude of influences on a human decision.

The boundary of analysis in the SAM method does not extend to extra-organizational factors. For example, in many organizations, dangerous cut backs in maintenance arise during financial shortfalls brought about by new competitors or substitutions available in the market. Inclusion of organizational context is necessary to understand the behavior of an organization and assess the risk of an accident.

Lastly, SAM does not consider how the design of the organization influences system behavior. Interestingly, the SAM risk assessment of the technical process does include the technical system design. By choosing to focus on the operations of the organization, and lack of consideration of organizational context, SAM misses a system view of human and organizational factors.

Another attempt to account for organizational influences in quantitative risk assessment is the Work Process Analysis Model (WPAM) [104]. This method uses organizational factors to calculate failure probabilities by treating the organizational factors as common-cause failure modes that can influence multiple poor human decisions. In one example, the use of the WPAM method increased the calculated likelihood of a power plant accident from 6.7 x 10^-9 per year to 5.5 x 10^-7 per year [103] [104]. While this method rightly notes the multitude of calamitous outcomes that can arise from a poorly designed and nonfunctioning organization, WPAM is not suitable for complex systems. WPAM bears the same flaws of the SAM method, does not address risk migration, nor does it consider the effects of feedback.

In contrast to SAM and WPAM, an attempt to bind a systems approach (system dynamics) to the PRA methodology was proposed by Mohaghegh et al. [57]. In their research, they adopted classical system dynamics archetypes of operator job training experience and management commitment to safety and

appended PRA-style calculations for error-producing conditions for several variables. In their system dynamics models, several variables are informed by point probabilistic estimates created using PRA. By following this approach, the system dynamics were simplified, and much of the human and organizational interactions and feedbacks were removed. The accidents were analyzed in a fault tree structure, with an encapsulated system dynamics model for the human elements such as "engine failure due to mismanagement by crew." This was in turn informed by static calculations of human error conditions. While the authors are correct that hybrid approaches to modeling systems using system dynamics can be useful and capture a wide range of behaviors, the use of failure-based approaches removes one of the key strengths of system dynamics—modeling feedbacks and interactions.

Hazard Analysis: HAZOP and HAZOP Extensions

HAZOP was created by the Institute of Chemical Industry in the 1960s [28]. The method is based on guidewords such as *no*, *less*, and *more*, that engineers use when considering how accident scenarios could occur [87]. A complete table of guidewords is shown in Table 1.

Table 1 HAZOP Guidewords [91]

No (not, none)	Late
More	Other than
Less	Before
As well as	After
Part of	Reverse
Early	

The standard HAZOP process is shown in Figure 10.

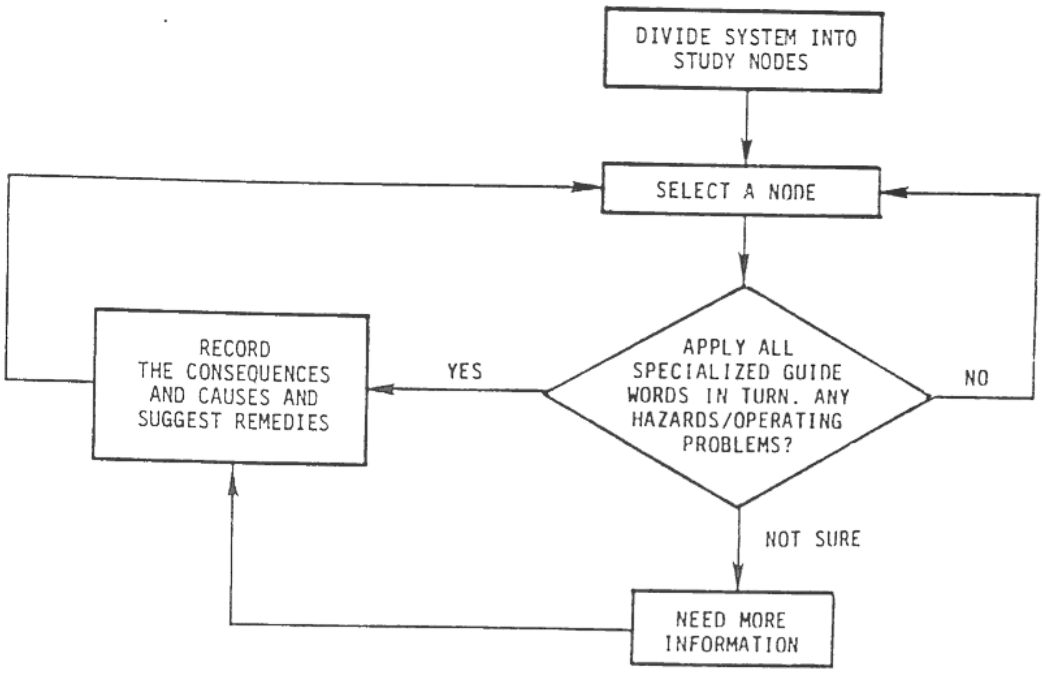

Figure 10 HAZOP Process Source: [88]

For example, when considering the possibility of a tank rupture in a chemical plant, engineers applying the guideword *less* may consider the too-little release of a toxic-acid-reducing reagent. Subsequently, engineers may choose to focus design efforts to the release of sufficient reagent quantities.

Human HAZOP

Human HAZOP is a method for the analysis of human deviations as people operate and implement procedures [27]. The technique, like HAZOP, is performed once the initial design is set. Human HAZOP essentially uses the same guidewords as HAZOP and applies them to human task analysis to find possible deviations from predefined procedures. A diagram showing the Human HAZOP process is shown Figure 11. The resulting table from application of Human HAZOP is shown in Figure 12.

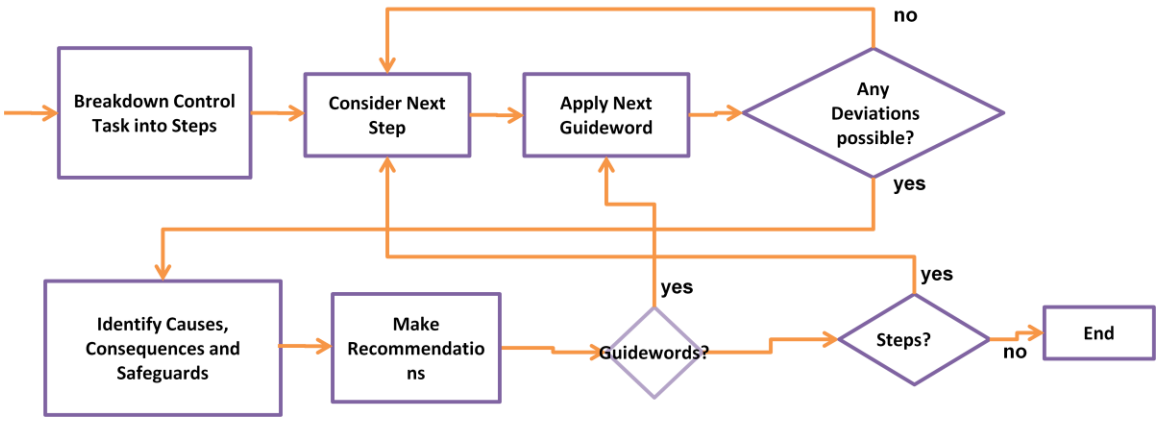

Figure 11 Human HAZOP Process [83]

Project: Time Based Separation		System: Sequence Aircraft following Arrivals Manager advice		
Guideword Deviation	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
1. Wrong Action	1.1. Incorrect information displayed on arrival manager. (flight plan information incorrect)	1.1. Higher workload if controller notices.	1.1. Flight planner and controller training.	1. TBS requires higher equipment reliability and there also needs to be a review of the resolution of radar display and its accuracy to ensure sufficient to support TBS.
		1.2. Potential loss of separation if controller does not notice.	1.2. Airline operator training.	2. More RT required and hence a need for better RT discipline to minimise extra errors. General tightening up of monitoring needed as TBS requires higher controller vigilance.
			1.3. Equipment reliability.	
2. Wrong Action	2.1. Controller reads AMAN display incorrectly.	2.1. If controller realises mistake quickly higher workload	2.1. Well designed HIM	3. How the display flags up changing AMAN information to be investigated (e.g. visual / audible warnings)
		2.2. Potential loss of separation if controller does not notice.	2.2. Controller training.	
3. Wrong Action	3.1. Pilot call sign confusion.	3.1. Higher workload if pilot and controller notices.	3.1. General pilot training.	4. If call sign confusion was shown to be high risk issue, data link or new technology might need to be considered.
		3.2. Potential loss of separation if controller does not notice.		
4. Wrong Action	4.1. Incompatibility between display and real weather conditions.	4.1. Loss of separation when headwind drops.	4.1. ATC detection via radar display.	5. How warnings of incompatibility between display and real life weather conditions are processed need to be reviewed (whether the warnings be from ground equipment, a/c, pilots, etc)
		4.2. Headwind increases, controller has higher workload.		

Figure 12 Human HAZOP Worksheet Example Source: [154]

Human HAZOP was created for task-based operational analysis and does not consider the mental models of the operators. This is unfortunate, as an operator's mental model is the basis for deciding how, when and which actions they will select, which all affect task performance. Furthermore, the mental model provides the basis for decisions to perform tasks in a manner that deviates from accepted norms. Two other limitations of Human HAZOP are that it does not consider broader organizational decisions or design flaws and only considers deviations that occur during operations rather than the design flaws that lead to conditions where human deviations in operations are likely to occur.

Multi-Level HAZOP

Multi-level HAZOP [27] seeks to extend risk analysis to complex systems by integrating the HAZOP and the Human HAZOP methods and applying them to levels of the system in a hierarchical fashion. As in Human HAZOP, Multi-level HAZOP analyzes the operator's procedure step by step. However, Multi-level HAZOP analyzes each step in the operator's procedure along three dimensions: operator, control system and plant/process. For each of the steps in the procedure, the actions required of each component of the system (operator, control system and plant/process) are noted. For example, if the operator is to fill a tank once a certain internal tank pressure has been reached, these actions for each component could be [27]:

Operator: Must check the internal tank pressure, identify appropriate control valve on the display, and command it 'open'.
Control System: Must indicate the correct internal pressure of the tank and actuate the control valve
Plant/Process: The pipe connecting the fluid to the tank must be open and the tank must be at the correct temperature.

The guidewords are used to find deviations and the causes of deviations that could occur during the execution of an operating step. For each deviation at the operator level, a HAZOP analysis is conducted for possible deviations at the control system level. For each control system action, deviations at the Plant/Process level are identified and analyzed. For example, the analysis could find deviations due to humans (e.g., wrong control valve selected), the control system (e.g., wrong display information), and the plant itself (e.g., pipe is ruptured). This process continues until all steps in the operator's procedure have been analyzed, for all written procedures.

The example above demonstrating an application of multi-level HAZOP to a nuclear power plant [27] falls short, as the system is characterized not by dynamic complexity but by detail complexity. The authors use an event decomposition approach and subsequently apply HAZOP to lower-level components

such as valves. The method is focused on the technical process and will not include an analysis of organizations or the human, beyond task execution. While the method may uncover technical problems, similar to the original HAZOP method, it is unsuited for hazard analysis of humans and organizations. Multi-level HAZOP is also unsuited for dynamically complex systems, where task execution cannot neatly be decomposed as in the example above. All of the HAZOP methods are based on linear-event models and must be applied in a bottom-up fashion to designs that are all but complete.

Accident Analysis for Humans and Organizations: HFACS

The most widely used, formal technique for the analysis of the role humans and organizations play in accidents is the Human Factors Analysis and Classification System (HFACS) [15]. This method is based on the linear event-chain model and Reason's Swiss Cheese Model. HFACS seeks to describe the "holes in the cheese," instead of how the holes in the cheese were created and why they persist. It does not offer any guidance to discovering ways to prevent holes from forming in the future or how to assess the risk of the holes "lining up."

HFACS is a lengthy error classification list that can be used to label types of errors, problems, or irksome decisions made by humans and organizations. Using the Swiss Cheese model, HFACS categorizes the holes in the first slice of cheese, *Unsafe Acts*, as "violations" (willful acts) or "errors" (non-willful acts). While it seems reasonable to distinguish between the two, it is probably impossible to know the true intent of operators, and hindsight bias would play a large part in attempts to discern their true intent. Within the error category, there are three refinements: skill-based errors, decision errors, and perceptual errors, which were identified using Rasmussen's work [77].

Skill-based errors occur during the performance of tasks that don't require conscious thought or occur due to a memory or skill slip [77]. Decision errors are the result of bad judgment. In an example of a risk-based decision about a pilot's choice to fly through a patch of bad weather, Shappel and Wiegmann report that sometimes we simply choose well, and sometimes we do not. They go further to say that pilots may behave riskily under the influence of certain conditions, which they and Reason call "preconditions for an unsafe act" [15][3]. For example, one such precondition is time pressure due to the eagerness to return home to family ("get-home-itis,"). The last category of HFACS is perceptual errors, where operator perceives things that do not match reality. For example, perceptual errors are common in flying, where the vestibular organs confuse operator's sense of up and down, and front and back [66]. Examples of Unsafe Acts can be seen in Table 2.

Table 2 HFACS Classification of Unsafe Acts [15]

Errors	Violations
Skill-based Errors	Failed to adhere to brief
Breakdown in visual scan	Failed to use the radar altimeter
Failed to prioritize attention	Flew an unauthorized approach
Inadvertent use of flight controls	Violated training rules
Omitted step in procedure	Flew an overaggressive maneuver
Poor technique	Failed to properly prepare for the flight
Omitted checklist item	Briefed unauthorized flight
Over-control the aircraft	No current/qualified for the mission
Decision Errors	Intentionally exceeded the limits of the aircraft
Improper procedure	Continued low-altitude flight in VMC
Misdiagnosed emergency	Unauthorized low-altitude canyon running
Exceeded ability	
Inappropriate maneuver	
Poor decisions	
Perceptual Errors (due to)	
Misjudged distance/altitude/airspeed	
Spatial disorientation	
Visual illusion	

Examples of Preconditions for an Unsafe Act can be seen in Table 3.

Table 3 HFACS Classification of Preconditions for Unsafe Acts [15]

Substandard Conditions of Operators	Substandard Practice of Operators
Adverse Mental States	**Crew Resource Management**
Channelized attention	Failed to use back-up
Complacency	Failed to communication/coordinate
Distraction	Failed to use all available resources
Mental Fatigue	Failure of leadership
Get-home-itus	**Personal Readiness**

Adverse Physiological States
- Mental illness
- Physical fatigue

Physical/Mental Limitation
- Incompatible intelligence/aptitude
- Excessive physical training
- No current/qualified for the mission
- Violation of crew rest requirements
- Violation of bottle-to-throttle requirement

Examples of Unsafe Supervision can be seen in Table 4.

Table 4 HFACS Classification of Unsafe Supervision [15]

Inadequate Supervision
- Failed to provide guidance
- Failed to provide oversight
- Failed to track performance

Planned Inappropriate Operations
- Failed to provide correct data
- Improper manning
- Failed to provide adequate brief time

Failed to Correct a Known Problem
- Failed to correct document in error
- Failed to identify an at-risk aviator
- Failed to report unsafe tendencies

Supervisory Violations
- Authorized unnecessary hazard
- Failed to enforce rules and regulations
- Authorized unqualified crew for flight

Examples of Organizational Influences can be seen in Table 5.

Table 5 HFACS Classification of Organizational Influences [15]

Resource/Acquisition Management
- Human Resources
  - Section
  - Staffing
  - Training
- Monetary/budget Resources
  - Excessive cost cutting
- Equipment /facility resources
  - Poor design

Organizational Climate
- Structure
  - Chain of command

Organizational Process
- Operations
  - Operational tempo
  - Time pressure
  - Production pressure
- Procedures
  - Standard
  - Documentation
- Oversight
  - Risk management
  - Safety programs

Delegation of authority

Policies

Hiring and firing

Culture

HFACS translates the term "human error" to seemingly more precise intellectual terms, such as working memory, long-term memory, etc. But the cloak of psychological terms hides the fact that conceptualizing human error is tricky. "Human error" is intimately dependent on context and system structure, and the HFACS classification tree—built using a linear-accident model—cannot capture the subtle system complexities that influence human error with "smarter-sounding" terms. As Dekker, a psychologist and pilot, bluntly states "Don't put blame in psychological terms [18].

The main shortcomings of HFACS are:

1) The definition and classifications of error and the inability to classify consistently. The buckets used to classify human error are too vague and are not disjoint. There are too many ways to label acts, conditions, and states as action, precondition for an unsafe act or influence. Furthermore, the categories are not disjoint. For example, errors (unsafe acts) can be further classified as perceptual errors. However, in many situations, the perceptual error can be considered a precondition for an unsafe act, e.g. misreading a dial in itself was not unsafe, but performing a high bank maneuver as a result could be. No two people using HFACS would derive the same identification and classification given identical accidents [51]. This problem does not occur within the STAMP-based methods, as all classifications are grounded in control theory.

2) The classification of actions that have already occurred without context is subject to hindsight bias.

3) The HFACS system has also not been incorporated into a prospective analysis that may assist in classifying potentially hazardous behavior.

4) The method lacks a systems foundation and so is only able to address failures and does not address other causes of accidents. The method classifies events rather than inadequate control. Furthermore, the 'failure' events that it does classify blame the person and not the environment.

It does not account for feedback within systems or how mental model flaws may arise. Individual human acts are only examined if they are directly causal to the accident.

5) The chief issue with HFACS is that classifying errors does not necessarily help an engineer design or re-engineer systems to prevent accidents. The classification scheme does not go far enough to provide information that engineers can use to create safe systems. The classification does not provide guidance for how to make pilots robust to "get-home-itis" or design changes than can push decision-making regarding risk back to conservative baselines.

Accident Analysis Method for Organizations: SOAM

The Safety Occurrence Analysis Methodology (SOAM) is an organizational safety accident analysis method that, like HFACS, seeks to push the analysis beyond the actions of individuals [44]. Based on Reason's accident model, it focuses analysis on the "Swiss cheese" holes, as opposed to how the holes appeared in the first place. Each "fact of the accident" is categorized as an absent or failed barrier, human involvement (unsafe act), contextual condition (precondition for an unsafe act) or organizational factor. The SOAM classification is problematic, though, because depending on the point of view of the human involved, the same act may be categorized as an unsafe act or a precondition. The classification will depend on the position within the control structure.

The SOAM approach also requires direct causality, and seems to create a more detailed, readable version of an AcciMap [84]. In an independent comparison to STAMP, SOAM has been described as quick but lacking in substance [45].

Accident Analysis for Humans and Organizations: ECF

The Events and Causal Factors (ECF) [126] method and diagrams uses a visual approach to analyze accidents. ECF diagrams are composed of events, denoted as boxes, and causal factors, denoted as ovals connected to events. Solid ovals are contributing factors found from direct facts and dashed lines are inferred factors. An example of ECF applied to a car accident is shown in Figure 13.

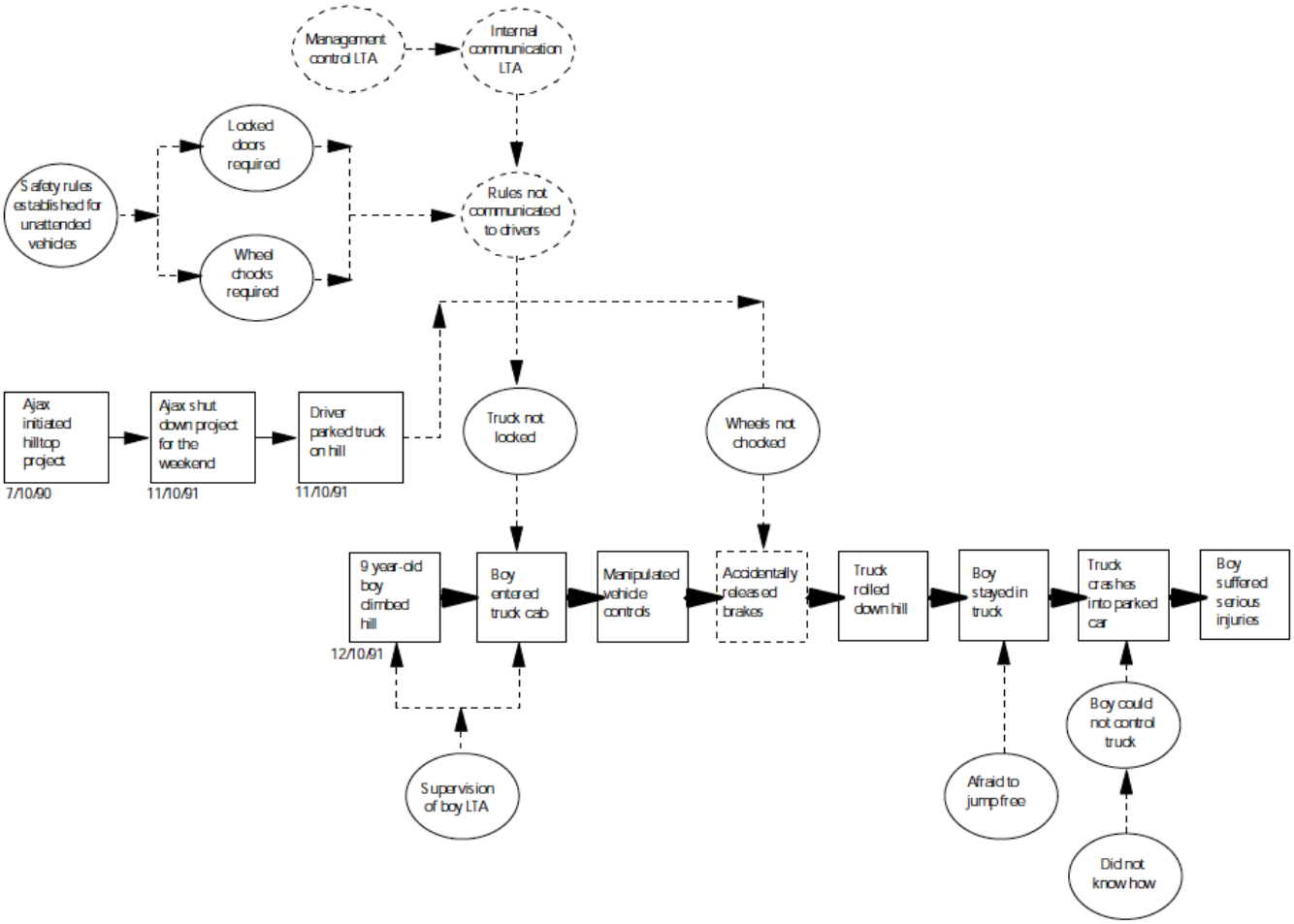

Figure 13 ECF Source: [126]

The organizational and human contextual factors (shown in ovals) are linked to many of the events (shown in rectangles). The method for creating ECF factors relies on a linear sequence of accident causation and is based on the Swiss Cheese Model. Causal factors that "occur" close to the time of an event, or are somehow closely proximate, are connected. When several contextual factors are related to an event, but the relationships cannot be represented with a chain, they are grouped together in a causal factor cloud.

The main shortcomings of ECF are:

1) The relationships within the causal factor cloud are not explored. In most ECF diagrams, the causal factor cloud consists of organizational factors. Most of the ECF analysis focuses on

individual controllers. Without analysis of organizational factors, systemic flaws cannot be addressed.

2) ECF analyzes events rather than design or controls.

3) ECF does not capture feedback relationships or indirect relationships.

4) Being a Swiss Cheese-based method, the classification of contributing factors and events is not clear. For example, in the ECF diagram above, "Driver parked on a hill" is an event, however, "Wheels not chocked [by the driver]" is a contributing factor.

5) Without a clear classification algorithm, classifications may be subject to hindsight bias.

Accident Analysis for Humans and Organizations: AcciMap

AcciMap, another method for accident analysis based on the Swiss Cheese model, is also designed to capture human and organizational factors [84]. The method uses an abstraction hierarchy for analyzing events and causal factors at each level of the organization. The particular levels used depend on the system analyzed, but in general they are: Government, Regulators Association, Strategic management, Tactical Management, Operative level and Physical system.

At each level, the events, actions, and relevant decisions preceding the accident are listed along with their consequences. Each decision is connected to either decisions or plans at other levels of abstraction, or is connected to the critical event (the accident). For example, a decision at a high level of the organizational hierarchy is connected to plans implemented at lower levels of the hierarchy.

An example AcciMap is shown below:

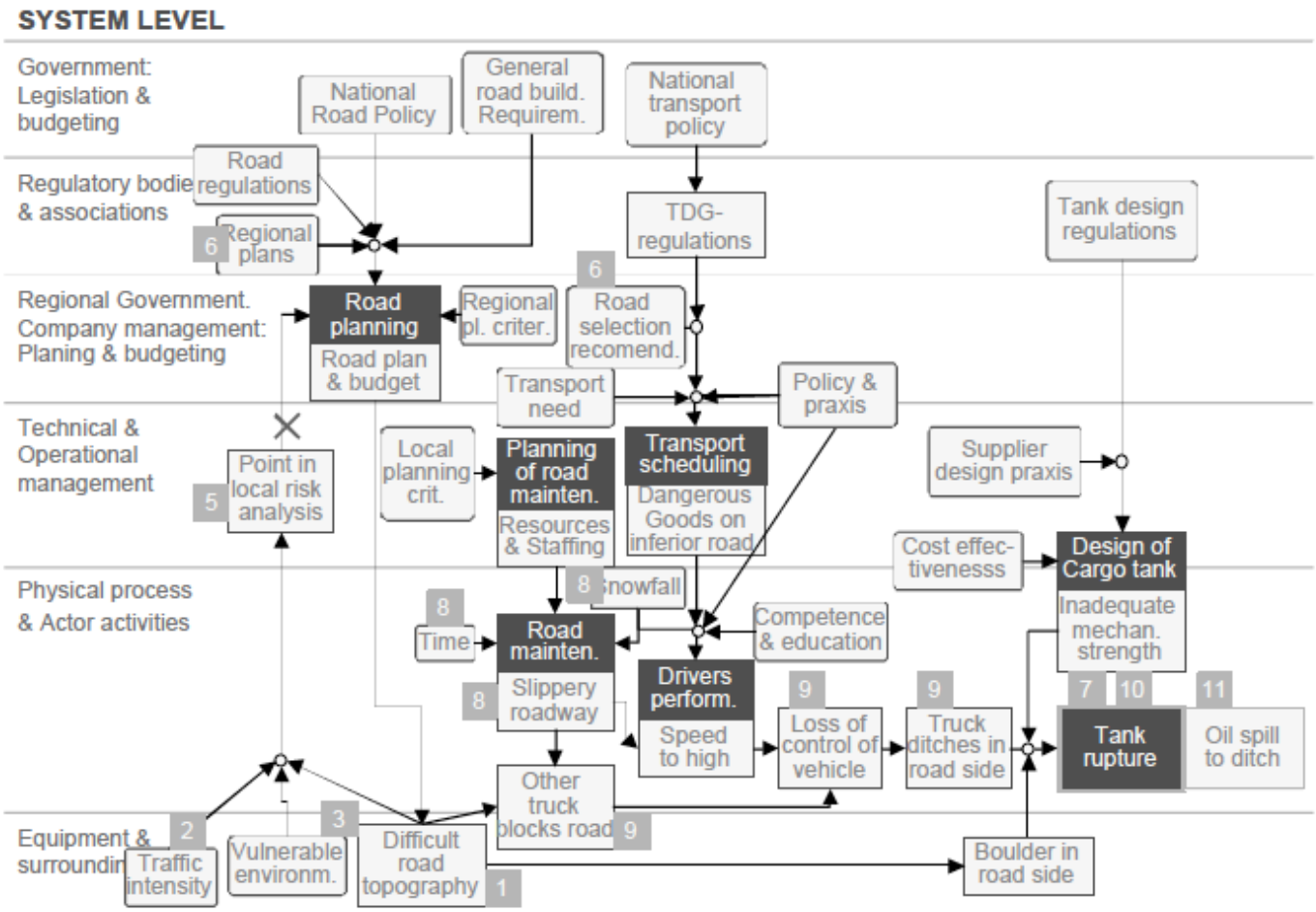

Figure 14 Example AcciMap for Road Transportation Accident Source: [159]

The AcciMap can be notated with numbers or letters where additional information can be included in a textual description of the accident. For example, notation 6 in Figure 14 can be linked to text that describes the regional plans used in more detail. AcciMap notations usually consist of quoted or paraphrased content from accident investigations or interview transcripts.

The critical problem with AcciMap is that it doesn't examine why the decisions and actions were made as they were. For example, the AcciMap above does not go into any detail regarding the poor roadway maintenance program; it merely notes that poor roadway maintenance contributed to the accident. AcciMap goes into the "why" for physical factors, but does not go into the "why" for organizational factors.

Another issue with AcciMap is that it is subject to hindsight bias. For example, the AcciMap users will suggest that humans did something wrong, but do not explain why it made sense to do as they did. In

many accidents, inadequate decisions were made at management level, but analyzed with AcciMap, these decisions would only be represented in abstract ways (e.g. "corporate policies") without further exploration. On the other hand, operator decisions are described in more detail. AcciMap focuses attention on decisions made by operators that contributed to the loss rather than management decisions.

AcciMap is based on Reason's Swiss Cheese model, and so it inherits the faults of that model. However, the organizational abstraction levels used in the AcciMap are useful and indeed informed Leveson's development of Intent Specifications [72].

2.6.2 Summary: The Problem with Post-hoc Human and Organizational Factors Classifications

Many incident reporting and learning schemes used in organizations focus on identifying root causes [67]. This is problematic because there is no such thing as a "root cause." The selection of a root cause, like the selection of an initiating even in an accident, is a matter of convenience [9] [29] [53]. Furthermore, most incident reporting methods focus on the classification of failures. Interestingly, many classifications provide a multitude of examples for technical component failures, but for organizational issues, labels become scarce and vague [67].

The lack of fidelity in organizational failure reporting schemes (e.g. risk management failure, poor budgeting, inadequate leadership) provides a clue as to the challenge of designing safety in socio-technical systems—it is not known what to do about organizational failures. As Carroll states [67], "There is the presumption that organizations are like machines, whose problems can be decomposed into parts, the causes identified, and fixes put in place." However, organizations are far more complex and understanding how organizations impact safety is critical.

2.6.3 Systemic Hazard Analysis: STAMP-based Analysis

STAMP-based Analysis (STPA) is a hazard analysis technique based on the STAMP model of accident causation. The objectives, as described in [5], are to identify instances of inadequate control that could lead to the presence of hazards and the safety-related constraints necessary to ensure acceptable risk. Furthermore, performing STPA produces information about how the safety constraints may be violated and this information can be used to control, eliminate, and mitigate hazards in the system design and operation [12].

Underlying the STPA process is the notion that hazards are eliminated or controlled through system design. Figure 15 presents a generic, low-level process control loop in STPA. As seen in the figure, the control input is a reference signal. The controller uses the control input in conjunction with received measurements to generate control commands. Continuing along the loop, the command is sent to the actuator, which implements the command through the arrow labeled U. The U vector refers to actions of the actuator that influence the controlled process. The control algorithm used by the controller is based on an internal process model of the controlled process. The controlled process, or plant, is subject to process inputs and disturbances. The process output may become input into another linked process control loop. The sensors measure the output resulting from the actuator's actions and disturbances, and generate measurements that are then fed into the estimator.

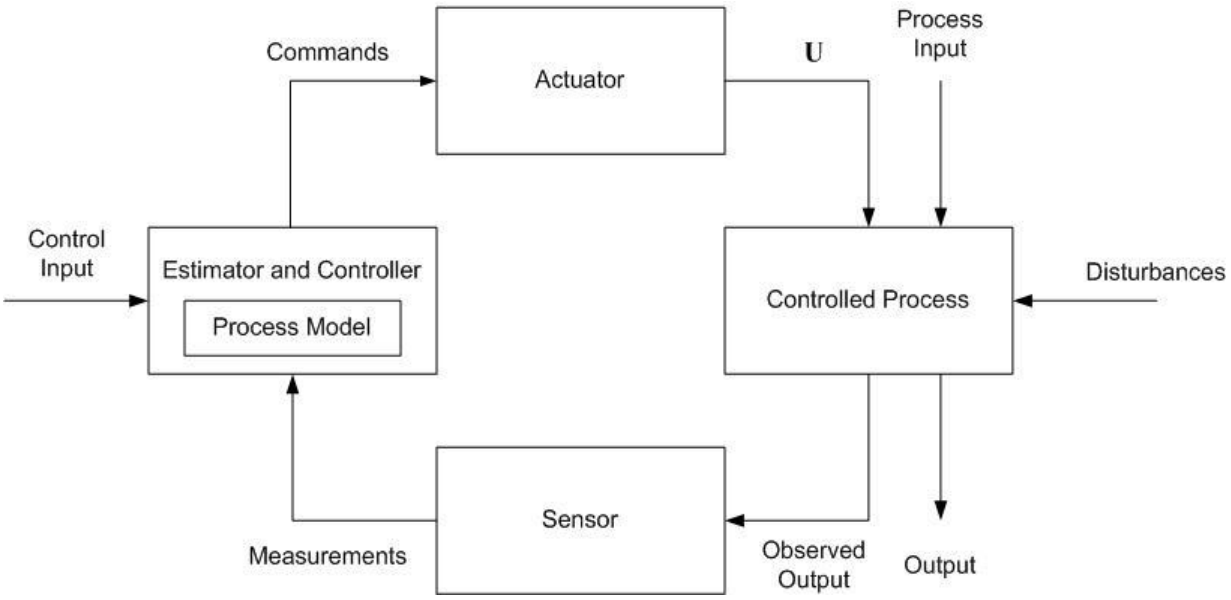

Figure 15 Generic STPA Low-level Process Control Loop

Depending on the particular system, the control input may be referred to as a goal, plan, sequence, directive, or set point (in spacecraft engineering parlance). The controller may send directives to a lower-level controller rather than to an actuator in order to affect control on that process. Similarly, the lower-level control loop, rather than a sensor, may pass measurements or status information (such as its health and other components of its current state) to the higher-level control loop.

Each hazard and related safety constraint is analyzed using STPA. Hazards occur as the result of ineffective control, so the first step of STPA is to identify *inadequate control actions* Starting with a

hazard and a safety constraint to control the hazard, inadequate control actions that could violate the safety constraint are identified. Inadequate control actions come in four forms [8]:

1. A required control action to maintain safety is not provided.
2. An incorrect or unsafe control action is provided that induces a loss.
3. A potentially correct or adequate control action is provided too early or too late.
4. A correct control action is stopped too soon.

Using knowledge of the current system design, the next step in the STPA process is to investigate each inadequate control action. An inadequate control action arises due to *flaws* in the design or operation of the system. Such flaws are called *causal factors* and are the mechanisms that could lead to inadequate control actions due to errors in the control algorithm, poor understanding of the process, or poor coordination between multiple controllers. The STPA taxonomy of causal factors [8] can be seen below.

1. Design of the control algorithm does not enforce constraints
    - Flaw(s) in creation process
    - Process changes without appropriate change in control algorithm (asynchronous evolution)
    - Incorrect modification or adaptation
2. Process models inconsistent, incomplete, or incorrect
    - Flaw(s) in creation process
    - Flaw(s) in updating process
    - Inadequate or missing feedback
        - Not provided in system design
        - Communication flaw
        - Time lag
        - Inadequate sensor operation
    - Time lags and measurement inaccuracies not accounted for
    - Expected process inputs are wrong or missing
    - Expected control inputs are wrong or missing
    - Disturbance model is wrong
        - Amplitude, frequency or period is out of range
        - Unidentified disturbance
3. Inadequate coordination among controllers and decision makers

The STPA taxonomy is used to identify inadequate control actions and the flaws that lead to inadequate control actions. From there, engineers create new constraints or refine the existing constraints and create new design or modify the existing design until all hazards are mitigated, eliminated, or controlled. Engineering judgment is used to determine when the design is "safe and complete enough."

To reduce the probability of undesirable events and the occurrence of hazards, instances of inadequate control should be eliminated. STPA uses the STAMP model of accidents for the hazard analysis, which allows engineers to find causal factors that lead to inadequate control. Once inadequate control actions and causal factors (flaws in the system design or operation) are identified, engineers can use that information to attempt to eliminate, mitigate, or control all hazards in the system [12]. The STPA process is described in detail in [110].

STPA was designed for the analysis of complex systems starting from system loss events and hazards. STPA looks at system interactions and gives guidance for the identification of conditions for inadequate control before they occur. However, while providing great insights, application of STPA to the human and organizational aspects of systems have been ad hoc so far. Further refinement and guidance must be made available to engineers to use an appropriately modified process for a rigorous hazard analysis of complex socio-technical systems.

2.7 Safety Approaches Used in Operations

Currently, engineers have tried to compensate for a lack of safety engineering methods to deal with human and organizational factors with operation-based safety methods, including checklists and Behavior-Based Safety. Checklists have been helpful in improving safety, especially in aviation [92] and healthcare [93] but are not cure-all safety tools. Checklists are not sensitive to subtle variations of common or uncommon tasks found in real operating conditions. Adherence to a checklist is not automatic, as the dynamic influence of environment plays a key role in decision-making. Safety comes not from ironclad checklists and procedures but from skilled judgments made by people who choose when and how to apply them. Checklists and procedures are simply resources for safe decision-making [18] and do not guarantee safety.

Another technique commonly used to fix safety problems in operations, after the design is set, is Behavior-based Safety (BBS), a method that relies on procedure change and compliance. Typically, BBS proposals are implemented by operators rather than by an integrated operator-management team. This division of labor is problematic because management assumes safety problems are owned by operators

and cease to push for system safety. BBS approaches tend to widen the gulf between operators and management and contribute to increased risk within systems [38][42]. Fixing system design flaws through human behavior and procedure task compliance alone have failed [42]. Challenging safety problems are designed into the entire system, not just operator procedures. Therefore, safety solutions must be built in, rather than tackled through procedures alone. One way to ensure that safety is built into the system is to use a hazard analysis as part of the system engineering process.

2.8 Safety Models and Methods in Practice at the FAA

This section presents an overview of current safety practices at the FAA. An assessment of the Safety Management System (SMS) and discussion of why new approaches are needed and they could be incorporated into current practice follows the SMS overview.

2.8.1 FAA Safety Management System (SMS)

In 2000, the FAA Administrator saw the need for the design and implementation of a Safety Management System (SMS). The SMS was created to formally integrate the safety-related operational processes, procedures, policies, and programs of the FAA [111]. The SMS is a framework for the safety analysis and approval process for proposed changes to the NAS, such as air traffic procedures and standards, airport procedures and standards, and new or modified equipment. Products produced via the SMS include safety risk assessments, safety data, and safety evaluation reports. The SMS supports decision-making regarding proposed changes that impact safety, prioritization of safety enhancements, and implementation of safety enhancements to the NAS. Furthermore, the SMS helps facilitate the management of safety between the multitude of people and organizations involved in the provision of air traffic control (ATC). The SMS is applicable to all FAA employees, managers and controllers who are directly or indirectly involved in the provision of ATC or navigation services [111][112].

The development of the SMS is grounded in Reason's Swiss Cheese model of accidents: The SMS documents contain discussion of "active," "latent," and "organizational" failures. One of the main strategies to assure safety, noted in the SMS, is defense-in-depth [111]. The defense-in-depth strategy is supported by theory cited in the SMS documentation: "accidents and incidents often result from a chain of independent errors." According to the SMS documentation, use of defense-in-depth is helpful as it ensures that single errors cannot lead to an accident. In particular, the SMS cites "human error or violation" as one of the key error sources that can cause a gap in NAS defenses. Strategies that may be used to deal with human error and other causes for gaps in the NAS defenses include [111]:

Equipment

a. Redundancy
    1. Full redundancy providing the same level of functionality when operating on the alternate system
    2. Partial redundancy resulting in some reduction in functionality (e.g., local copy of essential data from a centralized network database)
b. Independent checking of design and assumptions
c. System designed to ensure that a critical functionality is maintained in a degraded mode in the event that individual elements fail
d. Policy and procedures regarding maintenance, which may result in loss of some functionality in the active system or loss of redundancy
e. Automated aids or diagnostic processes designed to detect system failures or processing errors and report those failures appropriately
f. Scheduled maintenance

Operating Procedures

a. Adherence to standard phraseology and procedures
b. Read back of critical items in clearances and instructions
c. Checklists and habitual actions (e.g., requiring a controller to follow through the full flight path of an aircraft, looking for conflicts, receiving immediate coordination from the handing-off sector)
d. Inclusion of a validity indicator in designators for Standard Instrument Departures and standard terminal arrival routes
e. Training, analyses, and reporting methods

Organizational Factors

a. Management commitment to safety
b. Current state of safety culture
c. Clear safety policy
    1. Implemented with adequate funding provided for safety management activities
d. Oversight to ensure correct procedures are followed
    1. No tolerance for willful violations or shortcuts
e. Adequate control over the activities of contractors

The overall process of approval and regulation of new technologies, procedures, or other changes to the NAS, has been modeled by Weibel [113]. His model describes in detail, the following process: First, the technology or change is decomposed to identify all affected artifacts (e.g. avionics, operational procedures, communication infrastructure). Then a safety analysis on each artifact is performed. The safety analysis drives the identification of safety-related requirements on NAS components and operation. In the next step, these requirements are implemented as procedures and technologies. Finally, the procedures and technologies go through an approval process and subsequently regulated.

The SMS, which governs the safety aspects of the above process, includes Safety Analysis, for the analysis of changes to the NAS; Safety Assurance, to collect and analyze safety-related data to continuously monitor and ensure safety of the NAS; Accident Analysis, to learn from safety-related incidents; and finally Safety Promotion, to continually promote a strong safety culture [111][112].

2.8.2 Safety Analysis

The safety analysis process component of the SMS is called safety risk management (SRM).

The SRM process is a means to [111]:

a. Document proposed NAS changes regardless of their anticipated safety impact
b. Identify hazards associated with a proposed change
c. Assess and analyze the safety risk of identified hazards
d. Mitigate unacceptable safety risk and reduce the identified risks to the lowest possible level
e. Accept residual risks prior to change implementation
f. Implement the change and track hazards to resolution
g. Assess and monitor the effectiveness of the risk mitigation strategies throughout the lifecycle of the change
h. Reassess change based on the effectiveness of the mitigations

The overall SRM process is described in Figure 16.

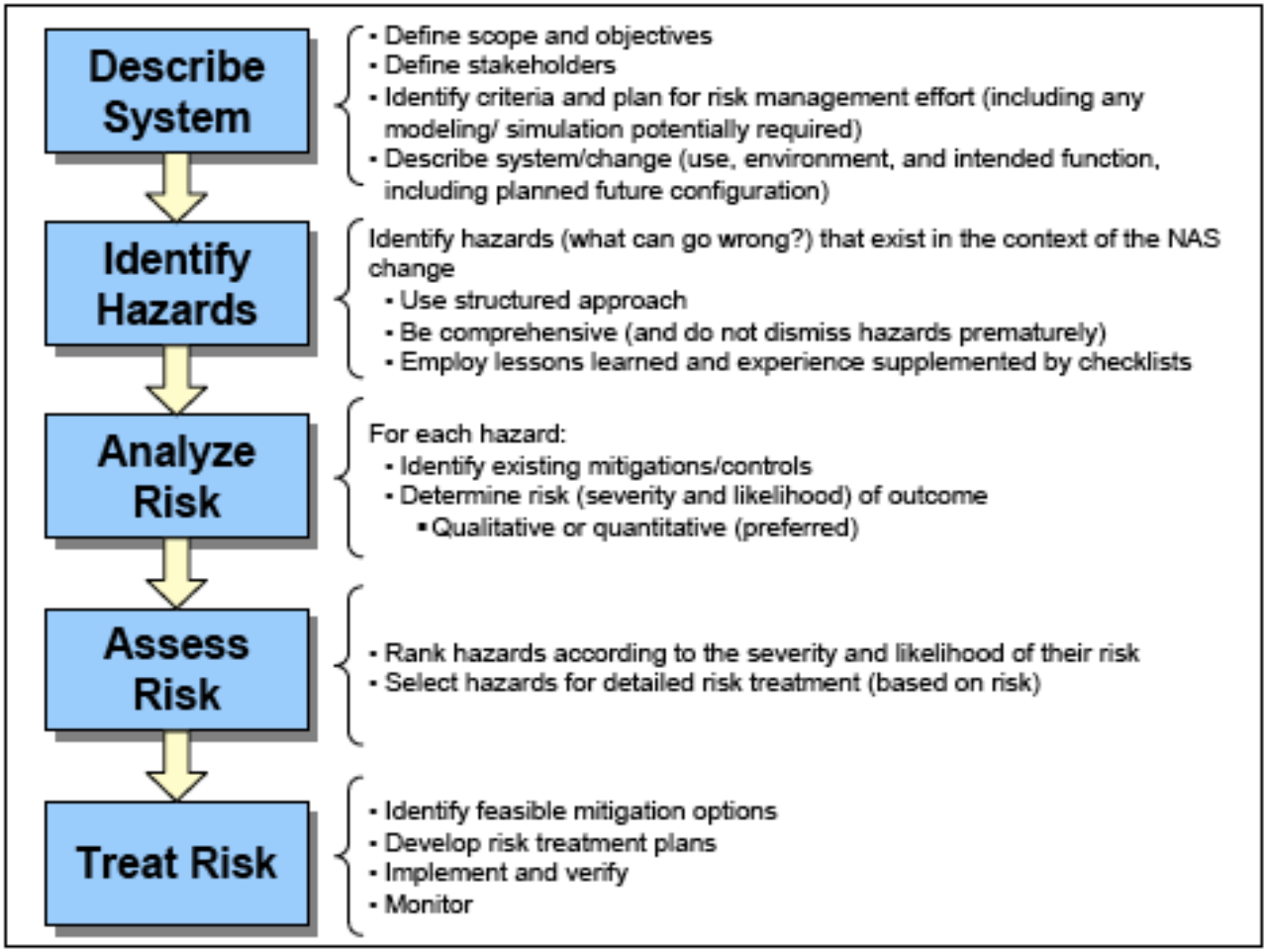

Figure 16 Phases of Safety Risk Management Source: [111]

The SRM fits into the SMS process as shown in Figure 17.

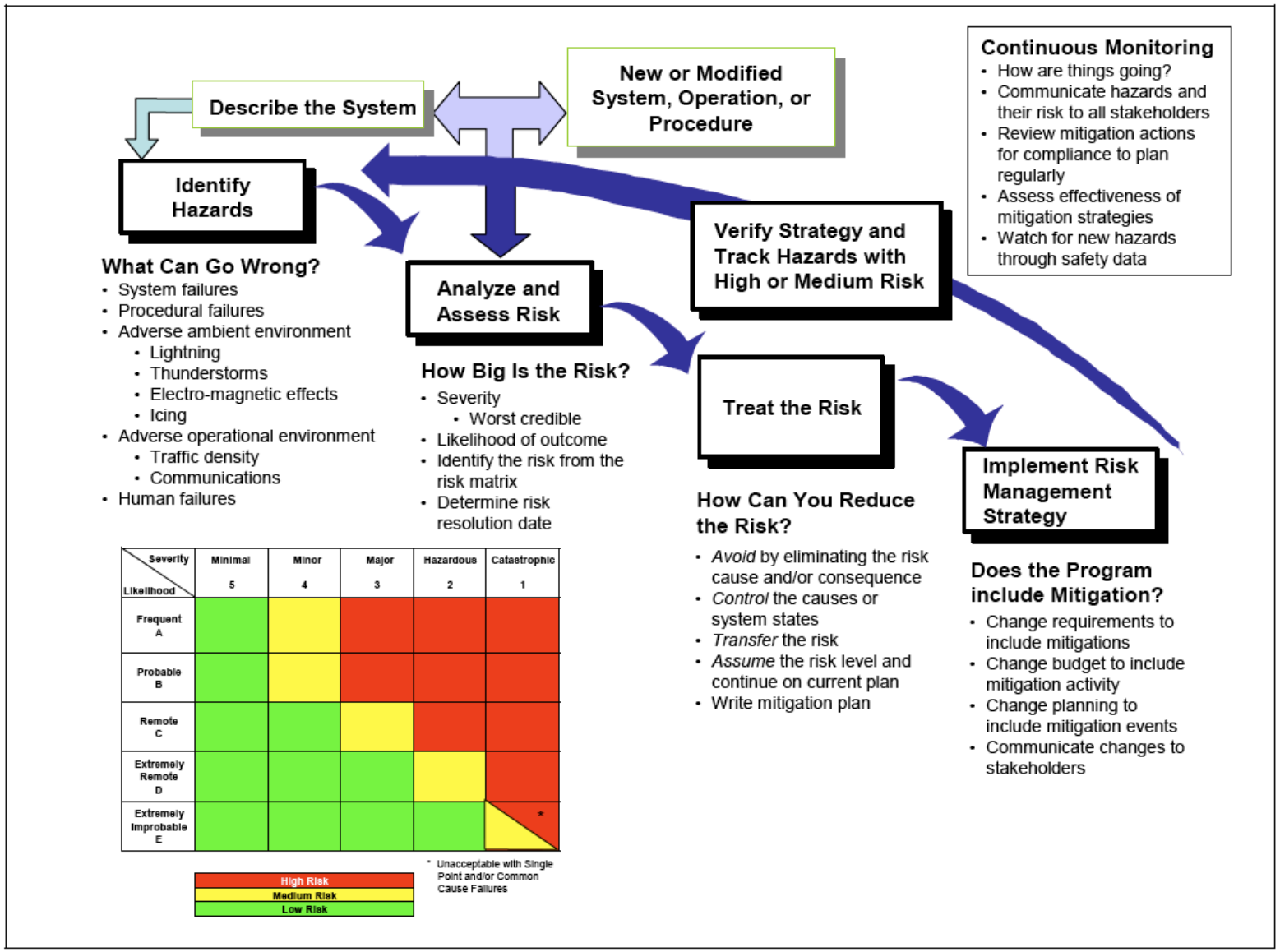

Figure 17 How to perform System Risk Management Source: [111]

The SRM provides great flexibility regarding the specific tools that engineers can use, and to what level of detail their analyses should be performed. For example, engineers may determine the level of safety required for each component, and may choose whichever hazard analysis method or risk assessment method they deem appropriate. The SMS does, however, specify that the risk assessment phase of the SRM should include an analysis of risk likelihood as part of risk factor ranking. Risks are ranked using a risk matrix, which maps risk factors based on the hazard likelihood and hazard severity. An example of a risk matrix can be seen in Figure 18. When risk factors are ranked, the treatment of red items is considered high priority, and green items are considered low priority. According to the SMS, ranking risk factors in this way allows engineers to determine appropriate resource allocation to each risk item [111][112].

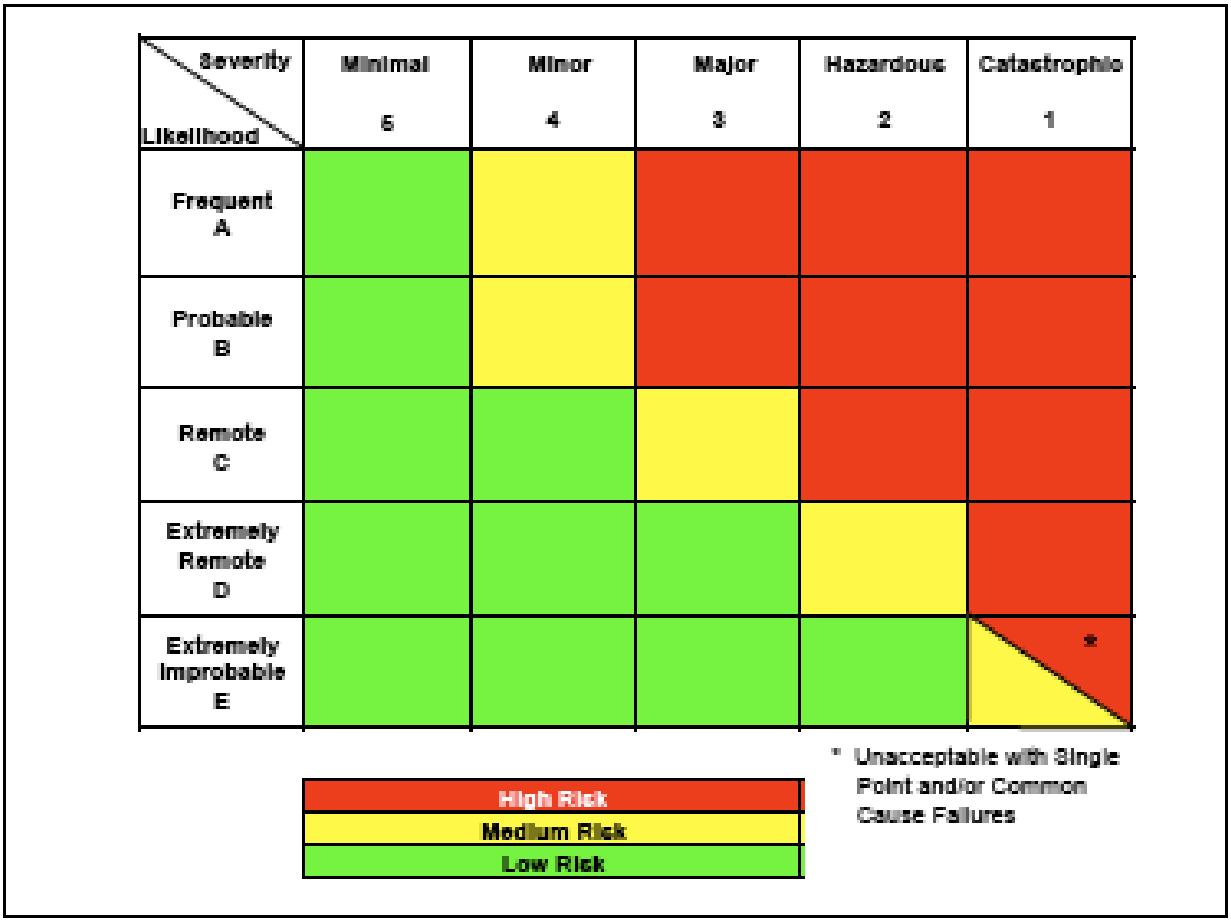

Figure 18 Risk Matrix Source: [111]

The human and organizational factors addressed in the SRM portion of the SMS concentrate on human ergonomic considerations, and human reliability and error considerations. A major source of human limitation is considered to be human performance variability. The SMS suggests that systems be designed to be robust to human errors caused by performance variation [111].

2.8.3 Safety Assurance

The SMS provides for continuing assurance of safety though safety reviews, audits and inspections of systems, as well as through tracking and analyzing accidents and incidents. The safety data collected as part of safety assurance within the SMS is used to [111]:

a. Identify risks and verify the effectiveness of implemented controls
b. Identify areas in which safety could be improved
c. Contribute to accident and incident prevention
d. Assess the effectiveness of training

2.8.4 Safety Promotion

The SMS also encourages safety promotion: "communication and dissemination of safety information to strengthen the safety culture and support the integration of the SMS into operations" [111]. The main purpose of safety promotion is to promote safety culture, which is done through training for all FAA employees. Senior managers are trained in safety culture and encouraged to demonstrate their commitment to safety.

2.8.5 Accident Analysis

The SMS includes provisions for the analysis of accidents that occur due the NAS itself, rather than those that are caused by NAS intra-element failures, such as aircraft engine failure. The SMS and related SMS accident analyses do cover the interactions between an intra-element failure and the rest of the NAS. For example, the NAS includes safety analysis of an out of control airplane and the rest of the NAS. Part of the SMS accident analysis component is FAA reporting systems. The reporting systems highlighted by SMS are in most cases voluntary, and do not result in punishment for involved individuals. To learn the most from incidents, the SMS has policies for the sharing of safety-related data between all components of FAA.

2.8.6 SMS Assessment

The Air Traffic Organization's Safety Assessment System is comprehensive, yet flawed. The SMS includes assessment of the interactions between aspects of the NAS, rather than analyzing their

"reliability" in isolation, and it places a strong emphasis on safety culture and continuous risk assessment. Another good feature of the SMS is its flexibility. For the most part, the SMS does not require particular methods for any of the required stages, leaving safety professionals free to choose whatever method is best suited for the problem at hand.

There are, however, several limitations to the SMS as it currently stands. First, because it uses a linear event-chain based accident theory, it is does not examine safety issues thoroughly. None of the hazard analysis or risk assessment methods listed in the SMS manual is capable of finding systemic flaws in either the technical or social aspects of the NAS. For example, the SMS is incapable of finding the flawed interactions between the Iridium satellite system and the Predator aircraft in the Nogales accident [125] nor would it have identified flaws in the safety culture of the operating organization of the Predator [125]. Secondly, the SRM requires that risk likelihoods be identified and used for risk ranking. Particularly for hazards related to human and organizational aspects, such a likelihood calculation is unlikely to be accurate. Alternate risk assessment techniques use hazard severity, rather than a combination of severity and likelihood, to guide engineers in their design for safety, and could provide a substantial improvement to the SMS [113]. A third flaw in the SMS is its treatment of human and organizational aspects. Human performance variation is not a source of system accidents in itself per se, but an indicator that the system is flawed. Rather than design the system to limit human performance variation, which can serve an indicator of increasing risk, the system must be designed to support human performance and decision-making. Organizational issues are superficially addressed in the safety culture section of the SMS. Few actionable requirements, processes or procedures are given for the assurance of safety with respect to organizations. Especially in a system such as the NAS, where a multitude of different organizations work together delivering high risk services to the nation, a more comprehensive view of the role of organizations in safety must be included in the SMS.

The methods presented in this thesis could be used in conjunction with the SMS as an alternate accident analysis method and an alternate hazard analysis method for human and organizational factors. Furthermore, the hazard analysis methods could be applied to a re-design of the SMS itself (the safety-related processes, procedures, and policies used to control safety in the NAS).

2.9 Summary of the Literature

In brief summary of the literature surveyed in this thesis proposal, the main good points identified in the literature are:

- The contributions from Systems Thinking. The thought-leaders in systems thinking have identified key goals for a hazard analysis suitable for human and organizational factors: avoidance of symptomatic and knee jerk reactions; the need for system operating transparency and the avoidance of excessive delays; the ability to design stable and safe feedback relationships that keep the system operating in a safe regime, robust to risk migration; and the ability to deal with dynamics complexity.

- Aspects of NAT. Designing in loose coupling and controlling interfaces has improved safety in aviation. Instances of tight coupling and un-controlled interfaces may be a guide for accident investigators.

- Just Culture and Safety Culture. The design of organizations predicated on a human and organizational hazard analysis must encourage and support a just safety culture.

- STAMP and STPA. The STAMP accident model will be the foundation of a systemic human and organizational factors appropriate hazard analysis. STPA will serve as the starting point for an extension appropriate for human and organizational factors.

The limitations found in the literature:

- Aspects of HRO. Many of the organizational traits lauded in HRO have not been scientifically proven (or even shown to be correlated) to safety. Others are superficial statements or true of all organizations and all qualities (not particularly safety). For example, of course good communication within the organization is desirable (even if the organization has nothing to do with safety) but the key is how to design the communication, reporting and feedback channels within the organization to increase safety.

- HFACS and HAZOP and other methods based on the Swiss Cheese model. The classification of human and organizational errors does not go far enough to create safe systems. Furthermore the classification must be grounded in an engineer-based logic, rather than based on kinds of events that may occur in a particular industry.

  In particular, Human HAZOP only considers the task execution process for deviations. This is akin to only looking for inadequate executions in STPA!

Any method based on a event-based accident model will not have a systems view of safety, and thus will be inadequate for use in the design or analysis of complex systems.

- Quantitative Risk Assessment. All of the quantitative risk assessment techniques lack a system view of accidents and safety. While precise calculations give a comforting sense of certainty, they are an illusion when applied to human and organizational factors.

- In practice, the SMS used for air traffic safety is based on flawed theory and could benefit from a redesign using the method presented in this thesis.

2.10 Terminology

Accident: An undesired and unplanned (but not necessarily unexpected) event that results in an [unacceptable] level of loss [Leveson, 1995].

Safety: The freedom from accidents [Leveson, 1995].

Hazard: 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) [Leveson, 1995].

Accident Analysis: The process by which the reasons for the occurrence of an accident are uncovered. Information and lessons learned from accident analysis are used to re-engineer the same or other systems so that future accidents (which may or may not be of the form) do not occur.

Hazard Analysis: The process by which hazardous scenarios are identified through the discovery of design flaws and potential system interactions in the social and technical system.

Risk Analysis: The process by which indentified flaws are assessed for their relative importance or likelihood of occurrence.

Safety Driven Design: A design process that includes an integrated hazard analysis process so that the design is analyzed for safety in the earliest stages of the design process.

Reliability: The probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated environmental conditions *[Leveson, 1995]*.

Software is the implementation of an abstraction and aside from computer hardware failures is 100% reliable, yet can be 100% unsafe.

2.11 Thesis Outline

Chapter one of this thesis motivates the need for safety engineering methods suitable for the social aspects of complex systems. In short, the challenges of today's systems are not being met with current state-of-the-art accident analysis methods or hazard analysis methods. The first chapter continues with a statement of the research goals and hypothesis and the research approach followed. The second chapter starts with a literature review of relevant aspects of safety engineering: safety philosophical approaches, accident models, accident analysis methods, risk assessment techniques, hazard analysis methods and operational methods. In particular, this section presents the basis for the accident and hazard analysis methods developed in this thesis: STAMP [5] and STPA [8]. The end of chapter two concludes with the thesis outline.

Chapter three presents the author's view of control theory as it applies to people. Chapter three starts with a description of how each aspect of complex system design (design, safety, management and the operating technical process) is related to each other. Next, the control requirements for individual human controllers and organizations are presented. The chapter continues with a discussion of the canonical human and organizational factors that lead to accidents are discussed and linked to the control requirements. The chapter concludes with the presentation and discussion of taxonomy for the classification of human and organizational error based on the control requirements and canonical human factors. The control requirements are based upon control theory, systems thinking, and human factors and organizational factors. The principles of control, including undershoot, overshoot, delay, mental model flaw, etc, have already been defined in the control theory literature and system safety literature. The human and organizational error classification taxonomy translates these terms into human and organization factors terminology.

In chapter four the overview for the crash of an unmanned aircraft (UA) in Nogales, AZ is given. This accident will be referenced throughout the thesis and will serve as the main example for the method applied to accident analysis. In chapter five, the guidewords for analyzing the social context of complex systems are presented.

In chapter six the author discusses how the guidewords are combined with the control requirements to create a cohesive method applicable to accident analysis and hazard analysis: following safety

engineering pedagogy[5], the "**S**TAMP extension for **H**umans and **O**rganizations using guide**W**ords" (SHOW) method is presented. The SHOW method provides a structured approach to the identification and analysis of human and organizational factors in accidents. The analysis focuses on the context that humans operate in, which can be changed, rather than the human himself or herself, which cannot. This accident analysis technique is in the form of specific analytic tools that designers, engineers and other system development participants can use to evaluate the human and organizational aspects of the design for safety. Feasibility of the method is demonstrated with the analysis of the Nogales, AZ accident.

Chapter seven compares the SHOW method to other state of the art methods. Next, chapter eight shows how the SHOW method can be extended using advanced concepts from system dynamics.

The SHOW method is applied to hazard analysis in chapter 9 and is demonstrated on several complex systems in several industries, including aviation, healthcare, and energy. (The safety principles that provide the foundation to the method described in this thesis make the method applicable to a wide range of complex systems.) Finally the dissertation finishes with a discussion of research contributions, limitations, and future work.

2.11.1 Thesis Roadmap and SHOW Building Blocks

Looking ahead, the relationships between the contributions—the canonical human and organizational factors, the requirements for control, the human error taxonomy, the guidewords, and the SHOW method—are depicted in Figure 47.

[5] A review of safety engineering course syllabus [132] and texts [7] [8], show that safety engineering pedagogy begins with accident causation theory and accident analysis. The next stage in safety engineering is to attempt to prevent accidents from occurring in the future by implementing lessons learned and using hazard analysis to find system flaws in existing systems before they lead to accidents. Finally, as safety engineers progress in their training, they learn to design systems that are free of hazards and related control flaws through safety driven design.

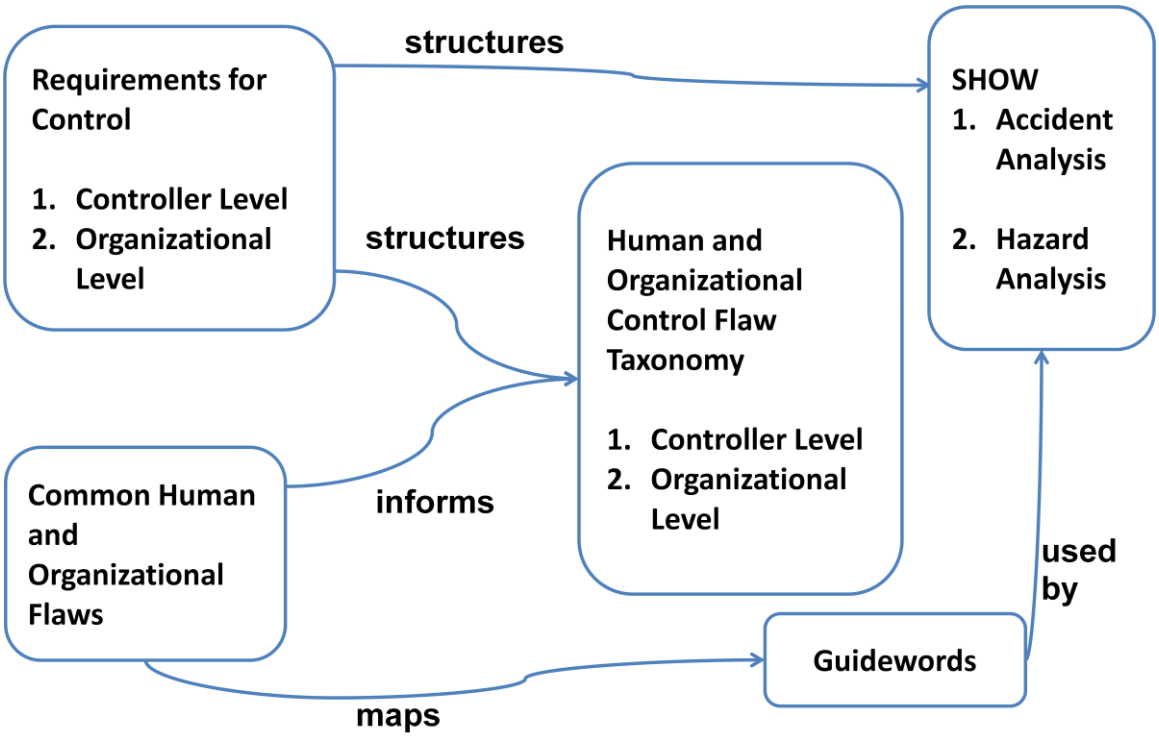

Figure 19 The Hazard Analysis Building Blocks

The descriptions of the human and organizational flaws in section 3.6 provide a thorough description of the human-centered phenomena associated with accidents. The common human and organizational flaws inform the categorization and taxonomy of human and organizational errors. The requirements for control described in 3.5 provide the structure and backbone for the human and organizational control flaw taxonomy. The taxonomy in section 3.7 provides a complete hierarchical categorization of control flaws. The guidewords presented in section 5.3, which are based not on control theory, but on the context we analyze, are derived from the common human and organization flaws.

The guidewords bridge the gap between the taxonomy and the safety analysis process. They are used to drive the accident and hazard analysis process forward. Together, they provide a systematic and practical way to find conditions, states and situations in the system design that can lead to flawed control actions or the poor decisions itemized in the taxonomy.

CHAPTER 3 A CONTROL-THEORETIC VIEW OF HUMAN AND ORGANIZATIONAL ERROR

3.1 Chapter Overview

The accident and hazard analysis methods presented in this dissertation are predicated on several theories and observations found in the human factors and safety literature. The most fundamental and important of these is that accidents arise through unintended interactions and these interactions can be prevented by the design of a robust and resilient control system. The notions of control, design, management, and operations are explored. A set of human or organizational factors that have contributed to accidents are discussed and together form a canon of human and organization errors. In order to govern interactions and failures that can lead to accidents, my goal is for the accident, hazard and design analysis methods described in this thesis to account for the canonical factors identified in this chapter. To accomplish this goal, a foundation from first principles for the application of control theory to human error is developed. The foundation, which extends principles from STAMP and psychology, forms a framework that can be used for safety engineering techniques. Each factor in the error canon is linked to the control theory framework. The control theory framework is then fleshed out to create a taxonomy and classification scheme for human and organizational error to complete this chapter.

3.2 How Human and Organizational "Errors" relate to Control Theory

This chapter describes how common human and organizational factors cited in accidents are manifestations of inadequate control. Rather than categorizing human and organizational "errors" using an event-based or cognition-based framework ala Human HAZOP [27] and HFACS [15], I framed these errors with control theory. It is important to highlight and categorize the social factors frequently cited in accident reports because these are the scenarios safety professionals wish to avoid in the first place. The goals of any hazard analysis method suited for human and organizational factors should be a process that elucidates scenarios that permit the aforementioned human and organizational "errors" to occur. I will decompose safety flaws into those associated with design, operation, technical process or product, and regulation; discuss what kind of interactions occur between these elements throughout the system lifecycle; and demonstrate how the hazard analysis can find hazardous relationships between these elements of the system.

3.3 Safety Throughout the System

All aspects of the system design influence system safety. For the system as a whole to be safe, each system aspect and interactions between them must be designed to be safe. To understand how all the acting processes of a system design relate to and impact safety, we turn to a discussion of the processes of system safety and the System Safety Control Structure Nucleus.

3.3.1 System Design

The first aspect of a system that influences its safety is the system design. The system design includes the design of the technical, operating and regulation processes. The operating process includes, for example, procedures and plans for how operators will interact with the technical process to deliver the desired product or service. The safety regulation process is the part of the operating process and technical process that enforces safety constraints throughout the system. The safety regulation process provides a needed counter balance, in a metaphorical safety free-body diagram, to counter forces that would increase risk.

The safety regulation process design includes, for example, how management will communicate incident and accident information with operators and how management will communicate with regulators. The regulation design stems risk migration and enforces safety constraints in the pursuit of achieving system goals. Regulation can come in the form of system safety personnel, safety culture, just culture, and regulatory policy and compliance procedures. Whether or not regulation is performed by the operating body or an external entity, regulation is an important aspect of a safe organization.

The system design provides the plan and implementation of a system. The design, like DNA, has a large impact on the safety of the system. If the system design is unsafe, the system cannot be "safe" and no matter how attentively operated or tightly regulated, an accident is likely to occur. The design encapsulates the potential for disaster as it defines the ability to cope with challenges encountered during operations.

The execution of an adequate safety regulation system must involve the system operators, system managers and *all* internal human controllers. Each human controller is a sensor capable of noticing odd system behaviors and phenomena that may indicate an unsafe system state. Humans are capable of problem solving beyond any software program, therefore each person in the system must be a part of the implemented safety regulation system. Of course, the safety regulation system must also be a part of the technical system design as well.

Safety regulation can be performed formally or informally, internally or externally. Internally, self-regulation can be accomplished with a group of respected system safety professionals with the ear of top management. Informally, cultural norms can act as a powerful regulatory force within the organization. Externally, safety regulation can be performed via regular audits by government officials with intimate domain expertise. Regulation can also be provided by a connected, but external group with vested interest in the success of the system. For example, the school's PTA can take part in decision-making regarding school leadership and school curriculums. External regulation is also important in cases where risk is high and the potential financial downside cannot be born by the industry itself. The nuclear industry, for example, is regulated by the Nuclear Regulation Committee, a federal agency, per their request. At its birth, the nuclear industry could not find an insurance agency willing to underwrite them, and so the federal government was the only entity capable of doing so [7]. In aviation, Designated Engineering Representatives (DERs) fall in-between internal and external regulation. DERs are trained by the FAA and serve as their designee to certify that certain subsystems meet federal guidelines and regulations, but are employed by the manufacturer. Typically, manufactures nominate their best people to become DERs and pay them well [143]. No matter how it is implemented, a force that resists migration to high risk within the organization is crucial to system safety.

The challenge of designing a safely operating plant is immense and ongoing. System launch does not signal the end of the design phase. For the social aspects of the system in particular, the design is continually moving and changing. For example, the design of the organization happens periodically (promotions and re-organizations), and the design of new procedures or processes can occur frequently.

Safe operation (e.g. excellent informational and reporting channels) is not a simple or static system attribute. Risk assessments must be conducted and decisions made under uncertainty. Using data from process sensors, operators must identify leading indicators of risk migration and feedback so that the system safety may be maintained. The operators make decisions to cope with new demands (e.g. new market constraints or demands) so that the system can continue to exist. The operations phase routinely leads to situations that impact the safety of the designed system. For example, operators can:

1. Change the design of the technical system or operations infrastructure (e.g. rules and procedures) that create unsafe behaviors and hazards that designers did not anticipate.

2. Change the system's operating context or environment and transform the relationship between system and environment in a way that designers did not intend that can lead to accidents.

Given the dynamic nature of safe operations and the challenge of designing a safety regulation system that resists risk migration, it is clear that modern systems are unlikely to evolve an effective regulation system by happenstance. The design of the operation infrastructure and the regulation infrastructure should work synergistically to deliver both the system value and safety.

In the next section, discussion of the system safety control structure nucleus, a theoretical structure, allows us to see all of the processes that work together to produce a safe system.

3.3.2 System Safety Control Structure Nucleus

A control structure can be used to analyze how the essential aspects of a system design work together to deliver a safe service or product. The "nucleus" metaphor underscores the essential nature of each system element to safety. The aspects of the system design encompass:

1) the technical design, which includes hardware and software design and the technical system under control

2) the operational management, which includes procedures, policies, staffing policies, and the management team used to deliver system goals and

3) the safety regulation design, which includes aspects of the technical and operational design to enforce safety constraints. The safety regulation design also includes the actors involved in regulation, which can include government officials and the cultural norms of the operators.

4) the design process, which describes how all of the above aspects of the system are created.

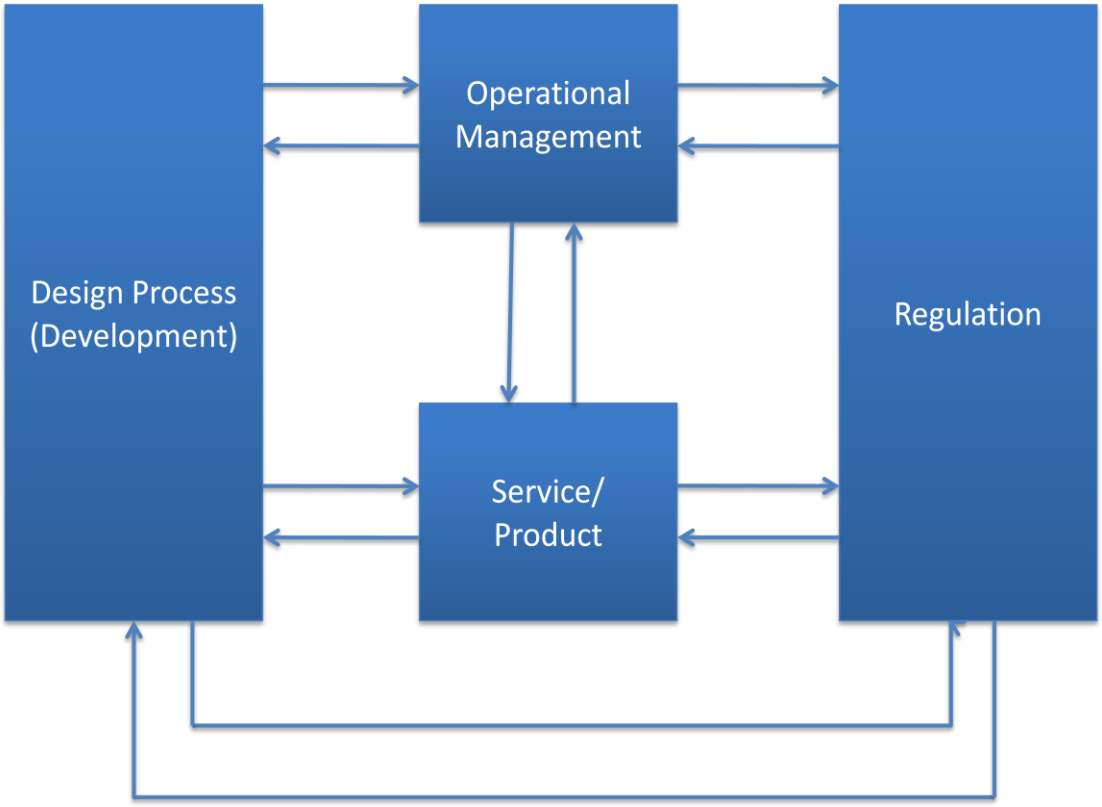

Figure 20 System Safety Control Structure Nucleus

This system safety control structure nucleus shows the control and feedback relationships between the essential system aspects. Each aspect influences, and is influenced by, every other aspect. The design process is used to design each system aspect, the technical product, the operation management processes and the safety management processes. In turn the design process can be changed, initiated, regulated, or curtailed by system management or system safety regulators. The design process itself is not static, and may change based on information from the technical process, or feedback from managers and regulators.

The safety control loop nucleus can be useful for the early design of systems. With the system goals in hand, the relevant actors to perform the operation and regulation functions can be identified and the control structure can be created. Once the relevant individuals or organizations have been identified, constraints on the design, operation and regulation can be identified. The relationship between operators and regulators can be influenced inexpensively early in the design process. During the financial crisis of 2008, despite explicit design of the operating and regulating relationships of the financial industry, the system eroded. The operator-regulator relationship must be designed correctly initially, and the design must contain measures to maintain the safety of the relationship over time.

3.4 Control Theory Applied to People

A control theory framework is an appealing construct for thinking about systems and categorizing social errors because the human and organizational factors that contribute to accidents are numerous, complex and interrelated. Using an engineering framework, allows us to use hierarchy, which both helps us organize human and organizational factors in an understandable fashion and to create a *complete* decomposition of human organization factors that can be used to categorize any human or organizational factor (no matter how nuanced or nonmathematical) that contributes to accidents. The use of control theory applied to complex systems generally has been discussed in Leveson's STAMP work [5]. In this chapter, I have extended the application of control theory to human-based systems and elements and present a theory and examples.

When the process being controlled is composed of human beings or a control loop element[6] is a human being, the way engineers typically think of a control loop changes somewhat. In completely human-composed systems, people are the controllers, people are the actuators, people are the sensors and people are the process being controlled. The difference between designing a system with human-based control elements and engineered control elements is striking. For example, for an engineered actuator, inadequate control can include component failure (e.g. the failure of a brake). However, when the actuator is a person, a simple failure abstraction is not useful because the human actuator is in and of itself a complex system. Engineers need more guidance to analyze a system for how human-based inadequate control manifests itself in a given system.

Just as for control loops composed exclusively of engineered components, the requirements of controllability for human-composed control loops are, succinctly, a goal, the ability to affect state, and a mental model of the process being controlled. In more detail, the controller (a person) must have correctly prioritized control goals for the process, they must understand and be able to use the control levers available to them to affect the process state, and they must have a (correct enough) mental model of the process, the sensor and the actuators (all of which could be people). Furthermore, it follows that the controller needs a mental model of how human-based actuators will respond to disturbances that affect them. For example, the mental model of a human actuator should include how the actuator would

[6]A control loop element can be a Controller, Communication Channel, Actuator, Sensor or the Process being controlled.

respond to each command in nominal circumstances and how the actuator would respond to each command in the presence of certain pressures or incentives.

For control loops composed of humans, it can be helpful to create a feedback loop between each control element and the controller, rather than using just one feedback channel from the process through the sensor. Specifically, a feedback channel between each control element and the controller allows the controller more immediate feedback regarding the state actuators and sensors themselves. For example, if the actuator is human, a feedback channel to the controller would allow the actuator to tell the controller if more resources were required to actuate the commands given. Figure 21 depicts a control loop with feedback or communication[7] channels between the control elements. Furthermore, humans have intelligence; each human is a controller of their own control loop(s). When humans are sensors or actuators in a control loop, they are the controller of a control loop at a deeper level of abstraction. For example, a project manager is in control of mission software and he or she can direct a software engineer to implement software requirements. To the project manager, the software engineer is an actuator. The software engineer, in turn, is in control of software implementation and may director junior programmers to assist with the implementation. Furthermore, human controllers and human sensors have their own mental models of the process. Those mental models may or may not match that of the main controller, which may cause communication problems (both ways). Figure 22 depicts the notion of controller-control element abstraction.

[7]Information communicated to the controller from an actuator can be used by the controller to assess the actuator's state, and update the controller's mental model of the actuator. Thus information directed from the actuator to the controller can be considered "feedback".

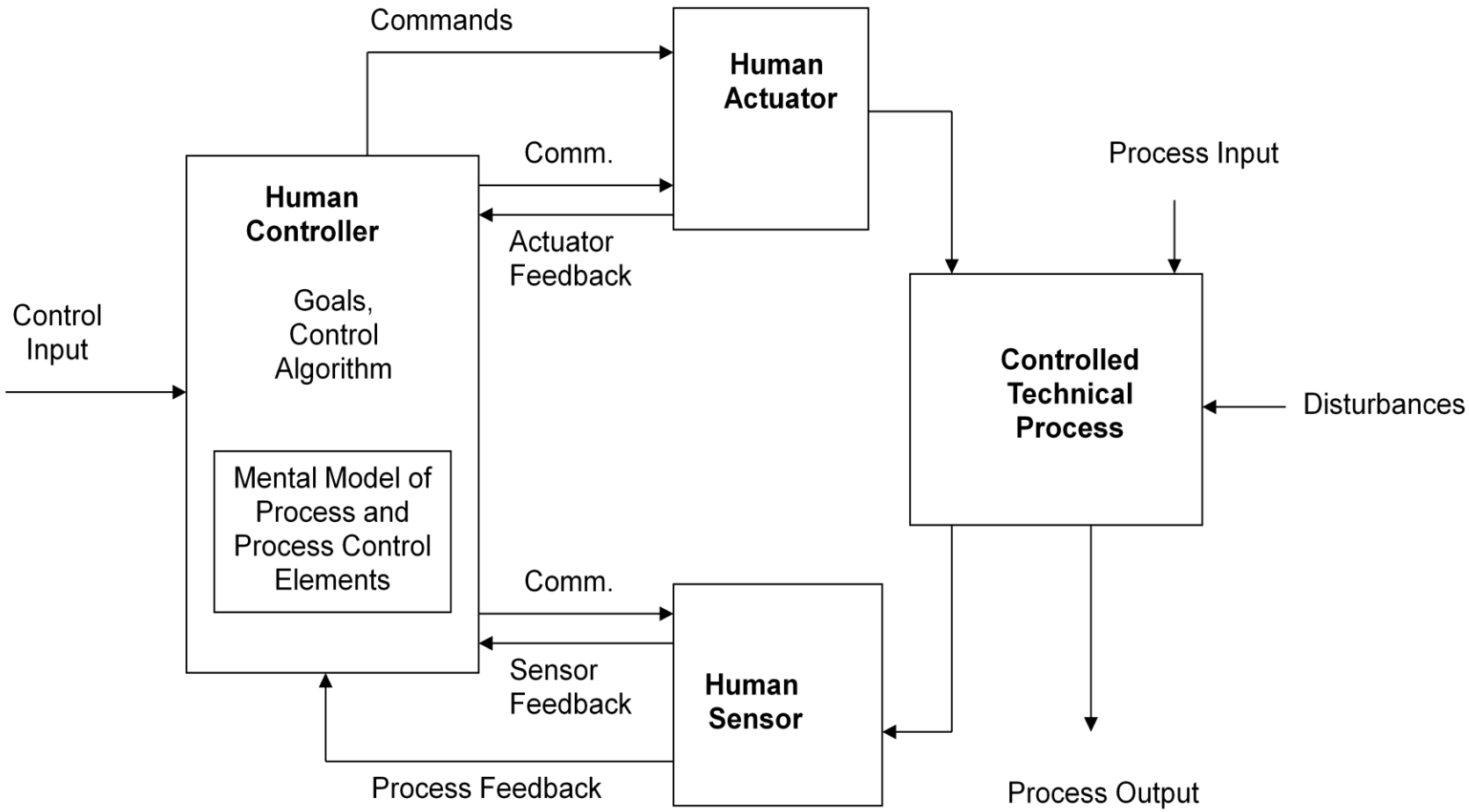

Figure 21 Human-composed Control Loop

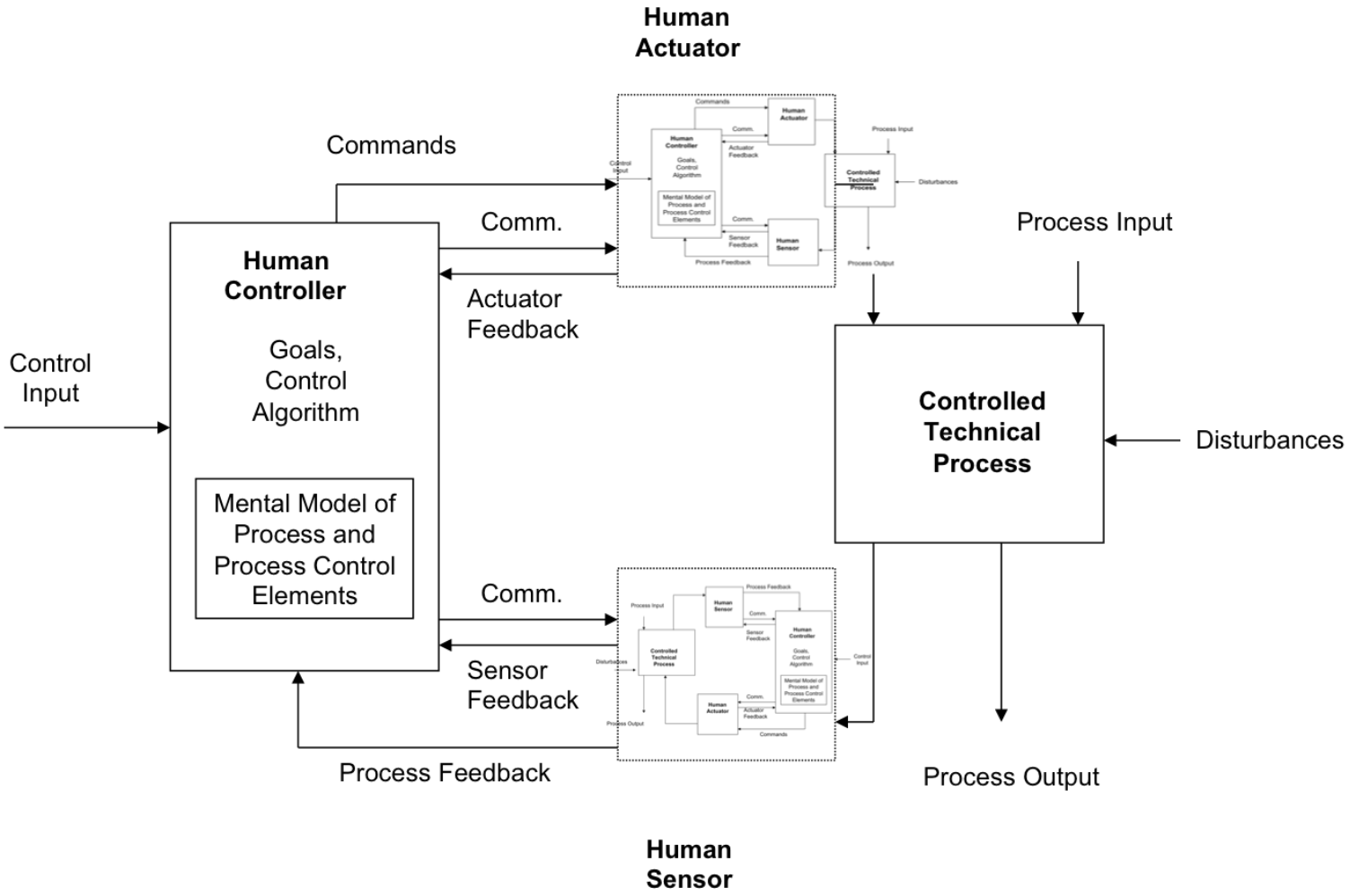

Figure 22 Controller Abstraction within the Control Loop

As described in STAMP [5], levels of abstraction are important for understanding the relationship between controllers, be they human-based or software-based. For example, inadequate control from controller X can happen not because of an inadequate mental model or inadequate control algorithm, but can occur due to an inadequate control on the part of another controller. For example, if the output of controller Y's process is a required input for controller X and it is missing, controller X may execute ineffective control. We can trace the missing (process or control) inputs of controller X to investigate the reasons for inadequate control on the part of controller Y.

A full description of what the mental model of the controller should include with respect to each control element will be described in Chapter 9, as part the description of the hazard analysis. However, it should be clear that for the sufficient control of each human-based control loop, a great deal of complex information must be carefully understood and used in the design of a socially-controlled system. With this in mind, we will now turn to the linking of the canonical human and organizational factors that "cause" accidents to control theory and discover what role they play in subverting the safe control of socio-technical systems.

3.5 Control Theory and Safety for Social Systems

The original STPA control taxonomy created an innovative new method for identifying hazards based on control theory. This work extends the original taxonomy to elaborate on the important role of human and organizational "errors" that contribute to inadequate control actions. This new approach applies control theory to the analysis of human and organizational factors, rather than categorizing flaws using a psychology-based framework or task-based framework. The approach uses an extended taxonomy to construct a structured process that practitioners can use to find manifestations of human-related flaws in the system's organizational and technical design.

3.5.1 Control Requirements

To analyze a system for safety, we must first understand what people and organizations need to control a system safely and adequately. These needs are the "control requirements." The mistakes and poor decisions of humans and organizations we call "inadequate control actions" are *all* due to a violation of one of the *control requirements*. To enforce safety constraints and prevent inadequate control actions, the control requirements must be upheld. We must design a system that both fulfills the control requirements initially and ensures that the requirements will continue to be met as the system evolves. To create robust designs, we must understand how control requirements can be eroded or negatively influenced and what can be done to enforce safety constraints and prevent risk migration.

The requirements for control are presented below and divided into two groupings: those for the individual and those for the organization as a whole. This separation is useful because different aspects of the system contribute to the presence of design or operation flaws at each level of abstraction. Analysis of individual controllers occurs at the control loop level, while organizations are best modeled at a higher level of abstraction and can be modeled with a control structure. For example, the control requirements are different for an individual pilot and an airline. An individual pilot is responsible for providing self-separation during flight, while an airline might be responsible for setting the training requirements for all pilots, planning safe and profitable operation schedules, and creating a safety culture that ensures that safety is not compromised to seek short-term profits.

The requirements for adequate control at the controller level are shown in Table 6.

Table 6 Controller-level Requirements for Control

Adequate…
1) control goal
2) control algorithm
3) model of the controlled process
4) model of the organization
5) coordination with other decision-makers

Controller's Control Requirements

This analysis expands the control requirements listed in STPA with an additional control requirement, the "model of the organization." Each of the STPA control requirements, and the addition, are identified in the notional control loop shown in Figure 23.

If all of the above requirements for control are met, the controller's selected control action must be executed to assure adequate control. The control action can be inadequately executed if the communication link between the controller and the actuator fails or if the actuator fails. Furthermore, the controller may execute inadequate control if needed process inputs are missing or control inputs are wrong or missing. For example, if the controller is to take a picture of a scientifically interesting site at a particular time, the controller, while meeting all of the control requirements, may still not be able to take the image if the power to the camera (a needed process input) is missing. The camera's power may be the *process output* of another controller (such as the power management controller) in the control structure. In another example, the controller may have an adequate control goal, such as "Control the level of

Chemical ABC in the tank," but still may execute inadequate control if the safety constraints regarding the tank fill maximum are missing. In short, a controller may meet the control goals for their own process, but still execute inadequate control due to the inadequate control actions of other controllers in the group, organization, or system.

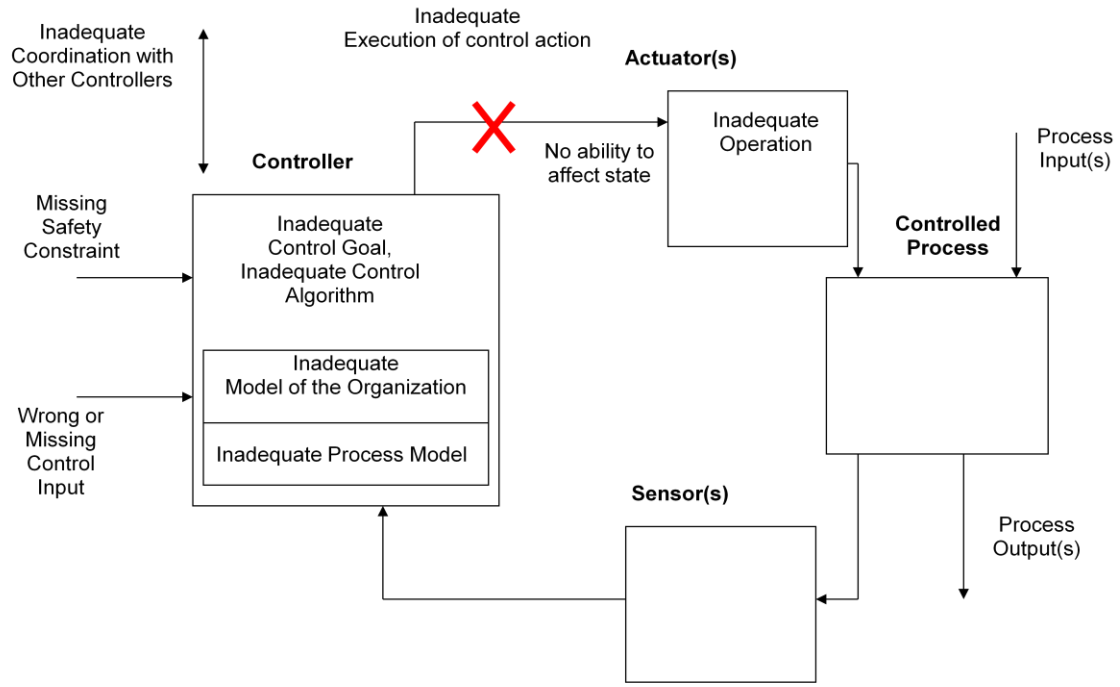

Figure 23 Controller Requirements for Control

The controller-level control requirements are discussed in detail:

1) Adequate Control Goal: The control goal is the plan, purpose, or set point that the human controller is attempting to achieve. The control goal can come directly from a superior controller (such as one's boss) or the organization's documented mission statement. Control goals can also be decided upon by the individual controller from an array of possible goals, with the choice dictated by the controller's own assessment of which is most important at the time.

2) Adequate Control Algorithm: The control algorithm is what the controller uses to achieve the control goal via control of the process. An adequate control algorithm leverages the controller's mental model of the process and the process goals to determine how to operate control levers to change the process state to meet process goals. Support for the development and maintenance of an adequate control algorithm over the course of the system's operation must be designed into the system. Control algorithms can be formalized as procedures or checklists, or may reside solely within the

minds of human controllers. Controllers may need to collect data in order to determine the appropriate action in a given situation. The design of tools to support the investigation of various courses of action must be provided in order to assure an adequate control algorithm.

3) Adequate Model of the Controlled Process: The control algorithm relies on an assessment of process state. All controllers must have a mental model of the process under control. This mental model of the controlled process includes the current state of the process and how they expect the process will evolve over time. The process model must also contain an understanding of how the process changes in response to inputs, as well as how the process transforms inputs into outputs. The process model includes a model of all the control elements (actuators and sensors), inputs, outputs, and disturbances that can affect the process. Furthermore, the process model includes a model of the environment.

   Process models are key to resilience. Resilient systems "recognize, absorb and adapt to disruptions that fall out of a system's design base" [20]. A model of potential disturbances helps controllers recognize disruptions when they occur. The model allows engineers to anticipate system states and use "feed-forward control," which can enable quicker response times to disturbances.

4) Adequate Model of the Organization: The human controller must also have a model of the organizational and how he or she fits within the organizational framework. Humans are adaptable, capable of learning and are able to perform in ways that were not preprogrammed. Because of a human's unique capacities, they are able to leverage their model of the organization to improve system safety in a wide variety of circumstances. For example, when a disturbance affects the performance of the process in a unique way, a human controller may need help from other members in the organization and must have a model of the organization to know with whom to discuss the issue. Alternatively, if the human disagrees with its control input (which may be a planned work assignment or a production target), he or she will need a model of the organization that includes an assessment of the viability of certain communication channels and a projection of the political feasibility of his or her desired changes.

   Humans are best used as controllers when there are potential disturbances, uncertainty about the process, uncertainty about the system environment, or all three. Humans are the only controllers that can successfully solve unprecedented problems, learn, and adapt to new situations. Technical controllers such as thermostats, or even complex pieces of software, cannot adapt to unprecedented situations and have no need for an organizational model.

In the organization literature, the proactive use of a model of the controller's organization has been called mindfulness [86], or heedful interrelating [59][82]. Developing a model of the whole system rather than merely the principle task assigned is important for a resilient organization. In a weak, non-resilient system, operators may not have a model of the organization. They do not share their insights into system safety issues, such as persistent maintenance problems.

Changes in the organizational structure have the potential to introduce high-risk operations while individuals update their model of the organization. Safety should be in mind while handling organizational transitions so that safety constraints continue to be enforced.

5) Adequate Coordination with Other Controllers or Decision-makers: Coordination with other controllers or decision-makers is necessary when multiple people are responsible for control over a process. At times, this may mean that control of the process is accomplished through mutual agreement on the performance of sub-tasks and agreed-upon roles in the control task. Requests for information can also fall under the "coordination" requirement. For example, controllers may need advice regarding their control action choices, they may need information about the process that is not available from their sensors, or they may request any other kind of information that would help them control the process.

In aviation, the coordination decision-making is commonly referred to as CRM delegation: many aspects of flying an airplane are jointly controlled by the captain and first officer.

When humans act as a control loop element (an actuator or sensor), coordination within the control loops is especially important. For human actuators or sensors to be effective they must:

1. Be motivated by, trust, and understand controller commands.
2. Be able to communicate information (give feedback) to the controllers about any problems or concerns that arise with the directive and be able to articulate an alterative option, if available.
3. Be able to freely communicate safety concerns up the command and control structure (e.g. without fear of retribution, concern that communication is 'unimportant', or concern that the boss will be upset).
4. Know the protocol for communicating with the controller: for example, sensors may need to know whether it is the responsibility of the controllers to ask sensors for information, or whether it is the sensor's responsibility to filter and relay relevant information to the controller.

Organization's Control Requirements

Decision makers removed from the immediate vicinity of an incident can also cause accidents through inadequate control actions. For example, the decision to enact a hiring freeze for non-production related staff could violate the requirement to have adequate staffing in the maintenance department. To prevent organizational "fuzzy" factors from causing accidents, inadequate control actions from those not at physically or temporally close to the accident must be identified. Fortunately, the process of finding instances of inadequate control on the part of organization is not a fuzzy process; organizations do have control requirements. The requirements for organizational success shown in the boxed text in Table 7 Organizational-level Control Requirements are new, but they are informed by the controller requirements discussed in the previous section and organization literature. These requirements capture the "structural" view of organizations, but also support a cultural and political view [144].

The requirements for adequate control at the organizational level are shown Table 7.

Table 7 Organizational-level Control Requirements

Adequate…
1) assignment of goals, control authority, and responsibilities
2) management of intra-organizational functional interactions to support safety-related decision-making
3) allocation of resources
4) organizational communication and feedback channels
5) safety management and learning processes
6) interaction with external bodies and stakeholders

The responsibilities of the organization include:

1) Adequate Assignment of Safety and Performance Goals, Control Authority and Responsibilities throughout the Organization to Support Safety-related Decision-making: Goals may range from specific production tasks, to general statements about core organizational purposes. Goals may be an expression of how the organization self-identifies. Many roles and responsibilities are assigned to controllers at the organizational level. Proper assignment of roles and responsibilities includes the assurance that the roles assigned are sufficient to meet system-level goals and enforce system-level safety constraints. The assignment of roles and responsibilities will inform the creation of the control

structure. As noted previously, many accidents arise when the organization has either too many individuals or no one responsible for a safety-related task.

2) Adequate Management of Organizational Functional Interactions: Hierarchies exist in the organization established by control over organizational processes such as staffing and budgeting. Individuals with power and political clout granted by such control over organizational processes must not subvert the control authority established by the safety-related control structure. For example, middle managers whose primary tasks concern organizational processes must not use their political influence to erode the decisions made by controllers over the safety process. In practice, many successful organizations create safety divisions that have the ear of the top management and whose budgets are set by company executive. Such divisions are more resistant to short-term company financial downturns.

3) Adequate Allocation of Resources: The organization must adequately allocate resources throughout the organization so that each controller has the necessary resources (staff, time, equipment, money) to accomplish their assigned goals. When resources are insufficient, controllers will use their allotted resources to the best of their ability, but safety will be compromised and the risk of an accident will increase. For example, a cut in a manager's maintenance budget can negatively impact system safety in two ways: 1) reduced resources make fulfilling all responsibilities impossible; and 2) reduced resources send a signal that maintenance (and safety) are low priority and that the controller should favor production goals over equipment maintenance goals.

4) Adequate Organizational Communication and Feedback Channels: Successful organizations must create communication infrastructure to support controllers in their efforts to achieve system goals. Communication channels should be in place both to accomplish predetermined goals and tasks and also to communicate information through the system in response to, or in anticipation of, disturbances that could impact the enforcement of safety constraints. Communication channels can be created through several avenues: procedures that establish reporting structures; required reports; meetings; the physical layout of the organization; and a staff devoted to listening and monitoring these channels. For example, if a particular safety group's monthly report to top management is ignored, the communication channel (the monthly report) has low bandwidth that will not adequately communicate safety concerns.

As the entity with a system-level view, the organization is responsible for communicating system-level goals, requirements, and constraints throughout the system and to external bodies. From prospect theory, we know that individual controllers may be risk-seeking in the face of potential loss and conservative in the face of potential gain. Without a system-level view to guide controller decision-making, the aggregate effect of individual controllers acting as individual decision-makers could move the organization as a whole into an increased state of risk.

The organization must not only set priorities for each system-level goal and constraint, it must ensure that organization-level decisions match stated priorities. The organization must communicate goals to provide motivation for safety-related tasks. This can be challenging, as the section of the organization responsible for safety messaging can be different from the section responsible for setting safety-impacting maintenance budgets and schedules. For example, the Baker panel report revealed that BP had a highly productive safety messaging organization with a multitude of new safety messages/procedures released each year. At the same time, however, BP also under-funded many refineries, and did not "always ensure that adequate resources were effectively allocated to support or sustain a high level of process safety performance" [70].

5) Adequate Dynamic Safety Management and Learning Processes: The organization must have an adequate learning and change process in place in order to adapt to disturbances or remain resilient when new opportunities become available. Organizational learning processes are key to incorporating lessons learned from incidents and accidents. An adequate safety management and learning process should involve reactive measures such as internal incident and accident investigations and applying resulting insights.

Proactive measures can include regularly performed audits to discover flaws in the operating system. Other aspects of dynamic safety management and learning processes are benchmarking, creating "feed forward" models of the system, managing the living organization and continual process of assessing [145].

A typical example of dysfunctional safety management and learning process is "blame and train." When the organization has an inadequate or ineffective safety group (either because of skill, or a shortage of sustainable resources) managers often respond to safety incidents or accidents by blaming individual operators, firing them, and training the rest. This kind of behavior leads to reticence among operators to report safety concerns and can move the organization to a state of higher risk.

6) Adequate Interaction with External Bodies and Stakeholders: The organization affects and is affected by its operating environment, whether that environment is the earth surrounding the factory or the unions whose members it employs. Stakeholders in the system can include potential accident victims, the public, and the government. External bodies can affect the priorities of individual controllers and may make safety-decreasing demands. For example, labor negotiations could impact the safety of a factory when union demands for guaranteed overtime hours leads to an exhausted workforce.

3.6 The Canonical Human and Organizational Factors that Contribute to Accidents

Several human and organizational factors cited in accident reports, human factors literature and organizational safety literature have been highlighted as recurrent contributors to accidents. Several of these canonical factors have been addressed and cited in current hazard analysis methods such as HFACS. However, they have not been included in a structured framework that is complete or that relates these factors to the occurrence of hazards in a systematic way. The HFACS method attempts to frame these factors in a cognitive fashion using Rasmussen's theory of errors [1]. However, these cognitive models, rooted in psychology, are not based on engineering principles. Furthermore, they are of little use when connecting the categorization of errors to the identification of hazardous scenarios that lead to errors and, finally, to the system engineering required to prevent errors. A useful taxonomy of human and organizational factors that contribute to accidents should be based on psychological principles and be structured using engineering principles to ensure completeness. Control theorists have already identified all the necessary conditions for adequate control, therefore I will use control theory as the framework for categorizing the human and organizational factors that contribute to accidents.

3.6.1 Inadequate Assignment of Roles to Controllers

Overlaps of responsibility: Assigning the same responsibility to multiple controllers causes overlap in the enforcement of safety constraints [7]. In many systems, overlap of safety-related responsibilities (those responsibilities which are assigned to enforce safety constraints) has been done with the intention of creating operational redundancy. Redundancy is a technique commonly used to increase safety in electro-mechanical systems that has been frequently misapplied to other types of systems and system components. The assumption that a human controller can step in and adequately control a process in the event that the "primary" human controller fails to fulfill their assigned task is often fantasy.

For example, in the Zeebrugge accident [8], the responsibility of ensuring that the ferry bow was closed was assigned to both the Assistant Bosun and the First Officer. When the Assistant Bosun was unavailable and did not close the door, the designers of the ferry's operating procedures may have assumed that the task would be done by the First Officer. However, the First Officer was also unavailable to close the door. In fact, the "redundant state" wherein both the Assistant Bosun and the First Officer were available to perform the task was typical only of routine operations. The factors that led to the unavailability of the Assistant Bosun also affected the availability of the First Officer (which is the common mode failure problem in engineering). Each of the ferry operators may have assumed that their "backup" would perform the role.

Duplication of role assignment between people can backfire when system issues lead to an unavailability of anyone to perform the role. It is safer to design in formal role assignment handoffs and transitions. The assumption that the probability of each controller being unavailable to perform a task is independent is not sound for human systems.

Gaps in responsibility: Gaps in safety-related responsibilities play a role in accidents as well. A gap in responsibility occurs when no controller is responsible for the enforcement of a particular safety constraint. Gaps can occur because the role to enforce the safety constraint, or the safety constraint itself was overlooked, or because there was confusion surrounding whom in particular was responsible for the enforcement task.

For example, in 1999 a Titan IV B-32/Centaur TC-14/Milstar-3 launch to place a satellite in orbit was unsuccessful in part due to a gap in responsibility. While safety-related hardware testing was common up until launch, there was no one in charge of testing or verifying software safety once the software had been loaded on the rocket hardware. Incorrectly entered constant values in the software led to loss of control of the rocket and resulted in an ineffective and unusable final orbit for satellite operations. All roles and actions required to ensure safety must be identified and assigned.

Gaps and overlaps in the assignment of responsibilities occur when the organizational control requirement— *Adequate assignment of goals, control authority, and responsibilities*— is violated and creates confusion for the individual controller and can interfere with their ability to understand what they are responsible for. At the individual controller level, this can lead to a violation of their requirement to have an *Adequate control goal* or *Adequate model of the controlled process.*

3.6.2 Missing or Delayed Feedback and Communication to Controllers

Examples of delayed or missing feedback or communication contributing to accidents abound within the organizational safety and human factors literature [4][5][9][9][17][25][26][76]. The Titan IV B-32/Centaur TC-14/Milstar-3 launch was also unsuccessful because of missing feedback between controllers. In particular, a guidance engineer noticed anomalous readings in the launch software, but the message was not heard in time by managers who were able to understand and resolve the issue. And so an identified, yet insufficiently communicated software bug resulted in the loss of an expensive military asset.

Missing or delayed feedback is typically labeled a "communication problem". The crux of accidents due to communication issues is that the needed safety-related information does not reach the acting controllers (decision-makers and influential people within the organization) at the needed time. This is akin to a time delay or missing feedback from a sensor in a typical control loop.

Failing or inadequate communication channels can result from an organizational inability to enforce the requirement *Adequate organizational communication and feedback channels* or *Allocation of resources* and other requirements. At the individual level, this can cause an inability to fulfill the requirements to have an *Adequate Coordination with other decision-makers,* or *Model of the controlled process*. Any requirement that requires communication from others in the organization could be violated if appropriate communication channels are not in place.

The challenge for a hazard analysis is to:

1. Identify scenarios where there is no adequate channel to communicate needed information.
2. Identify how information can be delayed or stopped.

The communication processes and the physical and organizational structure that support communication must be in place and designed with safety in mind.

3.6.3 Assumption of Goal Independence and Incorrect Prioritization

System operators typically have several goals in mind for the performance outputs of the system. Accidents can occur when efforts to achieve one goal causes an unsafe outcome for the system. For example, decision-makers in the healthcare system try to simultaneously achieve goals centered around safety, clinical effectiveness, cost-effectiveness and accessibility. Due to the effects of long delays, complex feedbacks, and the sometimes conflicting goals of system decisions-makers, attempts at

achieving one system goal without adequate consideration of system interactions has led to a failure to make significant gains along any dimension. In particular, in an effort to increase cost-effectiveness, hospitals have expanded their ad hoc patient referral base and overloaded their operation schedules without a corresponding increase in resources to treat the increased patient load. Without adequate resources to treat patients, patients are at increased risk of an adverse event; which increases the cost of care [71].

The relative priorities of goals can be informed by the organization, which has an obligation to provide *Adequate communication of system-level goals and constraints*. If a particular controller has ranked their multiple responsibilities in a way that harms safety, they will violate their requirement to have an *Adequate control goal.*

The hazard analysis method must help engineers identify scenarios where controllers can inadvertently subvert system level goals in pursuit of their own individual goals. If a safety constraint is put in place to constrain an individual controller, it must be understood and motivated so that it will not be violated. Furthermore, in the case of multiple goals, the hazard analysis method must identify scenarios where goals are incorrectly prioritized, creating unsafe behaviors.

3.6.4 Local Optimization

Local optimization is the maximization of benefits given the incentives and constraints levied upon controllers. Such optimization can be expected to happen and is not necessarily negative—free markets are based on the idea that individuals in pursuit of their own good create value that the entire country enjoys. However, local optimization can become a problem when the controllers operate the system in such a way that system-level goals are subverted and hazards can occur. From a performance point of view, local optimization is problematic when it makes system-level goals (global maximums) unachievable. The hazard analysis method must expose situations that can lead to undesirable local optimization or similar control requirements can be violated as in noted in 3.6.3.

3.6.5 Optimistic Risk Assessment Under Uncertainty

Research has shown that optimistic risk assessment is a common problem when uncertainty about the probability of negative consequences is high, and the benefits of "risky" decisions are clearly known [115]. Given that much safety-related decision-making occurs under these conditions, it is imperative to constrain behavior to an accepted level of risk. The ability for a controller to make decisions about risk depends on their ability to maintain an *Adequate model of the controlled process.* In some cases it is

possible for the organization to make safety-related tradeoffs more clear through the use of *Adequate safety management and learning processes.* The hazard analysis should identify situations where controllers must make decisions about safety but do not have sufficient data or tools to make accurate assessments.

3.6.6 Decision-making with a Distant Relationship between Cause and Effect

As has been discussed previously, people have difficulty predicting the evolution of state and making decisions in cases where there is a large remove (either time delay, spatially distant, or a change in form) between an action or decision and its effect. Such a remove can make it impossible for a human to have an *Adequate model of the controlled process* or even an *Adequate model of the organization.* Examination of the system design should include looking for ways large disconnects between control actions and control outputs can arise and identifying strategies to eliminate or mitigate the effect of the disconnect.

3.6.7 Inadequate Understanding of the Effect of Feedback

Humans have difficulty predicting the effects of accumulation and feedback. Without direct access to a process state and with only access to process inflows and outflows, the controller's mental model will often be incorrect [24][63]. When this canonical factor occurs, it leads to the violation of the *Adequate model of the controlled process.* The hazard analysis method should identify situations where people will have to take feedback into account. Then system engineers can modify the design to either eliminate the need to take feedback into account to accurately predict system state, or they can provide estimation tools to support the creation of an accurate mental model.

3.6.8 Non-events

The identification of "non-events" is simple for software-based controllers using "watchdog timers," but is nearly impossible for human controllers. That is, the *absence* of a signal, reading, or key piece of information is not immediately obvious to humans, and they are not able to recognize that an absent signal is an indication of a change in the process state [120]. Succinctly put, humans operate in an "out of sight out of mind" fashion. In Dekker's Turkish Airlines flight TK 1951 accident analysis [146], he notes that pilots did not notice the *absence* of a critical mode shift. Without noting that the mode was *staying the same*, the pilots' mental modal of the aircraft state was incorrect, and they consequently did not know actions were needed to save the aircraft. In general, without a dynamic change, the continuance of a persistent signal does not lend itself to keeping an accurate mental model. Especially in alert situations, the signals, communication, feedback and information from the operating process must be able to be

registered and noticed by humans. This factor is yet another condition that can lead to an inadequate *Model of the Controlled Process*. The hazard analysis should identify how inadequate control can occur due to "non-events".

3.6.9 Control of High Order Systems[8]

Humans are not suited for the control of higher order systems because they require anticipation and prediction of accumulated states. From controlling a mouse position [147] to piloting a sailboat for the first time [148], humans have difficulty with the control of high order systems. Humans typically attempt to control high order systems as if they were able to directly control the state variable of interest (rather than a 2nd order time derivative of it). Overshoots and undershoots and oscillatory behavior are the common result of human control of high order systems[149].

A common high order control task occurs in management: Managers are tasked with the control of backlogged orders. Unable to directly control the rate at which work is completed, they can only control the workforce. Furthermore, managers are not able to directly control the workforce, but only the rate at which people are hired. This leads to a 2nd order control situation and expensive over-hires and firings can result.

For some systems, a reasonable "settling period" to reach steady state is acceptable, and small overshoots and undershoots can be tolerated. But the hazard analysis method must consider what kind of control (0th order, 1st order, 2nd order or higher) is implicated by the design, what form the repercussion of that may take (stability, settlings time, overshoot, etc.) and what the costs of consequent overshoots, undershoots, and instabilities will be. Deviations caused by higher order control demands may be acceptable, but they must be anticipated and planned so they do not result in inadequate control. The inability to control a high order system leads to an *Inadequate Control Algorithm.*

3.6.10 Cognitive Factors

Risk aversion: The gravitation of an individual, or a group of individuals, to some point on a continuum from completely risk averse to extremely risk seeking, is based on the situation they are analyzing, their assets, their resources at hand, and their personality [116].

[8] A high-order system is one that requires controllers to control the second derivative of the state variable of interest. For example, many manual control contexts require that humans control the position of an object by controlling the objects acceleration (rather than controlling the object's position directly (0th order) or the object's velocity (1st order)).

The design of a controller's roles and responsibilities should take into account what kind of risk situation is presented to the controller. Relative to one's current position or assets, people are generally more risk seeking to avoid potential losses than they would be when considering potential gains [116] as shown in Figure 24.

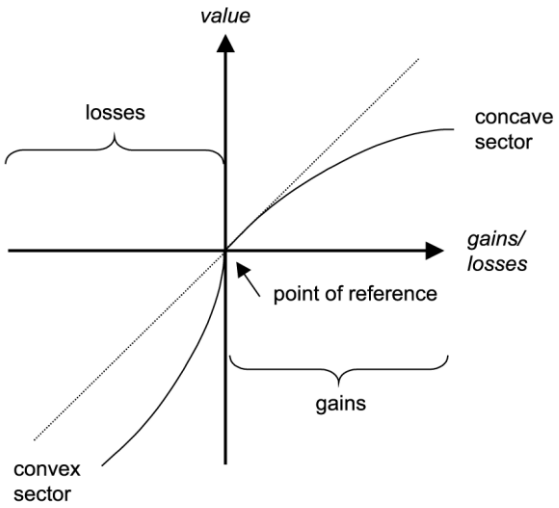

Figure 24 Prospect Theory: Risk Seeking to Avoid Potential Losses and Risk Averse when Faced with Potential Gains Source: [121]

Finally, the personality of the human acts as a baseline risk state and can have an impact on system operation. Psychiatric tests exist that can determine an individual's risk-seeking propensity. Such psychiatric evaluations are commonly used in CEO searches because it is often desirable to have risk-seeking CEOs in charge [150]. As Jeffrey Pfeffer said, "You can't be normal and expect abnormal returns [119]." Other roles are more suitable to risk-averse people, but it should be noted that safety-roles need not be staffed by risk-averse people, as new safety-related innovations and ideas can stem from risk-seeking individuals. The hazard analysis should find scenarios where the situation, as well as the assets and personality of the controller, will lead to unacceptable decision-making. The system can be designed to influence the risk tolerance of decision-makers by framing decisions in terms of losses and gains. When risk aversion or risk-seeking behavior produces undesirable results, the controller was not able to deliver an *Adequate Control Algorithm.*

History: System engineers cannot set the initial conditions for a human controller. Everyone has past experiences that will inform their assessment of the controlled process, influence how they choose to control it, and influence how they regard data and information used to inform their mental model of the

process. Past experience is an important consideration for determining how new and continuing controllers will act.

The perspective of new controllers may be influenced by prior organizational cultures to which they have been exposed. Their past experiences may blind them to some sources of data or may influence their preference for certain decisions. As controllers gain experience in their role, their history with tools will influence their resistance or eagerness to use them again. For example, requiring users to use a safety screening tool that is perceived to waste time and have little value will not work; controllers will find ways to avoid using it. Even the introduction of a new tool that is defect free may still require a significant adoption time while experienced controllers overcome their distrust of it due to their experience with similar tools [71]. The history (or the lens) that controllers use to understand the system under control and develop their control algorithm can affect their ability to enforce each of the controller-level control requirements. The hazard analysis must identify scenarios where a controller's history (e.g. with data collection tools or with the process itself) will negatively impact safety.

Culture: Some cultural expectations translate to simple operating constraints, such as particular operating hours or holidays. However, other culturally imposed constraints can be difficult to discern. Both cultural norms and the commitment to cultural norms vary from place to place. For example, in Korean culture, age seniority dictates communication style and ability. Younger pilots are not easily able to speak up and question the actions of older pilots, and their suggestions are made in "soft" language, rather than more direct speech used by Western pilots. During this time, for some pilots, it was more important to be polite to elder captains than communicate safety-related observations to superior controller. The communication in Korean Air Lines cockpit was so hampered by this that crew resource management (CRM) was absent and the airline had one of the worst safety rankings in the world in the late 1990s. With CRM training, the pilots were able to learn a new way of communicating in the cockpit that was able to transcend their culturally imposed communication style. Today Korean Airlines maintains a high safety record [163]. Due diligence in the hazard analysis phase can unearth potentially hazardous cultural constraints. Similar to the History human factor, the cultural considerations can also lead to a violation of all the control requirements.

Monitoring: Humans do not make good monitors of all automated processes [123]. They are best used as active controllers with engaged minds. After about twenty minutes, most humans get bored with monitoring to the point that their mental model of the process becomes inaccurate [147]. If after twenty minutes, the monitored-for event occurred, the controller may not have the situational awareness to react

effectively or may not notice that anything of significance has happened at all. People cannot monitor automated tasks and be expected to recover the system in a disaster. Automating human control takes away opportunities to practice and to form a good mental model of the current state of the system [124]. The field of human factors is actively pursuing research to discover the appropriate balance between "man and machine" control [147].

Another type of monitoring includes using people as perfunctory "double-checkers." This type of monitoring role consists of merely checking or verifying that someone else has done their job when no proof is required other than a checkmark. There should be some task created that engages the checker or regulator in the verification task, otherwise in the face of other pressures, they may choose to skip the verification task. Furthermore, if others in the organization know about the double-checking procedure, they may develop a sense of security that a mistake may be caught further down the line, leading to a false sense of redundancy [124].

Considering the ineffectiveness of human monitors, their use may give misleading sense of security [124]. Monitoring can lead to poor *Coordination with other decision makers* as well as inadequate *Control Algorithms.* The hazard analysis must call attention to the use of human monitors and make sure that the choice to use monitoring is safe.

3.6.11 Constraints from external bodies

Complex systems do not exist in a vacuum[9]; external systems will impose design constraints upon them. For example, change that affects laborers must comply with the laws of federal and local governments and regulatory bodies such as the Occupational Safety and Health Administration (OSHA). External systems, such as unions or advocacy groups, can impact internal company procedures such as overtime pay or local labor hiring quotas. For example, unsafe overtime requirements from unions may lead to a safety constraint violation of operator rest constraints. When requirements and constraints from external bodies are not considered by designers, they may conflict with safety-related constraints and engender hazardous scenarios and may lead to the violation of the *Adequate interaction with external bodies and stakeholders* requirement.

[9] and even if they do…

3.6.12 Following Checklists

In a staggering number of accidents, operators or pilots are blamed for not following the checklist or procedure; either skipping steps, doing the wrong step in a list or omitting the checklist or procedure all together [125][134][135][136][137][138]. These kinds of accident reports typically excoriate the operators for the checklist problems and suggest more training as the solution that will bring about proper checklist behavior. However, these accident investigations are predicated on several checklist assumptions, including that needed tasks can be completed in the time allotted in the present conditions and that steps can be completed in a linear, sequential (non-overlapping, non-feedback) fashion [122]. In real-life however, this assumption is rarely true. Complex control tasks often require overlapping tasks, and operators must continually use feedback in order to safely control the process [19]. Furthermore, checklists are often brittle, they cannot suggest a course of action for each disturbance humans may encounter, and aren't able communicate to the controller when they are best laid aside or deferred [124].

The checklist debate is nuanced. The introduction of checklists has improved cockpit CRM and aviation safety [155]. For this reason, healthcare practitioners have sought the introduction of more checklists in healthcare settings and have been met with mixed results [17] [93]. It seems that the "right" checklist is helpful in some situations. An examination of how people use and respond to the use of checklists should be a part of a human and organizational hazard analysis. Poorly designed and integrated checklists can impact the controller's ability to fulfill any of the individual control requirements.

3.6.13 Summary

The human and organizational factors described above are the commonly cited causes of human and organizational "failure". It is these factors that enable hazardous scenarios to occur and accidents to happen. What is needed now is a method that formally identifies design flaws in the technical, organizational, operational and regulatory aspects of the system that can lead to the human and organizational factors highlighted in section 3.6.

3.7 Human and Organization Human Error Taxonomy

The STPA taxonomy of causal factor was changed to focus on human and organizational factors as presented below. While the causal factors for human error taxonomy provides coverage of individual controllers and the organization as a whole, it does not explicitly highlight the flaws associated with teams. The dynamics of teams are a separate study and have been discussed in Lamb [156]. A causal factors taxonomy that is specially designed to focus on teams is left for future work.

3.7.1 Individual Error Taxonomy

At the controller level, inadequate control actions occur due to:

1. Inadequate control goal
   1.1. Goal(s) necessary for enforcement of safety constraints are unknown
   1.2. Achievement of control goal violates safety constraints
   1.3. Goals are wrongly prioritized

2. Design of the control algorithm does not enforce constraints
   2.1. Control algorithm does not match the scope of the process under control.
   2.2. Control algorithm is incompatible with control levers.
   2.3. Controller has inadequate understanding of their own control authority
      2.3.1. Does not know that the process is controllable
      2.3.2. Does not know the scope (process boundaries) of their area of responsibility
      2.3.3. Does not know how their control authority evolves with the state of either the controlled process or the actions of other controllers.
   2.4. Controller is not able to execute or perform the control algorithm
      2.4.1. Does not understand how to execute the control algorithm
      2.4.2. Control algorithm is incompatible with the controller

3. Model of the controlled process inconsistent, incomplete, or incorrect
   3.1. Inadequate understanding of process boundaries
   3.2. Inadequate understanding of how one's controlled process is influenced by
      3.2.1. Outputs of other controlled processes in the system
      3.2.2. Process inputs from outside the process/system boundary
      3.2.3. Control inputs from outside the process/system boundary
      3.2.4. Disturbances to the process, actuator, sensor or communication and feedback channels
   3.3. The method for updating process model is inadequate
      3.3.1. Inadequate understanding of how to process feedback and command history to form an accurate mental model of process state over time.
         3.3.1.1. Feedback and accumulation is not understood

4. Model of organizational structure (other controllers in the control hierarchy) is inconsistent, incomplete or incorrect

5. Inadequate coordination between decision makers

6. Inadequate execution of control loop
   6.1. Inadequate actuator operation
   6.2. Expected process inputs are wrong or missing
   6.3. Expected control inputs are wrong or missing
   6.4. Communication flaw
      6.4.1. Control action not communicated to actuator
      6.4.2. Feedback to controller is inadequate, late, or missing
         6.4.2.1. Feedback channel has insufficient bandwidth

At the organization level, inadequate control actions occur due to:

3.7.2 Organizational Error Taxonomy

1. Inadequate assignment of goals, control authority and responsibilities to controllers
   1.1. Inadequate coordination among controllers and decision makers
      1.1.1. Overlaps of responsibility
      1.1.2. Gaps in responsibility
   1.2. Role is not suitable for human control
   1.3. Inadequate organizational change process for the reassignment of roles and goals

2. Inadequate allocation of resources to controllers throughout the organization

3. Inadequate assignment of controller hierarchy
   3.1. Hierarchy surrounding organizational processes do not support safe control

4. Inadequate communication channels provided for in the organization
   4.1. Communication channels do not exist
   4.2. Communication channels do not have sufficient bandwidth
   4.3. Communication channels are not created or eliminated in response to changing circumstances.

5. Inadequate communication of system-level goals and constraints

6. Inadequate safety management and learning processes

7. Inadequate interactions with external bodies

3.7.3 Taxonomy assessment

The causal factor taxonomy is a framework that can be used for understanding previous accidents and anticipating how system behavior may be inadequately controlled. However, I found that the guidance provided by the taxonomy of limited use when applied to the prospective analysis of social systems that had not yet had an accident. The leap between error classification and use of the taxonomy to forestall the occurrence of errors in design is less clear with humans and organizations than it is for technical systems. A process that shortens the leap between the classification of human and organizational errors to preventing them from occurring was needed. While a taxonomy of causal factors that lead to inadequate control from a human and organizational point of view is useful in accident analysis and investigation, it is only part of the solution. For this reason, I created a structured technique using guidewords to allow engineers to seek out flawed design (organization interactions, procedures, and etc.) before they lead to inadequate control and hazards. Useful safety engineering methods must identify *how* flaws in the mental models of humans or organizations can occur and what will lead to mismatches between reality and the mental model that adversely affects safety.

The accident and hazard analysis methods presented in this dissertation use a process to analyze the human's social and technical context to discover causal factors for inadequate control. The method for accident analysis will be demonstrated using the accident discussed in the next chapter.

CHAPTER 4 ACCIDENT EXAMPLE: NOGALES

4.1 Chapter Motivation and Overview

To test the feasibility of my accident analysis approach, I applied it to the crash of an unmanned aircraft (UA) in Nogales, AZ. This National Airspace System (NAS) is a complex socio-technical system that is on the cusp of a major change. Companies such as FedEx and UPS have expressed interest in UA-provided transport of cargo, as they believe there is financial reward in doing so. Military groups have pushed the FAA for more waivers to fly military drones through the NAS on the way to flight testing zones or to patrol the US borders.

The addition of unmanned aerial systems (UASs) into the NAS would present a major disruptive technology with great potential financial and security rewards. However, UASs are not only complex machines with millions of lines of code, they are operated by teams of ground-based pilots. These pilots do everything from manual flight control of the planes (e.g. keeping the wings level) to high-level mission-based planning (selecting waypoints and routing aircraft to interesting spots). The organizational control over UAS and NAS integration is also complex, involving private industry, unions, civilian advocacy groups, all military branches and civil regulators. At this point, it is unknown what level of control or influence each of these groups should contribute to *making decisions* about how to integrate UASs, much less what their *role* should be in the integrated NAS. The hazard analysis should be applicable to the design of the organization *developing* (creating the new rules and making design decisions) the new UAS integration as well as the organization that will *operate* the integrated UAS–NAS system.

This chapter provides an overview of the UA accident. This accident will serve as a continuing example referenced throughout this dissertation for explaining concepts and processes in the accident analysis method described later in this thesis. A full analysis of the accident is included in Appendix 1.

4.2 Nogales, Arizona: Loss of Predator Unmanned Aircraft

On April 25, 2006, a Predator-B unmanned aircraft crashed within 100 yards of a home in Nogales, Arizona [125]. The accident illustrates the number of human and organizational factors that typically contribute to an accident. If current flaws in unmanned aircraft system (UAS) design are left uncorrected, future accidents could have more serious consequences. While this accident did not result in human

causalities, the crash has managed to cast doubt on whether safe UAS operation in the national airspace system (NAS) is possible.

The UAS had been issued a waiver by the FAA to fly a surveillance mission within the NAS. The waiver issued is called a Certificate of Authorization (COA) that allows an air vehicle that does not nominally meet FAA safety standards access to the NAS. The COA is issued to public agencies for aircraft that do not meet standard FAA certification requirements that are believed to achieve *benefits* to the national good (e.g. increased national security) that outweigh the *risks* of granting them access to the NAS. The COA application process includes measures to mitigate risks, such as sectioning off the airspace to be used by the UAS and preventing other aircraft from entering the space.

In the Nogales accident, the COA was issued to the Customs and Border Patrol (CBP) agency, which was responsible for operating a UAS for border security purposes. The CBP had contracted with General Atomics Aeronautical Systems Inc. (GA-ASI) to design and fly the UAS. As the CBP did not have in-house flying expertise, it had agreed to hire Air Force personnel to oversee the GA-ASI pilot training records and approve them for flying the UAS.

4.2.1 Overview of the Unmanned Aerial System

The UAS in this accident consisted of the Predator-B unmanned aircraft (UA), ground control station (GCS), the communication channels connected to the UA, and the interfaces between these subsystems.

The UA was controlled through a GCS that houses the UA flight controls and displays. Because the datalink between the GCS and the UA was line of sight (LOS), the UA had to be visible to the GCS to be controllable. The system included safeguards to prevent loss of control due to lost communications. If the LOS communications were lost, the UA would initiate a "lost link profile" on board that causes the UA to fly a preprogrammed flight plan within a specified airspace region that would create an opportunity for pilots at the GCS to restore communications. If communications cannot be restored before fuel reserves are exhausted, the lost link profile directs the UA to crash in a remote area.

Air traffic control (ATC) maintained safety of the NAS by issuing a temporary traffic restriction (TFR) in the area that the UA is permitted to fly. General aviation aircraft, which practice self-separation techniques to avoid mid-air collisions, were alerted of TFRs and do not fly into these areas. This procedure ensured the UA (a "non-cooperative aircraft" that other pilots are not able to communicate with) do not fly in the same airspace as general aviation aircraft.

Within the GCS, the UA is controlled by a pilot who sits at one of two control positions at a workstation. An example control position is shown in Figure 25. Next to the pilot in Pilot Payload Operator Position 2 (PPO-2), a Customs and Board Patrol (CBP) agent surveys sensor data from the UA looking for evidence of security threats along the US-Mexico border. While the pilot usually sat in position PPO-1 to control the UA and the CBP agent usually sat in PPO-2 to control the UA camera, the positions are reversible. Control of the UA can be performed from PPO-2 and the UA camera may be controlled from PPO-1. The control stick used by the pilot to control the aircraft, shown in Figure 25, is labeled with controls suitable for the control of the aircraft, but it is physically identical to the control stick used by CBP agents to control the camera.

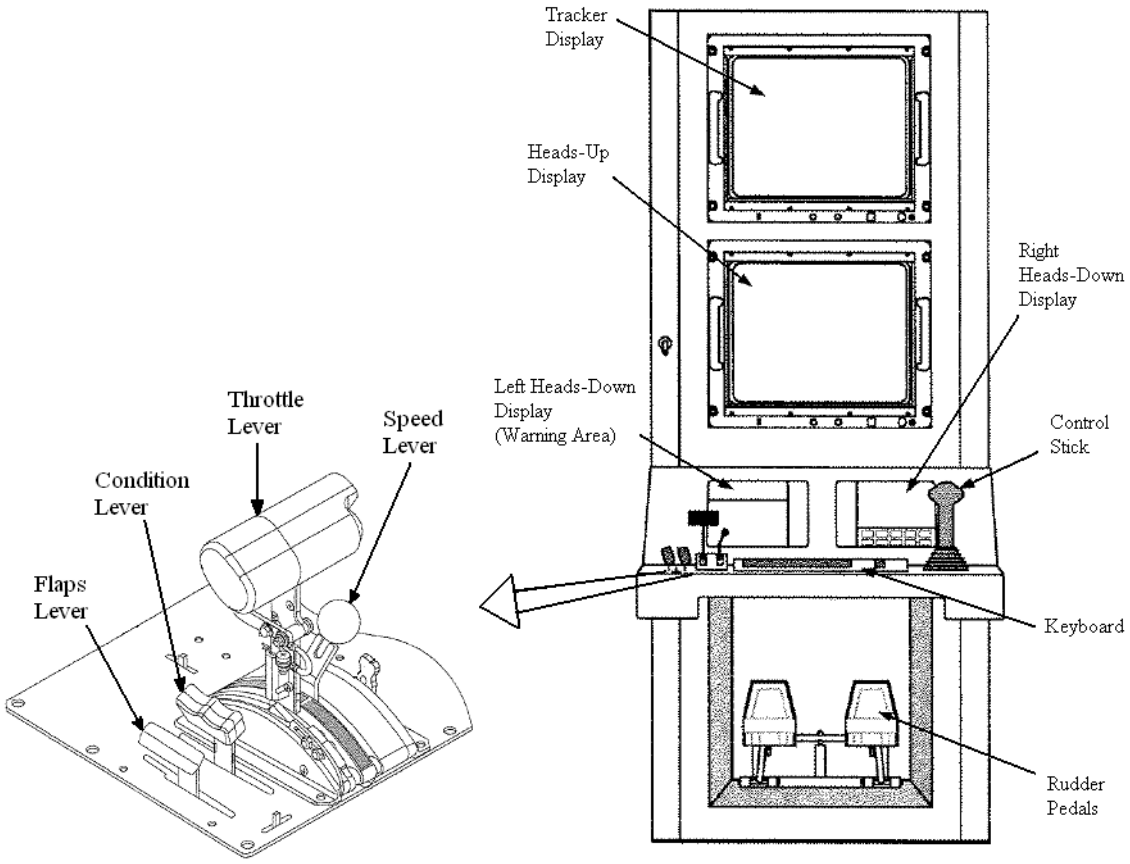

Figure 25 Pilot and Payload Operator Workstation located in the Ground Control Station Source: [125]

4.2.2 Causal Events related to the Loss.

A lockup on the PPO-1 console occurred and caused the pilot's data display to freeze. Without following a checklist, the pilot moved to the PPO-2 position and switched the piloting controls from PPO-1 to PPO-

2. The CBP agent that had been operating the camera left the area. Unnoticed, the PPO-2 control stick was in fuel cutoff position, and with PPO-2 position in control, the UA engine starved. As the UA's engine ran out of fuel, the UA lost altitude, descending below line of sight from the GCS. Unable to diagnose the cause of the altitude loss, the pilot power cycled the workstation controls in order to initiate the lost link profile and buy more time to diagnose the fault. Once the lost link profile was initiated, the onboard UA software automatically cut off backup communication with the Iridium satellite datalink. Without a high enough preprogrammed altitude, the lost link profile did not allow the UA to regain LOS communications with the GCS. The UA flew uncontrolled through the NAS until it ran out of fuel and crashed near a populated area in Nogales, Arizona.

Simplified Events Timeline

Lockup on PPO-1 occurs

Pilot switches control to PPO-2

PPO-2 control positions shuts off fuel to the UA engine.

UA loses altitude

Pilot power cycles Ground Data Terminal, which initiates the lost link profile.

On reserve battery power, the UA starts to fly a lost link mission profile that does not achieve sufficient altitude to re-establish LOS communication.

UA flies uncontrolled through the NAS outside the TFR.

UA crashes

These events, causally related to the loss, do not begin to give insight into the multitude of human and organizational factors related to the loss. The key to preventing future accidents is to understand why each event or decision occurred. The high level analysis begins below.

4.2.3 High Level Analysis

The accident analysis starts by identifying the loss event that occurred and the related hazards.

Actual Loss Event:

UA is lost (crashes)

The hazards directly related to the Nogales accident and the loss event above, are:

Loss Event Hazards[10]:

Populace is exposed to an uncontrolled UAS landing.

UA flight (including landing) is not controlled.

[10] The loss event hazards could have also led to another potential loss event: Ground-based populace or assets are killed, injured or damaged by UA crash

Other hazards occurred during the accident, but by chance they did not lead to a loss event. These hazards will be analyzed as well. It is important to include all hazards that the system was exposed to as the accident analysis process is useful not only for understanding the accident and the related design flaws that contributed to it, but it is also useful for discovering design flaws that didn't result in an accident, but could have.

Other Experienced Hazards[11]:

UA flies in the NAS without separation services. (Potential Loss Event: Mid-air collision)

UA position or trajectory is unknown (Potential Loss Event[12]: Partial NAS shutdown).

Safety constraints, as have been described in [8] are requirements that eliminate or mitigate a hazard. Safety constraints are derived from the hazards by translating the hazard to an engineering goal that would prevent the hazard from occurring. The safety constraints necessary to prevent all hazards discovered are:

Safety Constraints:

- UA must not crash in a populated area.
- UA must maintain 5 nautical miles horizontal separation and 1000 ft vertical separation between itself and other aircraft in the NAS.
- UA flight (and landing) must be controlled at all times.
- UA position or trajectory must be known at all times.

If the above safety constraints are violated, safety constraints at a lower level of design can be applied. For example:

- Emergency procedures must be available and followed for loss of contact with UA.
- All sectors of the NAS that could be affected by a UAS hazard must be alerted.

4.2.4 Control Structure

The control structure was created through a thorough examination of the NTSB investigation report. The responsibilities for each controller in the control structure were identified using the NTSB accident report. In turn, the NTSB identified the responsibilities in the course of their investigation using source documents such as manuals and organization charts. The safety constraints for each controller are derived

[11] There are additional loss events and associated hazards that can occur with the integration of public-use UAS into the NAS not included here that will be discussed in the extended example in chapter X.

[12] Partial shutdown of the NAS would result in the loss of revenue to multiple stakeholders. As was stated previously in this thesis, loss events include harm to people, property or a great deal of money. Safety practitioners can define loss events to be whatever must not occur in pursuit of system goals.

from the system-level safety constraints and responsibilities. The roles, responsibilities and safety constraints for each element in the control structure shown in Figure 26 are below:

Roles, Responsibilities, and Safety Constraints:

FAA:

- Issue a Certificate of Authorization (COA) to public-use applicants to allow flight of UA in the NAS for reasons that support the national good. The FAA creates the requirements for what the COA applicant must provide as evidence of a safe system.
- Ensure the Safety of the NAS and protect against aircraft-related crashes.
    - Ensure that the Air Traffic Controllers are able to adequately separate aircraft in the airspace.
    - Ensure that the UA can safely fly in the NAS
        - Ensure that the UA operator is capable
        - Ensure adequate maintenance of the UAS
        - Ensure that the COA issuance process is adequate
        - Ensure that the CBP provides enough evidence that its UAS mission will be safe.
        - Must not allow unsafe UAS access to the NAS.
        - Must not allow UAS access to airspace above populated areas.

CBP

- Fulfill the requirements of the COA.
    - Ensure that GA-ASI is operating a safe UAS
        - Ensure that pilots are adequately trained to fly the UA.
        - Ensure that the GA-ASI provides enough evidence that its UAS mission can be conducted safely.
            - Demonstrate that injury to persons or property along the flight path is extremely improbable.
            - Demonstrate the maintenance program outlined by GA-ASI is adequate.
    - Verify lost link profile from OSI meets COA requirements.
        - CBP supplies safety-related requirements for the lost link profile to OSI.
        - Ensure that UAS operations are not conducted over populated areas or heavily trafficked roads.

GA-ASI

- Ensure the UAS is operated in a safe manner
    - Ensure interactions between the UA, GCS, and pilots, are safe
    - Ensure GCS meets requirements for safe operation
    - Ensure that pilots are capable of adequately flying the UA
        - Review pilot training records
        - Require pilots to demonstrate adequate flying skills before being approved
- Provide CBP with information about UAS safety
    - Provide evidence to CBP that pilots are capable
    - Provide reports to CBP that demonstrate UAS safety

GA-ASI Pilots:

- Fly the mission safely. The pilot has final authority[13] and responsibility for the operation and safety of the flight.
    - Follow safety related procedures.
    - Perceived requirement: Activate loss link profile in the case of unexpected loss of control over UA.
- Must be in contact with relevant ATC facilities at all times and share safety-related information:
    - Notify ATC in the event of an emergency
    - Must notify ATC regarding any changes to lost link profile.
    - Must inform ATC if she/he loses link with UA.
- Perform a pre-flight inspection.
    - Ensure that the lost link profile is set correctly:
        - Lost link profile minimum altitude must allow UA to be viewable from the GCS.
        - Verify that route does not cross populated areas or busy roads.
        - Verify that lost link profile landing target is unpopulated.
        - Lost link profile must be within the TFR set by ATC.

[13] The term "final authority" comes from documentation from the NTSB reports. While the term is not something the author might assign the pilot in this situation, the NTSB report indicates that it was the term used by GA-ASI and CBP.

- If controls must be switched between PPO-1 and PPO-2, follow procedure for doing so.
    - Procedure is: With pilot and payload operators remaining in their stations, match positions for secondary controls to primary controller. Switch control between primary and secondary control.
- PIC: In the event of a lost link with UA, transmit the following:
    1. The UAS call sign.
    2. UAS "Identification, Friend or Foe" squawk.
    3. Lost link profile.
    4. Last known position (as per FAA procedures, position information will be given relative to navigation aids).
    5. Pre-programmed airspeed.
    6. Usable fuel remaining (expressed in hours and minutes).
    7. Heading/routing from the last known position to the lost link emergency mission loiter.

CBP Payload Operator

- If controls must be switched between PPO-1 and PPO-2, follow procedure for doing so.
    - Procedure is: With pilot and payload operators remaining in their stations, match positions for secondary controls to primary controller.

UA

- Follow LOS commands from pilots.
- If LOS communication is lost:
    - Attempt to connect with pilots via backup communication system using Iridium satellite system.
    - Follow lost link profile.

OSI:

- Develop safe Lost link Profile that satisfies CBP requirements

Air Force GFR

- Evaluate pilot training schedules and requirements.
- Certify that pilots have completed training sufficiently.
- Provide input to CBP about what training is necessary.

ATC

- Clear the TFR allocated to the UAS of other traffic
- Continually track the UA position and monitor communications from GA-ASI.
- Alert other sectors in the event of emergency
- Declare an emergency if one exists.
- Provide separation service to ensure the UAS does not enter uncontrolled airspace.

The controls, feedback, and communication links between each controller are represented with a solid, numbered links. Dashed links indicate a control or feedback that was largely absent at the time of the accident. A description of the intended control mechanism, feedback, or communication link is described below.

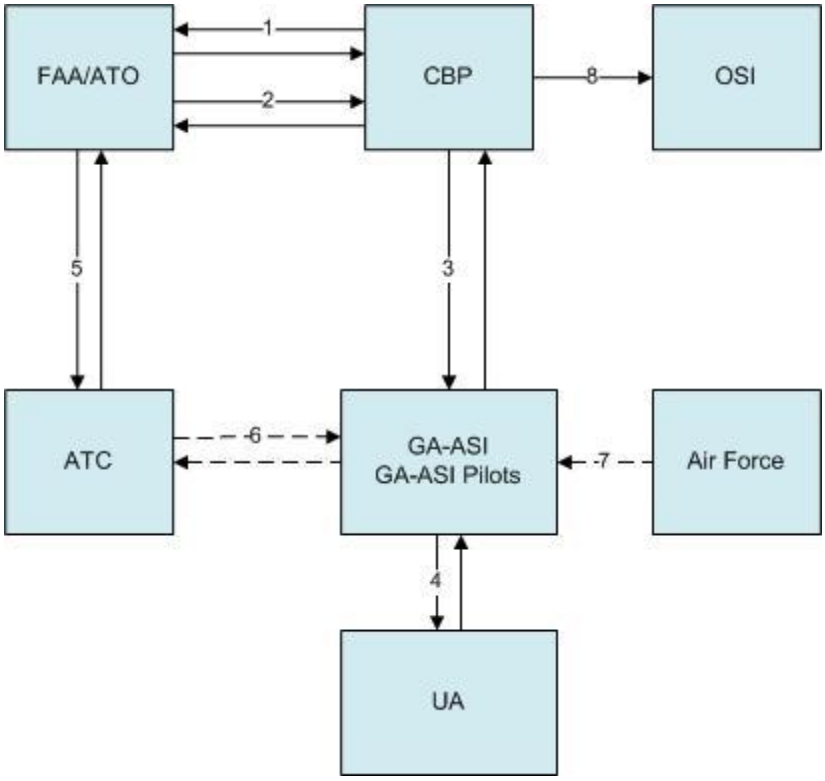

Figure 26 UAS Control Structure at the Time of the Accident

Controls, Feedback and Communication

1. CBP → FAA

Controls: COA application

Control Actions: The CBP may request a COA for operation of a public use UAS in the NAS. The CBP provides all of the information required by the COA to the FAA, such as:

a. Description of proposed flights
b. Maintenance program description

Feedback: In response to the CBP request, the FAA may approve, reject, or work with the CBP to modify the application.

2. FAA → CBP

Controls: COA Application

Control Actions: The FAA may approve, reject, or work with the CBP to modify the application. The FAA may request further safety studies from the CBP.

Feedback: The CBP will provide reports to the FAA that say that safety studies have been performed. When the FAA approves a COA the CBP notifies that FAA of all UAS-related activities.

3. CBP → GA/ASI, GA/ASI pilots

Controls: UAS contract bidding Process, Pilot Approval Process

Control Actions: The CBP sets the requirements for the UAS system and selects the contractor that will build and operate the UAS. When the UAS is operating, the CBP may approve or reject GA-ASI pilots to operate the UAS.

Feedback: CBP officers assess the safety of the GA-ASI operation of the UAS via insitu observations of the UAS system in the GCS.

4. GA-ASI, GA-ASI pilots→ UA

Controls: Typical Pilot controls (Throttle, Position), Payload Controls (Camera Aperture) via Workstation in the GCS, via Iridium Satellite

Control Actions: Selects waypoints for UA flight path, Uploads Lostlink profile, Controls UA throttle, Controls UA camera aperture

Feedback: UA status (e.g. UA altitude and velocity) is updated through displays in the GCS through a Line of Sight (LOS) datalink.

Note: Iridium satellite could not be used as backup datalink system due to design flaws in the UAS.

5. FAA → ATC

   Controls: Budgetary Controls, Sets Requirements for ATC Duties and training.

   Control Actions: Delivers information about UAS missions (e.g. flightplans, equipage) to ATC.

   Feedback: ATC briefs FAA regarding UAS missions.

6. ATC → GA-ASI, GA-ASI Pilots

   Controls: ATC clearance

   Control Actions: ATC directs GA-ASI as to what airspace at which time is available for UAS missions. ATC can also direct the GA-ASI to cease operations.

   Feedback: ATC cannot directly monitor the UA position, however they are given status updates (including lost link profile and call number) from GA-ASI and should be notified in an emergency if the UA must fly outside the prescribed airspace. Also, the GA-ASI reports any loss of contact to the ATC.

7. Air Force → GA-ASI, GA-ASI Pilots

   Controls: Pilot training process

   Control Actions: The Air Force GFR approves the training record of GA-ASI pilots. There were no Air Force personnel hired by the CBP to implement this control.

8. CBP→ OSI

   Controls: Contract process

   Control Actions: CBP directs OSI to provide Lost Link profile

The following chapter will describe the importance of social context and how it leads to inadequate control actions. Then, in Chapter 6 the method for exploring human and organizational context to understand why accidents occur and how the system can be improved is demonstrated using examples from the Nogales accident.

[Page intentionally left blank]

CHAPTER 5 CONTEXTUAL ANALYSIS: GUIDEWORDS

5.1 Chapter Overview

Knowing the control requirements for both individuals and organizations is not enough to discover *how* and *why* they might be violated. Engineers must examine the context surrounding human decisions and actions. This chapter starts with an explanation for using contextual analysis as the driver for accident analysis and hazard analysis of socio-technical system. Next, a set of *guidewords* are introduced that can be used to explore, discover, and analyze relevant system context and causal factors that can lead to inadequate control. These guidewords will be used in accident analysis and hazard analysis methods presented later in this dissertation.

5.2 A Context-based Approach

In accident analysis, the situation an individual was in when they made a decision that was later found to contribute to an accident often contains the key for re-designing the system and understanding *why* the accident happened rather than just *how* the accident occurred. The human context of an existing system may also be prospectively analyzed with a hazard analysis to find potential causal factors that can lead to inadequate control. For example, a hazard analysis can unearth inadequately designed procedures or an ineffective company safety policy. It is standard to include the environment in the analysis of a technical system; for a socio-technical system, at the organization level, the environment includes pay policies and at the organization-level, the environment includes union rules and safety management authority. Furthermore, the contextual analysis of an organization can include HR policies, contracting bidding practices, and the nationality of its workforce.

The choice to create a context-based approach for a human and organization hazard analysis was inspired by the work of skilled accident analyzers. High quality accident investigations do more than identify inadequate control actions made by the operator. The writers of these reports go beyond blame of individuals and organizations, and analyze the *context* in which decisions and actions were made. Analysis of the context points engineers to flaws in the system that can be changed to prevent future accidents. Furthermore, system changes can prevent entire classes of accidents from occurring, rather than just the reoccurrence of the accident under investigation [5].

In STAMP-based accident analyses, engineers analyze the context in which humans were operating and making decisions in order to understand why the accident occurred and how it can be prevented in the

future. STAMP-based accident analysis never stops with "operator error;" engineers performing STAMP analyze the operator's context to understand why it made sense for the operator to act as they did. This allows engineers to avoid blame and hindsight bias and discover flaws in the system that can actually be changed and fixed. Trying to eliminate operator error with platitudes or more training when training is not relevant to the accident is not effective. It follows then that a hazard analysis method must anticipate flaws in the manager's and operator's context that can lead to "errors".

Context is a key factor influencing safety. In a surprising example, Reason found that in some potentially dangerous systems, controllers performing in a maintenance-related context had more severe problems than when performing under nominal or *emergency* conditions. Reason has noted that in potentially dangerous systems, maintenance-related operations lead to larger human factors problems than control under normal conditions or control under emergency conditions [124]. Several contextual factors contribute to make maintenance tasks so risky: 1) risk tolerances may be high because maintenance is not an emergency procedure; 2) maintenance does not deliver a useful product to stakeholders, and so is subject to time pressures to complete quickly or the opposite, lack of emphasis on performing timely maintenance; 3) regulations often do not require or mandate the high levels of training for maintenance technicians that is required for nominal operators; and 4) maintenance technicians are not trained in control hand-off procedures. Much more effort is spend on certifying personnel, developing cogent procedures and designing man-machine interfaces in the case of nominal and emergency operations. The challenge for the hazard analysis is to draw attention to contextual factors that can lead to inadequate control.

5.3 Guidewords Approach to Analysis of Human and Organizational Factors

While accident investigators and safety professionals know that decision-making context (provided for in the system design) is important, understanding which contextual factors are relevant, or how to explicitly link context to human actions and decisions, remains vague. The approach presented in this thesis tackles each of these uncertainties. We address the latter concern by identifying the requirements that humans and organizations have for adequate control of a system. These "requirements for control" are subsequently fleshed out to form a typology of causal factors that violate the requirements for control. The human and organizational causal factors include the decision-making context and control environment that cause inadequate control actions. For the former concern, a set of guidewords has been developed to identify context that can lead to hazards.

5.3.1 Guidewords

A review of accident reports brought to light several themes among the contextual factors influencing human and organizational decision-making. From these reports, nine factors were distilled that can be used to drive the analysis of the system design and decision-making context to find the flaws leading to inadequate control as described in the human and organizational causal factor error taxonomy.

The guidewords were selected by using a grounded theory qualitative research approach [170] [171] using accident reports and analyses for data. The accident reports and accident analyses were drawn from the fields of aviation, energy, manufacturing, and medicine. Since the purpose of the guidewords is to find the context that leads to inadequate control actions that cause hazards, the first step was to highlight all of the inadequate control actions by both individual controllers and organizations. This process involved creating control structures, safety constraints and responsibilities for each controller in the system for each accident studied.

The next step was to identify the context (the system design) that explained, permitted, or encouraged each inadequate control action for each controller in the control structure (i.e. the reasons *why* the inadequate control occurred). Then the key words or phrases in the human and organization context were highlighted and grouped into categories. Finally, these categories were distilled to identify essential guidewords. The process of contextual factor distillation was finished as each category reached theoretical saturation [170] [171].

Confidence was gained that the set of guidewords were sufficient for identify relevant context by applying them to the analysis of new accidents. No new guidewords were needed, and each guideword was used, giving confidence that the set of guidewords identified had reached theoretical saturation as a whole, and that the set spanned the set of contextual factors that may contribute to inadequate control.

The following guidewords were chosen to be applicable to all human-centered systems and do not rely on a particular domain. In contrast, HFACS [15], which attempts to analyze human and organizational factors was created with the aviation domain in mind (e.g. from the HFACS tables: "Inadvertent use of flight controls") and does not readily apply to factors that are not part of that domain[14]. In addition,

[14] Modifications to HFACS have been developed for other domains (e.g. HFACS-ME [131]).

HAZOP [28] uses guidewords to discover inadequate control actions, but not the causal factors that contribute to them. The guidewords are shown in Table 8.

Table 8 Causal Factor Guidewords

History: Experiences, Education, Cultural Norms, Behavior patterns	**Pressures:** Time, Schedule, Resource, Production, Incentives, Compensation, Political
Resources: Staff, Finances, Time	**Safety Culture:** Values, Expectations, Incident reporting, Work-arounds, Safety Management
Tools and Interface: Risk Assessments, Checklists, Human-machine interface, displays	**Communication:** Language, Procedures, Data, Need to know Information
Training	**Human Physiology** Intoxication, Sleep deprivation,
Human Cognition Characteristics: Person-task compatibility, Risk Tolerance, Control-role	

History

The *History* guideword encourages safety engineers to consider how the historical context of a controller or organization may impact their ability to maintain the requirements for control. *History* can include any part of the makeup of a controller or organization that is informed by his or her past experiences, education path, or culturally imposed norms. *History* can also refer to a controller's pattern of behavior.

Pressures

The *Pressures* guideword is intended to lead engineers to examine how contextual pressures may impact the ability of a controller or organization to maintain the requirements for control. *Pressures* can include any positive or negative force that can influence a controller or organization, including time, schedule, political, resource or production pressure, incentives, or compensation.

Resources

The *Resources* guideword encourages safety engineers to consider how the availability of resources to a controller or organization may impact their ability to maintain the requirements for control. *Resources* can include staff, financial, and time resources.

Safety Culture

The *Safety Culture* guideword leads engineers to examine how the safety culture may impact the ability of a controller or organization to maintain the requirements for control. A safety culture is something that

an organization has that can be influenced (even engineered) by changing the processes and procedures of the organization. *Safety culture* can include how individuals *view* the organization's incident reporting and safety management processes and whether or not work arounds are tolerated. Discovering safety culture issues may involve interviews with individuals and are not likely to be solely ensconced in a company vision statement.

Tools and Interface

The *Tools* guideword encourages safety engineers to consider how the quality, availability, design and accuracy of tools to a controller or organization may impact their ability to maintain the requirements for control. *Tools* can include risk assessments, checklists and instruments.

The *Interface* guideword encourages safety engineers to consider how the design of man-machine interfaces may impact the controller's or organization's ability to maintain the requirements for control. A thorough discussion of the design of displays from a human factors point of view can be found in [157]. Important interfaces to consider when using this guideword include any displays, control levers, or tools used by controllers.

Communication

The *Communication* guideword leads engineers to determine how communication techniques, form or styles may impact the ability of a controller or organization to maintain the requirements for control. Engineers should consider how to get the right information to the right people in a way they can understand. The *Communication* guideword should also encourage the analysis of the control task to ensure that all data and needed information is communicated adequately. *Communication* can include language of communication, procedures, data, and needed information.

Training

The *Training* guideword encourages safety engineers to consider how the quality, frequency, availability and design of training protocols for a controller or organization may impact their ability to maintain the requirements for control. The *training* guideword is intended to focus engineers on training for the job processes, rather than the operator's entire educational experience (which is covered under the *history* guideword). *Training* can include on the job training, formal training, and informal training.

Human Cognition Characteristics

The *Human Cognition Characteristics* guideword encourages safety engineers to consider the suitability of various system aspects for human use or consumption from a cognitive point of view. Many aspects of a controller's personality, such as risk tolerance, can influence safety. Furthermore, the innate limitations

of human beings make them, in general, unsuitable for use as monitors or controllers of high-order systems. Engineers should use the guideword to consider the impact of risk tolerance, monitoring, and high-order control.

Human Physiology

The *Human Physiology* guideword encourages safety engineers to consider the suitability of various system aspects for human use or consumption from a physiological point of view. Humans have several constraints or limitations that must be considered, including sleep requirements and ergonomic constraints. Engineers should use the guideword to consider the impact of aspects of human physiology, such as sleep deprivation and intoxication, on safety.

The guidewords themselves are not intended to be mutually exclusive. For example, some might consider a 'tool' a 'resource' and visa versa. The guidewords selected were intended to be helpful and practical for teasing out the relevant context and human and organizational design flaws that can lead to hazards. In the next chapter, the guidewords will be used to drive the accident analysis of a recent aerospace accident.

CHAPTER 6 EXAMPLE OF GUIDEWORDS APPROACH APPLIED TO ACCIDENT ANALYSIS

6.1 Chapter Overview

This chapter demonstrates the use of SHOW as an accident analysis method. By applying SHOW to an accident that has already occurred, we focus our analysis those aspects of the design that contributed to the loss rather than analyzing the entire design.

6.2 Who Should Perform Accident Analysis

Accident analysis can be enhanced when performed by diverse teams, according to a study of root cause analysis by Carroll in chemical plant safety [67]. Analysis teams can be composed of internal and external technical experts, nontechnical employees, and individuals from all levels of the organizational hierarchy [67] [43]. By creating diverse teams, upper management communicates to the rest of the organization that "no one person or group knows everything," [67] and that different viewpoints are necessary to understand the system and foster safety. Any method—including accident analysis—that seeks to gather expert opinion must be staffed with individuals that are able to understand factors related to any of the wide-ranging fields related to the design and operation of a socio-technical system. A team that includes experts in human factors and organizational theory as well as safety engineers is better able to incorporate domain-specific information and form a comprehensive understanding of the accident than a less diverse team of experts.

6.3 How to perform Guideword-based Accident Analysis

Guideword-based accident analysis SHOW is an iterative three-phase process. The safety engineer begins by analyzing each element (controller) in the control structure, and then broadens the analysis to the control structure as a whole. Each element in the control structure can represent an actual individual or an entire organization. The FAA, for example, is an organization, but is represented by one element in the Nogales control structure of Figure 26. In the first stage of the analysis, each element of the control structure is analyzed as an individual. In the next phase, each element is examined as an organization in and of itself. Finally, analysis is conducted on the entire socio-technical system shown in the control structure as a whole (as an organization).

6.3.1 Individual Analysis of Control Element

The analysis of an individual controller includes identification of inadequate control actions made by the controller, analysis of the control loop elements and the functioning of the control loop as a whole, and most importantly, the reasons for the inadequate control. As shown in the human error taxonomy on page 107, inadequate control can happen at the individual controller level for a variety of reasons (taxonomy items 1-6), including inadequate controls available to the controller (e.g. the COA application process used in the Nogales accident), an inadequate control algorithm, an inadequately *implemented* control algorithm (e.g. the pilot-in-command's actions during the UA flight), and so on.

Inadequate control actions are identified using high-level accident analysis that includes the responsibilities and safety constraints. In Chapter 4, an overview of the Nogales accident was given along with the responsibilities and control structure of the system at the time of the accident. ICAs can be found by comparing the controller's requirements with their actions. The actions and decisions of each controller are the embodiment (or the *implementation*) of their control algorithm.

The analysis of ICAs can include relevant control or process inputs. In other words, if the ICA is in response to the absence of a needed input or in response to a particular stimulus, such as a control input, the stimulus should also be recorded. The purpose of listing the ICAs is to move onto finding the contextual factors that contributed to the inadequate control.

An example ICA from the Nogales accident is shown below. In this example, the violated constraint or relevant responsibility is also included.

ICA1: The FAA issued a COA to the CBP for UAS flight in the NAS.

- Granted Airworthiness waiver to CBP.
- Allowed CBP to self-certify UAS.
- Issued COA for regions outside of LOS communications.

Responsibilities and constraints violated by the FAA ICA1:

Ensure the Safety of the NAS

Ensure that the UA can safely fly in the NAS.

As a matter of theoretical interest, we can identify the *control requirements* (Table 6 and Table 7) that were violated. This step is not intended to be performed by practitioners. While every inadequate control

action is due to a violated control requirement, in a social system, it is impossible to classify each inadequate control action according to which control requirement was violated—we cannot read minds. It is not always possible to discern from evidence if an incorrect process model with a correct control algorithm or a correct process model with an incorrect control algorithm caused an operator's inadequate control action—nor does it contribute to an understanding of *why* the ICA occurred. However it is important to show how SHOW theory (control requirements for individuals and organizations) links to how inadequate control actions occur in practice. Therefore, an example is included next.

Unmet Control Requirements for the FAA that led to ICA1:

Adequate Model of the Controlled Process

Adequate Control Algorithm

Adequate Assignment of Control Authority

Adequate Interaction with External Bodies and Stakeholders

Adequate Safety Management and Learning Processes

The next step after the inadequate control actions have been identified is to examine the controls. For an individual controller, the controls implemented between it and lower-level controllers must be examined. For social systems, the purpose of one controller may be to direct (or control) the actions of lower-level controllers. In the Nogales accident, one of the responsibilities of the FAA was to determine if the CBP could be permitted to fly UA in the NAS. Hazards can occur if the implemented controls, even perfectly applied, are not sufficient to enforce safety constraints.

An analysis of the control loop as a whole is also helpful for identifying causal factors related to the inadequate control. If process inputs or key information is absent, even a perfectly executed control action can result in inadequate control. Analysis of the control loop to identify causal factors can be informed by the human error taxonomy (listed on page 107) and depicted in Figure 22.

Lastly, a guideword analysis (using the guidewords found in Table 8) of the context that contributed to the ICAs is conducted to find causal factors. The purpose of the contextual analysis is to discover why the ICAs occurred so that they can be prevented in the future.

An example of this process applied to the FAA control element is shown next. For clarity, only one element in the control structure will be analyzed in this section. A full analysis of the Nogales accident can be found in Appendix 1.

Nogales - FAA Analysis: as an Individual Controller

Process Being Controlled by the FAA: Determining whether public use agencies may access the NAS.

Control Input: Request from CBP to waive airworthiness requirement when issuing COA.

Result: Unsafe UAS was approved.

Controls implemented between FAA and CBP: COA

The COA application and approval process is an important control that the FAA has for assuring the safety of the NAS. The intent of the COA is two-fold: to assure the safety of the UAS and to assure ATC is fully informed regarding UAS missions and will be able to fulfill their own responsibilities (separate air traffic from regions used by the UA). Unfortunately, the COA control at the time of this accident had several weaknesses. The COA lacked specific requirements detailing UAS safety and risk assessments. The COA also lacked provisions for applicants to supply evidence that the UAS was safe. Supplemental material in the COA was limited to proposed flight plans.

ICA1: Issued a COA to the CBP for UAS flight in the NAS.

- Granted Airworthiness waiver to CBP.
- Allowed CBP to self-certify UAS.
- Issued COA for regions outside of LOS communications.

ICA2: Did not ensure that ATC had sufficient understanding of the UAS operations within the NAS.

Sensor/Actuator Operation: Normal
Process Inputs: Normal
Coordination with other Controllers: Normal

Guideword based Causal Factor Analysis

History:

CBP had operated the predator without accidents several times already on the same route. This may have contributed to the belief that the CBP was operating a safe UAS.

Pressures:

FAA felt great political pressure to approve the UAS mission for national security.

FAA was under time pressure to complete the COA approval in an expedient fashion in the interest of national security.

Resources:

FAA did not have the resources to certify the UAS. The FAA lacked in-house expertise that would enable them to assess the safety of the UAS. The FAA also did not have resources to assess whether CBP was able to safely operate the UAS.

FAA may not have had access flight plan information for the UA to the level that it would for a civil aircraft due to classified information transfer.

Safety Culture:

Reports [129] have indicated that the FAA is in need of improvement. However, without greater regulatory authority over public use agencies, even a strong safety culture is not enough to ensure the safety of the NAS.

Tools:

COA application approval process does not include a risk assessment. Public use missions are allowed to operate without assessments of the risks. The COA application focuses on operations.

FAA has inadequate risk assessment tools to analyze the risk of UAS operations in the NAS. Tools are quantitative, rather than systemic.

Communication:

CBP missions are classified, and open communication may have been hindered between the FAA and CBP.

Safety-related information about prior problems with the UAS were not reported to the FAA

Training:

The FAA did not assure adequate training of ATC in UAS operations. It is unclear what authority the FAA had to require CBP to provide enough information to ATC so that ATC could provide adequate tracking and separation service.

Interface:

The COA application may have not have provided enough detail for evidence that the UAS was safe; for example it did not provide information about the lost link profile, pilot training, pilot

operation policies, UA maintenance policies, etc. A more rigorous COA application process may have unearthed problems with CBP UAS operations in the NAS.

6.3.2 Organizational Analysis of Control Element

The FAA can also be analyzed as an organization. The purpose of the organizational analysis is to find causal factors that contributed to the inadequate control actions identified previously. Examination of the FAA as an organization can also lead to identifying flawed organizational policies, processes and decisions. The organizational error taxonomy on page 109 can be used to find organizational errors and causal factors.

For example, item 4 should lead engineers to examine the communication protocols and policies in place at the FAA and possibly identify problems with information flow that affect decision-making within the FAA. The causal factors surrounding organizational flaws can be aided by using the guidewords. Item 4 in combination with the guideword 'resources' would encourage analysis that looks for evidence of resource shortages affecting communication abilities.

Nogales – FAA Analysis: as an Organization

The NTSB report did not include much evidence of organizational problems, so further investigation is needed to delve into the organizational causal factors for the inadequate control actions identified above. Using the taxonomy and guidewords, one area that could be further investigated is the intra-FAA communication issues that led to ATC's insufficient understanding of the UAS mission in the NAS.

The NTSB report does have sufficient detail for exploring taxonomy item 1. The FAA was not able to give the COA evaluation team enough control authority over the public agencies so that they could acquire enough information to have sufficient understanding of the UAS safety. The relationship between the FAA and the public use agencies does not support safe decision-making within the FAA. The tools available to the FAA to exert influence over the public use agencies were too slim: the COA application did not ask applicants to provide sufficient evidence of UAS safety.

The FAA was probably aware of their lack of control authority over the public use agencies and the inadequacy of the COA application process, but was hindered by the powers granted to them by higher levels of government. Their ability to move public opinion or Congress to grant them greater regulatory

authority over public use agencies in support of NAS safety could be strengthened through public outreach and aerospace safety watchdog groups.

6.3.3 Organizational Analysis of Entire Control Structure

Analysis of the socio-technical system as a whole can be conducted as well by examining the control structure. The control structure can be used to identify and analyze the adequacy of the controls implemented by each controller.

In practice, the number of controls that are implemented by each element in the control structure can be too numerous to easily notate in a single control structure diagram. In such cases, a control structure showing each type of control can be made. For example, a control structure can be created that shows policy controls, another for hiring controls and another showing funding controls. The relationship between two controllers can be analyzed by taking into account all of the controls and feedbacks that exist between each controller as described next.

To determine if the controls implemented by each controller are adequate, engineers should:

1) Ensure that feedback regarding the executing controller's control actions exists.
2) Ensure that time delays are sufficiently brief. Feedback that relies on the state of a process controlled by a controller N levels into the hierarchy may be too slow to ensure the top-level controller has as an adequate process model. In some cases, a reorganization of controllers may be necessary to eliminate dangerously long time delays.
3) Assess the strength of controls. Weak controls may be worse than no control at all, because weak controls can lead to a false sense of safety.

These three concepts are depicted the figures below.

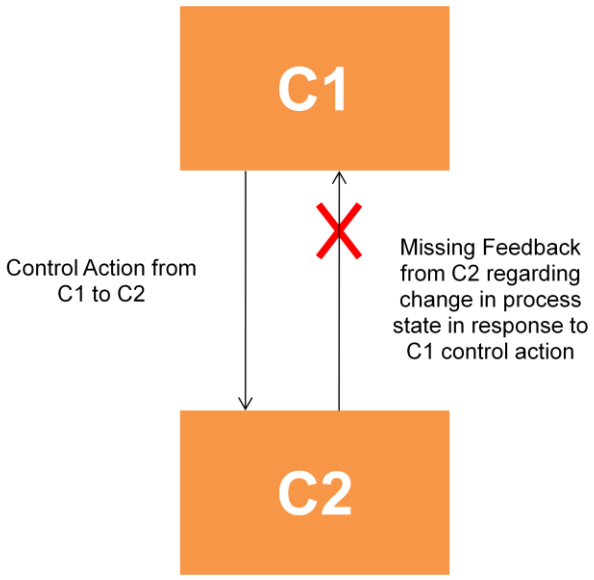

Figure 27 Missing Feedback

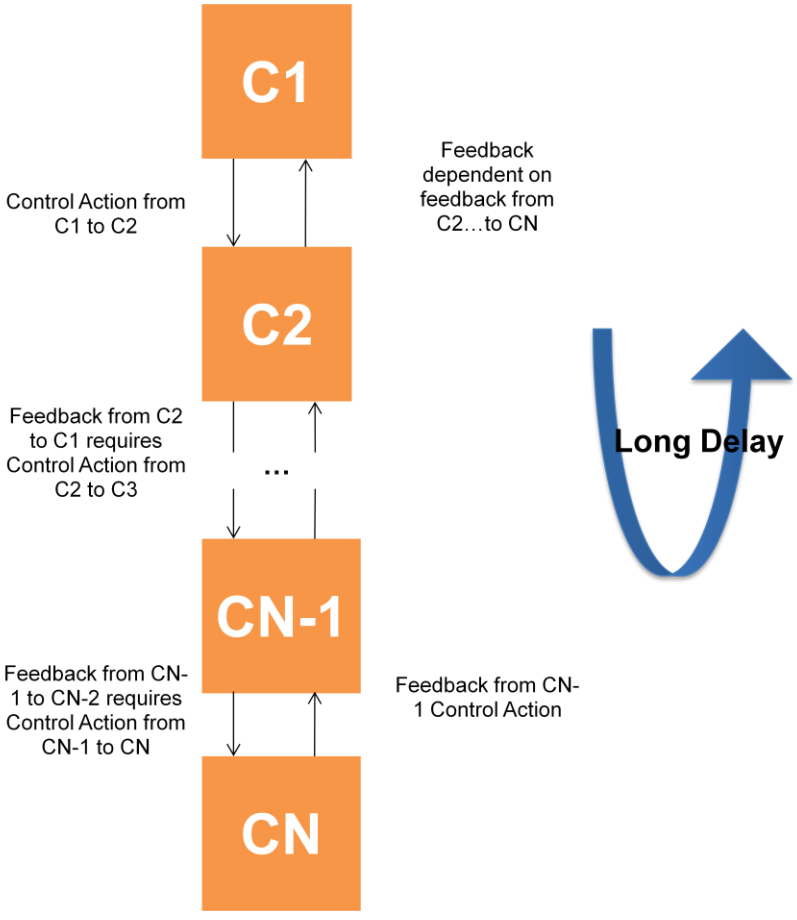

Figure 28 Long Feedback Delays

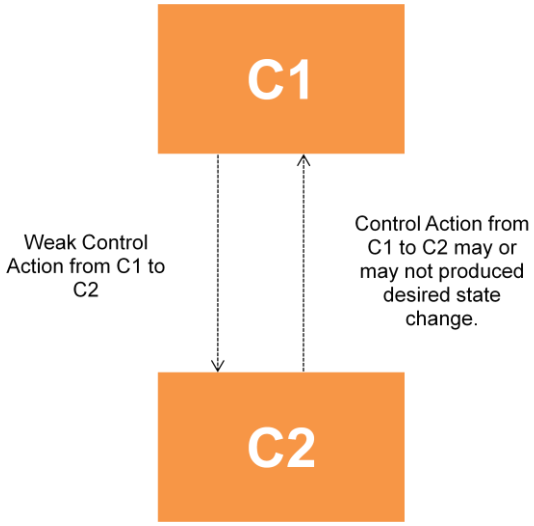

Figure 29 Weak Controls

More information on work in this area and other approaches can be found in Nicolas Dulac's thesis [158].

6.3.4 System Dynamics in Accident Analysis

System dynamics can be used to convey how context contributes to human and organizational decision-making graphically through causal loop diagrams (CLDs) and can be used to test the impact of various design changes on decision-making through executable models. System dynamics CLDs are particularly useful for understanding the dynamics underlying an accident while the executable models are best suited for testing new organizational designs (e.g. interventions, incentives, staffing number). Teaching system dynamics modeling to all accident analysts may not be practical, so in this section, we focus only on CLDs which are effective at demonstrating accident dynamics and are intuitive and easy to learn [63].

System dynamics causal loop diagrams are useful at each level of accident analysis: they can show the human factors (e.g. influences and pressures) surrounding individual controllers, the dynamics of each organization in the control structure, and inter-organization dynamics.

A CLD shown in Figure 30 was constructed for the FAA element from the Nogales accident. This CLD is able to succinctly represent the textual causal analysis. The CLD does not have enough detail to stand alone, but serves to synthesize the analysis conducted so far. The 'Resources' factor affecting the 'Ability to Ensure Safe UAS' in this case includes resources such as expertise and staff. Creating causal loop diagrams using the guidewords and interviews can be an efficient way of gathering data to gain

understanding of a system. More about the use of CLD and STAMP can be found in Dulac's dissertation [158].

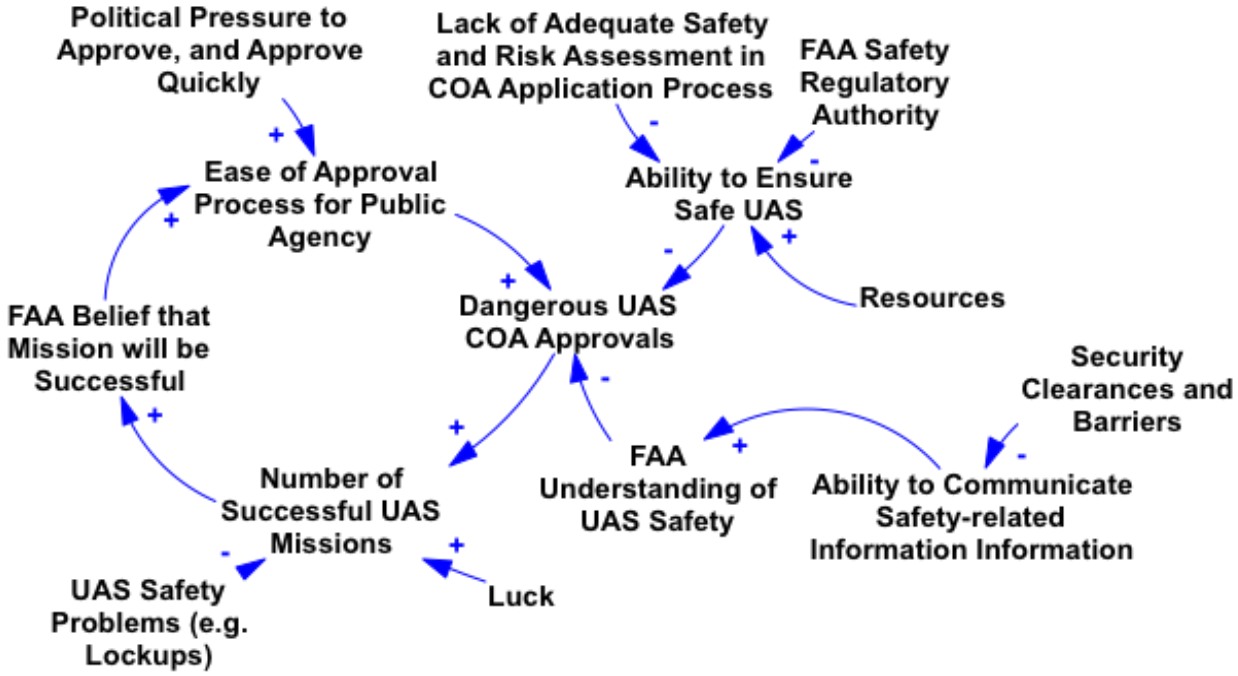

Figure 30 Nogales - FAA Causal Loop Diagram

CLDs may be created by simply translating the analysis earlier in this chapter into causal loop diagrams. Diagrams created in this way are useful for two reasons, 1) by synthesizing analysis on one "sheet of paper," omissions or errors are easy to see, [158] and 2) the analysis can be shared with domain experts to incorporate their expert feedback, [158] which may gain further understanding of casual factors that led to inadequate control actions. Experts may participate more when graphical CLDs that may be consumed and understood quickly are available, instead of or in addition to pages of text. . Any relationship represented by an arrow may be shared by jumping to the relevant textual analysis.

Another approach to the accident analysis process is to create the CLDs to explain inadequate control actions directly by applying the guidewords to explore causal factors. After each element in the control structure has been developed, and the ICAs for each controller have been identified, the guidewords can be applied to find causal factors. For example, in the Nogales accident, the ICA regarding the approval of an unsafe UAS COA can be explored by applying the resources guideword to discover whether a lack of resources impacted the approval process. Causal factors that influence the dynamics of a system or controller can be identified by applying the guidewords to construct the CLD. Starting from a core loop or factor, use a guideword (e.g. 'pressure') to discover causal factors that drive system behavior.

Experienced system dynamics practitioners have also discovered SD Safety archetypes present in several accidents, and these in turn have been used to create CLDs to understand complex system[65]. A deep dive into system dynamics applied to human and organizational systems will be discussed in Chapter 8.

6.3.5 Iteration and Stopping Criteria for SHOW

The accident analysis can continue iteratively, controller by controller, using control loop analysis and organizational analysis until all inadequate control actions have been explained.

The stopping criteria for SHOW are left to engineering judgment. The number of inadequate control actions analyzed can be vast. Engineers must consider ICAs made by operators, groups throughout the organizational hierarchy, and external bodies. The sheer number of connections and control relationships that comprise a complex system might suggest that engineers would be required to struggle with a massive web of contextual analysis that seems to include everyone (each controller that impacts the complex system) throughout time (from the earliest design stages through operations). However, in practice, this is not the case. The analysis starts with the controlled process and then includes those components (working upward through the control structure) needed to explain the flaws found. Engineering judgment is used to decide what level of detail is required for inadequate control explanation.

The flexibility of SHOW potentially leaves the method open to hindsight bias and convenient stopping points. However, flexibility also allows skilled engineers to explore what they find relevant and ultimately generate comprehensive and grounded analysis of system faults. SHOW errs on the side of openness and thoroughness.

In some cases, engineers using SHOW may be analyzing an accident that has previously been analyzed by the NTSB or other organization. Because the NTSB and other organizations use methods that are unsuited to human and organizational factors, engineers may wish to derive more insight by applying SHOW to a previously analyzed accident. The accident analysis method presented in this thesis can be used to uncover contextual factors that contributed to an accident that was already analyzed according to conventional methods, or it can be used to analyze an accident that has only been investigated.

6.3.6 Recommendations:

After highlighting the flaws in the operational context that contributed to inadequate control actions, an accident analysis must give recommendations to prevent future accidents from occurring. With the broad

accident analysis method demonstrated here, the recommendations are not narrowly confined to preventing the same kind of accidents, but should address all hazards discovered during the analysis process.

Nogales Recommendations

1. There are many ways to address the inadequacies of the relationship between the FAA and public use agencies such as the CBP. The underlying issue is that the FAA has the responsibility for maintaining the safety of the NAS, but does not have the ability to ensure that UAS operations do not violate the safety of the NAS. The FAA does not possess regulatory authority over the public use agencies, and the COA process is inadequate. While the FAA may require that public use agencies perform a safety assessment, they are not privy to the details of the safety assessment, and must trust that safety assessments conducted are comprehensive. The FAA does not have the same auditing authority over public use agencies that it does over commercial aircraft manufactures or airlines.

   Interestingly, the asymmetry between the FAA's responsibility for maintaining the safety of the NAS and their inability to regulate public use agencies has always existed and heretofore the overall safety of the NAS has not suffered. However, before the development of UASs, the public agencies were in the same business as commercial manufactures and airlines: they built and operated safe human-piloted aircraft. The safety standards, cultural values, and design processes used by public agencies were on par with those used by commercial ventures. The engineers that designed fighter jets came from the same educational background and often worked at the same companies as the engineers that designed commercial aircraft.

   With the introduction of unmanned aircraft to the NAS, that may change. The technical challenges of coordinating a remote pilot and air traffic control are astounding. There is no history of shared values with commercial manufacturers to support the development of safe UAS in the NAS. The FAA has always been an outsider in UAS use and does not have the vast technical expertise that the public agencies do with this new technology. Given the expertise gap and the communication roadblocks between the defense agencies and the FAA imposed by classified information requirements, it is hard to imagine how the FAA will be able to evaluate UAS safety in the NAS.

One potential solution is to enhance the ability of the FAA to fulfill their responsibility for protecting the NAS by bringing FAA personnel into the public agencies, including air traffic controllers and the FAA officials charged with the development of procedures and NAS regulations. With adequate clearances, these FAA officials could evaluate the safety of UAS in the NAS. If the FAA personnel are accepted by the public agency, they will be better able to assess safety, refine requirements and regulations, and evaluate whether the public use agencies have met safety requirements.

2. All agencies analyzed in this system, including the FAA, CBP and GA-ASI, should evaluate their safety assessment programs. None of the agencies have a safety management system capable of assessing both the technical and social aspects of the system, nor do they appear to have a practice of regular auditing and risk assessments of potential changes.

3. The airworthiness requirement must not be waived without a risk assessment. In times of crisis, it may be obvious that the air worthiness requirement should be waived so that UAS operations are possible, but in the absence of immediate crisis, it is not clear which missions could provide benefits to the public good that would outweigh safety risks to the NAS. A risk assessment should be conducted to evaluate potential risk tradeoffs surrounding UAS flight in the NAS by parties with an understanding of both the NAS (such as FAA safety professionals) and the public use agencies (such as cleared military intelligence professionals).

4. The CBP did not have the expertise to assess the safety of the GA-ASI manufactured and operated UAS. Although the CBP was the acting operator of the UAS and had the final authority for the safety of the UAS, it did not have the ability to carry out that responsibility. The CBP should establish a better safety management group (as described previously in this thesis) and consider integrating GA-ASI into their safety assessments.

5. The human interface design of the pilot and payload operator must be re-engineered with input from human factors professionals. Flaws in the design, particularly the lack of queuing for the pilot, indicate a problem not just with the display, but also with the design process as a whole.

6. The technical design of the UA system must be re-evaluated with a comprehensive hazard analysis. The design flaw that prevented backup communications with Iridium may not be the only one.

7. The policies for training pilots must be re-engineered. At minimum, requirements for training pilots on a system must specify which systems the pilots are permitted to fly. A simulator must be available to train pilots for both nominal and off-nominal situations. The program should specify how many hours of training are required for pilot certification. If an air force GFR is required to supervise pilot training that requirement must be clear and non-waiveable.

8. Safety professionals in both GA-ASI and CBP must audit the operating system for evidence of workarounds, so that they can understand why workarounds are occurring and propose permanent solutions. The NTSB report noted two such workarounds, the PPO-1 to PPO-2 switch, and the pilot training waivers, but there may be many more.

9. Policies for spare parts stocking and maintenance performance and procedures must be investigated. The UA must not be permitted to fly with damaged parts. If a restocking delay cannot be tolerated, then spare parts must be stored on site.

10. The unhealthy safety cultures of CBP and GA-ASI indicate serious problems within the organization. An investigation into both organizations, and the relationship between the two, should be conducted. The inadequate maintenance performed on the UAS, the lack of importance placed on maintaining a spare parts supply on site, and the abundant evidence of operational workarounds (e.g. the PPO-1-PPO-2 switch, and waived pilot training requirements) are evidence of organizational dysfunction. Without an investigation, one can only speculate as to what solutions could solve these problems. For example, the GA-ASI may have been under great time and financial pressure to deliver the completed system, and was not able to do so without cutting corners. Likewise, the CBP could have been under political pressure to get the system up and running without adequate time to understand the GA-ASI system.

11. The contracting system for the development of the UAS and the operational relationship between the CBP and GA-ASI must be investigated. Since CBP has final authority for the safety of the UAS, they need more insight and understanding into the system. Using a DER system might help assure the safety of the GA-ASI system.

12. The ATC needs to better monitor UA aircraft. UA positions must be known at all times. This could be accomplished through better electronic tracking and alerting systems. If the ATC loses track of a UA, an automatic emergency alert must be initiated.

6.4 Summary of Accident Analysis

The human and organizational factors accident analysis method described above uses taxonomy and guidewords to elicit the contextual factors that were the mechanisms for the inadequate control actions.

[Page intentionally left blank]

CHAPTER 7 COMPARISON OF SHOW TO OTHER ACCIDENT ANALYSIS METHODS

7.1 Chapter Overview

This section will discuss and compare three accident analysis techniques, HFACS, ECF and AcciMap to SHOW. The reader can recall that a description and brief discussion of the limitations of the current methods used today was given in section 2.6.

7.2 Dimensions for Accident Analysis Comparison

Similar to Marais' finding in her assessment of risk assessment, little has been written in the literature regarding the criterion for an assessment of accident analysis. Using Marais' criterion for risk assessment [76] (which were informed by work by Fischoff [160] and Haimes [161]) as a starting point, this author has taken into account the criticisms of safety engineering techniques discussed in Chapter 2 and developed the following dimensions for comparing SHOW to state-of-the-art accident analysis methods for human and organizational factors:

Theoretical Basis: Events vs. Control
Comprehensiveness
Ease of Use: Form and Application
Resources Required
Learnability
Consistency
Facilitates the Creation of Recommendations for Re-engineering the System
Domain Independence

Theoretical Basis: Events vs. Control. The theoretical foundation of an accident analysis method has considerable impact on the accident analysis process, including which system design flaws its users will discover, and what recommendations its users will generate.

Comprehensiveness. Accident analysis methods should be comprehensive. Before diving into critique with this dimension, first let's see how others have approached this hard-to-empirically-measure dimension:

Naïve approaches to accident analysis method comparisons have taken the following approach: A non-partial panel creates a list of *every* factor they think contributed to an accident in a complex system and then use quantitative assessment to compare the percentage of factors captured the method [77].

The above assessment technique is unsatisfying for two reasons:

1. There is no consistency of assumptions across accident analysis methods regarding what constitutes a contributing factor to an accident. Without consistency, a quantitative comparison that assesses the number of factors identified by each method is not possible. A 'master list' of causal factors may include factors that are defined at a broader or finer level of abstraction than defined by each method under comparison. Factors identified by the methods that contain abstract categorizations could potentially capture several detailed factors, while other methods with greater resolution might capture several detailed factors precisely, but miss others. A 'master list' of factors would inevitably embed biases.

2. Every accident analysis method will have different assumptions regarding which factors are the most important to analyze. Important factors may receive a high degree of analysis, and other factors considered tangential will receive superficial analysis. Nonetheless, in a quantitative, binary counting approach, these differences will not matter. Without a consistent notion of which factors should be included, or to what level of detail they should be analyzed, a quantitative comparison is meaningless.

A variety of assumptions regarding the relevance of contributing factors makes direct completeness comparisons between methods challenging. Others have suggested comparing the recommendations generated by each accident analysis method. However, this solution suffers the same flaws as comparing a list of factors: inconsistent assumptions.

Rather than measuring 'completeness', the comprehensiveness of methods can be compared by reviewing the method to assess its scope, the kinds of factors included in the analysis, and the level of abstraction used in the analysis. In particular, the method's suitability for organizational factors and interactions is critical. Accident analysis methods can be differentiated based on their suitability for 1) identification of inadequate control actions made by organizations and 2) explaining inadequate control actions executed by any element in the control structure using organizational causal factors.

Methods that are not suitable for finding organization-level ICAs will only find human errors—which may only be symptoms of organization-level ICAs. Recommendations generated using an analysis

method that is not suitable for organizational factors may not identify system-level changes to prevent organization ICAs from reoccurring. In essence, engineers may not be able to learn from the accident and prevent future mishaps.

Resources Required: Several kinds of resources are relevant to accident analysis, including expertise required, time required and size of team required. Any accident analysis method is merely a framework for organizing expert opinion, but the amount of skill required of the safety engineer is a matter of interest. The amount of work devoted to each analysis may be limited by practical concerns such as budget, schedule, or the need to quickly respond to recommendations. A quick turnaround time for accident analysis provides more time to re-engineer the system to improve safety and minimize risk to stakeholders. However, using a quick method that does not lead to a full understanding of why the accident occurred may lead to insufficient "fixes" that obscure problems and lead to future disasters.

As an example, it is helpful to illustrate how two leading national safety investigators conduct their accident investigations and analyses.

The NTSB structures their investigations in a hierarchical fashion where sub-teams composed of domain experts (e.g. avionics, structures, human factors) are deployed to perform detailed non-interacting investigation and analysis of particular sub-systems. In the fact-gathering phase of a major accident, the investigation team may compromise 70 people. Team leaders convene and review the detailed reports to generate a big picture of the accident and write up an accident analysis with recommendations. At this point the accident analysis is conducted by about 12 people [130]. The structure used by the NTSB allows them to move sequentially through the investigation process quickly—usually in about 3 weeks. The analysis phase may take several months and the complete accident report is usually released within a year after the accident [130].

The Dutch Safety Board, on the other hand, uses small teams (2-10 people) composed of a diverse set of experts for each accident. The small, diverse teams do detailed investigation work and conduct high-level analysis [62]. The Dutch Safety Board usually takes longer for their investigation and analysis process, and may require three years for a single accident report. Their process includes frequent revisiting of early data and questions throughout their process [62]. The process used by the Dutch Safety Board produces more comprehensive accident analyses than the NTSB, but may not be scalable to large teams or tight schedule deadlines.

The resources required by an accident analysis method and the degree to which analysis may be conducted by independent teams can determine its suitability for use by organizations that conduct holistic analyses or than those that wish to follow a linear analysis process.

Consistency: Consistency is the degree to which similar engineers are able to apply an analysis method to the same accident and classify salient factors.

Facilitates the Creation of Recommendations for Re-engineering the system. The ease with which recommendations are generated by the accident analysis is important. The accident analysis should identify factors that lead to solutions and recommendations, not merely restate human errors in fancier terms. The difficulty of measuring the power of an analysis method to generate recommendations does not diminish its importance.

Domain Independence: Some accident analysis methods can only be applied to the type of industry or process they were developed to analyze, and this limits their usefulness. Therefore, the domain independence of an accident analysis method is a key dimension. Methods that are applicable in a wide variety of domains may not have enough support for gathering expert opinion in a particular domain, while methods created for a particular domain may be impossible to extend to other contexts.

7.3 Comparison of ECF, HFACS, AcciMap and SHOW

In this section each dimension is used to logically compare SHOW, ECF, HFACS and AcciMap. Following each comparison, the argument is concretized with examples.

Theoretical Basis: Events vs. Control. The accident analysis model used by SHOW is Stamp and is centered on control, while ECF, HFACS and AcciMap use the Swiss Cheese model and are centered on events. The Swiss Cheese-based methods analyze events (unsafe acts), and then identify contributing factors to the events. SHOW analyzes ICAs, (aka inadequate decisions and actions) but it also analyzes inadequate *controls*. The underlying accident model means that a poor decision or action does not need to occur for SHOW to discover the flawed control. In the course of an accident analysis with SHOW, engineers are able to uncover inadequate controls that can give rise to any number of hazards (whether the hazard actually occurred or not) and address them through system redesign. Swiss-cheese based methods are only able to address events that actually occurred in the course of the accident.

Rather than using the HFACS classification scheme on every action identified in an event chain, an HFACS classification would be more comprehensive if it was applied to each inadequate control action in the STAMP control structure. Examination of each controller in the control structure would allow a more comprehensive view of organizational influences to be formed.

> Example: The accident analysis created with SHOW examines the organizational causal factors surrounding the poor communication between the FAA and ATC. While ATC's inadequate control of the airspace did not result in a mid-air collision, the mid-air collision hazard existed. Because the actions of ATC were not directly related to the UAS crash, this issue is not explored by the other accident analysis methods.

Comprehensiveness: Each of the methods is able to identify human errors, some organizational errors and capture at least some of the *whys* for each error. However, the Swiss cheese-based methods are not suited for organizational factors, and only cover a select number of why-factors.

SHOW uses augmented STPA with nine guidewords to analyze human and organizational context. While SHOW doesn't give provide a list of every possible factor that could influence human and organizational decision-making, it does provide a set of control requirements that if violated can result in inadequate control. The theoretical foundation of SHOW is complete, so application of the guidewords is not limited and can potentially include all relevant factors.

HFACS is based an ad hoc hierarchy derived from the Swiss Cheese model and uses 144 factors to analyze human errors. Without abstractions that span all possible contextual factors, HFACS compensates by listing a multitude of factors for each Swiss Cheese slice. However, without an engineering foundation, no level within the Swiss cheese can ever be complete. HFACS risks over-specifying the factors, which can curb creativity and cause analyzers to miss important factors simply because they were not "on the list."

Only SHOW is suitable for the identification and analysis of intra- and inter-organizational factors. The Swiss Cheese-based methods consider individual actions at its starting point, so interactions between groups and organizational decisions are often not included in the analysis. The method presented in this thesis includes the direct analysis of the interactions between organization-level controllers.

In particular, in SHOW, one of the requirements for control at the organizational level includes a consideration of the control authority of controllers within the organization. HFACS analysis only addresses this obliquely, through such factors as the *Organization Influences* → *Organizational Climate* → *Chain-of-command* factor, which must be related through the HFACS hierarchy *unsafe supervision, preconditions for an unsafe act* and finally an *unsafe act*. HFACS is much better at identification of relevant context for some types of individual actions.

ECF comprehensively examines factors related to human error, but only covers organizational factors in a superficial manner. ECF clumps organizational factors together in an indistinct cloud and doesn't analyze the intra-organizational factors. Furthermore, ECF does not include analysis of the *controls* available to each controller. Engineers that use ECF have a distinct advantage over those using HFACS. ECF does have a regimented list of factors like HFACS does, and analysis is not encouraged to stop after exploration of just a few levels. In particular, engineers may identify several organizational factors that are not available to practitioners of HFACS. With more freedom to analyze the accident, practitioners may also be able to recommend more comprehensive design changes.

AcciMap is comprehensive in that analysis is conducted at all levels of the system organizational hierarchy. However, the analysis at each level is superficial, and only includes factors linearly related to the loss. While HFACS, ECF and AcciMap can identify relevant context for many individual human actions, it lacks support for unearthing system flaws in human and organizational systems.

> Examples: In Carrigan's analysis [126], HFACS is used to identify the pilot's unsafe acts (inadequate control actions in Stamp parlance), and link the human error to the poor design of the control stick. No analysis or questions are asked of the CBP's budgeting processes that allowed such an inadequately control stick to be implemented. Furthermore the HFACS analysis did not include analysis of the ATC or the FAA's COA approval process. I argue that the reason for this is that HFACS does not point the analyst to the FAA and ATC because the accident was a crash of the UA and no midair collision occurred. HFACS helps identify inadequate control actions that occurred, and a few contextual factors, but without a complete model of accident causation, it misses important flaws.
>
> Chris Johnson and Christine Shea used the Events and Causal Factors (ECF) [126] method and diagrams to aid in his analysis of the Nogales accident in a paper presented at the System Safety Conference [128]. An excerpt from their analysis showing an organizational factors cloud is in

Figure 31. The ECF analysis does not explore reasons for the organizational culture of using work arounds. Without understanding what caused this problem, the organization cannot be fixed or redesigned. If, for example, the CBP had been under budgetary pressure and was forced to cut cost at the expense of a safety management department, then no amount of solutions implemented at the level of individual controllers would help because the organization as a whole is broken. The authors did underscore the importance of organizational factors, but the ECF method was not able to support their analysis.

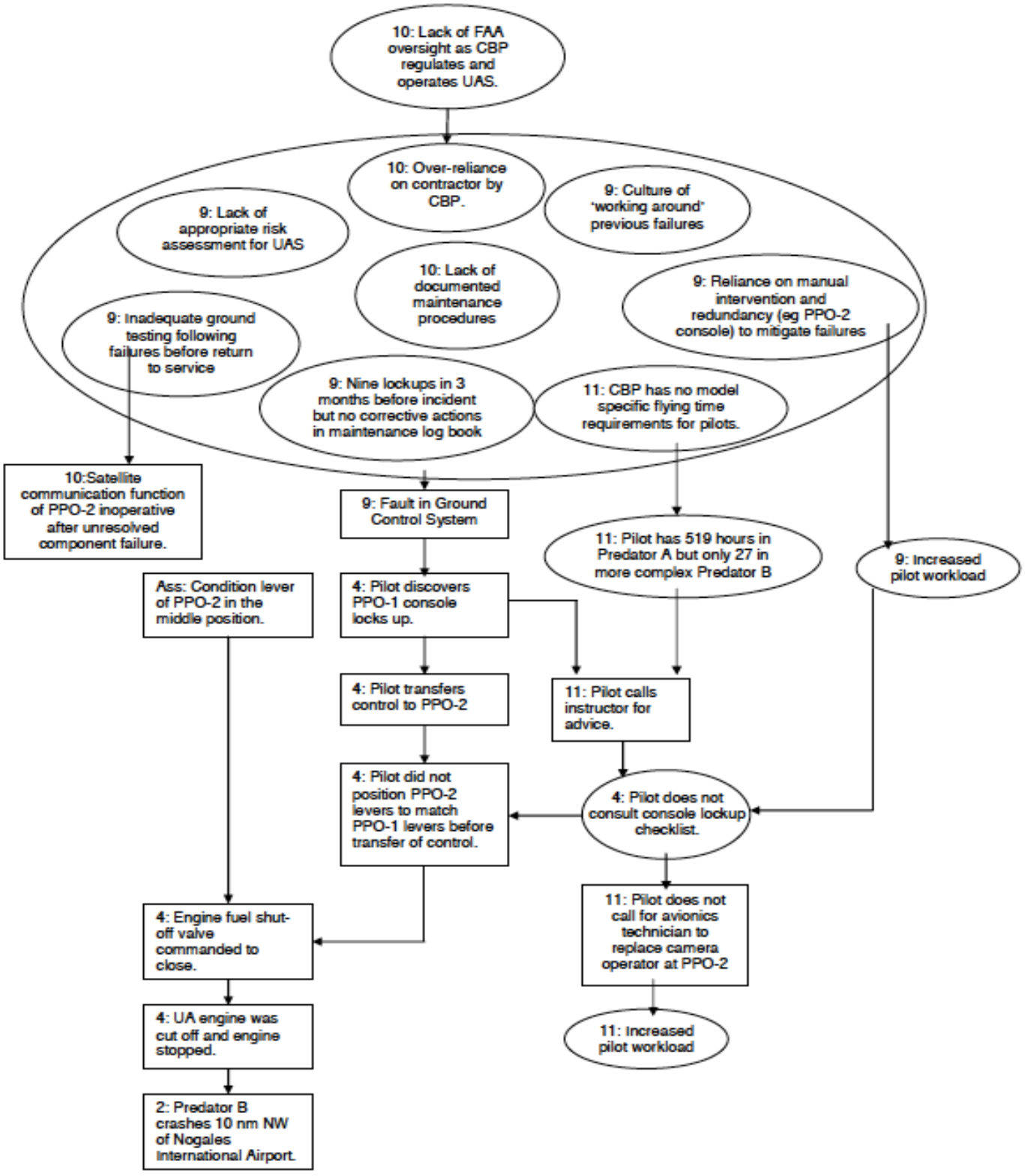

Figure 31 ECF Diagram of Causal Factor Contributing to the Pilot's switch from PPO-1 to PPO-2 Source: [128]

The AcciMap analysis shown in Figure 14 created by Svedung captures more organization factors than the other Swiss Cheese methods do. However, factors such as 'National transport policy' highlight what would be called an 'inadequate control' in STAMP parlance, and the AcciMap method does not include the reasons explaining why the national transportation policy was inadequate. For example, could the transportation office funded by industry via a pay-for-service model? With AcciMap, the question is not asked.

Resources Required The amount of skill required for each method, and the amount of time each method takes to apply can be determined by a logical analysis of each method. The more superficial the analysis, the less time and skill it will take to execute. Furthermore, the less flexible analysis methods will also be faster to apply. The HFACS method, which is essentially an accident analysis "search tree" with 144 leaves, is easy to apply and can be performed by novices. Its ease of use has contributed to its broad application within military organizations [162]. ECF and AcciMap provide more flexibility and rely on the skill of the engineer more than HFACS does. SHOW in turn allows even more creative freedom and thus may require more skill and time to apply than do the Swiss Cheese-based methods. A method that is quick and easy to apply may not be attractive however if it cannot find all the flaws in the system.

Consistency. Because Reason's Swiss Cheese Model does not have an engineering foundation, the related methods do not classify factors consistently. SHOW has an advantage in terms of consistency because inadequate control actions are defined clearly as violations of safety constraints. Inadequate control actions in HFACS, ECF or AcciMap can be classified as an *unsafe act* or a *precondition for an unsafe act* depending on what moment is chosen as the "start" of the analysis. A decision classified as a *precondition for an unsafe act*, is not analyzed to the same degree as a decision classified as an *unsafe act*.

Examples: In Carrigan's analysis [126], the failure to update the lost link profile is categorized as a *precondition for an unsafe act* rather than as an *unsafe act*. There is no HFACS analysis to explore the context surrounding lost link profile oversight, although with investigation, further preconditions for this human error could be found. The distinction between preconditions and unsafe acts may be subject to hindsight bias or convenience. Therefore, because HFACS results are based on subjective *unsafe act* or *precondition* decisions, results of the analysis may not be consistent when performed by different groups. This is important because it indicates that each application of HFACS has the potential to focus on some critical factors while missing other critical factors.

In the ECF diagram in Figure 31 "Pilot does not call for avionics technician to replace camera operator at PPO-2" is an event, however, "Pilot does not consult console lockup checklist" is a contributing factor. The latter factor would be classified as an inadequate control action in SHOW.

AcciMap fares better than HFACS and ECF, as inadequate decisions or actions can occur at any level of abstraction.

Facilitates the creation of Recommendations for Re-engineering the system

The organizational influences in HFACS are incredibly important, and are incorporated into SHOW, but the organizational influences listed in HFACS, and the organizational factors identified by ECF and AcciMap do not go far enough for engineers to create recommendations to address organizational problems. For example, the analysis stops upon reaching labels like 'deficient planning' and 'time pressure'. However, the first is merely a convenient stopping point that sounds like a systemic flaw, yet an argument can be made that it is truly an *unsafe act*—which would direct HFACS engineers to the bottom of the Swiss Cheese hierarchy. Engineers using SHOW would call 'deficient planning' an inadequate control action, and it would serve as a starting point for contextual analysis, rather than as an ending point. Many factors cited in the Swiss Cheese-based methods don't point to solutions; many factors are another label for human error in disguise.

For example, the HFACS Nogales analysis cites [126], "Complacency in maintenance supervision" and "No simulation training available" as issues. However, in the HFACS framework, these issues are *end points of inquiry* as they both represent factors at the top of the HFACS Organizational Influences chart in Table 5.

In contrast, SHOW extends the analysis further: context is analyzed for each inadequate control action. With SHOW it is possible for analysts to:

1) Identify the lack of maintenance supervision as an ICA and

2) use the guidewords to explore the reasons surrounding maintenance supervision complacency: Were CBP officials "lazy?" Or did the CBP fail to deliver a well-maintained product because the CBP lacks expertise or staff to devote to activities that do not produce measurable national-security-increasing outputs?

and similarly:

1) Identify the decision to not require simulation training as an ICA and
2) use the guidewords to draw out the reasons for the decision: Did safety culture problems result from a distrust between human factors engineers and management? Or the inability to devote additional funds to an over-budget design?'

Interestingly, the NTSB report does not include data that would answer the questions above. This indicates that SHOW leads the analyst down paths that were overlooked by both HFACS and the NTSB processes.

In addition to recommendations, the SHOW accident analysis also produces a list of questions to further understand how the accident occurred and how to prevent accidents in the future. In contrast, HFACS and ECF did not encourage analysts to identify additional questions.

Domain Independence

HFACS was designed for aviation related mishaps. HFACS had to be re-created for maintenance related aviation accidents [131]. The level of specialization and domain specific terms means that it must be recreated for every application outside of the aviation domain. AcciMap, ECF, and SHOW have been applied in several domains and are domain-agnostic.

7.4 Summary

Final judgment of SHOW must be reserved for future safety practitioners who use it to analyze accidents in complex systems. If engineers using the method generate more comprehensive insights into accidents than other methods, it will be a success. This chapter showed that while the other analyses claimed the importance of contextual factors, they did not have a way to make an explicit connection between *context* and *inadequate control*.

[Page intentionally left blank]

CHAPTER 8 SYSTEM DYNAMICS DEEP DIVE

8.1 Overview

The use of system dynamics as part of SHOW can be extended through the use of executable models and archetypes. This chapter introduces advanced system dynamics concepts and demonstrates their use with examples from aviation, healthcare, and the chemical industry.

8.2 Executable Models

Executable system dynamics models are useful for the deconstruction of complex interactions and analyzing the effects of policies on system states over time. System dynamics is particularly useful for demonstrating the effects of policies that produce striking and unexpected results in the long-term. System dynamics modeling makes it possible, for example, to understand and predict instances of policy resistance or the tendency for well-intentioned interventions to be defeated by the response of the system to the intervention itself. The models can be used to devise and validate fixes for the problems and to design systems with lower risk. Furthermore, the simulation can be run without the assumption that the system structure and context remains constant.

In addition to characterizing problematic system interactions and helping decision-makers understand the system, the model is a useful test-bed for the exploration of new policy. Decision-makers may systematically test potential policies and select those with favorable results for actual implementation. Furthermore, at the level of executable models, principles from decision theory may be employed [116]. System dynamics models can also be generalized to examine the effects of system-level strategic decisions on safety in a variety of settings.

For example, modelers and managers can experiment with various incentive structures or various workforce experience make-ups and learn how decisions about risk change as a result. For a single controller with multiple goals, models can be built to explore how local operator optimization in the face of pressures (e.g. time, resource) can affect system-wide performance. The model-building process can increase system understanding, which can lead to the discovery of new hazards, and a chief value is using the model to convey the importance or danger of hazardous scenarios and potential solutions.

8.3 Safety Archetypes

The safety archetypes discussed in section 2.2 can be used to build CLDs as part of an accident analysis, risk assessment or hazard design analysis. They may be used as a hypothesis-driven process where engineers experiment with various archetypes to explain certain system behaviors. The archetype-based CLDs are particularly useful for communicating fundamental dynamics to others without building a domain-specific model from scratch.

8.3.1 Getting Away with Risky Decisions Seems Safe Enough

This research identified a new safety archetype shown in Figure 32. This archetype concerns human decision-making about risk, or whether or not to follow through with a risky choice.

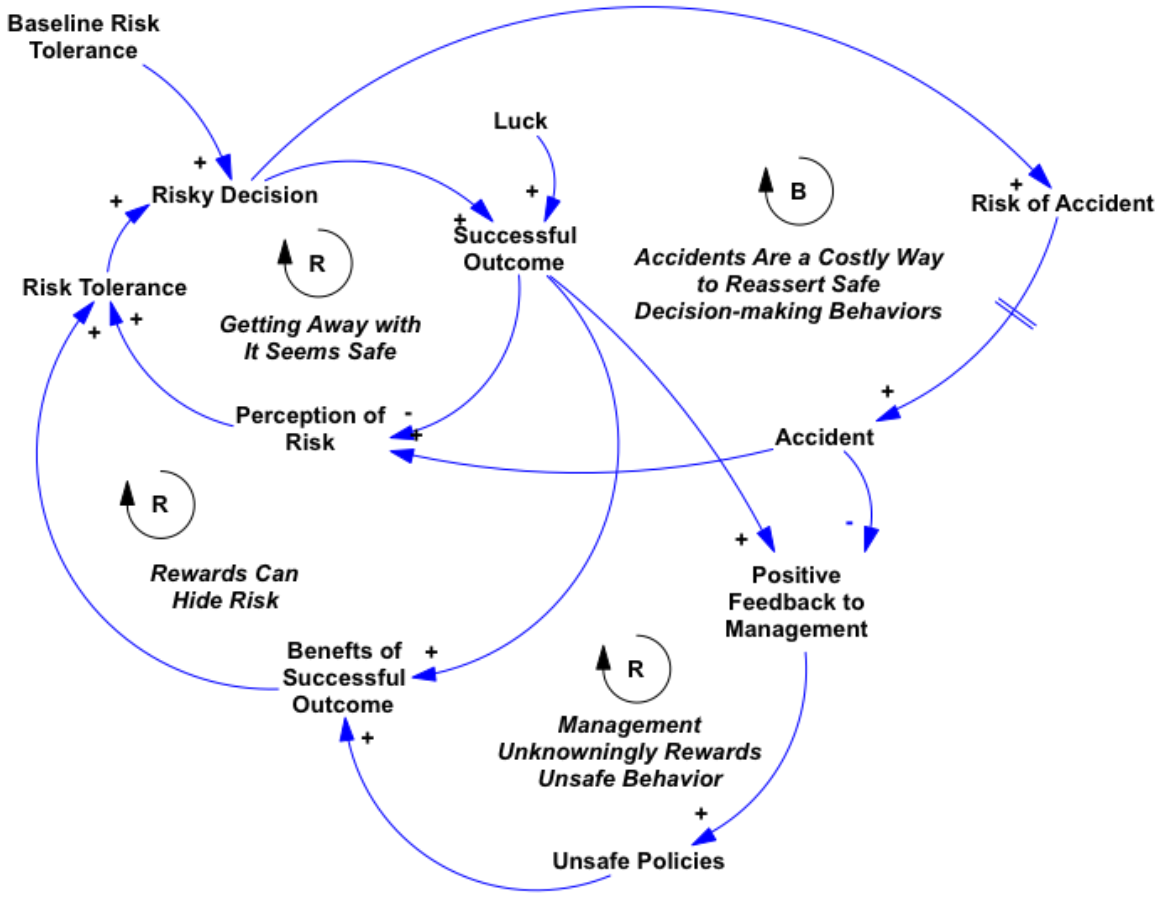

Figure 32 Getting Away with It Increases Risk

The basic dynamic of this loop is that the risky decisions that individually have a small probability of causing a disaster and do not have immediate negative consequences or costs do not provide the decision-

maker with accurate feedback as to how risky his or her actions truly are. By behaving in a risky fashion, the number of immediately obvious successful outcomes increases and decision-makers are rewarded by management. The rewards, combined with the lack of negative consequences, lower the decision-maker's perception of risk, and increase his or her risk tolerance. In the future, the decision-maker will be ever more likely to continue to make risky decisions.

In most complex systems, decision-makers are rewarded according to policies enacted by management. The rewards that management (or higher-level controllers) have made available to the lower-level decision-makers are consumed in close temporal proximity to the decision outcome. Management-provided rewards can include financial bonuses or preferential work assignments. Without understanding the consequences of risky decisions, unless there is an accident management will not consider (or be aware of) the ever-increasing system risk. Management will see the increase in successful outcomes, and will continue to believe that the behavior-shaping policies in place are successful.

To prevent a migration to a state of high risk in this scenario, solutions must focus on factors that eliminate the safety-decreasing feedback loops, introduce immediate, negative consequences to the decision-maker, or provide accurate feedback to decision-makers regarding the aggregate effect of their risky decision-making.

8.3.2 Common Factors that Decrease Safety Exhibited by Complex Systems

The *Getting Away with Risky Decisions Seem Safe* archetype incorporates several factors that decrease safety: 1) long delays before negative consequences reach decision makers combined with immediate rewards for risky decisions; 2) numerous decision makers; and 3) an asymmetric distribution of benefits and negative consequences resulting from risky decision-making to system stakeholders.

Long delays in the system are characteristic of disaster: a small increase in risk (resulting from each risk-increasing decision made) may take a while to accumulate before an accident or major disaster occurs.

Decision-makers often experience a long delay between when a safety-decreasing decision is made and when its consequences are felt due to thick layers of controller hierarchy. In some systems, negative consequences are first felt by higher-level controllers who in turn pass along negative consequences or change policies to modify lower-level controller's risky behavior. Often, the consequences of safety-decreasing decisions may go through several higher-level controllers, possibly including stakeholders

from other organizations. This pattern, first depicted in Figure 28, is explored further with system dynamics in Figure 33.

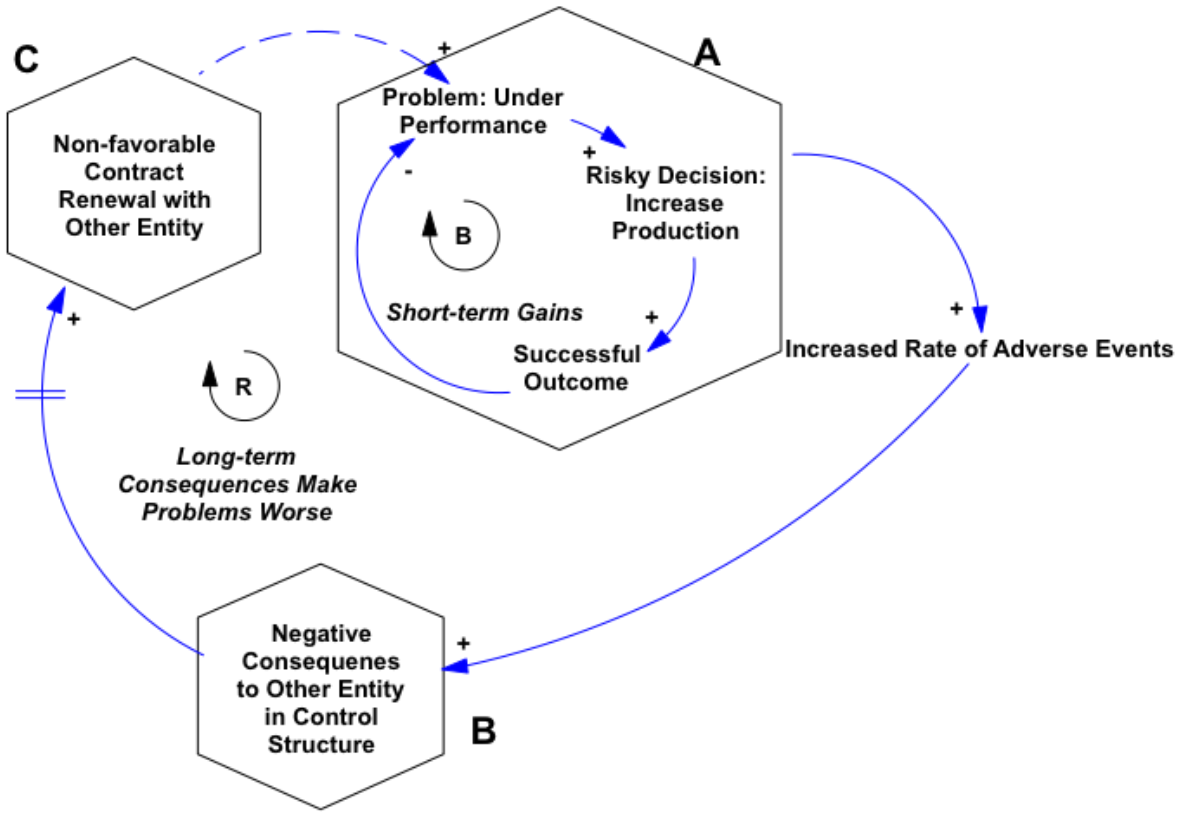

Figure 33 Factors that Erode Safety in Complex Systems

In the system depicted Figure 33, each hexagon represents a unique controller. In the 'Short-term Gains' loop, decision-makers 'A' are faced with a shortfall in production (a.k.a. a gap between desired production and current production). Consequently, they choose to increase production and are rewarded with short-term gains that make up the gap. However, in a variation of the classic 'burning the midnight oil loop', the negative effects of the increased production are not limited to the acting organization. Controller A's management doesn't see the increased rate of adverse events, dealt with by different part of the organization (controller B). In this scenario, costs are paid by second party 'B' via an increased rate of adverse events. In turn, the second party passes along the increase in their costs to a third party 'C' through renegotiated contracts. With varying degrees of delay, increased costs may be passed throughout the complex system, through a number of controllers (as depicted by the dashed line in Figure 33). In this example, the increase in costs impacts decision makers 'A' though another production shortfall.

The multitude of decision makers clouds the consequences of policies and actions throughout the system. As each decision maker (controller) attempts to maximize his or her utility function, overall system safety is compromised. The connection between the increased production and the increase in adverse events may not be observable to the decision-makers 'A'. Decision-makers 'A' may receive feedback regarding the quantitative output of their process, while decision makers elsewhere in the system are left to account for the quality of the process. Furthermore, each decision maker that passes along successive penalties may not understand how their decisions and actions affect subsequent controllers. Without appropriate design in place, decision makers misinterpret the sensor information they receive and continue to make unsafe or costly decisions. While the number of entities of a complex system cannot be reduced, it can be planned for: design can affect the information shared.

Another common feature of complex systems represented in the safety archetype is that of the asymmetric distribution of costs and benefits that result from risky decisions. Benefits are consumed by decision maker A, but the financial consequences are felt by stakeholder B. Consequences may occur with certainty, or they may occur with a greater probability. The effects of an asymmetric distribution of risks and benefits may be exasperated by delays. Often times, the benefits of risk-taking are experienced by a decision-maker in the short term while the consequences to other stakeholders are experienced or not discovered (or 'measured') for years. For example, in healthcare, surgeons that rush a case increase the likelihood of an adverse event for the patient. The adverse event may be experienced by the patient during surgery (e.g. cardiac arrest), or the consequences may not become obvious for years (as in the case of a radiation overdose). The asymmetry of who experiences the rewards and who experiences the consequences presents a challenge for systems safety: but while it cannot be eliminated, the asymmetry can be designed for.

8.4 Solutions to the Common Factors

System design can prevent long delays, multiple decision makers, and asymmetric risk and benefit distribution from leading to accidents. Some solutions may target each controller's model of the system, such as tools for decision makers to show how they depend on and are influenced by the actions and decisions of other controllers. Other solutions aim to provide missing feedback. As shown in Figure 34, decision-makers receive needed feedback when a connection between the rate of adverse events and the risky decision to increase production is implemented. When these adverse events are visible to decision-makers, they are less inclined to overlook unacceptable rates of adverse events. . The rate that is considered to be unacceptable can be formally defined by company policy, reinforced or redefined by company safety culture, or may be a control-imposed limit.

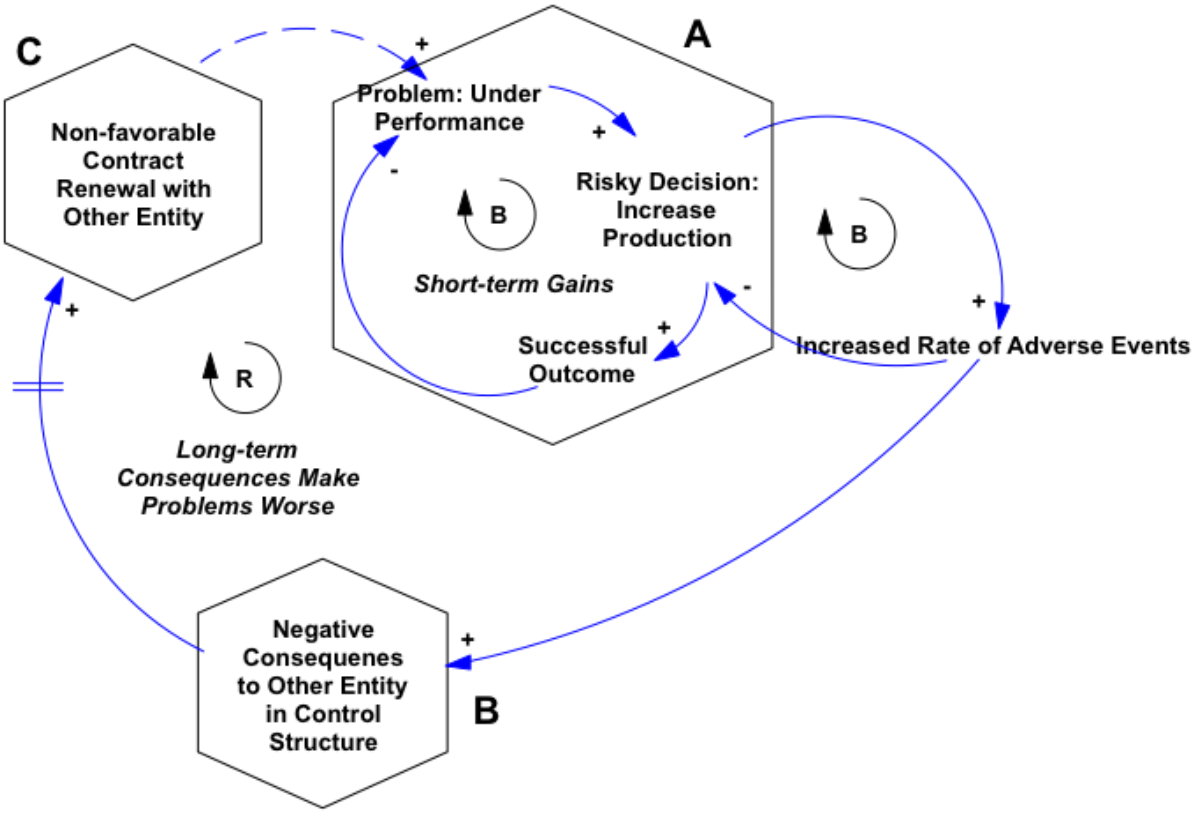

Figure 34 Solution

Domain-dependent solutions can be discovered, demonstrated, or discarded using system dynamics. The guidewords from the SHOW method can be used to build the CLD or discover problems after the CLD has been created. For example, engineers can apply the 'pressures' guideword to discover which state variables influence controller behavior. The CLD can then be made into an executable model for the purposes of experimenting with design solutions, options, or recommendations when using SHOW. For example, the requirements for a safety reporting system (e.g. which controllers need access, how soon should incidents be reported to stem risk migration) can be explored using an executable model. A CLD in Figure 35 suggests that a safety reporting system can improve system safety, but its potential effectiveness is design dependent.

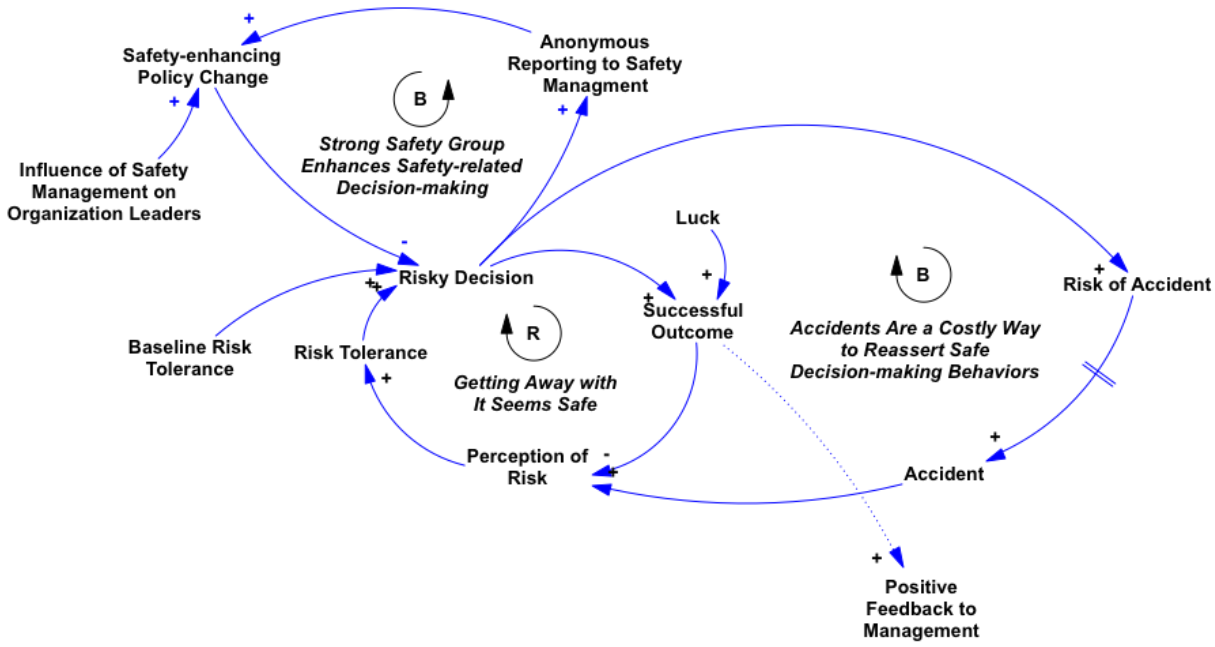

Figure 35 Safety Group

8.5 In Depth Examples

Examples from aviation, healthcare, and chemical industries are used to illustrate the principle problems in human and organizational systems, and potential solutions.

8.5.1 Aviation: Dominance of Dynamics

Feedback is a powerful influence on system safety, yet it is ill understood and ill planned for. Many of the recommended solutions following accident reports address only static factors. Because dynamic factors are neglected, the recommended solutions are not able to bring the system into a safe state for the long term. Executable SD models are perfect for demonstrating the dominance of loop dynamics over static factors or influences.

Misunderstanding loop dominance is common in accident reports. For example, accident reports that cite "human error" as the major cause often propose better training to improve human decision-making [17][19][18]. However, oftentimes, the level of training is a static factor, rather than dynamic factor, and organizational problems are the dominant contributors to risk because dynamic safety-decreasing feedback loops are present.

Many interventions are directed at static factors that do not mitigate the dominant safety-decreasing dynamics of the system. In the example depicted in the causal loop diagram Figure 36, the organization is pursuing strategies that increase the likelihood of "bad" pilot decision- making. In this case, the pilot is faced with the decision of whether or not to land in poor weather. If the weather is dangerous enough, pilots should choose to divert to an alternate airport. Factors that influence the pilots' decision-making process include their baseline risk tolerance (a factor that is largely personality-dependent), their expertise (which can be increased through training), their perception of risk (which is informed by their experience or history with the system performance), and organization-provided incentives.

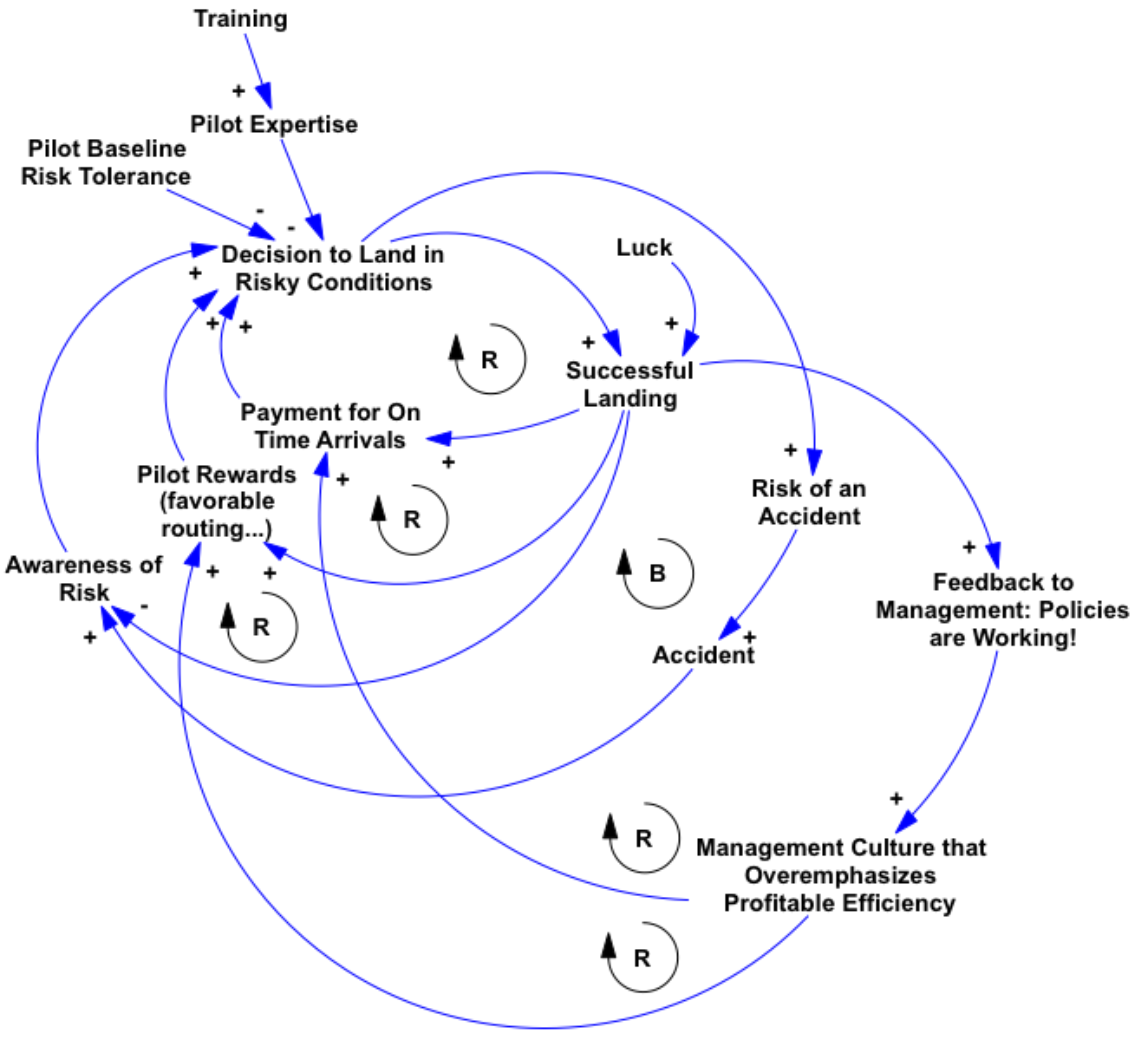

Figure 36 Pilot Go/ No-Go Landing CLD

Common organization incentives for pilots include financial bonuses for on-time arrival, and non-monetary rewards such as the assignment of preferential routings. From management's point-of-view,

these bonuses are rewarding good pilots that provide excellent service to the airline. As discussed in 8.3, management rewards pilots based on successes—usually without looking deeply into the context in which those successes were achieved. Management does not anticipate that these incentives, in the face of bad weather prospects, encourage unsafe decision-making.

In the CLD above, training is a static influence that does not change the loop dynamics or change the relative dominance of the balancing and reinforcing loops. Increasing the level of training for pilots increases their expertise, which subsequently lowers their risk tolerance. The pilots' response to management incentives is to temporarily increase their willingness to land in risky conditions, which in turn increases the chance that they will again decide to land in poor weather, which begets more risk-increasing rewards.

In this case, management measures only the increased number of successful landings and consequently management's sole feedback indicates that whatever policies it has in place (pilot incentives) are working to produce desirable and profitable outcomes. It is not until an accident occurs that management's view is (hopefully) corrected and the pilot's willingness to land in risky conditions is dramatically reduced.

To test the common solution purported by accident reports, an executable version of the CLD in Figure 36 was implemented. Notional values were used for each state variable. The exact value of each state variable is less important than the relative behaviors and trends demonstrated by the model. The model was executed under four different scenarios: 1) the status quo: nominal training, with the pilot incentives in place; 2) nominal training, without pilot incentives; 3) increased training with the pilot incentives in place; and 4) increased training without the pilot incentives in place. The results of these four scenarios on pilot behavior are plotted in
Figure 37.

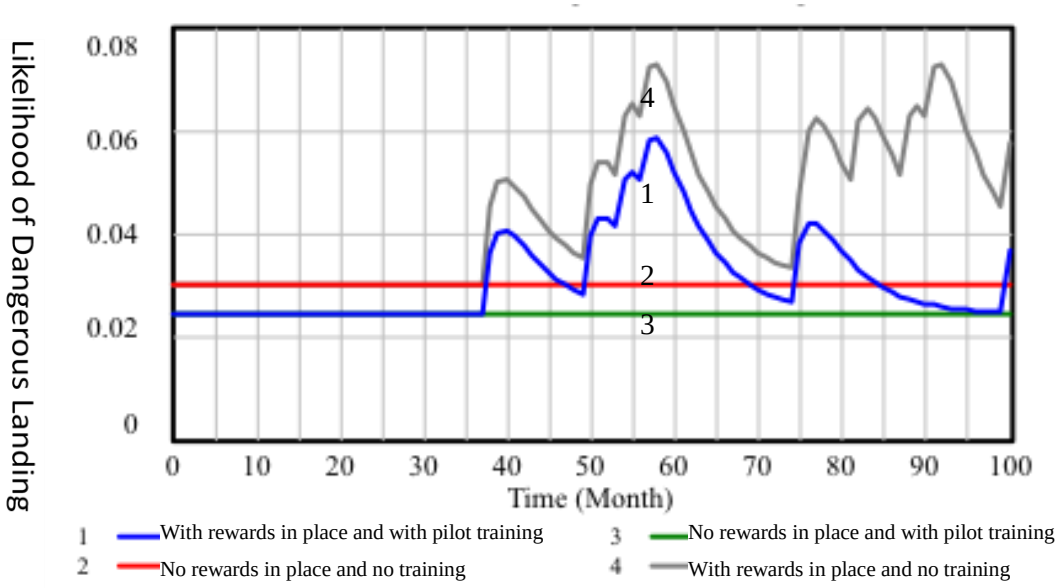

Figure 37 Likelihood Pilot Will Land

In this case, as shown by the gray line, the business-as-usual scenario produces the least safe system, in which the pilot chooses to land the most. The scenario that accident reports usually recommend, increased training, leaves incentives in place but with a 20% reduction in overall willingness to land in poor conditions. As shown by the blue line, the pilot is still susceptible to the effects of the rewards and the pilot still exhibits a varying and high willingness to land.

After the reduction in overall risk tolerance provided by the training, the pilot's risk tolerance is lowered so that he or she does not land at month 80. When there are no rewards for risky landing, at month 80 the pilot's willingness to land continues to decrease, and his or her risk tolerance is low enough that he/she does not land at month 85 and 90. When the rewards are removed, with or without training, the pilot there is a 70% reduction in poor weather landings.

By making this CLD model executable we are able to demonstrate the power of dynamic solutions (such as removing or changing the pilot reward incentives) over static solutions (such improved training for pilots). Solutions that affect either safety-decreasing loops or change the relative dominance of safety-decreasing and safety-increasing loops are effective and necessary. In complex systems, it is often impossible to measure, with metrics, the level of system safety. Accidents, though catastrophic when they occur, are rare, so it is important to have systems able to change the loop dynamics to ensure that accidents are not the sole "balancing loop" keeping risk in check.

8.5.2 Healthcare: Delays, Multiple Decision Makers, Risk/Benefit Asymmetry

In many real systems, decision makers in a 'Short-term Gains' loop may not realize that their actions lead to reoccurring shortfall. A case study of a teaching hospital revealed a state of high-risk operations due to long delays, multiple decision-makers operating without an accurate process model, and asymmetric distribution of risks and rewards.

Overview

The operation of hospitals in a low-risk state has become more challenging as cost-of-care increases have forced hospitals to find alternative revenue sources. In particular, hospitals have compensated for increasing costs by expanding their ad hoc patient referral base and overloading their operation schedules without a corresponding increase in resources to treat the increased patient load. Without adequate resources to treat patients, proceduralists respond to throughput pressure by reducing time spent on individual patient treatment, thereby exposing the patient to greatly increased risk of an adverse event. The subsequent treatment of the consequential adverse events increases the cost-of-care, because hospitals charge related treatment to insurance companies. In response, third-party payers have renegotiated their contracts with hospitals to deny coverage of adverse event treatment.

Third party payors believe that denying payment for treating adverse events would encourage practitioners to be more careful and cause fewer adverse events. However, because hospitals, most of which are non-profit, are under tremendous pressures to stay solvent and have few ways of dealing with financial shortages, the denial of payment causes further pressure to increase production. Hospital administrators that put pressure on surgical practitioners are often not aware of the adverse event increase. An increase in adverse events can by obscured by admission to other units within the hospital, or by adverse event treatment that occurs at a different hospital or treatment that is temporally removed from the surgery. The delays and locally optimal decisions create policies and pressures that catch surgical practitioners in a 'short-term gains' loop.

The asymmetric distribution of risk and benefits is also present in the healthcare system. Patients bear the downside to increased surgical throughput: adverse events. The surgeon enjoys the benefit: increased productivity. Without an opposing pressure to push surgeons to operate more conservatively, the asymmetry between surgeons and patients allows system risk migration.

The CLD representing the system described above is shown in Figure 38.

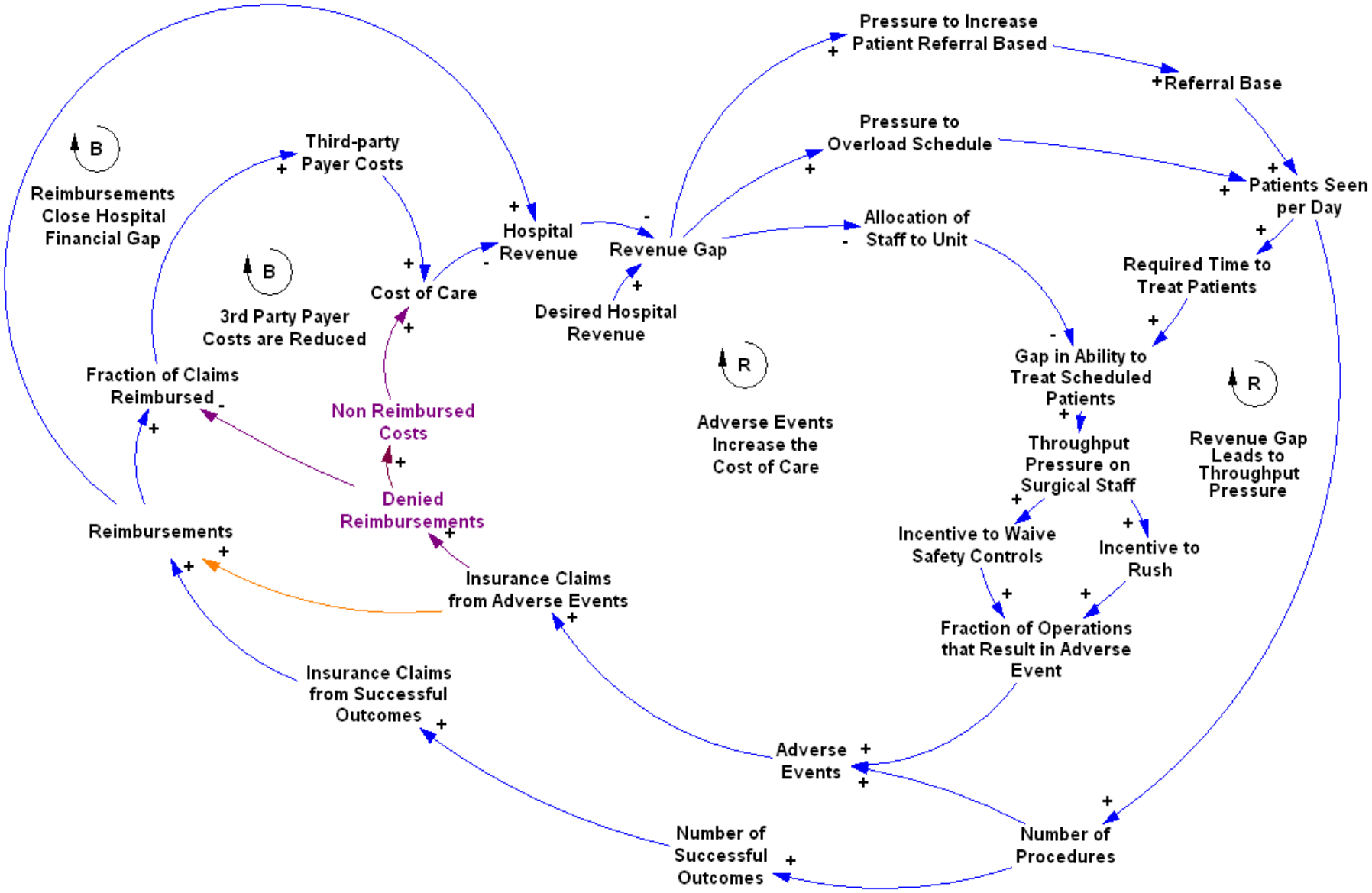

Figure 38 Healthcare

Analysis

The graph in Figure 39 shows that the policies adopted are able to sustain the hospital financially, but at the cost of safety, as shown in Figure 40. Whether or not adverse events are reimbursed, hospital finances dip due to unfavorable contract renegotiations with third-party payors, but because of the strong pressure to increase throughput, the finances recover until the yearly contract renegotiation with the third party payors. The graph in Figure 40 shows how the incidence of adverse events is affected by the policy to deny reimbursement for adverse event complications: while the system was operated in a high-risk state with ever increasing adverse events before the change, the policy has since made the situation even worse.

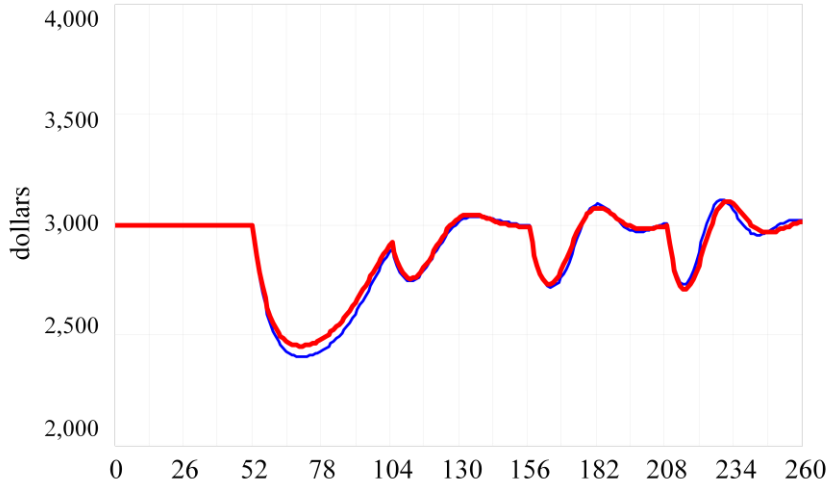

Figure 39 Change in Hospital Finances

The thin line shows hospital finances when reimbursement for adverse event treatment is denied. The thick line shows hospital finances when reimbursement for adverse event treatment is permitted.

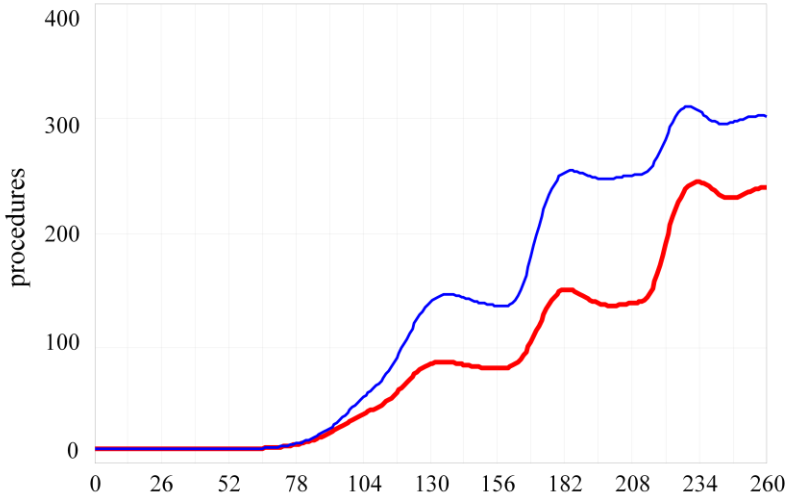

Figure 40 Increased Adverse Events

The thin line shows number of adverse events when reimbursement for adverse event treatment is denied. The thick line shows number of adverse events when reimbursement for adverse event treatment is permitted.

The change to the reimbursement policy is another example of a fix that fails: a well–meaning action is undermined by unintended consequences [64]. The effects of new policies are not obvious to system stakeholders who do not have a system view and treat the system goals (safe, clinically effective, cost effective and sustainable operations) as independent.

Partial solutions that change the link between the control action and the unintended system reaction can be made within the purview of the surgical unit include risk-based scheduling and tools that are better able to identify high risk patients whose surgeries must not be rushed. However these solutions are limited, as they do not align the incentives of the hospitals, third-party payers and providers to that of patient safety.

A policy of provider accountability would add the missing feedback between the control action (the decision to rush) and the system reaction, aligning stakeholders. If proceduralists treat adverse event complications without fee-for-service they may better able to negotiate throughput pressure and patient safety. Without such a solution, in the presence of throughput pressure, physicians may work in a riskier fashion than they realize, and adverse events will occur. Providers must have the freedom to work at a rate that maximizes their compensation when they are working safely. While hospitals would lose revenue in the short-term in the form of lower surgeon productivity, they reap long-term gains in the form of more favorably negotiated reimbursement contracts.

In addition, immediate feedback to hospitals regarding a rise in the rate of adverse events would help to highlight the relationship between adverse events and throughput pressure. Tools such as electronic monitoring of patient outcomes by surgeon, wing, unit, floor, day admitted, or time admitted, may be required. But, to maintain safety, this feedback must not remove hospital reimbursement for adverse events. In surgical care, some adverse events are inevitable, because an individual's response to surgery is not predictable even if surgical skill is high and safety measures are followed. Without adverse event reimbursement, costs due to surgical complication treatment may drive the system into an unsafe state.

As in the aviation example, interventions that target loop dynamics are powerful solutions for preventing the 'Adverse Events Increase the Cost of Care' loop from becoming dominant.

The system dynamics literature contains several customizable executable archetypes for the examination of aggregate behavior. In particular, the models concerning rework in manufacturing demonstrate the same kind of problems seen in system safety. In both manufacturing and system safety, proactive investment that reduces the incidence of defects and increases overall system efficiency follows the same worse-before-better effect on costs.

8.5.3 Citichem

Based on sample accidents in the chemical industry [167], the following example demonstrates the important feedback loops that enhance safety or increase risk.

Overview:
In this accident, a corporate manager feeling financial pressure from industry competitors directs his subordinate plant manager to increase production of a dangerous chemical. Without additional funds, the plant manager in turn directs operators to ramp up production. Meanwhile, the city nearby the chemical plant feels financial pressure and relaxes city regulations governing plant operations oversight. Operating over capacity, an explosion occurs within the plant killing plant operators and nearby townspeople.

This relevant dynamics leading to the accident are depicted in the figures below.

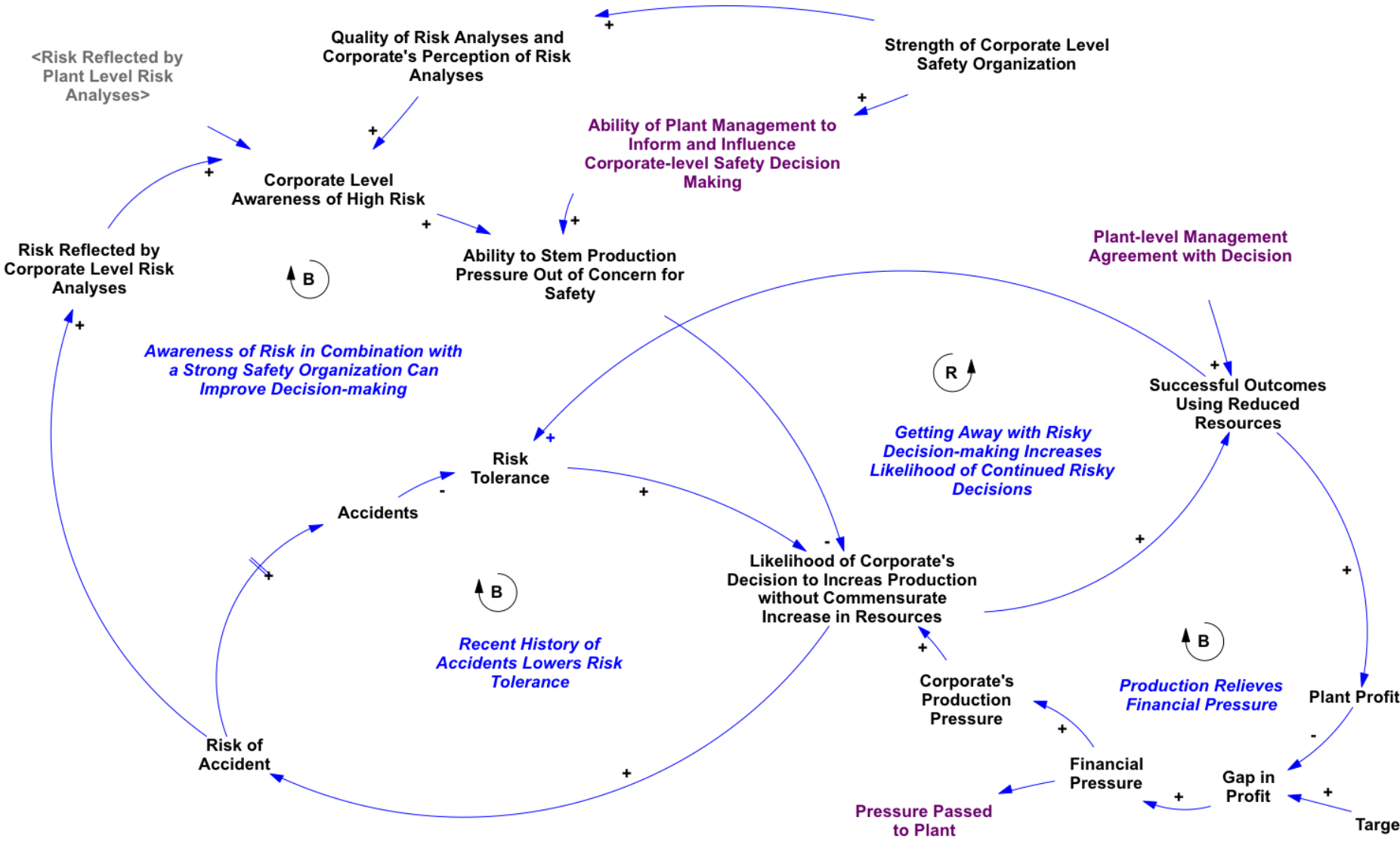

Figure 41 Corporate

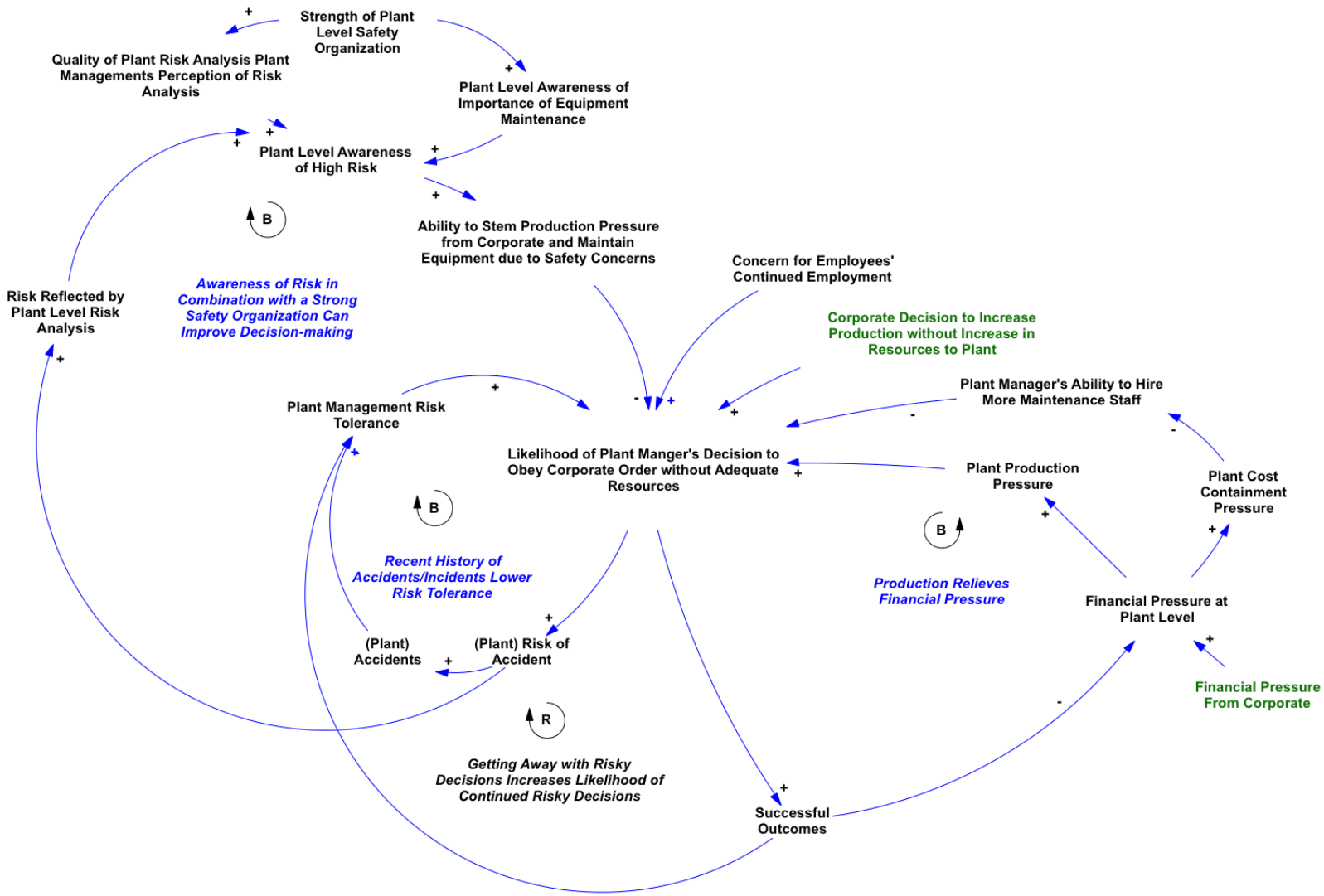

Figure 42 Plant Manager

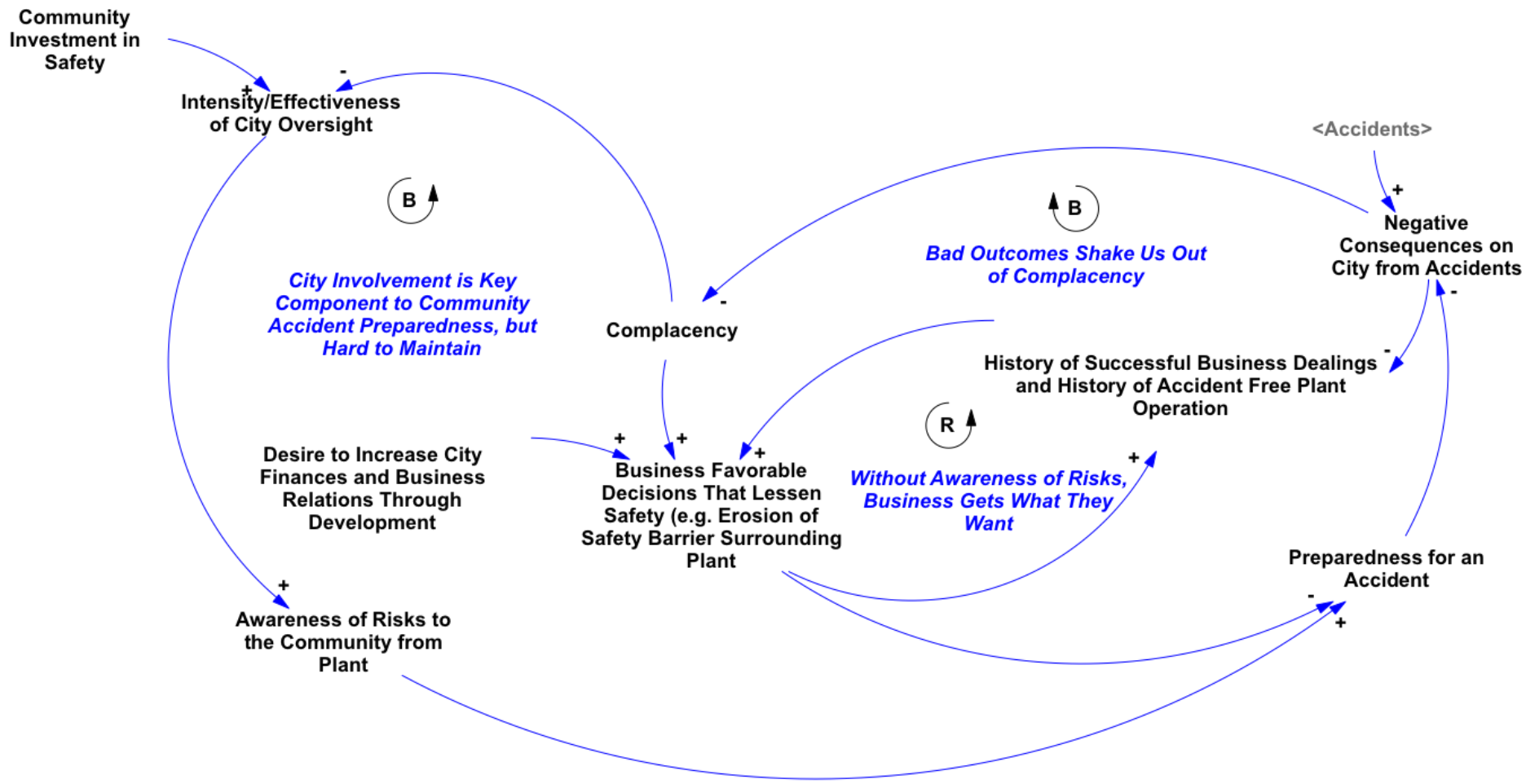

Figure 43 City

The loops in Figure 41 and Figure 42 show the same loops discussed in the Pilot Go/No-go example and the healthcare example: increased risky decisions lead to short-term gains and increasing risk tolerance. Furthermore, as in many complex systems, decisions-makers are not aware of leading indicators of risk, so there risk tolerance increase until an accident occurs. Safety groups acts as counter-forces to increasing risk tolerances.

At the heart of the city CLD in Figure 43, the short-term risk increasing decision loop pops up again. This time, the city's risky decisions in and of themselves don't increase the likelihood of accident (as was the case with rushing production of chemicals or surgical cases), but the city's decisions remove the barriers that preventing an accident (loosening oversight regulations) and the increases the potential impact severity of an accident if one occurs (by allowing residential development to occur near potential blast zones).

The fundamental dynamics of accidents and safety, which are driven by human and organizational factors (pressures, resources, communication, etc.), manifest in repeated patterns. The same loops— short-term benefits, increasing risk tolerance, accidents shake us from complacency, and the benefits of independent safety groups— exist in each of the accidents studied in this thesis. The system dynamics extension to SHOW can be useful in accident analysis, by providing a 'big picture' view to engineers and stakeholders. The extension may also be useful prospectively, as part of a hazard analysis that allows engineers to experiment with policy implementations without testing new policies on the actual system.

The next chapter develops the use of SHOW prospectively for use as a hazard analysis method.

[Page intentionally left blank]

CHAPTER 9 SHOW APPLIED TO HAZARD ANALYSIS

9.1 Chapter Overview

This chapter describes the SHOW hazard analysis process. The hazard analysis is demonstrated through a series of examples and continues with a discussion of the method and applicable assessment dimensions.

9.2 Hazard Analysis Overview

Hazard analysis for humans and organizations is different from the old hazard analyses used for physical systems. Rather than finding a physical mechanism for an accident to occur, we seek to find the flaws in the organizational design that create an operating context in which humans make decisions that lead to inadequate control. Many processes can analyze how an inadequate control action may cause hazards that lead to an accident; what we seek to discover is how the system design, in particular the social aspects of the design, can lead to a flawed operational context.

In practice, analysis is now conducted on systems, after they have been launched, to discover inadequate design flaws. These are called *safety audits.* They are typically conducted on a periodic basis, and can find flaws in the organizational design and in human-centered design. There are two problems with this practice: 1) they are treated as a separate activity from hazard analysis, when really they are part of the hazard analysis for the whole system; and 2) they are often ignored. BP, for example, had conducted a safety audit of the Deepwater Horizon seven months before the disaster and had found 300 maintenance issues [168]. However, the audit was not taken seriously by the organization, and the problems were not addressed.

This hazard analysis method is intended to be a practical, systematic process with which to analyze the *context* in which controllers and organizations make decisions are take actions. The context can contribute to inadequate control via inadequate goals, controller algorithms, et cetera. The contextual analysis, which can include everything from the environment in which decisions are made, to the communication structures supporting controllers and the language spoken by operators, will identify flaws that can lead to hazards.

For example, the hazard analysis method can be used to identify gross mismatches between how operators are compensated for the achievement of goals and how management messaging prioritizes operator goals.

Mismatches lead operators to maximize rewards, rather than follow the safety priorities written in operating procedures. When organizations lower the priority of safety-related tasks, system risk increases. When engineers expose flawed design (e.g. compensation vs. corporate messaging goal priorities), the engineer must 1) change the design to eliminate the hazardous context mismatch and 2) identify auditable factors so that future mismatches do not occur. In general, the purpose of hazard analysis is two-fold: to find design flaws so that the system can be improved and to identify auditable factors that safety management can use to monitor system risk.

The process outlined here can be applied to a system that has not yet had an accident and in the development of new systems[15]. The hazard analysis also aids in the safety analysis and design of proposed changes to existing systems, such as new patient management techniques for the operating room. In either case, engineers need a method that can guide users to appropriately define the system boundary and develop a system that operates safely over its lifetime in ever-changing environments.

The hazard analysis method is presented in a series of stages that are performed at different degrees of abstraction. Each stage of the hazard analysis is motivated, explained and demonstrated through examples. The hazard analysis method, which extends STPA, shares many of the same process steps, which are repeated for completeness and clarity. The method is intended to integrate easily into the "design for safety" process in which design is created at the same time as the safety analysis is performed so that safety is "designed in." The first steps of the process are endemic to most design processes.

9.3 First Stage: High-level Goals, Loss Events, Hazards and Safety Constraints

The first stage of the hazard analysis process, like STPA, is to identify the unacceptable loss events. Safety is defined as the freedom from loss events, and can include the non-accomplishment of system-

[15] The definition of *system* to be used in this thesis is: An organized set of parts and interacting elements that perform a function that is more than the sum of its parts. A system may consist of things, people, and organizations. An important theoretical underpinning of the research presented in this thesis is that humans and social constructs are analyzed as part of the system. Humans and organizations must be analyzed beyond the "man–machine" interface. Humans must be treated as part of the system because their role (job) is designed, their interactions with the system and each other are designed, and their interactions with each other create the most powerful drivers of system safety (and system risk).

level goals. System-level goals describe the purpose of the system and specify what value or benefit the system delivers. The system goals are also important because they imply the set of potential accidents.

9.3.1 Goals

System-level goals are typically given to safety and design engineers by the customer, external organizations, or executives within the organization. Potential System-level Goals from various industries are shown in Table 9.

Table 9 Example System-level Goals from Various Industries

New System or System-level Change	**Goal**	**Industry**
Introduction of ADS-B	Increase NAS operating efficiency (e.g. more planes within the operating air travel corridors) via reduced separation standards made possible through the use of ADS-B.	Aviation
Electronic Health Records	Improve provider decision-making through greater data availability. Make improvements in drug efficacy models or disease models via data mining of new databases made possible by electronic health records.	Healthcare
New Automatic Refinement Technique	Increase oil throughput and increase profit margins through automated refinement process.	Oil
Creation of New Federal Department: Department of Homeland Security Department	Protect the security of the United States of America	Government/ Security

9.3.2 Loss Events

The next step in the hazard analysis process is the identification of unacceptable loss events or accidents. Each organization may define what they consider to be a loss even or accident. The FAA defines loss events or accidents as:

> "an occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight and until such time as all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage." [118].

In contrast with the FAA definition, where loss events come in the form of physical damages, a potential loss even in the space domain may be abstract, such as the loss of mission precipitated by the corruption of key scientific data. In other situations, loss events could include the loss of a great deal of money, such as the destruction of shareholder value due to tangible asset loss or damage to company reputation. Further loss event examples are shown in Table 10.

Table 10 Example Loss Events in Various Industries

New System or System-level Change	**Loss Events**	**Industry**
Introduction of ADS-B	Mid-air Collision.	Aviation
Electronic Health Records	Death or injury due to misinformation. Loss of privacy due to health data insecurity.	Healthcare
New automatic refinement technique	Explosion.	Oil
Creation of Homeland Security Department	Terrorist Attack.	Security

9.3.3 Hazards

Following the identification of accidents, the next step in the hazard analysis is to translate the accidents into hazards. Hazards are the state-based conditions of the system that can lead to an accident. Some hazard examples are shown in Table 11.

Table 11 Example Hazards in Various Industries

New System or System-level Change	Hazards	Industry
Introduction of ADS-B	ADS-B communication link is inoperative and the position of ADS-B equipped aircraft is unknown.	Aviation
Electronic Health Records	Operating surgeon obtains incorrect information from EHR system that leads to a patient injury. EHR data is obtained by unauthorized persons during transmission	Healthcare
New Automatic Refinement Technique	Pressures are exerted on fuel tank beyond that which it was designed to withstand.	Oil
Creation of New Federal Department: Department of Homeland Security Department	Terrorist plots are not detected in time to prevent them.	Government/ Security

9.3.4 Safety Constraints

Continuing in the hazard analysis process, high-level hazards are turned into safety constraints through a simple process. Example safety constraints and their related hazards are shown in Table 12.

Table 12 Example High-level Safety Constraints in Various Industries

New System or System-level Change	Hazards and Safety Constraints	Industry
Introduction of ADS-B	H: ADS-B communication link is inoperative and the position of ADS-B equipped aircraft is unknown SC: ADS-B communication link must be up for all time *t*. SC: Airplane position (and time derivatives)	Aviation

	state must be known for all of time *t* to X precision.	
Electronic Health Records	H: Operating surgeon obtains incorrect information from EHR system that leads to a patient injury. H: EHR data is obtained by unauthorized persons during transmission. SC: EHR must contain, and make easily available, accurate patient data. SC: EHR data must be securely transmitted.	Healthcare
New Automatic Refinement Technique	H: Pressures are exerted on fuel tank beyond that which it was designed to withstand. SC: New refinement process must not create pressures greater than designed tank pressure tolerances.	Oil
Creation of New Federal Department: Department of Homeland Security Department	H: Terrorist plots are not detected in time to prevent them. SC: Terrorism related data must be available to all terrorism-fighting national security agencies at all times.	Security

9.4 Second Stage: System Control Structure

At this point in the hazard analysis process, the overall system-level goals, accidents hazards, and safety constraints have been identified. In the next stage, the initial inclusion of organizational context takes place. Complex systems are subject to much environmental, customer design, and regulatory requirements that must be taken into consideration during hazard analysis. Constraints on complex systems do not just influence the system operation; the culture of the engineers and managers overseeing its development will also have significant impact on the system and will be analyzed in latter stages. Now

we move on to identify all the entities (e.g. individuals, unions, organizations, governments, regulating bodies) that are part of delivering system value or would be impacted by a loss event.

9.4.1 Control Structure Inclusion Criteria

In order to determine which actors or entities should be included in the system control structure, criteria have been outlined by Dulac in [158]. These inclusion criteria are repeated in Figure 44. In addition, I have added the following inclusion criteria for social system control structures shown in Figure 45.

For system development:

1. Is the component responsible for defining high-level system requirements and/or mission objectives and/or development schedule objectives?
2. Is the component responsible for funding decisions for the project or program?
3. Is the component responsible for enforcing schedule, budgets, and/or system requirements (including safety requirements) during development?
4. Is the component responsible for defining development standards and processes (especially safety-related standards and processes)? If so, does it have enforcement power?
5. Is the component responsible for, or heavily involved in, initial system certification?
6. Does the component have the knowledge and authority to halt or slow down system development when problems arise?
7. Does the component include a significant number of people working on activities such as technology development, safety analyses, system design, system integration, testing, and/or quality and safety assurance?
8. Is the component an important contractor of the main development organization, providing a significant portion of the organization's product and/or technical personnel?
9. Will the component be responsible for, or heavily involved in system evolution and upgrades?

For system operation:

1. Is the component responsible for or involved in defining criteria and metrics for system performance, production requirements, and/or mission objectives?
2. Is the component responsible for funding decisions for the system operation?
3. Is the component responsible for enforcing schedule pressure, budgets, and/or requirements (especially safety requirements) during

system operation?

4. Is the component responsible for defining operation standards and processes (especially safety-related standards and processes)? If so, does it have enforcement power?
5. Is the component responsible for, or heavily involved in, system certification renewal or review?
6. Does the component have the authority to delay or stop production when problems arise?
7. Does the component include a significant number of people working on activities such as safety analyses, system evolution and/or upgrades, system maintenance, system integration, testing, safety and quality assurance?
8. Is the component an important contractor of the main system operator, providing a significant portion of the system hardware and/or personnel?

Figure 44 Dulac Control Structure Inclusion Criteria Source: [158]

For system development:

10. Is the actor/entity/component capable of influencing the outcomes of those responsible for system requirements or system design? (Such as lobbyist groups or unions.)
11. Does the actor/entity/component have influence over allocation of resources (e.g. funding, staffing) to system developers?
12. Would the actor/entity/component be impacted in the event of an accident?

For system operation:

9. Is the actor/entity/component capable of changing the requirements, standards, procedures, or waivers for system operation or influencing others to do so?
10. Is the actor/entity/component capable of influencing the allocation of resources (e.g. funding, staffing) throughout the organization to system operators?
11. Is the actor/entity/component capable of hiring/firing controllers within the system?
12. Would the actor/entity/component be impacted in the event of an accident?

Figure 45 Additional Inclusion Criteria for the Control Structure

The new inclusion criteria listed above include individuals, organizations, and entities that may have no direct control over the system development process (they are not employed by the customer to develop the engineering system) or the system operation, (they are not managers or operators) but nevertheless have impact on how system activities are carried out. These entities are part of the system's contextual makeup that can increase system safety or could create conditions such that inadequate control actions can occur.

In addition, individuals and groups that can be affected by an accident should be included in the control structure. The system design greatly impacts how affected individuals can experience an accident, and the relationship between the system and potential victims should be carefully considered. Sensitivity to

victims is especially warranted because of the inequity between those "who enjoy the benefits vs. those who bear the risks" [34]. People negatively impacted by an accident are stakeholders that can exert significant leverage (via town hall meetings or propositions, etc). The avenues of influence for these stakeholders include:

1. New laws and regulations
2. Sitting requirements
3. Operating requirements (e.g. hours of operation)
4. Lawsuits

The next step in the hazard analysis method is to analyze the system to discover the roles and responsibilities that *should* be in the system design in order to deliver the system value and enforce safety constraints. Actors are identified that will serve the *design* role in the system, the day-to-day *operation* of the system, and the *regulation* of the system. In many systems, all three of these roles can be fulfilled by the same entity; although they are not always successful. For example, in the Nogales, AZ UAS accident, GA-ASI served as the UAS designer, operator, manager, and safety regulator. (It should be noted that it was not anyone's intention that GA-ASI fulfill all three roles: the CBP was supposed to serve as the operator and the safety regulator, but did not have the skills to do either.)

9.4.2 Forming a Control Structure

At this point in the process, a control structure is developed using the relationships between identified individuals, components, organizations, entities and regulators. A full control structure includes the roles and responsibilities of each entity in the control structure and a description of how each control and feedback relationship is conducted.

Common organizational documents can help engineers develop a control structure including:

- Organization Chart
- Documented Activities
- Problem identification and resolution processes
- Reports
- SOPs
- Emergency Procedures
- Funding sources and channels
- Hiring Policies

Dulac has identified level control structure relationship typologies used to classify the relationship between each element in the control structure [158]. The links can be used to identify how each element is connected to each other and include:

- Reports Directly To
- Oversees
- Information Report
- Participates in Performance Appraisal of
- Fund Directly
- Coordinates With
- Is Co-Located With
- Appoints Personnel of
- Provides Procurement Services

A control structure that incorporates the relationships of contextual actors (such as unions, universities, or local government officials) might also contain these additional connectors:

- Trains
- Allocates Resources to
- Is Affected by Accident
- Lobbies

9.4.3 Controller Goals, Roles and Responsibilities:

The next step is to list roles and responsibilities for each controller in the control structure. The roles and responsibilities of each entity should include both performance-related responsibilities and safety-related responsibilities when applicable.

An example control structure with the roles and responsibilities for each element for a hospital is depicted in Figure 46. The relationship between each controller is detailed and labeled with the type of relationship. Engineers may wish to create separate control structure diagrams for each kind of relationship. For example, one control structure diagram could show funding relationships and another could depict organizational communication channels.

Table 13 Example Goals, Roles and Responsibilities for Controllers in Healthcare

Hospital Administration:

The hospital administration seeks to operate in a financially sustainable manner and facilitate the delivery of high-quality safe healthcare.

Third-party Payors:

Third-party payors seek to operate in either a profit neutral or profitable fashion.

Surgeons:

Surgeons seek to deliver high-qualify safe healthcare.

Nurses:

Nurses seek to deliver high-qualify safe healthcare.

Anesthesiologist:

Anesthesiologists seek to deliver high-qualify safe healthcare.

Patient: N/A

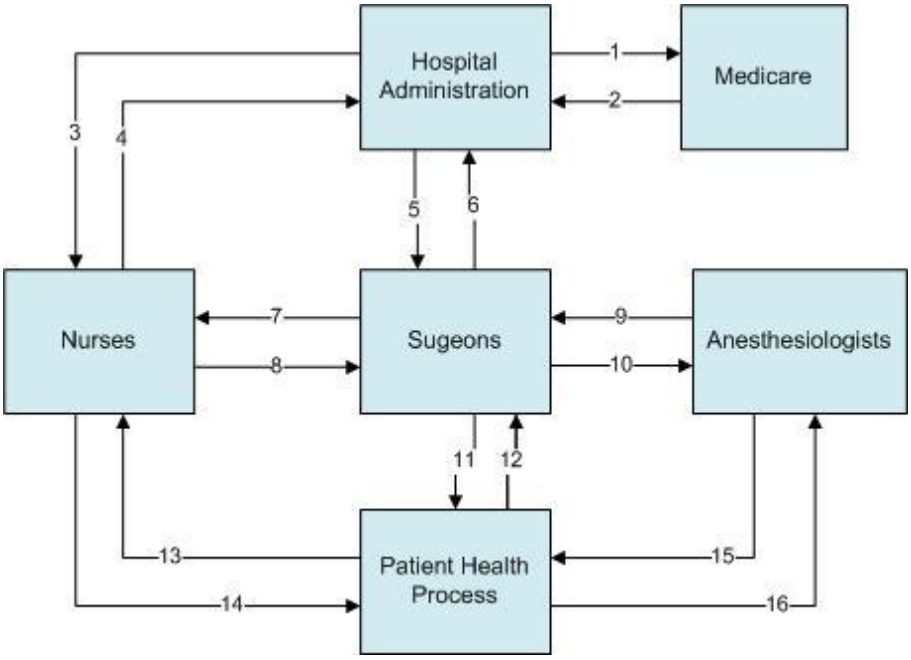

Figure 46 Healthcare Control Structure

Table 14 Example Healthcare Control Structure Interactions

1. Hospital Administration sends reimbursement requests to Medicare for payment rendered. Hospitals must also provide data for compliance with Medicare safety requirements. Hospital eligibility for Medicare funding is contingent on compliance with Medicare rules. [Funding Request, Subject to Performance and Safety Compliance by]
2. Medicare provides funding to Hospitals and assesses hospital accreditation status based on compliance with documented requirements. [Provides Funds for, Participates in Performance and Safety Appraisal of].
3. Hospitals employ nurses. Hospitals also monitor nurses' performance and safety statistics to ensure compliance with hospital standards and rules. [Hires, Participates in Performance and Safety Appraisal of].
4. Nurses provide data for hospital administrators to assess their performance and safety. [Provides data for assessment by]
5. Hospital administrators allow surgeons to use hospital facilities as contractors. [Permits Staffing and use of facilities]
6. Hospitals charge insurance companies for services rendered by surgeons. [Ability to charge for services]
7. Surgeons work with nurses. During surgical operations, the surgeon often gives directions to nurses. Surgeons also participate in assessment of nurse performance. [Coordinates with, participates in assessment of, Co-located].
8. Nurses can participate in assessments of surgeons. They also give surgeons updates regarding patient state and feedback about their own observations. [Coordinates with, participates in assessment of, Co-located]
9. Anesthesiologists provide patient status information to surgeons. [Coordinates with, participates in assessment of, Co-located]
10. Surgeons decide whether or not to involve anesthesia services in particular operations. [Decides involvement or not]
11. Surgeons can affect the patient health process through medical procedures. [Affects].
12. Patient status information is used to make decisions. [Feedback]
13. Patient status information is used to make decisions. [Feedback]
14. Nurses can affect the patient health process through medical procedures. [Affects].
15. Anesthesiologist can affect the patient health process through medical procedures. [Affects].

16. Patient status information is used to make decisions. [Feedback]

9.5 Third Stage: Controls and Inadequate Control Actions

Once the control structure has been developed, the next stage in the process is to identify *the controls* implemented by each controller in the control structure and the actions that could violate those controls.

9.5.1 Controls

A control is a mechanism that enforces safety constraints. Controls can be active, and manipulated by people. For any active control to be effective, all of the requirements for control must be met. Passive controls are those that a controller does not need to actuate to be effective. Examples of active and passive controls are provided below. Examples of controls are shown in Table 15.

Table 15 Example Controls in for the Enforcement of Safety Constraints

New System or System-level Change	**Controls**	**Industry**
Introduction of ADS-B	H: ADS-B communication link is inoperative and the position of ADS-B equipped aircraft is unknown SC: ADS-B communication link must be up for all time *t*. SC: Aircraft position (and time derivatives) state must be known for all of time *t* to X precision. Controls: * ADS-B avionics have independent power supplies so they can remain operable at all times. * Aircraft can be accurately tracked with multiple tools, including ADS-B, Mode-S	Aviation

	transponders, Radar returns and ground observation.	
Electronic Health Records	H: Operating surgeon has wrong information from EHR system. H: EHR system data is transmitted unencrypted. SC: EHR must contain, and make easily available, accurate patient data. SC: EHR data must be securely transmitted. Controls: * All patient health data is uploaded a secure cloud database. * Patient data is not stored locally on EHR display devices. * EHR data is encrypted with PGP encryption.	Healthcare
New Automatic Refinement Technique	H: Refinement technique exerts pressures on fuel tank beyond that which it was designed to withstand SC: New refinement process must not create pressures greater than designed tank pressure tolerances. Controls: * Operators can control pressure within the tank by opening outlet valves	Oil
Outsourcing Engineering	H: Engineering-Management communication is slow.	Aviation

	SC: Engineering-Management communication must maintained to the high standards that were in place before outsource change. Controls: Lead engineers and managers meet at each site every TBD days.	
Creation of Homeland Security Department	H: Key information regarding terrorist plot is held by disparate security agencies without adequate communication protocols. SC: Terrorism related data must be available to all terrorism-fighting national security agencies as per DOD policy. Control: Each piece of data collected by a security agency must be tagged with keywords. Regular DOD-wide database searches must be performed to combine relevant pieces of security data and form a cohesive picture of terrorist activities.	Security

An additional control from the detailed hospital example shown in Figure 46 is shown below.

Table 16 Continued Healthcare Example Control

Along connection 11, Surgeons have a safety control available to them to assess whether or not patient is high risk. If the patient is found to be high risk, surgeons are supposed to request anesthesiology support. The patient risk assessment screen acts as an active control.

9.5.2 Inadequate control actions

The purpose of the following step is to discover how each controller (actor or entity) could violate controls through inadequate control actions. The inadequate control actions are simple to find by referring to the responsibilities, safety constraints, and established safety controls for each controller

Continuing the healthcare example, inadequate control actions for a few of the controllers are shown below.

Table 17 Continued Healthcare Example Inadequate Control Actions

ICA1: Surgeon does not administer the patient risk assessment screen. ICA2: Surgeon administers the patient screen, but does not follow the procedure to request anesthesia support for the surgery. In this case the safety screen result is waived.

9.6 Fourth Stage: Context and Causality

9.6.1 Combining the guidewords with control requirements

The guidewords are used together with the control theory framework from Chapter 3 to together to find design flaws. The guidewords structure the technique to allow engineers to seek out flawed design (organization interactions, procedures and etc.) before they lead to inadequate control and hazards. The new hazard analysis method must identify *how*, for example, flaws in the mental models of humans or organizations can occur and *what* will lead to mismatches between reality and the mental model that adversely affects safety.

An example of how to use the guidewords for hazard analysis follows.

Individual Control Requirements**: Control Goal**
Guideword: **Pressures**
Human Error Taxonomy Item: **Incorrect Prioritization of Goals**

1) Identify pressures on the controller.
Typically encountered types of pressure can include schedule pressure, resources pressure, financial pressure, pressure to comply, and political pressure.

2) Determine how pressures on the controller can change over time; the relative influence of a particular pressure is dynamic and depends on other system states.

3) Determine how this set of pressures can change the initial prioritization of goals. If pressure can change goal priorities to be unsafe, then design changes should be made.
For example, schedule pressure, which is a dynamic influence, can lead controllers to value timeliness over low risk operations. Safety-related corners may be cut.

Revisiting the Building Blocks for SHOW

The relationship between the human and organizational factors highlighted in Chapter 3, the requirements for control, the error taxonomy, the guidewords, and the hazard analysis are depicted in Figure 47.

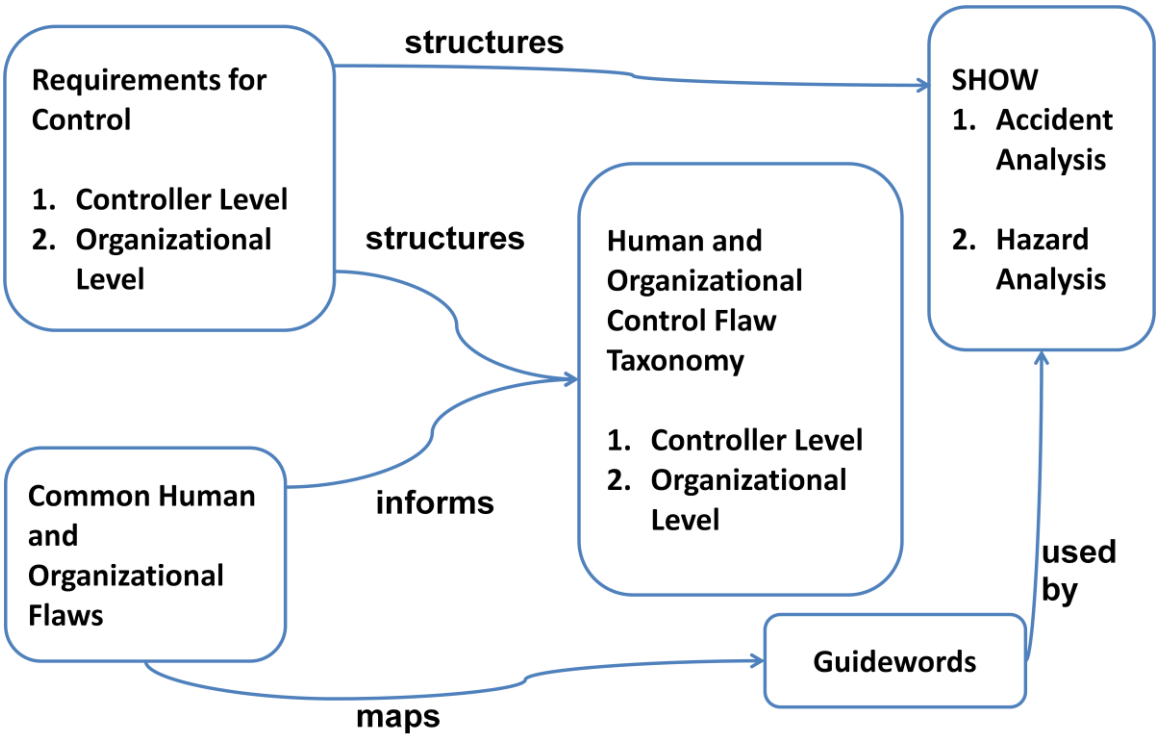

Figure 47 The Hazard Analysis Building Blocks

The descriptions of the human and organizational flaws in section 3.6 provide a thorough description of the human-centered phenomena associated with accidents. The common human and organizational flaws inform the categorization and taxonomy of human and organizational errors. The requirements for control described in 3.5 provide the structure and backbone for the human and organizational control flaw taxonomy. The taxonomy in section 3.7 provides a complete hierarchical categorization of control flaws.

The guidewords presented in section 5.3, which are based not on control theory, but on the context we analyze, are derived from the common human and organization flaws.

The guidewords bridge the gap between the taxonomy and the hazard analysis process. They are used to drive the hazard analysis process forward. Together, they provide a systematic and practical way to find conditions, states and situations in the system design that can lead to flawed control actions or the poor decisions itemized in the taxonomy.

9.6.2 Design Analysis of Context for Human and Organizational Inadequate Control

Once inadequate control actions are identified, the hazard analysis can be used to find human and organizational flaws in the system design. In practice, engineers may wish to list all inadequate control actions for a particular controller, or all controllers, before moving onto the discovery of causal factors. Alternately, engineers can switch between ICA identification and analysis in whatever way makes sense to them. For clarity, the hazard analysis approach described below is ordered using the control requirements; the ordering does not imply any step sequence for the hazard analysis application.

An example application of the method from one of several industries is given following each control requirement analysis description. The method is not domain specific, as emphasized by its application to systems from several industries.

9.6.3 Hazard Analysis of Individual Controllers

Building from the control requirements for individuals shown in Table 6 and the human error taxonomy starting on page 108, the hazard analysis of individual controllers is shown below. The analysis describes a high-level process for finding flaws and hazardous scenarios related to each individual-level control requirement.

Control Goal Analysis

The section demonstrates how a controller's goals can be examined to ensure that they are adequate to enforce safety constraints: the wrong control goals can lead to inadequate control actions and allow hazards to occur. Consideration of each controller's goals (be they low-level operators or high-level managers) is essential to assure safety. To understand how control goals influence safety, it is important to consider how the goals interact with the rest of the system. For example, the sufficiency of control goals can be assessed by identifying *incentives* that can weaken safety-related goals and increase risk.

Analyzing goals and the context in which goals are formed, influenced, and communicated throughout the system is critical because safety is formed by interactions within the system— not by components alone.

1. From the roles, responsibilities, and safety constraints for each controller, identify and list all the controller's control goals.
2. Ensure that the controller has a control goal associated with the enforcement of each safety constraint. This is also known as a "gap analysis."

   If the controller does not have a control goal associated with each safety constraint or safety requirement, inadequate control actions could occur. Refer to taxonomy item 1.1.
3. Analyze the collection of controller goals (both safety-related and performance-related), and identify any goals that conflict with each other.

   Goals related to the requirements and safety constraints may conflict. A safe system is not necessarily free of goal conflicts, but safety engineers should take them into account to ensure that the correct priorities are established to avoid accidents. Refer to taxonomy item 1.2.
4. Identify the controller's prioritization of goals.

   Controllers typically try to achieve several goals at once. The change of relative goal priorities is an important concern for socio-technical systems. Over the operational life of the system, controllers must correctly prioritize their control goals in order to meet performance requirements, safety requirements, and safety constraints. Refer to taxonomy item 1.3.
5. Establish the mechanisms for how goals are formed and influenced for each controller over time and in all situations.

   Use the guidewords or refer to the hazard guideword matrix to analyze the controller's context and system design to discover how a controller's goals are formed initially and influenced over time.

Throughout this section, a healthcare example will be used to demonstrate the feasibility of the method. The example will focus on a few specific controllers or system aspects, and should not be considered a full healthcare analysis.

Recall the description of ambulatory surgical care setting first described in Chapter 8. This example will examine the control goals of the surgeon.

1. Goals:

Provide care that is:

1. high quality,
2. safe,
3. efficient, and
4. minimize non-reimbursable costs to the hospital.

2. The safety constraints for a surgeon include:

Knowing that healthcare is a risk-risk system, wherein each activity brings a certain amount of risk to patient safety if is performed and even if it is *not* performed. If performed, a surgical procedure risks complications that can harm the patient. On the other hand, if a patient needs the procedure to treat their ailment and it is not performed, they may suffer harm from their condition. Therefore, the surgeon's safety constraint in a risk-risk system is: Surgeons shall not engage in activities that expose patients to a higher than anticipated and accepted level of risk.

In this case there is a control goal (safe care) associated with each safety constraint.

3. Using the guidewords 'resources' and 'pressures,' we saw in section 8.5.2 that the goal to provide safe care can conflict with the goal to provide efficient care. As the healthcare system has become overburdened, it has become critical for care to be delivered efficiently so that hospitals may continue to operate sustainably. Furthermore, a delay in the delivery of care to critically ill patients can result in great harm to patients. Potential conflicts can arise when safety is compromised in order to treat the full caseload assigned to a surgeon.

4. Safety is the top priority for surgeons. However, because the relationship between safety and the achievement of other goals can be unclear when pursuing care strategies, safety can be unknowingly compromised. More than just the correct goal priorities must be in place for surgeons. The implemented control strategies must reflect surgeon's desired goal priorities.

5. Applying guidewords 'history' 'training' 'pressures' and 'resources':
The surgeon's goals and their relative priorities are formed initially in medical school and through their formal training. As they gain experience and practice within a hospital setting, they may be pressured to emphasize cost-containment and efficiency goals. Hospital documents and procedures all state that safety is the highest priority. However, other pressures and incentives emphasize non-safety related goals, such

as the lengthy schedule assigned to each resident. Little hospital communication or training exists to help practitioners address conflicting goals.

Control Algorithm Analysis

This section demonstrates how a controller's control algorithm can be examined to ensure the enforcement of safety constraints. An inadequate control algorithm can lead to inadequate control actions and allow hazards to occur.

1. Identify the process(es) under control.

   To develop an adequate control algorithm, controllers must know what process(es) they are responsible for and what the boundaries for those processes are. If the process boundaries are unclear to the controller, significant control gaps (or overlaps) between controllers can occur. Additionally, assigned control responsibilities are not static; identify all control responsibilities that could fall to a controller in certain situations at certain times. For example, during an emergency, a controller may be responsible for additional processes.

2. Identify the control algorithm for each process under control and determine its ability to enforce safety constraints by using the guidewords.

   This step allows safety engineers to evaluate the control algorithm's adequacy for controlling the process. Identification of the control algorithm must include identification of the control levers and analysis to ensure that the range *of each control lever used in the control algorithm matches its* capabilities. *The control algorithm may be encoded in procedures, checklists, or training materials. Use the guidewords to assess the adequacy of the control algorithm and how it is influenced by the operating context.*

Assessment of the control algorithm should include the following:

2.1. Determine if the controllers understand their ability to affect the process.

Controllers must have the ability to take actions and make decisions that achieve system goals and enforce safety constraints. Controllers must have an adequate understanding of the algorithm, control levers and relevant tools available to them. Use the guidewords or hazard matrix to analyze how the control algorithm is learned and how controller's understanding can be affected.

2.2. Determine how control inputs affect the controller's control algorithm.

Unexpected control inputs can act as disturbances to the process. For example, a surge in demand (which serves as a control input) can put pressure on the controller to skip steps in order to meet output expectations. Use the guidewords or hazard matrix to aid this analysis.

2.3. Determine if the control algorithm is compatible with and executable by controllers.

There are several factors that can render a control algorithm incompatible or un-executable by humans. Use the guidewords or hazard matrix to aid in this analysis.

2.3.1. Ensure that control action can be executed if actuator failure or communication failure occurs. Analyze all execution and communication channels in the control loop for failure or delay.

The medium used to transfer the control action selected by the controller and the actuator can include email, telephone calls, voicemails, mail, memos, gestures, callouts, and physical cables. The robustness of each medium and technology must be assessed to ensure that commands and directives from the controller are communicated to the actuator and similarly information from the sensor is communicated to the controller.

2.4. Analyze change processes for the controller algorithm.

Control algorithms must evolve as goals change, priorities change, or more is learned about the process. It is important that these changes be evaluated for safety. The guidewords and hazard matrix can be useful in evaluating how the control algorithm can be influenced and change over time.

Continuing with the healthcare example, analysis of the surgeon's control algorithm:

1. The process under control is performing certain surgical procedures and related treatment planning.

2. Before surgery takes place, surgeons are responsible for treatment planning. Once the procedure has been decided upon, hospitals assign the roster of patients to surgeons and allocate the number of anesthesiologists available.

Surgical procedures are usually performed by a team consisting of the surgeon, one or more nurses, and an anesthesiologist. However, for some surgical procedures, the use of an anesthesiologist is discretionary. A surgeon may choose to manage the surgical procedure him or herself and direct a nurse to manage the sedation medication. However, for patients that are at a high risk for complications, the use of an anesthesiologist is mandatory. To determine if an anesthesiologist is required, a safety screen is administered. The screen consists of a series of checks, including blood pressure and age, to separate high risk from low risk patients. If a patient is found to be high risk, surgeons must wait for an anesthesiologist to become available before the surgical procedure begins. These waits can be long.

Surgeons also have the ability waive the use of the screen (not perform it at all) and determine for themselves if the patient is high or low risk, or to ignore the results of the screen and decide if an anesthesiologist is truly required.

Within the operating room, surgeons are responsible for the performing the procedure and directing a team of colleagues to assist as well as coordinating with other medical professionals such as an anesthesiologist. During a procedure, the speed at which the procedure is performed is largely up to the surgeon, although the nurses must be able to comply with the increased pace.

2.1 – 2.5 Analysis: Guidewords are applied to assess the control algorithm.

2.1 Surgeons never wish to contribute to an adverse event. Nevertheless, in an effort to move quickly, their behavior causes an increase in the rate of adverse events. Surgeons waive the safety screen and rush procedures due to an incomplete understanding of the how their unsafe behaviors aggregate to create a high-risk hospital environment. In many cases, a rushed or waived case does not result in a serious adverse event. If the risk of an adverse event is low, and an unsafe decision doubles the risk, the overall low rate will still be low. A better indicator for risk may be what is called ‘micro events,’ such as certain blood pressure fluctuations and patterns that indicate a stressed heart. Healthcare IT can be used to monitor surgeries for these kinds of events.

2.2 A dominating control input that influences surgeon’s behavior is the operating room schedule for the day. Surgeons feel pressured to work at a higher pace than they wish to. As the day wears on, surgeons may feel more and more time pressure and choose to rush cases.

2.3 The control algorithm is compatible with controllers, but inadequate. Surgeons have no way to withstand the pressures to waive safety screen and rush the procedure. They have incentives that push them to pursue cost containment and efficiency over safety. The surgeon has the ability to make decisions (e.g. waive the safety control or rush the procedure) that violate the safety constraint to deliver care at low risk. To better enforce the constraint, the surgeon should not be permitted to waive the safety control. If the safety control is too conservative, and labels too many low risk people as high risk, then a better safety control should be created. To prevent surgeons from rushing the procedure, engineers have several options, including empowering the nurse to report surgeons that rush. The use of video recordings is another potential solution.

2.4. Communication, Resources: Surgeons convene for department or unit briefings on a monthly basis. Surgeons may change their control algorithm on their own, and share their results with their colleagues during meetings. Monthly meetings are also used to discuss adverse events and poor outcomes in order to learn from them. Surgeons are more or less autonomous in making changes to their control algorithm, and as such, are often put in the position of dealing with, and responding to, inputs from other controllers, such as hospital management. For example, hospital management may increase the patient subscriber base, or increase the patient load for the week, without providing surgeons additional resources to treat the increased patient load.

Controller Process Model Analysis

This section demonstrates how a controller's process model can be examined to ensure safety constraints are enforced.

1. Determine what the controller's process model is. The process model includes:
    - A model of the process under control: An adequate model of the process under control includes correct process boundaries, a model of how inputs are transformed into outputs, and an assessment of current process state.
    - A model of each control element in the control loop: An adequate model of each control element (actuators and sensors) includes their current state, an understanding of information timeliness and uncertainty, and how control elements can be impacted by disturbances.
    - A model of how the process interacts with, or is impacted by, influences outside the control loop via outputs, inputs, and disturbances.

    The controller's process model can be described with text, system dynamics, or tools like SpecTRM.

2. Assess the controller's process model, and discover any gaps or inaccuracies in it. Use the guidewords to drive the analysis. In particular:

2.1. Find flaws related to process boundaries.

Determine how a controller comes to understand the process boundaries. What information sources does the controller use? How is an adequate understanding of the process boundaries maintained and updated? Use the guidewords to determine how the controller's understanding of process boundaries is formed and influenced.

2.2. Find flaws related to a controller's understanding of how inputs are transformed into outputs.

Verify that the controller's mental model of the process includes process dynamics and an understanding of how delays affect process state. Controllers often need more than an "input/output" model of the process. For example, if the process under control contains feedback loops, the same input will not necessarily produce the same output.

Identify the controller's sources of information for creating a model of how the process transforms inputs into outputs. How is an adequate understanding maintained and updated? Use the guidewords to determine how the controller's understanding is formed and influenced.

2.3. Find flaws related to the controller's assessment of current process state.

Identify the controller's sources of information for creating a model of current process state. How is an adequate understanding maintained and updated? Use the guidewords to determine how the controller's understanding is formed and influenced.

2.4. Find flaws related to the controller's model of a control element.

If a control element in the controller's control loop(s) is human, that control element will have their own goals and constraints because they too are controllers, albeit at a lower-level of control. The controller's goals may conflict with those of human control elements. If these conflicts are not known or properly addressed, unexpected behavior can occur. Understanding the goals and constraints of human control elements can help the controller create a model for how they will react to commands and what kind of feedback they will give. Determine if the controller can identify human control element's goals and safety constraints.

A model of the control elements can also include a model of the timeliness and uncertainty with regards to control element performance. For example, a controller's model of an actuator can include how long certain commands will take to be executed or if they will be executed at all.

Disturbances can also affect the performance of a control element. For example, a disturbance that can affect actuator performance can include: actuator is unexpectedly called away to perform some other duty.

Identify the controller's sources of information for creating a model of the control elements. How is an adequate understanding maintained and updated? Use the guidewords to determine how the controller's understanding is formed and influenced.

2.5. Find flaws related to control loop inputs, outputs, and disturbances.
Process inputs, disturbances, and outputs from other parts of the system can impact the process under control. These inputs can come in the form of technical resources, such as electrical power, or human resources, such as operators. Disturbances to the process can include the unexpected sickness of operators. Absent workers can decrease the rate at which work is performed or the quality of process outputs (work delivered).

Being purely reactive to process outputs (operating in pure feedback mode) means that the controller (and thus the system) may be sluggish in response to disturbances. If the controller has a model for what disturbances can be expected and how they can affect the controlled process (as well as the actuator, sensor, and communication links), the controller may use a feed-forward control algorithm and achieve faster responses as well as develop a more robust control algorithm. The controller should be able to identify types of disturbances and have a model that includes their frequency, amplitude and duration.

Identify the controller's sources of information for creating a model of process inputs. Adequate understanding can include both identifying and having a model for expected process inputs, outputs and disturbances. How is an adequate understanding maintained and updated? Use the guidewords to determine how the controller's understanding is formed and influenced.

2.6. Assess the functioning of the control loop for feedback, and communication flaws. Verify that feedback is present and compatible with the controller. In particular:

2.6.1. Verify that needed controller sensor data exists.

Missing feedback is a common design flaw.

2.6.2. Verify that needed feedback signals are not nulls.

Humans do not notice nulls signals and will not be update their process models with them.

2.6.3. Ensure that feedback signals or measurements are strong enough to overcome a conflict with current mental model.

2.6.4. Ensure that feedback signals or measurements are trustworthy.

2.6.5. Ensure that the process model is robust to a misread measurement (a slip).

2.6.6. Ensure that the process model is robust to disagreements between various information and feedback sources.

2.6.7. Verify that needed feedback signals are not high-order derivatives.

High order derivatives are difficult to integrate to determine current process state.

2.6.8. Verify that feedback is not susceptible to unplanned for, or un-designed for, time lags that could delay important information.

2.6.9. Verify that the commutation channels have sufficient bandwidth. Analyze channels in the control loop to determine how they can be negatively influenced. Use the guidewords to determine how execution and communication channels can be compromised.

In the case of human and organizational system, sufficient bandwidth for an information source can mean that the information source is important enough, or that the controller has sufficient resources to monitor and pay attention to it. For example, feedback from a low-ranked employee may not get to the relevant controller if they communication channel is not valued by the controller.

2.6.10. Analyze the system for the impact of sensor failure.

If the sensor-person in charge of providing needed system information to the controller does not, or cannot, do so, the controller's process model may be affected. Determine what design provisions are in place, if any, if the sensor fails. At minimum, there must be a way for the controller to be notified if the sensor-person is unavailable.

2.6.11. Analyze the system for the impact of actuator failure or delay.

If the person in charge of implementing or executing the controller's decision or plan does not or is not able to do so, the control action will not be executed. This

can affect the controller's process model. Determine what design provisions are in place, if any, if this occurs. At minimum, there must be a way to notify the controller that the actuator-person is unavailable. Risk assessments can be performed to determine if actuator failure is a concern that must be addressed.

Continuing with the healthcare example, analysis of the surgeon's process model:
The surgeon's process model includes:
A thorough assessment of patient health and risk: Surgeons view patients with certain factors (e.g. high blood pressure, overweight) to be high risk for complications.

The screening tool: Surgeons have reported that the screening tool is inaccurate and that they consider its use to be a waste of time. The tool identifies (what surgeons view as) low risk patients as high risk; causing the surgeon to wait around for (seemingly) unneeded anesthesia support.

Themselves: Surgeons consider their own assessment of patient risk to be superior to that of the screening tool.

Lower-level Controller: Nurses: Colleagues that help manage the case under direction from the surgeon. The relationship between nurses and surgeons is important. Surgeons believe that better nurses are assigned to practitioners that are able to meet hospital throughput desires and perform revenue-favorable cases.

Coordinated Controller: Anesthesiologists: Colleague that manages the sedation component of the case. The wait for anesthesia support can be very long. Floating anesthesiologists never seem to be available. Their assistance is not necessary for low risk cases.

The unavailability of a needed anesthesiologist can act as a disturbance to the surgeon's process. Because of the disturbance, the surgeon may choose to proceed without the anesthesiologist, or the surgeon may wait.

Control Inputs: The patient schedule. The weekly schedule of patients is constructed by administration.

Process Outputs: Treated patients. Generally, surgeons are not involved with the process outputs after the conclusion of the case. In particular, surgeons do not know if a patient develops a complication from the

procedure. Complications may be treated by another surgeon in the unit, another provider at the hospital, or at a different hospital all together. When the safety screen is waived or the procedure is rushed, they do not have a feel for the risk to patients post-surgery.

Assessment:

2.1, 2.3: One of the major flaws of the process model is the surgeon's view of the boundaries of the process output. Surgeons view surgical success in the short-term, when the surgeon is 'done' with the process at the close of the procedure. A longer-term view that included recovery (when complications can appear) would give the surgeon accurate feedback regarding the surgical success how well the surgeon performed the procedure and assessed patient risk.

2.2: The surgeons, as a group, may have more control over the surgical schedule than they think. If surgeons move away from a fee-for-serviced pay structure, their schedule may not be so overloaded. Furthermore, schedule approval by a safety professional might introduce needed resistance to the force to treat more and more patients.

2.3: With respect to the surgeon's judgment and the quality of the screening tool, the surgeon has an accurate process model. The tool is in need of improvement.

2.4: The surgeon is not able to forecast when the anesthesiologist will be busy. The surgeon doesn't have a predictive model that can show anesthesia availability throughout the day. If the surgeon knew that anesthesia support would not be available, he or she could reschedule procedures rather than operate unsafely.

2.5, 2.6: As stated previously, the surgeons do not have an accurate assessment of the impact that waiving and rushing has on aggregate hospital safety. The surgeons do not seem to have a sense of the flow of patients that experience an adverse event, and are not rewarded or incentivized to discover this kind of information. If surgeons had to treat their own complications, then they would have a reason to have a better understanding of the input and output of the patient safety process.

Tools: Surgeons are not given tools to anticipate or deal with unexpected delays or disturbances. If, for example, a patient takes a lot longer than expected to treat, then the schedule should be lightened for the rest of the day. Otherwise, the surgeon will either be working tired or needing to rush to get through the

rest of the schedule. Surgeons do not have a sense of the risk that the rest of the unit faces throughout the day.

Tools: The hospital does not use risk-based scheduling-scheduling that would grade the risk so that surgeons did not face high-risk patients at the same of time of day, which can lead to resource shortages. Anesthesia support scheduling should include a model of procedure risk and patient risk so that the anesthesiologist does not have times of unavailability when they are needed. Furthermore, patient risk-based scheduling would increase the overall utilization of the anesthesiologist and eliminate expensive (long) periods of non–utilization.

History: The surgeon's model of the process comes from experience.

Communication: Better communication channels should exist between surgeons and management. The information that surgeons have regarding anesthesiologist wait times and the surgeon's view of the safety screening tool should be communicated to management. In turn, management should educate surgeons regarding adverse events, and should change the management's policies regarding pay and adverse events. Benefits should go to surgeons with the least adverse events given a certain riskiness of patient.

Communication: Hospitals use memos to keep surgeons informed of adverse events and team meetings. These communication methods do not have the quick feedback that surgeon need in order to understand the impact of their own decisions on patient safety.

Controller Model of the Organization

This process step examines the controller's model of the organization.

1. Identify the controller's model or the organization which includes knowledge of the controllers that influence their own process and goals of those individuals or groups

2. Assess the controller's model of the organization. In particular:
   2.1. Ensure the controller can identify how influencing (other) controllers impact their own control including controllers that:
      - provide needed control and process inputs.
      - provide needed information.

- use the outputs of their controller process.

A model of the organization should include entities that directly impact the controller's process.

2.2. Ensure the controller knows how to access other controllers in case he or she:

- Needs to ask questions about control of their own process.
- Needs to ask questions about control of some other part of the system.
- Encounters a novel situation and require help.
- Discovers information or data that should be communicated to other controllers.

Inadequate control can occur when the controller does not understand the relationship between the process being controlled (the local control loop) and the rest of the system. An understanding of who impacts their control loop and how other people in the system impact their own control helps avoid potential ICAs. For example, a high-level view of the system control structure helps prevent detrimental local optimization.

Furthermore, knowing who to contact, and how to reach him or her, is essential. Each person in the organization acts as a sensor for information that could indicate risk migration or the violation of a system safety constraint. In particular, it is essential to ensure that controllers are aware of how to contact and communicate relevant safety information to the safety management group.

2.3. Assess how the mental model of the organizational structure may be formed and influenced over time.

Use the guidewords to aid in this analysis.

Continuing with the healthcare example, analysis of the surgeon's organization model:

The controller's model of the organization is:

The hospital: Surgeons are aware of the different groups within the hospital that either affect their own process or who they may need to reach out to, including the quality review committee. In the surgeon's view however, the quality review committee is not a helpful one to bring their throughput concerns to—it is staffed by people whose compensation is tied to productivity. Anonymous reporting is also available to the surgeon, however it is only used for low level issues rather than systemic problems, such as throughout pressure [169]. Surgeons feel they are pressured by the hospital through various means (e.g.

higher priority access to operating rooms or the best nurses to highly productive surgeons) to compensate for financial pressures from outside the hospital by cutting corners and overloading the schedule [169].

Assessment:

Training/Communication: The surgeons' model of the organization reveals several organizational flaws that should be resolved to ensure safety. In particular, the surgeons are not aware of groups within the hospital that could allow them to address their problems with the scheduling and operations groups. In particular, surgeons do not receive training on hospital operations or administration. It is left up to interested practitioners to learn how the hospital is administered.

The control structure that the surgeon has in mind serves as their mental model of the organization. Their control structure is informed by policies, memos and emails, mediums that seem to be adequate. Surgeons are informed of the groups in the organization they can contact, even if surgeons don't view these groups as very effective.

Decision-maker Coordination Analysis

This process step demonstrates how to find hazard scenarios associated with inadequate coordination between decision-makers. Inadequate coordination between decision-makers can arise when multiple people are jointly responsible for control of a process.

1. Identify decision-makers who are jointly responsible for the control of a process.

2. Assess the controller's coordinated control. In particular:
   2.1. Identify the kind of communication and data-sharing necessary to perform the task. Identify mechanisms for delegation and temporary assignment of duties within the coordinated control arrangement.

   While both people may be jointly responsible for a controlled process, the controllers may divide up certain tasks between them. The process used to assign control responsibilities can go awry and lead to hazards.

   2.2. Use the guidewords to discover how communication, delegation, task sharing, and other aspects related to controller coordination can be influenced.

Continuing with the healthcare example, analysis of the surgeon's coordinated control process:

In the GI ambulatory unit, nurses, surgeons and anesthesiologists are jointly responsible for the health of the patient during surgery.

Assessment:
Each member of the surgical team has tools to monitor the patient. They communicate verbally and have established CRM practices that work well. The flaws in their coordinated control arise when mismatched personalities are teamed together. For example, if the surgeon is working a pace that is potentially unsafe, nurses may push back and insist that the pace is slowed down. However, when a pushy and fast surgeon is teamed with a deferential nurse, the pace pushback may not occur.

Auditing Individual Controllers

The hazard analysis described in this section should be performed periodically, however, like all hazard analysis methods, this method provides a process to frequently to assess current system state. An audit should be tailored to each particular system it is applied to, but any audit should include questions that verify each requirement for control is met. As an example, the following questions could be used to elicit the state of the system and verify that individual controllers are meeting the control requirements.

Audit an individual's goals:

- What are your goals and can you expound on their relative importance.
  If possible, verify this (using observation studies, or other data collection methods) through the actions of controllers.

- What do you think your higher-level, peer and lower-level individual controllers view your goals and safety constraints to be, and how do you rank their importance?
  Oftentimes asking someone what he or she supposes others think *about a situation gives a more accurate answer than a self-assessment.*

- Do your procedures and training include explanation of controller goals, safety constraints and how your control of the process can impact safety?

Audit an individual's control algorithm:

- How do you do your job? How does the way you perform your job differ from stated procedures?

- Do you rely on backup or redundant systems as part of doing your job?

Audit an individual's process model:

- What time delays exist in the system that make your job hard or impact safety?

- Can you create a model of their process?
  Such a model could include all process inputs and outputs, a description of the process responds to commands or directives and how each control element behaves.

- Can you identify the processes controlled by others and identify the controls and feedbacks and communications between you and other controllers?

Audit an individual's model of the organization:

- Can you draw a control structure?

Audit an individual's coordinated control:

- Who else do you share control duties with? How do you divide tasks and coordinate control?

9.6.4 Hazard Analysis of the Organization

The following analysis steps consider the entire organization and are performed at a higher level of abstraction than the analysis of single control loops and controllers.

Organizational Goal and Role Assignment Analysis

The purpose of the analysis described in this section is to find flaws related to the organization's assignment of goals, roles, and responsibilities.

1. Identify each safety-related requirement and constraint. Map the fulfillment or enforcement of each requirement and constraint to processes and controllers in the control structure. Examine control boundaries for gaps and overlaps. Ensure that the control of each process has been assigned and that control handoff design is adequate.

This step can be used to find gaps, overlaps and conflicts in the assignment of roles and goals throughout the organization. Accidents can occur due to gaps and overlaps in the roles and responsibilities of controllers. Analyze the people in the control structure periodically to ensure that control authority allocation is adequate and that roles are correctly assigned. This could be accomplished by comparing formal documents to interviews with individuals within the organization.

2. For processes that are controlled by multiple people, ensure that the goals for each controller are not conflicting, or ensure that the relative priorities of conflicting goals are known and understood by all relevant controllers.

3. Analyze the roles and responsibilities assigned to controllers and ensure that they are appropriate for human control.

   Human factors analysis can be performed to ensure that the workload entailed by the assigned responsibility is not too little or too much. The use of monitoring should also be carefully considered in this analysis. Humans are usually bored by monitoring tasks, which can lead to inadequate control.

   Certain control responsibilities are better suited to particular individuals or groups. For example, safety-related activities such as risk assessments and the issuance of safety-related waivers should be performed by safety personnel rather than production staff. Safety-related decisions are best made by qualified safety personnel who do not have incentives to cut safety corners in favor of production.

4. Use the guidewords to analyze the system and organizational change processes to determine how the assignment of roles and responsibilities can be influenced or changed.

The example for this section is from the field of Aviation: Air Traffic Control [164][165].

1. Safety Constraint: Maintain separation of air traffic within the ARTCC area.
Controller: Air Traffic Controller
Process: Air traffic controllers look at aircraft flight plans and current headings and altitudes to anticipate upcoming conflicts. To avoid loss of separation, air traffic controllers direct aircraft to specified headings at specified altitudes. To slow aircraft down, controllers will often direct a pilot to make a left turn at, for example, 15 degrees, and then a right turn at 15 degrees.

Handoff procedures: Handoff procedures are followed to maintain aircraft separation during shift changes. The procedure is this: The outgoing air traffic controller (controller A) waits for air traffic to settle down, and then briefs the incoming controller (controller B) on the current sector status. Controller B then takes over, while controller A remains and monitors the sector until controller B informs controller A that controller A is no longer needed. This period typically does not last more than a few minutes. After this period, controller A leaves the area.

Analysis Guidewords: Tools and Interface, Communication, Human Cognition Characteristics
This process is not compatible with human control.
Background: Controllers have several tools available to them during active control, including monitors with a map of aircraft displaying altitude and headings and a list of aircraft with identifying information and flight plan. During normal control, controllers will command a pilot to change their course or change to a new radio frequency channel. Controllers rely on verbal feedback from pilots to ensure that the command was heard and will be followed. If a long period of time passes without acknowledgement, controllers should repeat the command. Without an acknowledgement from the pilot, the controller should try to investigate what is happening with the pilot.

The new controller relies on the displays and the verbal briefing from the old controller to come up with a model of the system state. The procedures for what is discussed during shift changes are flexible, and controllers do what makes sense to them. Because missing pilot acknowledgements are a lesser priority than de-conflicting aircraft, controllers may not mention missing acknowledgements during controller transition periods. Additionally, there are no tools to display controller-pilot interaction history so that missing acknowledgements could be brought to the controller's attention. Therefore, Controller A is not able to transmit their full process model to controllers coming on shift. If the new controller's process model does not match the old controller's process model, there is a danger of inadequate control.

2. The control of airspace is divided into sections. The overall process of maintaining aircraft separation is divided between several roles within air traffic control that are each controlled by one or more individuals. When traffic gets heavy, additional controllers are added to each sector.

3. Controller workload analysis:
The workload for controllers is very high. To compensate, shifts are usually only 30-90 minutes long. Without maps that show current flight paths, controllers must mentally project flight paths and potential conflicts from a list of waypoint acronyms and current headings represented by lines. The organization

has recognized the difficulties of the job and the NextGen system promises additional tools to address controller workload.

Analysis of Organizational Functional Interactions

The purpose of this analysis is to discover flaws related to the organizational (controller) functional interactions.

1. Create a diagram showing the control structure for:
   - Control of value delivering processes and safety processes
   - Budget setting
   - Staffing Decisions
   - Pay
   - Information: Reports, Commands

   The intra-organizational interactions of organizational functions are determined by control over processes, budgets, staffing, resources and etc. To avoid the compromise of safety-related control, control over safety-related groups should be at a high level in the organization and independent from the production-related groups

2. Use the control structure to identify organizational dependencies within the organization (e.g. hiring and pay).

   This analysis will help to find conflicts of interest and ensure that they do not lead to unsafe conditions.

3. Use the guidewords to identify mechanisms for the controller hierarchy to be influenced or changed.

The example for this section comes from pharmaceutical safety as described in Couturier's Thesis [166].

Background: The FDA is underfunded and has more oversight and inspection work than it can manage. As the organization became more and more cash strapped, it began to create a backlog of new drugs submitted for approval. To hire enough safety officials to approve or reject drugs, the FDA introduced a new method to pay for the tests. Rather than being funded by the FDA, the FDA began to charge drug companies for the approval process. This policy became known as 'pay to play'.

Guideword Analysis: 'Incentives/Pressures',

The control over the analysis of the drug was done by safety officials. These safety officials were influenced by the operations staff of the FDA and by the drug companies themselves because their own salaries were being paid by the fees for the approval. The fees paid by the drug companies put pressure for fast approval on the FDA. This policy blurs the safety management aspects of the organization with the financial parts of the organization.

Analysis of Organizational Resource Allocation

The purpose of the analysis described in this section is to find flaws related to the organization's allocation of resources.

1. Identify the resources needed by each high-level controller to achieve their performance goals and enforce safety constraints.

   Examine the organizational processes to ensure that needed resources are available to each controller at the time they are needed. Without adequate resources to perform the job, controllers may be forced to compromise, which can affect, for example, delivered product quality, on-time delivery, or safety-related task performance (e.g. maintenance). This step can be performed iteratively, so that the analysis moves from high-level to low-level controllers.

2. Analyze the control structure to determine how resources flow throughout the organization. Ensure that conflicting interests do not cause a shortage of resources of safety-constraint enforcement activities.

   Controller's whose primary activities are safety related should not be subjected to budgets that are tied to production metrics (e.g. sales). During down times in an organization, safety practices are even more important to maintain. The budgets for safety-related activities should be established by top management.

3. Use the guidewords to determine how resources budgets and distribution can be influenced. Organizational change processes must be analyzed to ensure that changes to resource budgeting (e.g. financial, staff) for safety-related activities cannot be eroded without a safety assessment.

The example for this section continues the healthcare example from 8.5.2.

Guideword Analysis: 'Pressures'

One of the chief resources needed by surgeons to safely perform procedures is time. However, by attempting to minimize costs, the organization puts pressures on surgeons so that they do not have enough time to perform procedures safely. Organizational decision makers who are aware of the hospital's financial needs, but do not understand the impact of time shortages on patient safety, apply time pressure to surgeons.

The time pressure is passed from hospital administration through to surgeons by assignment of the best resources to the most productive providers. At the end of every week, a nurse manager examines the blocks of time assigned to each surgeon and ranks him or her according to utilization and completion of cases. Utilization is examined weekly and monthly. Surgeons with high utilization are assigned preferential blocks of time, their preferred team of nurses and other resources. Surgeons, who use average procedure times to create the weekly schedule, feel pressure to complete all cases they are assigned for the day, even if some cases take longer than planned. As my data analysis at a major teaching hospital in Boston has shown, this leads to high risk operations however, because the actual distribution of surgical time varies widely by procedure: any one gastrointestinal procedure may take between 10 minutes and several hours.

Analysis of Organization Communication Channels

The purpose of this step in the hazard analysis is to find flaws related to organizational communication channels and processes.

1. Verify that the organization has ensured each controller's understanding of high-level system safety information including the system goals and system safety constraints.

2. Identify communication channels within the organization. For example, communication mediums can include email, voice, mail, reports, and gestures.

3. Identify all people and groups that could potentially be affected by an accident and ensure that communication channels are able to deliver safety-related information to those groups.
   It is important to inform outside groups (such as citizens near plant where hazardous chemicals are made) of the potential hazards and what to do in emergency situations.

4. Determine the importance of each channel and the priority of the channel as viewed by the sender and receiver.

The priority of the communication channel will determine when the information will be examined, and how it will be treated. Safety related information should be communicated on high priority channels.

5. Examine the timeliness of messages transmitted within communication channels.
   Ensure that communication channels do not have a single point of failure. Time-critical safety-related information should not be communicated asynchronous methods such as voicemail or text message. If using such a method, an acknowledgement of understanding the information contained (not just receipt) should be sent back to the sender.

6. Use the guidewords to assess the adequacy of organizational communication channels and determine how they can be influenced.

This example draws from the Citichem plant described in 8.5.3 and described in detail in [167].

Guideword Analysis: History/Culture, Resources, Safety Culture

Communication in the Citichem organization was ineffective. The communication mechanisms within the plant consisted of small group meetings and phone calls. Regular communication between the plant and the city for discussion of safety issues did not exist. There was no communication channel between the plant and the nearby communities for warning residents in the event of an emergency. The city official dedicated to safety does not have the resources to ensure safety information from Citichem is communicated.

Communication channels between the city and the plant were viewed as unimportant by top management. The long disaster-free history of the plant has made city officials and plant management complacent.

Organizational Safety Management and Learning Processes Analysis

The purpose of this step is to analyze the organization to find flaws associated with safety management:

1. Analyze how Incident and Accident Investigations are run at the organizational level.
   Incident and Accident investigations should be performed with the goal of finding flaws in the system and addressing them, rather than finding culpable individuals and punishing them. The results of

investigations should be acted upon in a timely fashion. If the organization is not capable of following up with systemic changes, hiring an outside safety group may be helpful in implementing changes.

2. Examine how safety waivers are issued and treated after issuance.

   The goal of this analysis is to determine if organizational procedures and processes are strong enough to resist pressures to issue waivers and to determine when it is appropriate to remove or lift safety constraints from controllers. Furthermore, waivers issued must be monitored and have an expiration date. Waivers must be issued with the buy-in from safety management after risks have been appropriately assessed.

3. Examine how safety-related information is communicated throughout the organization.

   Reasons and motivation for procedures that affect safety must be communicated. If safety-related decision-making is not explained, it can be ignored as people try to achieve other system goals.

4. Identify how safety reporting and incident reporting is handled.

   Reporting must be encouraged. Anonymous reporting can encourage the disclosure of important safety-related information, as participants are not subject to punishment or loss of reputation.

5. Examine risk and hazard analysis processes and procedures. Ensure that everyone (from the operator up through their managers and higher level executives) is appropriately educated regarding hazardous and safe operating conditions.

   It is important for high-level managers to be aware of the hazards as they make decisions (e.g. budget decisions or production schedules) that have an impact on the safety of operators and low-level operating processes. High-level decisions must be risk assessed.

6. Examine the corporate safety policy and ensure that:
   - It exists.
   - Everyone in the organization is aware of it, and that detailed safety plans comply with it.
   - Includes minimum operational standards (safety constraints) regarding staffing, risk assessments and etc.
   - Specifies conditions for declaring emergencies, including ceasing operations. For instance, shutting down operations can include canceling flights in aviation and in chemical industry can include shutting down plants.

7. Examine safety management:
    - Responsibilities can include:
        - Perform hazard analysis.
        - Conduct risk assessment.
        - Advise management on safety-related decisions.
        - Create and maintain a plant process safety information system.
        - Perform or organize process safety audits and inspections using hazard analysis results as the preconditions for operations and maintenance.
        - Investigate hazardous conditions, incidents, and accidents in a timely fashion.
        - Establish leading indicators of risk.
        - Establish procedure for quality control and checking of safety-critical activities and collect data to ensure process safety policies and procedures are being followed.
    - Reporting structure.

      High-level safety management should report directly to the highest level of the organization while also receiving information and reports from the lowest-level operators.
    - Make-up.

      Safety management should use a committee with mixed representation, including union representatives, operators, engineers and executives. Mixed membership can avoid safety concerns being ignored by groups that are not included in the management of safety.

8. Use the guidewords to explore how the safety management can be influenced.

This example draws from material provided by GasCo [85].

Guideword Analysis: Safety Culture

1. GasCo has an internal safety group that investigates accidents and audits safety. When an accident occurs, they use a formal checklist to identify causes. These causes are mainly restatements of ‘operator error’. Their safety management system did not allow engineers to find systemic problems or find solutions that prevented future errors.

2. The waiver system in place at GasCo included waiver tracking, but allowed waivers to build up indefinitely. Each waiver issued is prioritized, but many outstanding waivers are 'high priority' and can take months to fix.

3. The safety information coming from the top level management is high-level 'safety is our number one priority'-type messaging. Top-level management did not respond to increasing levels of safety waivers, either because they were not communicated to executives, or because the information was ignored.

4. Personal safety incidents are reported and concerns that arise are addressed. For example, a slip on a particular staircase will be investigated and the appropriate traction material will be applied. Other incidents that are related to system safety are not always reports. Many GasCo operators for example feel their jobs are at stake if they report problems to management. The culture at GasCo is one of fear and denial. Fear of getting into trouble on the part of operators and denial on the part of management.

5. The risk analysis conducted at GasCo consists of a risk table, similar to the SMS process described on page 73.

6. The safety management group at GasCo was not autonomous, nor did they have the tools that would allow them to make comprehensive fixes or redesigns of the system. Their role within GasCo was primarily to ensure personal safety and create the image, but not the reality, of safety.

Organization and External Bodies Analysis

The goal of this stage of the hazard analysis is to find hazardous situations related to the interaction of the organization with outside entities.

1. Identify outside entities that can influence the organization.
   Outside entities can include national unions, neighborhood groups, and governmental bodies.

2. Analyze the mission statements of outside organizations to identify performance or safety constraints they may levy on the organizations. Analyze the external constraints to ensure they do not violate organization safety constraints.
   External bodies can have significant influence on the safety of an organization. Mismanaged interactions can lead to hazardous conditions within the organization. Agreements between the

organization and external bodies can create unsafe human resources policies and unsafe operating conditions within the organization. For example, agreements to allow N hours of overtime per operator violate safety constraints related to human readiness and rest. Overtime can lead to exhausted workers that are not able to perform safety-related duties adequately.

3. Examine contracts with external agencies.

   Contracts typically set the price and schedule of delivered goods or services. These contracts must be analyzed for their potential to violate safety constraints directly, or set up conditions that will push the system in a state of high risk. In particular, the financial compensation agreements should be examined, as this can set financial pressures within the organization. For example, in a recent accident in Syracuse, NY, pilots were operating an unfamiliar aircraft while they were exhausted and everyone on board perished. An examination of the contracts between Continental and the contracting commuter airline shows that Continental only paid for completed flights, rather than scheduled flights. This payment scheme led to huge financial pressure to not cancel flights, at the expense of safety. The same agreement further outsourced safety assessments of pilot skills on the commuter airplanes to the commuter organization rather than Continental. Under financial pressure, the contracting airline waived skill requirements for pilots for operation of new aircraft. Continental did not have means to audit safety waiver processes within the contracting airline.

4. Use the guidewords to determine how safety could be impacted by the relationship between the organization and each interacting external organization.

This example draws from the Citichem plant described in 8.5.3 and described in detail in [167].

Guideword Analysis: History, Communication, Pressures
The external stakeholders analyzed are the City and local real estate developers.

The real estate developers seek to expand development in areas close the city. The safety no-build zone between the city and the Citichem plant is a potentially profitable area to build. The city is run by officials that are influenced by real estate developers. The city needs to expand its tax base with new developments.

The Citichem plant does not have formal procedures or safety audits for re-evaluating building in the no-build buffer zone between it and the plant. Without any recent history of mishaps known to the city, the city does not have evidence to suggest that building in the buffer zone would violate safety constraints. The real estate development erodes the safety barriers and introduces the hazard of allowing people to live near a plant where dangerous chemicals are made.

Auditing the Organization

To verify that the organization as a whole is meeting its control requirements, assessment must include controllers from all levels of the organization. As an example, the following questions could be used to elicit the state of the system.

- What are the system hazards, system-level goals, constraints, and requirements?
  This question can verify that each individual has an understanding of the high-level safety-related information.

- Does the organizational culture allow for honest reporting by lower level individuals? Do you feel comfortable disclosing safety-related information to your boss? Do you fear repercussions?
  These questions attempt to assess the safety culture as felt by this individual.

- How is safety-related information communicated to you?

- Are people in your organization using work-arounds? If not, how can you be sure?

- Are individuals ever punished for disclosing safety-related information that either uncovers the occurrence of an incident or could be used to improve future safety of the organization?

- Do you have sufficient resource slack in order to remain resilient?
  Resource slack can help achieve organizational flexibility. Flexibility is key to maintaining robustness and resilience.

- How are safety concerns treated?

- How is reporting and disclosure handled?

- Do you feel top-level executives value the safety division's input into decisions that affect the entire company?

- What kind of audits or analysis is performed when procedures are changed?

- What processes exist to change the organizational structure as system needs change or more is learned about the system?

- How do you verify that controllers are still able to adequately control their process?

- Is safety an integral part of the design process?

- Are safety personnel brought in early for design of system in the first place?

- How are trade offs made between other goals and safety?

- How are waivers treated? When waivers are issued to satisfy other goals, does the safety group support the decision? Are risk assessments performed for all safety waivers?
  Requiring a risk assessment for safety waivers should be somewhat costly. The cost will act as a disincentive to waive a safety-related process or requirement.

9.7 Comparison of SHOW to Human HAZOP and Assessment

The Human HAZOP method, as discussed previously, starts from a description of a task and then uses guidewords (e.g. *less action, no action, more time*) to discover possible deviations from the task description. The structure of the guidewords in HAZOP helps identify the human errors, or inadequate control actions, as termed by SHOW. Guidewords such as "no action" are used to find all of the inadequate control actions that can arise because an individual did not take a specified action. The next step of Human HAZOP is to identify all causes of the deviations, consequences and safeguards.

It is left to the expertise of the HAZOP team to discover all the causes of the human error. The Human HAZOP method provides no support for discovering relevant context or contributing factors that may lead to a task deviation (inadequate control action in SHOW parlance). The structure provided by the guidewords in Human HAZOP is only intended to assist the team in discovering inadequate control actions.

Structure: SHOW emphasizes the discovery of relevant contextual factors that lead to human and organizational error and Human HAZOP emphasizes the discovery of task deviations. It is interesting to note that some of the guidewords used in Human HAZOP are also used in SHOW, albeit in different ways. In Human HAZOP, the "no information" guideword is used to discover inadequate control actions along the lines of "No information communicated from the air traffic controller to the pilot." In SHOW, the same inadequate control action would be found by comparing the responsibilities and goals of the air traffic controller with the inadequate control action types and the requirements for control. Next, engineers using SHOW would use a guideword to find potential problems. For example, the "interface" guideword can be used to find user interface design flaws: ATC display does not indicate which frequency to use in order to communicate with pilots.

Theoretical Basis: Task analysis

The Human HAZOP method is centered on task analysis. Tasks can include activities to accomplish goals and procedures. The tasks analyzed are needed to control the technical system. Human HAZOP does not include analysis of systemic factors related to of organizational goals, such as subcontracting activities, pilot training activities, or safety management auditing.

Human HAZOP team members consider human factors that contribute to error. For example, a Human HAZOP of a new air traffic control technology cited inadequate training, as a cause of call sign confusion. However, the organizational influences, such as inadequate funding for air traffic controller training, are not explored. SHOW, on the other hand, is explicitly structured to promote team members to explore how organizational influences may lead to inadequate control actions.

Consistency: It is unknown which method would produce more consistent results. The HAZOP has more structure governing the progression of task-based step analysis, but does not provide structure for discovering contributing human and organizational factors.

Ease of Creating Recommendations: Users of SHOW are encouraged to explore the contextual factors that are directly addressable with system redesign. Human HAZOP does not provide structure for creating recommendations.

Domain Independence: Both methods are domain independent.

In summary, thinking of the control structure, Human HAZOP is able to draw out the ICAs that occur on the control arrows connected to the technical process, but it is unsuited for discovering organizational inadequate control actions and contributing design flaws. SHOW is able to find ICAs and design flaws at both levels of social system abstraction. The organizational influences are critical and permeate throughout the system, and a method that is able find organizational causal factors is essential for the safety of complex systems.

CHAPTER 10 CONTRIBUTIONS, FUTURE WORK, LIMITATIONS AND CONCLUSION

10.1 Contributions

In accident analysis practice, much effort has been devoted to analyzing the contributions of humans, and even organizations, to the accident. However, many accident investigators have complained that 1) their accident reports still seem to blame the operators, despite their intent to create blame-free reports; and 2) there is little guidance for how to proceed in the investigation that will draw out the relevant human and organizational factors [77].

The existing safety literature has a major gap in the area of hazard analysis and humans. Most hazard analyses focus on hazards in the technical process, and those that consider humans rarely extend analysis beyond task performance of operators. While some organizational safety research claims to have created a comprehensive analysis of organization's role in safety, it is merely an ad hoc classification of organizational influences. A prospective method that considers humans and organizations and their influences on and within the system does not exist.

Given the engineering needs mentioned above, the contributions of this thesis are:

1.) The development of control requirements for both individual controllers and organizations.
2.) A classification of human and organizational error based on control and systems theory.
3.) A new accident analysis method based on STAMP for use in social systems that is able to bridge the gap between human context and the technical mishap to engender solutions that focus on the system rather than blaming the individual.
4.) Comparison of SHOW for accident analysis and state of the art accident analysis methods.
5.) Deep dive into an extension of SHOW using system dynamics.
6.) Discovery and analysis of new generic safety archetype.
7.) A new methodology for conducting hazard analysis for use on complex socio-technical systems.
8.) Demonstration of SHOW for hazard analysis feasibility on complex systems from several industries.

10.2 Future Work

10.2.1 Executable Templates for Policy Exploration

Executable templates have the potential to allow system engineers and safety professionals to harness the power of system dynamics as part of the SHOW method to identify problematic organizational design or policies. Many policy makers could benefit from executable system dynamics models, but do not have the resources to build them for their organization themselves. The creation of executable templates that could be tuned by user-inputted static factors (e.g. rates) could allow managers to easily create models of basic organizational structures and policies. Executable templates could allow engineers to quickly build several organizational designs or experiment with several policies and identify unsafe behavioral trends without putting the actual system at risk.

10.2.2 Accident investigation guide

The SHOW accident analysis method, like all accident analysis methods relies on sound accident investigation. However, as seen from the accident analyses using SHOW (e.g. the list of questions regarding context identified by each application of SHOW), more information is required for a SHOW analysis than for a traditional analysis. SHOW may require advances or changes in how accident investigations are typically conducted. (For example, accident investigators do not currently ask system stakeholders for their 'process model'.) A companion accident investigation method would complete the SHOW accident analysis method.

10.3 Limitations

10.3.1 Application

The SHOW method is applicable to the analysis of individual controllers and the organization as a whole. Furthermore, the 'organization' may consist of more than just one incorporated entity. For example, 'safety regulation' is the organizational design that enforces safety constraints—often by governmental bodies—on companies (e.g. the regulation of pharmaceutical companies by the FDA). By analyzing safety constraints on companies and their operational context, SHOW can be applied to entire complex socio-technical systems to identify inadequacies in regulatory procedures, design, and implementation.

However, in this thesis, examples of SHOW applied to inter-organization regulatory relationship are not as comprehensive as the examples of SHOW applied to a single organization. Future work must validate application of SHOW to the safety-driven design of engineering systems (e.g. NextGen [172]).

Another challenge not addressed in this thesis is the prospect of getting buy-in from management to apply SHOW within their organization. Not all managers may see management as 'part of the system' and therefore 'part of the problem'. Without endorsement by management it is unlikely that engineers using SHOW would be successful.

10.3.2 Resources

The resources required by SHOW are most likely more than those required by traditional accident analysis or hazard analysis methods. Without a detailed checklist of causes, SHOW provides the means for inquiry into relevant human and organizational factors, but requires engineers to determine the relationship between a guideword and a control requirement for themselves. Given that, SHOW application is enhanced when performed by a diverse team. For example, experts in displays would understand the relationship between the 'process model' control requirement and the 'tools/interface' guideword better than a standard system engineer. However, SHOW does not *require* more expertise than do other methods. Yet because SHOW is not a superficial checklist of causal factors, the results of a SHOW analysis will be more comprehensive with a diverse team of engineers.

Furthermore, a SHOW analysis may take more time than other safety engineering methods. However, an investment in safe system design by using a time intensive method that produces comprehensive results seems like a reasonable tradeoff.

10.3.3 Completeness

While the SHOW method cannot be proved to be complete, we can have confidence that method will be able to find the context that contributes to inadequate control for two reasons. First, the method is based on STAMP, which has shown to be useful in finding inadequate control actions in a number of different systems across a wide variety of domains [8]. Because the SHOW method uses a similar process for finding ICAs (by comparing safety constraints and responsibilities to actions or potential actions) we have high confidence that all ICAs can be found[16]. As discussed previously in chapter two, the process for finding hazards and safety constraints is simple and stems from the loss events (accidents) that must be avoided.

[16] Of course, if the engineers do not have sufficient resources (e.g. time) to perform the safety analysis, the resultant analysis will not be complete or thorough.

Next to direct analysis of context, the SHOW analysis method is structured using the control requirements. These requirements, based in control theory, span all the requirements needed to ensure adequate control. The true challenge in the method, and the biggest hurdle that was bridged by SHOW is discovering how these control requirements may be violated—finding the human and organizational factors that contribute to inadequate control.

This brings us to the second reason we may have confidence that the SHOW method is complete enough to be useful in preventing accidents—the guidewords. The guidewords are not based on engineering principles; the author arrived at the guideword set presented in this thesis through a grounded theory research approach. The set of guidewords selected had reached theoretical saturation, which gives confidence that the set is adequate. However, it should be noted that anyone can do a poor job of analyzing each control requirement (e.g. process model) with the guidewords and the resulting analysis would be poor as well. Furthermore, it may be the case that one engineer might identify the same design flaw with one guideword (e.g. communication) that was found by another engineer using a different guideword (e.g. pressures).

10.3.4 Prioritization

By design, the SHOW method does not provide any guidance as to the prioritization of which design flaw should be addressed first, or over and above other design flaws. Each design flaw is related to an inadequate control action and thus a safety constraint, hazard, and loss event. If one wants to ensure that a particular accident does not occur, *every* design flaw identified must be addressed. In some systems, particular loss events may be deemed acceptable, and so the design flaws related to those accidents may be lower priority than the design flaws associated with accidents deemed unacceptable. Other than accident-based prioritization, it is left to the domain of risk analysis to assist engineers with design flaw priorities.

10.4 Conclusion

This thesis has presented an extension of STAMP and STPA that can provides structure for the discovery and understanding of human and organizational factors that contribute to accidents and inadequate control: The SHOW method. Differing from other state of the art methods, the SHOW method allows for great freedom of application by safety engineers, yet uses an engineering-based structure to allow for methodical analyses. The key to the SHOW method is using control theory to link commonly cited reasons for accidents (various manifestations of ‘human error’) and the contextual factors—in the environment and system design—that encourages inadequate control.

APPENDIX 1: NOGALES ACCIDENT ANALYSIS

A1.1 Guideword Analysis of the Nogales Accident

A.1.1. FAA Analysis

FAA ICAs

Control Input: Request from CBP to waive airworthiness requirement when issuing COA.
Result: Unsafe UAS was approved.

FAA Controls

Controls implemented between FAA and CBP: COA
The COA application and approval process is an important control that the FAA has for assuring the safety of the NAS. The intent of the COA is two-fold; to assure the safety of the UAS has been vetted and assure that the ATC is fully informed about the UAS mission and is able to separate air traffic from regions used by the UA. Unfortunately the COA control at the time of this accident had several weaknesses. The COA lacked specific requirements detailing UAS safety and risk assessments. The COA also lacked provisions for applicants to supply evidence that the UAS was safe. Supplemental material in the COA was limited to proposed flight plans.

ATC also implemented control of ATC by setting their budgets and developing requirements for ATC Duties and training.

ICA1: Issued a COA to the CBP for UAS flight in the NAS.

- Granted Airworthiness waiver to CBP.
- Allowed CBP to self-certify UAS.
- Issued COA for regions outside of LOS communications.

ICA2: Did not ensure that ATC had sufficient understanding of the UAS operations within the NAS.

FAA Guideword based Contextual Analysis

History:

CBP had operated the predator without accidents several times already on the same route. This may have contributed to the belief that the CBP was operating a safe UAS.

Pressures:

Great political pressure to approve mission for national security.

FAA was under time pressure to complete the COA approval in an expedient fashion in the interest of national security.

Resources:

FAA did not have the resources to certify the UAS. The FAA lacked in-house expertise that would enable them to assess the safety of the UAS. The FAA also did not have resources to assess whether CBP was able to safely operate the UAS.

FAA may not have had access flight plan information for the UA to the level that it would for a civil aircraft due to classified information transfer.

Safety Culture:

Reports [129] have indicated that the FAA is in need of improvement. However, without greater regulatory authority over public use agencies, even a strong safety culture is not enough to ensure the safety of the NAS.

Tools:

COA application approval process does not include a risk assessment. Public use missions are allowed to operate without assessments of the risks. The COA application focuses on operations.

FAA has inadequate risk assessment tool to analyze the risk of UAS operations in the NAS. Tools are quantitative, rather that systemic.

Communication:

CBP missions are classified, and open communication may have been hindered between the FAA and CBP.

Safety-related information about prior problems with the UAS were not reported to the FAA

Training:

Inadequate training of ATC in UAS operations. It is unclear what authority the FAA had to require CBP to provide enough information to ATC so that ATC could provide adequate tracking and separation service.

Interface:

The COA application may have not have provided enough detail for evidence that the UAS was safe; for example it did not provide information about the lost link profile, pilot training, pilot

operation policies, UA maintenance policies, etc. A more rigorous COA application process may have unearthed problems with CBP UAS operations in the NAS.

The guideword analysis can be synthesized and represented using system dynamics as shown in Figure 48.

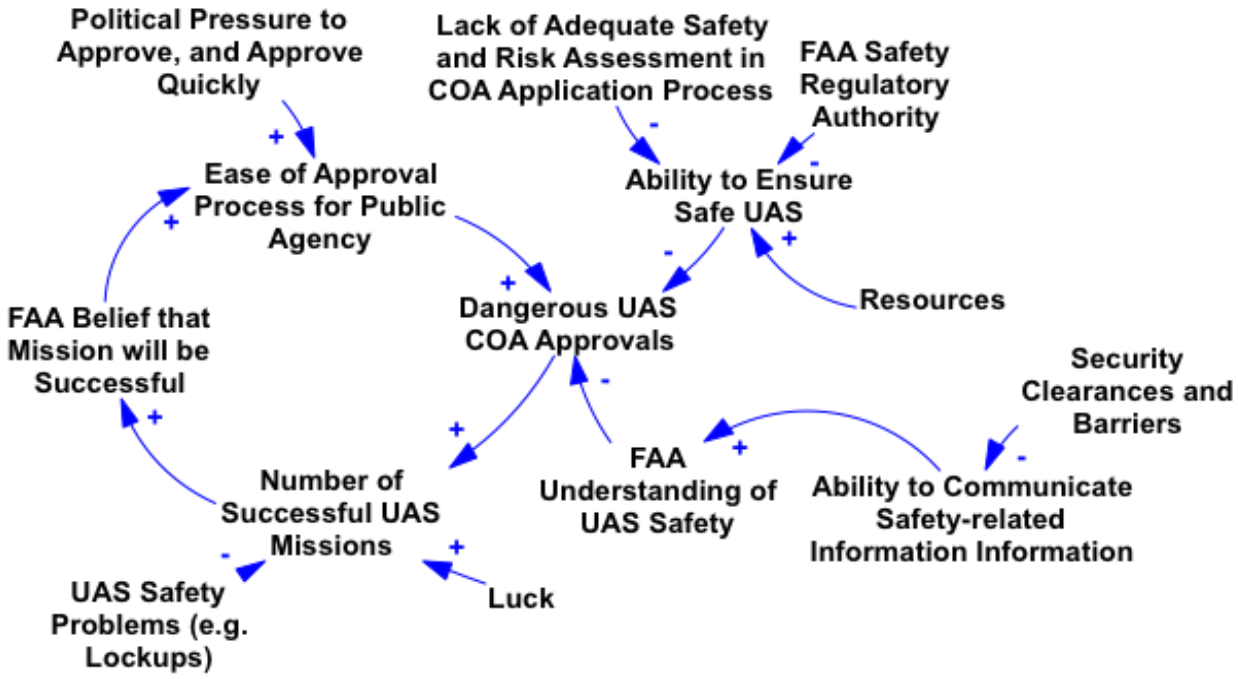

Figure 48 ATC Guidewords Analysis Illustrated with System Dynamics Causal Loop Diagram

A.1.2. CBP Analysis

CBP Controls

An important control existing between the CBP and GA-ASI was the use of an Air Force GFR to inspect and verify the adequacy of pilot training. However an Air Force GFR had not been hired by the CBP at the time of this accident.

Another important control governing the relationship between the CBP and GA-ASI was the contract for development and operation of the UAS. Details about this contract have not been made public, but a thorough analysis of this complex system would include an examination of the requirements and agreements made in this contract.

CBP ICAs

ICA1: Requested Airworthiness requirement waiver of for an unsafe UAS.

Responsibilities and constraints violated by the CBP ICA1:

Ensure that GA-ASI is operating a safe UAS

Provide FAA with information about the safety of the UAS

ICA2: Did not verify airworthiness of UAS.

Responsibilities and constraints violated by the CBP ICA2:

Ensure that GA-ASI is operating a safe UAS

Ensure that the GA-ASI provides enough evidence that its UAS mission can be conducted safely.

ICA3: Did not audit maintenance records from GA-ASI to ensure the UAS was maintained properly.

Responsibilities and constraints violated by the CBP ICA3:

Ensure that the GA-ASI provides enough evidence that its UAS mission can be conducted safely.

Ensure that GA-ASI is operating a safe NAS

ICA4: Granted waiver of pilot training requirements: Issued verbal waiver that permitted inadequately trained pilot to fly the UA as long as flight instructor was in the room.

Responsibilities and constraints violated by the CBP ICA4:

Ensure that GA-ASI is operating a safe UAS

ICA5: Did not enforce safety control: GA-ASI pilot flew UAS without the required supervision of the flight instructor in the ground control room.

Responsibilities and constraints violated by the CBP ICA5:

Ensure that GA-ASI is operating a safe UAS

ICA6: Did not coordinate with the Air Force to hire trained officer for the review of pilot training.

Responsibilities and constraints violated by the CBP ICA6:

Provide final approval of pilots certified to fly the UA.

CBP Guideword based Contextual Analysis

History:

CBP had operated the predator without accidents several times already on the same route without any accidents.

9 locks up in the previous 3 months, yet work arounds had been found so that the continued operation of the UAS was possible.

Pressures:

Great political pressure to fly mission for national security. Border security is a high priority to the government.

Great pressure for high in-air operating time for the UAS, there seemed not to be time to wait for spare part delivery.

Resources:

Insufficient skilled personnel to verify airworthiness of the UAS.

Extremely short notice to start the surveillance program. Insufficient time to hire skilled workers to adequately verify airworthiness of the GA-ASI UAS. Insufficient time to hire an Air Force officer to review GA-ASI pilot training.

Insufficient funds to stock spare parts. Spare parts were ordered directly from the manufacturer and delivery took weeks and so the UAS was flown without properly maintained parts.

Safety culture:

Unsafe work arounds (new techniques and procedures that had not been verified for safety) were common at CBP.

UAS are seen as experimental, higher risk is acceptable.

Insufficient safety management processes. Maintenance procedures not documented, corrective actions undocumented. Lack of incidents and accident investigation and learning processes. No effort to understand the reason for the lockups; once work-arounds were discovered, no further efforts were made. No safety analysis of new procedures (the PPO-1 to PPO-2 switch after the lock up)

Insufficient spare parts stocking and procedures.

No Safety analysis of lost link profile.

Tools:

CBP did not have risk assessments to assess the safety of its operation of UAS in the NAS.

Communication:

The classified mission of the UAS may have affected communication between CBP and the FAA.

Training:

CBP was supposed to have on staff an Air Force trained officer capable of assessing pilot training. Without this professional, CBP was not able to adequately fulfill its safety responsibility to give final approval/disapproval of UA pilots.

Interface:

The COA application may have not have provided enough detail for evidence that the UAS was safe. A more rigorous COA application process may have unearthed problems with CBP UAS operations in the NAS.

The guideword analysis is synthesized and represented using system dynamics as shown in Figure 49.

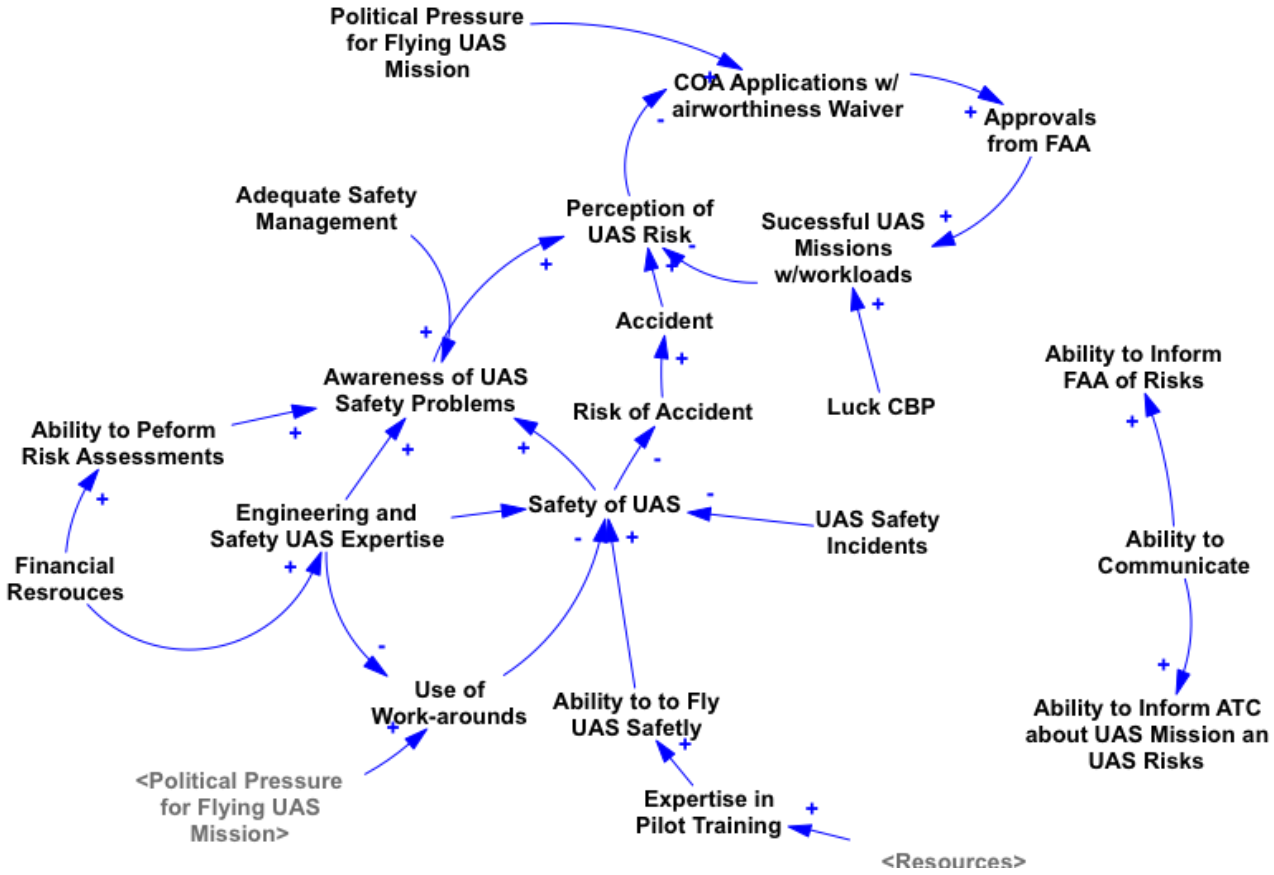

Figure 49 CBP Guidewords Analysis Illustrated with System Dynamics Causal Loop Diagram

A.1.3. GA-ASU, GA-ASI Pilot, and CBP Payload Operator Analysis

GA-ASI, GA-ASI Pilot, and CBP Payload Operator Controls

Typical Pilot controls (Throttle, Position), Payload Controls (Camera Aperture) via Workstation in the GCS, via Iridium Satellite

ICAs for GA-ASI

ICA1: Did not verify that the maintenance tasks were correctly performed.

Responsibilities and constraints violated by GA-ASI.

Ensure that the entire UAS (UA + GCS + other) is safe.

ICA2: Did not investigate lockups.

Responsibilities and constraints violated by GA-ASI.

Ensure that the entire UAS (UA + GCS + other) is safe.

ICA3: Did not report lockups to CBP or other agencies.

Responsibilities and constraints violated by GA-ASI.

Provide CBP with reports that demonstrate UAS safety.

ICA4: Inadequate procedure for addressing with lockups (switching control from the locked up PPO to the unlocked PPO).

Responsibilities and constraints violated by GA-ASI.

Ensure that the entire UAS (UA + GCS + other) is safe.

ICA5: Requested that inadequate trained pilot be permitted to fly the UA.

Responsibilities and constraints violated by GA-ASI.

Ensure that pilots are able to adequately able to fly the UA

ICA6: Created inadequate design of payload operator and pilot interface to the UA.

Responsibilities and constraints violated by GA-ASI.

Ensure that the entire UAS (UA + GCS + other) is safe.

Ensure that pilots are able to adequately able to fly the UA

Technical Inadequate Control: Backup communication system interface with Iridium was inadequate. Continued hazard analysis of this ICA can be conducted with STPA without guidewords.

ICAs for Pilots

ICA1: Did not verify that the lost link profile met safety constraints.

Responsibilities and constraints violated by Pilot.

Perform a pre-flight inspection.

ICA2: Did not follow procedure for control switch from PPO-1 to PPO-2. Did not move control stick on PPO-2 to match that of PPO-1 before control switch.

Responsibilities and constraints violated by Pilot.

Did not follow specific procedure for switching control from PPO-1 to PPO-2.

ICA3: Did not move control stick out of throttle cutoff position while controlling from PPO-2.

Responsibilities and constraints violated by Pilot.

Did not monitor the throttle cutoff position.

ICA4: Did not restart engine after fuel shutoff.

Responsibilities and constraints violated by Pilot.

Must try to restart engine upon engine failure

ICA5: Power cycled ground data transmission unit.

Responsibilities and constraints violated by Pilot.

Follow flight control procedures.

ICA6: Did not communicate all relevant factors of UAS status to ATC when link was lost.

Responsibilities and constraints violated by Pilot.

Must be in contact with relevant ATC facilities at all times and share safety-related information:

- Notify ATC in the event of an emergency
- Must notify ATC regarding any changes to lost link profile.
- Must inform ATC if she/he loses link with UA.

ICA7: Did not operate UAS with flight instructor present.

Responsibilities and constraints violated by Pilot.

Did not required instructor's presence in the command room.

ICA for CBP payload operator

ICA1: CBP payload operator did not follow the procedure for switching control between PPO-1 and PPO-2.

Responsibilities and constraints violated by CBP payload operator.

Follow safety related procedures.

GA-ASI, GA-ASI Pilot, and CBP payload operator Guideword based Contextual Analysis

History:

GA-ASI had operated the predator without accidents several times already on the same route with an accident.

History of 9 locks up in the previous 3 months, yet work arounds had been found so that the continued operation of the UAS was possible.

Most of the PIC's previous UAS experience was with Predator A. Predator A had different controls than Predator B.

Pressures:

Great pressure for high in-air operating time, there seemed not to be time to wait for spare part delivery.

Pilot stated he felt rushed when the lockup occurred on PPO-1.

Resources:

Inadequate resources devoted to pilot training.

No resources for the development of a training simulator.

Safety culture:

Unsafe work arounds were common.

UAS are seen as experimental and so higher risk was thought to be acceptable.

Insufficient safety management processes at GA-ASI: maintenance procedures and corrective actions were undocumented.

GA-ASI lacked incident and accident investigation and learning processes. No effort was made to understand the reason for the lockups after work arounds were discovered. No safety or human factors analysis of new procedures (the PPO-1 to PPO-2 switch after the lock up) were conducted.

The GA-ASI pilot instructor that was supposed to be onsite while the PIC flew was in another building. This indicates that the safety requirements violations were tolerated.

There was an insufficient supply spare parts at the GCS and procedures related to maintenance were inadequate.

Allowing an inadequately trained pilot to fly shows that risk tolerance within GA-ASI was high.

Tools:

The PIC did not have tools to support the diagnosis of the engine shutoff.

GA-ASI did not have safety assessments or auditing tools to diagnose the problems with the Iridium backup system. GA-ASI assumed that the backup system was functional and did not know that the Iridium datalink would be shutdown during lost link operations.

GA-ASI did not have a safety management system that alerted them to the design flaws in the GCS and PPO-X design.

Communication:

The pilot did not verify that the lost link profile enforced safety constraints. The pilot may not have known that this was part of his/her responsibilities, or may not have understood the safety requirements for the lost link profile.

The PIC was not in communication with ATC. (Pilot did not communicate emergency due to lost link status with ATC.) Perhaps he did not have experience with the lost link procedures. . Or, perhaps poor communication is typical and pilots rarely communicate lost link status.

The PIC did not coordinate with the instructor to help fly the UAS.

Training:

Pilot thought that switching from PPO-1 to PPO-2 would resolve lockup. (When in fact the control switches the fault from PPO-1 to PPO-2 and PPO-2 may lockup as well.)

Pilot thought lost-link profile would stop UA from losing altitude.

Poor understanding of how the UAS worked. Pilot had not completed all training modules, including handoff procedures. Pilot had only about 27 hours of training on the UA model he was flying.

All training was done with a live UAS, as there was no simulator available. This limits the kind of training missions possible, particularly for off-nominal situations.

Interface:

After the lockup, pilot lost UA state information from his display. The pilot's workstation had design flaws that caused the lockups to occur. Without accurate telemetry data, the pilot was not able to form an accurate mental model to fly the UA.

The identical interfaces of PPO-1 and PPO-2 allowed the controls for the surveillance operator and the pilot to be flipped. The design however was flawed, as the same control levers (the

throttle / camera aperture control) not behaved very differently without any queuing for the pilot. Once the controls were switched, it was not obvious to the pilot that the throttle was now in a cutoff position and the fuel starved.

The control switching allowed the pilot to initiate control form PPO-2 in an unsafe state (with the throttle in a different position from that in PPO-1).

Labeling on the workstation display was inadequate. Namely, the PPO-2 did not have engine data displayed. The data was not observable by the pilot. The control stick position was not labeled.

Alert system was inadequate.

Human Physiology:

The pilot may have been tired, he was flying the last two hours of his shift.

A.1.4. ATC Analysis

ATC Controls

ATC has the ability to set clearance for access to airspace sector. In particular ATC can declare certain sectors as TFR. Declaring a TFR tells general aviation and other aircraft that they are not permitted to fly in a particular airspace. In this accident, the TFR is where the UA flying and while the UA is supposed to remain in this airspace, in the case of uncontrolled flight the UA "busted" the TFR and flew into general airspace. There is no technology in place to monitor the boundaries of TFR explicitly to alert the air traffic controller of such a bust, only monitoring the position of the aircraft relative to the TFR, which did not happen in this case.

ATC was able to receive feedback regarding the enforcement of this control by tracking the UA with its Mode-C transponder. However, this feedback link was eliminated when the UA turned off the transponder midflight.

ATC ICAs

ICA1: Did not declare emergency when they lost track of UA. Did not alert neighboring sectors of lost UA.

Responsibilities and constraints violated by ATC.

Continually track the UA position and monitor communications from GA-ASI.

Alert other sectors in the event of emergency

Declare an emergency if one exists.

Provide separation services to ensure the UAS does not enter uncontrolled airspace.

ATC Guideword based Contextual Analysis

History:

GA-ASI had operated the predator without accidents several times already on the same route.

Pressures:

It is unknown what pressure ATC may have felt that led to their Inadequate Control Action

Resource:

Unknown. Information not contained in the NTSB report.

Safety Culture:

The classified nature of CBP missions may led to their lack of follow through on lost link protocol.

Tools:

Unknown. Information not contained in the NTSB report.

Communication:

Did not receive pertinent communication from PIC.

Training:

ATC may not have known that the lost tracking of the UA was an emergency, or if they did, they may not have known what to do if this occurred.

Training for UA-ATC operations was 30 minutes long. This training may have been insufficient for communicating lost link procedures and tracking requirements for the UA.

Interface:

Unknown. Information not contained in the NTSB report.

Human Physiology:

Unknown. Information not contained in the NTSB report.

A.1.5. OSI Analysis

OSI ICAs

ICA1: Created inadequate lost link profiles. The lost link profiles created by the OSI flew over populated areas and/or heavily trafficked roads.

Responsibilities and constraints violated by OSI.

Develop safe Lost link Profile

Insufficient information provided in NTSB report for contextual analysis of the OSI ICA.

A.1.6. Air Force Analysis

The Air Force was supposed to approve pilot training for CBP. However, the CBP had not hired any Air Force personnel. This element was missing from the control structure at the time of this accident.

A1.2 Recommendations

After highlighting the flaws in the operational context that contributed to inadequate control actions, an accident analysis must give recommendations to prevent future accidents from occurring. With the broad accident analysis method demonstrated here, the recommendations are not narrowly confined to preventing *the same kind of* accidents, but should address all hazards discovered during the analysis process.

1. There are many ways to address the inadequacies of the relationship between the FAA and public use agencies such as the CBP. The underlying issue is that the FAA has the responsibility for maintaining the safety of the NAS, but does not have the ability to ensure that UAS operations do not violate the safety of the NAS. The FAA does not possess regulatory authority over the public use agencies, and the COA process is inadequate. While the FAA may require that public use agencies perform a safety assessment, they are not privy to the details of the safety assessment, and must trust that safety assessments conducted are comprehensive. The FAA does not have the same auditing authority over public use agencies that it does over commercial aircraft manufactures or airlines.

   Interestingly, the asymmetry between the FAA's responsibility for maintaining the safety of the NAS and their inability to regulate public use agencies has always existed and heretofore the overall safety of the NAS has not suffered. However, before the development of UASs, the public agencies were in the same business as commercial manufactures and airlines: they built

and operated safe human-piloted aircraft. The safety standards, cultural values, and design processes used by public agencies were on par with those used by commercial ventures. The engineers that designed fighter jets came from the same educational background and often worked at the same companies as the engineers that designed commercial aircraft.

With the introduction of unmanned aircraft to the NAS, that may change. The technical challenges of coordinating a remote pilot and air traffic control are astounding. There is no history of shared values with commercial manufacturers to support the development of safe UAS in the NAS. The FAA has always been an outsider in UAS use and does not have the vast technical expertise that the public agencies do with this new technology. Given the expertise gap and the communication roadblocks between the defense agencies and the FAA imposed by classified information requirements, it is hard to imagine how the FAA will be able to evaluate UAS safety in the NAS.

One potential solution is to enhance the ability of the FAA to fulfill their responsibility for protecting the NAS by bringing FAA personnel into the public agencies, including air traffic controllers and the FAA officials charged with the development of procedures and NAS regulations. With adequate clearances, these FAA officials could evaluate the safety of UAS in the NAS. If the FAA personnel are accepted by the public agency, they will be better able to assess safety, refine requirements and regulations, and evaluate whether the public use agencies have met safety requirements.

2. All agencies analyzed in this system, including the FAA, CBP and GA-ASI, should evaluate their safety assessment programs. None of the agencies have a safety management system capable of assessing both the technical and social aspects of the system, nor do they appear to have a practice of regular auditing and risk assessments of potential changes.

3. The airworthiness requirement must not be waived without a risk assessment. In times of crisis, it may be obvious that the air worthiness requirement should be waived so that UAS operations are possible, but in the absence of immediate crisis, it is not clear which missions could provide benefits to the public good that would outweigh safety risks to the NAS. A risk assessment should be conducted to evaluate potential risk tradeoffs surrounding UAS flight in the NAS by parties with an understanding of both the NAS (such as FAA safety professionals) and the public use agencies (such as cleared military intelligence professionals).

4. The CBP did not have the expertise to assess the safety of the GA-ASI manufactured and operated UAS. Although the CBP was the acting operator of the UAS and had the final authority for the safety of the UAS, it did not have the ability to carry out that responsibility. The CBP should establish a better safety management group (as described previously in this thesis) and consider integrating GA-ASI into their safety assessments.

5. The human interface design of the pilot and payload operator must be re-engineered with input from human factors professionals. Flaws in the design, particularly the lack of queuing for the pilot, indicate a problem not just with the display, but also with the design process as a whole.

6. The technical design of the UA system must be re-evaluated with a comprehensive hazard analysis. The design flaw that prevented backup communications with Iridium may not be the only one.

7. The policies for training pilots must be re-engineered. At minimum, requirements for training pilots on a system must specify which systems the pilots are permitted to fly. A simulator must be available to train pilots for both nominal and off-nominal situations. The program should specify how many hours of training are required for pilot certification. If an air force GFR is required to supervise pilot training that requirement must be clear and non-waiveable.

8. Safety professionals in both GA-ASI and CBP must audit the operating system for evidence of workarounds, so that they can understand why workarounds are occurring and propose permanent solutions. The NTSB report noted two such workarounds, the PPO-1 to PPO-2 switch, and the pilot training waivers, but there may be many more.

9. Policies for spare parts stocking and maintenance performance and procedures must be investigated. The UA must not be permitted to fly with damaged parts. If a restocking delay cannot be tolerated, then spare parts must be stored on site.

10. The unhealthy safety cultures of CBP and GA-ASI indicate serious problems within the organization. An investigation into both organizations, and the relationship between the two, should be conducted. The inadequate maintenance performed on the UAS, the lack of importance placed on maintaining a spare parts supply on site, and the abundant evidence of operational

workarounds (e.g. the PPO-1-PPO-2 switch, and waived pilot training requirements) are evidence of organizational dysfunction. Without an investigation, one can only speculate as to what solutions could solve these problems. For example, the GA-ASI may have been under great time and financial pressure to deliver the completed system, and was not able to do so without cutting corners. Likewise, the CBP could have been under political pressure to get the system up and running without adequate time to understand the GA-ASI system.

11. The contracting system for the development of the UAS and the operational relationship between the CBP and GA-ASI must be investigated. Since CBP has final authority for the safety of the UAS, they need more insight and understanding into the system. Using a DER system might help assure the safety of the GA-ASI system.

12. The ATC needs to better monitor UA aircraft. UA positions must be known at all times. This could be accomplished through better electronic tracking and alerting systems. If the ATC loses track of a UA, an automatic emergency alert must be initiated.

A1.3 Summary of Accident Analysis

The human and organizational factors accident analysis method described above uses guidewords to elicit the contextual factors that were the mechanisms for the inadequate control actions. All of the factors identified in this much-studied accident [125], [128], [48], [127], were categorized with the human error taxonomy and traced to guidewords that describe the context surrounding the inadequate control actions. The recommendations generated by this accident analysis may include changes to controllers at higher levels of the control structure than an accident analysis that focuses on tasks and the man-machine interface.

APPENDIX 2: SHOW MATRIX ITEMS

A2.1 Overview

This appendix contains an example of how each guideword can be applied to find design flaws associated with each control requirement. The first section shows how guidewords are combined with the control requirements, the next section gives guideword examples for hazard analysis of the individual controller, and the last section gives examples for hazard analysis of the organization as a whole. The information in this appendix is included for reference only and should not be considered additional hazard analysis steps.

A2.1 Example Structure

The guidewords, combined with the control requirements, are organized to form a matrix-based hazard analysis tool. The number in each cell represents an example that shows how a particular guideword (identified in the column) could contribute to inadequate control via the violation of a particular control requirement (identified in the row). For example, from the partial individual matrix shown in Table 18, the paragraph (on page 253) corresponding to item 11 explains how flaws could give rise to an *inadequate control algorithm* via *resources* or *training*.

Table 18 Partial Hazard Analysis Matrix

	History	**Pressures**	**Resources**	**Tools**	**Training**	**Interface**
Control Goal	1	2	3	4	5	6
Control Algorithm	10	11	12	13	14	15
Model of the Controlled Process	19	20	21	22	23	24
Model of the Organization	28	29	30	31	32	33

An example of each guideword applied to each control requirement for individual control is shown in Table 19 and for organization control, where applicable, in Table 20.

A2.3 Examples for Hazard Analysis of the Individual Controller

Table 19 Complete Hazard Analysis Matrix for Human Factor Analysis

	History	Pressures	Resources	Tools Interface	Training	Safety Culture	Data Communication	Human Cognition Characteristics	Human Physiology
Control Goal	1	2	3	4	5	6	7	8	9
Control Algorithm	10	11	12	13	14	15	16	17	18
Model of the Controlled Process	19	20	21	22	23	24	25	26	27
Model of the Organization	28	29	30	31	32	33	34	35	36
Decision-maker Coordination	37	38	39	40	41	42	43	44	45

Matrix Items:

1. History: How someone comes to know, understand and prioritize their control goals can be influenced by their personal history and experience. Determine if a controller's individual history may indicate a controller's likeliness to pursue goals that may violate safety constraints. This should include an examination of what effect their cultural norms may have on how they view their goals and goal priorities. Cultural norms can include norms set by the controller's country, class, and even occupational training (for example norms set by CEO, Operator, or Engineering culture) [74]. See section 3.6 for a cultural example from aviation. History can also include patterns of behavior. For example, controllers with a history of ignoring or waiving goals related to safety constraint enforcement may continue to do so. An assessment of a controller's history should include how they have pursued goals in the past.

2. Pressures: Identify pressures and incentives on the controller that can influence how they form or perceive their goals and goal priorities. Typically encountered pressures include schedule pressure, resources pressure, financial pressure, pressure to comply and political pressure. Incentives may come in the form of financial compensation, bonuses, political favor or intangibles.

   Determine how pressures and incentives on the controller can change over time (the relative influence of a particular pressure is dynamic and depends on other system states.) In some systems, perverse incentives only occur during times of lower system performance, or adverse conditions. Determine how this set of pressures can change the initial prioritization of goals. If pressure can change goal priorities to be unsafe, then design changes (to eliminate, mitigate, and control the effect of pressures) should occur.

   For example, schedule pressure, which changes over time, can lead controllers to value timeliness over low risk operations. Safety-related corners may be cut. In another example, when operator rewards are not tied to safety-related outputs, operators may pursue production-related goals that maximize rewards rather than pursue safety-related goals that enforce safety constraints but do not bring the controller personal gain.

   System dynamics can be especially helpful for experimenting with policies that may influence decision-making over time. In this case, system dynamics could be used to explore policies that would shift a decision-maker's goal priorities throughout operations.

3. Resources: Determine if the controller has sufficient resources to be kept informed of safety-related goals. Resources, such as staff, money, or time, may be required to keep abreast of changing situation-dependent goals. For example, if safety-related goals change rapidly, keeping up with changes may require more resources than the controller has available, and consequently, the controller may not know the correct goals to pursue.

4. Tools: Assess the sufficiency of decision-making tools for goal selection. Goal-related tools are devices that assist in decisions regarding which control goals to pursue. For example, in the military, ground troops may use risk assessment tools that determine immediate mission goal priorities such as the decision to retrieve captured intelligence assets or not.

   Interface: Controllers must be able to send and receive timely information regarding goals and goal priorities. In many systems, controllers receive updates regarding new control goals (such as "Divert to Newark airport" or "Pull Up! Pull Up!") through a visual or aural display. Determine if the controller's interface to information and communication channels is adequate. A human factors analysis, including an assessment of workload and ergonomics, can be helpful.

5. Training: Assess the training that controllers receive regarding control goals and goal priorities. Training should not only identify control goals in nominal and off-nominal situations, but should motivate goals so that they are easily understood and valued. Verify that training materials identify goal conflicts (if they exist) and provide guidance for how to manage existing conflicts.

6. Safety Culture: The safety culture of an organization will greatly influence how operators, managers, and technicians feel about their role within the organization and the goals they are assigned to pursue. The organizational safety culture will color every communication received, procedure read, or decision made. The safety culture across different groups, product lines, missions, or geographical locations may vary.

   Assess the safety culture within the organization from the perspective of the control element under consideration. If the safety culture is found to be unhealthy, the solutions required may be far-reaching, such as new top management.

7. Data Communication: Controller goals and priorities must often be communicated to the controller. Identify information needed by the controller in order to understand their goals and goal priorities.

Determine how goal-relevant information is transmitted to the controller and ensure that it is transmitted in a way that the controller can understand. Communication may be formal or informal. Formal communication can include meetings agendas, meeting minutes, procedures, training materials, and etc. Informal communication regarding goals can include casual conversations between colleagues or informal mentoring.

Analyze communications to identify how they motivate, communicate, and verify safety control goals for each controller. Ensure that safety-related goals for the controller and high-level safety system goals are included in goal communications. The absence of goal communication for one controller could indicate a problem with either organizational goal assignment or communication.

Determine if informal goal-related communication conflicts with formal communication. Conflicts of this sort can indicate a problem with:

a. employee morale, indicating problems at the organizational level that impact how employees are treated
b. the formal goal priorities of the organization
c. lack of resources available to controllers to achieve state-related goals

8. Human Cognition Characteristics: Human cognition characteristics can impact how controllers prioritize their control goals. For examine, in the face of potential losses humans take on more risk than they would in the face of gains. Determine if human cognition characteristics may interfere with how goals are learned, identified, or prioritized.

9. Human Physiology: The human body itself may impact how goals are learned, identified, or prioritized. Physiological concerns can include exhaustion, intoxication, strength, speed, or disability. For example, an exhausted pilot, no matter how effective the goal communication infrastructure may be, may prioritize goals relating to an expedited trip home over those related to following safety-related procedures.

10. History: How someone comes to know and implement their control algorithm can be influenced by his or her personal history and experience. For example, controllers that have modified the control algorithm to make the control process more efficient or interesting may continue to follow a modified control algorithm. In medicine, surgeons who waived safety protocols were rewarded with quicker procedure times and were found to be more likely to waive safety controls in the future. This

behavior pattern has been called the "getting away with it" loop in system dynamics. In another example, controllers that have not experienced a recent adverse event or incident may omit or cut corners of safety-related control algorithms. This behavioral pattern has been called the "complacency" loop.

Determine if a controller's individual history may indicate a controller's likeliness to control the process that may violate safety constraints. This should include an examination of what effect their cultural norms may have on how they view their goal algorithm. Cultural norms can include norms set by the controller's country, class, and even occupational training (for example norms set by CEO, Operator, or Engineering culture) [74]. Some control steps may be perfectly acceptable to one culture but unacceptable to controllers from a different culture. See section 3.6 for a cultural example from aviation.

11. Pressures and Incentives: Identify pressures and incentives on the controller. Determine the mechanism for how these pressures and incentives may influence the controller's control algorithm. Time pressure, for example, can lead operators to skip steps, or shorten time devoted to decision-making. Incentives can be used to encourage desirable behaviors such as notifying supervisors of software bugs. After all incentives and pressures have been analyzed, determine if the net result of the pressures and incentives is safety increasing or safety decreasing. System dynamics can be a useful tool to perform this analysis.

12. Resources: Identify the resources required to perform the control algorithm. Resources can include time, budgets, political power, and staffing resources. Determine if the controller has adequate resources to fulfill their responsibilities at all times. For example, when controllers are responsible for system maintenance, safety critical replacement parts should be immediately available for use. Many accidents have occurred due to an inadequate supply of parts.

13. Tools: Tools can include control algorithm implementation aids such as procedures or checklists, or physical aids for performing the control algorithm such as hydraulic lifts. For example, the control algorithm may be encoded in a checklist (a tool) and used by controllers to choose their next action. Identify needed tools for implementing the control algorithm. Also identify tools that would be *helpful* in performing the control algorithm. Identify tools available to the controller and see if they would benefit from additional of different tools.

Next assess whether controllers find the tools available to them adequate. Determine if the levers controllers have to affect the process state compatible and useful. If controllers find the tools difficult to use, or not useful, they may not be used, to the detriment of safety.

Interface: Analyze the sufficiency of the interface between the controller and the levers used to affect state. The control interface can display of procedures and checklists. Displayed information must be visible, accessible, and designed to aid the controller. Important information must not be buried within impenetrable menu hierarchy on the control or tool displays. If the control algorithm is complex, encoding the steps into a display can be helpful.

14. Training: Controllers often learn how to control the process through training. The training may be part of a formal program offered by the organization, or may consist of informal, one-on-one job training with a mentor. Conflicts between formal and informal training experiences may indicate a problem with the training materials, resources available to the controller, or even organizational as a whole. Analyze training to determine if its sufficient for learning, developing, forming, and motivating the control algorithm.

    The level of training required depends on what the operator is training for. For example, operators training for an entirely new role (e.g. a new pilot) will require different training than experienced operators preparing a new control algorithm for a familiar job (e.g. pilot becoming qualified on a new jet). Training for context is sensitive. If an operator has been trained for a particular task in one context, the learning may or may not translate to performing the same tasks in a different context [117]. Ensure that there is an adequate training program for re-training operators to change their control algorithm if the process changes. Re-learning a similar set of steps with a key difference can be very difficult. Operators may slip into the "old" way of doing things, and perform the incorrect, but similar steps, and not even realize it. In some situations, re-training the same person for a similar, but different control algorithm, may be too risky, and it may instead make sense to a train a new person instead.

15. Safety Culture: The control algorithm used will be affected by the safety culture of the organization. If the safety culture is unhealthy, controllers may not perform the control algorithm sufficiently. See item 6 for more information.

16. Data Communication: Determine if all of the information necessary to perform the control algorithm has been given to controllers. This analysis may include trainings, procedure manuals, and company policies. Needed data communication might include advice about how to implement the control algorithm and why it is important to do it a certain way. The control algorithm description should have timing requirements. For example, a triple engine failure of flight Eastern L1011 in 1983 was due to the maintenance team's failure to run the engines for long enough. If the engines were run for tens of seconds longer, they would have seen an oil leak which would have indicated a problem with the O-ring install. O-rings were missing from three engines [151].

    Identify differences between the organization's control algorithm procedures and how operations personnel actually implement the control algorithm. Organizational procedures that diverge significantly from common practice indicate a potential drift towards risk. In particular, a procedure divergence may be due to an inadequate procedure update process, or could indicate that management does not actually know how the plant is operating in practice.

17. Human Cognition Characteristics: Ensure that human cognition characteristics, such as personality and risk tolerance, have been taken into account during the design of the control algorithm. Controllers with high risk tolerance will select control actions that are more "risky" than control actions selected by conservative individuals. Analyze the control algorithm to ensure that its compatible with individuals across a broad range of risk tolerances.

    Another human cognition consideration is inability of humans to control high-order systems. The control algorithm should be designed to require 1^{st} order control or direct control if possible.

    The workload engendered by the control algorithm is another human cognitive characteristic to consider. Verify that human factors professionals have analyzed control tasks to ensure that job duties do not exceed human cognitive limitations.

18. Human Physiology: Analysis of the control algorithm should include human physical characteristics that may affect the controller's ability to carry out the control algorithm. Physiological characteristics can include factors such as height, strength, and eyesight. Additionally, the control algorithm may be executed by individuals with disabilities or those at the extreme ends of ergonomic distributions. Perform a human factors assessment to determine if the control algorithm's physiological

requirements are suitable to the human in control. Human factors and ergonomics references have a full breadth of factors that should be examined.

It is important to consider physical factors in nominal and off-nominal situations. In some situations, the control algorithm may be executed by exhausted or otherwise physically debilitated individuals. It is better to avoid having physiologically inhibited controllers operating altogether, but if this cannot be avoided, some mechanisms can alleviate the effects of impairment. For example, in the trucking industry, drivers can chew mints to maintain alertness for a few additional minutes.

19. History: A controller's model of the controlled process may be influenced by their culture and experience. Determine how a controller's model of the process may be influenced by their history. A controller's cultural biases can include norms set by the controller's country, class, or even occupational training (e.g. a CEO's business school, an operator's on the job training, or an engineer's college education) [74]. A controller's occupational training influences how they use and view data. For example, from studies of CEO culture, we know that CEOs tend not to trust data that are handed to them up through the chain. CEOS prefer to directly observe the controller process to inform their process model [74].

    A controller's control history should be understood, as previous experience can adversely influence their mental model for the current process. For example, because the process model is informed by sensor readings and other data, "mode confusion" can arise when operators have similar interfaces for differently operating processes they have controlled in the past.

    Determine how a controller's model of the process may be influenced by their history.

20. Pressures and Incentives: Determine if pressures and incentives can lead to controllers ignoring or missing feedback. Certain pressures can blind controllers to various pieces of data. For example, time pressure can lead to an inadequate model of the controlled process if controllers do not have enough time to examine or assimilate information and data.

21. Resources: Identify the resources required to create and sustain an adequate model of the controlled process. Resources can include time, financial budget, political power, or staff. Inadequate resource availability to controllers can lead to an inability to perform tasks associated with updating the process model.

22. Tools: The ability of controllers to assess current process state and project it into the future is directly influenced by data acquisition tools such as software tools, procedures, and practices. Identify tools that controllers use to create a model of the controlled process and evaluate them for effectiveness. Particular attention should be paid to the assessment of risk assessment tools. Risk assessments gather more information about the state and greatly inform decisions.

    Interface: Identify data needed to form an adequate process model. Verify that all data is available to the controller through tool outputs or displays. Perform a human factors analysis on all data interfaces and verify that they allow controllers to form an adequate model of the process. In particular, ensure that:

    - needed data is not missing from displays
    - needed data is observable rather than just available.
    - physical data interfaces (e.g. Manuals, dials, reports) are designed according to human factors principles (For example, are dials designed to reduce mode confusion?)

23. Training: To construct an adequate model of the controller process, training must give controllers the opportunity to form a model of how the system works, rather than just an "I/O model" as discussed in [117]. When operators encounter situations outside the scope of their training, a fundamental understanding of the process under control can help them create novel solutions to problems. Nadine Sarter [152] has warned engineers that increasingly, pilots are trained how to *work* the system, rather than how the system *works*.

24. Safety Culture: The safety culture can affect the controller's process model. If the safety culture is unhealthy a controller may not notice, may not be able to attend to, or may ignore key pieces of data. See item 6 for more information.

25. Data Communication: Inadequate communication may lead to missed, misinterpreted, or dismissed data that is crucial for influencing the process (mental) model. Identify sources of data related to safety. Assess communication sources (e.g. manuals and people) and mechanisms (e.g. emails and meetings) for their ability to get the right information to the right people so that they can form an accurate mental model of the controlled process.

Language: Verify that the language chosen to communication in is understandable by operators and managers. Accidents have occurred because of language differences [18].

26. Human Cognition Characteristics: Perform a human factors analysis to ensure that controllers with normal variance along physiological characteristics does not lead to misinterpreted information and an inaccurate mental model. For example, risk-seeking individuals may not identify situations as "dangerous" as readily as those who are innately more cautious.

27. Human Physiology: Human physiology can affect the formation of a process model through the human's physical interaction with sensors and data manipulators. For example, if tasks associated with forming a model of the controlled process include reading valves located outside, and the valves are located too high to be easily read, or controllers are exposed to extreme temperatures, the controller may not perform related tasks often enough to maintain an accurate mental model. Identify all tasks associated with forming an accurate mental model and ensure that they are designed to be ergonomically compatible with the population that will be performing the work.

28. History: A controller's model of the organization may be influenced by their personal culture and experience. For example, a new controller hired from an organization whose management always gave "lip service" to operator feedback may not offer safety-related feedback in the new organization. In another example, individuals from hierarchical cultures may feel uncomfortable seeking out their peers in a flat organizational structure for advice or mentorship. A controller's model of the organization and their place within it will determine how they act when an unplanned-for event occurs and they need to reach others within the organization.

    A controller's cultural biases can include norms set by the controller's country, class, and even occupational training (e.g. norms set by CEO, Operator, or Engineering culture) [74]. For example, if operators do not think that management reads their reports, they may stop providing accurate reports. In another example, CEOs tend to distrust data received from subordinates and may choose to rely on their own observations instead leading to an inaccurate mental model

    Determine how a controller's model of the organization may be influenced by their history. For example, some controllers may be biased to distrust certain roles within the organization (such as safety professionals) or certain organizational functions (such as auditors). New controllers may need

time to acclimate to the organization and recalibrate their biases in order to build an accurate organization model.

29. Pressures: The model of the organization can be influenced by pressures and incentives. Time or resource pressure can lead to superficial effort to understand the organization. Examine what pressures and incentives exist for the controller and determine how the controller's model of the organization could be affected. Incentives that improve the controller's model of the organization can include rewards for cross organization communication. At an informal level, a controller's model of the organization can potentially be improved through office-wide social events.

30. Resources: Identify the resources required to create and sustain an adequate model of the organization. Resources can include time, budgets, political power, or staff. Ensure that adequate resources are allocated to allow controllers to create and sustain a model of the organization.

31. Tools and Interface: Determine if there is sufficient tool support for controllers to form an adequate model of the organization. Assess the interface between individuals and tools available for forming a model of the organization. An example of a tool for developing a model of the organization is an organization chart or employee directory. While a simple chart may be adequate for some employees, other controllers may need detailed information regarding the roles and responsibilities of key controllers in the organization. Ensure that information contained in the tools is updated regularly and accurate.

32. Training: Identify and assess the training given to controllers and ensure that is sufficient for developing a model of the organization. In many organizations, formal training for creating this model is part of a first day initiation lecture. Often, informal training from peers helps controllers form a model of the organization. For example, experienced operators may instruct new operators never to bring safety concerns to a management.

33. Safety Culture: The safety culture can affect the controller's model of the organization. A poor safety culture can lead controllers to believe that others in the organization do not care about, or will not respond to, safety problems. See item 6 for more information.

34. Data Communication: Identify what data is needed by controllers to create a model of the greater organization. At minimum controllers need to know how to notify in the case of an emergency, or if

they have safety concerns that should be communicated. Ensure that processes exist to update the controller's model in a timely fashion when key pieces of data change (e.g. personnel changes).

35. Human Cognition Characteristics: Abstraction and hierarchy enables people to understand complex systems, such as organization. Identify mechanisms that enable humans to build adequate model of the organization so that they are able to enforce safety-related constraints in unplanned-for situations.

36. Human Physiology: N/A

37. History: A controller's ability to adequately coordinate process control with other decision-makers is influenced by their personal culture and experience. A controller's cultural biases can include norms set by the controller's country, class, and occupational training (e.g. norms set by CEO, Operator, or Engineering culture) [74].

    For example, the ability of a team to share sub-tasks requires that their cultural backgrounds are amenable or that they are able to overcome cultural clashes in some way. For example, foreign athletes whose home countries are at war may not work well together on an American collegiate soccer team. In another example, the occupational training and culture of a foreign doctor may conflict with expectations of American nurses. CRM training may be required to overcome cultural biases and differences so that information from all parties is valued and used.

    Determine how the ability of controllers to coordinate with each other (either peer, subordinate, or superior controllers) is affected by history and culture. For example, some controllers may be biased to distrust certain roles within the organization (such as safety professionals) or certain organizational functions (such as auditors). New controllers may need formal training in order to adequately coordinate with other decision-makers.

38. Pressures: The ability to coordinate with other decision-makers can be affected by pressures and incentives. For example if pressures are setup so that decision-makers are rewarded for individual, heroic efforts, controllers may act in isolation. Ensure that incentives and pressures do not put joint or coordinated decision-makers at odds to the detriment of system safety. Bonuses should be tied to the end process result rather than to one individual controller in a joint control situation. See items 11 and 29 for more information.

39. Resources: Identify the resources required for all relevant decision-makers to coordinate and control the process. Resources can include time, budgets, political power, or staffing resources. Ensure that each controller in the joint decision-making process have resources to coordinate. In particular, if joint decision-makers are team with one member representing the business function and the other representing a safety function, each person must have control of their own resources. Without access to adequate resources, the controller representing safety could be squeezed out of the decision-making process.

40. Tools and Interface: Identify tools for the support of coordinated decision making. Identify and assess the interface used to aid in coordinated decision-making. Tools may come in the form of risk assessments and analysis software. Ensure that the tools used by one decision-maker are available to other members of the team. Assess the adequacy of all tools as discussed in item 13. Accidents have occurred when one decision-maker had an outdated flight simulator while the other decision-maker had a current version of the flight simulator.

41. Training: Identify and assess the training given to joint decision-makers and ensure that is sufficient for developing an understanding of what kinds of coordination are necessary to fulfill control goals and satisfy safety constraints. For more information, see item 14.

42. Safety Culture: Controllers may not want to coordinate openly or honestly to solve problems if the safety culture is unhealthy. Controllers may feel the other decision-makers may try to capitalize on wrong decisions or negatively impact them in some way. See item 6 for more information.

43. Data Communication: Identify what information needs to be exchanged between decision-makers so they are able to jointly control the process. Ensure that data sharing processes are designed so that decision makers are encouraged to share information, rather than hide or hoard it.

44. Human Cognition Characteristics: If possible, engineers should create situations where decision-makers respect each other and work well together. Also, to avoid groupthink, (which can erase many of the benefits of coordinated decision-making) consider a team with a diverse set of views that are able to challenge each other's thinking.

45. Human Physiology: The method by which decision-makers coordinate should be analyzed for ergonomic considerations. Many types of communication are best accomplished when joint decision-

makers are in the same room. The ability to make eye contact can also be important for nuanced decision-making.

A2. 3 Examples for Hazard Analysis of the Organization

Table 20 Complete Hazard Analysis Matrix for Organization Analysis

	History	Pressures	Resources	Tools Interface	Training	Safety Culture	Data Communication	Human Cognition Characteristics	Human Physiology
Assignment of Goals, Control Authority and Responsibilities	1	2	3	4	5	6	7	8	9
Organization Functional Interactions	10	11	12	13	14	15	16	17	18
Allocation of Resources	19	20	21	22	23	24	25	26	27
Organizational Communication and Feedback Channels	28	29	30	31	32	33	34	35	36
Safety Management and Learning Processes	37	38	39	40	41	42	43	44	45
Interaction with External Bodies	46	47	48	49	50	51	52	53	54

1. History: "History" can impact the assignment of goals, control authority, and responsibilities in two ways: via the history of the *organization* and via the history of the *individuals* to which it assigns goals, control authority and responsibilities.

   Hazard analysis of this contextual factor should include an examination of how the organization has assigned goals, control authority, and responsibilities over various time horizons. Personnel records are useful for discovering a devaluation of safety. For example, safety devaluation can be expressed through a reduction of authority or reduction of safety personnel. Another way in which safety can be comprised is by increasing the number of roles or goals individuals are responsible for—as the docket of responsibilities expands, the amount of time and attention available for each one shrinks. Personnel charged with enforcing safety constraints may become overwhelmed with other duties and may cut corners.

   Other historical records that should be taken into account are management changes (through promotions, outside hires, buyouts, or major changes to contracts). Management changes may impact how roles are assigned and provide opportunities for a dilution or concentration of control authority to safety professionals within the organization.

   Other safety-related historical records to examine can include incident reports. Organizations without recent incidents may marginalize the role of safety groups within the organization and seek to eliminate them to cut costs.

   For the assignment of goals, control authority, and responsibilities to an individual their personal history must be accounted for. This topic is explored in more detail in hazard item #1.

2. Pressures and Incentives: Identify pressures and incentives that can lead to changes in how or what roles and responsibilities are assigned. For example, financial pressure may cause a collapsing of multiple safety-related roles satisfied by multiple controllers into fewer controllers in a mistaken attempt to reduce costs. Change processes must be in place that will trigger risk assessments before such organizational changes are made.

   The ability of production process controllers to exert pressure (e.g. political pressure) on safety-related controllers can be dangerous. For example, cutting the safety organization's funding will save money in the short-term, but will dramatically increase risk. The control structure within the

organization should be designed to maintain independence of safety professionals from production professionals.

3. Resources: Identify the resources required to create and sustain adequate assignment of safety and performance goals, control authority and responsibilities through the organization. Resources can include time, budgets, political power, or staffing resources. Organizational top management may require time to understand process needs and organizational needs when making decisions about what kinds of goals should be assigned to each. Example goals include cost targets and budgets for the human resources department, production targets for a business unit, and staffing allowances for the safety organization. Resources allocations will affect the relative power and constraints levied on each branch of the organization.

4. Tools and Interface: The use of appropriate tools with adequate interfaces is critical in the assignment of goals and control authority throughout the organization. The assignment of goals to individuals can create dysfunctional interactions that may not be anticipated without the use of simulators. Identify how high-level management will levy goals and responsibilities throughout the organization and ensure available tools are sufficient. For more information see item 4.

5. Training: Determine and assess how the organization ensures that the individuals selected for a particular role, job, or task are sufficiently trained and able. In particular, identify staffing transition policies that ensure newly assigned staff are adequately trained for their new job. For more information, see item 14.

6. Safety Culture: The safety culture within the organization may affect how organizational decision-makers exercise their control authority or assign it to others. Examine how management handles the re-assignment or re-alignment of staff or executives within the firm. Identify how does the organization prevents critical safety information from being lost. Additionally, determine how the organization preserves its safety culture during staff transitions (including layoffs or firings). See item 6 for more information.

7. Data Communication: The organization must communicate goals and responsibilities throughout the organization. The processes and procedures for this communication should be analyzed for gaps and weaknesses. Identify how new data regarding new safety-related tasks is analyzed and incorporated

into the organizational decision-maker process. Identify feedback mechanisms available to organizational decision-makers to indicate safety-related tasks are completed adequately.

8. Human Cognition Characteristics: Ensure that tasks assigned to individuals are compatible with human control. In particular ascertain that controllers are not required to merely check off that others have completed a task. If a "double check" is required, a substantive analysis must be required of the verifying controller.

9. Human Physiology: The tasks assigned to different controllers should take into account their physical needs. Assigning tasks that require humans to be awake or alert for hours at a time should be reconsidered. For more information, see 18.

10. History and Culture: The backgrounds and prior experiences of non-safety related organizational functions or groups can have an impact on safety as these factors will shape how they interact with safety groups. Individuals coming from organizations where safety engineers only dealt with personal safety may not understand how their own policies can impact system safety.

11. Pressures: Non safety-groups are often very powerful. Groups that govern organization budgets or control the organizational product are often the most powerful. It is important that these groups are not able to erode the ability of safety groups within the organization to do their job. In particular safety group should not report to production-related groups as this puts pressure on the safety group to be swayed by production goals over safety goals.

12. Resources: The manner in which resources are allocated throughout organization will greatly influence the power of each group. This process must be performed so that safety is remains independent as possible from the production side of the organization. See items 19-27 for more information.

13. Tools and Interface: Functional groups should all have access a model of the organizational control structure so that they can see the safety constraints, controls and feedbacks between each organizational function group.

14. Training: Managers from each functional group within the organization should know what each other does. Policies pursued by one group can affect other functions within the organization, and each group should know how their pursuit of policies will affect others.

15. Safety Culture: The organizational safety culture is not confined to just the groups that produce the product; it is also influenced by the operational groups, such as accounting. Each group should be invested in safety.

16. Data Communication: To maintain safety and balance of the functional groups, data must be communicated throughout the organization. If for example, cost-cutting initiatives will negatively impact safety in another group, this information should be shared.

17. Human Cognition Characteristics: N/A

18. Human Physiology: N/A

19. History: The manner in which organizations distribute resources throughout the organization can dramatically affect safety. Performing a trend analysis on resource allocation for different product lines and organizational units can uncover marginalization of safety. For example, when reducing the size of a safety organization, (reducing staffing resources) an accurate risk assessment should be conducted. Organizational short-term thinking often comes in the form of workforce reduction (or lack of commensurate expansion during periods of organizational growth) of non-product production related activities. While this kind of behavior may save money in the short-term, accidents can be extremely costly and potentially ruinous

    Historical trend analysis can also be used to examine organizational goals for indications of increasing risk. When organizational goals surrounding resources change dramatically, it can indicate the presence of bubbles or overreaction. In times of stress or change, overreaction can occur and lead to a temporary, yet costly, bubble [46].

20. Pressures: The ability to distribute resources throughout the organization without being subject to pressures that would lead to the violation of safety constraints is important for safety. Assess whether typically encountered pressures (e.g. production pressures) will negatively affect resource distribution.

21. Resources: The organizational process of allocating resources will require resources in and of itself. Ensure that the organization has sufficient resources (including knowledge and skill) in order to accomplish this goal.

22. Tools and Interface: Tools can greatly impact the ability of the organization to adequately allocate and distribute resources throughout the organization. No company can allocate infinite funds or staff to each safety-critical controller; trade offs must be made. Evaluate the interfaces used by organizational decision-makers to allocate resources throughout the organization. For example, an interface for resources allocation can include tools such as SAP [153], which is used to explore budgets allocated to groups in the company. Identify suitable tools for aiding decision-makers in resource trades.

23. Training: Proper allocation of resources will require training for organizational decision-makers. Identify training required and ensure that organizational members are receiving it. For more information, see item 14.

24. Safety Culture: A poor safety culture can lead to an unsafe allocation of resources throughout the organization. See item 6 for more information.

25. Data Communication: Identify what data is needed by those allocating resources throughout the organization. Ensure that data-driven are in place so that the controllers of safety-related tasks have adequate resources, but not an over-abundance of resources that could be better used elsewhere in the system.

26. Human Cognition: Human cognition requirements and limitations should be taken into account when allocating recourses. Controllers that must perform high load cognitive tasks may benefit from additional support, such as expert staff that can participate in the decision-making process. The amount of time allotted to tasks can also be made with cognitive requirements in mind. An excess of time give to a task can lead to slow human performance, while too little time can lead to corner cutting at the expense of safety.

27. Human Physiology: The resources allocated to people should account for the physical needs. After intense periods of exhausting work, resources such as extra time off, or a place to take a nap and recover, should be available.

28. History: Hazards can arise through the failure of communication and feedback channels within the organization: the right information does not get to the right people in a way that can be understood. History can be used to identify potential problems with communication channels within the firm. For example, regular meetings that produce reports that are never read or acted upon indicates that that particular communication channel has dangerously atrophied. An organization that has a history of bombarding individuals with safety platitudes may not be taken seriously when attempting to communicate important safety-related messages. The manner in which the safety goals and constraints are communicated also has a bearing on how the content of the message is viewed and understood. Messages sent in an email on Friday afternoon that may not be read until the following week may not be effective. Powerful messaging may require use of several mediums at once; including group-wide meetings for announcements combined with smaller breakout meetings for discussions.

    The culture of individuals within the organization will impact how well certain communication methodologies will be received or understood. The comfort-level that various age groups have with communication technologies (e.g. email, letters, reports or text messages) will influence their use of them. During the hazard analysis, ensure that communication means used in the organization are amenable to the age cohorts within the organization.

29. Pressures: Determine if typically encountered pressures may be high enough that communication channels could be eliminated or weakened. Analyze the abilities of system-wide communicators to deliver safety-related messages without interference from others. Individuals with a system-level view of safety constraints and goals may be surveyed to determine if they feel they are able to communicate important safety-related information freely. If, for example, some individuals have information regarding safety that affects the whole organization but are not able to communicate it, hazards could occur. See item 2 for more information.

30. Resources: Like roads, organizational communication and feedback channels require maintenance and attention in order to succeed. New channels may be needed to connect the organization as it grows. For example, a product team review process, (a common, important communication channel)

requires resources such as high-level staff assigned to chair and attend meetings to be effective. The communication of system-level goals and constraints requires resources. Identify all resources required for this task, including the right people to perform the communication. Choosing high-status well-respected people within the group will increase its importance and convey the earnestness of the message.

31. Tools: The communication of system-level goals and constraints may be aided by certain tools. Identify needed tools and ensure they are suitable for the task. Messaging tools can include media publications or use of other communication methods. Furthermore, tools can be used by management to assess the adequacy of organization communication and feedback channels. For example, an online anonymous web-form could be made available to rank and file employees so that they can notify top management if they feel certain meetings have become obsolete. The interfaces used to understand and observe organization communication and feedback channels may include meeting schedules observed through "Microsoft Exchange" or other web tools.

32. Training: Organizational decision-makers may require training to learn how to maintain organizational communication channels. Identify training available to decision-makers and assess its adequacy. For more information, see item 14.

33. Safety Culture: Organizations with a poor safety culture may only give lip service to the communication of system-level goals. They may communicate goals throughout the organization, but do so in way that the goals are not heard or paid attention to by others. The organization may also demonstrate that such missives are to be ignored though other actions. A poor safety culture may lead to the atrophy of organization communication and feedback channels. See item 6 for more information.

34. Data Communication: Identify what data is needed by decision-makers to create and maintain communication and feedback channels. Meetings should be called when they are needed rather than as a perfunctory function that leads to complacency. Identify how system level goals and constraints are communicated throughout the organization. Assess each communication channel or medium used to determine whether messages are understood and acted upon. Identify assessments the organization has available that would inform them of feedback channel atrophy. For more information see 25.

35. Human Cognition Characteristics: Organizational communication channels should be constructed so that important information calls for a human's attention, rather than using the human as a monitor for potentially important information. The approach taken by organizations to communicate system-level goals and constraints should include a notion of importance. Not all organizational goals can usually be accomplished[17]. Guidance must be given to humans so that they know the relative importance of each goal; otherwise humans will filter the information given by top management in a potentially undesirable way. For more information see 17.

36. Human Physiology: N/A

37. History: The impact of the history and culture of individuals on safety management and learning processes should be considered. Hazard analysis should ensure that safety assessments throughout the organization are performed by a diverse group of people: all levels throughout the organization should be represented, including operators, engineers, business professionals, and top management. Even the results of the best auditing process can be ignored if individuals do not trust the groups performing it. Gaining trust and respect for safety management processes can be aided through the use of a diverse team staffed with respected individuals.

38. Pressures: Safety management and learning processes are affected by incentives and pressures. First, ensure that the incentives in place to encourage healthy safety management and learning practices actually do so. For example, in medicine, incentives based on the number of "fall free days" probably do nothing to increase system safety. Incentives are often tied to "symptoms" and operators may be able to squash one symptom of a system operating in a state of high risk, but symptoms in other forms will appear. Furthermore, stemming symptoms without addressing systemic issues can lead to a decreased awareness of safety-related issues.

    Time and resource pressures can often lead to superficial incident reporting. Examine procedures related to safety management and ensure that procedures are adequate and engineers are able to follow them.

39. Resources: Safety management and learning processes will require resources. Identify all the resources required and ensure they are readily available. Resources might include skill, staff, or

[17] How many aerospace systems come in on-time, on-budget and to spec?

funds. Determine if there is sufficient resource slack or "emergency resources" that can be brought to bear during emergencies.

40. Tools and Interface: Safety management and learning processes can be significantly affected by tools. For example, incident-reporting processes may be too cumbersome for operators to use, or they may not have open-ended space for operators to express rich insights. Analyze tools used by both reportees and safety management professionals and determine if they are adequate.

41. Training: Individuals and groups in charge of maintaining and following the organization's safety management and learning processes may require significant training in order to their jobs. In particular, safety professionals may acquire most of their understanding of the job from on the job training rather than through formal education in university. Establish a program that ensures each person understands what the safety management principles are within the organization and are able to implement the policies built from them. For more information see item 14.

42. Safety Culture: The effect of safety culture on safety management and learning processes is strong. Safety management processes should be designed to improve the safety culture. Some tenets for a good safety management system that endangers a healthy safety culture are:

    *as much as possible, incident reports are anonymous and reportees will not be punished as a result of making the report or disclosure. This can be aided through review by the safety group, rather than the supervisors of potential reportees. This has been successfully implemented at NASA and British Airways [124].

    *incident reporting or disclose is an simple. Richer and fuller accounts will result of the reporting system includes free comment space and open-ended questions. The system must be available near to the time that incidents can take place, before important details become lost.

    *System safety management reports should not be filled with targets and bar charts. System safety is not measured by such devices.

    *finally, the organization must react to reports in a sufficient and timely manner. If the reports are ignored, individuals will be less likely to make them.

Fore more information see item 6.

43. Data Communication: Identify how company safety management and learning processes communicate information to:

43.1. Superior controllers: The seriousness with which top management and executives take messages and advice from the safety management group can indicate the strength of the safety culture.

43.2. Inferior controllers: The assessments and recommendations from the safety management group must actually be implemented by middle managers, engineers, and operators. Determine how successfully absorbed lessons-learned and recommendations flow throughout the system.

44. Human Cognition Characteristics: Safety management should be staffed with well-respected individuals. Safety management can be a tough job, and safety professionals are often seen as the ones that say "no" on the organization. At times, the safety management may be one of the only forces counteracting increasing risk. The recommendations of safety personnel carry more weight if the group is respected.

45. Human Physiology: N/A

46. History: Examining the history of interaction with external bodies can reveal hazards. For example, a string of recent waivers granted to external agencies may indicate that regulatory processes are weak. A recent history of accident-free operations may lead to hazards, for example, in the form of growing complacency and the demand for faster product delivery.

47. Pressures: The effect of pressures on interaction with external bodies can be great. Organizations are subject to political and financial pressures to foster good relationships with external organization such as governments, suppliers, citizens groups, and unions. Hazards can occur when decision-makers within the organization attempt to please outside organizations at the expense of safety via waiving, violating, ignoring, or reprioritizing safety constraints.

48. Resources: For adequate interaction with external bodies, resources must be made available. The United States, for example, sets aside funds for State Department interactions with foreign countries for the promotion of US culture and goodwill. Identify the external bodies that the agency should interact with and set aside time, attention, and funds to support exchanges.

49. Tools and Interface: Tools for the aid of interaction with external bodies can be advantageous to secure good outcomes. For example, during negotiations, information sharing can be aided through the use of executable real-time simulation tools that show the affect of various policy options.

50. Training: Complex negations and decisions take place with groups outside the organization. Identify and ensure that training for organization decision-makers is adequate for these kinds of interactions.

51. Safety Culture: The safety culture of external bodies can affect the interaction or agreements reached during interactions with external bodies. See item 6 for more information.

52. Data Communication: Identify what communication procedures and policies exist to ensure that external bodies are kept informed as to the organization's ongoing vision, goals, and operational state. Assess external stakeholders to determine if they are aware of the consequences of potential accidents to them and the risk of such accidents. Determine what stakeholders understand about how risk of potential accidents has been minimized and what mitigations have been implemented.

53. Human Cognition Characteristics: N/A

54. Human Physiology: N/A

REFERENCES:

[1]. J. Rasmussen, "Risk management in a dynamic society: A modeling problem," *Safety Science*, vol. 27, no. 2/3, pp. 183-213, 1997.

[2]. J. Reason, "The Contribution of Latent Human Failures to the Breakdown of Complex Systems," *Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences*, vol. 327, no. 1241, pp. 475-484, 1990.

[3]. J. Reason, "A Systems Approach to Organizational Error," *Ergonomics*, vol. 38, no. 8, pp. 1708-1721, 1995.

[4]. E. Hollnagel, *Barriers and Accident Prevention.* Ashgate Publishing Ltd., 2004.

[5]. N. Leveson, "A new accident model for engineering safer systems," *Safety Science*, vol. 42, no. 4, pp. 237-270, 2004.

[6]. F. Manuele, *On the practice of safety*, 3rd ed. Hoboken, NJ: John Wiley & Sons, 2003.

[7]. N. Leveson, *Safeware: System Safety and Computers*. Addison-Wesley Publishing Company, 1995.

[8]. N. Leveson, *Engineering a Safer World*. MIT Press, expected 2010.

[9]. C. Perrow, *Normal accidents: Living with high-risk technologies*. Princeton University Press, 1999.

[10]. K. Weiss *et al.*, "An Analysis of Causation in Aerospace Accidents," in *Proceedings of the Digital Aviation Systems Conference*, Daytona, FL, 2001, pp. 137-147.

[11]. B. Tyler *et al.*, *HAZOP: Guide to Best Practice*, 2nd ed. IChemE, Rugby, 2008.

[12]. M. Stringfellow, "A Safety-driven System Design Process," S.M. thesis, Dept. Aero. and Astro. Eng., MIT, Cambridge, MA, 2008.

[13]. D. Pumfrey, "The principled design of computer system safety analyses," Dept. of Computer Science, Univ. of York, 1999.

[14]. J. McDermid, "Software Hazard and Safety Analysis," in *Proceedings of the Ninth Annual Conference on Computer Assurance*, Gaithersburg, MD, 1994, pp. 17-25.

[15]. S. Shappell and D. Wiegmann, "The human factors analysis and classification system—HFACS," Civil Aeromedical Institute, Oklahoma City, OK, Office of Aviation Medicine Technical Report DOT/FAA/AM-00/7, 2000.

[16]. E. Hollnagel *et al*., Eds., *Resilience Engineering: Remaining sensitive to the possibility of failure*, Aldershot, UK: Ashgate Publishing Co., 2008.

[17]. S. Dekker, *Just culture: Balancing safety and accountability*, Aldershot, UK: Ashgate Publishing Co., 2007.

[18]. S. Dekker, *The field guide to understanding human error*, Aldershot, UK: Ashgate Publishing Co., 2006.

[19]. S. Dekker, *Ten Questions About Human Error: A New View of Human Factors and System Safety*. Mahwah, NJ: Lawrence Erlbaum Associate Inc., 2005.

[20]. S. Dekker, "Resilience Engineering: Chronicling the Emergence of Confused Consensus," in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, *et al.*, Eds. Burlington, VT: Ashgate Publishing Co., 2006, pp. 77-92.

[21]. M. Cummings, "Ethical and social issues in the design of weapon control computer interfaces," in *Proceedings of the 2003 International Symposium on Technology and Society, Crime Prevention, Security and Design*, ISTAS/CPTED, 2003, pp. 14-18.

[22]. M. Cummings and P. Mitchell, "Automated scheduling decision support for supervisory control of multiple UAVs," *AIAA Journal of Aerospace Computing, Information, and Communication*, vol. 3, no. 6, pp. 294-308, 2006.
[23]. J. Drury and S. Scott, "Awareness in Unmanned Aerial Vehicle Operations," *International Journal of Command and Control: Special Issue on Awareness in Command and Control Environments*, vol. 2, no. 1, pp 1-28.
[24]. E. Diehl and J. Sterman, "Effects of Feedback Complexity on Dynamic Decision Making," *Organizational Behavior and Human Decision Processes*, vol. 62, no. 2 pp. 198-215, May 1995.
[25]. N. Repenning and J. Sterman, "Getting quality the old-fashioned way: self-confirming attributions in the dynamics of process improvement," in *Improving Theory and Research on Quality Enhancement in Organizations*, R. Cole and R. Scott, Eds. Thousand Oaks, CA: Sage, 1997.
[26]. P. Senge *et al.*, *The Fifth Discipline Fieldbook.* New York, NY: Currency Doubleday, 1995.
[27]. E. Cagno *et al.*, "Risk analysis in plant commissioning: the Multilevel HAZOP," *Reliability Engineering and System Safety*, vol. 77, no. 3, pp. 309-323, 2002.
[28]. T. Kletz, *HAZOP and Hazan*, Rugby, UK: Institution of Chemical Engineers, 1974.
[29]. E. Hollnagel, *Barriers and accident prevention*, Aldershot, UK: Ashgate Publishing Ltd., 2004.
[30]. B. Kirwan, "Validation of human reliability assessment techniques: Part 1 -- Validation issues," *Safety Science*, vol. 27, no. 1, pp. 25-41, Oct. 1997.
[31]. B. Kirwan, "Validation of human reliability assessment techniques: Part 2 -- Validation results," *Safety Science*, vol. 27, no. 1, pp. 43-75, Oct. 1997.
[32]. A. Swain and H. Guttmann, "Human reliability analysis with emphasis on nuclear power plant applications" USNRC, Washington, DC, Report No. NUREG/CR-1278, 1983
[33]. A. Swain, "Accident sequence evaluation program human reliability analysis procedure," USNRC, Washington, DC, Report No. NUREG/CR-4722, 1987.
[34]. A. Klinke and O. Renn, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies," *Risk Analysis*, vol. 22, no. 6, pp. 1071-1094, 2002.
[35]. D. Krathwohl, *Methods of educational & social science research: An integrated approach*. Reading, MA: Addison Wesley Longman Inc., 1998.
[36]. T. LaPorte and P. Consolini, "Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations," *Journal of public administration research and theory*, vol. 1, no. 1, pp. 19-48, 1991.
[37]. D. Learmount, (2009, September 24). "Computers can't replace pilots - yet, say experts," Available: http://www.flightglobal.com/articles/2009/09/24/332716/computers-cant-replace-pilots-yet-say-experts.html.
[38]. D. Petersen, *Techniques of safety management: a systems approach*, 4th ed., New York, NY: American Society of Safety Engineers, 1989.
[39]. T. Kletz, "Engineer's view of human error," Inst. of Chemical Eng., 2008.
[40]. W. Hammer, *Handbook of system and product safety*. Englewood Cliffs, NJ: Prentice-Hall, 1972.
[41]. S. Simon, "The Culture Change Model of Behavioral Safety," in *Proceedings of Light Up Safety in the New Millennium*, Des Plaines, IL, 1998, pp. 192–207.

[42]. T. Smith, “What’s wrong with behavior-based safety,” *Professional Safety*, vol. 44, no. 9, pp. 37–40, 1999.
[43]. T. Backstrom, “Risk Assessment As a Part of Continuous Safety Management,” in Society for Risk Analysis-Europe, June 1997.
[44]. T. Licu *et al.*, “EUROCONTROL--Systemic Occurrence Analysis Methodology (SOAM)--A "Reason"-based organisational methodology for analysing incidents and accidents,” *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1162-1169, Sept. 2007.
[45]. A. Arnold, “A Qualitative Comparative Analysis of SOAM and STAMP in ATM Occurrence Investigation,” M.S. thesis, Lund Univ., Lund, Sweden, 2008.
[46]. P. Gonçalves, “When do minor shortages inflate to great bubbles,” in *Proceedings of the 2002 International System Dynamics Conference*, System Dynamics Society: Albany, NY, 2002.
[47]. C. Johnson, “Interactions between Night Vision and Brownout Accidents: The Loss of a UK RAF Puma Helicopter on Operational Duty in Iraq, November 2007,” in *Proceedings of the US Joint Weapons Systems Safety Conference*, Huntsville, AL, 2009.
[48]. C. Johnson, “Insights from the Nogales Predator Crash for the Integration of UAVs into the National Airspace System under FAA Interim Operational Guidance 08-01,” in *Proceedings of the 27th International Conference on Systems Safety*, Huntsville, AL, 2009.
[49]. C. Johnson, “Military Risk Assessment in Counter Insurgency Operations: A Case Study in the Retrieval of a UAV Nr Sangin, Helmand Province, Afghanistan, 11th June 2006,” in *Proceedings of the Third IET Systems Safety Conference*, Birmingham, UK, 2008.
[50]. T. Quinn *et al*., “Lab turnaround time and delayed discharges: a systems-based action research investigation,” in *Proceedings of the 2005 International System Dynamics Conference*, System Dynamics Society: Boston, MA, 2005.
[51]. E. Hollnagel and R. Amalberti, “The emperor’s new clothes: Or whatever happened to “human error”,” in *Proceedings of the 4th International Workshop on Human Error, Safety and Systems Development*, pp. 1–18, 2001.
[52]. N. Leveson *et al.*, “Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems,” *Organization Studies*, vol. 30 no. 2-3, pp. 227, 2009.
[53]. C. Perrow, *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press, 1999.
[54]. K. Weick *et al.*, “Organizing for High Reliability,” *Research in Organizational Behavior*, vol. 21, pp. 81–123, 1999.
[55]. T. La Porte and P. Consolini, “Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations,” *Journal of Public Administration Research and Theory*, vol. 1, pp. 19–47, 1991.
[56]. A. Swain, “Human reliability analysis: Need, status, trends and limitations,” *Reliability Engineering & System Safety*, vol. 29 no. 3, pp. 301-313, 1990.
[57]. Z. Mohaghegh *et al.*, “Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization,” *Reliability Engineering and System Safety*, vol. 94, no. 5, pp. 1000-1018, 2009.

[58]. D. Vaughan, "The dark side of organizations: Mistake, misconduct, and disaster", *Annual Review of Sociology*, vol. 25, no. 1, pp. 271–305, 1999.
[59]. K. Weick and K. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks", Administrative Science Quarterly, vol. 38, no. 3, pp. 357-381, 1993.
[60]. N. Leveson, "Role of software in spacecraft accidents", Journal of spacecraft and Rockets, vol. 41 no. 4, pp. 564–575, 2004.
[61]. R. Lutz and R. Woodhouse, "Requirements analysis using forward and backward search," *Annals of Software Engineering*, vol. 3 no. 1, pp. 459-475, 1997.
[62]. W. Verhoeff from Dutch Safety Board, personal communication, November, 2009.
[63]. J. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston, MA: Irwin/McGraw-Hill, 2000.
[64]. E. Wolstenholme *et al.*, "Coping but not coping in health and social care: masking the reality of running organizations beyond safe design capacity," *System Dynamics Review*, vol. 23, no. 4, pp. 371-389, 2007.
[65]. K. Marais *et al.*, "Archetypes for organizational safety," *Safety Science*, vol. 44 no. 7, pp. 565-582, 2006.
[66]. F. Previc and W. Ercoline, *Spatial Disorientation in Aviation*, Reston, VA: American Institute of Aeronautics & Astronautics, 2004.
[67]. J. Carroll, "Incident reviews in high-hazard industries: sense making and learning under ambiguity and accountability," *Organization & Environment*, vol. 9, no. 2, pp. 175, 1995.
[68]. K. Roberts *et al.*, "Must Accidents Happen? Lessons from High-Reliability Organizations [and Executive Commentary]," *The Academy of Management Executive*, vol. 15, no. 3, pp. 70–79, 1993.
[69]. K. Roberts, "Some characteristics of one type of high reliability organization," *Organization Science*, vol. 1 no. 2, pp. 160–176, 1990.
[70]. J. Baker *et al*., "The report of the BP US refineries independent safety review panel," *British Petroleum*, 2007.
[71]. M. Stringfellow *et al.*, "Healthcare Industry Incentive Structures Pressure System Operators to Operate in a High-risk Risk State," in *Proceedings of the International System Dynamics Conference*, Albuquerque, NM, 2009.
[72]. N. Leveson, "Intent specifications: An approach to building human-centered specifications," *IEEE Transactions on Software Engineering*, vol. 26, no. 1, pp. 15–35, 2000.
[73]. P. Shrivastava, *Bhopal: Anatomy of a crisis*. Cambridge, MA: Ballinger Publishing Company, 1987.
[74]. E. Schein, "Three cultures of management: The key to organizational learning," *Sloan Management Review*, vol. 38, no. 1, pp. 9–20, 1996.
[75]. D. O'Hare *et al.*, "Cognitive failure analysis for aircraft accident investigation," *Ergonomics*, vol. 37, no. 11, pp. 1855-1869, Nov. 1994.
[76]. K. Marais, " A New Approach to Risk Analysis with a Focus on Organizational Risk Factors," PhD. dissertation, Dept. of Aero. and Astro., MIT, Cambridge, MA, 2005.
[77]. J. Rasmussen, "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models," *IEEE TRANS. SYS. MAN CYBER.*, vol. 13 no. 3, pp. 257–266, 1983.
[78]. Meeting with the Dutch Safety Board. Den Haag, Netherlands, November 4, 2009.

[79]. C. Holloway and C. Johnson: "On the Prevalence of Organizational Factors in Recent U.S. Transportation Accidents," in *Proceedings of the 23rd International System Safety Conference*, San Diego CA, Aug. 2005.
[80]. K. Rygh, "Accident Investigations-Meeting the challenge of new technology," in *Constituents of Modern System-safety Thinking*. F. Redmill and T. Anderson, Eds. London, UK: Springer, 2005.
[81]. K. Amos, (2009, December 13). "Accidents and disasters keep happening—but why?" Available: http://findarticles.com/p/articles/mi_qa3739/is_200005/ai_n8901678/
[82]. K. Weick, "Making sense of blurred images: Mindful organizing in Mission STS-107," in *Organization at the Limit-Lessons from the Columbia Disaster*, W. Starbuck, M. Farjoun, Eds. Malden, MA: Blackwell Publishing, 2005, pp. 159–177.
[83]. S. Shorrock *et al.*, "Individual and group approaches to human error prediction - a tale of three systems," in *IBC Conference on Preventing Human Errors and Violations*, London, Feb., 2003.
[84]. I. Svedung and J. Rasmussen, "Graphic representation of accident scenarios: Mapping system structure and the causation of accidents," *Safety Science*, vol. 40, pp. 397-417, 2002.
[85]. GasCo Report, MIT CSRL, 2008.
[86]. E. Wiener and D. Nagel, *Human factors in aviation*. San Diego, CA: Academic Press, 1988.
[87]. *Hazard and operability studies (HAZOP studies)- Application Guide*, British Standards Institution, London, UK, 2002.
[88]. D. Kirmse. *Process Improvement Engineering: Hazard and Operability (HazOp) Studies*, University of Florida, Gainesville, FL, 2001.
[89]. *Attempted takeoff from wrong runway, Comair Flight 5191, Bombardier CL-600-2B19, N431CA, Lexington, Kentucky, August 27, 2006*, National Transportation Safety Board, Washington DC, Aircraft Accident Report NTSB/AAR-07/05.
[90]. R. Weibel, "Safety considerations for operation of different classes of unmanned aerial vehicles in the National Airspace System," S.M. thesis, Dept. of Aero. and Astro., MIT, 2005.
[91]. M. Peterson, "UAV and the Current and Future Regulatory Construct for Integration into the National Airspace System," *J. Air L. & Com.*, vol. *71*, pp. 521, 2006.
[92]. A. Degani and E. Wiener, "Cockpit Checklists: Concepts, design, and use," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. *35* no. 2, pp. 345–359, 1993.
[93]. B. Hales and P. Pronovost, "The checklist--a tool for error management and performance improvement," *Journal of Critical Care*, vol. 21 no. 3, pp. 231-235, 2006.
[94]. P. Checkland, *Systems Thinking, Systems Practice*. New York, NY: John Wiley & Sons, 1981.
[95]. M. Jackson, *Systems Approaches to Management*, New York, NY: Springer, 2000.
[96]. P. Checkland, "Systems Thinking," in *Rethinking management information systems*, W. Currie and R. Galliers, Eds. Oxford, UK: Oxford University Press, 1999.
[97]. L. Bertalanffy, *General System Theory: Foundations, Development, Applications*, Revised Edition, George Braziller, 1976.
[98]. G. Lewes, *Problems of Life and Mind*, vol. 2, 1st ed. London, UK: Trubner and Co., 1875.

[99]. H. Heinrich, *Industrial accident prevention: A scientific approach*. New York, NY: McGraw-Hill, 1931.
[100]. I. Ismail, "Assessment of Safety Level in Performing Building Maintenance Work in Malaysia," M.S. thesis, Dept. of Civil Eng., Univ. Teknologi, Malaysia, Dec. 2006.
[101]. F. Bird and R.G. Loftus, *Loss control management*, Loganville, Institute Press, 1976.
[102]. D.M. Murphy and M.E. Paté-Cornell, "The SAM Framework: Modeling the Effects of Management Factors on Human Behavior in Risk Analysis," *Risk Analysis*, vol. 16, no. 4, pp. 501-515, 1996.
[103]. J. Misumi *et al.*, *Nuclear Safety: A Human Factors Perspective*, Philadelphia, PA: Taylor and Francic Inc., 1999.
[104]. K. Davoudian *et al*., "The Work Process Analysis Model (WPAM)," *Reliability Engineering and System Safety*, vol. 45, pp. 107-125, 1994.
[105]. S. Cox and T. Cox, "The structure of employee attitudes to safety - a European example," *Work and Stress*, vol. 5, no. 2, pp. 93 – 106, 1991.
[106]. Health and Safety Commission, "Third report: organizing for safety," ACSNI Study Group on Human Factors, HMSO, London, UK, 1993.
[107]. N. Pidgeon and M. O'Leary, "Man-Made Disasters: why technology and organizations (sometimes) fail," *Safety Science*, vol. 34, pp. 15 – 30, 2000.
[108]. Eurocontrol, "Implementation of a "Just Culture" Concept," presented at the 36th Session of the Assembly of the International Civil Aviation Organisation (ICAO), Montréal , CA, 2007.
[109]. S. Dorsey *et al*., "Is Handwashing Teachable?: Failure to Improve Handwashing Behavior in an Urban Emergency Department," *Academic Emergency Medicine*, vol. 3, no. 4, pp. 360-365, 1996.
[110]. M. Stringfellow *et al*., "Safety-Driven Design for Software-Intensive Aerospace and Automotive Systems," *Proceedings of the IEEE Special Issue on Aerospace and Automotive Software*, vol. 98, no. 4, 2010.
[111]. *Air Traffic Organization Safety Management System Manual*, Version 2.1, Federal Aviation Administration, Washington DC, 2008.
[112]. FAA Advisory Circular AC 120-92, "Introduction to Safety Management Systems for Air Operators," 22 June 2006.
[113]. R. Weibel, "Assuring Safety through Operational Approval: Challenges in Assessing and Approving the Safety of Systems-Level Changes in Air Transportation," Ph.D. dissertation, Aero. and Astro. dept., MIT, Cambridge, MA, 2009.
[114]. N. Dulac and N. Leveson, "Incorporating Safety in Early System Architecture Trade Studies," in *International System Safety Conference Proceedings*, San Diego, CA, 2005.
[115]. A. Lo, "The Adaptive Markets Hypothesis: Market Efficiency from an Evolutionary Perspective," *Journal of Portfolio Management*, vol. 30, pp. 15-29, 2004.
[116]. Course Notes, Engineering Risk Benefit Analysis, MIT 16.862, Spring 2007.
[117]. D. Woods *et al., Behind human error: Cognitive systems, computers, and hindsight*. Wright Patterson AFB, OH: Crew System Ergonomics Information Analysis Center, 1994.
[118]. FAA Order 8020.11B, "Aircraft Accident and Incident Notification, Investigation, and Reporting," 16 August 2000.
[119]. J. Pfeffer, *The Human Equation: Building Profits by putting People First*. Cambridge, MA: Harvard Business Press, 1998.

[120]. E. Patterson and D. Woods, "Shift changes, updates and the on-call model in space shuttle mission control," *Computer Supported Cooperative Work: The Journal of Collaborative Computing*, vol. 10, no. 3-4, pp 317-346, 2001.
[121]. F. Jacob and M. Ehret, "Self-protection vs. opportunity seeking in business buying behavior: an experimental study," *Journal of Business & Industrial Marketing*, vol. 21, no. 2, pp. 106, 2006.
[122]. L. Loukopoulos *et al.*, *The Multitasking Myth*, London, UK: Ashgate, 2009.
[123]. T. Sheridan, "Human centered automation: oxymoron or common sense?" in *IEEE International Conference on Systems Man and Cybernetics*, vol. 1, Vancouver, BC, Canada, 1995, pp. 823–828.
[124]. J. Reason, *Managing the Risks of Organizational Accidents*, Aldershot, UK: Ashgate Publishing, 1997.
[125]. NTSB, "NTSB Incident CHI06MA121 – Full Narrative," Washington DC, 2007. Available: http://www.ntsb.gov/ntsb/brief2.asp?ev_id=20060509X00531&ntsbno=CHI06MA121&akey=1
[126]. J. Buys and J. Clark, *Events and Causal Factors Analysis*, Revised by J. Kington-Howlett, Idaho Falls, Idaho: Technical Research and Analysis Center, SCIENTECH Inc., 1995.
[127]. G. Carrigan *et al.*, "Human Factors Analysis of Predator B Crash," in *Proceedings of AUVSI: Unmanned Systems North America*, San Diego, CA, 2008.
[128]. C. Johnson and C. Shea, "The Hidden Human Factors in Unmanned Aerial Vehicles," in *Proceedings of the 26th International Conference on Systems Safety*, Vancouver, Canada, 2008.
[129]. E. Stimpson *et al.*, "Managing Risks in Civil Aviation: A Review of the FAA's Approach to Safety," Blue Ribbon Panel Appointed May 1, 2008 by Secretary of Transportation Mary E. Peters, Washington DC, September 2, 2008. Available: http://www.aci-na.org/static/entransit/irt_faa_safety_9-08.pdf.
[130]. D. Schulze, private communication, Feb. 2010.
[131]. J. Schmidt *et al.*, "Human Factors Analysis & Classification System-Maintenance Extension (HFACS-ME) Review of Select NTSB Maintenance Mishaps: An Update," School of Aviation Safety Naval Postgraduate School, Monterey, CA, 2000.
[132]. R. Wachter and P. Pronovost, "Balancing "No Blame" with Accountability in Patient Safety," *New England Journal of Medicine*, vol. 361, no. 14, pp. 1401-1406, 2009.
[133]. Course Notes, System Safety, MIT 16.863, Spring 2006.
[134]. NTSB, "NTSB Identification FTW04TA237 – Full Narrative," Washington DC, 2005. Available: http://www.ntsb.gov/ntsb/brief2.asp?ev_id=20040920X01463&ntsbno=FTW04TA237&akey=1
[135]. NTSB, "NTSB Identification DCA07MA310 – Full Narrative," Washington DC, 2010. Available: http://www.ntsb.gov/ntsb/brief2.asp?ev_id=20071005X01522&ntsbno=DCA07MA310&akey=1
[136]. NTSB, "NTSB Identification DCA05MA003 – Full Narrative," Washington DC, 2007. Available:

http://www.ntsb.gov/ntsb/brief2.asp?ev_id=20041015X01633&ntsbno=DCA05MA003&akey=1
[137]. NTSB, "Runway Overrun During Landing American Airlines Flight 1420 McDonnell Douglas MD-82, N215AA Little Rock, Arkansas June 1, 1999," NTSB/AAR-01-02, Washington DC, 2001. Available: http://www.ntsb.gov/Publictn/2001/AAR0102.pdf
[138]. NTSB, "NTSB Identification DCA10IA022," Washington DC, 2010. Available: http://www.ntsb.gov/Dockets/Aviation/DCA10IA022/default.htm
[139]. J.K. Liker, *The Toyota way: 14 management principles from the world's greatest manufacturer*, Madison, WI: CWL Publishing Enterprises, Inc., 2004.
[140]. *Procedure for performing a failure mode effect and criticality analysis*, United States Military Procedure MIL-P-1629, 9 November 1949.
[141]. E. Clifton, "Fault Tree Analysis – A History," in *Proceedings of the 17th International Systems Safety Conference*, Orlando, FL, 1999, pp. 1-9.
[142]. H. Kumamoto *et al*., *Probabilistic risk assessment and management for engineers and scientists*. New York, NY: IEEE press, 1996.
[143]. Course Notes, System Safety, MIT 16863, Spring 2006.
[144]. J. Carroll, "Introduction to Organizational Analysis: The Three Lenses," MIT Sloan School of Management Working Paper, 2002.
[145]. J. Carroll, private communication, May 2010.
[146]. S. Dekker, "Report of the Flight Crew Human Factors Investigation Conducted for the Dutch Safety Board into the Accident of TK1951, Boeing 737-800 near Amsterdam Schipol Airport, February 25, 2009," Lund, Sweden, 2009.
[147]. Course Notes, Human Factors, MIT 16.400, Fall 2001.
[148]. Course Notes, System Safety, MIT 16.863, Spring 2006.
[149]. R. Jagacinski and J. Flach, *Control Theory for Humans: Quantitative Approaches To Modeling Performance*, Mahwah, NJ: Lawrence Erlbaum Associates, Inc., 2003.
[150]. Course Notes, High-Tech Start-ups, MIT 15.962, Winter 2010.
[151]. NTSB, "Eastern Airlines Lockheed L-1011, N334EA Miami International Airport Miami, Florida May 5, 1983," NTSB/AAR-84-04, Washington DC, 1984.
[152]. N. Sarter and D. Woods, "Pilot Interaction With Cockpit Automation II: An Experimental Study of Pilots' Model and Awareness of the Flight Management System," *The International Journal of Aviation Psychology*, vol. 4, no. 1, pp. 1-28, 1994.
[153]. F. Soliman and M. Youssef, "The role of SAP software in business process re-engineering," *International Journal of Operations and Production Management*, vol. 18, pp. 886–895, 1994.
[154]. S. Shorrock, "Individual and Group Approaches to Human Error Identification: HAZOP and Tracer-lite Compared For Three ATM Systems," Eurocontrol Experimental Centre, Bretigny-sur-Orge, France, EEC Note No. 08/03 Volume II, 2003.
[155]. R. Helmreich *et al*., "The Evolution of Crew Resource Management Training in Commercial Aviation," The International Journal of Aviation Psychology, vol. 9, no. 1, pp. 19, 1999.
[156]. C. Lamb, "Collaborative Systems Thinking: An Exploration of the Mechanisms Enabling Team Systems Thinking," Ph.D. dissertation, ESD, MIT, Cambridge, MA, 2007.
[157]. M. Sanders and E. McCormick, Human Factors In Engineering and Design, 7th ed. New York, NY: McGraw-Hill Science/Engineering/Math, 1993.

[158]. N. Dulac, "A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems," Ph.D. dissertation, Dept. of Aero. Astro. Eng, MIT, Cambridge, MA, 2007.
[159]. I. Sveudng and H. Radbo, "Feedback for Pro-activity: Who Should Learn What from Events, When and How," in *Nordic perspectives on safety management in high reliability organizations: Theory and applications*, O. Svenson et al., Eds. Stockholm, Sweden: Nordic Nuclear Research, 2006.
[160]. B. Fischoff *et al.*, *Acceptable Risk*, Cambridge, UK: Cambridge University Press, 1983.
[161]. Y. Haimes, *Risk Modeling, Assessment, and Management*, New York, NY: Wiley-Interscience, 1998.
[162]. D. Wiegmann and S. Shappell, "Human error analysis of commercial aviation accidents: Application of the Human Factors Analysis and Classification System (HFACS)," *Aviation, Space, and Environmental Medicine*, vol. 72, no. 11, pp. 1006–1016, 2001.
[163]. M. Gladwell, "The Ethnic Theory of Plane Crashes "Captain, the weather radar has helped us a lot."" in *Outliers: The Story of Success*, New York, NY: Little, Brown and Company, 2008.
[164]. J. Thomas, Personal Communication, August 2010.
[165]. Course notes, Air Traffic Control 16.72, Fall 2006.
[166]. M. Couturier, "A Case Study of Vioxx using STAMP," M.S. thesis, Engineering Systems Division, MIT, Cambridge, MA, 2010.
[167]. *Citichem: Impossible Accident*, 1986, transcript, provided by Dutch Safety Board, 2009.
[168]. R. Brown (2010, August 27). "In Oil Inquiry, Panel Sees No Single Smoking Gun," Available: http://www.nytimes.com/2010/08/28/us/28hearings.html
[169]. M. Dierks, Personal Communication, September 2010.
[170]. B. Glaser, *Basics of grounded theory analysis*, Mill Valley, CA: Sociology Press, 1992.
[171]. C. Robson, *Real world research, 2*nd ed. Malden, MA: Blackwell Publishers Inc., 2002.
[172]. FAA, "NextGen Implementation Plan", Washington DC, 2010.