A Systems Approach to Patient Safety: Preventing and Predicting Medical Accidents Using Systems Theory

by

Aubrey Samost

S.B. Chemical Engineering
Massachusetts Institute of Technology, 2010

SUBMITTED TO THE ENGINEERING SYSTEM DIVISION IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTERS OF SCIENCE IN ENGINEERING SYSTEMS
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2015

Signature of author: _____
Engineering Systems Division
May 8, 2015

Certified by: _____
Nancy Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Co-Supervisor

Certified by: _____
Stan Finkelstein
Senior Research Scientist, Engineering Systems Division
Thesis Co-Supervisor

Accepted by: _____
Munther A. Daleh
William A. Coolidge Professor of Electrical Engineering and Computer Science
Acting Director, Engineering Systems Division

Page intentionally left blank.

A SYSTEMS APPROACH TO PATIENT SAFETY: PREVENTING AND PREDICTING MEDICAL ACCIDENTS USING SYSTEMS THEORY

by
Aubrey Samost

S.B. Chemical Engineering
Massachusetts Institute of Technology, 2010

Submitted to the Engineering Systems Division on May 8, 2015
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Engineering Systems

ABSTRACT

Patient safety has become a critical concept in healthcare as clinicians seek to provide quality healthcare to every patient in a healthcare system that has grown far more complex than the days of the independent doctor and his black bag making house calls. Accidents in present-day healthcare systems are complicated, with environmental factors, interactions between clinicians, and the pressures exerted by managerial decisions all contributing to these medical mishaps. Despite this complexity, accidents are analyzed using simplistic and outdated techniques modeling systems as mere linear chains of events, when the reality lies far from those neat cause and effect relationships. Further compounding efforts to promote patient safety is the reliance on reactive approaches to safety, waiting for accidents to occur before enacting changes, like a dangerous game of whack-a-mole. What little work is done in prospective hazard analysis tends to be concentrated in niche areas and relies heavily on older analytic techniques.

This thesis demonstrates the use of systems theory based accident and hazard analysis techniques, CAST and STPA respectively, in healthcare systems. It shows proof of concept applications in two distinct fields of healthcare, accident analyses in cardiac surgery and a prospective hazard analysis in a radiation oncology process. These techniques were very amenable to adaptation to healthcare applications. The accident analyses a rich set of accident causal factors leading to a large number of strong design options to prevent future accidents. The hazard analysis identified 84 potential unsafe controls and over 200 possible causal scenarios requiring a design change to create a safer system. This work sets up future work into direct comparisons with other hazard and accident analysis techniques applied in the healthcare domain as well as larger scale studies to understand the potential impact on patient safety. Finally, this work highlights the growing role for system and safety engineers in the healthcare field to help deal with the complexity of ensuring that every patient receives safe and effective healthcare.

Thesis Co-Supervisor: Nancy Leveson
Title: Professor Aeronautics and Astronautics and Engineering Systems

Thesis Co-Supervisor: Stan Finkelstein
Title: Senior Research Scientist, Engineering Systems Division

Page intentionally left blank.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisors, Professor Nancy Leveson and Dr. Stan Finkelstein. They introduced me to a new way of thinking and seeing the world around me. Additionally, they pushed me to learn the skills of a researcher and academic. For this knowledge, I will be forever grateful.

Second, thank you to all of the students in the lab for creating a wonderful environment for learning and trying new ideas. Being able to talk about safety across domains taught me a lot about how to approach my research. A special thanks for John Thomas and Cody Fleming for their invaluable advice and assistance throughout this entire process!

Next I need to thank my family for always supporting me. My parents instilled in me a love of learning from an early age, and encouraged me through all of my years of education. My brothers always put up with me and challenged me when I would come home with new ideas. For all of their love, I owe them a large debt of gratitude.

Finally, and most importantly, thank you to my wonderful fiancé, Chris. I love you with all of my heart, and I can't imagine walking the road of life without you. Anytime through this process that I would get frustrated or hit a wall, you were there to help me through. You helped me organize my thoughts and were always willing to serve as a sounding board, an editor, and a cheerleader, whichever I most needed at the time. I hope you always know how immensely grateful I am for you!

Page intentionally left blank.

Table of Contents

1 Introduction

In 1999, the Institute of Medicine declared that the US healthcare system killed between 49,000 and 98,000 patients per year with medical errors (Kohn, Corrigan, & Donaldson, 1999). To get comparable numbers, the aviation industry would need to crash a jumbo jet daily.

Since 1999 many researchers have attempted to replicate those early studies used in that report. Health systems across the country rallied to the cause of promoting patient safety. Checklists, crew resource management, LEAN, and the Toyota Production System became essential components of any hospital quality improvement and patient safety department. And yet, a 2013 meta-analysis concluded that the older studies were missing many medical errors and that there had been no improvement as an industry. Instead, 210,000-400,000 patients die prematurely every year because of medical errors in the US alone (James, 2013). This statistic makes medical errors potentially the third leading cause of death in all age groups in the US, a sobering metric for an industry that seeks to heal.

How can an industry that is painfully aware of its safety problems continue to struggle with this problem? Clinicians hold a patient's life in their hands and feel personally responsible when outcomes are poor. There is a well described phenomenon of the second victim, the psychological harm to the practitioner after a medical error has occurred and a patient has been hurt. These persistent safety problems are not due to a lack of caring amongst clinicians.

If clinicians are motivated to promote safety, then why has it been so challenging to change these trends? Healthcare has slowly been coming to the realization that safety is a system property and the only way to tackle a system property is through systems thinking and systems approaches. Systems engineers have begun to work in the healthcare space bringing with them an arsenal of tools and techniques to shake up healthcare.

Why is systems engineering an appropriate approach to the problems that healthcare faces with patient safety? Delivering care to the patient no longer depends on the solo doctor traveling around with his black bag full of tools making house calls to the patients he has known since birth. This romantic notion of healthcare has been replaced by a complex sociotechnical system. A single doctor cannot understand, let alone deliver, all of the complicated new treatments for disease that have multiplied in the last decades. It takes a team of personnel each with a specialized niche to work together and integrate their services into a cohesive care plan for the patient. To realize this treatment goal this human system must also interact smoothly and seamlessly with technology, which itself must show strong interoperability. And all of this must be accomplished across many unique healthcare settings and individual contacts with the patient as they move between inpatient hospitalizations, outpatient clinic visits, and home care.

Add all of the above mentioned complexity into a complicated payment and regulatory structure and suddenly one sees the value of taking a system perspective. Decisions made at the insurance companies can cause large effects at the level of the patient's bedside. Regulators pulling a drug off the market send pharmacies scrambling to renegotiate their formularies to try to provide continuous care to their

patients. Time pressure from financial incentives foisted on hospital management trickles down into pressure on the general practitioners, whose primary goal is to keep a patient healthy. Paradoxically, as the pressure to drive costs lower increases and the time with the patient decreases, the patients become sicker and the costs to the system merely rise. None of these problems can be solved at the level of the hospital or the level of the regulators. Rather we must look to the system as a whole to understand the effects of the changes that we make.

As in all of complex systems, though, it can be incredibly difficult to see the effects of our actions. As in the above examples, cause and effect is no longer a simple linear relationship. As a solo practitioner wandering around making house calls, we knew that if the patient got better it was because of our actions and, conversely, a worsening patient could also be linked to our actions. But what is the cause behind rising healthcare costs? Or the cause behind a patient of a multi-disciplinary team who fails to control their diabetes? What is the cause of a medication misadministration? Is it the nurse, who pushed the wrong drug? Or is it the pharmacist, who dispensed the wrong medication? The physician might have written the order wrong. Or maybe we should just blame management because they refused to upgrade from their poor computerized physician order entry system. Can we even identify just one cause to every effect in a complex system?

This loss of clear causality makes the job of understanding errors and mistakes incredibly challenging. And yet, how can a system grow safer if it cannot understand the roots of its risk? Many researchers have tackled this problem and yet there is no consensus in the field of how best to investigate accidents, learn from mistakes, improve the system, or predict where our greatest risk lies. The goal of this thesis is to adapt an accident model and its attendant analytic techniques for use in healthcare to promote learning from accidents and improvements to system design to promote safety.

This thesis will begin with a review of the current literature in system safety. It will first delve into accident models building from the Domino Theory, through to reliability based models, and then into systems theory based models. It will then explore the hazard and accident analysis techniques derived from the accident models with a focus on their applications in healthcare.

The second chapter of this thesis delves into application of a systems theory based accident analysis technique through the analysis of a series of 30 incidents in a cardiac surgery department. The results from the analyses as well as the design recommendations for prevention of future accidents will be discussed. The individual accident analysis results will then be aggregated to try to elucidate an understanding of how a systems theory based accident analysis technique compares to the industry standard techniques as well as what can be learned about the underlying risks in the system.

In the third chapter, this thesis will move on to look at radiation oncology system as a model for applying a prospective hazard analysis technique also based in systems theory. This hazard analysis technique has been applied extensively to medical devices and in most industries, but has yet to be demonstrated for investigating risk in clinical workflows in the radiation therapy arena.

Finally, this thesis will conclude with several ideas for future research directions in the field of applying systems engineering ideas to safety in healthcare, specifically in the fields of accident and hazard analyses.

Overall, this thesis represents an incremental, yet hopefully important, step towards safety in healthcare. It presents a proof of concept application of a systems theory based accident and hazard analysis techniques to a new domain, opening the door to future work in creating healthcare specific adaptations to these techniques or further understanding of implementation of new ideas in promoting learning and safety.

2 Literature Review

To increase the safety of a system, one can take two major approaches. The first is to learn from accidents, and the second is to identify hazards in order to guard against accidents in the future. This literature review will look briefly at several accident causality models, move on to accident analysis techniques based on those models, and then end with a brief survey of hazard analysis techniques. The emphasis will be on the techniques utilized most commonly in healthcare and will survey several examples of their applications.

2.1 Accident Causality Models

Accident causality models are the theories of how accidents occur. These models underpin the analytic techniques and can greatly influence the results found in analysis. How an analyst believes an accident occurred leads to what they investigate and how they think about preventing future accidents. It shapes the entire investigative approach, impacting the data collected and the framework the data are considered within (N. G. Leveson, 2011; Shealy, 1979).

2.1.1 Domino Theory

One of the earliest models of accident causation is the Domino Theory. It was first proposed by H.W. Heinrich in 1931. This theory promotes the idea that accidents are caused by a series of dominoes collapsing in a chain. The last event in the chain is the accident, but it only falls because of the "dominoes" that come before. The accident occurs because of an unsafe act of a person or exposure to unsafe machinery. These unsafe acts or mechanical conditions are caused by faults of people, which are themselves the results of genetics or the environment (Heinrich, 1931). However, assuming their faults are due to genetics leads to the idea that if we fire operators involved in accidents then we can make our workplace safer. The human error perspective on accidents persists even as researchers have argued against that limiting perspective (Dekker & Leveson, 2014; N. G. Leveson, 2011; Reason, 1995).

2.1.2 Swiss Cheese Model

The field of system safety and human factors realized that an accident model based mostly on human behavior limited the effectiveness of the responses to accidents and limited understanding. Several models that looked beyond just the front-line operators and included management began to show up beginning in the 1970s, most prominently a new school of thought that organizational and managerial factors greatly influenced accidents (Turner & Pidgeon, 1997; Turner, 1978). The model most utilized in healthcare has been Reason's Swiss Cheese Model (Reason, 2000).

The Swiss Cheese Model, like the Domino Theory, assumes that a linear chain of events leads up to an accident. Unlike Heinrich's work, Reason builds in corporate culture. Corporate culture is comprised of management decisions and organizational processes, which act to create error and violation producing conditions in the local climate. The local climate then impacts the behavior of the front line workers, leading to errors or violations. These errors or violations then can find holes in the defense barriers and lead to accidents. The holes in the defense barriers are called "latent failures" in this model, and they

are impacted by the management decisions and organizational processes at the start of the chain (Reason, 1995).

Reason builds a framework that describes human error associated with this accident causation model. The first distinction he proposes is slips and lapses versus mistakes. Slips and lapses are a failure of the execution of a task, and mistakes are a failure of the planning or problem solving phase. The second distinction is in errors versus violations. Violations are intentional deviations from defined practice; these are not typically intended to produce bad outcomes. An example of a routine violation might be a worker "cutting corners" from a defined procedure to save time. The final distinction made in this model is between active and latent human failures. Active failures are those actions taken (or not taken) that immediately lead to an accident. Latent failures are temporally distant from the accident and typically set up conditions that will lay dormant until an active, local failure coincides to cause an accident (J Reason, 1995).

The Swiss Cheese Model moves away from blaming the individual for accidents. It recognizes that there are other organizational factors contributing to these unsafe scenarios. Reason argues that "when an adverse event occurs, the important issue is not who blundered, but how and why the defences [sic] failed" (Reason, 2000). A system moves towards an accident as unsafe acts breach each sequential layer of defense. This accident trajectory can only occur when the "holes" in the defensive barriers have aligned. This mindset leads to a probabilistic perspective, where additional layers of defense are built in search of a higher reliability system.

2.1.3 Systems-Theoretic Accident Model and Processes (STAMP)

As systems have grown more complex, accident causes have become proportionately complicated. Simple linear chain of events models cannot always capture the complex interactions in present-day accidents. Accidents can occur without any system components failing, making a new accident causation model necessary. Leveson utilized systems theory to describe these non-linearities in a novel accident causation model called Systems-Theoretic Accident Model and Process (STAMP) (N. G. Leveson, 2011).

The foundation of STAMP is the concept that safety is an emergent property. It arises from the interactions of the components of a system, rather than from those individual components themselves as linear chain of event models propose. To this end, accidents are modeled as problems of control, where an accident occurs because the system controls were insufficient to constrain the behavior to a safe operating realm.

STAMP is based primarily on three key concepts: safety constraints, hierarchical control structures, and process models, all derived from systems theory.

Safety constraints, rather than events, are the basic unit of analysis in techniques using STAMP. These are requirements placed on the system to ensure safe operation. For example, Leveson looks at the case of an automated train door. A top level system safety constraint on the door is that it must only open when it is safe for passengers to exit the train. This safety constraint is then translated into

requirements on all of the components of the system. For example, the behavior of the door might have a requirement such as the door must not open if the train is not aligned with the station. STAMP theorizes that accidents occur when these constraints are violated (N. G. Leveson, 2011). People fall out of the door when the door opens and the train is misaligned from the platform.

Systems theory is based on the understanding of a system as a series of controllers organized in a hierarchical control structure. The control structure can be used in analyzing the above mentioned safety constraints. A controller constrains the behavior of the controller below it in the structure through issuing control actions. For every control action, the controller also requires feedback from the layer below to understand how its controls are impacting the system. The presence of this feedback allows the controller to adapt to changes in the system. It is through this dynamic structure that systems can constrain behavior to safe behaviors while still adapting to exogenous changes. While the control structures may themselves be static, the control algorithms and control action create a dynamic equilibrium in which the system exists.

Feedback, therefore, plays a key role in allowing the system to remain in this safe operating equilibrium. This feedback is used by the controller to update its process model, the last key element of the STAMP accident causation model. The process model, sometimes called the mental model in a human, is the controller's understanding of the system that it is controlling.

There are four conditions required in a control loop. The first is a goal for the system, which is also known as a safety constraint. Safety constraints, discussed above, define the safe operating space for the system. The second requirement is an action condition. This is the control action issued by the controller to alter the behavior of the process that is down a layer in the control structure. Without these actions, a controller would be unable to impact or control the system around it. The third condition is called an observability condition, which is merely that there must be some way for the controller to observe the current state of the system being controlled. The fourth condition required in a control loop then is the model condition, which in this case is the controller's process model. It is the synthesis of the feedback into a coherent understanding of the state of the system under the controller's control. Process models are comprised of the feedback received from the system synthesized with the controller's understanding of how the system behaves and responds to its control actions. Incorrect or incomplete process models can explain unsafe actions in many, if not most, accidents (N. G. Leveson, 2011).

STAMP uses these four conditions to identify how accidents occur. This model of accident causation can then be expanded into techniques for accident analysis, hazard analysis, and early conceptual design analysis. This thesis will consider two of these basic types of analysis—accident analysis and hazard analysis. Accident analysis is a retrospective analysis aimed at understanding why an adverse event occurred. Hazard analysis attempts to identify accident causes before they occur so the accident can be prevented.

2.2 Accident Analysis Tools

"Incident reviews are important vehicles for self-analysis, knowledge sharing across boundaries inside and outside specific plants, and development of problem resolution efforts" (Carroll, 1998). An organization learns by studying what went wrong in accidents. Towards this end, there have been many accident analysis tools created and researched over the last several decades. This literature review will look at the general idea of a root cause analysis in healthcare: a specific RCA technique from the Department of Veterans Affairs and a STAMP-based approach called CAST, Causal Analysis Based on STAMP.

2.2.1 Root Cause Analysis in Healthcare

Root cause analysis (RCA) is a general term for investigating accidents with the goal of understanding the underlying errors and causes of the incident. There is no one formal methodology for completing a root cause analysis. Healthcare RCA processes (Wu, Lipshutz, & Pronovost, 2008) have marked heterogeneity. However, all RCAs specifically answer three different questions (Wu et al., 2008):

1. What happened in the accident?
2. Why did the accident occur?
3. What can be done to prevent it in the future?

Root cause analyses have lofty goals, but frequently fail to successfully or optimally answer the above questions. Some of the common issues are "root cause seduction," prioritization of causes with easy solutions, and self-censoring in the final reports (Carroll, 1998). "Root cause seduction" is the idea that because the analysis is called a root cause analysis it subconsciously leads to the idea that there is one primary reason for the error. This assumption is satisfying, making it appear that there is one obvious and easy way to fix the solution and prevent a similar accident in the future. The assumption also leads to the widely accepted idea that a root cause analysis should identify no more than two or three findings because of fear of diluting the report (Carroll, 1995).

Another common issue with root cause analyses is the desire to focus solely on causes that appear to be immediately linked to the accident and have an easy fix. This desire leads to a focus on component failure problems and human errors (Carroll, 1998). Systemic fixes tend to be less apparent and larger fixes to implement, so analysts tend to shy away from making these recommendations for preventing future accidents (Carroll, 1998).

Finally, a common issue with RCA comes from the way that it is implemented. Any investigation and recommendation must require the approval of both management and front line workers. This approval requirement raises challenges in that any identified causal factors of the accident that appear to implicate either group tends to become watered down in the political process of reporting and creating changes in the system (Carroll, 1998). This is the idea of an "acceptability heuristic" where changes that

are not going to pass this political process are not recommended in the final reports, even when they may lead to safety (Carroll, 1995).

The aforementioned problems with root cause analysis are not inherent to any one accident analysis technique. Root cause seduction comes from the idea of a root cause, but the desire to focus on politically acceptable and easy to fix solutions is a hurdle that any accident analysis technique will have to cross.

2.2.2 VA Root Cause Analysis

In healthcare, the Department of Veterans Affairs uses a specified methodology, called the VA RCA, designed to force the user to consider systemic factors beyond the performance of the operator. Specifically, in each RCA the analysts aim to answer four questions: "What happened? Why did it happen? What action can we take to prevent it from happening again? How will we know if the action we took made a difference?" (*Root Cause Analysis Tools*, 2015). Procedurally, the VA RCA procedures lead the analyst to answer these larger questions by guiding the analyst through a series of more detailed questions, such as details about the rules in place, the work environment, or the IT system, explicitly pushing the analyst away from considering only the human operator.

Beyond the analysis process itself, researchers at the VA also created a tool for assisting managers in deciding which close calls and accidents warrant investigation called the safety assessment code (SAC). The SAC is a risk matrix that takes the probability of reoccurrence and the severity into account to generate a number from one to three, where three represents the highest priority incidents ("Safety Assessment Code Matrix," 2014). The most severe incident category involves death or permanent disability, and the least serious category involves no clinically significant harm. Probability ranges from frequent, occurring multiple times in a year, to remote, occurring maybe once in the next 5-30 years. Both severity and probability have four coded categories ("Safety Assessment Code Matrix," 2014). These scores are used to prioritize incidents to assist in distributing analytic resources.

The VA health system serves 8.76 million patients per year at over 1700 clinics and hospitals ("Veterans Health Administration," 2015), which all use the VA RCA methodology to investigate their incidents. Results of RCAs can be reported centrally and used to share lessons learned in patient safety. A study of 139 of the VA medical centers showed that hospitals and clinics completed between 3 and 59 RCAs per year, averaging 4.86 analyses per hospital per year. Hospitals that spent more money tended to complete more accident analyses than more resource-poor facilities. The relationship of the number of RCAs to safety was tougher to tease out because of these confounding factors, but the data suggested a reduction in postoperative complications as more RCAs were completed (Percarpio & Watts, 2013).

Additionally, the outcomes of RCAs themselves have been analyzed in several studies. The results of 137 RCAs for suicidal and parasuicidal behavior in a hospital setting showed that only 68.1% of recommendations were ever implemented. Of these recommendations, 48% involved a policy change, 30% staff re-training, and 14% generated a specific clinical change (Mills, Neily, Luan, Osborne, & Howard, 2006). A similar study looking at aggregate RCAs for falls showed that 61.4% of

recommendations were fully implemented and another 20.9% had been partially implemented. Despite this, 34.4% of facilities reported a decrease in falls, and 38.9% reported a decrease in major injuries due to falls (Mills, Neily, Luan, Stalhandske, & Weeks, 2005).

2.2.3 Causal Analysis Based on STAMP (CAST)

Unlike RCAs, which treat accidents in a narrative, linear fashion, Causal Analysis Based on STAMP (CAST) is grounded in systems theory, making the analysts more likely to capture more causes as well as those that are indirectly linked to the accident. Additionally, it forces the analyst to consider causes at all levels of the control structure, beyond merely looking at the clinical workers and clinical work environment. The focus of CAST is to understand not only what someone did wrong but to take it further and describe why they might have made the wrong decision or taken the wrong action (N. G. Leveson, 2011).

The analysis begins by taking a system view and asking what hazards were involved in the loss. It then moves on to consider the loss from the perspective of each level of the hierarchical control structure. Each controller is analyzed with a focus on understanding their safety requirements and responsibilities, the controls in place, the context of their unsafe actions, and the reasons for their flawed actions or communications (N. G. Leveson, 2011).

In aviation accidents, CAST has been shown to lead analysts to identify more causal factors beyond operator error. One such example is in the investigation of the Comair 5191 failed takeoff at the Blue Grass Airport in Lexington, KY. The official NTSB investigation declared the accident the result of pilot error for breaching sterile cockpit protocol. A CAST analysis however, prompted the analyst to consider other aspects of the accident. This analysis found that, for example, one of the contributors to the accident was the ongoing construction at the airport with inadequate signage and outdated airport maps (Nelson, 2008). The CAST analysis drew a very different conclusion from the NTSB's analysis and pointed towards a cause that could have impacted any pilot taking off at LEX during that time span.

Prior to this thesis work, CAST had not been applied to a healthcare accident. CAST was used as a comparison to VA RCA in analyzing a practice clinical case from the VA health system (O'Neil, 2014). The fictional accident involved a patient receiving a fluoroscopically guided fine needle aspiration of a lung nodule. The patient then suffered from an unrecognized iatrogenic pnuemothorax, which grew to 50% of the lung field before being recognized and treated, leading to an unanticipated extension of the hospitalization. CAST identified more causal factors than the VA RCA analysis.

2.3 Hazard Analysis Tools

Hazard analysis is a prospective risk analysis, complementary to accident analysis, which is a retrospective analysis of the system. Like accident analysis techniques, there are many ways to analyze a system prospectively. Hazard analysis tools may be quantitative, qualitative, or some combination of both. Quantitative tools tend to be probability based, providing some quantitative measure of the likelihood of various unsafe outcomes in the system. Qualitative tools typically provide some form of model of the system and describe potential accidents, using those descriptions to help design safety

counter-measures. Combined techniques tend to use some form of qualitative model, which then gets translated into quantitative estimates using real world data or expert estimates. This literature review will focus on techniques that have been used in the medical field. Specifically, we will consider failure mode effects analysis, fault tree analysis, and systems-theoretic process analysis.

2.3.1 Failure Mode Effects Analysis

Failure mode effects analysis (FMEA) is a bottom-up technique for analyzing risk prospectively based on a linear chain of events accident causality model. There are many variations of FMEA, but the one most commonly used in healthcare is referred to as a functional FMEA. This type of analysis is built off of the process map, where each stage of the process is analyzed for potential failures. One process for completing a functional FMEA in a healthcare setting is as follows (Ford et al., 2009). First the process is mapped into separate steps. Each step then is analyzed, beginning with the analyst considering potential failure modes, such as the corruption of an image file or the use of a file for the wrong patient. Then the analysts are prompted to come up with a cause of this failure mode. Finally, they consider the effects of this failure mode. The analysts then assign each potential failure mode an RPN (risk probability number). The RPN is derived by multiplying the assumed likelihood of the cause leading to the failure mode, the severity of the patient's outcome should the failure mode occur, and a likelihood that the failure mode will not be identified. Each of these metrics is scored 1-10 and then multiplied together to give the RPN, ranging from 1-1000. The RPN is designed to prioritize the failure modes, so resources can be assigned where they are most needed (Huq et al., 2008). Note that the probabilities used are usually unknown and often unknowable.

Failure mode effects analysis has been applied to many different areas in healthcare. The Joint Commission, a hospital accrediting body, requires a hazard analysis as part of the hospital's accreditation package (Stewart, 2015). Pursuant to fulfilling this requirement, hospitals have used FMEA on a wide range of processes, including providing external beam radiation therapy (Ford et al., 2009), delivering chemotherapy to pediatric inpatients (van Tilburg, Leistikow, Rademaker, Bierings, & van Dijk, 2006), and selecting new intravenous administration pumps (Wetterneck et al., 2006).

FMEA has several limitations that hamper its use in analyzing healthcare processes. From a theoretical standpoint, through the use of the process map, FMEA focuses on the idea of direct cause and effect relationships between underlying causal factors and potential accidents. Particularly, it looks at the likelihood of a component failing, making it an analysis of the reliability of a system rather than its safety. Reliability and safety are not the same thing. Numerous accidents have occurred in systems that behaved reliably, with no failing components, and yet still had an accident (N. G. Leveson, 2011). From a practical standpoint, many groups researching healthcare applications highlight the large amounts of time and personnel required to complete an analysis, which requires a large commitment from management (van Tilburg et al., 2006; Wetterneck et al., 2006). Additionally, teams bring a bias to the analysis based on the most recent or most publicized incidents that they have seen, leading them to rate these as more likely or more severe than incidents that have not recently occurred (Ford et al., 2009; van Tilburg et al., 2006). Finally, and arguably most importantly, there is concern regarding the

reproducibility of the RPN, which is a semi-quantitative measure of risk and based heavily in expert estimates rather than being grounded in empirical data (Ford et al., 2009) Nobody knows what these probabilities are in most situations leading to a wide range of heuristic biases in making these estimations. These biases introduce systemic bias in the hazard analysis (N. G. Leveson, 2015). Despite these limitations, FMEA remains the predominant hazard analysis methodology utilized in healthcare safety.

2.3.2 Fault Tree Analysis

Fault tree analysis, FTA, is a top down hazard analysis technique. It was developed in 1961 for the intercontinental ballistic missile system. Several researchers have applied the idea to healthcare systems (Marx & Slonim, 2003; Wreathall & Nemeth, 2004).

The analyst begins by defining the scope of the system and the hazards of interest. The analyst then moves on to constructing trees comprised of events linked by Boolean logic to form scenarios leading to the top level hazard identified. The scenarios can provide the basis for a qualitative analysis of the system. Analysts can go further and assign probabilities to each component of the analysis to get an overall metric of the probability of the hazard occurring in their system (N. G. Leveson, 1995). However, to complete this quantitative analysis typically involves more data than are available regarding the system's future behavior, which is the same problem with FMEA.

Additionally, fault trees are not designed to handle human behavior in a system beyond the simple descriptor "human or operator error." In applying FTA to healthcare, researchers have made an effort to include more guidance on modeling humans in the system, using different values for the probability of human error by using clinicians' experiences to decide how likely a human is to make a mistake at any given point in the system (Marx & Slonim, 2003). However, at the end of the day, these are still estimates and subject to heuristic biases and lack of information. In addition, such estimates provide little insight into the behavior of humans in the larger systems in which they are working. Assigning a probability for a human mistake (in any system) means implying that human behavior is unrelated to the design and conditions of the system in which it occurs. In addition, forcing each step in a process into a decision with a binary outcome removes the nuance that can be important in creating safe systems, especially when dealing with humans. Human behavior is a spectrum, but a model with binary outcomes forces the analyst to draw an artificial line between "good" and "bad" behavior, which does nothing to contribute to design solutions for safety (Wreathall & Nemeth, 2004). Additionally, this technique remains less accessible to clinicians with no engineering background, making FTA spread more slowly in a healthcare context (Marx & Slonim, 2003).

2.3.4 System-Theoretic Process Analysis (STPA)

System-Theoretic Process Analysis (STPA) is a top down hazard analysis technique based on STAMP. As a top down hazard analysis technique, the analyst begins with identifying the system level hazards and accident and the overall system structure. There are two main steps to performing the STPA analysis once these top level characteristics have been identified. For convenience the analysis can be divided

into two steps, but that is not necessary. In step one, the analyst identifies potential unsafe control actions that could move the system outside of its safe operating region. In step two, the analyst identifies scenarios that might lead to these unsafe control actions (N. G. Leveson, 2011). These scenarios can then be used to guide design changes to increase system safety.

There are four types of unsafe control actions: a control action required for safety is not provided, a control action that should not be provided is provided, a control action is provided in the wrong timing or order, or a control action is continued for too long or too short a duration. Once the unsafe control actions are identified for a particular system, they can then be used to create formal requirements for the system to operate safely. A formal (mathematical) semantics has been defined for unsafe control actions which allows for the automation of step 1 of the hazard analysis as well as for the introduction of formal logical rules to ensure completeness (Thomas, 2013).

In step two, potential causal scenarios are identified for each of the unsafe control actions. For example, an analysis of a radiation therapy proton gantry identified the unsafe control action "treatment is started when there is no patient at the treatment point" (Antoine, 2013). This unsafe control action could be caused by a scenario where the operator is required to turn on the beam for some other activity, such as trouble shooting, but the dose is accidentally given to a patient (Antoine, 2013). These scenarios are best identified by having a safety engineer and a domain expert working together collaboratively.

STPA has been applied to medical device design and use, as in the example above with the proton gantry (Antoine, 2013). Additional uses in the healthcare and medical device domain include interoperability of medical devices (Proctor, Hatcliff, Fernando, & Weininger, 2015), analysis of a recalled medical device (Balgos, 2012), and the use of a new electronic health record system in radiation oncology (Daartz & Kang, 2015).

2.4 Summary

Improving system safety requires learning from past and preventing future accidents. Learning and prevention are limited by the analytic tools available to the analysts. Currently most of the research and work in healthcare is done using older tools, such as root cause analysis for accident investigation and FMEA for hazard analysis. The use of these tools limits the results because of the limitations of the linear accident causality models underlying them. Other industries have applied STAMP, based on systems theory, to analyze accidents and hazards with great success, finding more accident causal factors and identifying more hazardous scenarios. STAMP is much newer than the other techniques and experience with the associated analysis tools is limited, but early experimental and clinical results look promising.

3 Applying CAST to Healthcare Accidents: A Cardiac Surgery Case Study

One critical aspect of moving an organization towards becoming safer is the ability to learn from mistakes and apply those lessons to make effective system changes. Uses of CAST on real accidents have identified many important causal factors not found by other traditional techniques (Arnold, 2009; Dong, 2012; Hickey, 2012; Nelson, 2008) and has been applied to a training case in the healthcare domain (O'Neil, 2014). This chapter demonstrates the application of CAST to a group of accidents from a cardiac surgery department with the goal of identifying common causal factors and recommending strong potential approaches to preventing future accidents.

Rush Medical Center has been collecting data on incidents for the past three years using an in-house incident reporting system. Additionally, unexpected clinical outcomes are investigated by the clinical team to determine if the outcomes were caused by preventable errors. Through this process, 30 incidents were identified from 380 consecutive complex cardiac surgical cases. In conjunction with the Rush Medical Center research team, these incidents were reanalyzed using CAST. No further accident investigation was possible because of the temporal distance from several of the events. The data for the analysis came from the initial incident report, the department's subsequent investigation (where applicable), and personal observations of workflows and equipment at Rush Medical Center in the cardiac operating rooms.

This project initially began as an evaluation of the surgical checklist used throughout all of the operating rooms. The hospital had implemented a generic checklist derived from the WHO Surgical Safety Checklist (Haynes et al., 2009), which they were using across all of the operating rooms, regardless of surgical specialty. Despite this surgical checklist, there were still accidents occurring in cardiac surgery. The working hypothesis of the Rush Medical Center research team was that improving the checklist would prevent these accidents. CAST was used to identify the causal factors underlying the accidents and develop recommendations for preventing future accidents moving beyond merely changing the checklists.

3.1 Event Details

The thirty incidents ranged in severity from no clinical consequences to unexpected patient death. Distributions are shown in Table 1.

Patient Outcomes	Number (%)
Death	2 (7.7)
Prolonged Hospitalization	1 (3.8)

Prolonged “on-pump” time	3 (11.5)
Prolonged anesthetic (off-pump)	16 (61.5)
Aborted Procedure	2 (7.7)
No clinical or sub-clinical consequences	2 (7.7)

Table 1. Patient Outcomes (data missing for four incidents)

The outcomes in Table 1 are laid out in order of decreasing severity, where patient death is the most severe outcome and sub-clinical consequences the least severe. Prolonged procedure time is divided here into two categories, prolonged “on-pump” time and prolonged anesthetic (off-pump) because of the differences in clinical risk to the patient. “On-pump” time refers to the period of the surgery where the patient’s heart is not beating and their physiology is being supported by a cardiac bypass pump. The risk of bleeding, stroke, and hemodynamic instability is elevated during this period relative to the remainder of the operative time.

There was also heterogeneity in the proximal events leading up to the accident. These were coded and are presented in Table 2. These proximal events were the frontline events directly leading up to the accident, analogous to the symptoms that a patient presents with when they are ill. These events’ causes, though, lay in the system design.

Incident Category	**Number (%)**
Miscommunication during staff handoff throughout the procedure	4 (13.3)
Missing medication prior to incision	4 (13.3)
Missing instrumentation leading to intra-operative delay	8 (26.7)
Missing implants leading to delays and sub-optimal implants being used	3 (10.0)
Broken and/or improperly handled specialized instruments	9 (30.0)
Miscellaneous incidents	2 (13.3)

Table 2. Proximate Accident Events

As a physician uses lab data and imaging to diagnose a patient, so the safety engineer uses analytic techniques to identify the factors contributing to accidents in a system.

3.2 Representative Analysis

To better understand these incidents, we performed CAST analyses of all thirty incidents. The level of detail in each analysis varied with the level of detail available this far after the accidents. Where the detail existed, analysis was completed and recommendations were generated. If the accident was missing details, questions were generated to help guide a potential investigation. One accident analysis is detailed here to illustrate the process utilized with emphasis on healthcare specific aspects of the analytic process.

3.2.1 Incident Description

A 56 year old African American male with a history of heart failure was stable with an implanted left ventricular assist device. He moved to the top of the UNOS transplant list after experiencing persistent drive line infections. An organ became available and he was taken to the operating room. The transplant was completed without complication and the patient returned to the Intensive Care Unit in stable condition. Several hours post operatively the patient showed signs of decreased cardiac function. He was treated with immunosuppression for presumptive acute graft rejection. Despite maximal support for several days the patient's cardiac function never returned and he expired. Upon reviewing his chart several weeks later it was discovered that pre-operative immunosuppression had been ordered but had never been given to the patient, contributing to the patient's death.

Upon discovering this incident, two more incidents of missing pre-operative immunosuppression were discovered by the clinical staff. It was proposed that the preoperative checklist be changed to include a check of preoperative immunosuppression in transplant cases. As of this writing, that recommendation had not been implemented.

3.2.2 Control Structures

Individual control structures were created for each incident to capture the level of detail appropriate for the incident. Generally, they all followed a similar structure with operating room or nursing management at the top and the patient at the bottom. In the middle, typically the physician filled the role of directing treatment goals through placing orders or surgical requests and the nurse carrying out those orders on the patient. The control structure for this particular incident is shown in Figure 1. This structure represents the system as it ideally operates. The best way to create this control structure is through observation and working with a domain expert who has been immersed in the system. The role of the safety analyst is then to ask the right questions to elicit the system details from the domain expert.

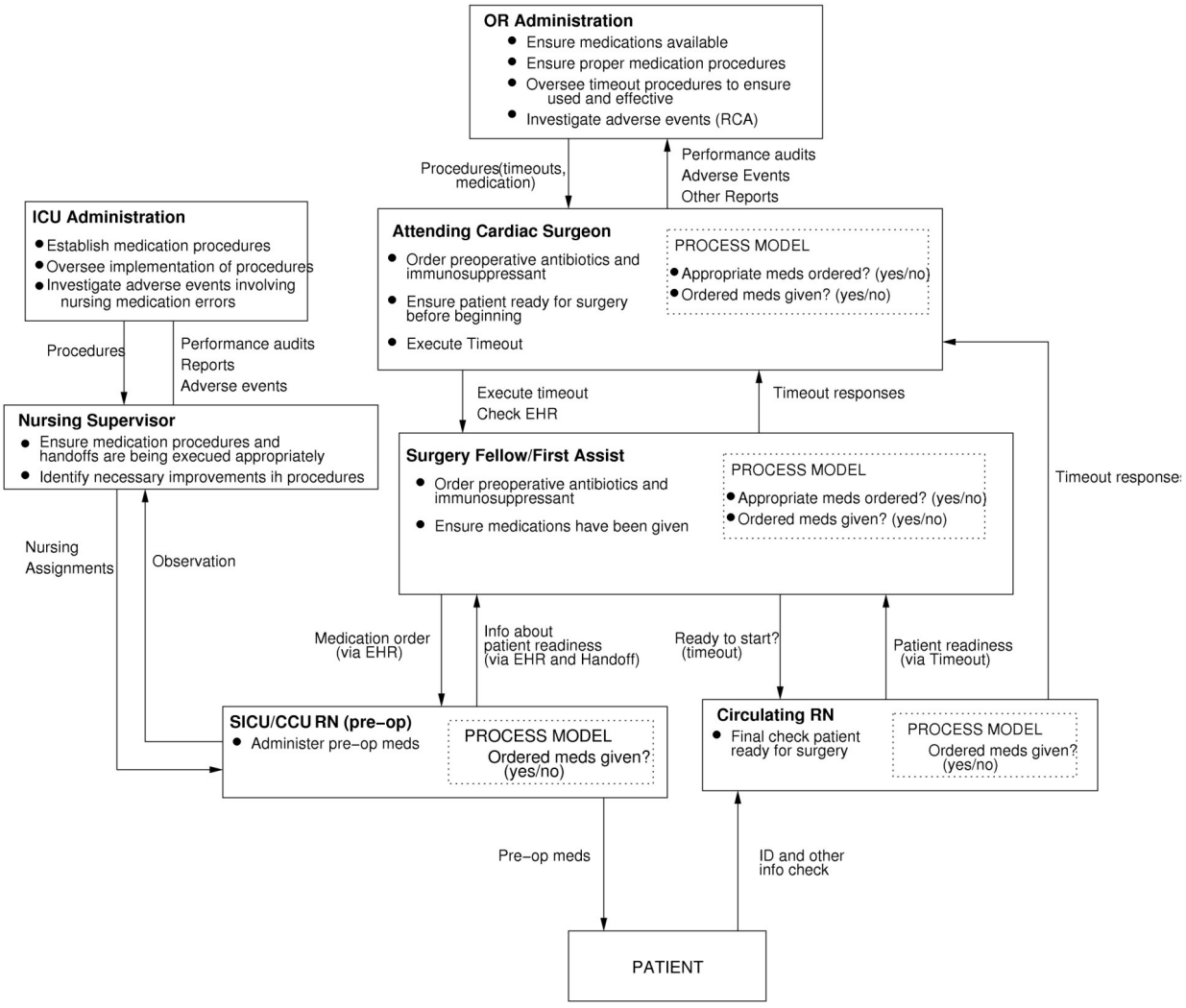

Figure 1. Hierarchical control structure for missing immunosuppression cases

The hierarchical control structure for this incident is limited to the controllers in two clinical areas, the Surgical Intensive Care Unit/Critical Care Unit (SICU/CCU) and the operating room. These are modeled as two separate control hierarchies. Functionally, these two units operate independently of each other with separate responsibilities, personnel, policies, and geographic space despite sharing ultimate responsibility for providing safe care to the patient. There may, however, be communication between them.

An important modeling decision was to treat the electronic health record (EHR), a piece of software, as an actuator and a sensor rather than as a controller. Typically software is considered as a controller. However, in this particular model, the EHR is used to communicate information between the nursing and physician staff as a way of passing control actions or providing information about the controlled process. The EHR will become important in considering the actions of those particular controllers in the analysis.

3.2.3 Analysis of Controllers

CAST, as outlined in (N. G. Leveson, 2011), is done by first identifying the controllers in the relevant control structure with respect to their responsibilities for ensuring safety and the unsafe control actions that occurred in this particular accident. Then the reasons why those unsafe actions seemed correct to them are identified. These reasons may include process model flaws, the environmental context, or communication problems, for example.

Many accident investigations stop with identifying what a person did wrong and then conclude that they have identified the cause of the accident. However, stopping after identifying unsafe actions is akin to merely blaming the operator or attributing the accident to human error. The purpose of an accident analysis is not to define blame or culpability for the accident. Rather analysts seek to prevent this type of accident in the future. Therefore, after identifying the proximate events leading to the accident, the next step is to explain why it made sense to the operator to take the action that in retrospect was incorrect. How did the context impact their behavior? Understanding why something happened, instead of just "who did what to whom", leads to changes in system design that promote safety in the future.

In explaining "why", the analysis look at flaws in the person's mental model that might explain their actions, as well as the contextual factors that might have influenced the unsafe behavior. Then, in the discussion, the analysis moves toward understanding why the mental model was wrong or why it made sense for the person to act the way they did. The final step is to identify recommendations for changes that might improve decision making or actions in the future.

Following this process allows for direct traceability from accident causal factors (process model flaws and contextual factors) to recommendations. This traceability serves two functions: ensuring that all causal factors are addressed and providing a rationale for system changes. This rationale allows analysts and engineers in the future to understand why these particular policies exist and what to consider when changing them.

The analysis begins at the level of the local actors, looking at the Surgical Intensive Care Unit (SICU)/Critical Care Unit (CCU) and Operating Room (OR) nurses and the surgical team, as shown in Table 3.

Controller	**Analysis**
SICU/CCU RN (pre-operative nurse)	***Safety Responsibilities*** • Administer pre-operative medications • Report concerns about patient to the surgical team ***Unsafe Control Actions*** • Did not give pre-operative immunosuppression • Did not tell surgical team that the patient had not received the medication ***Process Model Flaws*** • Not aware that they needed to give the immunosuppression [PF-2]

	Contextual Factors • New leadership in cardiac surgery pushing cardiac transplants after several years of doing very few, so they weren't very familiar with that particular operation [CF-3] • Antibiotics are ordered as part of the pre-operative order set but the floor nurses do not give them; they are instead given in the OR. This could have caused confusion about who was responsible for giving the immunosuppression [CF-4] • The order in the EHR does not specify who is responsible for carrying out the order [CF-5]
Circulating RN (Operating Room Nurse)	***Safety Responsibilities*** • Final check that the patient is ready for surgery ***Unsafe Control Actions*** • Did not stop surgery from proceeding despite the patient not having received immunosuppression ***Process Model Flaws*** • Believed the patient had received immunosuppression [PF-1] ***Contextual Factors*** • Nobody mentioned a concern in the timeout [CF-6] • On the order screen of the EHR there is no record of whether an order has been acknowledged and carried out [CF-1] • The pre-operative time out checklist is a generic OR checklist, so it does not explicitly ask about pre-operative immunosuppression [CF-7]
Surgical Team (Attending and Fellow or Physician Assistant)	***Safety Responsibilities*** • Order pre-operative antibiotics and immunosuppression • Ensure that patient is ready for surgery before beginning • Execute Time-Out ***Unsafe Control Actions*** • Began surgery without patient received prophylactic immunosuppression ***Process Model Flaws*** • Ordered the immunosuppression and so believed that the patient had received it [PF-1] ***Contextual Factors*** • On the order screen of the EHR there is no record of whether an order has been acknowledged and carried out [CF-1] • Patients all came from Cardiac Care Unit where the surgical team knows and trusts the nurses so don't feel the need to check up on their work. These nurses also specialize in cardiac patients so (in the mind of the surgical team) they should be very familiar with the pre-operative medications [CF-2]

Table 3. Analysis of local (frontline) controllers

One factor in this accident is the electronic health record (EHR) and the processes for electronically ordering medications. These patients were very sick and would have been at the hospital prior to their

surgery. This means that all pre-operative medications and testing would be ordered by the surgical team the night before to be given by the nurses the morning before the procedure. However, the EHR has a rather poor layout in terms of giving clear orders from the physician to the nursing staff and feedback back to the physician regarding the carrying out of those orders. Orders for pre-operative care are given as an order set. This decreases the chances of the surgical team forgetting to place important orders. On investigating these incidents, it was found that the orders were actually placed, so this intervention worked as intended. However, the order sets do introduce a different source of confusion. These sets include orders that should be carried out by the CCU or SICU nurses as well as orders that are to be carried out by the surgical or anesthetic team in the OR. The orders are given a time to be carried out, but they do not explicitly say who is responsible. In many cases this omission is not a problem. Common surgeries such as a bypass always require pre-operative antibiotics, which are ordered the night before to be given by the anesthetic team in the OR. The nurses in the CCU or SICU know that it is not their responsibility to give these antibiotics despite seeing the order in their order set. However, in the case of a less common surgery like a cardiac transplant, which includes less common orders like immunosuppression, the ambiguity of these order is far more likely to cause confusion about who gives that medication and when.

The other aspect of the EHR that can lead to confusion is the lack of very clear feedback regarding the status of the medications being ordered. To see if the orders were completed, one has to go to an entirely separate screen in the EHR, the electronic medication administration record (eMAR). This lists the medications and the time they were given to the patient. There is nothing in the EHR that will flash bright red or be otherwise very obvious to show that an order was given and not carried out. One has to be looking specifically for it to pick up on this scenario.

There are other factors at work here outside of just the EHR. Another source of feedback to the surgical team from the SICU or CCU nurses about the patient's readiness for the OR is during their handoff when the surgical team picks up the patient for transport to the OR. The handoff is the opportunity for the nursing staff to communicate any concerns and where the surgical team can ask any questions about the patient. However, there is no formal structure to this handoff, leading to important information being forgotten at this time. There are tradeoffs to standardizing the hand off format. The benefit is that information deemed important is always shared or discussed. However, patients are unique, and information that is important in one patient may not important in another. Standardized handoffs may miss some of the nuanced differences between patients that can be critically important in clinical practice.

Another important opportunity for feedback on the patient's readiness for the operation is the pre-operative timeout. The timeout has no question on it regarding pre-operative immunosuppression. The only medication explicitly asked about is the pre-operative antibiotic. It was a design decision to make the timeout checklist generic for every operating room. Designers adapted this checklist from the WHO Surgical Safety Checklist (Haynes et al., 2009). However, neither the original WHO checklist, nor this adapted version, was ever validated in cardiac surgery. Are there components of this checklist that can be improved to prevent this type of accident in the future? There are many questions on the checklist

that do not apply to a cardiac case. Questions regarding the laterality of the surgery and the site marking by the surgeon are made superfluous in the setting of a cardiac patient. You cannot operate on the wrong heart. A question asking specifically whether the patient had gotten pre-operative immunosuppression would have been far more helpful in this scenario. However, there is a balance in writing checklists. Too much detail makes the checklist too long and people will not complete it in a setting with such time pressure as an OR. Too little detail and important things get missed, as in these three scenarios.

Many of the causal factors and unsafe control actions identified at the clinical frontline level can be traced back to problems at the higher levels of the control structure, so the same analysis was completed for the various managerial controllers, shown below in Table 4.

Controller	**Analysis**
OR Administration	***Safety Responsibilities*** • Ensure safe practices in the OR • Maintain medication stocks • Investigate accidents ***Unsafe Control Actions*** • Did not ensure safe practices in the OR ***Process Model Flaws*** • Believed staff knew how to order and administer all medications [PF-3] ***Contextual Factors*** • Separate management silos for surgery and intensive care complicate communication between the two departments [CF-8] • New surgical management [CF-3]
SICU/CCU Administration	***Safety Responsibilities*** • Ensure safe practices in the SICU/CCU • Maintain safe staffing levels • Establish safe medication procedures ***Unsafe Control Actions*** • Did not establish safe, standardized medication procedures for preoperative immunosuppression ***Process Model Flaws*** • Believed staff knew how to order and administer all medications [PF-3] ***Contextual Factors*** • Separate management silos for surgery and intensive care complicate communications between the two departments [CF-8]

Table 4. Management Level Controller Analysis

In analyzing the management levels, the analysis identified many factors that are seen throughout healthcare. Management is divided into autonomous silos operating each division of the hospital. This division makes the boundaries between divisions, such as the line between the SICU/CCU and the OR, risky areas for patient care. Differences in protocols, communication styles, assumptions and expectations all increase the risk of information being missed.

The other contextual factor that played into both the local controllers' actions and the management actions was the new cardiac surgery management. The entire leadership team turned over with new leaders coming to the hospital from other academic medical centers. Every medical center operates slightly differently. They have different specialties and different styles. At this medical center they perform relatively few cardiac transplants every year. Cardiac transplants were an uncommon procedure and thus required a lot of attention when they were performed. Conversely, the new leadership came from a hospital that specialized in performing cardiac transplants. Their goal for Rush was to transform it into a cardiac transplant specialty center. There was no plan in place to help move from a center that rarely performed transplants to one that specializes in them. Cardiac transplants require a team effort, far more than just bringing in surgeons with that specialized surgical experience. The idea of managing change and ensuring safety during these transitions is not an idea that healthcare uses much as an industry. There is no standard procedure for introducing new surgical techniques or transitioning to different types of care delivery. Most institutions improvise as best they can and solve issues when they arise instead of trying to take a proactive approach to safety during periods of transition.

This incident provides an opportunity to consider accident investigation and incident reporting systems. One of the safety responsibilities for the OR management team is to investigate all accidents and implement changes to prevent future incidents. In this case, the accident was not recognized and investigated until several months later after two other similar incidents had occurred. This incident points to several challenges with accident investigation in healthcare. The first is the challenge of even recognizing that an accident has happened. It can be challenging to tease out whether a patient's death or complication was an expected side effect or the result of an adverse event. Cardiac transplant patients can show signs of rejecting the organ and die even in the presence of correct immunosuppressive regimens. It was not until a pattern of harm was seen that a clinician recognized that this was not an unfortunate adverse outcome but was rather an example of preventable harm.

Secondly, there is the incident reporting structure. What constitutes a reportable incident differs from hospital to hospital and department to department. Implementing something more standardized, such as any unexpected hospital death gets reported and investigated might help catch some of the incidents that are not clearly due to accidents or expected physiologic changes.

Finally, there is the process of investigation. Once an accident has been identified and reported to management, management still needs to perform an investigation that will capture meaningful recommendations for system changes to prevent future incidents. In this case, as stated above, the investigation was delayed. When it was finally discovered that the immunosuppression had been ordered but not given, the recommendation was made to add immunosuppression to the checklist. This recommendation has yet to be implemented, suggesting that there is room for improvement in the way that management investigates and responds to accidents.

Interestingly, overall amongst all of the controllers, there were only three unique process model flaws. Many controllers had the same false belief about the system. This finding strongly points to the idea that

there are systemic problems at the root of this accident. An accident cannot be the result of one bad apple or weak clinician when nearly every controller had the same flawed understanding of the system.

There was more diversity among the identified contextual factors relative to the process model flaws. Intuitively, it makes sense to identify more contextual factors. Every controller has a different perspective on the system. They receive different information from different sources to update their mental models. Management controllers rely heavily on incident reports and aggregate metrics while clinicians depend on other clinicians, equipment, and electronic health records to update their mental model. As a result, contextual factors can range from issues with reporting system and management structures to interpersonal communication issues or poor user interface designs.

3.2.4 Recommendations

From the identified process model flaws and contextual factors the research team generated a series of recommendations. These recommendations are all traced back to the contextual factor or process model flaw that they are designed to address. Recommendations can cover more than one causal factor.

> **R-1** Change the EHR to give better feedback to the user about orders that have not been carried out or missing doses of medication [CF-1], [PF-1]
>
> **R-2** Evaluate the pre-operative checklist and consider making changes to make it more specific to cardiac surgery. A checklist designed for every OR is likely to be less useful than more specific designs [CF-6], [CF-7], [PF-1]
>
> **R-3** Make the wording more explicit on order sets as to who is responsible for carrying out the orders in addition to when they should be completed. [PF-2], [CF-4], [CF-5]
>
> **R-4** Institute a more formal handoff of the patient when the surgical team picks up the patient to bring them to the OR. [CF-2], [PF-1]
>
> **R-5** Consider a formal process for management of change [CF-3]
>
> **R-6** Implement an incident reporting system to help track problems, especially on the line between two services (surgery and intensive care) [PF-3]
>
> **R-7 Conduct** weekly meetings between each department's leadership to facilitate communication and create policies and procedures for interactions between staff of two departments [CF-8]

Importantly, these recommendations all went beyond merely changing the checklist. While adding some surgical specificity to the checklist was suggested, other larger and more systemic changes were also recommended. Changes such as implementing a formal management of change procedure go well beyond just preventing missed immunosuppression to promoting safety in other areas of cardiac surgery. While the initial thinking was that a checklist change would prevent most of these accidents in the future, what we found instead was that CAST led us to identify systemic changes that worked by

enforcing safety constraints on the entire safety control structure rather than just improving the reliability of the human operator at the system's lowest level.

3.3 Aggregate Results

CAST analyses were completed on the 30 identified incidents. Some accidents had more detail available than others, so some analyses generated recommendations while others stopped short of that, instead just posing questions that should be answered in the investigation. However, even given the limited information, the analyses give insight into the types of issues that are common in healthcare by looking across these incidents instead of focusing in minute detail on each case individually.

The purposes of accident analyses are to understand the systemic problems contributing to unsafe actions and to be able to generate recommendations based on those problems. The quality of recommendations that an analyst or manager can generate is directly proportional to the quantity and quality of the causal factors identified as well as their creativity and understanding of the system. Therefore, it was important to understand the breadth of contextual factors identified and how that breadth impacted the quality of recommendations that were generated.

To understand and describe the contextual factors, a set of codes was created using a grounded theory approach. With each pass through the contextual factors, data codes became more clearly specified and tailored until a set of five codes remained. These five codes were comprehensive and mutually exclusive within the dataset analyzed. The codes are shown in Table 5 with a definition and representative example.

Code	**Definition**	**Example**
Communication	Human to human communication either face to face, including team interactions, or via some other media (i.e. electronic communication)	Referring to equipment using various names including technical names and eponyms to mean the same thing
Equipment	Issues regarding design of equipment, typically usability problems or lack of feedback. Broken equipment was not considered a contextual factor but rather an incident that needed an explanation.	Poor EHR design does not provide feedback on the status of order fulfillment
Infrastructure	Design and layout of the physical plant space ranging from layout of buildings around campus to the design of the patient rooms.	Blood bank is located nearly ½ mile from the SICU
Management	Department or hospital-wide factors typically dealing with financial decisions, hospital goal setting, and development of safety culture	Financial pressures leading to cutting overtime and forcing staff to cover areas outside of their specialization and training
Process/Policy	Policies and procedures that are either flawed or missing at both the department	No standardized process across specialty services for calling a consult

	level and at the hospital-wide level	

Table 5. Contextual Factor Codes

Coding the contextual factors revealed several insights about these incidents. The majority of the equipment factors were specific to the incident. The various incidents involving broken equipment all had different problems with different pieces of equipment. On the other end of the spectrum, the same management contextual factors kept appearing over a wide range of incidents. New cardiac surgery management and financial and time pressures contributed to many of the accidents, ranging from missing immunosuppression to a delay while a piece of equipment was located. Figure 2 shows the percentage of cases involving contextual factors from each category. On average, each incident had 6.9 contextual factors contributing to the unsafe decisions and actions. As shown below, process/policy and management factors contributed to nearly every accident, while infrastructure played less of a role. This suggests that targeting recommendations that block these management and process contextual factors will have broader impacts than implementing recommendations that work more on a specific piece of equipment or changing the infrastructure of the medical campus.

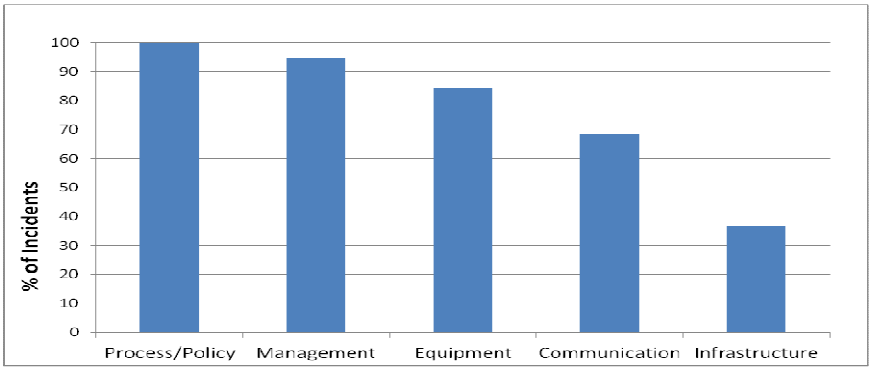

Figure 2. Percentage of incidents involving at least one contextual factor from the given category

As discussed above, the purpose of an accident investigation is to make the system safer by generating recommendations from the identified causal factors that can help controllers constrain the system behavior to the safe realm. The discussion above covered the wide range of types of contextual factors identified and the large number identified per incident, so the next step in evaluating the CAST analyses is to look at the quality of recommendations that these causal factors suggested. While a grounded theory approach to coding was used to analyze the types of contextual factors, for evaluating recommendations the healthcare literature already provides a framework, the Veterans Administration (VA) Action Hierarchy, shown in Figure 3.

ACTION	PAC GLOSSARY
Stronger Actions	• Architectural/physical plant changes • New devices with usability testing before purchasing • Engineering control, interlock, forcing functions • Simplify the process and remove unnecessary steps • Standardize on equipment or process or care maps • Tangible involvement and action by leadership in support of patient safety
Intermediate Actions	• Redundancy/back-up systems • Increase in staffing/decrease in workload • Software enhancements/modifications • Eliminate/reduce distractions • Checklist/cognitive aid • Eliminate look- and sound-alikes • Enhanced documentation/communication
Weaker Actions	• Double checks • Warnings and labels • New procedure/memorandum/policy • Training • Additional study/analysis

Figure 3. VA Action Hierarchy (*Root Cause Analysis Tools*, 2015)

The VA Action Hierarchy was used to code recommendations as either stronger actions, intermediate actions, or weaker actions. There were an average of 3.9 recommendations generated per incident with 35% in the stronger action category, 27.5% in the intermediate action category, and 37.5% in the weaker action category. The majority of recommendations falling in the weaker action category were new procedures and further study of a system component, for example surgical equipment stocking processes.

No other studies of aggregate analysis of accident investigation results in cardiac surgery were available for benchmarking these recommendations. The closest available study analyzed the investigations of patient suicide or attempted suicides in VA healthcare facilities (Mills et al., 2006). This study looked at 137 root cause analyses and found that 78% of the recommendations were policy changes or clinician and patient training, which fall into the weaker action category. Drawing any solid comparison between this study and the CAST analysis results can be misleading because of several key differences. In the VA study, the analyses were completed by clinicians for the express goal of changing clinical practice, while the CAST analyses were completed partially as an academic exercise in system safety. Additionally, suicidal behaviors tend to be issues in emergency departments and inpatient psychiatric floors, a different environment than operating rooms with a different potential set of contextual factors. However, despite these limitations, the comparison suggests that more research into the potential differences in the quality and strength of recommendations generated by CAST versus the VA RCA process would be of interest in future work.

3.4 Summary

Overall, the use of CAST to analyze healthcare incidents showed several potential strengths over the current methodologies used in hospitals. Systems theory more readily captures causal factors such as managerial decisions and organizational flaws than trying to fit those concepts into a linear chain of events model.

An additional benefit of CAST is that the analysis is driven by a common model of the system. The hierarchical control structure depicts the system such that everyone on the team has a common idea of how processes work, how components fit together and interact, and what lies within and outside of the scope of the investigation. Having this clear model and picture facilitates communication and makes assumptions about system design explicit.

Like the newer generations of root cause analysis tools, CAST takes away the focus on blaming the operator and shifts the analyst to considering the impacts of the system design. This movement towards identifying system contributions to accidents is essential for healthcare. In addition, the field needs to move away from blaming individuals and instead consider accidents as occurring due to flaws in the system design, not individual errors.

Finally, CAST has the potential to create more strong recommendations than other techniques. This thesis showed a higher proportion of strong recommendations than a study using the VA RCA technique in a slightly different clinical setting. The theoretical underpinnings of each technique also analytically support this claim. Stronger actions are defined as environmental changes to the system around the human operators and changes to the way that management makes decisions. Because CAST is grounded in systems theory, it forces the analyst to consider such things as the feedback that the human controllers received from the system around them. This consideration leads to recommendations that change the nature of the system, for example to provide feedback that was found to be missing or inadequate. Techniques grounded in linear chain of events models focus on the actions that the operator took and promote recommendations that seek to change those actions, most frequently training or implementing new policies, which are both weaker actions in the VA Action Hierarchy. This theoretical difference helps explain the observed difference in recommendations.

This chapter supports the conclusion that CAST is a useful technique for exploring accidents in healthcare. Because it is grounded in systems theory, more accident causal factors can be identified than when using linear chain of events accident models. From these identified causal factors, strong recommendations for changing the system can be made and implemented, preventing repeated incidents. Finally, because CAST uses one common model of the system it promotes easier and clearer communication amongst the accident investigation team, whether they are clinicians or safety engineers. This clarity of communication makes CAST an easy to adapt tool for healthcare settings.

4 Applying STPA to Healthcare Systems: A Radiation Oncology Case Study

As discussed in chapter 2, system safety can be accomplished both through looking retrospectively at what happened in an accident as well as look prospectively at potential future accidents. Chapter 3 covered research in accident analyses, leaving hazard analysis for this chapter. Despite requiring a prospective risk analysis on a hospital process for accreditation of the hospital (Stewart, 2015), the use of hazard analyses remain limited.

Radiation oncology has embraced the idea of prospective risk analysis more than any other field in medicine. In 2008, the American Association of Physicists in Medicine commissioned a working group to look at the application of FMEA in radiation oncology (Huq et al., 2008). However, FMEA is based in a linear chain of event accident causation model, making it less suitable to applications involving human operators and non-linear interactions (N. G. Leveson, 2011). Theoretically, STPA will identify more hazardous scenarios in a complex sociotechnical system like radiation oncology, but this hypothesis while analytically true, needs to be validated and demonstrated on real medical systems.

The goal of the work presented in this chapter is to demonstrate the application of STPA to human-operator intensive medical workflow in radiation oncology. The process to be analyzed is a proposed compressed workflow process for stereotactic radiosurgery, described in subsection 4.1. The specific goals of this project include identifying hazardous scenarios to guide design changes to reduce the potential for accidents as well as using the analysis to specify design requirements for software supporting the new process.

This chapter begins with a description of the process of delivering stereotactic radiosurgery currently as well as details of the proposed changes. It then shows the STPA analysis, with observations about applying the analysis to this domain as well as example findings. The chapter will next cover several examples of potential system design changes and software requirements generated from the analysis before concluding with a look at future research directions.

4.1 System Description

Stereotactic radiosurgery (SRS) is a multi-hour, or occasionally multi-day, treatment process used to deliver high doses of radiation to brain tumors and other neurological lesions. Traditionally this is considered a high risk procedure because the same dose of radiation is delivered in 1-5 treatment fractions instead of the traditional 40 treatment fractions. The high doses per treatment mean that there is little margin for error. These treatments must be provided with millimeter level accuracy to prevent serious damage to healthy tissue in the patient.

The steps in the treatment process are: 1) patient consultation with a radiation oncologist, 2) acquiring a treatment planning CT scan and MRI for tumor delineation, 3) radiation treatment planning for

delivery, and 4) delivering the treatment to the patient. These steps are conserved between the current process and the proposed process.

The details of each step for the current state of the process are shown below:

1. **Patient consultation with a radiation oncologist** – The physician meets with and examines the patient as well as reviews all available diagnostic information before recommending a radiation treatment strategy. If radiation is recommended for the patient's tumor, then the patient must consent to receive the treatment before proceeding. This process takes 1-3 hours.

2. **Acquiring a treatment planning CT scan and MRI for tumor delineation** – The MRI scan is typically taken prior to the patient seeing the radiation oncologist. This type of imaging is almost always part of the initial cancer work up process. Once the patient has seen the radiation oncologist, they undergo a CT scan of the brain, called the treatment planning CT. The treatment planning CT is a high resolution image taken with the patient secured in treatment planning. The MRI and CT scans will be used jointly to determine the extent of the tumor and treatment areas. Both imaging modalities are necessary for completing a plan. The MRI shows an exquisite level of detail of the structures in the brain that cannot be seen on CT. However, the CT encodes important information regarding radiation dose attenuation that cannot be gleaned from the MRI. Additionally, CT technology has sub millimeter spatial resolution without image warping, both of which can be concerns in MR images. The CT scan can take 1-2 weeks to get scheduled, and the appointment will take approximately one hour.

3. **Radiation treatment planning for delivery** – The medical physicist uses a computer program that utilizes the patient's CT and MRI scans as well as a model of the radiation machine to create a plan which will deliver the desired dose of radiation to the patient's tumor. The first step in developing a treatment plan is to fuse the two images together. This process aligns and reshapes the MRI image to match the CT scan, which was completed in treatment position. The fused images can then be used to understand the tumor location relative to the radiation delivery system, in this case a linear accelerator, when treatment will be delivered. The medical physicist uses a computer program to determine the optimal arrangement of radiation beams to deliver the prescription radiation dose to the tumor while minimizing radiation dose to adjacent normal tissues. Creating the plan is an iterative process as the proposed plan passes between the physicist and radiation oncologist for optimization and approval. The entire cycle typically takes several days before all parties are satisfied with the proposed plan.

4. **Delivering the treatment to the patient** – The patient comes back to the department to receive the radiation dose at the treatment machine about 1-2 weeks after their CT simulation was taken. The therapist, the person who treats the patient, places the patient on the treatment table utilizing the accessories they set up when positioning the patient several weeks prior during the CT Simulation. There are many parameters utilized to ensure accurate positioning. Once the therapist believes that the patient is in place correctly, they use on-board imaging

from the treatment machine, called a cone-beam CT (CBCT). This allows them to adjust their positioning so that the patient is in the exact same position as they were in the treatment planning CT scan. All of the adjustment and positioning takes about 20-30 minutes. Once the therapist is satisfied with the positioning, the radiation oncologist and medical physicist complete a final check and give approval to begin treating. At this point, the process is fully automated by the treatment software, which delivers the treatment based on the treatment plan file. Should anything unexpected happen, the therapist, radiation oncologist, and medical physicist have the power to override the software and abort the treatment. The entire treatment from positioning to completion takes about one hour. A full course of treatment involves between one and five of these treatments, with the patient coming in for one treatment per day.

Beyond the efficacy of SRS, an advantage of SRS is that the treatment can be completed in as little as one treatment day compared to 40 days of treatment in a standard course of radiation therapy. The short duration of treatment makes SRS ideal for patients who need to travel to specialized centers or for whom travel to the hospital is burdensome. However, the requirement of staying for an entire day or traveling multiple-days, for the treatment planning CT scan (CT Simulation) and then later for treatment, can be a major quality of life problem. A better solution for patients would be to come in for consultation and receive the treatment that same day, omitting the need to travel in for the treatment planning CT scan. Researchers at UCSD in the department of radiation oncology are currently exploring the technical feasibility of delivering care in this manner. This thesis chapter represents the safety analysis of this proposed process.

The proposed process would work in the following manner:

1) **Acquiring an MRI scan for tumor delineation** –For brain cancers, MRI images are the ideal way to clearly visualize the extent of the tumor and the healthy structures that might be nearby. If the patient is being considered for radiation therapy, then their physician should acquire these images. The images will be sent to the radiation oncology clinic before the patient has been seen.

2) **Creating a plan on the MRI** – The medical physicist and the radiation oncologist will use the MRI from the patient's chart to create an initial pre-plan in the two weeks prior to the patient arriving for the consultation. Just as in the traditional process, the radiation oncologist will draw contours around the tumor and important structures in the brain. The medical physicist will then use this image to calculate the beam angles to best create the desired dose distribution for the radiation treatment. The biggest difference from the normal process at this point is in calculating the dose because dose attenuation information is encoded in the CT. Several assumptions are made to create a plan with a good estimate of the dose to the tumor.

3) **Patient consultation with a radiation oncologist** – Once the MRI-based plan, the pre-plan, has been created, the physician meets with and examines the patient to recommend a radiation

treatment strategy. Before proceeding, the radiation oncologist must decide if this patient is a good candidate for this compressed work flow treatment process. The patient must be able to remain motionless for about 30-40 minutes, which involves both physical and mental fortitude. The consultation and ensuing discussion will take 1-3 hours.

4) **Delivering the treatment to the patient** – Following the consultation and decision to pursue radiation therapy, the patient would be taken directly to the treatment machine. The process from this point differs from the current process because the patient has not received planning CT scan (CT Simulation). The plan has been completed on an MRI image, which was not taken in treatment position. The lack of imaging in the treatment position has implications for the set up for the treatment, which are outlined in the following steps:

    a. **Positioning** – The therapist places the patient on the treatment couch and secures them with generic binding accessories instead of the patient specific accessories that are commonly used. The patient needs to be in a comfortable position that they will be able to adequately hold for the duration of treatment, typically 30 minutes.

    b. **Imaging** – Once the patient is secured to the treatment couch, the therapist exits the room and acquires a cone-beam CT (CBCT). The CBCT is a low resolution image designed to highlight the bony structures of the patient in their current treatment position. The detail on the soft tissue is low compared to the MRI, but the bony structures show excellent contrast, allowing them to be easily visualized.

    c. **Fusion and Re-Calculation** – The CBCT and the MRI with the plan are fused together utilizing software that is commercially available. However, the existing workflow of the commercial software is not suitable for this new procedure so new software will need to be developed. Following the image fusion, the plan will need to be checked and possibly re-optimized. The image, and therefore the plan, through this process will have been adapted to the patient's actual position. The process of fusing these images may alter the dose distribution in unacceptable ways, prompting a re-optimization of the plan. Additionally, the CBCT gives dose attenuation data, which may show that the approximations were unacceptable and the plan needs to be altered. Calculating the new dose distribution and checking the output could be a quick process or it may require several iterations of optimization, re-calculation, and checking.

5) **Radiation delivery** – Once the team is satisfied that the plan is optimal and the patient has not moved, the therapist will begin the treatment. After the CBCT has been acquired the patient will be monitored closely for movement outside of the tolerances of the linear accelerator; typically about 1mm of movement is the maximum allowed. Monitoring will be through a continuous surface imaging system that is commercially available and currently in use for treatments at the facility. As in the current system, the team has the ability to issue an emergency abort treatment command in the event of any unforeseen incidents occurring.

4.2 Top-Level Accidents, Hazards, and Safety Constraints

System level accidents for stereotactic radiosurgery are listed below. They are adapted from general radiation oncology accidents, as first identified in (Antoine, 2013). Notably, in this analysis worsening physiologic status from cancer spread was not considered as an accident. Most radiation oncology systems must consider cancer spreading as an accident because of the risk of delay in treatment allowing the cancer to metastasize. However, the system under consideration in this project is a novel compressed workflow of traditional SRS treatment. The safe decision at any step in this procedure is to abort this protocol and restart the patient the following day in a traditional SRS process. By eliminating the accident of delayed care leading to cancer metastasis from consideration, the analysis could be done such that aborting the procedure never resulted in a hazard.

The accidents considered in this analysis are as follows:

A-1. Patient injured or killed due to radiation

A-2. Non-patient injured or killed due to radiation

A-3. Damage to equipment

A-4. Death or injury of patient or non-patient not due to radiation

The system level hazards identified are linked to these accidents and are listed below.

H-1. Wrong radiation delivered

- H-1.1. Right patient, right dose, wrong location
- H-1.2. Right patient, wrong dose, right location
- H-1.3. Right patient, wrong dose, wrong location
- H-1.4. Wrong patient

H-2. Staff is unnecessarily exposed to radiation

H-3. Equipment subject to unnecessary stress

H-4. Persons subjected to the possibility of non-radiation injury

These hazards can be directly translated into safety constraints, shown below. These are the top level requirements that the system must use to constrain behavior to safely perform the new SRS procedure. This analysis, therefore, will consider the behavior of the components necessary for the system to meet these requirements. These safety constraints can also be used to evaluate future design trade-offs as managers consider the impacts of changing the system on safety, cost, and other metrics.

SC-1. Radiation must be delivered in the right dose, to the right location, for the right patient

SC-2. Staff must not be exposed to radiation

SC-3. Equipment must not be subjected to unnecessary stress

SC-4. Persons must not be subjected to the possibility of non-radiation injury

4.3 Control Structures

The STPA analysis begins with creating hierarchical control structures to represent the system being studied. The narrative description from the process above was deconstructed into the abstract functions and the controllers responsible for them. The analysis initially began with a high level control structure, which was decomposed into more detailed structures at a lower level of abstraction.

4.3.1 High-Level Control Structure

The analysis begins with a top-level control structure representing the system from the regulatory bodies governing radiation oncology down to the patient receiving the stereotactic radiosurgery treatment procedure, shown in Figure 4.

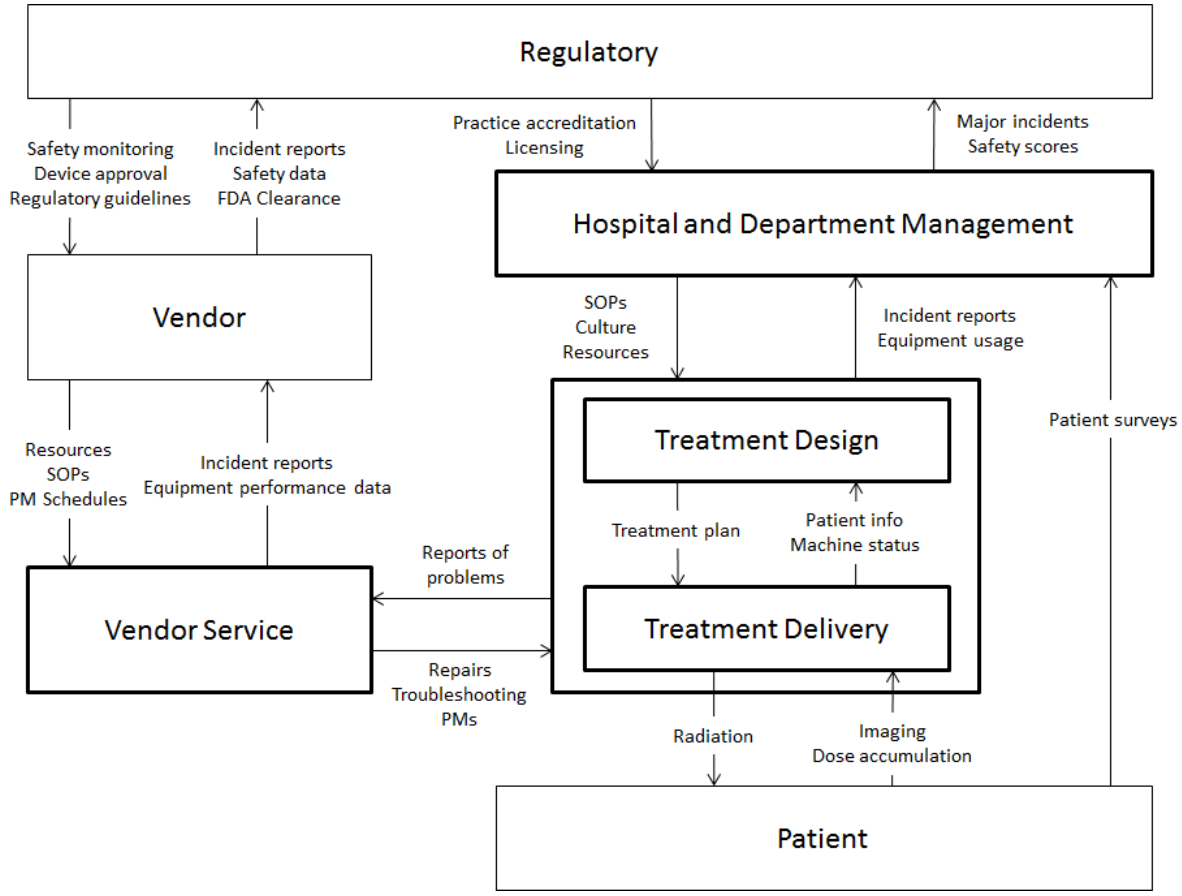

Figure 4. Top Level Control Structure (PM = preventive maintenance, FDA = Food and Drug Administration, SOP = Standard Operating Procedures**)**

The goal of Figure 4 is to show the entire system to better understand where the radiation oncology clinic sits within the larger healthcare system. It is a functional control structure, distinguishing it from an organizational chart, because each controller is described by a particular function as opposed to a job

title or a person fulfilling that particular job. Designing and delivering treatment, for example, are functions fulfilled by the joint operations of several different people in different occupational roles. Following is a description of what each functional controller encompasses:

- **Regulatory:** These are the regulatory bodies that oversee the healthcare or radiation oncology practice. This function encompasses a wide array of bodies including the Nuclear Regulatory Commission, the Food and Drug Administration, the Joint Commission, and others. Their primary responsibility depends on whether they are controlling the hospital's clinical practice or the device design practices. On the device design side, they are responsible for monitoring the safety of the device in use and approving product development practices. On the clinical practice side these organizations are responsible for accreditation as well as disseminating "best practice" guidelines and ensuring adherence to these guidelines.

- **Management:** This controller also encompasses multiple entities. In this diagram, management refers to the entire management structure from the level of the institution's health system, to the hospital, the Cancer Center, and the radiation oncology department. There are many unique positions and roles within this management structure, but they all work towards the same general purpose, by setting the culture of the hospital, setting budgetary and staffing constraints, and setting standard operating procedures. They receive information from patients and staff regarding the quality and processes of care in each individual area of the health system.

- **Treatment Design:** The function of this block is to assess the needs of the patient in terms of radiation requirements and translate those needs into a plan that can be delivered. This includes both the pre-treatment plan and the day of changes to the treatment plan including image fusion, plan optimization, dose calculation, and plan checks. This functional group controls the Treatment Delivery group by providing them with the plan that they will follow in treating the patient. This one block includes medical physicists, radiation oncologists, and radiation therapists utilizing the treatment planning software, image fusion software, and the plan optimization software.

- **Treatment Delivery:** This controller is responsible for delivering the radiation treatment to the patient. The treatment this controller delivers is governed by the plan created by the Treatment Design controller. Inside of this functional unit are radiation therapists, the treatment console software, and the linear accelerator.

- **Vendor:** This functional block encompasses the entirety of the medical device company's operations in designing and managing the design of the linear accelerators used to deliver treatment. While there is a lot to learn by delving into this block in more detail, this is not the primary focus of this analysis and so will be treated as a black box.

- **Vendor Maintenance:** There are some problems with the linear accelerator that can be addressed by the therapists and medical physicists. However, the majority of machine fault

repairs and scheduled maintenance are performed by vendor-based technicians. Their relationship with the radiation oncology department is important for providing these repairs and maintenance in a timely fashion, which is critical to keeping a well-calibrated machine. Additionally, staff members provide feedback on the machines if they malfunction. This feedback helps the vendor understand what safety problems plague their devices and any changes that are needed in the design to promote safety.

The scope of the above control structure, shown in Figure 4, is at too high of a level of abstraction to understand the details of the safety of the new compressed workflow. To better understand the hazards in this particular process, the analysis will focus on the department level, looking from management through to the linear accelerator with a focus on the operators, the software, and their interactions.

4.3.2 Detailed Structure for Treatment Design

To facilitate the analysis, and prevent detail overload, the high level structure was broken down into three more detailed structures, taking a closer look at treatment design, treatment delivery, and management respectively. The first of these detailed control structures is shown in Figure 5, expanding the "Treatment Design" controller from the high level control structure. The context of the controller in the larger system is maintained through consideration of input from other parts of the system and control output from the overall Treatment Design controller to the Treatment Delivery and Patient component below in the hierarchical control structure.

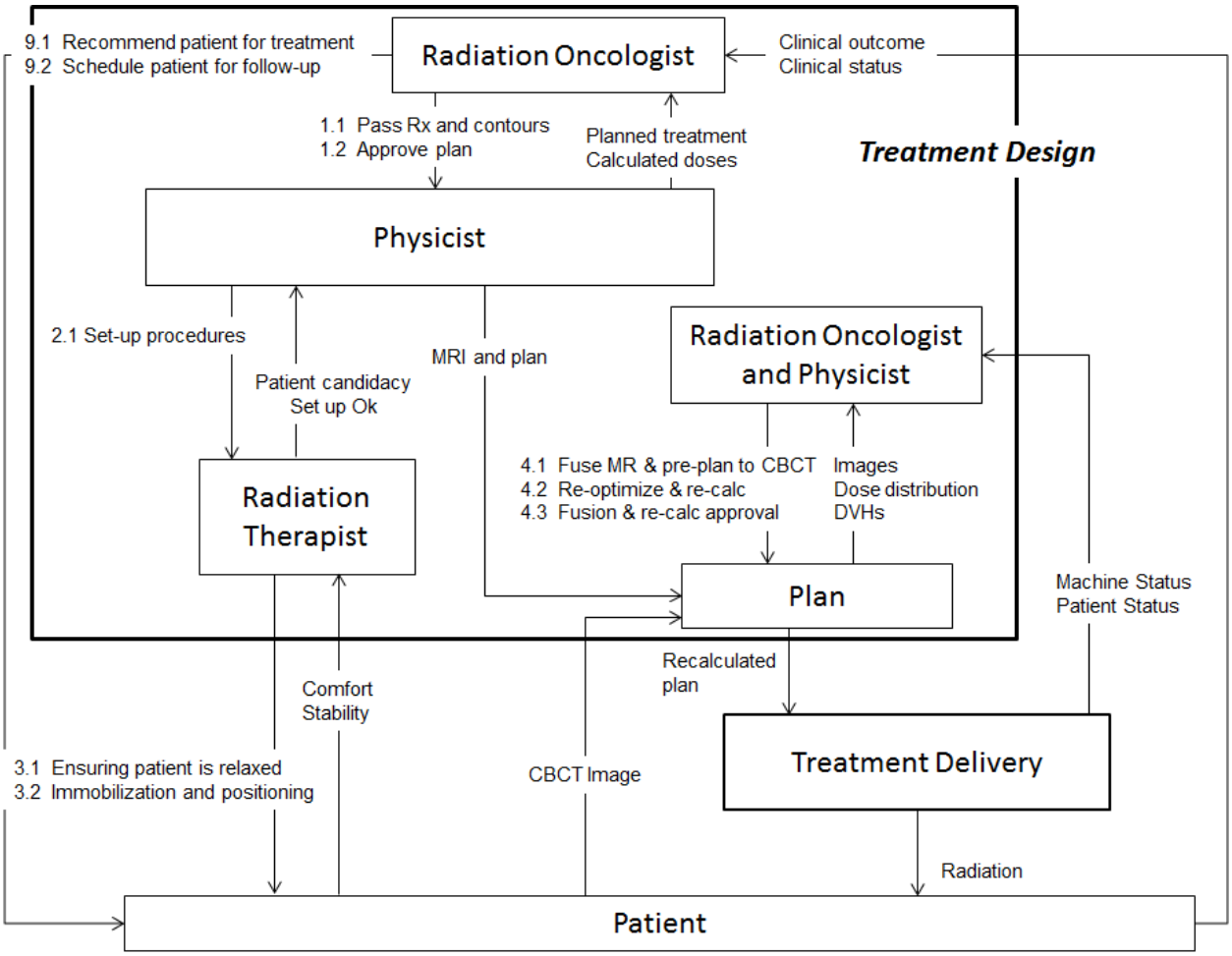

Figure 5. Details of Treatment Design Functional Controller, delimited by the thick black box (Rx = Prescription, MR = MRI image, CBCT = cone beam computed tomography,)

The Treatment Design controller, at a high level, is responsible for creating the plan that will be eventually delivered to the patient. The process being modeled here is the creation of an MRI-based pre-plan for the patient, bringing the patient to the treatment suite, positioning them, and then using the data from positioning to create a new, optimized plan. This optimized plan is then sent to the Treatment Delivery controller so treatment can proceed.

Each control action is numbered as follows; the first digit corresponds to the controller/controlled process pair and the second number corresponds to the control action. The numbered pairs are described below:

1 – These control actions are the radiation oncologist controlling the physicist as they make an initial MRI-based pre-plan for the patient. The radiation oncologist uses the treatment planning software to share MRI images with the tumor contours. The physicist uses this information and the treatment

planning software to create a plan and calculate a dose distribution, which is returned to the radiation oncologist for approval.

2 – This control action is from the physicist controlling the radiation therapist by giving them instructions for positioning the patient. System designers have not decided on how the instructions will be communicated. Potential options include separate verbal instructions for each patient or a standing order for all patients undergoing this procedure.

3 – These control actions are from the radiation therapist to the patient. There are two separate control actions involved at this stage. The first is for the therapist to determine patient adequacy for the treatment. Patient's frequently feel more comfortable discussing their fears or discomfort with the therapist than with the radiation oncologist, making it an important part of the therapist's job to double check that the oncologist was correct in deciding to proceed with this compressed treatment for each patient. The other control action is to physically immobilize the patient in a position that can be comfortably held for 30-40 minutes using generic immobilization devices. Feedback for these control actions mostly comes from what the patient says about their comfort and security in their treatment position.

4 – There are three control actions in this control structure. These actions come from the radiation oncologist and the medical physicist who are now working together as one controller. This "hybrid" controller uses the MRI image, the pre-plan, and the CBCT as input. Their first action is to fuse the images, followed by recalculating the pre-plan for adjustment to the treatment position. Finally, they are responsible for checking that the fusion and plan are adequate. This process may iterate through several revisions of the plan or the fusion before the radiation oncologist and medical physicist are satisfied with the treatment.

There are several metrics available for assisting the clinicians in the plan evaluations. Fusion images are typically evaluated visually, tracing the contours of the bony structures to ensure proper alignment of the two fused images. A variety of metrics are used to evaluate the optimization of the treatment plan including the dose to the tumor, the dose to the adjacent healthy tissues, and visual representations of the dose distribution.

9 – These control actions are from the radiation oncologist to the patient. The first is an early control action involving the initial meeting with the radiation oncologist where the oncologist decides if the patient is an ideal candidate for the new process. This involves understanding their tumor status and biology as well as their personal characteristics, i.e. can they sit still for 45 minutes comfortably or are they too old or too anxious to manage that? To make this decision, they consult the patient's diagnostic studies and medical chart as well as discuss the procedure with the patient. The other control action is seeing the patient in follow up, which provides an important source of feedback about the treatment process. The follow up is the chance for the radiation oncologist to receive information on the tumor's clinical course as well as any side effects suggestive of a misadministration of radiation, potentially suggesting the machine or process. However, radiation injuries take days or months to become clinically

apparent, making the patient status a delayed source of information and decreasing its value as a real-time indicator of system status.

4.3.3 Detailed Structure – Treatment Planning

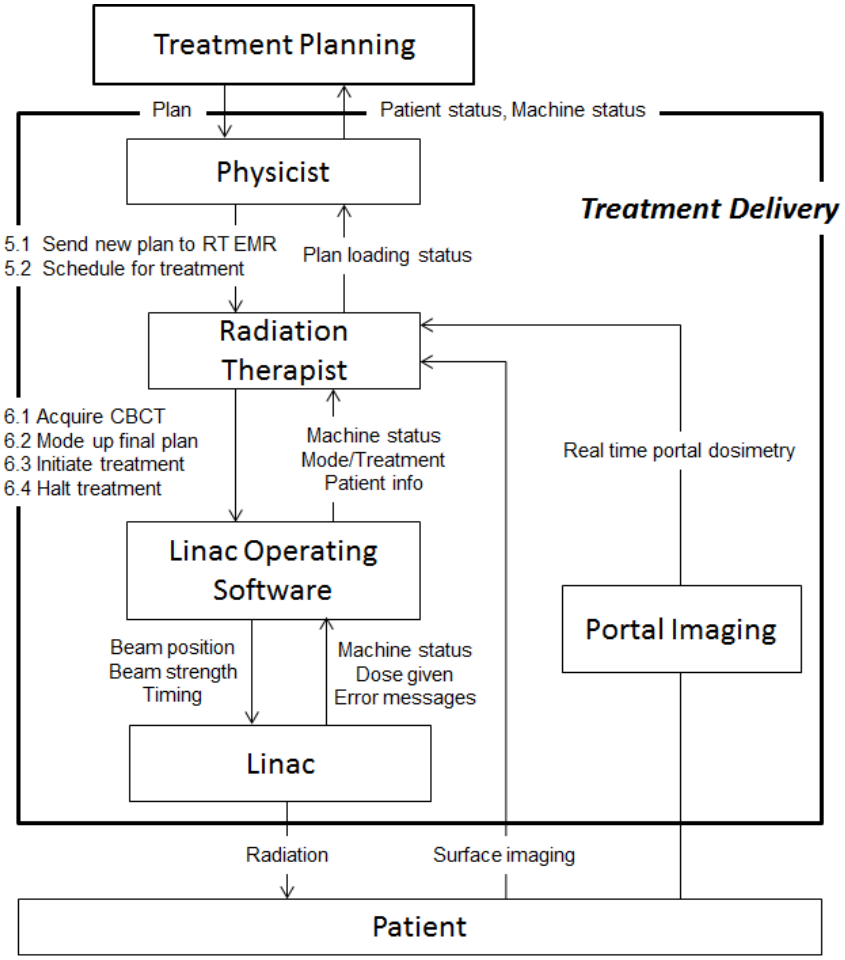

Figure 6. Detailed Controls in Treatment Delivery Controller (Treatment Planning is equivalent to Treatment Design, RT EMR = radiation therapy electronic medical record, linac = linear accelerator)

Figure 6 shows a close up on the Treatment Delivery controller from the high level control structure. Treatment Delivery controls the patient by providing radiation per the constraints from the Treatment Design controller. This analysis will look in detail at the actions of the medical physicist and the radiation therapist, considering the linear accelerator or its controlling software only as the therapist interacts with it. For analysis of the medical device itself, see (Antoine, 2013).

Control actions labeled as 5.1 and 5.2 in Figure 3 in this diagram are the medical physicist controlling the radiation therapist by transferring the plan files from the treatment planning software to the treatment console software and scheduling the patient. These are two actions that are necessary for the radiation

therapist to actually deliver the treatment. They are also two areas where there is a high risk of sending the wrong plan, scheduling the wrong treatment, or accidentally corrupting the file.

Control actions labeled with a 6 are the actions of the radiation therapist on the linear accelerator's operating software. These include acquiring the CBCT, which is used as an input to the treatment planning controller and "moding up" the final treatment plan, as well as initiating treatment. "Moding up" the plan refers to using the software to translate the treatment plan into a set of instruction for the linear accelerator.

4.3.4 Detailed Structure - Management

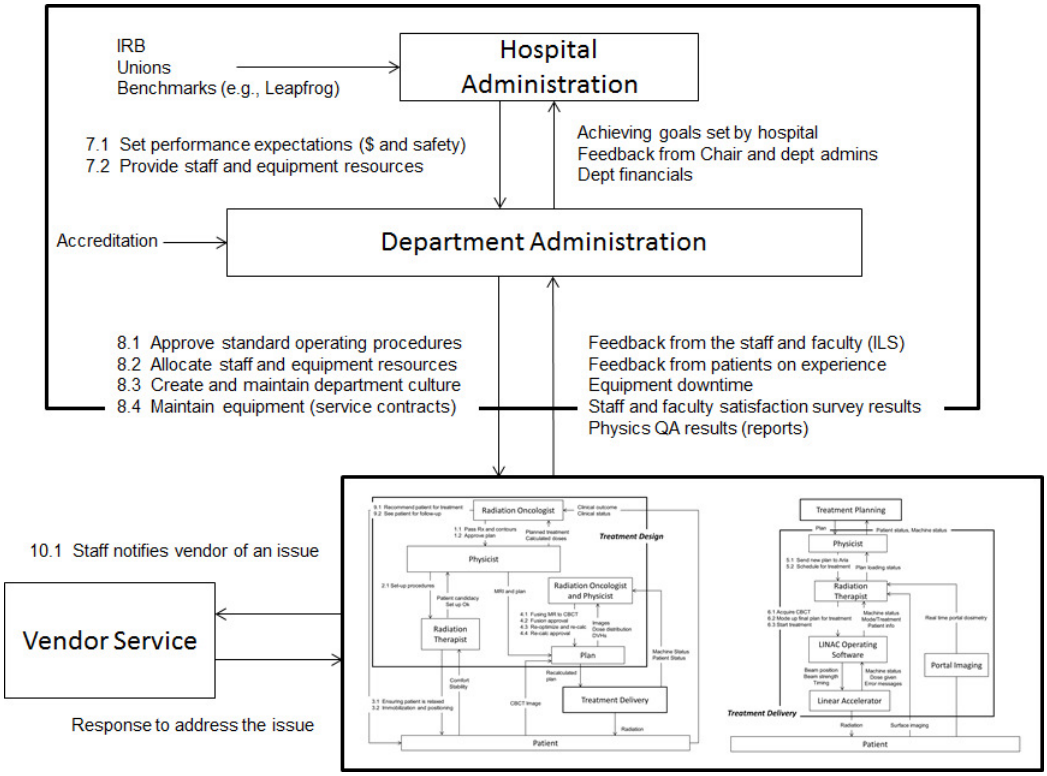

Figure 7. Detailed Control Structures of Management and Vendor Service Relations

The final structure, shown in Figure 7, offers a detailed look at the management controller of the high-level control structure. Management was divided into hospital administration and department administration because each has its own responsibilities, background knowledge, and experience. Frequently, these two management controllers will interact in to create conflicting responsibilities or set unrealistic expectations for budgeting or output, for example. Control actions labeled as 7.1 and 7.2 come from the hospital administration down onto the department administration. Everything labeled as 8.1-8.4 goes from the department administration down to the various components of the department. Management impacts every piece of the system underneath it through its control actions. Likewise, the department administration receives input from all levels of the system below, as shown in the wide range of inputs received.

4.3.5 Summary of Control Structures

The control structures themselves can yield important insight and understanding into the system before even beginning the analysis. The abstract, high-level control structure shown in Figure 4 is a generic model for almost all healthcare systems. Regulatory bodies oversee management. Management sets policies and goals for the clinical care areas. Within the clinical care areas personnel decide, design, and order treatment for the patient to undergo. Then clinical personnel carry out this planned treatment in fulfilling the treatment delivery function. The exact treatment can vary; medications, radiation, surgery, or any other clinical intervention are all interchangeable at this level of abstraction. Parallel to this, just as we can see in the general control structure template (N. G. Leveson, 2011), there is a vertical structure involving the design of the medical devices, medications, or healthcare processes required to care for the patient.

The more detailed structures at the lower level of abstraction begin to differentiate a radiation oncology process from a surgical or psychiatric process. As details get filled in, the analyst can already begin to see if the detailed controllers are fulfilling the requirements described in the more abstract model. Gaps, such as missing feedback, that impact safety can be identified at this level even before analysis begins.

4.4 Identification of Unsafe Control Actions

After completing the control structure, the next step in analysis is to identify unsafe control actions. This was completed using traditional Step 1 tables. These tables ask four questions of each control action, outlined in (N. G. Leveson, 2011):

1) Is there a context where it is hazardous to not provide the control action?
2) Is there a context where it is hazardous to provide the control action?
3) Is it hazardous to perform the control action too early, too late, or with the wrong timing?
4) Is it hazardous to apply the control action for too long a duration or stop providing the control action too early?

Each question should prompt the analyst to decide whether there is any context under which the control action is unsafe given the prompts in the question. For this system, 23 control actions were analyzed, yielding 84 unsafe control actions. Table 6 shows the Step 1 table for the control actions of the medical physicist and radiation oncologist as they create an image fusion, recalculate and optimize the plan, and approve the new plan. The three control actions expand into 16 potential unsafe control actions. The unsafe control actions (UCA) are all written in the form of the context under which the control action could be unsafe. The UCAs have been numbered such that they can be tied back to their associated control actions as well as traced to the hazards they may cause. This numbering and tagging scheme promotes traceability in the analysis and any resultant system design changes.

Control Action	Not providing causes	Providing leads to	Wrong timing leads to	Applied too long or too short leads to

	hazard	hazard	hazard	hazard
4.1 Fuse MR and pre-plan to CBCT	4.1.1: The physicist does not perform the fusion when the images and pre-plan are ready. [H1]	4.1.2: The physicist fuses the images and pre-plan incorrectly when using the fusion software. [H1]	4.1.3: The images are fused before the final or most recent CBCT is acquired and transferred for fusion. [H1]	4.1.4: The fusion takes too long when transferring images or using the fusion software. [H1]
4.2 Re-optimize and re-calculate	4.2.1: Suboptimal treatment occurs when a suboptimal pre-plan is scheduled for treatment. [H1]	4.2.2: An inaccurate dose calculation is provided when the physicist uses the software to perform the re-calc. [H1]	4.2.3: Re-optimize and re-calculate before fusion is complete [H1.1-3]	4.2.4: Re-optimization or re-calculation takes too long when using the treatment planning software. [H1] 4.2.5: Re-optimization ends before completed after the physicist initiates the optimization. [H1]
4.3 Fusion and final plan approval	4.3.1: The fusion is not checked by the radiation oncologist when it is suboptimal. [H1] 4.3.2: The final plan is not checked by the radiation oncologist when it is suboptimal. [H1.1-3]	4.3.3: The radiation oncologist approves the fusion when it is suboptimal. [H1] 4.3.4: The radiation oncologist approves the final plan when it is suboptimal. [H1.1-3]	4.3.5: The fusion is approved after the plan has been scheduled for treatment. [H1] 4.3. 6: The radiation oncologists approves a plan before the final plan is completed. [H1]	4.3.7: The fusion and final plan approval are delayed when they are ready to be checked. [H1]

Table 6. Step 1 Table to identify UCAs for the radiation oncologist-medical physicist controller

The remainder of the Step 1 tables for this analysis can be found in Appendix A.

4.5 Identification of Causal Factors and Scenarios

Step 2 involves identifying how the unsafe control actions found in Step 1 might occur in the actual system.. Unlike Step 1, there is nothing formulaic about scenario generation. It requires insight into how the system operates, as does any hazard analysis done by any existing hazard analysis technique. Typically, Step 2 is best completed by having a safety engineer work with a domain expert to understand how the system may move towards the identified unsafe control actions and violation of safety constraints, as this is how the process is done for FMEA, fault trees, HAZOP, etc.

At a high level, scenarios provide the answer to two questions. First, why would the controller issue an unsafe control action? Second, even if the controller issued a necessary control action to prevent an accident, why might that control action not be executed?

Here is one example of a Step 2 scenario generated by STPA.

Control Action: Physicist performs the fusion of the MRI and CBCT images

UCA 4.1.1: The physicist does not perform the fusion when the images and pre-plan are ready. [H1]

Scenario 1: The physicist is unaware that the clinical team is now ready for him/her to perform the fusion. This could be because the CBCT was not loaded into the computer, which is what the physicist uses as his/her signal to proceed with the fusion. Even if he/she knew that the fusion needed to be completed, he/she could not proceed without this image. Another possibility is that the physicist is away working on another patient and does not receive a page or phone call telling them that the fusion needs to be completed.

Scenario 2: The physicist may decide to not proceed with the fusion on the false belief that the patient has moved too much from the original treatment position. This could be because of a false alarm from the surface image monitoring, which may have been miscalibrated to the patient. Alternatively, this false belief of movement could be a result of the poor quality video feed from the room giving the impression that the patient had moved when the reality is that the patient remains within safe treatment parameters.

Scenario 3: The physicist may know that he needs to work on the fusion, but he is otherwise occupied with another patient. He selects to stay with the other patient, even if in reality he should have stopped that action and come over to complete the fusion. This could be further caused by managerial decisions to cut back on staffing, such that the staffing levels are inadequate to support all of the patient treatments.

Scenario 4: The physicist may believe that somebody else already completed the fusion. The physicist may not be specifically assigned to cases, so there is confusion over which physicist is responsible. Then if there is no feedback from the software regarding this status of the fusion (whether it has been completed), then the physicist may incorrectly believe that someone else completed the fusion for the patient whose case he started.

After considering accident scenarios contributing to an unsafe control action, the next step is to consider how a safe control action might be given but not successfully executed. For the control action of fusing the MRI and CBCT the analysis yields the following scenarios:

Scenario 5: The physicist tries to perform the fusion but the software crashes and cannot be recovered. Alternatively, the physicist may not be able to access the software because of licensing issues. Frequently, the hospitals acquire a limited number of licenses and other physicists may be using all of the software copies on other patients making it impossible for the physicist to perform the fusion for this patient.

Scenario 6: The physicist knows that he must complete this fusion, and he has access to the software to complete the fusion. However, he may not know how to use the software. He may lack this knowledge

because he is a new physicist, new to this clinical workflow, or inadequate training was offered at the start up of this new process.

4.6 Requirements Generation

The two goals for this project at the outset were to generate requirements for the fusion and recalculation software and to provide a description of safety requirements for the clinicians involved in operating this new process to assist as it begins to be used day to day. These requirements can then be translated into systemic design changes to promote safety.

STPA has been used to generate requirements for software that can be verified and validated. This is commonly done by re-writing unsafe control actions in a format such that they can be used as requirements. In this case, however, we were not interested in these detailed specifications. Rather we wanted to understand the requirements of the software as it applied to interacting with the remainder of the clinical system surrounding the patient. These would be general guidelines that could be passed to the designer in addition to more detailed requirements. At the level of abstraction in the system the software of interest was not modeled as a controller, but rather as a sensor and actuator assisting other controllers in carrying out their jobs. Therefore, we needed to take a different approach to generating requirements because the software was never involved in Step 1 of the analysis.

To overcome this, we used the Step 2 causal scenarios generated from the unsafe control actions of the controllers using the software as an actuator and sensor. The software of interest, the fusion and recalculation software, is used by the medical physicist and radiation oncologist combined controller to control the radiation plan. Specifically, we need to identify causal scenarios relating to the use of the software. Once these scenarios are identified they can be translated into requirements.

Going back to our previous example, the causal scenarios pertaining to the software include the following:

- The physicist believes that the fusion has already done. There could have been confusion over who is responsible for completing the image fusion or the computer program makes it appear that the fusion was already completed.
- The physicist tries to run the fusion software, but the software crashes. However, the physicist may not realize that the fusion was never completed because there is no error message so he or she does not try to run the fusion again.
- The physicist does not know how to use the fusion software, possibly because they are new to this process and the training was inadequate.

These scenarios can be translated into requirements by pulling out the behavior required of the actuator or sensor. Doing this we can derive the following requirements from the limited Step 2 example above:

R-1 Software must output an error message that is perceivable by the user if the fusion algorithm cannot be completed given the inputs (4.1.1)

R-2 Software must contain an obvious signal that the fusion has been completed or has yet to be completed (4.1.1)

These requirements are not complete; they are just an example from one set of causal scenarios. The way these requirements are written cannot be verified and validated. However, as written, they can serve as a bridge between the clinical workflow designers and the software engineers. These are the requirements for the software to function safely given the details of this clinical workflow. Implementing these requirements will serve to prevent those scenarios identified in the analysis above from leading to their respective unsafe control actions.

A similar exercise can be done with the human controllers in the system to help communicate their job requirements and to design the process, policies, and procedures to be used. While it is useful to explain to people their role in safely operating a system, it would be naïve to expect that telling people to do the right thing will always ensure safety. People make mistakes even when they are trying to do things correctly. Changing the system to prevent this reliance on human perfection will have a far stronger impact. This idea leads to the last goal of this project, designing system changes to promote safety when the new SRS process begins.

These system design changes are drawn from the Step 2 causal scenarios generated from considering the entire control loop involving a human controller. For example, consider the UCA 4.3.3: The radiation oncologist approves the fusion and plan when it is suboptimal. Under the current process the radiation oncologist has nearly unlimited time to evaluate the plan and decide if it meets their specifications. However, under this new process the radiation oncologist will be under intense time pressure to make this decision. They will not have the luxury of time to evaluate the plan by hand, making it more likely that they will approve a suboptimal plan. One possible solution to prevent this decision is to provide stronger metrics of the quality of the plan and fusion. These metrics are not currently used in the SRS process, but several different metrics have been explored in experiments. The system designer can use this hazard analysis to consider several potential options for providing this augmented feedback.

4.7 Summary

Overall STPA provides clear guidance and a strong theoretical model for identifying hazards and design requirements as well as potential accident scenarios for a radiation oncology workflow. Chain of event accident models provide the analyst with the insight that humans can make a mistake but offer no guidance to think beyond that to the broader system to understanding why they made the incorrect decision. STPA analyzes the system as a whole, creating a clear framework for understanding the role of the system in a human operator's decisions. This perspective allows the analyst to create strong design recommendations that change the human's behavior through changing the system. Theoretically, these changes will make the system safer.

An additional benefit of STPA in analyzing clinical workflows is in the ability to clearly trace these design changes to the hazards they were intended to prevent. Adding intention to the design changes helps ensure that in the future when components are replaced or redesigned important safety measures are not lost. Having a safety analysis that is a “living document” will help with design changes, implementation of new technologies, and maintaining safety through changes in management.

Overall, the proof of concept case study presented in this chapter should serve to encourage further exploration of STPA applications in healthcare systems.

5 Conclusions

This thesis presented a proof of concept application of CAST and STPA to healthcare problems. CAST, when applied to cardiac surgery, identified causal factors not previously identified by the clinical team. Additionally, CAST helped generate a higher proportion of "stronger" recommendations for design changes compared to traditional accident analysis techniques when applied to different areas of healthcare. CAST was easy to use with a research team because it provided a shared model of the system for discussion between safety experts and clinical experts. Pulling the focus away from blaming the healthcare providers and instead focusing on how the system contributed to the accident promoted openness and a lack of defensiveness in the discussion, which also contributed to the strong investigation results.

The STPA analysis showed equally positive and promising results in analyzing the radiation oncology process. From a theoretical standpoint, STPA will identify more potential accident scenarios than techniques grounded in linear chain of event models. STPA is based in STAMP, which is a more complete model than component failure-only models. While the work in this thesis did not show a head to head comparison, there have been comparisons done in other fields to a variety of techniques including in aviation (N. Leveson, Wilkinson, Fleming, Thomas, & Tracy, 2014) and nuclear energy (Torok & Geddes, 2013), finding that STPA identified more causal scenarios. A strength cited by both studies was the ability of STPA to handle humans beyond merely assigning a risk of human error or human "failure." STPA was easily applied to healthcare processes and should have the same benefits based on the theoretical underpinnings.

Based on this work and the growing body of literature around STPA in other industries future work in healthcare should be directed to three potential research paths. The first research path is in understanding the barriers to implementation of hazard analyses in healthcare. FMEA has been around for decades and is required for hospital accreditation, yet still hospitals do not apply FMEA frequently outside of experimental projects. STPA is a new technique, and therefore has even less penetration into the healthcare domain. What would it take to make health systems adapt STPA and hazard analyses in general?

The second potential research direction would be to understand the role of hazard analyses and accident analyses in patient safety. There exists in healthcare this "undercurrent of sentiment that this approach [accident investigation] has limited effectiveness" (Wu et al., 2008), which undermines accident and hazard analyses. Leaders in patient safety have called for investigations into the efficacy of accident analyses (Wu et al., 2008). However, any study trying to correlate accident and hazard analyses with patient safety at this point in time would be heavily biased to the negative result because of ineffective implementation of weaker analytic techniques. If a health system could implement STAMP based analyses, though, the negative bias due to weak analytic techniques disappears. Data showing efficacy, in terms of lives saved or decreases in accident rates, in a real-world setting, would provide patient safety leaders with the ammunition needed to challenge hospital leadership to dedicate the resources to performing these analyses.

The third potential research approach would be in the exploration of a "template" for the healthcare control structure. This template could be utilized for both CAST and STPA, decreasing the time needed to complete the analyses. A template for the control structure was briefly discussed in Chapter 4. To recap, it would start at the top with a regulatory function, which controls management at the health system level. The management then controls the "clinic," which is comprised of two functional groups, treatment design and treatment delivery. If this control structure could describe almost any system in healthcare, then it would be a powerful tool for several possible applications. From an implementation perspective it makes the process of creating a control structure much easier for clinicians with no background in control theory or systems theory. Additionally, it opens the door to creating more automation. An automated analysis tool would save time for busy clinicians and potentially allow them to get more safety analysis work done around their other clinical duties. Finally, it could assist with regulation of patient safety and hospital licensure by providing a framework for hazard analyses to follow and licensure decisions to be based on. The idea of a template for regulatory required analysis that is based in systems theory is especially exciting for the up and coming fields of medical device interoperability and healthcare IT. These add a high degree of complexity to already complex systems, and a technique based in reliability theory is simply not adequate to understand the potentially dangerous interactions. However, a systems theory based technique could identify these interactions and predict those risks, making it an appropriate choice for future regulation.

In the end, the goal of healthcare is to heal patients, not to harm them. This thesis showed that STAMP can easily be applied to healthcare processes, and a growing body of literature has shown the benefits of STAMP over existing chain of event accident models. While there is always more research that can be done into STAMP and other hazard and accident modeling techniques, if patients are ever going to be safer, the industry needs to move forward with implementation. Keeping STAMP, and more generally accident and hazard analysis, in the realm of experimentation and research is antithetical to the engineering spirit and the findings of this thesis.

References

Antoine, B. (2013). *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: An example from the medical device industry*. Massachusetts Institute of Technology.

Arnold, R. (2009). *A qualitative comparitive analysis of SOAM and STAMP in ATM occurrence investigation*. Lund University.

Balgos, V. (2012). Safety Analysis of a Diagnostic Medical Device. In *First STAMP/STPA Workshop*.

Carroll, J. S. (1995). Incident reviews in high-hazard industries: Sensemaking and learning under ambiguity and accountability. *Industrial and Environmental Crisis Quarterly*, *9*, 175–197.

Carroll, J. S. (1998). Organizational Learning Activities in High-Hazard Industries: The Logics Underlying Self-Analysis. *Journal of Management Studies*, *35*, 699–717.

Daartz, J., & Kang, J. (2015). STPA in radiation oncology. In *4th Annual STAMP Workshop*.

Dekker, S. W. a, & Leveson, N. G. (2014). The systems approach to medicine: controversy and misconceptions. *BMJ Quality & Safety*, (August), 1–3. doi:10.1136/bmjqs-2014-003106

Dong, A. (2012). *Application of CAST and STPA to railroad safety in china*. Massachusetts Institute of Technology.

Ford, E. C., Gaudette, R., Myers, L., Verderver, B., Engineer, L., Zellars, R., … DeWeese, T. L. (2009). Evaluation of safety in a radiation oncology setting using failure mode and effects analysis. *Internation Journal for Radiation Oncology and Biologic Physics*, *74*(3), 852–858. doi:10.1016/j.ijrobp.2008.10.038.EVALUATION

Haynes, A. B., Weiser, T. G., Berry, W. R., Lipsitz, S. R., Breizat, A.-H. S., Dellinger, E. P., … Gawande, A. A. (2009). A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population. *New England Journal of Medicine*, *360*(5), 491–499.

Heinrich, H. W. (1931). *Industrial accident prevention: A scientific approach* (1st ed.). New York: McGraw-Hill.

Hickey, J. (2012). *A system theoretic safety analysis of U.S. Coast Guard aviation mishap involving CG-6505*. Massachusetts Institute of Technology.

Huq, M. S., Fraass, B. a, Dunscombe, P. B., Gibbons, J. P., Ibbott, G. S., Medin, P. M., … Yorke, E. D. (2008). A method for evaluating quality assurance needs in radiation therapy. *International Journal of Radiation Oncology, Biology, Physics*, *71*(1 Suppl), S170–3. doi:10.1016/j.ijrobp.2007.06.081

James, J. T. (2013). A new, evidence-based estimate of patient harms associated with hospital care. *Journal of Patient Safety*, *9*(3), 122–8.

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (1999). *To Err is Human* (p. 287). Washington, DC.

Leveson, N. G. (1995). *Safeware: System safety and computers* (p. 680). Boston: Addison-Wesley Publishing Company, Inc.

Leveson, N. G. (2011). *Engineering a Safer World* (p. 534). Cambridge, MA: MIT Press.

Leveson, N. G. (2015). A Systems Thinking Approach to Risk Management Through Leading Safety Indicators. *Reliability Engineering and System Safety*, 17–34.

Leveson, N., Wilkinson, C., Fleming, C., Thomas, J., & Tracy, I. (2014). *A comparison of STPA and the ARP 4761 safety assement process* (p. 72).

Marx, D. A., & Slonim, A. D. (2003). Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. *Quality and Safety in Health Care*, *12*, 33–38.

Mills, P., Neily, J., Luan, D., Osborne, A., & Howard, K. (2006). Actions and implementation strategies to reduce suicidal events in the Veterans Health Administration. *Joint Commission Journal of Quality Improvement*, *32*(3), 130–141.

Mills, P., Neily, J., Luan, D., Stalhandske, E., & Weeks, W. B. (2005). Using aggregate root cause analysis to reduce falls. *Joint Commission Journal of Quality Improvement*, *31*(1), 21–31.

Nelson, P. S. (2008). *A STAMP Analysis of the LEX Comair 5191 Accident*. Lund University.

O'Neil, M. (2014). *Application of CAST to Hospital Adverse Events*. Massachusetts Institute of Technology.

Percarpio, K., & Watts, B. (2013). A cross-sectional study on the relationship between utilization of root cause analysis and patient safety at 139 Department of Veterans Affairs medical centers. *Joint Commission Journal of Quality Improvement*, *39*(1), 32–7.

Proctor, S., Hatcliff, J., Fernando, A., & Weininger, S. (2015). Using STPA to support risk management for interoperable medical systems. In *4th Annual STAMP Workshop*.

Reason, J. (1995). Understanding adverse events: human factors. *Quality and Safety in Health Care*, *4*(2), 80–89. doi:10.1136/qshc.4.2.80

Reason, J. (2000). Human error: models and management. *British Medical Journal*, *320*(March), 4–6.

Root Cause Analysis Tools. (2015) (p. 30).

Safety Assessment Code Matrix. (2014). Retrieved April 20, 2015, from http://www.patientsafety.va.gov/professionals/publications/matrix.asp

Shealy, J. E. (1979). Impact of theory of accident causation on intervention strategies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 225–229.

Stewart, K. J. (2015). Joint Commission Standards Applicable to the Provision of Respiratory Care Services In Hospitals. Retrieved April 21, 2015, from https://www.aarc.org/aarc-membership/community/specialty-sections/management/joint-commission-standards/

Thomas, J. (2013). *Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis*. Massachusetts Institute of Technology.

Torok, R., & Geddes, B. (2013). Systems theoretic process analysis (STPA) applied to a nuclear power plant. In *Second STAMP/STPA Workshop*.

Turner, B. (1978). *Man-Made Disasters* (p. 254). Wykeham.

Turner, B., & Pidgeon, N. (1997). *Man-Made Disasters* (2nd ed., p. 250). Butterworth-Heinemann.

Van Tilburg, C. M., Leistikow, I. P., Rademaker, C. M. a, Bierings, M. B., & van Dijk, a T. H. (2006). Health Care Failure Mode and Effect Analysis: a useful proactive risk analysis in a pediatric oncology ward. *Quality & Safety in Health Care*, *15*(1), 58–63. doi:10.1136/qshc.2005.014902

Veterans Health Administration. (2015). Retrieved April 20, 2015, from http://www.va.gov/health/

Wetterneck, T. B., Skibinski, K. a, Roberts, T. L., Kleppin, S. M., Schroeder, M. E., Enloe, M., … Carayon, P. (2006). Using failure mode and effects analysis to plan implementation of smart i.v. pump technology. *American Journal of Health-System Pharmacy : AJHP : Official Journal of the American Society of Health-System Pharmacists*, *63*(16), 1528–38. doi:10.2146/ajhp050515

Wreathall, J., & Nemeth, C. (2004). Assessing risk: the role of probabilistic risk assessment (PRA) in patient safety improvement. *Quality and Safety in Health Care*, *13*(3), 206–212. doi:10.1136/qshc.2003.006056

Wu, A. W., Lipshutz, A. K. M., & Pronovost, P. J. (2008). Effectiveness and efficiency of root cause analysis in medicine. *JAMA : The Journal of the American Medical Association*, *299*(6), 685–7. doi:10.1001/jama.299.6.685

Appendix A – Stereotactic Radiosurgery STPA

Step 1 Tables

Control Action	Not providing leads to hazard	Providing leads to hazard	Wrong timing leads to hazard	Applied too long or too short leads to hazard
1.1 Pass Rx and contours	N/A	1.1.1: The radiation oncologist approves the prescription and contours when one or both are suboptimal. [H1.1-3] 1.1.2: The radiation oncologist approves the prescription and contours when it was intended for another patient. [H1.4]	1.1.3: The physicist creates the pre-plan before the final prescription and contours are passed along. [H1.1-3]	N/A
1.2 Approve plan	1.2.1: The patient gets treated even though the radiation oncologist did not approve the pre-plan. [H1]	1.2.2: The radiation oncologist approves the pre-plan when the pre-plan is suboptimal. [H1.1-3] 1.2.3: The radiation oncologist approves an optimal pre-plan when it was intended for a different patient. [H1.4]	1.2.4: The radiation oncologist approves the pre-plan before pre-plan is complete. [H1] 1.2.5: The radiation oncologist is delayed in approving the pre-plan when the pre-plan is ready for review. [H1]	N/A

Table 7. Radiation Oncologist Controlling Medical Physicist

Control Action	Not providing causes hazard	Providing leads to hazard	Wrong timing leads to hazard	Applied too long or too short leads to hazard
2.1 Set-up procedures	2.1.1: The SOPs are not communicated to the new radiation therapist when the radiation therapist changes linear accelerator coverage. [H1, H2, H4]	2.1.2: The SOPs are incorrect or incorrectly communicated when the procedure is introduced into clinical use. [H1, H2, H4] 2.1.3: The SOPs do not get updated and/or communicated when there is a planned process modification. [H1, H2, H4]	2.1.4: The same-day SRS program is started before the SOPs are completed. [H1, H2, H4]	2.1. 5: The SOPs are finalized before getting input from all team members (radiation oncologists, physicists, therapists, schedulers). [H1, H2, H4]

Table 8. Medical Physicist Controlling Radiation Therapist

Control Action	Not Providing Causes Hazard	Providing Leads to Hazard	Wrong Timing Leads to Hazard	Too Long or Too Short Leads to Hazard
3.1 Ensuring patient is relaxed	3.1.1: Therapist does not ensure candidacy of patient when patient is actually non-ideal for this treatment. [H1.1, H2]	3.1.2: A junior or otherwise inexperienced therapist incorrectly identifies the patient status when meeting the patient. [H1.1, H2]	3.1.3: Therapist assesses patient's comfort with treatment (i.e., ability to hold still) after patient is already on table and immobilized making stopping less likely if the patient is not ideal. [H1.1, H2]	
3.2 Immobilization and positioning	3.2.13: The therapist does not *securely* immobilize the patient [H1]	3.2.2: The therapist does not position the patient per the SOP when setting up the patient for treatment. [H1.1, H2]		3.2.3: The radiation therapist takes a long time to position the patient when setting up the patient for treatment. [H1.1 H2]

Table 9. Radiation Therapist Controlling the Patient

Control Action	Not providing causes hazard	Providing leads to hazard	Wrong timing leads to hazard	Applied too long or too short leads to hazard
4.1 Fuse MR and pre-plan to CBCT	4.1.1: The physicist does not perform the fusion when the images and pre-plan are ready. [H1]	4.1.2: The physicist fuses the images and pre-plan incorrectly when using the fusion software. [H1]	4.1.3: The images are fused before the final or most recent CBCT is acquired and transferred for fusion. [H1]	4.1.4: The fusion takes too long when transferring images or using the fusion software. [H1]
4.2 Re-optimize and re-calculate	4.2.1: Suboptimal treatment occurs when a suboptimal pre-plan is scheduled for treatment. [H1]	4.2.2: An inaccurate dose calculation is provided when the physicist uses the software to perform the re-calc. [H1]	4.2.3: Re-optimize and re-calculate before fusion is complete [H1.1-3]	4.2.4: Re-optimization or re-calculation takes too long when using the treatment planning software. [H1] 4.2.5: Re-optimization ends before completed after the physicist initiates the optimization. [H1]
4.3 Fusion and final plan approval	4.3.1: The fusion is not checked by the radiation oncologist when it is suboptimal. [H1] 4.3.2: The final plan is not checked by the radiation oncologist when it is suboptimal. [H1.1-3]	4.3.3: The radiation oncologist approves the fusion when it is suboptimal. [H1] 4.3.4: The radiation oncologist approves the final plan when it is suboptimal. [H1.1-3]	4.3.5: The fusion is approved after the plan has been scheduled for treatment. [H1] 4.3. 6: The radiation oncologists approves a plan before the final plan is completed. [H1]	4.3.7: The fusion and final plan approval are delayed when they are ready to be checked. [H1]

Table 10. Medical Physicist and Radiation Oncologist Controlling the Treatment Plan

Control Action	Not Providing Causes Hazard	Providing Leads to Hazard	Wrong Timing Leads to Hazard	Too Long or Too Short Leads to Hazard
5.1 Send new plan to RT EMR	N/A	5.1.1: The wrong final plan wrong patient's final plan is sent to the linac with the final plan has been approved by the radiation oncologist. [H1]	5.1.2: The final plan is not available at the linac when the patient is positioned correctly and ready for treatment. [H1]	N/A
5.2 Schedule for treatment	5.2.1: The physicist does not schedule the final plan for treatment when it is approved. [H1]	5.2.2: The physicist schedules the plan for treatment with an incorrect number of fractions when using the scheduling software. [H1]	5.2.3: The physicist takes too long to schedule the plan for treatment after it has been approved by the radiation oncologist. [H1]	N/A

Table 11. Medical Physicist Controlling the Radiation Therapist

Control Action	Not providing causes hazard	Providing leads to hazard	Wrong timing leads to hazard	Applied too long or too short leads to hazard
6.1 Acquire CBCT	6.1.1: The radiation therapist does not acquire the CBCT when the patient is positioned on the treatment table. [H1.1-3]	6.1.2: The radiation therapist acquires the CBCT when the patient is not in the correct position. [H1.1-3] 6.1.3: The radiation therapist acquires the CBCT with the wrong scan parameters. [H1]	6.1.4: The radiation therapist aquires the CBCT too quickly when the patient isn't relaxed. [H1.1-3]UCA 5: The radiation therapist acquires the CBCT after the patient has been lying on the table for a long time. [H1.1-3]	N/A
6.2 Mode up final plan for treatment	6.2.1: The radiation therapist does not mode up the final plan for treatment when it is ready. [H1]	6.2.2: The radiation therapist modes up the wrong plan for treatment when working at the treatment console. [H1]	6.2.3: The radiation therapist modes up the final plan for treatment before it is approved or scheduled. [H1] 6.2. 4: The radiation therapist takes too long to mode up the final plan for	N/A

			treatment when working at the treatment console. [H1]	
6.3 Initiate treatment		6.3.1: The wrong plan is delivered to the patient when the treatment is initiated. [H1] 6.3.2: The final plan is incorrect in some parameter(s) when the treatment is initiated. [H1.1-3] 6.3.3: There is a problem with the linac when the treatment is started (or re-started). [H1]	6.3.4: The treatment is initiated before it is appropriate to give the signal to start treatment. [H1.1-3] 6.3.5: The start of treatment is delayed after the signal is given to start treatment. [H1.1-3] 6.3.6: The treatment is appropriately ready to proceed but the signal to start is not given. [H1.1-3]	
6.4 Halt treatment	6.4.1: The therapist does not halt the treatment when it is indicated to do so. [H1.1-3]	6.4.2: The therapist halts the treatment when the best course of action is to allow the treatment to continue. [H1.1-3]		6.4.3: The therapist halts the treatment for a long time when it can be safely resumed. [H1.1-3]

Table 12. Radiation Therapist Controlling the Linear Accelerator (Linac)

Control Action	Not Providing Causes Hazard	Providing Leads to Hazard	Wrong Timing Leads to Hazard	Too Long or Too Short Leads to Hazard
7.1 Set performance expectations (financial and safety)	7.1.1: Hospital administration does not provide safety and financial expectations for the department when planning new procedures. [H3, H4]	7.1.2: Hospital administration provides conflicting safety and financial expectations when the expectations are requested. [H1, H3, H4]	N/A	N/A
7.2 Provide staff and equipment resources	7.2.1: Hospital administration does not provide staff and equipment resources when they are requested. [H3, H4]	7.2.2: Hospital administration provides staff and equipment resources at an inadequate level when they are requested. [H1, H3, H4]	7.2.3: Hospital administration takes too long to provide the requested staff and equipment resources when they are requested. [H1, H3, H4]	N/A

Table 13. Hospital Management Controlling Department Management

Control Action	Not Providing Causes Hazard	Providing Leads to Hazard	Wrong Timing Leads to Hazard	Too Long or Too Short Leads to Hazard
8.1 Approve standard operating procedures	8.1.1: Department administration does not approve the SOPs when a new procedure is started. [H1, H2, H3, H4]	8.1.2: SOPs are approved when they are incorrect or incomplete. [H1, H2, H3, H4]	8.1.3: SOPs are approved after the procedure has been clinically implemented. [H1, H2, H3, H4]	N/A
8.2 Allocate staff and equipment resources	8.2.1: Department administration does not allocate additional staff or equipment when a new procedure is created. [H2, H3, H4]	8.2.2: Department administration under (or over) estimates the resources when starting a new procedure. [H1, H2, H3, H4]	8.2.3: Department administration allocates resources after the new procedure has started. [H1, H2, H3, H4]	8.2.4: Department administration stops the process of resources estimate and request when working with the hospital. [H1, H2, H3, H4]
8.3 Create and maintain department culture	8.3.1: Department administration does not emphasize a safety culture when starting a new procedure. [H1, H2, H3, H4]	8.3.2: Department administration does not set culture correctly or completely (i.e. does not emphasize that the incident learning system should be used) when starting a new procedure. [H1, H2, H3, H4]	8.3.3: Department administration promotes a safety culture after the new procedure has already started. [H1, H2, H3, H4]	8.3. 4: Department administration stops promoting the safety culture after the new procedure has been working successfully for a while. [H1, H2, H3, H4]
8.4 Maintain equipment (service contracts)	8.4.1: Department administration does not maintain equipment when a new procedure is used. [H1, H2, H3, H4]	8.4.2: Department administration under maintains the equipment with inadequate service contract. [H2, H3, H4]	N/A	8.4.3: Department administration lets the service contracts lapse when assessing recurring department needs. [H2, H3, H4]

Table 14. Hospital Management Controlling Radiation Oncology Clinic (Treatment Design and Treatment Delivery)

Control Action	Not Providing Causes Hazard	Providing Leads to Hazard	Wrong Timing Leads to Hazard	Too Long or Too Short Leads to Hazard
9.1 Recommend patient for treatment	N/A	9.1.1: The radiation oncologist recommends the patient for the new procedure when they are not a suitable case. [H1]	N/A	N/A

		9.1.2: The radiation oncologist recommends the patient for the new procedure when the new procedure is not available. [H1]		
9.2 Schedule patient for follow-up	9.2.1: The Radiation Oncologist does not schedule the patient for a follow up visit after the new procedure has been administered. [H1]	9.2.2: The radiation oncologist finds identifies a poor outcome as part of the disease when it is related to the new procedure. [H1]	N/A	9.2.3: The Radiation Oncologist does not see the patient in follow up long enough to identify any problems related to the new procedure. [H1]

Table 15. Radiation Oncologist Controlling the Patient