Systems-Theoretic Process Analysis of the Air Force Test Center Safety Management System

by

Nicholas Chung

B.S. Electrical Engineering (2005)
University of California: San Diego

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

Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology

February 2014

Signature of Author___ Signature redacted

Nicholas Chung
System Design and Management Program
January 17, 2014

Certified by__ Signature redacted

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

Accepted by_____ Signature redacted

Patrick Hale
Director, System Design and Management Program

This Page Intentionally Left Blank

ACKNOWLEDGEMENTS

I would like to sincerely thank my thesis advisor, Professor Nancy Leveson, for changing my perspective regarding safety management and motivating this thesis. As my instructor for System Safety, Professor Leveson expanded my view of accident causation from a focus on linear causality to a more holistic systems-theoretic perspective. With her instruction and guidance, I came to realize the value of taking a systems approach to understand accident causation and hazard analysis. Equally important, she provided me with the tools necessary to analyze systems using Systems-Theoretic Accident Model and Processes (STAMP). Over the past year, it has been inspiring to witness firsthand how Professor Leveson's ideas are rapidly improving the way that people think about safety. Her work has significantly advanced safety engineering in a wide range of fields, including the automotive, healthcare, aviation, and security industries.

I would also like to thank my mentors at the Air Force Test Center. Tony Rubino, Rob Warner, and Chris Klug, I will always appreciate your friendship and guidance. Over the past eight years, you have shown me what true leadership is about. Thank you for all your support, without which I would never have had this opportunity at MIT.

Finally, I would like to thank my family. Mom, thanks for inspiring me with your strength and drive. Dad, thanks for instilling in me a holistic perspective of the world. Christina, thanks for helping me grow up. I hope I'm still making you proud. And Abby, my loving wife, thank you for your everlasting patience and unwavering faith in me. I could not have done any of this without you.

This Page Intentionally Left Blank

Systems-Theoretic Process Analysis of the Air Force Test Center Safety Management System

by

Nicholas Chung

Submitted to the System Design and Management Program
on January 17, 2014 in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

The Air Force Test Center (AFTC) faces new challenges as it continues into the 21st century as the world's leader in developmental flight test. New technologies are becoming ever more sophisticated and less transparent, driving an increase in complexity for tests designed to evaluate them. This shift will place more demands on the AFTC Safety Management System to effectively analyze hazards and preempt the conditions that lead to accidents.

In order to determine whether the AFTC Safety Management System is prepared to handle new safety challenges, this thesis applied Dr. Nancy Leveson's Systems-Theoretic Process Analysis (STPA) technique. The safety management system was analyzed and potential safety constraint violations due to systemic factors, unsafe component interactions, as well as component failures were investigated. The analysis identified the key features that make the system effective; gaps in the sub-processes, roles, responsibilities, and tools; and opportunities to improve the system. These findings will provide insights on how the AFTC Safety Management System can be improved with the aim of preventing accidents from occurring during flight test operations. Finally, this thesis demonstrated the effectiveness of the STPA technique at hazard analysis on an organizational process.

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

This Page Intentionally Left Blank

TABLE OF CONTENTS

CONTENTS

CHAPTER 1: INTRODUCTION

"Technology is changing much faster than our engineering techniques are responding to these changes. New technology introduces unknowns into our systems and creates new paths to losses [1]." This statement from Dr. Nancy Leveson provides a warning for those organizations and individuals that are involved in the development, test, or operation of new technology. For the Air Force Test Center (AFTC), the warning has particular salience since the organization is responsible for conducting research, development, test, and evaluation of the latest aerospace systems from concept to combat. The increasing prevalence of remotely piloted aircraft, focus on more integrated test scenarios, and new complex technologies on the horizon represent significant changes to the nature of testing. The purpose of this thesis is to apply a systems approach called Systems-Theoretic Process Analysis (STPA) to evaluate the completeness and adequacy of the current AFTC Safety Management System in the context of these new types of challenges.

MOTIVATION

Since its establishment in 1951, the AFTC has faced the challenge of safely testing unproven technologies prior to fielding. It has been the site of some of the most important aerospace breakthroughs in history. Among these milestones are the first manned supersonic flight of the X-1, and the extreme high speed flight tests (>4500 mph) of the X-15. Today, Edwards AFB is the focal point for the developmental test of nearly all United States Air Force fighters, bombers, tankers, transports, unmanned aerial systems, as well as many other advanced projects [2].

To manage to the inherent dangers from flight test, a safety management system was developed and implemented. Since its implementation, the safety management system has been highly effective at reducing accident rates during flight test missions. Yet, there is no guarantee that the incidence of accidents will remain low. New technology and more demanding operational needs may change the nature of test in a way that requires new robust methods for analysis. One such concern is the increased focus on developing remotely piloted aircraft. The shift towards unmanned aircraft has brought new risks and test challenges due to the lack of a pilot physically in the cockpit. The opaqueness of the software process models that translate human operator inputs into actions increases the difficulty of recognizing erroneous behavior and limits the operator's ability to take corrective action. Furthermore, the difficulty in accomplishing these two tasks is compounded by the limited feedback to the operator and reliance on data links at risk of delay or interruption – both of which increase uncertainty. Moreover, the operational implementation of aircraft such as

the MQ-1 Predator, where multiple operator elements may share control of the same aircraft at different stages of a mission, can result in unexpected coordination issues. Another concern is an increased emphasis on more integrated test scenarios. This type of testing can be useful for validating that a system can meet the needs of the warfighter in more operationally representative scenarios. While the benefits are significant, these types of tests generally involve multiple aircraft and range assets operating in the same range space. The result is significant component and dynamic complexity. The complexity is even greater if remotely piloted aircraft and actual weapon releases are considered. These are just two concerns with regards to the changing nature of test and subsequent implications to system safety. Is the AFTC Safety Management System prepared to handle these safety challenges?

This discussion can be summarized in two observations:

1. Accidents have been reduced significantly at the AFTC, yet they continue to occur.
2. The nature of aviation technology and flight test for such technology is changing.

Thus the goals of this thesis are:

1. To perform a STPA on the AFTC Safety Management System and identify the features which contribute to its effectiveness.
2. To identify any gaps in the processes, roles, responsibilities, and tools.
3. To identify possible opportunities to improve the process.

RESEARCH QUESTION

Hazard analysis techniques provide a reasonable starting point because process failures can be defined as accidents and the goal of hazard analysis is to identify how accidents can occur before they happen. Commonly used hazard analysis techniques such as Fault Tree Analysis, Event Tree Analysis, Hazard and Operability Analysis, and Failure Modes and Effects Analysis are based on linear event-chain accident models such as Reason's Swiss Cheese model or Heinrich's Domino model. These models assume that losses occur due to a sequence of failure events or conditions that directly lead to an accident. The result is a focus on specific component failures and individual human error rather than considering the system and the system interactions. Applying a technique based on such a limited view would be ineffective for the goal of analyzing the overall safety management system at the AFTC because the system structure and context are precisely the focus of this thesis. In contrast to linear accident models, Leveson has developed an accident model that

applies a system view. It includes the structural and other contextual factors contributing to an accident. The hazard analysis technique based on this understanding is called STPA. STPA uses hierarchical control structures to model the process. Analysis consists of examining control loops for possible unsafe control actions and identifying the factors that can contribute to unsafe actions rather than merely considering component failures.

By applying STPA, this thesis seeks to answer the questions:

1. What are the factors that make the AFTC Safety Management System so effective?
2. Is the AFTC Safety Management System prepared to handle the changing nature of test?
3. If not, what must be done to improve the process?

ORGANIZATION

Chapter 2 presents an overview of accident models that explain how accidents occur. Included in the discussion are a summary of systems theory, critical discussion of linear causality models such as H.W. Heinrich's Domino model and James Reason's Swiss Cheese model, and a summary of Nancy Leveson's Systems-Theoretic Analysis and Process (STAMP) model. From there, the literature review provides a detailed description of the STPA process. Chapter 3 provides key definitions for accidents, system hazards, and system safety constraints for the system under analysis. The AFTC Safety Review Process is then summarized, followed by its hierarchical control structure. Next, Chapter 4 describes the way that the STPA Step 1 was carried out on the AFTC Safety Review Process and lists the component level safety constraints for each controller. In Chapter 5, a discussion of how unsafe control actions from STPA Step 1 can occur is provided. Chapter 6 contains a discussion of the findings from STPA and recommendations for possible improvements in the AFTC Safety Review Process. Finally, the thesis is concluded in Chapter 7 which summarizes the findings of this thesis.

CHAPTER 2: LITERATURE REVIEW

A literature review was conducted to assess the major existing models of accident causation and to select an approach for the hazard analysis of the AFTC Safety Management System. This section begins with a short primer on systems theory followed by a critical review of commonly used accident models based on event-chains and their drawbacks. Accident models form the basis for hazard analysis because they provide a conceptual framework for understanding why accidents occur. Choosing an accident model that considers factors beyond component failure is essential for effective hazard analysis where the goal is to identify accidents before they occur. Following the review of accident models is a brief analysis about the advantages of applying STAMP for hazard analysis. The chapter concludes with a summary of the STPA technique based on STAMP.

SYSTEMS THEORY

A common approach to analyzing systems is the application of a technique called analytic reduction. Analytic reduction is the idea that a system can be decomposed into separate physical components and system behavior can be separated into discrete events over time. From Leveson, the approach is based on three main assumptions [1, pp. 61]:

1. Each component or subsystem operates independently and analysis results are not distorted when the components are considered separately.
2. Components or events are not subject to feedback or nonlinear interactions and the behavior of components is the same when examined individually as when operating as a part of the whole.
3. Interactions among subsystems are simple enough that they can be considered separate from the behavior of subsystems themselves.

According to Leveson, analytic reduction can be appropriate in cases where "the precise nature of component interaction is known and interactions can be examined pairwise." However, where system properties are derived from interactions between the parts of the system, a different approach is necessary [1].

In contrast to analytic reduction, systems approaches apply the concept of holism. Holism is the recognition that a system or component of a system does not operate in a vacuum. By existing, it must share the world with other entities and operate in the context of particular relationships with respect to one another. The relationships imply a level of interaction in which one entity may have

an effect on another and vice versa. Moreover, systems exhibit the key characteristics of hierarchy, emergence, and control [3]. As Leveson says, a system can be considered as a hierarchy of levels of abstraction where interactions at each level of abstraction contribute to emergent properties at the next level up. An emergent property does not exist below the level that it is observed. Safety is an emergent property because it results from component function, their interactions with each other, and interactions with contextual factors at a lower level of abstraction which gives rise to accidents or the absence of accidents. Because control enacted from one level constrains the interaction of components at one or more other levels, it is a key determining factor for the emergent properties of a system. Leveson applies the ideas of hierarchy, emergence, and control to a new model of accident causation. Her model treats safety as dependent on the enforcement of constraints on component behavior and their interactions in a system [1].

Event-Chain Based Models

Traditional event-chain based models were originally developed around industrial accident prevention with the focus on unsafe conditions and human error. These models assume that accidents are caused by chains of directly related events. The assumption about chains of directly related events implies that by examining the sequence of causal events leading to the accident, one can understand the causes, assess risk, and implement preventative measures. At the center of the chain of events model is the idea that if the one link of the chain of events is broken, the accident cannot occur [4][1].

One of the earliest published models is the Heinrich Domino Model (Figure 1). This model visualizes the sequence of actions that lead to an accident as a line of five dominos. Each domino is associated with a key factor that leads to an injury. There is a direct causal relationship between the key factors where one factor causes the next in sequence which eventually leads to an injury. The factors in sequential order are [4]:

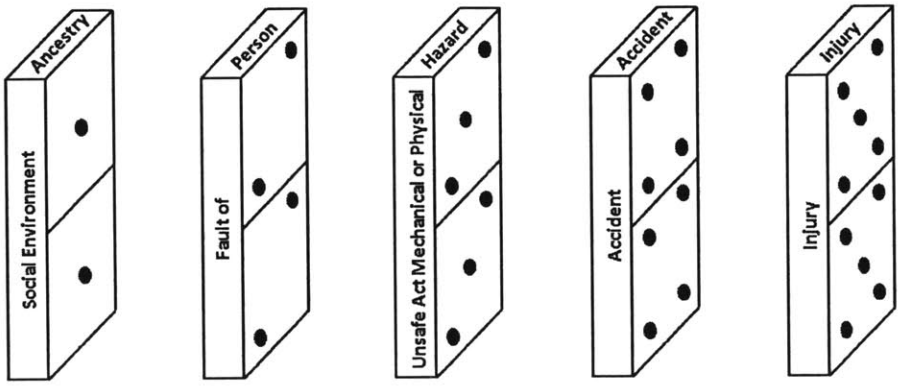

Figure 1: Heinrich Domino Model [4]

1. Ancestry and social environment
2. Fault of person
3. Unsafe act and/or mechanical or physical hazard
4. Accident
5. Injury

The implication of this is that by preventing any one of these factors in the domino sequence, an injury can be prevented. Furthermore, Heinrich proposes that 3. Unsafe act and/or mechanical or physical hazard is the most important factor in the accident chain and safety efforts should primarily focus on preventing unsafe acts [4].

Frank Bird Jr. modifies the original Domino model (Figure 2) by updating the factors to the following:

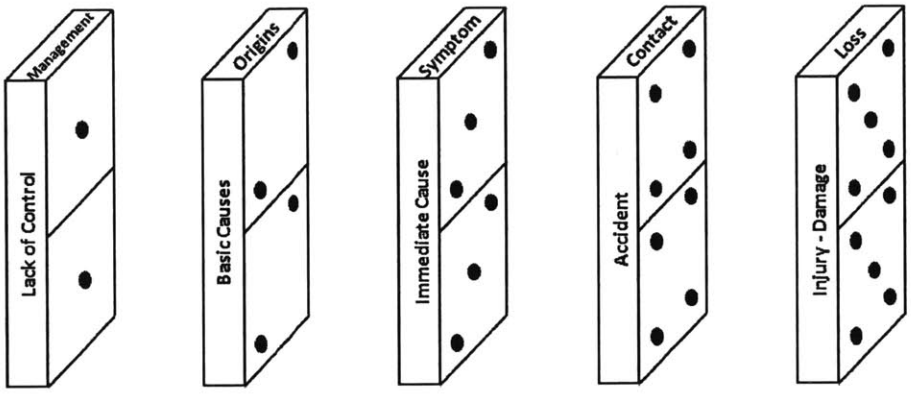

Figure 2: Bird's Update to Heinrich's Domino Model [4]

1. Lack of control by management

2. Basic causes or origins
3. Immediate causes or symptoms
4. Accident or contact with a source of energy
5. Injury, damage, loss

The first domino considers the role that management has in establishing controls by clearly defining roles, establishing standards, measuring management performance, and correcting performance to enforce safe operations. These controls limit the effects of the second domino, basic causes or origins of accidents, by ensuring that employees perform their work within the clearly established management bounds. The remaining three dominos are identical to Heinrich's original model [5][6].

James Reason developed a somewhat different view of accident causation (Figure 3) that remains focused on human error and chains of events but acknowledges some systemic factors [7]. It is upon this view that the Department of Defense Human Factors Analysis and Classification System is based [8]. Reason explains that accidents are caused by what he calls latent failures and active failures. He defines latent failures as human contributions to systems disasters where the "adverse consequences lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defenses." Examples he provides include system defects created by poor design, incorrect installation, faulty maintenance, and bad maintenance decisions. Some latent failures arise because decision makers make strategic and design decisions in the context of a perceived trade-off between applying resources to production versus safety. When high-level decision maker choices contribute to adverse consequences, he calls the choices fallible decisions. Line managers operationalize decision maker choices and in doing so may contribute to what Reason labels preconditions for unsafe acts. Preconditions for unsafe acts are defined as system states that create the potential for a wide variety of unsafe acts. Examples of line management deficiencies are poor scheduling; poor procedures; deficiencies in skills, rules, or knowledge; and maintenance inadequacies. Reason notes that the relationship between latent failures from decision makers and line management and preconditions to unsafe acts is complex. Each line management deficiency may contribute to one or many preconditions to unsafe acts and a combination of line management deficiencies can contribute to one specific precondition or many preconditions. Reason states that there is a lack of clear and direct causation from fallible decisions and line management deficiencies to preconditions for unsafe acts. Preconditions for unsafe acts then contribute to active failures. Reason defines active failures as human contributions to systems

disasters where adverse "effects are felt almost immediately." Reason identifies front-line operators of a complex system as the source of active failures. Active failures are due to unsafe acts which Reason explains are "an error or a violation committed in the presence of a potential hazard." He says that unsafe acts are determined by a complex interaction between the influences from the fallible decisions made by decision makers, line management deficiencies, the preconditions to unsafe acts, and the outside world. "Unsafe acts can only be defined in relation to the presence of a particular hazard [7]."

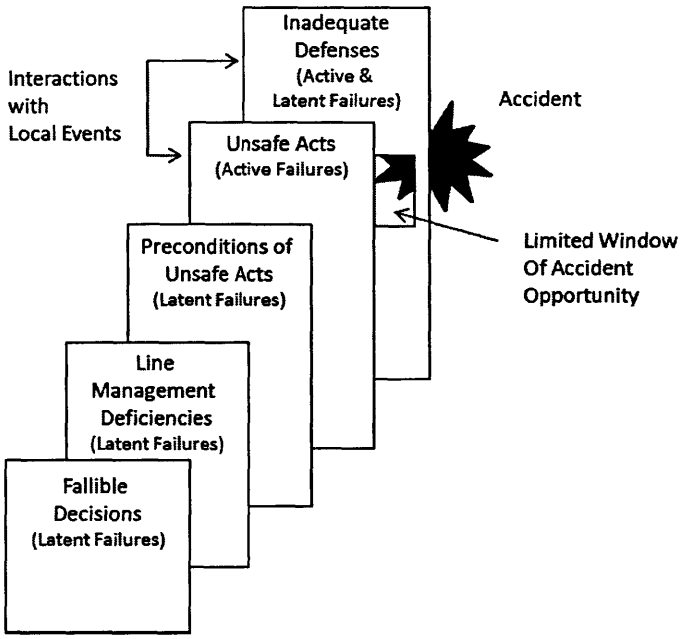

Figure 3: Reason's General Model for Accident Causation [7]

To prevent unsafe acts from becoming accidents, defenses can be established to interrupt the accident chain. In [9], Reason describes what is commonly referred to as the Swiss Cheese model of accident causation (Figure 4). The Swiss Cheese model focuses on the unsafe acts and defenses in depth portions of his original model. He explains that it is the latent and active errors that create holes in the layers of defense or removes them entirely. When the holes line up, hazards are able to come in contact with people or assets and cause an accident. The model most prominently emphasizes the idea of defenses in depth and the causal event-chain with a limited treatment of latent failures.

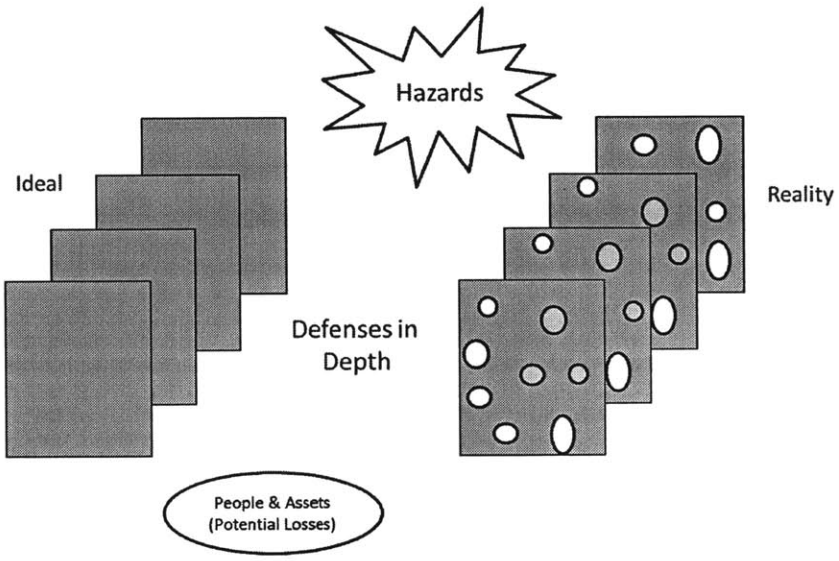

Figure 4: Reason's Swiss Cheese Model [9]

Limitations and Deficiencies in Event-Chain Based Models

Leveson identifies a number of limitations and deficiencies inherent to Event-Chain Based models that have important implications for the way that accidents are interpreted and hazards are identified [1]:

1. Safety vs. Reliability – In event-chain models, the focus is on identifying failure events and how to prevent them. Yet, reliability does not ensure safety. In complex systems, all components may function as intended but their interaction may give rise to unsafe behavior. Conversely, failed components may still be safe provided they fail in a safe manner [1].

   In the original Domino model, the first two dominos relate to human reliability and character. The theory is that if employees were less susceptible to flaws in character they would be more reliable and would not cause accidents. Bird's extension to this model adds the idea that the role of management control is to constrain the behavior of employees and prevent personal or job-related factors that were believed to be the cause of accidents [4]. In effect, strictly constraining employee behavior would increase the reliability of personnel. However, by emphasizing only reliability, the Domino model view ignores the emergence of unsafe behavior due to interactions among people, processes, and machines that are operating reliably. Reason considers unsafe acts to be determined by a complex

interaction between the influences from the fallible decisions made by decision makers, line management deficiencies, preconditions to unsafe acts, operator actions, and the outside world. "Unsafe acts can only be defined in relation to the presence of a particular hazard [7]." Despite recognizing that accidents occur due to complex interactions, Reason makes no attempt to explain how the complex interactions occur. Nor does he consider how adverse interactions can occur among components that are fully functional.

2. Modeling Accident Causation as Event-Chains – The prime assumption in event-chain models is that accidents are caused by chains of directly related events. The implication is that by preventing one or more events in the chain, an accident can be prevented. This type of model ignores systemic factors such as structural, management, and safety culture deficiencies that contribute to accidents because these factors don't have a direct causal relationship [1].

   The Domino model attributes failures to specific events or conditions related to the individual employee's character and actions [4]. While Bird's extension includes management, the model is still constrained to tying the accident to a specific failure event perpetrated by management or the individual. Reason's model mentions systemic factors and categorizes them as "latent errors" and "preconditions to unsafe acts" [7]. Still, his treatment of systemic factors is an oversimplification. Reason recognizes that there is no direct relationship from latent errors and preconditions for unsafe acts to the direct causal chain. However, he explains adverse systemic factors as simply creating holes in the layers of defense or removing the layers all together. While this explanation presents an intuitive representation to describe how accidents occur, the model does not show a meaningful link between systemic factors and the direct causal chain. The inability to express how systemic factors and the direct causal chain actually relate limits the usefulness of Reason's model for considering factors beyond event-chains.

3. Limitations of Probabilistic Risk Assessment – Probabilistic risk assessment is often associated with event-chain models because event-chain models usually assume sequential and independent events that lead to accidents. These assumptions allow a probability to be assigned for each event. From the probabilities, a value can be determined for the likelihood of the event. However, even if probabilities for events could be determined, factors and

events in complex systems are not mutually exclusive. They are often coupled with unquantifiable dependencies. Furthermore, coupling implies that the same systemic factor could affect multiple aspects of a system. The lack of consideration for coupled interactions and systemic factors illustrates a fundamental flaw in the event-chain view and attempts to apply probabilistic risk assessment in the context of complex systems [1].

Both the Domino model and Reason's model center on the idea of sequential and independent events either as dominos that fall or as defensive layers that are breeched sequentially [4][7][9].

4. Role of Operators in Accidents – The event-chain perspective leads to a bias that commonly blames operators for accidents. Event-chain models typically stop at the operator because they are limited in the ability to handle factors upstream of the operator such as systemic factors that contribute to accidents. Moving beyond the operator is difficult because upstream factors do not have direct causal links and cannot be easily incorporated into the event-chain. As a result, event-chain models tend to limit the consideration of safety measures implemented upstream from the direct causal events [1].

   Both Heinrich and Bird's versions of the Domino model provide a limited consideration of influences that are upstream of the operator. In addition, the two models blame the operator for accidents and thus aim prevention measures at the operator [4]. Reason's theories incorporate aspects beyond the front-line operator and recognize some upstream influences that have an effect on accident causation. Furthermore, he suggests that the most effective way of managing safety is to examine and act on line management implementations of high level decisions and precursors to unsafe acts. The improvement of factors upstream from the operator allows for proactive safety control [7]. Even so, Reason's model remains focused on human error, whether during production, management, or design operations. His model does not include the engineering design of the system. Nor does the model provide a method for examining the specifics of how systemic factors contribute to safety or how to control them.

5. Static versus Dynamic Views of Systems – Event-chain models generally ignore systemic factors and consider only the immediate causes of an accident. In doing so, contextual

influences that contribute to accident causation are missed. Moreover, by missing contextual influences, the way that they change over time is also overlooked. Systems may migrate toward states of higher risk due to systemic factors such as shifts in culture or a change in objectives. These changes can have far reaching effects on the way that different aspects of a system operate. By examining only proximal causes in an accident, not only are the systemic factors missed but the changes to these factors over time are also missed [1].

Neither Domino model takes into account general systemic factors or the effect of their dynamics on accident causation [4]. Reason, however, recognizes the broad impact that management and design decisions have on downstream operations. Reason goes further to recognize that the implementation of feedback loops to monitor accidents, unsafe acts, unsafe system states, and adverse line management policies and actions can be used to improve or prevent the erosion of safety over time [7]. Yet, Reason provides no explanation for how safety in organizations may change over time due to dynamics and no details on how to identify and manage the forces that adversely influence safety.

6. The Focus on Determining Blame – Because event-chain models are concerned with identifying the root cause, the result can be a narrow view that blames an individual operator or a specific component failure. Attributing an accident to the root cause is limiting because it ignores other reasons why accidents occur and restricts the possible set of solutions [1].

   The Domino models emphasize the individual operator as the cause of accidents. Solutions are directed at preventing the operator from committing unsafe actions [4]. Reason describes the role of the front-line operator error in accidents but also explains that management and design decisions affect operations. Yet, he still cites human error as the primary cause of accidents [7]. Without a method to understand how systemic factors contribute to safety control, efforts remain primarily aimed at disrupting the causal chain. Blame is then focused on the operator because of the operator role in the causal chain.

The basic event-chain models such as the Domino model and Reason's model are inadequate for understanding hazards in complex sociotechnical systems. They are ill-suited for identifying interactions in failure events and reasons for accidents with no component failure. Additionally, they do not include systemic factors such as organizational design, system design, culture, or

societal pressures. Typical direct causal chain models focus on component failure and human errors because their relationships to accidents are more easily understood than indirect factors. As a result, event-chain models limit opportunities for system-wide improvement. Reason talks about how fallible decisions and line management deficiencies interact in a complex way with precursors of unsafe acts which then interact in a complex way with the "task being performed, the environmental influences, and the presence of hazards. Yet, his treatment for these factors is superficial and inadequate. Moreover, his model does not provide any real explanation for the relationship between specific systemic factors and safety. The lack of explanation for the interaction of systemic factors that contribute to the causal chain makes Reason's model unusable for any worthwhile analysis of systemic factors. For an effective hazard analysis of the AFTC Safety Management System, a new model that adequately handles systemic factors and component interactions is required.

SYSTEMS-THEORETIC ACCIDENT MODEL AND PROCESSES

In order to address the need for a systemic perspective of accidents and analyze them, Leveson developed STAMP. Under STAMP, safety is viewed as an emergent property. Accidents occur when the inadequate enforcement of safety constraints allow unsafe behavior and interaction of components in the system. The system can be defined broadly and include aspects such as societal regulations, design, and operations. Control must be applied to enforce constraints on system components to achieve safety. By considering safety as a control problem, the set of accident causes can be expanded to include flawed control processes involving physical, process, and social aspects of the system. Viewing safety as a control problem represents a paradigm shift from focusing on reliability and component failures to a broader examination of how controls fail to or succeed at enforcing safety [1].

The main aspects of STAMP are safety constraints, the hierarchical control structure, and process models. Controls used to enforce safety constraints may be passive in that they improve safety simply by being present. Examples of passive controls are designs that fail into a safe state and interlocks. In contrast, active controls must be actuated at the appropriate time to enforce a limitation. Active controls incorporate sensors, a decision maker, and actuator to control a process. The decision maker may be a computer or a human being. In both cases, process models allow controllers to consider the current state of the system and implement control actions to achieve desired system behavior [1].

A system may be modeled as a hierarchical control structure. Controllers at each level of the structure enforce safety constraints on lower levels of the hierarchy. The constraints allow desired system behaviors and states while disallowing hazards. Factors affecting safety are traceable from hazards or actual accident events back to inadequate controls at higher levels of the system. By examining each control loop in the control system structure, inadequate control arising from "missing constraints (unassigned responsibility for safety), inadequate safety control commands, commands that were not executed correctly at a lower level, or inadequately communicated or processed feedback about constraint enforcement" can be identified. Hierarchical control structures can be used to assess technical system design, such as the way a hardware system interacts. Social systems or combination sociotechnical systems can also be modeled using a hierarchical control structure [1]. Examples include the military chain of command or the operations of an air traffic control system.

Understanding controller process models in a system can provide insights on component interaction accidents where there are no component failures but the way that components interact is unsafe. Process models are either algorithms programmed into a non-human controller or mental models contained in a human controller's mind. Process models contain information about the perceived current state of the controlled process, how the state of the process might change, and how changes to system variables affect the process state. Using the process model, the controller can compare observed input to the goal condition, select a course of action, and apply control actions, if necessary, to achieve the desired process state. Accidents may occur due to mismatches between the process model and the actual process resulting in [1]:

1. Incorrect or unsafe control commands provided
2. Required control actions not provided
3. Incorrect timing of correct control commands
4. Controls stopped too soon or applied too long

WHY STAMP?

STAMP overcomes many of the limitations found in models based merely on event-chains [1]:

1. Accidents are seen as occurring due to adverse interactions "among people, societal and organizational structures, engineering activities, and physical system components that lead to violating the system safety constraints." This view of accident causation is more inclusive than the view that accidents occur due to direct causal chains of events.

2. With STAMP, the focus of safety management is not on merely stopping component failures but to establish a control structure that enforces safety constraints. Applying and enforcing safety constraints may be more effective and allow more flexibility than focusing only on incorporating specific defenses to interfere with the causal chain.

3. Hierarchical control structures that model systems can be used to examine societal regulation, design, development, operations, and manufacturing and their relationships rather than just focusing on operations.

4. In viewing safety as a control problem and recognizing the role process models play for safety control, STAMP includes not only component failures but also unsafe component interactions. Controllers enforce safety constraints with control loops to prevent both component failures and component interactions leading to hazardous states.

5. The traceability of controls through each level of the hierarchical control structure from component safety constraints to system safety constraints allows for a more comprehensive understanding of accidents beyond direct causal events leading to a failure; an understanding which includes systemic and component interaction factors.

6. Because STAMP recognizes systems as dynamic processes that change due to internal and external forces, system changes over time can be modeled and impact on safety assessed.

Systems-Theoretic Process Analysis

Thus far, this chapter has covered basic aspects of systems theory, critiqued event-chain accident models, and presented STAMP, which addresses many of the limitations inherent in event-chain accident models. In addition to explaining accidents, STAMP can also be used to identify and understand hazards before they become accidents.

Leveson developed a hazard analysis technique based on STAMP called STPA. This technique operationalizes STAMP to systematically evaluate the hierarchical control structure of a system and consider how hazards might occur. The steps for this process from Leveson are [1: pp. 213]:

1. Identify the potential for inadequate control of the system that could lead to a hazardous state. Hazardous states result from inadequate control or enforcement of the safety constraints, which can occur because:
    a. A control action required for safety is not provided or not followed.
    b. An unsafe control action is provided.
    c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.
    d. A control action required for safety is stopped too soon or applied too long.
2. Determine how each potentially hazardous control action identified in Step 1 could occur.
    a. For each unsafe control action, examine the parts of the control loop to see if they could cause it. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems.
    b. Consider how the designed controls could degrade over time and build in protection, including
        i. Management of change procedures to ensure safety constraints are enforced in planned changes.
        ii. Performance audits where the assumptions underlying the hazard analysis are the preconditions for the operation audits and controls so that unplanned changes that violate the safety constraints can be detected.
        iii. Accident and incident analysis to trace anomalies to the hazards and to the system design.

CHAPTER 3: SYSTEM DEFINITION

This chapter provides information describing the system that will be analyzed, the AFTC Safety Management System. It begins with key definitions for the system, accidents, and hazards. Next, the safety constraints for the system are listed. Then, a summary of the AFTC safety management process is provided. Following the summary, the safety control structure that controls safety in the process is illustrated and descriptions for each of the controllers are provided.

SYSTEM DEFINITION, ACCIDENTS, HAZARDS, AND SAFETY CONSTRAINTS

SYSTEM DEFINITION

The subsequent analysis focuses specifically on the AFTC Safety Management System used to analyze hazards, mitigate them, and accept residual risk prior to the initial developmental test flight. STPA can be conducted with an even broader scope to include the original design of the safety management system, the larger organizational system that the safety management system operates in, and flight operations. However, a narrower scope was chosen to allow greater focus on identifying potential gaps in the current safety management system and characterizing the features in the system that make it effective at controlling safety.

ACCIDENTS

The definition of accident as provided by Leveson is "an undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on)" [1]. Leveson's definition of accident is nearly identical to the Air Force Flight Test Center Instruction (AFFTCI) 91-105 definition for mishap [10]. In order to avoid confusion, the term 'accident' will be used throughout this document except when describing the AFTC Risk Assessment Process. Identifying accidents is an important step in defining the goals of the system. The AFTC Safety Management System accidents are:

1. People are killed.
2. Property is damaged or destroyed.
3. Equipment is damaged or destroyed.

SYSTEM HAZARDS

After identifying accidents, the next step is to define the system hazards. This analysis will apply Leveson's definition of hazard. She defines a hazard as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident

(loss)" [1]. By requiring that hazards be the system state or conditions that a system should not be in, Leveson's definition avoids the ambiguity associated with many other definitions. For instance, AFFTCI 91-105 provides a less specific and less useful definition by including all conditions that "can" cause an accident [10]. An airplane in flight can cause an accident but not flying would prevent flight test from occurring. It is more productive to focus efforts on preventing the system state and conditions that the system should not be in rather than including states that the system needs to be in to successfully operate [1]. The system hazards for the safety management system are:

1. The test team does not identify test hazards that will lead to an accident.
2. The test team prescribes inadequate or erroneous mitigation measures that will lead to an accident.
3. Reviewers and approvers accept tests with risks that have not been adequately mitigated or understood.

System Safety Constraints

The system safety constraints are based on the system hazards and provide the safety requirements for the system. An effective safety management system should enforce the system safety constraints to prevent the system hazards from occurring.

In order to prevent the system hazards, the process must satisfy the following system level constraints (requirements):

1. The test team must identify and mitigate test hazards that will lead to an accident.
    a. Clear and effective safety policies for preventing test accidents must be established, maintained, understood, and adhered to consistently at all levels of the organization.
    b. The test team must have a strong understanding of the system under test and the relationship it has to other components of the system including the operator and environment.
    c. The test team must have systematic hazard analysis tools and methods that can provide a consistent and comprehensive understanding of hazards.
    d. The test team must have adequate training in using hazard analysis tools.
    e. The test team must develop mitigation strategies that take into account system interactions in addition to component failures.

f. The test team must have adequate time and resources to complete hazard analysis and develop mitigation strategies.
g. The test team must have access to prior test and safety planning, as well as accident events.

2. Senior leadership must not approve tests with risks that have not been adequately mitigated or understood.
    a. The test team must effectively communicate benefits and test risks after mitigation to senior leadership.
    b. Senior leadership must accept only risks for which the benefit outweighs the risk.

CURRENT AFTC SAFETY MANAGEMENT SYSTEM

SAFETY PLANNING PHASE

In accordance to AFFTCI 91-105, test teams perform hazard analysis on tests that they plan to conduct, devise mitigating strategies to reduce the effect or likelihood of hazard occurrence, and document their findings [10].

Safety Considerations during Test Planning

As prescribed by AFFTCI 91-105, test planning should be conducted with safety as a high priority. Test teams must clearly define the way a test approaches hazardous and unknown conditions. In conditions of greater uncertainty, testers should consider the best way to sequence test points to reduce risk during the progression to higher risk test points. If the test plan is large and/or complex, testers may consider a phased approach that breaks the tests into separate safety packages and reviews [10].

Safety Planning

Hazard analysis, elimination, and control are central to the safety planning effort. AFFTCI 91-105 recommends the following [10]:

To identify hazards:

a. Review hazards, mitigation techniques, and lessons learned from previous tests.
b. Contact personnel or test teams with experience in similar test activities.
c. Research technical aspects of the test.

To eliminate and control hazards (in order of precedence):

a. Design the test to prevent the hazard from occurring.
b. Change the test methodology to reduce the probability, severity, or exposure to the hazard.
c. Incorporate safety devices.
d. Provide caution and warning devices to detect an unsafe condition or trend.
e. Develop procedures and training when it is impractical to change the design or test methodology.

Once analysis is complete, the Project Safety Lead (PSL) works with the Unit Test Safety Officer (UTSO) to document the findings per the format outlined by AFFTCI 91-105.

Test Unit Review

Per AFFTCI 91-105, once safety package documentation is complete, the PSL initiates the Test Unit Review. During this process, the UTSO, Project Pilot, Test Unit Chief Engineer or Technical Director (Unit/CE), and Test Unit Commander (Unit/CC) review the safety package for maturity [10].

Final Safety Review Phase

As described in AFFTCI 91-105, the purpose of this phase is to ensure that all test unique hazards have been identified and mitigated by the safety planning. It is also to assess residual risk and ensure that the documentation provides clear and sufficient information for senior leadership decision-making. AFFTCI 91-105 states that there are four types of independent safety reviews however for the purposes of this thesis, only the safety review board (SRB) meeting will be analyzed because it is the most common and rigorous safety review [10].

Safety Review Board Meeting

The purpose of the SRB meeting is to carefully examine the proposed testing and safety plan to determine whether safety planning has sufficiently mitigated risk and if the safety package is ready to enter the approval phase. Independent safety reviewers and project personnel attend this AFTC System Safety Representative (AFTC/SET) chaired meeting. During the meeting, the test team briefs the audience on the test background, test item description, system maturity, and test methodology. The team also briefs any additional test related documentation. Next, the safety reviewers carefully review the safety package and provide recommendations to change, add, or remove test hazard analyses and general (hazard) minimizing considerations. After the review is complete, the safety reviewers and AFTC/SET representative discuss concerns, perform a risk

assessment, and assign a risk level to the test. Following the SRB meeting, the test team resolves and closes action items identified during the SRB meeting and collects SRB member signatures. Any remaining safety related concerns are documented in the safety package for senior leader review. If substantial changes were made, the test team notifies the Unit/CC and may notify the other test unit reviewers [10].

Risk Assessment

The independent safety reviewers participating in the SRB meeting assess the test risk and recommend a risk level to AFTC leadership for the approval phase. Reviewers are expected to use system safety techniques to identify test unique hazards and assess risk. The AFTC defines risk as a combination of mishap severity and mishap probability.

Mishap Severity

Mishap severity is determined through a qualitative assessment of the most reasonable credible mishap consequence that could occur for each hazard with all mitigation in place. This assessment is based on engineering judgment and/or past experience with similar tests or systems. They are defined in Table 1 [10].

MISHAP SEVERITY	CATEGORY	CONSEQUENCE OF MISHAP
Catastrophic	I	Death, system loss, or severe environmental damage. System loss or equipment damage exceeding $2,000,000 (e.g. Aircraft Class A Mishap).
Critical	II	Severe injury, severe occupational illness, or major system/facility/ environmental damage. For personnel, severe injury or illness equates to lengthy hospital stays and/or permanent injury. Major system/facility/ environmental damage equates to equipment or property damage loss exceeding $500,000 but less than $2,000,000 (e.g. Aircraft Class B Mishap).
Marginal	III	Minor injury, occupational illness, or minor system/ facility/ environmental damage. For personnel, minor injury or illness requires medical treatment resulting in lost work days but no permanent injury. Minor damage equates to losses exceeding $50,000 but less than $500,000 (e.g. Aircraft Class C Mishap).
Negligible	IV	Less than minor injury or system damage. For personnel, the impact of the injury or illness equates to no work days lost. For equipment or facilities, less than minor damage equates to losses less than $50,000.

Table 1: Mishap Severity Classification [10]

Mishap Probability

For each hazard, safety reviewers subjectively assess the mishap probability with all hazard mitigation in place. Reviewers consider contractor or system program office system safety analysis, past experience with similar tests or systems, and use their engineering judgment to determine the mishap probability level that best describes the likelihood of the mishap occurring. Their assessments consider accident causes due to personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system/subsystem component failure or malfunction. The mishap probability definitions shown in Table 2 [10].

PROBABILITY DESCRIPTORS	LEVEL	DESCRIPTION
Very Likely	A	Highly expected to occur - Many significant concerns even after mitigation applied
Likely	B	Expected - Significant concerns remain even after mitigation applied
Less Likely	C	Not expected but possible – Some concern exists even with mitigation applied
Unlikely	D	Unexpected - Minor concerns after mitigation applied
Very Unlikely	E	Highly unexpected – Little or no concern after mitigation applied

Table 2: Mishap Probability Classification [10]

Individual Risk Assessment

The safety reviewers plot their severity and probability assessments for each hazard on the risk assessment matrix. The high, medium, low, and negligible regions are subjectively drawn in the plane and are shown in Table 3 [10].

Probability of Mishap Occurring During the Test	Mishap Severity Category			
	Catestrophic – I Death, System/Facility Loss, Severe Environmental Damage (e.g. Class A Mishap)	**Critical – II** Severe Injury, Occupational Illness, or Major System/Facility/ Environmental Damage (e.g. Class B Mishap)	**Marginal – III** Minor Injury, Occupational Illness, or Minor System/Facility/ Environmental Damage (e.g. Class C Mishap)	**Negligible – IV** Less than Minor Injury, Occupational Illness, or System/ Facility/Environmental Damage (e.g. Class E Mishap)
Very Likely (A) Highly expected to occur – Many significant concerns even after mitigation applied	1	3	7	13
Likely (B) Expected to occur – Significant concerns remain after mitigation applied	2	5	9	16
Less Likely (C) Not expected but possible – Some concern exists even with mitigation applied	4	6	11	18
Unlikely (D) Unexpected – Minor concerns after mitigation applied	8	10	14	19
Very Unlikely (E) Highly unexpected – Little or no concern after mitigation applied	12	15	17	20

HIG
MEDIU
LO
NEGLIGIB

Table 3: Individual Risk Assessment Classification [10]

Overall Risk Assessment

Once the mishap severity and probability for each hazard has been defined, an overall risk assessment is conducted. Reviewers consider all individual hazard mishap severity and probability determinations in the context of the safety control measures, their experience with the test type, understanding of the system under test, complexity of the test, and uncertainty to provide an opinion on the appropriate residual risk level. Reviewers deliberate about the overall risk assessment until consensus is reached. If no consensus is reached, the SRB chairman makes the final risk assessment. Any dissenting opinions are documented. Each risk assessment level is described in Table 4 [10].

ASSESSMENT	DESCRITION AND IMPLICATION
LOW RISK[1]	Tests or activities that present no greater risk than normal operations. Routine supervision is appropriate.
MEDIUM RISK	Tests or activities that present a greater risk to personnel, equipment, or property than normal operations and requires more than routine supervision.
HIGH RISK	Tests or activities that present a significant risk to personnel, equipment, or property, even after all precautionary measures have been taken.

Table 4 Overall Risk Level Descriptions [10]

APPROVAL PHASE

Following the SRB meeting, the safety package enters the approval phase. At this point, the test team has completed safety analysis and risk mitigation on the test and obtained concurrence from test unit leadership, technical experts, aircrew, and system safety. The objective of this phase is to allow AFTC leadership to assume residual test risk by approving the test. This process may require additional briefings, coordination, or actions. Once complete, the Unit/CC and AFTC/SET are notified of any changes and the document is archived. The key senior approvers are shown in Table 5 [10].

ORGANIZATION LEVEL	LOW RISK	MEDIUM RISK	HIGH RISK
System Safety Office	Coord	Coord	Coord
Chief of Safety	Coord	Coord	Coord
412 Test Wing Technical Director	Coord	Coord	Coord
412 Operations Group Commander[2]	Approve	Coord	Coord
412 Test Wing Commander	Info	Approve	Coord
AFFTC Technical Director	Info	Info	Coord
AFFTC Commander	Not Required	Info	Approve

NOTES:

1 For initial test packages. See Chapter 9 for AFFTC Document 5028 amendment approval authorities.

2 Low Risk Approval Authorities:

412 Operations Group Commander (412 OG/CC)--All flight tests and ground tests that involve aircraft operations. All flight training or aerial events not covered under a test plan or approved publication.

412 Test Engineering Group Director (412 TENG/CL)--Tests in EN controlled facilities. Joint approval with 412 OG/CC if assets under OG control are involved in the test.

412 Electronic Warfare Group Commander/Director (412 EWG/CC or EWG/CL)--Tests in EWG controlled facilities. Joint approval with 412 OG/CC if assets under OG control are involved in the test.

412 Maintenance Group Commander (MXG/CC)--Logistics tests conducted in maintenance facilities not associated with a specific test organization or not included as part of a flight test.

Table 5: Leadership Approvals [10]

HIERARCHICAL CONTROL STRUCTURE

The hierarchical control structure was modeled to illustrate the control processes and how they relate to one another to enforce the safety constraints in the safety management system (Figure 5). A summary describing each controller and the controller interaction with the process being controlled is provided. Each individual interface arrow in the diagram is labeled with a number associated with its respective description in the text. Detailed controller model descriptions are provided in Appendix A.

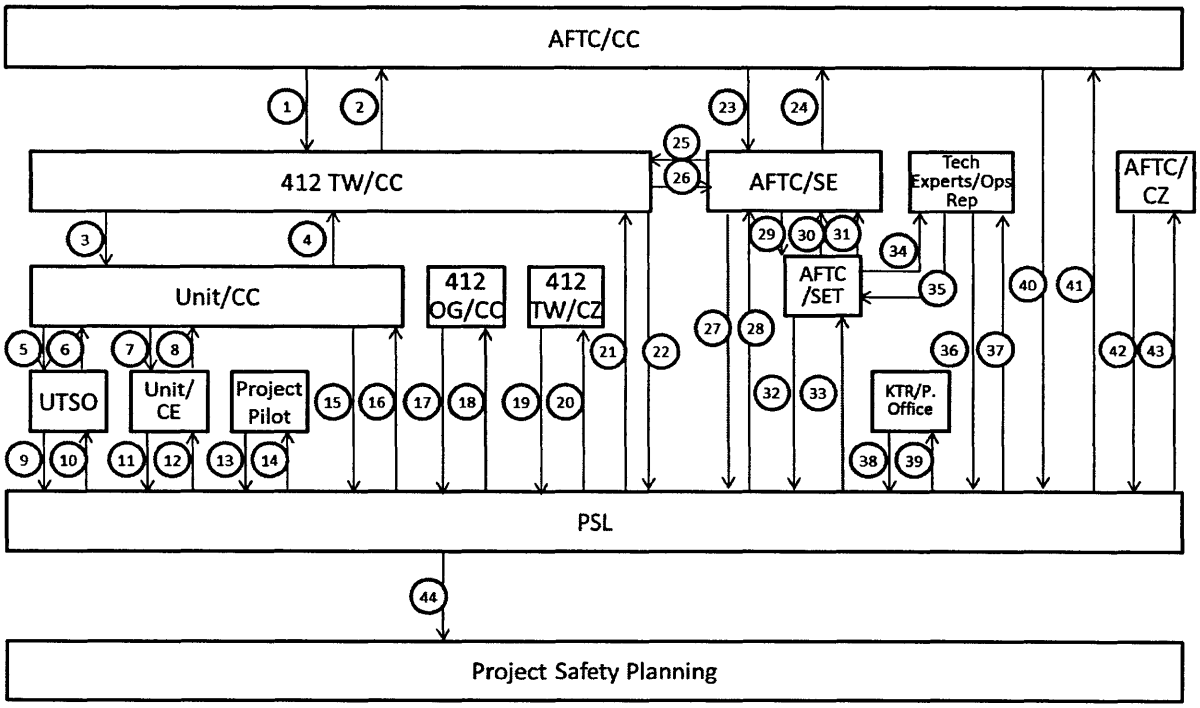

Figure 5: AFTC Safety Management System Hierarchical Control Structure

AFTC/CC

The AFTC Commander (AFTC/CC) is at the top of the chain of command for the test center. AFTC/CC is responsible for implementing higher level safety policies from Air Force Materiel Command (AFMC) at the center. AFTC/CC establishes policies that assign responsibilities for the safety process to the 412 Test Wing Commander (412 TW/CC) and the AFTC Chief of Safety (AFTC/SE). As a safety package reviewer, AFTC/CC provides technical insights as a pilot as well as judgment as to whether the risks outweigh the costs for the proposed testing. In particular, for high risk safety packages, AFTC/CC reviews, provides feedback, and approves the document produced by the PSL. Approval signifies that the proposed testing has sufficiently mitigated risk to the point

where benefits qualitatively outweigh the risks. The control and monitor relationships between AFTC/CC, 412 TW/CC, AFTC/SE, and the PSL are as follows:

Control	Monitor
(1) AFTC/CC provides policy guidance to the 412 TW/CC to ensure the safety of the general public and that the Center is compliant with Air Force Instruction (AFI) 91-202 AFMC Supplement 1.	(2) Through the command relationship and policy review, AFTC/CC monitors 412 TW/CC for compliance.
(23) AFTC/CC provides policy guidance to AFTC/SE to ensure the safety of the general public and that the Center is compliant with AFI 91-202 AFMC Supplement 1.	(24) Through the command relationship and policy review, AFTC/CC monitors AFTC/SE for compliance.
(40) AFTC/CC provides feedback and approval to the PSL during safety reviews to enforce safety policy compliance and sufficient safety risk reduction.	(41) AFTC/CC reviews safety packages and completed action items from the PSL to monitor safety policy compliance and sufficient safety risk reduction.

412 TW/CC

The 412 Test Wing Commander (412 TW/CC) is responsible for all operations including testing at the AFTC. 412 TW/CC receives policy guidance from AFTC/CC regarding safety responsibilities and policy guidance from AFTC/SE regarding the specific implementation of the safety management system. 412 TW/CC provides guidance about the safety management system to the Unit/CC for squadron level implementation. For medium and high risk safety packages, 412 TW/CC provides another pilot's perspective and an opinion regarding the value of accomplishing proposed. Specifically, 412 TW/CC reviews, provides feedback, and approves the document produced by the PSL. Approval for the high risk safety package signifies the 412 TW/CC's opinion that the testing should proceed. The control and monitor relationships between 412 TW/CC, Unit/CCs, and the PSL are as follows:

Control	Monitor
(3) 412 TW/CC provides policy guidance from AFTC/SE and AFTC/CC to the Unit/CCs.	(4) Through the command relationship, 412 TW/CC monitors Unit/CC for compliance

(22) 412 TW/CC provides feedback and approval to the PSL during safety reviews to enforce safety compliance and sufficient safety risk reduction.	(21) TW/CC reviews safety packages and completed action items from the PSL to monitor safety policy compliance and safety risk reduction.

Unit/CC

Each test squadron is commanded by a Unit/CC. The Unit/CC is responsible for the personnel, aircraft, and operations for a particular test squadron. For the safety management process, the Unit/CC ensures that safety guidance from the 412 TW/CC is implemented by the squadron. While safety guidance is provided to all members of the test squadron, the Unit/CC works through the UTSO and Unit/CE to ensure that the test teams are compliant with safety policy. The Unit/CC also reviews all squadron safety packages to provide feedback and approval prior to the documents entering the final safety review process. From the reviewer perspective, the Unit/CC provides pilot insight and determines whether the benefits of testing justify putting people and equipment at risk. During flight operations, if there is an unexpected test result, the Unit/CC also has the responsibility to halt testing until the safety of the tests can be reevaluated. The control and monitor relationships are as follows:

Control	Monitor
(5) Unit/CC provides policy guidance from 412 TW/CC to the UTSO.	(6) Unit/CC informally monitors the UTSO for compliance.
(7) Unit/CC provides policy guidance from 412 TW/CC to the Unit/CE.	(8) Unit/CC informally monitors the Unit/CE for compliance.
(15) Unit/CC provides feedback and approval during safety reviews to the PSL to ensure that the safety package is compliant with policies and sufficiently mitigates risk. During test execution, Unit/CC may rescind approval for PSL to execute tests if there is an unexpected test result.	(16) Unit/CC reviews safety packages and completed action items from the PSL to monitor safety policy compliance and sufficient safety risk reduction. Unit/CC monitors tests execution results from PSL.

UTSO

The UTSO supports the implementation of policy by receiving updates on safety from AFTC/SET, tracking and administering policy related training, and providing formatting guidance for safety

packages. The UTSO accomplishes these tasks to help the project safety leads avoid delays from noncompliant formatting. None of the UTSO responsibilities actually enforce safety constraints; rather the guidance they provide improves efficiency. The control and monitor relationships are listed below:

Control	Monitor
(9) The UTSO provides PSL with policy updates, training, and safety plan format guidance.	(10) The UTSO reviews all safety plans to monitor compliance and collects procedural lessons learned from PSL. The UTSO monitors PSL training completion, maintains training materials, and tracks test and safety packages.

Unit/CE

The unit chief engineer (Unit/CE) is in charge of the engineering team at the squadron. Unit/CEs generally have broad expertise on the squadron specific aircraft platform as well as some deeper experience in various engineering disciplines. For safety, the Unit/CE is focused on two primary goals. The first is ensuring that safety packages produced by squadron PSLs are compliant with test center safety policies. The second is to make sure that sufficient engineering rigor has been applied to identify and mitigate potential violations of safety constraints. As a reviewer, the Unit/CE provides inputs and action items to the PSL to meet these goals. The control and monitor relationships are listed below:

Control	Monitor
(11) Unit/CE provides policy guidance from Unit/CC to the PSL to support the test safety review process. Unit/CE provides feedback and approval from safety reviews to the PSL to ensure that the safety package is compliant with policies and sufficiently mitigates risk.	(12) Unit/CE reviews safety packages and completed action items from PSL to monitor compliance and sufficient safety risk reduction.

Project Pilot

The squadron project pilot is assigned to support the development of the safety package. Project pilots provide a key perspective that combines their years of operational experience on various

aircraft platforms, including the squadron specific platform, with a rigorous test engineering background from test pilot school. The project pilot can identify situations where desired test points are not safely executable due to operational, technical, or human factors limitations. During the safety package review, the project pilot has the opportunity to provide such feedback to the PSL and require action items to address concerns. The control and monitor relationships are summarized below:

Control	Monitor
(13) The Project Pilot provides inputs and action items to the PSL to control safety from the operations perspective.	(14) Project pilot reviews safety package and completed action items from PSL to ensure sufficient safety risk reduction.

412 OG/CC

The 412 Operations Group Commander (412 OG/CC) is responsible for the operations of the test squadrons at the AFTC. As aircrew and a senior leader, the 412 OG/CC provides another operator's perspective on the testing and an opinion regarding the benefits versus the risks of testing. For safety packages of any risk level, the 412 OG/CC reviews, provides feedback, and approves the document produced by the PSL. For low risk testing, the 412 OG/CC makes the final determination as to whether testing should proceed. The control and monitor relationships are summarized below:

Control	Monitor
(17) 412 OG/CC provides feedback and approval to the PSL during safety reviews to control safety from the Operations Group perspective.	(18) 412 OG/CC reviews safety packages and completed action items to ensure sufficient safety risk reduction.

412 TW/CZ

The 412 Test Wing Technical Director (412 TW/CZ) generally has both broad and deep test experience with a variety of aircraft platforms and engineering disciplines. From the perspective of an experienced engineer, the 412 TW/CZ provides technical inputs and action items to the PSL to ensure that sufficient engineering rigor has been applied to identify and mitigate potential violations of safety constraints. The control and monitor relationships are summarized below:

Control	Monitor

(19) 412 TW/CZ provides inputs and action items to the PSL to control safety from the 412 TW/CZ perspective.	(20) 412/CZ reviews safety packages and completed action items to ensure sufficient safety risk reduction.

AFTC/SE

The AFTC Chief of Safety (AFTC/SE) is responsible for developing safety policy and implementing it throughout the center. AFTC/SE adapts AFMC provided guidance to local procedures and issues the AFTC-specific policies to the 412 TW/CC for dissemination to the operational squadrons. AFTC/SE also provides safety policy to AFTC/SET to guide the safety planning and safety review board process. As a reviewer, AFTC/SE ensures that the safety package has fulfilled the safety policy requirements before it continues on to the senior leadership review phase. The control and monitor relationships are summarized below:

Control	Monitor
(25) AFTC/SE sets, maintains, and disseminates safety policy to be implemented by 412 TW/CC ensures the integrity of the test safety review process.	(26) AFTC/SE monitors compliance through informal feedback from 412 TW/CC.
(29) AFTC/SE sets, maintains, and disseminates policy to be implemented by AFTC/SET and ensures the integrity of the test safety review process.	(30) AFTC/SE monitors compliance through informal feedback and lessons learned from AFTC/SET.
(27) AFTC/SE provides inputs and action items to the PSL to control safety from the AFTC/SE perspective.	(28) AFTC/SE reviews safety packages and completed action items to ensure compliance and sufficient safety risk reduction by the PSL.

AFTC/SET

The AFTC system safety representative (AFTC/SET) is typically an experienced engineer that has been a PSL for a number of safety packages in various engineering disciplines and on multiple aircraft platforms. AFTC/SET is responsible for executing AFTC/SE safety policies to conduct an independent safety review on planned testing. AFTC/SET approves the SRB members and moderates the SRB meetings to ensure that safety plans are carefully assessed for technical rigor. As a reviewer, AFTC/SET provides guidance for planning, technical inputs, and action items. Once

the safety review board meeting is complete, AFTC/SET documents and communicates the risk assessment recommendation from the safety review board meeting to AFTC/SE. The control and monitor relationships are summarized below:

Control	Monitor
(34) AFTC/SET requires an independent safety review and experienced board members for safety planning from the Technical Experts and Operations Reps (Tech Experts/Ops Reps).	(35) AFTC/SET oversees the safety review board meeting comprised of the Tech Experts/Ops Reps.
(32) AFTC/SET provides guidance on safety policy, inputs, and action items to the PSL.	(33) AFTC/SET reviews safety planning progress from the PSL to ensure safety review prerequisites have been completed. AFTC/SET also reviews safety packages for policy compliance and for sufficient safety risk reduction.
(31) AFTC/SET provides a recommendation to AFTC/SE on whether or not to allow execution of the test.	-

Technical Experts and Operations Reps

Tech Experts/Ops Reps provide domain expertise from their respective engineering and operational disciplines. Technical experts generally have many years of engineering experience in a field related to similar systems under test while operations representatives are aircrew with significant related operational experience. Technical experts and operations representatives review the safety package and provide action items during the safety review board meeting to ensure a sufficient level of technical rigor. They also provide a risk assessment recommendation to AFTC/SET and senior leadership. The control and monitor relationships are summarized below:

Control	Monitor
(36) Tech Experts/Ops Reps provide inputs and action items to the PSL.	(37) Tech Experts/Ops Reps review test and safety planning documentation and ask the PSL questions to determine whether hazards have been identified and controlled. They review

	documentation to ensure that it is understandable and review completed action items to ensure compliance.
(35) Tech Experts/Ops Reps provide recommendations to AFTC/SET on test risk to control the risk recommendation to leadership.	(34) Tech Experts/Ops Reps review the risk assessment memo generated by AFTC/SET for leadership.

Contractor/Program Office

As the system developers, the contractor (KTR) or in some cases the program offices provide unique insights regarding the system under test. They have a detailed understanding of the system under test from having designed the system and conducting lab testing. The KTR/Program Office provides a safety release that defines the safe operating conditions for the system under test. Oftentimes, the KTR/Program Office also provides a safety assessment or guidance on how to safely conduct testing. The control and monitor relationships are summarized below:

Control	Monitor
(38) The KTR or Program Office conducts safety assessment, provides safety release and safety-related technical expertise to PSL.	(39) The KTR or Program Office monitors the PSL proposed safety plan during the safety package planning and reviews for consistency with guidance.

AFTC/CZ

The AFTC Technical Director (AFTC/CZ) generally has both broad and deep experience with a variety of engineering disciplines and a test background from different test organizations. As an experienced engineer and scientist, the AFTC/CZ provides the PSL with technical planning inputs to help identify and mitigate potential violations of safety constraints. The control and monitor relationships are summarized below:

Control	Monitor
(42) AFTC/CZ provides inputs and action items to the PSL to control safety from the AFTC/CZ perspective.	(43) AFTC/CZ reviews completed action items to ensure that safety risk is sufficiently reduced.

PSL

The project safety lead (PSL) is the squadron engineer responsible for performing analysis to identify and mitigate potential violations of safety constraints, preparing the safety package, and gaining approval at each level of safety review. The PSL directly controls the project safety planning process while the controllers at each level above the PSL provide indirect control. Each reviewer provides a perspective from a unique vantage point to the PSL for incorporation into the safety package. Within the scope of the safety management system under analysis, the PSL does not have a channel from which to monitor the effectiveness of project safety planning. During the execution of testing the PSL may receive some feedback as to whether the safety planning is adequate.

Control	Monitor
(44) PSL controls project safety planning by identifying potential safety constraint violations implementing mitigations in the safety package.	-

Chapter 4: Determining Safety Requirements

The hierarchical control structure and the detailed models of each control loop provide key insights about how the AFTC Safety Management System operates and where the flaws in safety control may occur. The following chapter applies the first step of the STPA technique to the system model in order to identify unsafe control actions and the component requirements to ensure safety. The first section provides a description of how the technique is applied. Then, the technique is applied to the AFTC Safety Management System based on the definitions and controller relationships established in Chapter 3. From the analysis of each controller, component safety requirements are identified. The chapter concludes with a complete listing of the component requirements for each controller to prevent the system hazards from occurring.

STPA Step 1

STPA Step 1 consists of listing each controller control action and considering how the control relationship can be unsafe. In Step 1, only the unsafe behaviors are identified. Determining the causes for the unsafe control actions is done in STPA Step 2. From Leveson, the four types of unsafe control actions are [1: pp. 217]:

- A control action required for safety is not provided or is not followed.
- An unsafe control action is provided that leads to a hazard.
- A potentially safe control action is provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

Unsafe Control Actions in the AFTC Safety Management System

An example of the STPA Step 1 Unsafe Control Action analysis is provided in this section. A table containing the complete analysis is provided in Appendix B.

Controller	Control Action	Not Providing Control Action (CA) Causes	Providing CA Causes Hazard	Wrong Timing/Order of CA Causes Hazard	CA Stopped Too Soon/Applied Too Long

		Hazard			
AFTC/CC	Implement policy (412 TW/CC)	Policy for safety risk mitigation and acceptance is not provided to 412 TW/CC	Inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC	n/a	Existing policy becomes obsolete

Controller: AFTC/CC

Control Action: Implement policy to control safety operations in the 412 Test Wing through the 412 TW/CC.

Hazards (from Chapter 3):

1. The test team does not identify test hazards that will lead to an accident.
2. The test team prescribes inadequate or erroneous mitigation measures that will lead to an accident.
3. Reviewers and approvers accept tests with risks that have not been adequately mitigated or understood.

Unsafe Control Actions:

1. Not Providing Control Action Causes Hazard: If AFTC/CC does not provide the policy for safety risk mitigation and acceptance to the 412 TW/CC, Test Wing units operating without clear direction may inadequately identify and mitigate potential violations of safety constraints. Furthermore, approvers may approve testing that involves unacceptable risks. This unsafe control action may contribute to Hazard 1, 2, or 3.

2. Providing Control Action Causes Hazard: If inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC, Test Wing units may operate without leadership direction. As a result, PSLs from test units may inadequately identify and mitigate potential

violations of safety constraints and approvers may approve testing that involves unacceptable risks. This unsafe control action may contribute to Hazard 1, 2, or 3.

3. Wrong Timing/Order of Control Action Causes Hazard: Because the safety review process occurs over a period of weeks to months, a change in policy will not cause safety issues related to timing or order of the action. If updated policies rectify safety related issues, safety packages in the review process can be halted and revised before being approved.

4. Control Action Stopped Too Soon/Applied Too Long: Should AFTC/CC fail to update an obsolete policy issued to the 412 TW/CC, Test Wing units may operate in accordance to obsolete and potentially inadequate policies. If the nature of the change is safety related, test units may inadequately identify and mitigate potential violations of safety constraints or approvers may approve testing that involves no longer acceptable risks. As a result, Hazard 1 or 2 may occur.

COMPONENT REQUIREMENTS FOR SAFETY

From the STPA Step 1 process described in the previous section and the completed analysis presented in Appendix B, the component level safety requirements for each controller are identified. The safety requirements for each controller are categorized by each primary process under control by the safety management system. Controllers and control actions that do not contribute to safety were omitted.

Safety Policy

AFTC/CC

1. AFTC/CC must provide policy for safety risk mitigation and acceptance to 412 TW/CC.
2. AFTC/CC must not provide inadequate policy for safety risk mitigation and acceptance to 412 TW/CC.
3. AFTC/CC must update existing safety policy for 412 TW/CC before it becomes obsolete.
4. AFTC/CC must provide policy for safety risk mitigation and acceptance to AFTC/SE.
5. AFTC/CC must not provide inadequate policy for safety risk mitigation and acceptance to AFTC/SE.
6. AFTC/CC must update existing safety policy for AFTC/SE before it becomes obsolete.

Safety Review Process Policy

AFTC/CC

1. AFTC/CC must not issue waivers to 412 TW/CC that violate safety constraints.
2. AFTC/CC must not issue waivers to AFTC/SE that violate safety constraints.

AFTC/SE

1. AFTC/SE must provide policy for safety risk mitigation and acceptance to 412 TW/CC.
2. AFTC/SE must not provide inadequate policy for safety risk management and acceptance to 412 TW/CC.
3. AFTC/SE must update existing safety policy for 412 TW/CC before it becomes obsolete.
4. AFTC/SE must provide policy for safety risk mitigation and acceptance to AFTC/SET.
5. AFTC/SE must not provide inadequate policy for safety risk management and acceptance to AFTC/SET.
6. AFTC/SE must update existing safety policy for AFTC/SET before it becomes obsolete.
7. AFTC/SE must not provide modified policy guidance that weakens the safety process to AFTC/SET.
8. AFTC/SE must rescind modified policy guidance issued to AFTC/SET as soon as its use is no longer justified.

412 TW/CC

1. 412 TW/CC must provide policy for safety risk mitigation and acceptance to the Unit/CCs.
2. 412 TW/CC must not provide inadequate policy for safety risk mitigation and acceptance to the Unit/CCs.
3. 412 TW/CC must update existing safety policy for Unit/CCs before it becomes obsolete.

Approval

AFTC/CC

1. AFTC/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
2. AFTC/CC must not provide approval for safety packages before prior reviewer feedback to the PSL is incorporated.

AFTC/CZ

1. AFTC/CZ must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.

412 TW/CC

1. 412 TW/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
2. 412 TW/CC must not provide approval for safety packages before prior reviewer feedback to the PSL is incorporated.

412 OG/CC

1. 412 OG/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
2. 412 OG/CC must not provide approval for safety packages before prior reviewer feedback to the PSL is incorporated.

412 TW/CZ

1. 412 TW/CZ must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.

AFTC/SE

1. AFTC/SE must not provide approval for safety packages that have not met the requirements for safety planning and independent safety review.

AFTC/SET

1. AFTC/SET must not understate the risk assessment provided to leadership.

Unit/CC

1. Unit/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
2. Unit/CC must rescind approval to test if test has an unexpected result.

Unit/CE

1. Unit/CE must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.

Project Pilot

1. Project pilot must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.

Final Safety Review

AFTC/SET

1. AFTC/SET must not conduct the safety review board meeting too early (before final safety review prerequisites are complete).
2. AFTC/SET must select qualified safety review board members to participate in the safety review board meeting.
3. AFTC/SET must provide safety review board meeting guidance to safety review board members.
4. AFTC/SET must not provide safety review board meeting guidance that detracts from a focus on safety.
5. AFTC/SET must apply meeting guidance effectively throughout the safety review board meeting.
6. AFTC/SET must not provide approval for safety packages that have not met the requirements for safety planning and independent safety review.

Tech Experts/Ops Reps

1. Tech Experts/Ops Reps must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
2. Tech Experts/Ops Reps must not understate the risk assessment provided to AFTC/SET.

Safety Package Preparation

AFTC/CC

1. AFTC/CC must provide action items to the PSL if safety planning is inadequate.
2. AFTC/CC must not provide action items that lead to the violation of safety constraints to the PSL.

AFTC/CZ

1. AFTC/CZ must provide action items to the PSL if safety planning is inadequate.
2. AFTC/CZ must not provide action items that lead to the violation of safety constraints to the PSL.

412 TW/CC

1. 412 TW/CC must provide action items to the PSL if safety planning is inadequate.
2. 412 TW/CC must not provide action items that lead to the violation of safety constraints to the PSL.
3. 412 TW/CC must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

412 OG/CC

1. 412 OG/CC must provide action items to the PSL if safety planning is inadequate.
2. 412 OG/CC must not provide action items that lead to the violation of safety constraints to the PSL.
3. 412 OG/CC must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

412 TW/CZ

1. 412 TW/CZ must provide action items to the PSL if safety planning is inadequate.
2. 412 TW/CZ must not provide action items that lead to the violation of safety constraints to the PSL.
3. 412 TW/CZ must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

AFTC/SE

1. AFTC/SE must provide action items to the PSL if safety planning is inadequate.
2. AFTC/SE must not provide action items that lead to the violation of safety constraints to the PSL.
3. AFTC/SE must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

AFTC/SET

1. AFTC/SET must provide action items to the PSL if safety planning is inadequate.
2. AFTC/SET must not provide action items that lead to the violation of safety constraints to the PSL.
3. AFTC/SET must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

Tech Experts/Ops Reps

1. Tech Experts/Ops Reps must provide action items to the PSL if safety planning is inadequate.
2. Tech Experts/Ops Reps must not provide action items that lead to the violation of safety constraints to the PSL.
3. Tech Experts/Ops Reps must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package

Unit/CC

1. Unit/CC must provide action items to the PSL if safety planning is inadequate.
2. Unit/CC must not provide action items that lead to the violation of safety constraints to the PSL.
3. Unit/CC must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

Unit/CE

1. Unit/CE must provide action items to the PSL if safety planning is inadequate.
2. Unit/CE must not provide action items that lead to the violation of safety constraints to the PSL.
3. Unit/CE must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

Project Pilot

1. Project pilot must provide action items to the PSL if safety planning is inadequate.
2. Project pilot must not provide action items that lead to the violation of safety constraints to the PSL.

3. Project pilot must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

Hazard Analysis and Mitigation

KTR/Program Office

1. KTR/Program Office must provide a safety assessment.
2. KTR/Program Office must not provide an incorrect safety assessment.
3. KTR/Program Office must not provide a safety assessment late in or after the safety package review process.
4. KTR/Program Office must provide safe test conditions.
5. KTR/Program Office must not provide unsafe test conditions.

PSL

1. PSL must analyze and mitigate potential safety constraint violations.
2. PSL must not incorrectly analyze or mitigate potential safety constraint violations.

CHAPTER 5: CAUSES OF UNSAFE CONTROL ACTIONS

STPA Step 1 provided a listing of the unsafe control actions for each controller and the corresponding safety requirements. In this chapter, the causes of the unsafe control actions are discussed. First, a summary of Leveson's STPA Step 2 is provided, followed by a description of how Stringfellow's guidewords can be used to assist in the analysis of contextual factors. Next, an example of STPA Step 2 with guidewords is presented. At the end of the chapter, an analysis of systemic factors and their dynamics is conducted based on the complete STPA Step 2.

STPA STEP 2

In STPA Step 2, each detailed control loop is analyzed both as a whole and in parts to determine what can lead to unsafe control actions. Leveson provides a general control loop model that is useful in guiding efforts to analyze specific control loops (Figure 6).

The parts of the control loops and associated considerations regarding how unsafe control actions may occur are listed below [1]:

Control Inputs: How can missing or wrong control inputs or external information lead to the unsafe control action?

Inadequate Control Algorithm: What are potential flaws in the way the control algorithm works? Are there process changes, modifications, or adaptations to the control algorithm that can lead to the unsafe control action? Are control actions inappropriate, ineffective, or missing?

Process Model: Can a controller process model inconsistent with the process being controlled lead to a hazard? How can the controller process model become incomplete or incorrect? Is there feedback from the controlled process that is providing correct, complete, sufficient, and timely information to the controller so the controller can provide valid commands? If there is a sensor that samples information from the controlled process and provides it to the controller, is it accurate? Can it fail? Does it provide timely information?

Controlled Process: Are there component failures or changes over time that can lead to an unsafe control action? Are there other controllers that may provide conflicting commands? Are there environmental conditions that can cause the controlled process to be unsafe? Is there an actuator between the controller and the controlled process that could fail or delay the implementation of commands?

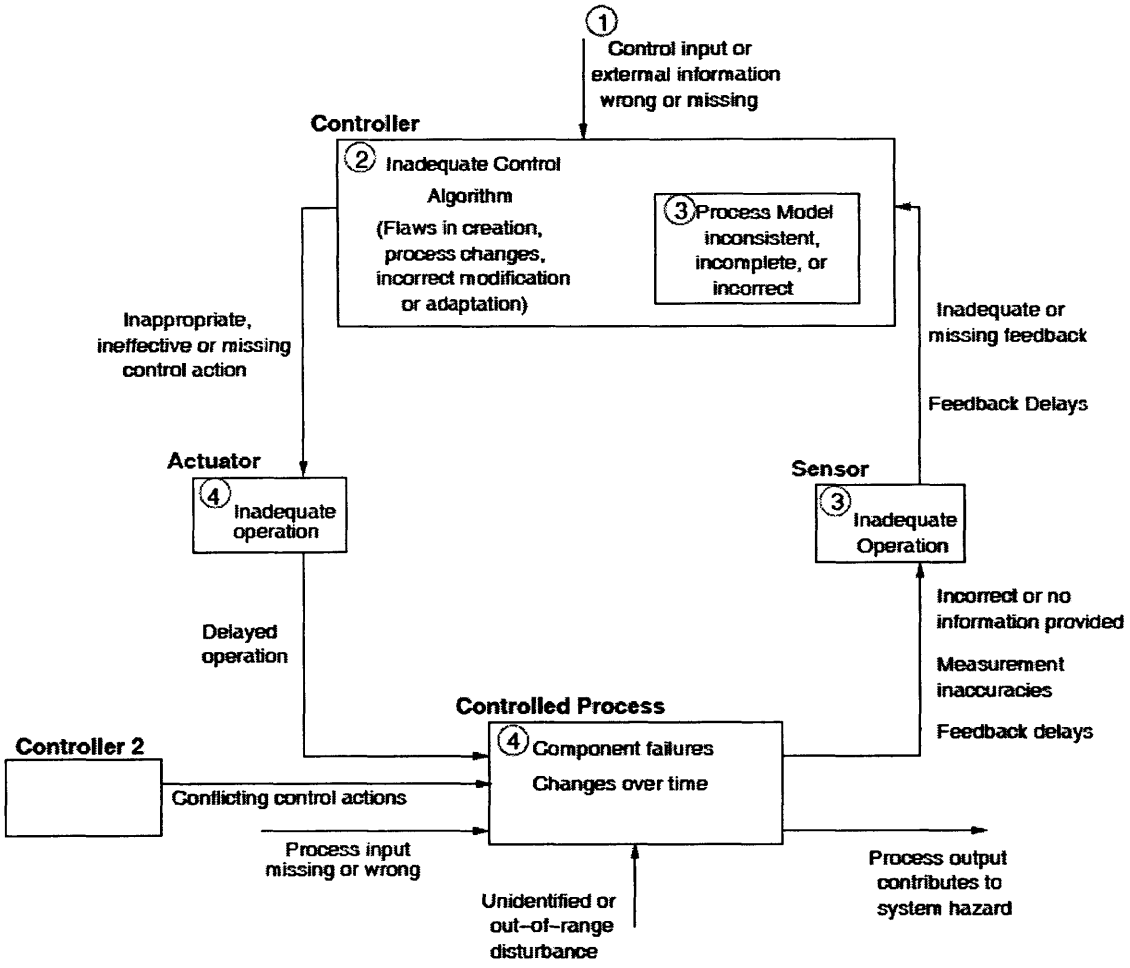

Figure 6: Causal Factors to Consider in STPA Step 2 [1]

CAUSAL FACTOR GUIDEWORDS

Based on the analysis of accident reports, Stringfellow identified nine generalizable contextual factors that influence human and organizational decision-making. The nine factors can be used as guidewords to help in the identification of issues in system design and decision-making that can lead to unsafe control. These guidewords are applied during STPA Step 2 for the AFTC Safety Management System to assist with analyzing the control loops. The guidewords are [11]:

History: History includes the past context of the organization, process, or controller.

Resources: Resources emphasizes the consideration of the effect of assets such as manpower, money, and time.

Tools and Interface: Tools consider how the quality, availability, design, and accuracy of tools can affect control. Interface deals with how interfaces between humans and machines affect the controller's ability to enforce safety.

Training: Training describes the quality, frequency, availability, and design of training.

Human Cognition Characteristics: The human cognition characteristics guideword refers to the suitability of system aspects for human use from the point of view of cognition. Factors include personality and level of mental stimulation.

Pressures: Pressures can include forces such as resource scarcity, political agendas, incentives, or production requirements.

Safety Culture: Safety culture involves how individuals in an organization perceive and consider safety in their tasks. Factors may be tolerance to workarounds and how safety is prioritized by individuals and the organization.

Communication: Communication focuses analysis on the way that information is transferred and how adequately it is transferred. Aspects of communication include the language, procedures, data, and required information.

Human Physiology: Human physiology is a guideword that emphasizes the consideration of human physiology in determining the suitability of control requirements assigned to people. Physiological factors may involve limitations such as sleep requirements or ergonomics.

Example of STPA Step 2 Analysis of Project Safety Planning

To illustrate how STPA Step 2 analysis is conducted, the following section analyzes the project safety planning aspect of the AFTC Safety Management System. It is a subset of the analysis provided in its entirety in Appendix C. Subsequent discussions in this thesis are based on the complete analysis.

KTR/Program Office

Unsafe Control Action for KTR/Program Office: Safety assessment not provided to PSL. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

a. KTR/Program Office does not have the required technical data to assess safety.
b. KTR/Program Office does not have adequate technical experience to assess safety.
c. KTR/Program Office does not have sufficient funding to assess safety.
d. KTR/Program Office does not have sufficient manpower to assess safety.
e. KTR/Program Office does not have sufficient time to assess safety.

Scenario 2: KTR/Program Office does not provide safety assessment to the PSL.

a. KTR/Program Office does not effectively communicate safety assessment to the PSL.

Scenario 3: KTR/Program Office assumes that the PSL has incorporated adequate safety measures into the safety package.

a. PSL provides no feedback about safety measures incorporated causing KTR/Program Office to assume that the PSL has incorporated sufficient safety measures.
b. PSL provides incorrect feedback about incorporating sufficient safety measures causing KTR/Program Office to believe that the PSL has incorporated sufficient safety measures.
c. KTR/Program Office misinterprets feedback and believes that the PSL has incorporated sufficient safety measures.

Scenario 4: PSL does not incorporate safety assessment recommendations into the safety package.

a. PSL does not receive safety assessment recommendations.
b. PSL overlooks safety assessment recommendations.
c. PSL ignores safety assessment recommendations.
d. PSL misinterprets safety assessment recommendations.

Unsafe Control Action for KTR/Program Office: Incorrect safety assessment provided to PSL. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

a. KTR/Program Office does not have the required technical data to provide correct safety assessment.
b. KTR/Program Office does not have adequate technical experience to provide correct safety assessment.
c. KTR/Program Office does not have sufficient funding to correctly assess safety.
d. KTR/Program Office does not have sufficient manpower to correctly assess safety.
e. KTR/Program Office does not have sufficient time to correctly assess safety.

Scenario 2: KTR/Program Office provides inadequate safety assessment recommendations to the PSL.

a. KTR/Program Office communicates unsafe safety assessment recommendations to the PSL.

Scenario 3: KTR/Program Office assumes that incorrect safety assessment recommendations are adequate.

a. PSL does not provide feedback about the adequacy of safety assessment recommendations causing KTR/Program Office to assume that the PSL has incorporated sufficient safety measures.
b. PSL provides incorrect feedback about the adequacy of safety assessment recommendations causing KTR/Program Office to believe that the PSL has incorporated sufficient safety measures.
c. KTR/Program Office misinterprets feedback and believes that the safety assessment recommendations are adequate when they are not.

Scenario 4: PSL incorporates unsafe safety assessment recommendations.

a. PSL assume that the safety assessment recommendations are safe when they are not.

Unsafe Control Action for KTR/Program Office: Safety assessment provided late in or after review process. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: Policies do not require safety assessment from the KTR/Program Office prior to entering the safety review cycle.

a. The possibility of a safety constraint violation due to insufficient information provided to reviewers from the KTR/Program Office is not recognized and requirements for key information are not written into policy.

Scenario 2: KTR/Program Office provides safety assessment recommendations that lead to the violation of safety constraints or change assessed risk levels after reviewers have completed their review.

a. Due to other priorities, the KTR/Program Office is unable to provide a timely safety assessment but allows the safety package to enter planning and review.
b. Safety recommendations are provided after the safety package has been partially or completely reviewed.

Scenario 3: KTR/Program Office assumes that safety assessment recommendations will not adversely affect safety.

a. KTR/Program Office perceives that providing safety assessment recommendations out of sequence will increase safety rather than reduce safety.
b. Unsafe recommendations may go undetected and no feedback to the KTR/Program Office will be provided.

Scenario 4: PSL incorporates safety assessment recommendations that lead to the violation of safety constraints.

a. PSL incorporates safety assessment recommendations that lead to the violation of safety constraints from KTR/Program Office after safety reviewers have reviewed and approved.
b. PSL incorrectly interprets safety assessment recommendations from KTR/Program Office and incorporates them in a way that may lead to the violation of safety constraints after reviewers have reviewed and approved.

Unsafe Control Action for KTR/Program Office: Safe test point conditions not provided to PSL. (CA: Provide Safety Release)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

a. KTR/Program Office does not have the required technical data to determine safe test conditions.
b. KTR/Program Office does not have adequate technical experience to determine safe test conditions.
c. KTR/Program Office does not have sufficient funding to determine safe test point conditions
d. KTR/Program Office does not have sufficient manpower to determine safe test point conditions.
e. KTR/Program Office does not have sufficient time to determine safe test point conditions.

Scenario 2: KTR/Program Office does not provide safety release to the PSL.

a. KTR/Program Office does not effectively communicate safety release to the PSL.

Scenario 3: KTR/Program Office assumes that the PSL has incorporated safe test conditions into the safety package.

a. PSL provides no feedback about planned test conditions causing KTR/Program Office to assume that the PSL has incorporated sufficiently safe test points.
b. PSL provides incorrect feedback about planned test conditions causing KTR/Program Office to believe that the PSL has incorporated sufficiently safe test points.
c. KTR/Program Office misinterprets feedback and believes that the PSL safe test conditions when PSL has not.

Scenario 4: PSL does not incorporate safe test point conditions into the safety package.

a. PSL does not receive safe test point condition guidelines.
b. PSL overlooks safe test point condition guidelines.
c. PSL ignores safe test point condition guidelines.

d. PSL misinterprets safe test point condition guidelines.

Unsafe Control Action for KTR/Program Office: Unsafe test conditions provided to PSL. (CA: Provide Safety Release)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

a. KTR/Program Office does not have the required technical data to correctly determine safe test conditions.
b. KTR/Program Office does not have adequate technical experience to correctly determine safe test conditions.
c. KTR/Program Office does not have sufficient funding to correctly determine safe test point conditions
d. KTR/Program Office does not have sufficient manpower to correctly determine safe test point conditions.
e. KTR/Program Office does not have sufficient time to correctly determine safe test point conditions.

Scenario 2: KTR/Program Office provides unsafe test conditions to the PSL.

a. KTR/Program Office communicates unsafe test conditions to the PSL.

Scenario 3: KTR/Program Office assumes that unsafe test conditions are safe.

a. PSL does not provide feedback about the safety of the test conditions causing KTR/Program Office to assume that the PSL has incorporated sufficiently safe test points.
b. PSL provides incorrect feedback about the safety of the unsafe test conditions causing KTR/Program Office to believe that the PSL has incorporated sufficiently safe test points.
c. KTR/Program Office misinterprets feedback and believes that the test conditions are safe when they are not.

Scenario 4: PSL incorporates unsafe test conditions into the safety package.

a. PSL assumes that the test conditions are safe when they are not.

PSL

Unsafe Control Action for PSL: Potential safety constraint violations not analyzed and mitigated. (CA: Analyze and Mitigate Potential Safety Constraint Violations)

Controlled Process: Hazard analysis by PSL

Scenario 1: PSL technical data, technical experience, and guidance are insufficient.

a. PSL does not have the required technical data from the KTR/Program Office or the Technical Library to identify safety constraints, how they might be violated, and how to avoid violating them.
b. PSL does not have adequate technical experience to identify safety constraints, how they might be violated, and how to avoid violating them.
c. PSL does not have enough guidance from technical experts to identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 2: PSL does not identify safety constraints and how they might be violated.

a. The hazard analysis process is inadequate to identify safety constraints, how they might be violated, and how to avoid violating them.
b. The PSL has insufficient time to identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 3: PSL assumes that past testing is representative of current tests.

a. PSL applies identical or similar safety constraints and mitigating procedures as previous tests when the previous test safety planning is inadequate or does not apply to current testing.

Scenario 4: PSL does not identify potential safety constraint violations.

a. PSL overlooks potential safety constraint violations during analysis.

Unsafe Control Action for PSL: Incorrect analysis or mitigation of potential safety constraint limitations. (CA: Analyze and Mitigate Potential Safety Constraint Violations)

Controlled Process: Hazard analysis by PSL

Scenario 1: PSL technical data, technical experience, and guidance are insufficient.

a. PSL does not have the required technical data from the KTR/Program Office or the Technical Library to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
b. PSL does not have adequate technical experience to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
c. PSL does not have enough guidance from technical experts to correctly identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 2: PSL does not correctly identify safety constraints and how they might be violated.

a. The identification process is inadequate to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
b. The PSL has insufficient time to correctly identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 3: PSL assumes that past testing is representative of current tests.

a. PSL applies identical or similar safety constraints and mitigating procedures as previous tests when the previous test safety planning is inadequate or does not apply to current testing.

Scenario 4: PSL does not correctly analyze potential safety constraint violations.

a. PSL overlooks potential safety constraint violations during analysis.
b. PSL misunderstands how safety constraints can be violated.
c. PSL applies mitigating procedures that cause safety constraint violations.

Contextual Factors Affecting Project Safety Planning

History: KTR/Program Office engineers and the PSL may employ techniques for safety analysis based on precedence however, they may be inadequate. Historical data may be used in determining safety constraints or mitigation measures but they may not be applicable to current testing.

Resources: Inadequate time, manpower, money, expertise, or information may be factors that cause KTR/Program Offices or the PSL to perform safety analysis and mitigation inadequately.

Tools and Interface: Inadequate tools for performing hazard analysis could result in potential safety constraint violations being overlooked or not sufficiently managed.

Training: KTR/Program Office engineers or the PSL may be inadequately trained on the systems under test or in safety analysis techniques leading to inadequately identified potential violations of safety constraints.

Pressures: Pressures to meet deadlines may limit KTR/Program Office engineer or PSL's ability to thoroughly analyze safety for test planning.

Safety Culture: A weak safety culture may cause the KTR/Program Office or the PSL to inadequately prioritize and perform safety analysis.

Communication: Inadequate communication and collaboration between the PSL and the KTR/Program Office could lead to misunderstandings about the existence of potential violations of safety constraints, appropriate ways to manage them, or whether they have been considered in safety planning. Inadequate communication of requirements and deadlines may also contribute to the KTR/Program Office engineers not providing safety analysis information on time.

Systemic Factors and Dynamics in the AFTC Safety Management System

Further analysis was conducted on the guidewords from the complete STPA Step 2 to determine additional factors that contribute to the context and how they might affect safety control over time.

History: The absence of accidents may be perceived as the result of an effective safety management system. Processes and procedures may be based on historical precedence and may only change incrementally, if at all. Controllers may be reluctant to invest resources in modifying a system that appears to work well. History, however, may not be indicative of the future. The test environment may change in subtle ways over time eroding the effectiveness of the safety management system to control safety.

Resources: Among factors that affect resources are governmental budget concerns such as sequestration that can limit hiring or reduce money for testing. Reduced money for testing may also reduce the amount of time available for testing. Reduced resources over a sustained period of time may drive iterations of cost reduction efforts that individually may not substantially reduce safety control but over time may erode safety requirements. Insufficient funding and reduced safety requirements may lead to reductions in the workforce and a longer term impact in technical experience. For a safety process that is as dependent on expert reviewers, loss of expertise will likely have an adverse impact on safety control.

Tools and Interface: Tools may not have been developed due to lack of expertise, resources, or perceived importance. A lack of tools to collect feedback on the effectiveness of processes and the implementation of policy can cause leadership to be misinformed about the effectiveness of the safety management system and miss indicators that change is needed. The lack of safety analysis tools may impede the identification of potential safety constraint violations for more complex systems under test. Over time, the safety management system may no longer be effective.

Training: Training may not be available due to the lack of expertise or priority to develop and conduct effective training. A lack of formalized training can lead to unclear and inconsistent processes as the processes change to adapt to pressures. For instance, an increased emphasis on shorter test timelines may erode safety controls such as the safety review board meeting.

Pressures: Pressures from schedule or budgetary constraints may affect policy implementation. For example, a perception that the warfighter has an urgent need may lead to the reduction in the enforcement of safety policy rigor in favor of more rapid testing and fielding. Major budgetary concerns such as sequestration may raise the concern of organizational consolidations and the elimination of organizations perceived as ineffective or redundant may also have a similar effect on safety. Pressures, real or perceived, may come from higher level leadership and affect lower levels of control such approval, final safety review, safety package preparation, or the identification of potential violations of safety constraints. Over time, pressures can lead to the acceptance of lower standards and the implementation of workarounds that may have adverse consequences.

Safety Culture: Safety culture may be weakened by a number of factors including a history of success, leadership views, lack of tools and training, pressures to produce, and inadequate communication. The conduct of controllers in the safety management system also contributes to safety culture. For instance, a lack of quality feedback can contribute to the perception that

reviewers don't consider safety important. Over time, factors that erode safety culture and a weakening safety culture can be mutually reinforcing. The reinforcing cycle of safety culture decline may continue until leadership increases the emphasis on safety. In some cases, attention is focused on safety only after an accident has occurred.

Communication: Inadequate communication may occur due many reasons including physical separation, inadequate resources, lack of established channels or tools for communication, or apathy by the controllers. In the long-term, poor communication may become the status quo and reduce the effectiveness of safety control by negatively impacting the way that controllers operate together as part of the safety management system.

CHAPTER 6: DISCUSSION – STPA FINDINGS

The following chapter captures the findings from conducting STPA on the AFTC Safety Management System. The first section revisits the AFTC Hierarchical Control Structure to examine the features that make the safety management system highly effective at controlling safety. Then, a comparison between the requirements described in AFFTCI 91-105 and those identified by STPA is provided. At the conclusion of this chapter, key findings, areas for further investigation, and high level recommendations are provided.

HIERARCHICAL CONTROL STRUCTURE

By examining the hierarchical control structure and the control loops found in Chapter 3, it can be seen that the AFTC Safety Management System is well-organized to control safety. Responsibilities are carefully outlined in the AFFTCI 91-105 document. At nearly every level of control, there is a control and monitor channel to ensure that controls are implemented as intended.

For general safety policy and safety review process policy (Figure 7), the responsibilities for establishing and disseminating safety policy are clearly allocated and monitoring channels are established to verify the desired result. An additional feedback channel between AFTC/SET and AFTC/SE provides a key linkage between operations and policy to provide AFTC/SE insight about operations and guide policy updates.

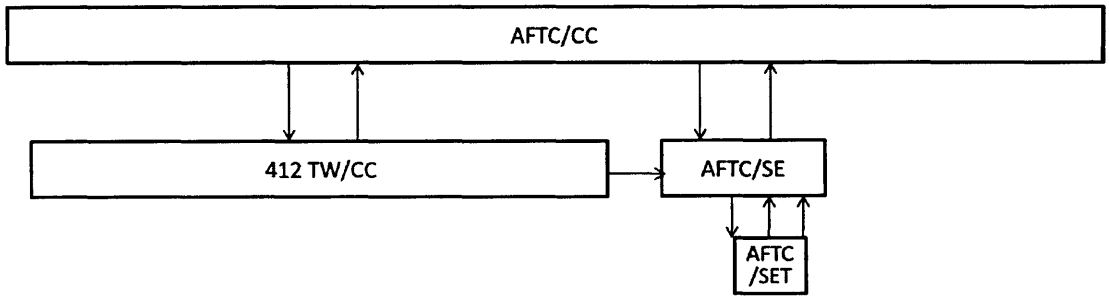

Figure 7: General Safety Policy and Safety Review Process Policy Control Structure

The approval process (Figure 8) is characterized by rigorous leadership oversight. A series of sequential control loops are established from the Unit/CC to the highest level of leadership at the AFTC. Each approver has the authority to stop the safety package from progressing to the next level review. At each control point, the safety package is reviewed and judged against a technical and administrative standard. The many control points permit many controllers to provide insights and concerns from their perspectives, thus ensuring a more complete assessment of safety planning.

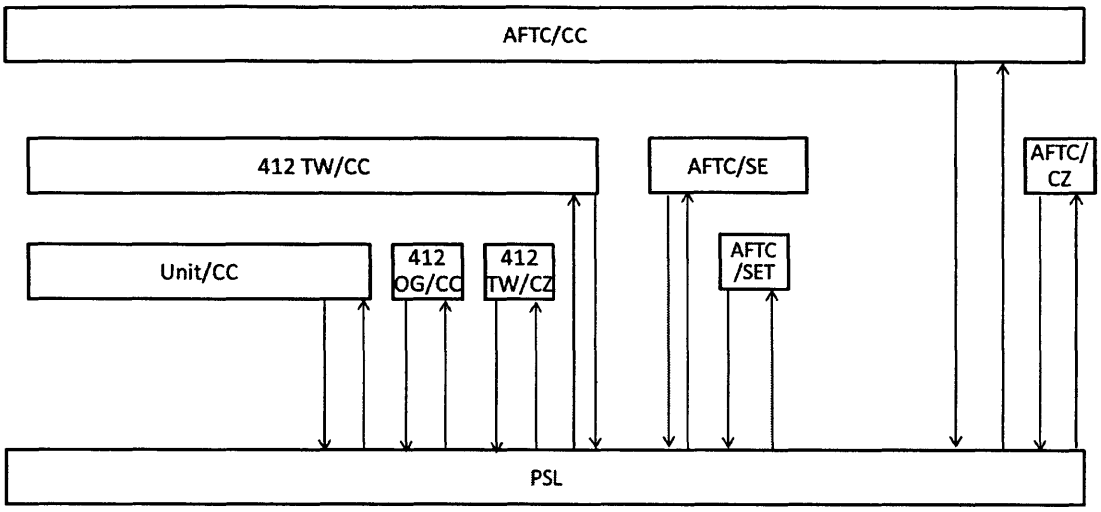

Figure 8: Approval Control Structure

The final safety review (Figure 9) provides an independent safety review of the planned testing. A key attribute of the safety review board is that none of the board members have a direct stake in the projects under review and therefore are not under program pressures. The independence helps the process and the board members avoid production pressures that have the potential to compromise safety. AFTC/SET plays a central role in ensuring the independence of the safety review by selecting independent technical experts and operations representatives, verifying the prerequisites for proceeding with the review are complete, and managing the conduct of the safety review board meeting. The safety review board meeting provides a forum for the test team and independent technical experts to perform a detailed and collaborative analysis of hazards.

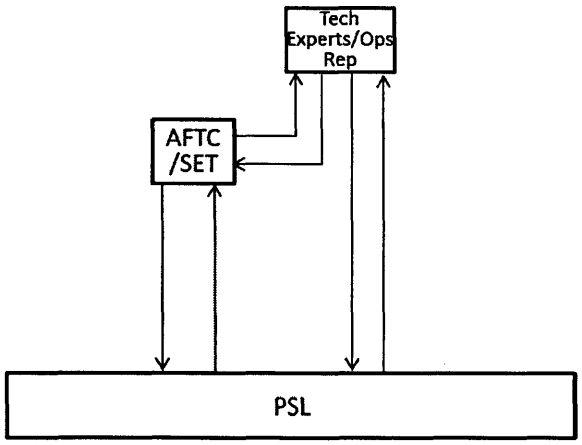

Figure 9: Final Safety Review Control Structure

The safety package preparation process (Figure 10) is conducted at each level of review from the unit level to senior leadership approvals. Each loop is established to allow the controllers to review planning for safety rigor, provide direction regarding safety planning, and to verify that issues are resolved. Because the control loops are executed in a specified and sequential order with the requirement to provide feedback and close action items before proceeding to the next review, the system is fairly robust. Each subsequent review provides a check of the prior reviewers in terms of technical rigor and policy compliance. If a reviewer is dissatisfied with the safety planning, approval to proceed is withheld until the issue is resolved. The deep involvement of leadership all the way to the AFTC/CC allows for clear communication and effective feedback channels because the PSL directly interacts with controllers at all levels.

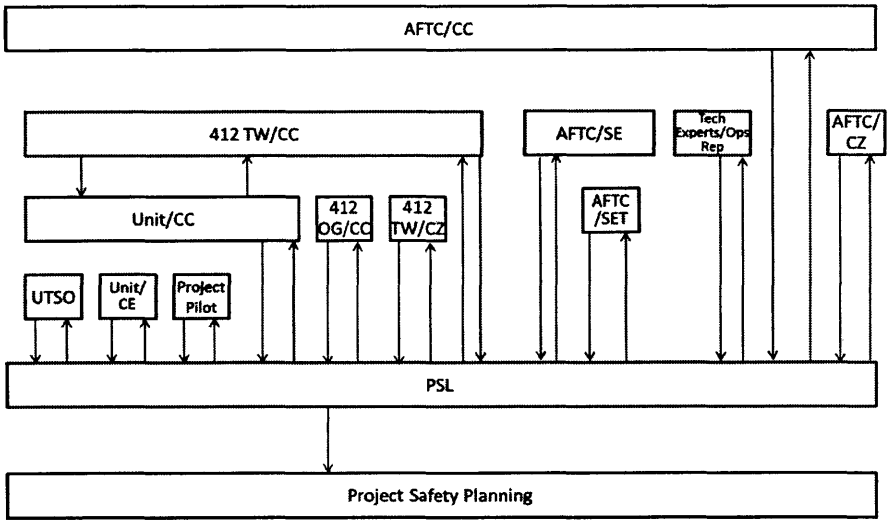

Figure 10: Safety Package Preparation Control Structure

The section of the control structure for project safety planning (Figure 11) shows a control loop between the KTR/Program Office and the PSL. The KTR/Program Office provides information regarding the system under test to the PSL for incorporation in the safety package. AFFTCI 91-105 does not specify requirements for the control relationship other than noting that information from the KTR/Program Office may be available and should be considered during the hazard analysis. The lack of a stringent requirement for KTR/Program Office information represents a possible weakness that is discussed later in this chapter. Between the PSL and the project safety planning process there is only a control channel and no monitoring channel. The PSL can make changes to project safety planning to incorporate inputs from each controller but cannot monitor the effectiveness of those changes during the safety review process.

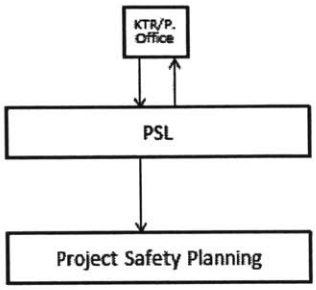

Figure 11: Project Safety Planning Control Structure

Safety Management System Requirements

STPA identified all of the AFFTCI 91-105 requirements that were within the scope of this analysis. A complete comparison of the AFFTCI 91-105 requirements with the STPA Step 1 derived component requirements was conducted and is presented in Appendix D. Several additional requirements regarding the assignment of responsibilities, policy establishment, and policy dissemination were also identified for AFTC/CC and 412 TW/CC though these may be captured in other policy documents. Far greater component requirement detail is provided in STPA Step 2, which identifies how each of the requirements can be violated. STPA Step 2 can be used to improve policies and provide guidance or training to controllers about potential safety constraint violations to assist with their decision-making process. The use of the contextual guidewords to analyze systemic factors provided insights and additional requirements regarding issues with broader impacts to safety control. The identified contextual factors within the system can be proactively managed and the effect from contextual factors outside of the system can be mitigated through improved policies and processes.

Findings and Areas for Further Investigation

From conducting STPA, a number of recurring themes were recognized and areas for further investigation and improvement were identified. They are described in this section along with high level recommendations.

Communication

Communication was regularly identified as an important issue that could compromise safety control, although the AFTC review process provides ample opportunities for controllers to communicate with the PSL. Communication for policy is essential for disseminating and implementing policies from the AFTC/CC down through the control hierarchy to the PSL. Feedback

is required to monitor compliance in each control loop and is also required to gain insight on how policies can be improved. AFFTCI 91-105 addresses the need for feedback by incorporating feedback loops between controllers and the PSL in the approval and safety package preparation phase. Furthermore, AFFTCI 91-105 specifies feedback channels between the PSL, UTSO, and AFTC/SET to allow for the transfer of lessons learned and suggested policy changes. While the structure of the AFTC safety review process facilitates communication, STPA showed that the serial review creates opportunities for unsafe control actions due to out of sequence inputs and reviews.

A more formal process for action item tracking and closure may be helpful in preventing changes to safety packages that are not reviewed by follow on reviewers. As identified in the analysis, ensuring that action items provided by each reviewer are addressed and closed before proceeding onto the next level review is crucial for safety control.

Resources and Pressures

Resources and pressures can affect all levels of the AFTC Safety Management System. Inadequate resources that result in limited personnel availability can degrade communication and enforcement of policy, the quality of feedback and reviews, and the rigor of project safety planning. The current Department of Defense fiscal environment will likely have an adverse impact to the availability of resources and is largely out of the control of AFTC leadership. External pressures such as requirements for shorter review cycles can also degrade the quality of reviews and project safety planning. At times, pressures to meet other requirements such as delivering technology rapidly to the field may merit the acceptance of increased risk. In situations where there are competing priorities, AFTC leadership determines which objective takes precedence.

Investigate changes to the safety process to improve efficiency and proactively reduce resource demands and schedule pressure. Improved hazard analysis techniques employed by the PSL combined with an alternative treatment for routine tests that do not qualify for a negligible risk review may provide opportunities for improved efficiency without adversely affecting safety control.

Safety Culture

Safety culture is a systemic factor that affects the way that personnel in all aspects of the AFTC Safety Management System view safety and participate in the safety review process. Approvers that do not enforce policies, have low standards for safety package quality, do not prioritize safety reviews, or do not accept safety related feedback can negatively affect safety culture. Subsequently, a poor safety culture can contribute to further lax safety control and inadequate communication.

The AFTC has a strong safety culture developed over a long history and AFTC leadership is effective at communicating a strong focus on safety.

AFTC leadership should continue to demonstrate a commitment to safety through rigorous enforcement of policies, high safety package standards, prioritization of safety reviews, and regular communication that highlights their position on safety.

Conflicts between Multiple Controllers

Potential conflicts were identified in two primary aspects of the AFTC Safety Management System. The first conflict is regarding the policy guidance to the 412 TW/CC from AFTC/CC and AFTC/SE. Because the 412 TW/CC receives guidance from both controllers, it is important that the information is either deconflicted or consistent. The AFTC deals with the potential conflict through coordination between AFTC/CC and AFTC/SE. AFFTCI 91-105 is currently maintained by AFTC/SE but any changes to the policy must be approved by the AFTC/CC. Requiring that AFTC/CC approve the document ensures that the policy guidance is consistent with the AFTC/CC's direction. The second potential conflict occurs during the serial review process. Action items provided by reviewers may cause changes to safety planning that invalidate prior reviewer reviews and result in the violation of safety constraints.

Consider the possibility of conducting reviews as board meetings rather than serially. For example, the UTSO, Project Pilot, and Unit/CE can comprise a lower level board to prepare the safety package prior to the Unit/CC approval. The safety review board meeting can remain the same. Then, another board meeting made up of senior leadership can be held to conduct the final approval. Meeting instead of using a serial review process will prevent issues that arise due to the timing of changes to the safety package. Board meetings may also expedite the safety review process by avoiding wasted time that occurs between each review due to other priorities and transfer overhead. Furthermore, meeting as a group may be more effective for safety review because it allows people with diverse viewpoints to collaborate.

Sequence

STPA Step 2 identified how out of sequence reviews can reduce the efficacy of the serial review process by allowing changes after subsequent reviewers have reviewed the safety package. In order to ensure that out of sequence reviews do not occur, AFFTCI 91-105 requires that action items be closed for each reviewer before proceeding to the next reviewer.

The AFFTCI 91-105 provides effective guidance to prevent out of sequence reviews though additional tools to track action items may be beneficial.

Monitoring Tools

Monitoring channels are incorporated during the safety package preparation, final safety review, and approval processes. Each individual reviewer receives direct insight with regards to the technical rigor and compliance of the safety planning and can provide feedback directly to the PSL or through the chain of command. In addition to the monitoring channels described by AFFTCI 91-105, additional monitoring may be beneficial.

Further investigation should be conducted to determine where additional monitoring tools and metrics can help provide controllers with key insights. Tools such as surveys or audits can be implemented as part of the review process to collect data on policy compliance and technical rigor. The information can be used to improve training and procedures. Data such as historical accident rates and corresponding risk levels may also be useful in determining whether policies have been effective or remain effective. Surveys, case studies, or timesheet analyses may be useful to measure the adequacy of resources.

Hazard Analysis Tools

To analyze hazards, AFFTCI 91-105 recommends that the test team consult the safety library to review safety planning from past tests, contact other testers with experience in similar testing, and conduct additional research. The test team is expected to apply critical thinking to identify potential safety constraint violations that may lead to accidents. Then, during the safety package review, the many layers of reviewers provide valuable additional perspectives and verification of the safety planning. While the current methods for hazard analysis may be effective, the assumption that past tests are representative of the system under test may not always hold true. Furthermore, in tests that are extremely complex, critical thinking may be inadequate on its own. More effective tools that can systematically consider potential violations of safety constraints will be needed.

Research should be conducted to seek out new methods for hazard analysis and determine in which cases they should be applied. The STPA technique may be an ideal candidate because it provides a systematic and versatile tool for analyzing system safety.

KTR/Program Office Involvement

The KTR/Program Office often has key technical insights because of its involvement in design and laboratory testing of the system under test. The AFFTCI 91-105 recommends that the PSL consider

safety assessments and other technical information from the KTR/Program Office. Collaboration often occurs between the two entities during the safety planning process, especially for high risk or high priority testing. However, there are no guidelines that define when the KTR/Program Office should provide key information and no requirement for the KTR/Program Office to verify that the safety package is consistent with its recommendations and restrictions. As identified in STPA Step 2, KTR/Program Office information that is provided must be correct, adequate, and timely to avoid unsafe control actions.

The KTR/Program Office should be included as a signatory early in the review process to indicate that it has provided a safety assessment and that the safety package is consistent with their recommendations.

Standards and Qualifications

The effectiveness of the safety review board is dependent on the quality of the safety package that is being reviewed, qualifications of the selected safety reviewers, and the accomplishment of the safety review board objectives. AFFTCI 91-105 provides clear safety package readiness criteria required for proceeding with the safety review board meeting and well-defined exit criteria. However, the document provides only vague guidelines regarding the qualifications for selectees. No specifics are provided regarding what constitutes sufficient experience participate as a reviewer. Because the guidelines are unclear, the review process may be compromised by choosing less experienced reviewers.

To assist with the selection of safety reviewers, a set of requirements describing experience levels should be developed to ensure that the reviewers have adequate subject matter knowledge to effectively review the safety package. The same set of requirements can also be used as a tool to identify and develop additional safety reviewers.

Waivers and Other Workarounds

As stated in AFFTCI 91-105, waivers and other workarounds may be approved by AFTC/CC and AFTC/SE. Non-standard procedures give AFTC leadership the ability to expedite processes in response to other priorities such as urgent warfighter needs. At the same time, by allowing non-standard procedures, leadership may be giving up safety rigor in favor of other priorities. The PSL and reviewers may also use informal workarounds to expedite the safety review process. One such example is the use of out-of-sequence reviews.

Formal alternative procedures should be used sparingly if at all because of negative effect they may have on the safety management system in the long run. To avoid making decisions under pressure, the types of waivers or alternative procedures with justifications for their use should be documented in advance. When such modifications are considered, leadership should establish criteria to define when the policy should revert back to standard procedures.

Feedback regarding unofficial workarounds should be collected and the workarounds assessed for risk. Policy should be updated to permit acceptable workarounds while controlling them to eliminate additional risk.

Risk Communication

Risk communication in the AFTC Safety Management System occurs in two primary ways. One is through the approval and safety package preparation processes. Through the direct reviews that comprise the processes, controllers gain first hand insights regarding the risk of the proposed tests. Reviewers can apply their intuition and experience to judge the risk level. The second way that risk communication occurs is through the safety memorandum provided by the safety review board following the safety review board meeting. As explained in AFFTCI 91-105, safety review board members consider the test hazard outcomes in terms of severity and probability. Accident severity can be assessed accurately as long as the accidents are understood because the value of the hardware and the people at risk are identifiable. However, determining the probability of accident occurrence for a complex system is difficult or impossible to calculate. AFFTCI 91-105 guidance acknowledges the difficulty and recommends that safety reviewers provide a subjective assessment of the mishap probability level instead. While the intuitive assignment of a mishap probability permits the use of the AFFTC Risk Assessment matrix, doing so does not make a lot of sense because the probability is often nothing more than a guess.

Investigate improved methods for risk communication that avoid misleading subjective probabilistic assessments. Instead of attempting to incorporate probability measures, perhaps a more appropriate method for assigning risk may be to merely allow safety reviewers to qualitatively determine the overall risk level without trying to explicitly assign a probability of occurrence. AFFTCI 91-105 provides a list of elevated risk activities that may merit a higher risk level. The combination of accident severity and the recognition that some test activities are inherently more risky may be sufficient for a risk assessment. Reviewers

can then provide justification for their recommendation in the final safety review memorandum.

Training

AFTC/SET and the PSL must each perform activities that have a major impact on safety control. AFTC/SET is responsible for selecting safety review board members, providing guidance during the safety review board meeting, and ensuring an independent safety review. The PSL is responsible for conducting hazard analysis which forms the basis of the entire safety review process. Current training is focused primarily on communicating policy requirements rather than hazard analysis techniques. Adequate training for AFTC/SET and PSL should be provided to enable them to successfully accomplish their responsibilities and enforce key safety constraints.

Training for AFTC/SET to manage the safety review process including the safety review board meeting should be reviewed for efficacy and improved as needed.

Hazard analysis training that provides engineers with knowledge about how to perform hazard analysis should be developed and provided.

CONCLUSION

The Air Force Test Center faces new challenges as it continues into the 21st century as the world's leader in developmental flight test. New technologies are becoming ever more sophisticated and less transparent, driving an increase in complexity for tests designed to evaluate them. This shift will place more demands on the AFTC Safety Management System to effectively analyze hazards and preempt the conditions that lead to accidents.

In order to determine whether the AFTC Safety Management System is prepared to handle new safety challenges, this thesis applied a systems-theoretic approach to analyze the safety review process. Specifically, the goals of this thesis were:

1. To perform a STPA on the AFTC Safety Management System and identify the features which contribute to its effectiveness.
2. To identify any gaps in the processes, roles, responsibilities, and tools.
3. To identify possible opportunities to improve the process.

The STPA performed in this thesis highlighted a number of key features of the AFTC Safety Management System that contribute to effective safety control. In particular, the current hierarchical control structure and well-designed policies were significant aspects that improved safety. Even so, STPA identified many potential safety constraint violations that could occur due to unsafe component interactions, systemic factors, or component failures. A comparison of the AFFTCI 91-105 policy document with the safety requirements identified by STPA showed that STPA identified all the requirements provided in AFFTCI 91-105 as well as a number of additional requirements. Moreover, the analysis of how the safety requirements could be violated provided valuable insights regarding opportunities where safety control could be improved. The STPA findings led to 13 recommendations for areas of further investigation and improvement. These recommendations focused not just on improving controls at the component level but also on component interactions and systemic factors.

Based on the analysis conducted, this thesis concludes:

- The AFTC should implement all 13 recommendations listed in Chapter 6 of this thesis to improve the AFTC Safety Management System.

- STPA is very effective for analyzing existing organizational processes and provides a comprehensive method for considering how safety constraints can be violated and how the violations can cause accidents.

APPENDIX A: DETAILED CONTROLLER MODELS

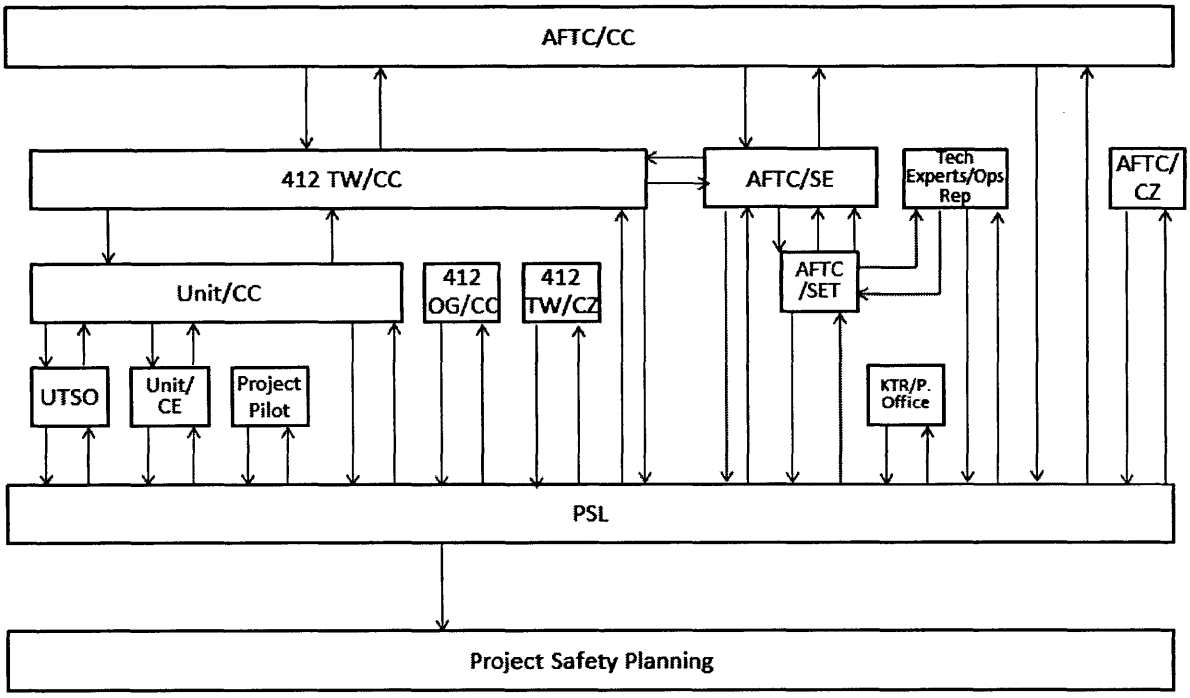

Figure 12: AFTC Safety Management System Control Loops

AFTC/CC – 412 TW/CC

Control Input (external command): AFMC policy guidance

Other Inputs (external info): Safety package reviews, emergency status of program

Feedback Inputs: Implementation status, Test Wing compliance with policy

Process Model: Implementing policy / Not implementing policy; Wavier justified / Not justified

Controller Algorithm: Policy implementation required; Wavier must be justified

Commands: Implement policy; Issue wavier

Actuator: 412 TW/CC

Controlled Process: Policy compliance from 412 TW/CC to Unit/CCs

Sensor: Perception (Informal feedback from 412 TW/CC)

412 TW/CC – Unit/CC

Control Input (external command): AFTC/CC and AFTC/SE policy guidance

Other Inputs (external info): Safety package reviews

Feedback Inputs: Implementation status, Test Unit compliance

Process Model: Implementing policy / Not implementing policy

Controller Algorithm: Policy implementation required

Commands: Implement policy

Actuator: Unit/CC

Controlled Process: Unit/CC provides policy guidance to UTSO, Unit/CE, Project Pilot, and PSL

Sensor: Perception (Informal feedback from Unit/CC)

Unit/CC – UTSO

Control Input (external command): 412 TW policy guidance

Other Inputs (external info): Safety package reviews

Feedback Inputs: Policy compliance and implementation by UTSO

Process Model: UTSO is or is not providing guidance that is consistent with 412 TW policy guidance

Controller Algorithm: Policy compliance required

Commands: Provide guidance; Require training

Actuator: UTSO

Controlled Process: Safety planning format and content verification

Sensor: Perception (Informal feedback)

Unit/CC – Unit/CE

Control Input (external command): 412 TW policy guidance

Other Inputs (external info): Test program requirements, Safety package reviews

Feedback Inputs: Policy compliance from engineering

Process Model: Engineering is or is not compliant with 412 TW policy guidance

Controller Algorithm: Policy compliance required

Commands: Provide policy guidance

Actuator: Unit/CE

Controlled Process: Engineering compliance with 412 TW policies

Sensor: Perception (Informal feedback)

UTSO – PSL

Control Input (external command): AFTC/SE policy guidance

Other Inputs (external info):

Feedback Inputs: Safety package quality, Lessons learned; Training status

Process Model: Safety package is formatted correctly? Safety package is compliant with latest policies?; Is PSL current with training?

Controller Algorithm: Formatting per guidance and compliance required; Training required

Commands: Approve; Return with Actions; Recommend training

Actuator: PSL

Controlled Process: Safety planning formatting and policy compliance; safety training

Sensor: Perception (Safety package review)

Unit/CE – PSL
Control Input (external command):

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Quality required

Commands: Approve; Return with Actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

Project Pilot – PSL
Control Input (external command): none

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with Actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

Unit/CC – PSL
Control Input (external command): 412 TW policy guidance

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package compliance, quality, risks, objectives, test execution results

Process Model: Safety package compliant with policies? Safety package sufficiently reduces risk?

Controller Algorithm: Compliance, quality, and benefits outweigh risks required

Commands: Approve; Return with actions; Rescind approval to execute

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

412 OG/CC – PSL

Control Input (external command): none

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with Actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

412 TW/CZ – PSL

Control Input (external command): none

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with Actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

412 TW/CC – PSL

Control Input (external command): AFTC/CC and AFTC/SE Policy guidance

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package compliance and quality

Process Model: Safety package compliant with policies? Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

AFTC/CC – AFTC/SE

Control Input (external command): AFMC policy guidance

Other Inputs (external info): Safety package reviews, emergency status of project

Feedback Inputs: Implementation status, Policy documents consistent with AFMC policy?

Process Model: Implementing policy / Not implementing policy ; Wavier justified / Not justified

Controller Algorithm: Policy implementation required; Wavier must be justified

Commands: Implement policy; Issue wavier

Actuator: AFTC/SE

Controlled Process: AFTC/SE issues local policies to 412 TW/CC in accordance to AFMC policy or AFTC/CC direction

Sensor: Perception (Review policy, informal feedback)

AFTC/SE – 412 TW/CC

Control Input (external command): AFTC/CC policy guidance

Other Inputs (external info): Lessons learned from AFTC/SET, Safety package reviews

Feedback Inputs: Policy implementation by 412 TW

Process Model: 412 TW/CC is compliant or not with issued AFTC/SE policies

Controller Algorithm: Policy compliance required

Commands: Issue policy

Actuator: 412 TW/CC

Controlled Process: 412 TW/CC provides policy requirements for Test Wing

Sensor: Perception (Informal feedback)

AFTC/SE – PSL

Control Input (external command): AFTC/CC policy guidance

Other Inputs (external info): AFTC/SET lessons learned, Personal experience

Feedback Inputs: Safety package compliance and quality

Process Model: AFTC/SET and 412 TW/CC are compliant with issued AFTC/SE policies which results in PSL complaint in AFTC/SE policies

Controller Algorithm: Policy compliance required

Commands: Approve; Return with actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

AFTC/SE – AFTC/SET

Control Input (external command): AFTC/CC policy guidance

Other Inputs (external info): Safety package reviews

Feedback Inputs: Policy implemented by AFTC/SET, Lessons learned from AFTC/SET

Process Model: AFTC/SET is compliant or not with issued AFTC/SE policies

Controller Algorithm: Policy compliance required

Commands: Issue policy, provide guidance

Actuator: AFTC/SET

Controlled Process: Safety process implementation

Sensor: Perception (Informal feedback)

AFTC/SET – AFTC/SE

Control Input (external command): Tech Experts/Ops Reps assessment

Other Inputs (external info):

Feedback Inputs:

Process Model: Safety package risk level

Controller Algorithm: Risk assessment required

Commands: Recommend overall risk level

Actuator: AFTC/SE

Controlled Process: Risk communication to AFTC/CC, 412 TW/CC, and 412 OG/CC

Sensor:

AFTC/SET – PSL

Control Input (external command): AFTC/CC and AFTC/SE policy guidance

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package compliance and quality

Process Model: Safety package compliant with policies? Safety package meets required prerequisites for Safety Review Board? Safety package sufficiently reduces risk?

Controller Algorithm: Compliance, prerequisites, and quality required

Commands: Allow to proceed with Safety Review Board, Approve; Return with actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review, Safety Review Board meeting)

AFTC/SET – Tech Experts/Ops Reps

Control Input (external command): AFTC/CC and AFTC/SE policy guidance

Other Inputs (external info): Personal experience

Feedback Inputs: Safety Review Board meeting conduct

Process Model: Discussion satisfies or doesn't satisfy independent safety review requirement; Safety Review Board member is or is not qualified

Controller Algorithm: Independent safety review is required; Qualified Safety Review Board members are required

Commands: Safety Review Board meeting guidance, Safety Review Board selection

Actuator: Tech Experts/Ops Reps

Controlled Process: Independent safety review, quality of review

Sensor: Perception (Safety Review Board meeting)

Tech Experts/Ops Reps – AFTC/SET

Control Input (external command):

Other Inputs (external info): Personal experience, AFTC policy guidance

Feedback Inputs: Safety package likelihood and severity description in risk assessment memo

Process Model: Planned testing is high, medium, or low risk

Controller Algorithm: Risk assessment required

Commands: Recommend overall risk level

Actuator: AFTC/SET

Controlled Process: Risk assessment

Sensor: Perception (Risk assessment memo)

Tech Experts/Ops Reps – PSL

Control Input (external command):

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Quality required

Commands: Approve; Return with actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review, Safety Review Board meeting)

KTR / Program Office – PSL Hazard Analysis

Control Input (external command): Program objectives, Safety requirements

Other Inputs (external info): Technical expertise

Feedback Inputs: Safety package compliance with safety release, hazard assessment, or recommendations and compliance with advised safety constraints

Process Model: System safe under planned conditions?

Controller Algorithm: Safety required

Commands: Provide safety release recommendations or safety assessment

Actuator: PSL

Controlled Process: Hazard analysis

Sensor: Perception (Safety package review, Safety Review Board meeting)

AFTC/CC – PSL

Control Input (external command): External safety policy (AFMC/SE, AFMC/A3)

Other Inputs (external info): AFTC/SE policies, Personal experience

Feedback Inputs: Safety package compliance and quality

Process Model: Safety package compliant with policies? Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

AFTC/CZ – PSL

Control Input (external command): none

Other Inputs (external info): Personal experience

Feedback Inputs: Safety package quality

Process Model: Safety package sufficiently reduces risk?

Controller Algorithm: Compliance and quality required

Commands: Approve; Return with Actions

Actuator: PSL

Controlled Process: Safety planning

Sensor: Perception (Safety package review)

PSL – Hazard Analysis

Control Input (external command): none

Other Inputs (external info): Safety library, opinions from other engineers, technical experience

Feedback Inputs: Test results from past testing

Process Model: Historical data and critical thinking identify potential safety constraint violations

Controller Algorithm: Safety constraints and how they might be violated must be identified

Commands: Identify and analyze potential safety constraint violations

Actuator: PSL

Controlled Process: Hazard analysis

Sensor: Perception of similarity with past tests, safety of past tests

APPENDIX B: STPA STEP 1 UNSAFE CONTROL ACTION ANALYSIS

Hazards:
H1. The test team does not identify test hazards that will lead to an accident.
H2. The test team prescribes erroneous mitigation measures that will lead to an accident.
H3. Reviewers and approvers accept tests with risks that have not been adequately mitigated or understood.

Controller	Control Action	Not Providing CA Causes Hazard	Providing CA Causes Hazard	Wrong Timing/Order of CA Causes Hazard	CA Stopped Too Soon/Applied Too Long
AFTC/CC	Implement policy (412 TW/CC)	Policy for safety risk mitigation and acceptance is not provided to 412 TW/CC - subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable risks (H1, H2, H3)	Inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC - subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable risks (H1, H2, H3)	n/a	Existing policy becomes obsolete - A policy may become inadequate because of changes in the operating context and test teams may not identify potential violations of safety constraints (H1, H3)

AFTC/CC	Issue Waiver (412 TW/CC)	n/a	Waiver that violates safety constraints is issued - Hazards may not be adequately controlled (H1, H2, H3)	n/a	n/a
412 TW/CC	Implement policy (Unit/CC)	Policy for safety risk mitigation and acceptance is not provided to Unit/CC - PSL inadequately identifies / mitigates potential violations of safety constraints and performs tests with unacceptable risks (H1, H2, H3)	Inadequate policy for safety risk mitigation and acceptance is provided to Unit/CC - PSL inadequately identifies / mitigates potential violations of safety constraints and performs tests with unacceptable risks (H1, H2, H3)	n/a	Existing policy becomes obsolete - A policy may become inadequate because of changes in the operating context and test teams may not identify potential violations of safety constraints (H1, H3)

Unit/CE	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	n/a	n/a
Unit/CE	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can	n/a

				lead to executing unsafe tests (H1, H2, H3)	
Project Pilot	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	n/a	n/a

Project Pilot	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a
Unit/CC	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points	n/a	Approval not rescinded - If a test has an "unexpected test result" but the Unit/CC does not rescind approval to test, this can lead to executing unsafe tests

			can lead to executing unsafe tests (H3)		(H3)
Unit/CC	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a

412 OG/CC	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	Approval provided before prior reviewer feedback incorporated - Providing approval before safety related feedback from other reviewers has been incorporated can lead to executing unsafe tests (H3)	n/a
412 OG/CC	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers	n/a

			(H1, H2, H3)	provide feedback can lead to executing unsafe tests (H1, H2, H3)	
412 TW/CZ	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	n/a	n/a

412 TW/CZ	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a
412 TW/CC	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points	Approval provided before prior reviewer feedback incorporated - Providing approval before safety related feedback from other reviewers has	n/a

			can lead to executing unsafe tests (H3)	been incorporated can lead to executing unsafe tests (H3)	
412 TW/CC	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a

AFTC/CC	Implement policy (AFTC/SE)	Policy for safety risk mitigation and acceptance is not provided to AFTC/SE - AFTC/SE doesn't issue local policy consistent with AFMC to 412 TW so subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable risks (H1, H2, H3)	Inadequate policy for safety risk mitigation and acceptance is provided to AFTC/SE inadequate local policies are issued as a result - subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable risks (H1, H2, H3)	n/a	Existing policy becomes obsolete - A policy may become inadequate but AFTC/SE is not notified to update local policies because of changes in the operating context and test teams may not identify potential violations of safety constraints (H1, H3)

AFTC/CC	Issue Waiver (AFTC/SE)	n/a	Waiver that violates safety constraints is issued - Hazards may not be adequately controlled (H1, H2, H3)	n/a	n/a
AFTC/SE	Issue policy (412 TW/CC)	Policy for safety risk mitigation and acceptance is not provided to 412 TW/CC - subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable	Inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC - subordinate units inadequately identify / mitigate potential violations of safety constraints and perform tests with unacceptable	n/a	Existing policy becomes obsolete - A policy may become inadequate because of changes in the operating context and test teams may not identify potential violations of safety constraints (H1, H3)

		risks (H1, H2, H3)	risks (H1, H2, H3)		
AFTC/SE	Approve safety package (PSL)	n/a	Unjustified approval for safety package - Approval for the safety package indicating that the required safety planning and independent safety review were conducted when it wasn't actually could lead to inadequately	n/a	n/a

			identified / mitigated potential violations of safety constraints and the execution of tests with unacceptable risks (H3)		
AFTC/SE	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can	n/a

				lead to executing unsafe tests (H1, H2, H3)	
AFTC/SE	Issue policy (AFTC/SET)	Policy for safety risk mitigation and acceptance is not provided to AFTC/SET - AFTC/SET does not provide guidance to subordinate units which leads to inadequately identified / mitigated potential violations of safety constraints and tests with	Inadequate policy for safety risk mitigation and acceptance is provided to AFTC/SET - AFTC/SET provides guidance to subordinate units which leads to inadequately identified / mitigated potential violations of safety constraints and tests with	n/a	Existing policy becomes obsolete - A policy may become inadequate because of changes in the operating context and test teams may not identify potential violations of safety constraints (H1, H3)

		unacceptable risks executed (H1, H2, H3)	unacceptable risks executed (H1, H2, H3)		
AFTC/SE	Provide modified policy guidance (AFTC/SET)	n/a	Modified policy guidance that weakens the safety process is provided to AFTC/SET - AFTC/SET provides incorrect guidance to subordinate units which leads to inadequately identified / mitigated potential	n/a	Modified policy guidance issued and not rescinded - Policy guidance that weakens the safety process may be applied for longer than justified resulting in violations of safety constraints (H1, H2, H3)

			violations of safety constraints and tests with unacceptable risks executed (H1, H2, H3)		
AFTC/SET	Recommend overall risk level (AFTC/SE)	n/a	Understated risk assessment provided to leadership - Providing an understated risk level assessment reduces the level of scrutiny and increases the likelihood that test points that may violate	n/a	n/a

			safety constraints are overlooked (H3)		
AFTC/SET	Allow to proceed with Safety Review Board (PSL)	n/a	n/a	Safety Review Board conducted too early - Proceeding with the Safety Review Board before the Project Pilot, Unit/CE, or Unit/CC has reviewed the safety package could result in change inputs from them that may lead to violation of safety constraints (H1, H2, H3)	n/a

AFTC/SET	Approve safety package (PSL)	n/a	Unjustified approval for safety package - Approval for the safety package indicating that the required safety planning and independent safety review were conducted when they weren't could lead to inadequately identified / mitigated potential violations of safety constraints and the execution of tests with unacceptable risks (H1, H2, H3)	n/a	n/a

AFTC/SET	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a
AFTC/SET	Provide safety review board meeting guidance (Tech Experts/Ops Reps)	Safety review board meeting guidance not provided - Not providing guidance may result in a less effective safety review board	Safety review board meeting guidance provided detracts from a focus on safety - Focus in meeting is diverted to non-safety related	n/a	Safety review board meeting guidance is not applied throughout meeting - AFTC/SET loss of control of meeting allows meeting focus to be diverted and safety

		meeting due to lack of focus and result in overlooking test points that may cause a safety constraint violation (H1, H2, H3)	issues and safety constraint violations are overlooked (H1, H2, H3)		constraint violations are overlooked (H1, H2, H3)
AFTC/SET	Select safety board review members (PSL)	n/a	Inadequately qualified safety review board members selected- this would limit the effectiveness of the safety review to identify and control safety constraint violations in test points (H1, H2, H3)	n/a	n/a

Tech Experts/Ops Reps	Recommend overall risk level (AFTC/SET)	n/a	Understated risk assessment provided to AFTC/SET - Providing an understated risk level assessment reduces the level of scrutiny and increases the likelihood that test points that may violate safety constraints are overlooked (H3)	n/a	n/a
Tech Experts/Ops Reps	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there	n/a	n/a

			are unsafe test points can lead to executing unsafe tests (H3)		
Tech Experts/Ops Reps	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided after follow-on reviewers - Providing feedback that leads to unsafe test points after follow-on reviewers provide feedback can lead to executing unsafe tests (H1, H2, H3)	n/a

KTR / Program Office	Provide safety release (PSL)	Safe test conditions not provided - Test points that violate safety constraints are overlooked. (H1, H2, H3)	Unsafe test conditions provided - Test points incorporated into the safety package that violate safety constraints (H1, H2, H3)	n/a	n/a
KTR / Program Office	Provide safety assessment recommendations (PSL)	Safety assessment not provided - Test points that violate safety constraints are overlooked. (H1, H2, H3)	Incorrect safety assessment provided - Test points that violate safety constraints are overlooked. (H1, H2, H3)	Safety assessment provided late in or after review process - reviewers may not review or adequately consider hazard assessments which may allow test points with safety constraint violations to be overlooked (H1, H2, H3)	n/a

AFTC/CC	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	Approval provided before prior reviewer feedback incorporated - Providing approval before safety related feedback from other reviewers has been incorporated can lead to executing unsafe tests (H3)	n/a
AFTC/CC	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests	n/a	n/a

			(H1, H2, H3)		
AFTC/CZ	Approve safety package (PSL)	n/a	Approval provided without providing feedback or verified closure of action items - Providing approval when there are unsafe test points can lead to executing unsafe tests (H3)	n/a	n/a

AFTC/CZ	Return safety package with actions (PSL)	Action items not provided - Not providing feedback when there are unsafe test points can lead to executing unsafe tests (H1, H2, H3)	Action items that lead to the violation of safety constraints are provided - Providing feedback that leads to unsafe test points can lead to executing unsafe tests (H1, H2, H3)	n/a	n/a
PSL	Analyze and mitigate potential safety constraint violations (Hazard analysis)	Potential safety constraint violations not analyzed and mitigated - Not analyzing and mitigating safety constraint violations can lead to executing unsafe tests. (H1, H2, H3)	Incorrect analysis or mitigation of potential safety constraint violations provided - Providing an incorrect analysis or mitigation of potential safety constraint violations can lead to executing	n/a	n/a

			unsafe tests. (H1, H2, H3)		

APPENDIX C: STPA STEP 2 CAUSES OF UNSAFE CONTROL ACTIONS

STPA STEP 2 FOR THE AFTC SAFETY MANAGEMENT SYSTEM

SAFETY POLICY

AFTC/CC

Unsafe Control Action for AFTC/CC: Policy for safety risk mitigation and acceptance is not provided to 412 TW/CC. (CA: Implement Policy)

Controlled Process: Policy implementation by 412 TW/CC

Scenario 1: AFTC/CC does not receive or receives wrong policy information from AFMC.

a. Updated policy information from AFMC not passed through an effective communication channel to AFTC/CC.

Scenario 2: AFTC/CC does not enforce policy compliance by 412 TW/CC.

a. AFTC/CC chooses other priorities over enforcing safety policy and does not adequately control safety implementation by 412 TW/CC.

Scenario 3: AFTC/CC is unaware of policy noncompliance by 412 TW/CC.

a. AFTC/CC does not perceive policy compliance from 412 TW/CC accurately, causing AFTC/CC to assume compliance.
b. AFTC/CC does not receive information from 412 TW/CC about policy compliance, causing AFTC/CC to assume compliance.
c. AFTC/CC misinterprets feedback from 412 TW/CC and incorrectly assumes policy compliance.

Scenario 4: AFTC/CC policy implementation is not adequately enacted by 412 TW/CC.

a. 412 TW/CC does not receive policy information from AFTC/CC.
b. 412 TW/CC is not directed to enact policy for the safety review process.
c. 412 TW/CC does not enact policy for the safety review process.

Unsafe Control Action for AFTC/CC: Inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC. (CA: Implement Policy)

Controlled Process: Policy implementation by 412 TW/CC

Scenario 1: AFTC/CC does not receive adequate policy information from AFMC.

a. AFMC provided policy information is incomplete or incompatible with AFTC organization or operations.

Scenario 2: AFTC/CC enforces inadequate policy for safety risk mitigation and acceptance from 412 TW/CC.

a. AFTC/CC requires 412 TW/CC to comply with inadequate policies for safety risk mitigation and acceptance.

Scenario 3: AFTC/CC assumes that inadequate policies for 412 TW/CC are adequate.

a. 412 TW/CC does not provide adequate feedback about the effectiveness or compatibility of policies to AFTC/CC, causing AFTC/CC to incorrectly assume policies are adequate.
b. 412 TW/CC provides incorrect feedback about the effectiveness or compatibility of policies to AFTC/CC, causing AFTC/CC to incorrectly assume policies are adequate.
c. AFTC/CC misinterprets feedback about the effectiveness or compatibility of policies from 412 TW/CC and assumes that policies are adequate.

Scenario 4: 412 TW/CC enacts inadequate policy for safety risk mitigation and acceptance.

a. 412 TW/CC is commanded to implement inadequate policies from AFTC/CC.
b. 412 TW/CC is commanded to implement inadequate policies from AFTC/SE.
c. 412 TW/CC ignores AFTC/CC and AFTC/SE policies and enacts inadequate policies.

Unsafe Control Action for AFTC/CC: Existing policy to 412 TW/CC becomes obsolete. (CA: Implement Policy)

Controlled Process: Policy implementation by 412 TW/CC

Scenario 1: AFTC/CC does not receive updated policy information from AFMC.

a. Updated policy information from AFMC not passed through effective communication channel to AFTC/CC.

Scenario 2: AFTC/CC does not enforce updated policy compliance from 412 TW/CC

a. AFTC/CC neglects to update policies for 412 TW/CC due to other priorities.

Scenario 3: AFTC/CC assumes that 412 TW/CC is following updated policies when 412 TW/CC is not.

a. 412 TW/CC does not provide adequate feedback about the currency of policies to AFTC/CC, causing AFTC/CC to assume currency.
b. 412 TW/CC provides incorrect feedback about the currency of policies to AFTC/CC, causing AFTC/CC to assume currency.
c. AFTC/CC misinterprets feedback about the currency of policies that 412 TW/CC is using and believes that 412 TW/CC is using current policies when it is not.

Scenario 4: 412 TW/CC continues to enact obsolete policies.

a. 412 TW/CC does not receive commands to enact new policies from AFTC/CC.
b. 412 TW/CC does not receive commands to enact new policies from AFTC/SE.
c. 412 TW/CC misses commands to enact new policies from AFTC/CC.
d. 412 TW/CC misses commands to enact new policies from AFTC/SE.
e. 412 TW/CC receives conflicting commands from AFTC/CC and AFTC/SE about which policies to enact.
f. 412 TW/CC ignores commands to enact updated policies.

Unsafe Control Action for AFTC/CC: Policy for safety risk mitigation and acceptance is not provided to AFTC/SE. (CA: Implement Policy)

Controlled Process: Policy implementation by AFTC/SE

Scenario 1: AFTC/CC does not receive or receives wrong policy information from AFMC.

a. Updated policy information from AFMC not passed through effective communication channel to AFTC/CC.
b. Updated policy information from AFMC does not mitigate safety risk or permits unacceptable risk acceptance.

Scenario 2: AFTC/CC does not enforce policy compliance by AFTC/SE.

a. AFTC/CC chooses other priorities over enforcing safety policy and does not adequately control safety implementation by AFTC/SE.

Scenario 3: AFTC/CC is unaware of policy noncompliance by AFTC/SE

a. AFTC/CC does not perceive policy compliance from AFTC/SE accurately, causing AFTC/CC to assume compliance.
b. AFTC/CC does not receive information from AFTC/SE about policy compliance, causing AFTC/CC to assume compliance.
c. AFTC/CC misinterprets feedback from AFTC/SE and incorrectly assumes policy compliance.

Scenario 4: AFTC/CC policy implementation is not adequately enacted by AFTC/SE.

a. AFTC/SE does not receive policy information from AFTC/CC.
b. AFTC/SE is not directed to enact policy in the safety review process.
c. AFTC/SE does not enact policy within the safety review process

Unsafe Control Action for AFTC/CC: Inadequate policy for safety risk mitigation and acceptance is provided to AFTC/SE. (CA: Implement Policy)

Controlled Process: Policy implementation by AFTC/SE

Scenario 1: AFTC/CC does not receive adequate policy information from AFMC.

a. AFMC provided policy information is incomplete or incompatible with AFTC organization or operations.

Scenario 2: AFTC/CC enforces inadequate policy for safety risk mitigation and acceptance from AFTC/SE.

a. AFTC/CC requires AFTC/SE to comply with inadequate policies for safety risk mitigation and acceptance.

Scenario 3: AFTC/CC assumes that inadequate policies for AFTC/SE are adequate.

a. AFTC/SE does not provide adequate feedback about the effectiveness or compatibility of policies to AFTC/CC, causing AFTC/CC to incorrectly assume policies are adequate.
b. AFTC/SE provides incorrect feedback about the effectiveness or compatibility of policies to AFTC/CC, causing AFTC/CC to incorrectly assume policies are adequate.
c. AFTC/CC misinterprets feedback about the effectiveness or compatibility of policies from AFTC/SE and assumes that policies are adequate.

Scenario 4: AFTC/SE enacts inadequate policy for safety risk mitigation and acceptance.

a. AFTC/SE is commanded to implement inadequate policies from AFTC/CC.
b. AFTC/SE ignores AFTC/CC policies and enacts inadequate policies.

Unsafe Control Action for AFTC/CC: Existing policy to AFTC/SE becomes obsolete. (CA: Implement Policy)

Controlled Process: Policy implementation by AFTC/SE

Scenario 1: AFTC/CC does not receive updated policy information from AFMC.

a. Updated policy information from AFMC not passed through effective communication channel to AFTC/CC.

Scenario 2: AFTC/CC does not enforce updated policy compliance from AFTC/SE

a. AFTC/CC neglects to update policies for AFTC/SE due to other priorities.

Scenario 3: AFTC/CC assumes that AFTC/SE is following updated policies when AFTC/SE is not.

a. AFTC/SE does not provide adequate feedback about the currency of policies to AFTC/CC, causing AFTC/CC to assume currency.
b. AFTC/SE provides incorrect feedback about the currency of policies to AFTC/CC, causing AFTC/CC to assume currency.

c. AFTC/CC misinterprets feedback about the currency of policies that AFTC/SE is using and believes that AFTC/SE is using current policies when it is not.

Scenario 4: AFTC/SE continues to enact obsolete policies.

a. AFTC/SE does not receive commands to enact new policies from AFTC/CC.
b. AFTC/SE misses commands to enact new policies from AFTC/CC.
c. AFTC/SE ignores commands to enact updated policies.

CONTEXTUAL FACTORS AFFECTING POLICY

History: Perceived safety success may lead to a lack of attention and application of resources by AFTC/CC, AFTC/SE, and 412 TW/CC toward reviewing, updating, and enforcing safety policies.

Resources: Inadequate time or staff may limit the AFTC/CC's ability to command and monitor the 412 TW/CC and AFTC/SE implementation of safety policies. The lack of resources may also make it difficult for AFTC/CC to reevaluate and update policies. A lack of resources may result in ineffective feedback provided by AFTC/SE and 412 TW/CC to AFTC/CC or AFTC/CC to AFMC as well.

Tools and Interface: If AFTC/CC does not have effective auditing tools to verify the implementation of safety policy, AFTC/CC may miss indicators that a greater emphasis on safety policy compliance is needed. The lack of tools to measure the effectiveness of safety policy may cause AFTC/CC, AFTC/SE, and 412 TW/CC to miss indicators that safety policy should be updated.

Pressures: Leadership's attention on managing political concerns may reduce their focus on monitoring, enforcing, and updating safety policy.

Safety Culture: A weak safety culture may lead 412 TW/CC and AFTC/SE to not prioritize the implementation of policies consistent with AFTC/CC expectations. AFTC/CC may not enforce safety policy implementation rigorously.

Communication: Lack of communication will limit AFTC/CC's ability to monitor, enforce, and update policy. It will also limit 412 TW/CC and AFTC/SE's ability to feedback information to AFTC/CC. Coordination issues may also arise because 412 TW/CC receives direction from both AFTC/CC and AFTC/SE. If AFTC/CC and AFTC/SE do not coordinate policy direction, conflicting information may be provided to 412 TW/CC.

SAFETY REVIEW PROCESS POLICY

AFTC/CC

Unsafe Control Action for AFTC/CC: Waiver that violates safety constraints is issued to 412 TW/CC. (CA: Issue Waiver)

Controlled Process: Safety process implementation by 412 TW/CC

Scenario 1: External forces drive AFTC/CC to issue waiver that violates safety constraints.

a. Pressure to field system under test drives AFTC/CC to issue waiver that allows the violation of safety constraints.

Scenario 2: AFTC/CC issues waiver that violates safety constraints.

a. AFTC/CC issues waiver that allows the violation of safety constraints to prioritize other goals over safety.

Scenario 3: AFTC/CC assumes that benefits of issuing waiver outweigh the risks.

a. 412 TW provides no feedback about adverse impacts from issuing a waiver to the safety process, causing AFTC/CC to assume that little or no additional risk is incurred.
b. 412 TW provides incorrect feedback about the adverse impacts from issuing a waiver to the safety process, causing AFTC/CC to assume that little or no additional risk is incurred.
c. AFTC/CC misinterprets feedback about issuing a waiver to the safety process and assumes little or no additional risk is incurred.

Scenario 4: 412 TW/CC operates under a waiver that allows the violation of safety constraints.

a. 412 TW/CC allows units to perform planning and test execution under a waiver that allows the violation of safety constraints.

Unsafe Control Action for AFTC/CC: Waiver that violates safety constraints is issued to AFTC/SE. (CA: Issue Waiver)

Controlled Process: Safety process implementation by AFTC/SE

Scenario 1: External forces drive AFTC/CC to issue waiver that violates safety constraints.

a. Pressure to field system under test drives AFTC/CC to issue waiver that allows the violation of safety constraints.

Scenario 2: AFTC/CC issues waiver that violates safety constraints.

a. AFTC/CC issues waiver that allows the violation of safety constraints to prioritize other goals over safety.

Scenario 3: AFTC/CC assumes that benefits of issuing waiver outweigh the risks.

a. AFTC/SE provides no feedback about adverse impacts from issuing a waiver to the safety process, causing AFTC/CC to assume that little or no additional risk is incurred.
b. AFTC/SE provides incorrect feedback about the adverse impacts from issuing a waiver to the safety process, causing AFTC/CC to assume that little or no additional risk is incurred.
c. AFTC/CC misinterprets feedback about issuing a waiver to the safety process and assumes little or no additional risk is incurred.

Scenario 4: AFTC/SE operates under a waiver that allows the violation of safety constraints.

a. AFTC/SE allows units to perform test planning under a waiver that allows the violation of safety constraints.

AFTC/SE

Unsafe Control Action for AFTC/SE: Policy for safety risk mitigation and acceptance is not provided to 412 TW/CC. (CA: Issue Policy)

Controlled Process: Safety process implemented by 412 TW/CC

Scenario 1: AFTC/SE does not receive or receives wrong policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.

b. Updated policy information from AFTC/CC does not mitigate safety risk or permits unacceptable risk acceptance.

Scenario 2: AFTC/SE does not enforce policy compliance by 412 TW/CC.

a. AFTC/SE chooses other priorities over enforcing safety policy and does not adequately control safety implementation by 412 TW/CC.

Scenario 3: AFTC/SE is unaware of policy noncompliance by 412 TW/CC.

a. AFTC/SE does not perceive policy compliance from 412 TW/CC accurately, causing AFTC/SE to assume compliance.
b. AFTC/SE does not receive information from 412 TW/CC about policy compliance, causing AFTC/SE to assume compliance.
c. AFTC/SE misinterprets feedback from 412 TW/CC and incorrectly assumes policy compliance.

Scenario 4: AFTC/SE policy implementation is not enacted by 412 TW/CC.

a. 412 TW/CC does not receive policy information from AFTC/SE.
b. 412 TW/CC is not directed to enact policy within the 412 TW.
c. 412 TW/CC does not enact policy within the 412 TW.

Unsafe Control Action for AFTC/SE: Inadequate policy for safety risk mitigation and acceptance is provided to 412 TW/CC. (CA: Issue Policy)

Controlled Process: Safety process implemented by 412 TW/CC

Scenario 1: AFTC/SE does not receive adequate policy information from AFTC/CC.

a. AFTC/CC provided policy information is incomplete or incompatible with 412 TW organization or operations.

Scenario 2: AFTC/SE enforces inadequate policy for safety risk mitigation and acceptance from 412 TW/CC.

a. AFTC/SE requires 412 TW/CC to comply with inadequate policies for safety risk mitigation and acceptance.

Scenario 3: AFTC/SE assumes that inadequate policies for 412 TW/CC are adequate.

a. 412 TW/CC does not provide adequate feedback about the effectiveness or compatibility of policies to AFTC/SE, causing AFTC/SE to incorrectly assume policies are adequate.
b. 412 TW/CC provides incorrect feedback about the effectiveness or compatibility of policies to AFTC/SE, causing AFTC/SE to incorrectly assume policies are adequate.
c. AFTC/SE misinterprets feedback about the effectiveness or compatibility of policies from 412 TW/CC and assumes that policies are adequate.

Scenario 4: 412 TW/CC enacts inadequate policy for safety risk mitigation and acceptance.

a. 412 TW/CC is commanded to implement inadequate policies from AFTC/CC.
b. 412 TW/CC is commanded to implement inadequate policies from AFTC/SE.
c. 412 TW/CC ignores AFTC/CC and AFTC/SE policies and enacts inadequate policies.

Unsafe Control Action for AFTC/SE: Existing policy to 412 TW/CC becomes obsolete. (CA: Implement Policy)

Controlled Process: Safety process implemented by 412 TW/CC

Scenario 1: AFTC/SE does not receive updated policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.

Scenario 2: AFTC/SE does not enforce updated policy compliance from 412 TW/CC

a. AFTC/SE neglects to update policies for 412 TW/CC due to other priorities.

Scenario 3: AFTC/SE assumes that 412 TW/CC is following updated policies when 412 TW/CC is not.

a. 412 TW/CC does not provide adequate feedback about the currency of policies to AFTC/SE, causing AFTC/SE to assume currency.
b. 412 TW/CC provides incorrect feedback about the currency of policies to AFTC/SE, causing AFTC/SE to assume currency.

c. AFTC/SE misinterprets feedback about the currency of policies that 412 TW/CC is using and believes that 412 TW/CC is using current policies when it is not.

Scenario 4: 412 TW/CC continues to enact obsolete policies.

a. 412 TW/CC does not receive commands to enact new policies from AFTC/CC.
b. 412 TW/CC does not receive commands to enact new policies from AFTC/SE.
c. 412 TW/CC misses commands to enact new policies from AFTC/CC.
d. 412 TW/CC misses commands to enact new policies from AFTC/SE.
e. 412 TW/CC receives conflicting commands from AFTC/CC and AFTC/SE about which policies to enact.
f. 412 TW/CC ignores commands to enact updated policies.

Unsafe Control Action for AFTC/SE: Policy for safety risk mitigation and acceptance is not provided to AFTC/SET. (CA Issue Policy)

Controlled Process: Safety process implementation by AFTC/SET

Scenario 1: AFTC/SE does not receive or receives wrong policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.
b. Updated policy information from AFTC/CC does not mitigate safety risk or permits unacceptable risk acceptance.

Scenario 2: AFTC/SE does not enforce policy compliance by AFTC/SET.

a. AFTC/SE chooses other priorities over enforcing safety policy and does not adequately control safety implementation by AFTC/SET.

Scenario 3: AFTC/SE is unaware of policy noncompliance by AFTC/SET.

a. AFTC/SE does not perceive policy compliance from AFTC/SET accurately, causing AFTC/SE to assume compliance.
b. AFTC/SE does not receive information from AFTC/SET about policy compliance, causing AFTC/SE to assume compliance.

c. AFTC/SE misinterprets feedback from AFTC/SET and incorrectly assumes policy compliance.

Scenario 4: AFTC/SE policy implementation is not enacted by AFTC/SET.

a. AFTC/SET does not receive policy information from AFTC/SE.
b. AFTC/SET is not directed to enact policy in the safety review process.
c. AFTC/SET does not enact policy within the safety review process.

Unsafe Control Action for AFTC/SE: Inadequate policy for safety risk mitigation and acceptance is provided to AFTC/SET. (CA: Implement Policy)

Controlled Process: Safety process implementation by AFTC/SET

Scenario 1: AFTC/SE does not receive adequate policy information from AFTC/CC.

a. AFTC/CC provided policy information is incomplete or incompatible with 412 TW organization or operations.

Scenario 2: AFTC/SE enforces inadequate policy for safety risk mitigation and acceptance from AFTC/SET.

a. AFTC/SE requires AFTC/SET to comply with inadequate policies for safety risk mitigation and acceptance.

Scenario 3: AFTC/SE assumes that inadequate policies for AFTC/SET are adequate.

a. AFTC/SET does not provide adequate feedback about the effectiveness or compatibility of policies to AFTC/SE, causing AFTC/SE to incorrectly assume policies are adequate.
b. AFTC/SET provides incorrect feedback about the effectiveness or compatibility of policies to AFTC/SE, causing AFTC/SE to incorrectly assume policies are adequate.
c. AFTC/SE misinterprets feedback about the effectiveness or compatibility of policies from AFTC/SET and assumes that policies are adequate.

Scenario 4: AFTC/SET enacts inadequate policy for safety risk mitigation and acceptance.

a. AFTC/SET is commanded to implement inadequate policies from AFTC/SE.
b. AFTC/SET ignores AFTC/SE policies and enacts inadequate policies.

Unsafe Control Action for AFTC/SE: Existing policy to AFTC/SET becomes obsolete. (CA: Implement Policy)

Controlled Process: Safety process implementation by AFTC/SET

Scenario 1: AFTC/SE does not receive updated policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.

Scenario 2: AFTC/SE does not enforce updated policy compliance from AFTC/SET

a. AFTC/SE neglects to update policies for AFTC/SET due to other priorities.

Scenario 3: AFTC/SE assumes that AFTC/SET is following updated policies when AFTC/SET is not.

a. AFTC/SET does not provide adequate feedback about the currency of policies to AFTC/SE, causing AFTC/SE to assume currency.
b. AFTC/SET provides incorrect feedback about the currency of policies to AFTC/SE, causing AFTC/SE to assume currency.
c. AFTC/SE misinterprets feedback about the currency of policies that AFTC/SET is using and believes that AFTC/SET is using current policies when it is not.

Scenario 4: AFTC/SET continues to enact obsolete policies.

a. AFTC/SET does not receive commands to enact new policies from AFTC/SE.
b. AFTC/SET misses commands to enact new policies from AFTC/SE.
c. AFTC/SET ignores commands to enact updated policies.
d. AFTC/SE misinterprets feedback about the currency of policies that AFTC/SET is using and believes that 412 TW/CC is using current policies when it is not.

Unsafe Control Action for AFTC/SE: Modified policy guidance that weakens the safety process is provided to AFTC/SET. (CA: Provide Policy Guidance)

Controlled Process: Safety process implementation by AFTC/SET

Scenario 1: AFTC/SE enforces inadequate policy for safety risk mitigation and acceptance from AFTC/SET.

a. AFTC/SE requires AFTC/SET to comply with inadequate policies for safety risk mitigation and acceptance.
b. AFTC/SE provides modified policy guidance to prioritize other factors over safety.

Scenario 2: AFTC/SE assumes that inadequate policies for AFTC/SET are adequate.

a. AFTC/SET does not provide adequate feedback about the effectiveness or compatibility of modified policies to AFTC/SE, causing AFTC/SE to incorrectly assume that modified policies are effective and compatible.
b. AFTC/SET provides incorrect feedback about the effectiveness or compatibility of modified policies to AFTC/SE, causing AFTC/SE to incorrectly assume that modified policies are effective and compatible.
c. AFTC/SE misinterprets feedback from AFTC/SET and incorrectly assumes that modified policies are effective and compatible.

Scenario 3: AFTC/SET enacts inadequate policy for safety risk mitigation and acceptance.

a. AFTC/SET is commanded to implement inadequate modified policies from AFTC/SE.

Unsafe Control Action for AFTC/SE: Modified policy guidance to AFTC/SET issued and not rescinded. (CA: Provide Policy Guidance)

Controlled Process: Safety process implementation by AFTC/SET

Scenario 1: AFTC/SE does not receive guidance to rescind alternative policy guidance from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.

Scenario 2: AFTC/SE does not enforce AFTC/SET compliance of original safety policy.

a. AFTC/SE neglects to update policies for AFTC/SET due to other priorities.

Scenario 3: AFTC/SE assumes that AFTC/SET is following original policies when AFTC/SET is not.

a. AFTC/SET does not provide adequate feedback about the policies being followed to AFTC/SE, causing AFTC/SE to incorrectly assume that AFTC/SET is operating under standard policies.
b. AFTC/SET provides incorrect feedback about the policies being followed to AFTC/SE, causing AFTC/SE to incorrectly assume that AFTC/SET is operating under standard policies.
c. AFTC/SE misinterprets feedback and incorrectly assumes that AFTC/SET is operating under standard policies.

Scenario 4: AFTC/SET continues to enact obsolete policies.

a. AFTC/SET does not receive commands to revert to original policies from AFTC/SE.
b. AFTC/SET misses commands to enact revert to original policies from AFTC/SE.
c. AFTC/SET ignores commands to enact updated policies.

412 TW/CC

Unsafe Control Action for 412 TW/CC: Policy for safety risk mitigation and acceptance is not provided to Unit/CC. (CA: Implement Policy)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 TW/CC does not receive or receives wrong policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to 412 TW/CC.

Scenario 2: 412 TW/CC does not enforce policy compliance by Unit/CC.

a. 412 TW/CC chooses other priorities over enforcing safety policy and does not adequately control safety implementation by Unit/CC.

Scenario 3: 412 TW/CC is unaware of policy noncompliance by Unit/CC.

a. 412 TW/CC misinterprets feedback from Unit/CC causing 412 TW/CC to believe that Unit/CC is compliant.
b. Unit/CC provides insufficient or no information about policy compliance causing 412 TW/CC to believe that Unit/CC is compliant.

c. Unit/CC provides incorrect information about policy compliance causing 412 TW/CC to believe that Unit/CC is compliant

Scenario 4: 412 TW/CC policy implementation is not adequately enacted by Unit/CC.

a. Unit/CC does not receive policy information from 412 TW/CC.
b. Unit/CC is not directed to enact policy for the safety review process at the unit level.
c. Unit/CC does not enact policy for the safety review process at the unit level.

Unsafe Control Action for 412 TW/CC: Inadequate policy for safety risk mitigation and acceptance is provided to Unit/CC. (CA: Implement Policy)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 TW/CC does not receive adequate policy information from AFTC/CC.

a. AFTC/CC provided policy information does not mitigate safety risk, permits unacceptable risk acceptance, or is incompatible with 412 TW organization or operations.

Scenario 2: 412 TW/CC enforces inadequate policy for safety risk mitigation and acceptance from Unit/CC.

a. 412 TW/CC requires Unit/CC to comply with inadequate policies for safety risk mitigation and acceptance.

Scenario 3: 412 TW/CC assumes that inadequate policies for Unit/CC are adequate.

a. Unit/CC does not provide adequate feedback about the effectiveness or compatibility of policies to 412 TW/CC causing 412 TW/CC to believe that Unit/CC is following effective policies.
b. Unit/CC provides incorrect feedback about the effectiveness or compatibility of policies to 412 TW/CC causing 412 TW/CC to believe that Unit/CC is following effective policies.
c. 412 TW/CC misinterprets feedback about the effectiveness or compatibility of policies from Unit/CC causing 412 TW/CC to believe that Unit/CC is following effective policies.

Scenario 4: Unit/CC enacts inadequate policy for safety risk mitigation and acceptance.

a. Unit/CC is commanded to implement inadequate policies from 412 TW/CC.

Unsafe Control Action for 412 TW/CC: Existing policy to Unit/CC becomes obsolete. (CA: Implement Policy)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 TW/CC does not receive updated policy information from AFTC/CC.

a. Updated policy information from AFTC/CC not passed through effective communication channel to 412 TW/CC.

Scenario 2: 412 TW/CC does not enforce updated policy compliance from Unit/CC

a. 412 TW/CC neglects to update policies for Unit/CC due to other priorities.

Scenario 3: 412 TW/CC assumes that Unit/CC is following updated policies when Unit/CC is not.

a. Unit/CC does not provide adequate feedback about the currency of policies to 412 TW/CC causing 412 TW/CC to believe that Unit/CC is following updated policies.
b. Unit/CC provides incorrect feedback about the currency of policies to 412 TW/CC causing 412 TW/CC to believe that Unit/CC is following updated policies.
c. 412 TW/CC misinterprets feedback about the currency of policies to 412 TW/CC causing 412 TW/CC to believe that Unit/CC is following updated policies.

Scenario 4: Unit/CC continues to enact obsolete policies.

a. Unit/CC does not receive commands to enact new policies from 412 TW/CC.
b. Unit/CC misses commands to enact new policies from 412 TW/CC.
c. Unit/CC ignores commands to enact new policies from 412 TW/CC.

CONTEXTUAL FACTORS AFFECTING SAFETY REVIEW PROCESS POLICY

History: Perceived success may lead to a lack of attention, reduced application of resources, and increased risk taking by AFTC/CC, AFTC/SE, and 412 TW/CC. AFTC/CC and AFTC/SE may issue more waivers or modify policy in ways that reduce the integrity of the safety process. AFTC/CC, AFTC/SE, and 412 TW/CC may become more lax in implementing and enforcing policies.

Resources: Inadequate time or staff may limit the AFTC/CC, AFTC/SE, and 412 TW/CC's ability to handle feedback from and maintain the processes that they control. AFTC/SET and Unit/CC may be unable to implement policies as directed by their controllers. More waivers or other workarounds may be implemented to reduce a backlog of safety packages for review.

Tools and Interface: If AFTC/CC, AFTC/SE, and 412 TW/CC do not have effective auditing tools to verify the effectiveness and implementation of the safety review process policy, they may miss indicators that the safety review process needs to be updated or more stringently enforced.

Pressures: Increased pressures divert AFTC/CC, AFTC/SE, and 412 TW's attention from focusing on implementing and updating the safety review process to managing external issues. Pressures may also encourage controllers to issue waivers or modified policy guidance, potentially eroding safety.

Safety Culture: A weak safety culture in the organization may increase the issuance of waivers or other workarounds to expedite the safety process while potentially reducing safety control. Enforcement may be lacking and the safety review process may be performed superficially.

Communication: Lack of communication can limit AFTC/CC, AFTC/SE, and 412 TW/CC's ability to monitor, enforce, and update policy. It may also limit AFTC/SE, AFTC/SET, and the Unit/CC's ability to feedback information to their controllers for effective decision-making.

APPROVAL

AFTC/CC

Unsafe Control Action for AFTC/CC: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: AFTC/CC does not require sufficient level of quality from PSL.

a. AFTC/CC chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: AFTC/CC does not verify closure of action items by PSL.

a. AFTC/CC chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: AFTC/CC assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to AFTC/CC, causing AFTC/CC to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to AFTC/CC, causing AFTC/CC to assume that safety planning is sufficient when it is not.
c. AFTC/CC misinterprets feedback from PSL about the quality of safety planning, causing AFTC/CC to assume that safety planning is sufficient when it is not.

Scenario 5: AFTC/CC assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to AFTC/CC, causing AFTC/CC to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to AFTC/CC, causing AFTC/CC to assume that action items have been closed when they have not.
c. AFTC/CC misinterprets feedback from PSL, causing AFTC/CC to assume that action items have been closed when they have not.

Scenario 6: PSL does not incorporate feedback and close action items.

a. AFTC/CC does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Unsafe Control Action for AFTC/CC: Approval provided before prior reviewer feedback incorporated. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items from prior review before initiating next review.

a. Policies do not include requirements for feedback or verified closure of action items from prior review before initiating next review.

Scenario 2: AFTC/CC assumes that PSL has closed all previous reviewer action items when they have not yet been closed.

a. PSL does not provide adequate feedback about the closure of prior action items to AFTC/CC, causing AFTC/CC to assume that prior action items have been closed.
b. PSL provides incorrect feedback about the closure of prior action items to AFTC/CC, causing AFTC/CC to assume that prior action items have been closed.
c. AFTC/CC incorrectly perceives that prior reviewer feedback has been incorporated.

Scenario 3: PSL does not incorporate feedback and close action items from prior reviewers.

a. AFTC/CC does not command PSL to incorporate feedback and close action items from prior reviewers.
b. PSL misses commands to incorporate feedback and close action items from prior reviewers.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

AFTC/CZ

Unsafe Control Action for AFTC/CZ: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: AFTC/CZ does not require sufficient level of quality from PSL.

a. AFTC/CZ chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: AFTC/CZ does not verify closure of action items by PSL.

a. AFTC/CZ chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: AFTC/CZ assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to AFTC/CZ, causing AFTC/CZ to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to AFTC/CZ, causing AFTC/CZ to assume that safety planning is sufficient when it is not.
c. AFTC/CZ misinterprets feedback from PSL about the quality of safety planning, causing AFTC/CZ to assume that safety planning is sufficient when it is not.

Scenario 5: AFTC/CZ assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to AFTC/CZ, causing AFTC/CZ to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to AFTC/CZ, causing AFTC/CZ to assume that action items have been closed when they have not.
c. AFTC/CZ misinterprets feedback from PSL, causing AFTC/CZ to assume that action items have been closed when they have not.

Scenario 6: PSL does not incorporate feedback and close action items.

a. AFTC/CZ does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

412 TW/CC

Unsafe Control Action for 412 TW/CC: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: 412 TW/CC does not require sufficient level of quality from PSL.

a. 412 TW/CC chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: 412 TW/CC does not verify closure of action items by PSL.

b. 412 TW/CC chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: 412 TW/CC assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to 412 TW/CC, causing 412 TW/CC to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to 412 TW/CC, causing 412 TW/CC to assume that safety planning is sufficient when it is not.
c. 412 TW/CC misinterprets feedback from PSL about the quality of safety planning, causing 412 TW/CC to assume that safety planning is sufficient when it is not.

Scenario 5: 412 TW/CC assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to 412 TW/CC, causing 412 TW/CC to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to 412 TW/CC, causing 412 TW/CC to assume that action items have been closed when they have not.
c. 412 TW/CC misinterprets feedback from PSL, causing 412 TW/CC to assume that action items have been closed when they have not.

Scenario 5: PSL does not incorporate feedback and close action items.

a. 412 TW/CC does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.

c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Unsafe Control Action for 412 TW/CC: Approval provided before prior reviewer feedback incorporated. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items from prior review before initiating next review.

a. Policies do not include requirements for feedback or verified closure of action items from prior review before initiating next review.

Scenario 2: 412 TW/CC assumes that PSL has closed all previous reviewer action items when they have not yet been closed.

a. PSL does not provide adequate feedback about the closure of prior action items to 412 TW/CC, causing 412 TW/CC to assume that prior action items have been closed.
b. PSL provides incorrect feedback about the closure of prior action items to 412 TW/CC, causing 412 TW/CC to assume that prior action items have been closed.
c. 412 TW/CC incorrectly perceives that prior reviewer feedback has been incorporated.

Scenario 3: PSL does not incorporate feedback and close action items from prior reviewers.

a. 412 TW/CC does not command PSL to incorporate feedback and close action items from prior reviewers.
b. PSL misses commands to incorporate feedback and close action items from prior reviewers.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

412 OG/CC

Unsafe Control Action for 412 OG/CC: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: 412 OG/CC does not require sufficient level of quality from PSL.

a. 412 OG/CC chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: 412 OG/CC does not verify closure of action items by PSL.

a. 412 OG/CC chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: 412 OG/CC assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to 412 OG/CC, causing 412 OG/CC to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to 412 OG/CC, causing 412 OG/CC to assume that safety planning is sufficient when it is not.
c. 412 OG/CC misinterprets feedback from PSL about the quality of safety planning, causing 412 OG/CC to assume that safety planning is sufficient when it is not.

Scenario 5: 412 OG/CC assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to 412 OG/CC, causing 412 OG/CC to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to 412 OG/CC, causing 412 OG/CC to assume that action items have been closed when they have not.
c. 412 OG/CC misinterprets feedback from PSL, causing 412 OG/CC to assume that action items have been closed when they have not.

Scenario 6: PSL does not incorporate feedback and close action items.

a. 412 OG/CC does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.

c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Unsafe Control Action for 412 OG/CC: Approval provided before prior reviewer feedback incorporated. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items from prior review before initiating next review.

a. Policies do not include requirements for feedback or verified closure of action items from prior review before initiating next review.

Scenario 2: 412 OG/CC assumes that PSL has closed all previous reviewer action items when they have not yet been closed.

a. PSL does not provide adequate feedback about the closure of prior action items to 412 OG/CC, causing 412 OG/CC to assume that prior action items have been closed.
b. PSL provides incorrect feedback about the closure of prior action items to 412 OG/CC, causing 412 OG/CC to assume that prior action items have been closed.
c. 412 OG/CC incorrectly perceives that prior reviewer feedback has been incorporated.

Scenario 3: PSL does not incorporate feedback and close action items from prior reviewers.

a. 412 OG/CC does not command PSL to incorporate feedback and close action items from prior reviewers.
b. PSL misses commands to incorporate feedback and close action items from prior reviewers.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

412 TW/CZ

Unsafe Control Action for 412 TW/CZ: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: 412 TW/CZ does not require sufficient level of quality from PSL.

a. 412 TW/CZ chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: 412 TW/CZ does not verify closure of action items by PSL.

a. 412 TW/CZ chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: 412 TW/CZ assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

d. PSL does not provide adequate feedback about the quality of safety planning to 412 TW/CZ, causing 412 TW/CZ to assume that safety planning is sufficient when it is not.
e. PSL provides incorrect feedback about the quality of safety planning to 412 TW/CZ, causing 412 TW/CZ to assume that safety planning is sufficient when it is not.
f. 412 TW/CZ misinterprets feedback from PSL about the quality of safety planning, causing 412 TW/CZ to assume that safety planning is sufficient when it is not.

Scenario 5: 412 TW/CZ assumes that PSL closed action items when PSL did not.

d. PSL does not provide adequate feedback about the closure of action items to 412 TW/CZ, causing 412 TW/CZ to assume that action items have been closed when they have not.
e. PSL provides incorrect feedback about the closure of action items to 412 TW/CZ, causing 412 TW/CZ to assume that action items have been closed when they have not.
f. 412 TW/CZ misinterprets feedback from PSL, causing 412 TW/CZ to assume that action items have been closed when they have not.

Scenario 6: PSL does not incorporate feedback and close action items.

a. 412 TW/CZ does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.

c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

AFTC/SE

Unsafe Control Action for AFTC/SE: Unjustified approval for safety package (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: AFTC/SE does not have clear guidelines about safety planning and independent safety review requirements from AFTC/CC.

a. Policy information from AFTC/CC not passed through effective communication channel to AFTC/SE.

Scenario 2: AFTC/SE does not require compliance with safety planning and independent safety review requirements.

a. AFTC/SE chooses other priorities over requiring compliance with safety planning and independent safety review requirements.

Scenario 3: AFTC/SE assumes that PSL has complied with safety planning and independent safety review requirements.

a. AFTC/SE does not receive adequate feedback about safety planning and independent safety review compliance, causing AFTC/SE to assume compliance.
b. AFTC/SE receives incorrect feedback about safety planning and independent safety review compliance, causing AFTC/SE to assume compliance.
c. AFTC/SE incorrectly perceives that safety planning and independent safety review is compliant.

Scenario 4: PSL does not comply with safety planning and independent safety review requirements.

a. AFTC/SE does not command PSL to complete safety planning and independent safety review requirements.

b. PSL misses commands to complete safety planning and independent safety review requirements.
c. PSL ignores commands to complete safety planning and independent safety review requirements.
d. PSL is unable to adequately complete safety planning and independent safety review requirements.

AFTC/SET

Unsafe Control Action for AFTC/SET: Understated risk assessment provided to leadership. (CA: Recommend Overall Risk Level)

Controlled Process: Approval of PSL safety package

Scenario 1: AFTC/SET does not have the correct criteria for generating an accurate risk assessment for leadership.

a. Ineffective guidelines for assessing and reporting risk are provided to AFTC/SET.
b. No guidelines for assessing and reporting risk are provided to AFTC/SET.
c. Inadequate training for assessing and reporting risk is provided to AFTC/SET.

Scenario 2: AFTC/SET provides understated risk assessment to leadership.

a. Safety review board meeting not conducted effectively and understated risk assessment is produced.

Scenario 3: AFTC/SET assumes that risk assessment report to leadership provides clear unequivocal information about the risk level of the test.

a. Leadership perceives test risk to be lower than AFTC/SET is attempting to report.

Scenario 4: Leadership accepts risks that outweigh the benefits.

a. Leadership accepts greater risks due to prioritizing other objectives over safety.

Unit/CC

Unsafe Control Action for Unit/CC: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: Unit/CC does not require sufficient level of quality from PSL.

a. Unit/CC chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: Unit/CC does not verify closure of action items by PSL.

a. Unit/CC chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: Unit/CC assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to Unit/CC causing Unit/CC to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to Unit/CC causing Unit/CC to assume that safety planning is sufficient when it is not.
c. Unit/CC misinterprets feedback from PSL causing Unit/CC to assume that safety planning is sufficient when it is not.

Scenario 5: Unit/CC assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to Unit/CC causing Unit/CC to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to Unit/CC causing Unit/CC to assume that action items have been closed when they have not.
c. Unit/CC misinterprets feedback from PSL causing Unit/CC to assume that action items have been closed when they have not

Scenario 6: PSL does not incorporate feedback and close action items.

a. Unit/CC does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Unsafe Control Action for Unit/CC: Approval not rescinded when testing has unexpected test result. (CA: Approve Safety Package)

Controlled Process: Approval of PSL safety package

Scenario 1: Policies do not require approval to test to be rescinded when testing has unexpected test result.

a. Policies do not include requirements for stopping test when an unexpected test result occurs.

Scenario 2: Unit/CC does not rescind approval and stop PSL from executing test when testing has unexpected test result.

a. Unit/CC chooses other priorities over stopping test due to an unexpected test result.

Scenario 3: Unit/CC assumes that there is no unexpected test result and approval does not need to be rescinded.

a. PSL and test team do not provide adequate feedback about unexpected test results, causing Unit/CC to assume that approval does not need to be rescinded.
b. PSL and test team provides incorrect feedback about unexpected test results, causing Unit/CC to assume that approval does not need to be rescinded.
c. PSL and test team do not recognize unexpected test results and do not report them to Unit/CC, causing Unit/CC to assume that approval does not need to be rescinded.

Scenario 4: PSL and test team do not stop testing when testing has unexpected test result.

a. Unit/CC does not command PSL and test team to stop testing when testing has unexpected test result.
b. PSL and test team do not stop testing when testing has unexpected test result.

Unit/CE

Unsafe Control Action for Unit/CE: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: Unit/CE does not require sufficient level of quality from PSL.

a. Unit/CE chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: Unit/CE does not verify closure of action items by PSL.

a. Unit/CE chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: Unit/CE assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to Unit/CE causing Unit/CE to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to Unit/CE causing Unit/CE to assume that safety planning is sufficient when it is not.
c. Unit/CE misinterprets feedback from PSL causing Unit/CE to assume that safety planning is sufficient when it is not.

Scenario 5: Unit/CE assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to Unit/CE causing Unit/CE to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to Unit/CE causing Unit/CE to assume that action items have been closed when they have not.

c. Unit/CE misinterprets feedback from PSL causing Unit/CE to assume that action items have been closed when they have not

Scenario 6: PSL does not incorporate feedback and close action items.

a. Unit/CE does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Project Pilot

Unsafe Control Action for Project Pilot: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: Project Pilot does not require sufficient level of quality from PSL.

a. Project Pilot chooses other priorities over enforcing a sufficient level of quality in safety planning and does not adequately control safety planning by PSL.

Scenario 3: Project Pilot does not verify closure of action items by PSL.

a. Project Pilot chooses other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: Project Pilot assumes that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

a. PSL does not provide adequate feedback about the quality of safety planning to Project Pilot causing Project Pilot to assume that safety planning is sufficient when it is not.
b. PSL provides incorrect feedback about the quality of safety planning to Project Pilot causing Project Pilot to assume that safety planning is sufficient when it is not.

c. Project Pilot misinterprets feedback from PSL causing Project Pilot to assume that safety planning is sufficient when it is not.

Scenario 5: Project Pilot assumes that PSL closed action items when PSL did not.

a. PSL does not provide adequate feedback about the closure of action items to Project Pilot causing Project Pilot to assume that action items have been closed when they have not.
b. PSL provides incorrect feedback about the closure of action items to Project Pilot causing Project Pilot to assume that action items have been closed when they have not.
c. Project Pilot misinterprets feedback from PSL causing Project Pilot to assume that action items have been closed when they have not

Scenario 6: PSL does not incorporate feedback and close action items.

a. Project Pilot does not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Contextual Factors Affecting Approval

History: A history of safety may lead to a lack of attention or priority by the AFTC/CC, AFTC/CZ, 412 TW/CC, Unit/CC, Unit/CE, and Project Pilot during their review and a lack of diligence in verifying the closure of prior action items. AFTC/SE may provide unjustified approvals for safety packages assuming that doing so will not adversely affect safety.

Resources: Inadequate time or staff may reduce the approver's ability to verify quality, provide useful feedback and verify the closure of prior action items. Delays in sequential reviews may result in out of sequence reviews to expedite the review process. Unjustified approvals from AFTC/SE may be provided to reduce workload and make up lost time. PSLs may have insufficient time to close all action items before assigned deadlines.

Tools and Interface: Inadequate tracking tools to verify the closure of action items for each reviewer may lead to inadequately managed safety issues in the safety package and approval to test. Inadequate risk assessment tools may make it difficult for AFTC/SET to adequately determine the safety risk for proposed testing and communicate it to leadership.

Training: AFTC/SET may be inadequately equipped to generate accurate risk assessments to leadership without a training program that gives them the required knowledge and tools. PSL may be inadequately trained to answer action items from reviewers.

Pressures: Pressures to produce may influence approvers to expedite their reviews of the safety package to the detriment of safety. The Unit/CC may be pressured to continue testing even after an unexpected test event occurs. AFTC/SE may provide unjustified approvals to safety packages to expedite their review. Out of sequence reviews may be implemented to accelerate the safety review process and AFTC/CC, 412 TW/CC, or 412 OG/CC may provide final approvals to test before prior feedback is incorporated.

Safety Culture: A weak safety culture may cause an even weaker safety culture as the attitude spreads. A weak safety culture can negatively impact the approval process. Approvers may review safety packages less rigorously. Unit/CCs may not view unexpected test events as significant enough to halt testing and investigate. The integrity of the safety process may be violated due to workarounds such as out of sequence reviews.

Communication: Inadequate communication between the PSL and approvers may lead to incorrect assumptions. Approvers may not recognize the need for feedback or that action items have not been closed. The PSL may not recognize that approvers have assigned action items. Approvers may not receive policy guidance that clearly explains the requirements for safety package approval. AFTC/SE may incorrectly assume that safety requirements have been met and provide approval. AFTC/SET may not have been provided guidelines about how to assess and report risk. Senior leadership may misunderstand risk assessments provided by AFTC/SET.

FINAL SAFETY REVIEW

AFTC/SET

Unsafe Control Action for AFTC/SET: Safety Review Board conducted too early (before prerequisites are complete). (CA: Allow to proceed with Safety Review Board)

Controlled Process: Final safety review – safety review board meeting

Scenario 1: Requirements for proceeding with Safety Review Board are not provided.

a. AFTC/SET does not have the requirements to confirm that the test team is ready to proceed with the Safety Review Board.

Scenario 2: AFTC/SET does not require that the requirements to proceed with the Safety Review Board are complete.

a. AFTC/SET prioritizes other factors over ensuring that the requirements to proceed with the Safety Review Board are complete.

Scenario 3: AFTC/SET assumes that the PSL has completed the requirements necessary to proceed with the Safety Review Board.

a. PSL provides incorrect feedback that the prerequisites for proceeding with the Safety Review Board are complete, causing AFTC/SET to believe that perquisites are complete when they are not.
b. PSL provides no feedback that the prerequisites for proceeding with the Safety Review board are complete, causing AFTC/SET to believe that perquisites are complete when they are not.
c. AFTC/SET misinterprets the feedback and thinks that the prerequisites for proceeding with the Safety Review Board are complete.

Unsafe Control Action for AFTC/SET: Inadequately qualified safety review board members selected. (CA: Select Safety Review Members)

Controlled Process: Final safety review – safety review board meeting

Scenario 1: AFTC/SET does not have required information to select qualified safety review board members.

a. AFTC/SET does not have standards from which to assess the qualifications of safety review board members.
b. AFTC/SET does not have information about safety review board candidates to adequately assess their qualifications.

Scenario 2: AFTC/SET chooses inadequately qualified safety review board members.

a. Qualified members are unavailable and less qualified safety review board members are chosen to save time.

Scenario 3: AFTC/SET thinks that safety review board member selectees are qualified when they are not.

a. AFTC/SET perceives that safety review board members are qualified when they are not.
b. Safety review board members provide feedback that they are qualified when they are not.

Scenario 4: Safety Review Board meeting is ineffective because safety review board members do not adequately review and assess safety.

a. Safety review board members have inadequate training or experience to review and assess safety.

Unsafe Control Action for AFTC/SET: Safety review board meeting guidance not provided. (CA: Provide Safety Review Board Meeting Guidance)

Controlled Process: Final safety review – safety review board meeting

Scenario 1: AFTC/SET has inadequate training.

a. AFTC/SET does not know what the relevant guidance is for running a safety review board meeting.
b. There is no guidance for running a safety review board meeting.

Scenario 2: AFTC/SET does not provide safety review board meeting guidance.

a. Safety review board meeting guidance not provided and board participants focus discussion on non-safety related issues.

Scenario 3: AFTC/SET assumes that safety review board meeting participants understand the goals and expected conduct for the safety review board meeting.

a. Safety review board members do not provide feedback that they need a review of the goals and expected conduct for the safety review board meeting.

b. AFTC/SET misinterprets feedback and believes that the safety review board members have sufficient understanding of the goals and procedures for the safety review board meeting when they do not.

Scenario 4: Safety review board members do not participate in the safety review board meeting effectively.

a. Safety review board members have objectives other than ensuring safe test.
b. Safety review board members are inadequately qualified to analyze and perform a risk assessment.

Unsafe Control Action for AFTC/SET: Safety review board meeting guidance is incorrect. (CA: Provide Safety Review Board Meeting Guidance)

Controlled Process: Final safety review – safety review board meeting

Scenario 1: AFTC/SET has inadequate training.

a. AFTC/SET does not know what the relevant guidance is for running a safety review board meeting.
b. Current guidance for running a safety review board meeting is inadequate.

Scenario 2: AFTC/SET does not provide adequate safety review board meeting guidance.

a. Safety review board meeting guidance provided diverts attention from effectively reviewing and assessing safety to less productive discussions.

Scenario 3: AFTC/SET assumes that the safety review board meeting guidance will ensure a productive safety review board meeting when it is inadequate.

a. Safety review board members do not provide feedback that the conduct of the meeting is not conducive to an effective safety review.
b. AFTC/SET misinterprets feedback and believes that the safety review board meeting is being conducted effectively.

Scenario 4: Safety review board members do not achieve the objectives of effectively reviewing and assessing safety.

a. Safety review board members do not recognize that the safety review board meeting is not being conducted in a way that achieves the objectives of reviewing and assessing safety.

Unsafe Control Action for AFTC/SET: Safety review board meeting guidance is not applied throughout meeting. (CA: Provide Safety Review Board Meeting Guidance)

Controlled Process: Final safety review – safety review board meeting

Scenario 1: AFTC/SET has inadequate training.

a. AFTC/SET does not know how to moderate the discussion to ensure that the meeting remains focused and productive.

Scenario 2: AFTC/SET does not consistently manage the safety review board discussion.

a. AFTC/SET considers the safety review board meeting unimportant and only superficially manages the safety review board meeting.

Scenario 3: AFTC/SET assumes that the safety review board participants know what they are doing.

a. Safety review board meeting participants indicate their confidence in executing safety review board process when they are actually ineffective.
b. AFTC/SET perceives that the safety review board meeting participants are executing the safety review board process correctly when they are actually ineffective.

Scenario 4: Safety review board members do not conduct an effective safety review board meeting.

a. Safety review board members focus on their own agendas while neglecting a focus on reviewing and assessing safety causing the meeting to be unproductive.

Unsafe Control Action for AFTC/SET: Unjustified approval for safety package (CA: Approve Safety Package)

Controlled Process: Final safety review – approval of PSL safety package

Scenario 1: AFTC/SET does not have clear guidelines about safety planning and independent safety review requirements from AFTC/SE.

a. Policy information from AFTC/CC not passed through effective communication channel to AFTC/SET.

Scenario 2: AFTC/SET does not require compliance with safety planning and independent safety review requirements.

a. AFTC/SET chooses other priorities over requiring compliance with safety planning and independent safety review requirements.

Scenario 3: AFTC/SET assumes that PSL has complied with safety planning and independent safety review requirements.

a. AFTC/SET does not receive adequate feedback about safety planning and independent safety review compliance causing AFTC/SET to assume compliance.
b. AFTC/SET receives incorrect feedback about safety planning and independent safety review compliance causing AFTC/SET to assume compliance.
c. AFTC/SET incorrectly perceives that safety planning and independent safety review is compliant.

Scenario 4: PSL does not comply with safety planning and independent safety review requirements.

a. AFTC/SET does not command PSL to complete safety planning and independent safety review requirements.
b. PSL misses commands to complete safety planning and independent safety review requirements.
c. PSL ignores commands to complete safety planning and independent safety review requirements.
d. PSL is unable to adequately complete safety planning and independent safety review requirements.

Tech Experts/Ops Reps

Unsafe Control Action for Tech Experts/Ops Reps: Approval provided without providing feedback or verified closure of action items. (CA: Approve Safety Package)

Controlled Process: Final safety review – approval of PSL safety package

Scenario 1: Policies do not require feedback or verified closure of action items.

a. Policies do not include requirements for feedback or verified closure of action items.

Scenario 2: Tech Experts/Ops Reps do not require sufficient level of quality from PSL.

a. Tech Experts/Ops Reps choose other priorities over enforcing a sufficient level of quality in safety planning and do not adequately control safety planning by PSL.

Scenario 3: Tech Experts/Ops Reps do not verify closure of action items by PSL.

b. Tech Experts/Ops Reps choose other priorities over enforcing closure of action items in safety planning by PSL.

Scenario 4: Tech Experts/Ops Reps assume that PSL is conducting safety planning with a sufficient level of quality when PSL is not.

d. PSL does not provide adequate feedback about the quality of safety planning to Tech Experts/Ops Reps causing Tech Experts/Ops Reps to assume that safety planning is sufficient when it is not.
e. PSL provides incorrect feedback about the quality of safety planning to Tech Experts/Ops Reps causing Tech Experts/Ops Reps to assume that safety planning is sufficient when it is not.
f. Unit/CC misinterprets feedback from PSL causing Tech Experts/Ops Reps to assume that safety planning is sufficient when it is not.

Scenario 5: Tech Experts/Ops Reps assume that PSL closed action items when PSL did not.

d. PSL does not provide adequate feedback about the closure of action items to Tech Experts/Ops Reps causing Tech Experts/Ops Reps to assume that action items have been closed when they have not.
e. PSL provides incorrect feedback about the closure of action items to Tech Experts/Ops Reps causing Tech Experts/Ops Reps to assume that action items have been closed when they have not.
f. Tech Experts/Ops Reps misinterprets feedback from PSL causing Tech Experts/Ops Reps to assume that action items have been closed when they have not

Scenario 5: PSL does not incorporate feedback and close action items.

a. Tech Experts/Ops Reps do not command PSL to incorporate feedback and close action items.
b. PSL misses commands to incorporate feedback and close action items.
c. PSL ignores commands to incorporate feedback and close action items.
d. PSL is unable to adequately research and address action items.

Unsafe Control Action for Tech Experts/Ops Reps: Understated risk assessment provided to AFTC/SET. (CA: Recommend Overall Risk Level)

Controlled Process: Final safety review – safety review board recommendation

Scenario 1: Tech Experts/Ops Reps do not have the right criteria for generating an accurate risk assessment for AFTC/SET.

a. Ineffective guidelines for assessing and reporting risk are provided to Tech Experts/Ops Reps.
b. No guidelines for assessing and reporting risk are provided to Tech Experts/Ops Reps.

Scenario 2: Tech Experts/Ops Reps provide understated risk assessment to AFTC/SET.

a. Safety review board meeting not conducted effectively and understated risk assessment is produced.

Scenario 3: Tech Experts/Ops Reps assume that risk assessment provided to AFTC/SET provides clear unequivocal information about the risk level of the test.

a. AFTC/SET misinterprets risk assessment from Tech Experts/Ops Reps and provides an understated risk assessment.

Scenario 4: AFTC/SET reports incorrect risk assessment to leadership.

a. AFTC/SET incorrectly documents risk assessment in safety package.

CONTEXTUAL FACTORS AFFECTING FINAL SAFETY REVIEW

History: A successful record of safety may lead AFTC/SET to assume that workarounds such as conducting safety review board meetings before requirements are met or selecting lesser

experienced safety review board members do not have a tangible impact on safety. Tech experts may review safety packages less rigorously. Tech experts are expected to contribute their substantial experience from related testing to accomplish the independent safety review. Historical lessons learned may not, however, be applicable to new contexts.

Resources: Inadequate time or manpower may lead AFTC/SET to select less qualified safety review board members due to the unavailability of more experienced reviewers.

Tools and Interface: Inadequate risk assessment tools may make it difficult for tech experts to adequately determine and communicate the safety risk for proposed testing.

Training: AFTC/SET may be inadequately trained to effectively manage a safety review board meeting to ensure an effective independent safety review.

Pressures: Pressures to approve testing may cause AFTC/SET to select less qualified safety review board members if more experienced reviewers are unavailable. AFTC/SET may also be pressured to provide approvals certifying that the requirements for an independent safety review have been met.

Safety Culture: Safety culture can affect the way that AFTC/SET and safety review board members perceive their work as independent safety reviewers. A weak safety culture may cause safety reviewers to allow workarounds, select less qualified reviewers, and perform the independent safety review less rigorously.

Communication: Policy may not have been communicated from AFTC/SE to AFTC/SET regarding requirements to proceed with testing or qualifications for safety review board members. Inadequate communication between AFTC/SET and safety review board members may be due to the lack of clear expectations or the inability to articulate clear expectations about meeting conduct. Inadequate communication between AFTC/SET and the safety review board members during the safety review can cause a mismatch of expectations for conduct during the safety review board meeting. As a result, the meeting may not effectively accomplish the independent safety review.

Safety Package Preparation

AFTC/CC

Unsafe Control Action for AFTC/CC: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require AFTC/CC to provide feedback to PSL.

a. Safety policy does not specify that the AFTC/CC must review the safety package and provide feedback to the PSL.

Scenario 2: AFTC/CC does not require actions from PSL when actions are required.

a. AFTC/CC does not prioritize the safety package review and provide action items where they are required.

Scenario 3: AFTC/CC assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to AFTC/CC that inputs are needed and AFTC/CC assumes that inputs are not needed.
b. PSL provides incorrect feedback to AFTC/CC that leads AFTC/CC to assume that inputs are not needed.
c. AFTC/CC does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. AFTC/CC reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. AFTC/CC does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for AFTC/CC: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: AFTC/CC's technical information is wrong or inadequate.

a. AFTC/CC does not have sufficient expertise about the system under test.

Scenario 2: AFTC/CC provides action items that lead to the violation of safety constraints.

a. AFTC/CC provides actions that prioritize goals other than safety in safety planning.

Scenario 3: AFTC/CC assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to AFTC/CC that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to AFTC/CC that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per AFTC/CC direction.
b. PSL incorrectly interprets action items from AFTC/CC and incorporates action items in a way that may lead to the violation of safety constraints.

AFTC/CZ

Unsafe Control Action for AFTC/CZ: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require AFTC/CZ to provide feedback to PSL.

a. Safety policy does not specify that the AFTC/CZ must review the safety package and provide feedback to the PSL.

Scenario 2: AFTC/CZ does not require actions from PSL when actions are required.

a. AFTC/CZ does not prioritize the safety package review and provide action items where they are required.

Scenario 3: AFTC/CZ assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to AFTC/CZ that inputs are needed and AFTC/CZ assumes that inputs are not needed.
b. PSL provides incorrect feedback to AFTC/CZ that leads AFTC/CZ to assume that inputs are not needed.
c. AFTC/CZ does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. AFTC/CZ reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. AFTC/CZ does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for AFTC/CZ: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: AFTC/CZ's technical information is wrong or inadequate.

a. AFTC/CZ does not have sufficient expertise about the system under test.

Scenario 2: AFTC/CZ provides action items that lead to the violation of safety constraints.

a. AFTC/CZ provides actions that prioritize goals other than safety in safety planning.

Scenario 3: AFTC/CZ assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to AFTC/CZ that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to AFTC/CZ that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per AFTC/CZ direction.
b. PSL incorrectly interprets action items from AFTC/CZ and incorporates action items in a way that may lead to the violation of safety constraints.

412 TW/CC

Unsafe Control Action for 412 TW/CC: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require 412 TW/CC to provide feedback to PSL.

a. Safety policy does not specify that the 412 TW/CC must review the safety package and provide feedback to the PSL.

Scenario 2: 412 TW/CC does not require actions from PSL when actions are required.

a. 412 TW/CC does not prioritize the safety package review and provide action items where they are required.

Scenario 3: 412 TW/CC assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to 412 TW/CC that inputs are needed and 412 TW/CC assumes that inputs are not needed.
b. PSL provides incorrect feedback to 412 TW/CC that leads 412 TW/CC to assume that inputs are not needed.

c. 412 TW/CC does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. 412 TW/CC reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. 412 TW/CC does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for 412 TW/CC: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 TW/CC's technical information is wrong or inadequate.

a. 412 TW/CC does not have sufficient expertise about the system under test.

Scenario 2: 412 TW/CC provides action items that lead to the violation of safety constraints.

a. 412 TW/CC provides actions that prioritize goals other than safety in safety planning.

Scenario 3: 412 TW/CC assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to 412 TW/CC that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to 412 TW/CC that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per 412 TW/CC direction.
b. PSL incorrectly interprets action items from 412 TW/CC and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for 412 TW/CC: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the 412 TW/CC prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: 412 TW/CC provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, 412 TW/CC is unable to review safety package but allows the safety package to proceed to next level review. 412 TW/CC reviews and provides actions out of sequence.

Scenario 3: 412 TW/CC assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. 412 TW/CC perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the 412 TW/CC will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from 412 TW/CC after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from 412 TW/CC and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

412 OG/CC

Unsafe Control Action for 412 OG/CC: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require 412 OG/CC to provide feedback to PSL.

a. Safety policy does not specify that the 412 OG/CC must review the safety package and provide feedback to the PSL.

Scenario 2: 412 OG/CC does not require actions from PSL when actions are required.

a. 412 OG/CC does not prioritize the safety package review and provide action items where they are required.

Scenario 3: 412 OG/CC assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to 412 OG/CC that inputs are needed and 412 OG/CC assumes that inputs are not needed.
b. PSL provides incorrect feedback to 412 OG/CC that leads 412 OG/CC to assume that inputs are not needed.
c. 412 OG/CC does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. 412 OG/CC reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. 412 OG/CC does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for 412 OG/CC: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 OG/CC's technical information is wrong or inadequate.

a. 412 OG/CC does not have sufficient expertise about the system under test.

Scenario 2: 412 OG/CC provides action items that lead to the violation of safety constraints.

a. 412 OG/CC provides actions that prioritize goals other than safety in safety planning.

Scenario 3: 412 OG/CC assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to 412 OG/CC that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to 412 OG/CC that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per 412 OG/CC direction.
b. PSL incorrectly interprets action items from 412 OG/CC and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for 412 OG/CC: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the 412 OG/CC prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: 412 OG/CC provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, 412 OG/CC is unable to review safety package but allows the safety package to proceed to next level review. 412 OG/CC reviews and provides actions out of sequence.

Scenario 3: 412 OG/CC assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. 412 OG/CC perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the 412 OG/CC will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from 412 OG/CC after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from 412 OG/CC and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

412 TW/CZ

Unsafe Control Action for 412 TW/CZ: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require 412 TW/CZ to provide feedback to PSL.

a. Safety policy does not specify that the 412 TW/CZ must review the safety package and provide feedback to the PSL.

Scenario 2: 412 TW/CZ does not require actions from PSL when actions are required.

b. 412 TW/CZ does not prioritize the safety package review and provide action items where they are required.

Scenario 3: 412 TW/CZ assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to 412 TW/CZ that inputs are needed and 412 TW/CZ assumes that inputs are not needed.
b. PSL provides incorrect feedback to 412 TW/CZ that leads 412 TW/CZ to assume that inputs are not needed.
c. 412 TW/CZ does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. 412 TW/CZ reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. 412 TW/CZ does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for 412 TW/CZ: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: 412 TW/CZ's technical information is wrong or inadequate.

a. 412 TW/CZ does not have sufficient expertise about the system under test.

Scenario 2: 412 TW/CZ provides action items that lead to the violation of safety constraints.

a. 412 TW/CZ provides actions that prioritize goals other than safety in safety planning.

Scenario 3: 412 TW/CZ assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to 412 TW/CZ that action items may lead to the violation of safety constraints.

b. PSL provides incorrect feedback to 412 TW/CZ that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per 412 TW/CZ direction.
b. PSL incorrectly interprets action items from 412 TW/CZ and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for 412 TW/CZ: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the 412 TW/CZ prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: 412 TW/CZ provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, 412 TW/CZ is unable to review safety package but allows the safety package to proceed to next level review. 412 TW/CZ reviews and provides actions out of sequence.

Scenario 3: 412 TW/CZ assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. 412 TW/CZ perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the 412 TW/CZ will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from 412 TW/CZ after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from 412 TW/CZ and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

AFTC/SE

Unsafe Control Action for AFTC/SE: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require AFTC/SE to provide feedback to PSL.

a. Safety policy does not specify that the AFTC/SE must review the safety package and provide feedback to the PSL.

Scenario 2: AFTC/SE does not require actions from PSL when actions are required.

a. AFTC/SE does not prioritize the safety package review and provide action items where they are required.

Scenario 3: AFTC/SE assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to AFTC/SE that inputs are needed and AFTC/SE assumes that inputs are not needed.
b. PSL provides incorrect feedback to AFTC/SE that leads AFTC/SE to assume that inputs are not needed.
c. AFTC/SE does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. AFTC/SE reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. AFTC/SE does not command PSL to address actions.

b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for AFTC/SE: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: AFTC/SE's technical information is wrong or inadequate.

a. AFTC/SE does not have sufficient expertise about the system under test.

Scenario 2: AFTC/SE provides action items that lead to the violation of safety constraints.

a. AFTC/SE provides actions that prioritize goals other than safety in safety planning.

Scenario 3: AFTC/SE assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to AFTC/SE that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to AFTC/SE that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per AFTC/SE direction.
b. PSL incorrectly interprets action items from AFTC/SE and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for AFTC/SE: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the AFTC/SE prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: AFTC/SE provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, AFTC/SE is unable to review safety package but allows the safety package to proceed to next level review. AFTC/SE reviews and provides actions out of sequence.

Scenario 3: AFTC/SE assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. AFTC/SE perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the AFTC/SE will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from AFTC/SE after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from AFTC/SE and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

AFTC/SET

Unsafe Control Action for AFTC/SET: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require AFTC/SET to provide feedback to PSL.

a. Safety policy does not specify that the AFTC/SET must review the safety package and provide feedback to the PSL.

Scenario 2: AFTC/SET does not require actions from PSL when actions are required.

a. AFTC/SET does not prioritize the safety package review and provide action items where they are required.

Scenario 3: AFTC/SET assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to AFTC/SET that inputs are needed and AFTC/SET assumes that inputs are not needed.
b. PSL provides incorrect feedback to AFTC/SET that leads AFTC/SET to assume that inputs are not needed.
c. AFTC/SET does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. AFTC/SET reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. AFTC/SET does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for AFTC/SET: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: AFTC/SET's technical information is wrong or inadequate.

a. AFTC/SET does not have sufficient expertise about the system under test.

Scenario 2: AFTC/SET provides action items that lead to the violation of safety constraints.

a. AFTC/SET provides actions that prioritize goals other than safety in safety planning.

Scenario 3: AFTC/SET assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to AFTC/SET that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to AFTC/SET that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per AFTC/SET direction.
b. PSL incorrectly interprets action items from AFTC/SET and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for AFTC/SET: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the AFTC/SET prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: AFTC/SET provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, AFTC/SET is unable to review safety package but allows the safety package to proceed to next level review. AFTC/SET reviews and provides actions out of sequence.

Scenario 3: AFTC/SET assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. AFTC/SET perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the AFTC/SET will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from AFTC/SET after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from AFTC/SET and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

Tech Experts/Ops Reps

Unsafe Control Action for Tech Experts/Ops Reps: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require Tech Experts/Ops Reps to provide feedback to PSL.

a. Safety policy does not specify that the Tech Experts/Ops Reps must review the safety package and provide feedback to the PSL.

Scenario 2: Tech Experts/Ops Reps do not require actions from PSL when actions are required.

a. Tech Experts/Ops Reps do not prioritize the safety package review and provide action items where they are required.

Scenario 3: Tech Experts/Ops Reps assume that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to Tech Experts/Ops Reps that inputs are needed and Tech Experts/Ops Reps assume that inputs are not needed.

b. PSL provides incorrect feedback to Tech Experts/Ops Reps that leads Tech Experts/Ops Reps to assume that inputs are not needed.
c. Tech Experts/Ops Reps do not review safety package or inquire about the safety plan and do not recognize that inputs are needed.
d. Tech Experts/Ops Reps reviews safety package and do not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. Tech Experts/Ops Reps do not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for Tech Experts/Ops Reps: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Tech Experts/Ops Reps' technical information is wrong or inadequate.

a. Tech Experts/Ops Reps do not have sufficient expertise about the system under test.

Scenario 2: Tech Experts/Ops Reps provide action items that lead to the violation of safety constraints.

a. Tech Experts/Ops Reps provide actions that prioritize goals other than safety in safety planning.

Scenario 3: Tech Experts/Ops Reps assume that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to Tech Experts/Ops Reps that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to Tech Experts/Ops Reps that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per Tech Experts/Ops Reps direction.
b. PSL incorrectly interprets action items from Tech Experts/Ops Reps and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for Tech Experts/Ops Reps: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the Tech Experts/Ops Reps prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: Tech Experts/Ops Reps provide action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, Tech Experts/Ops Reps are unable to review safety package but allows the safety package to proceed to next level review. AFTC/SET reviews and provides actions out of sequence.

Scenario 3: Tech Experts/Ops Reps assume that action items provided after follow-on reviewers will not adversely impact safety.

a. Tech Experts/Ops Reps perceive that providing feedback out of sequence will increase safety rather than reduce safety.
b. Adverse changes may go undetected and no feedback to the Tech Experts/Ops Reps will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from Tech Experts/Ops Reps after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from Tech Experts/Ops Reps and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

Unit/CC

Unsafe Control Action for Unit/CC: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require Unit/CC to provide feedback to PSL.

a. Safety policy does not specify that the Unit/CC must review the safety package and provide feedback to the PSL.

Scenario 2: Unit/CC does not require actions from PSL when actions are required.

a. Unit/CC does not prioritize the safety package review and provide action items where they are required.

Scenario 3: Unit/CC assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to Unit/CC that inputs are needed and Unit/CC assumes that inputs are not needed.
b. PSL provides incorrect feedback to Unit/CC that leads Unit/CC to assume that inputs are not needed.
c. Unit/CC does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. Unit/CC reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. Unit/CC does not command PSL to address actions.
b. PSL misses commands to address actions.

c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for Unit/CC: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Unit/CC's technical information is wrong or inadequate.

a. Unit/CC does not have sufficient expertise about the system under test.

Scenario 2: Unit/CC provides action items that lead to the violation of safety constraints.

b. Unit/CC provides actions that prioritize goals other than safety in safety planning.

Scenario 3: Unit/CC assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to Unit/CC that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to Unit/CC that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per Unit/CC direction.
b. PSL incorrectly interprets action items from Unit/CC and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for Unit/CC: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the Unit/CC prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: Unit/CC provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, Unit/CC is unable to review safety package but allows the safety package to proceed to next level review. Unit/CC reviews and provides actions out of sequence.

Scenario 3: Unit/CC assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. Unit/CC perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. If action items are provided after the safety review board meeting, adverse changes may go undetected and no feedback to the Unit/CC will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from Unit/CC after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from Unit/CC and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

Unit/CE

Unsafe Control Action for Unit/CE: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require Unit/CE to provide feedback to PSL.

a. Safety policy does not specify that the Unit/CE must review the safety package and provide feedback to the PSL.

Scenario 2: Unit/CE does not require actions from PSL when actions are required.

a. Unit/CE does not prioritize the safety package review and provide action items where they are required.

Scenario 3: Unit/CE assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to Unit/CE that inputs are needed and Unit/CE assumes that inputs are not needed.
b. PSL provides incorrect feedback to Unit/CE that leads Unit/CE to assume that inputs are not needed.
c. Unit/CE does not review safety package or inquire about the safety plan and does not recognize that inputs are needed.
d. Unit/CE reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. Unit/CE does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for Unit/CE: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Unit/CE's technical information is wrong or inadequate.

a. Unit/CE does not have sufficient expertise about the system under test.

Scenario 2: Unit/CE provides action items that lead to the violation of safety constraints.

a. Unit/CE provides actions that prioritize goals other than safety in safety planning.

Scenario 3: Unit/CE assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to Unit/CE that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to Unit/CE that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per Unit/CE direction.
b. PSL incorrectly interprets action items from Unit/CE and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for Unit/CE: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the Unit/CE prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: Unit/CE provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, Unit/CE is unable to review safety package but allows the safety package to proceed to next level review. Unit/CE reviews and provides actions out of sequence.

Scenario 3: Unit/CE assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. Unit/CE perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. If action items are provided after the safety review board meeting, adverse changes may go undetected and no feedback to the Unit/CE will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from Unit/CE after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from Unit/CE and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

Project Pilot

Unsafe Control Action for Project Pilot: Action items not provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require Project Pilot to provide feedback to PSL.

a. Safety policy does not specify that the Project Pilot must review the safety package and provide feedback to the PSL.

Scenario 2: Project Pilot does not require actions from PSL when actions are required.

a. Project Pilot does not prioritize the safety package review and provide action items where they are required.

Scenario 3: Project Pilot assumes that the PSL has produced an adequate safety package and action items are not required.

a. PSL does not provide feedback to Project Pilot that inputs are needed.
b. PSL provides incorrect feedback to Project Pilot that inputs are not needed.

c. Project Pilot does not review safety package or inquire about the safety plan.
d. Project Pilot reviews safety package and does not recognize a need for action items.

Scenario 4: Safety package from PSL is not adequate.

a. Project Pilot does not command PSL to address actions.
b. PSL misses commands to address actions.
c. PSL ignores commands to address actions.
d. PSL does not adequately conduct safety analysis and planning.

Unsafe Control Action for Project Pilot: Action items that lead to the violation of safety constraints are provided. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Project Pilot's technical information is wrong or inadequate.

a. Project Pilot does not have sufficient expertise about the system under test.

Scenario 2: Project Pilot provides action items that lead to the violation of safety constraints.

a. Project Pilot provides actions that prioritize goals other than safety in safety planning.

Scenario 3: Project Pilot assumes that action items are safe when they actually lead to the violation of safety constraints.

a. PSL does not provide feedback to Project Pilot that action items may lead to the violation of safety constraints.
b. PSL provides incorrect feedback to Project Pilot that action items will not lead to the violation of safety constraints.

Scenario 4: PSL incorporates action items that lead to the violation of safety constraints.

a. PSL incorporates action items that lead to the violation of safety constraints per Project Pilot direction.
b. PSL incorrectly interprets action items from Project Pilot and incorporates action items in a way that may lead to the violation of safety constraints.

Unsafe Control Action for Project Pilot: Action items that lead to the violation of safety constraints are provided after follow-on reviewers. (CA: Return Safety Package with Actions)

Controlled Process: Safety package preparation by PSL

Scenario 1: Policies do not require the closure of action items from the Project Pilot prior to the next level review.

a. Possibility of safety constraint violation due to out of sequence interaction of feedback not recognized and written into policy.

Scenario 2: Project Pilot provides action items that lead to the violation of safety constraints after follow-on reviewers.

a. Due to other priorities, Project Pilot is unable to review safety package but allows the safety package to proceed to next level review. Project Pilot reviews and provides actions out of sequence.

Scenario 3: Project Pilot assumes that action items provided after follow-on reviewers will not adversely impact safety.

a. Project Pilot perceives that providing feedback out of sequence will increase safety rather than reduce safety.
b. If action items are provided after the safety review board meeting, adverse changes may go undetected and no feedback to the Project Pilot will be provided.

Scenario 4: Action items that lead to the violation of safety constraints are incorporated after follow-on reviewers.

a. PSL incorporates action items that lead to the violation of safety constraints from Project Pilot after follow-on safety reviewers have reviewed and approved.
b. PSL incorrectly interprets action items from Project Pilot and incorporates action items in a way that may lead to the violation of safety constraints after other reviewers have reviewed and approved.

CONTEXTUAL FACTORS AFFECTING SAFETY PACKAGE PREPARATION

History: A successful record of safety may lead all the reviewers to assume that their individual feedback isn't critical to ensuring that safety packages effectively control safety. Workarounds such as out of sequence reviews may be employed to expedite the review process. Missing, incomplete, or inadequate action items may be provided by reviewers.

Resources: Inadequate time or manpower may lead reviewers to only superficially review safety packages and not provide key safety inputs important for controlling safety. Reviewers may overlook important information such as whether action items from previous reviewers have been closed.

Tools and Interface: Inadequate tools to track the closure of action items may allow reviewers to inadvertently review a safety package before previous reviewers have had their action items addressed.

Training: Reviewers have inadequate training or knowledge regarding the system under test or safety principles and are unable to provide useful feedback for controlling safety.

Pressures: Pressures to approve testing may cause reviewers to inadequately review safety packages and provide insufficient feedback for reducing safety risk. Workarounds such as out of sequence reviews may be employed to expedite the safety process.

Safety Culture: A weak safety culture may degrade the effectiveness of reviewers. Reviewers that do not view their work as important may only superficially review safety packages and provide inadequate feedback.

Communication: Inadequate communication between the PSL and reviewer may result in differing understandings about what action items must be closed, requirements for closure, and whether they've been closed.

PROJECT SAFETY PLANNING

KTR/Program Office

Unsafe Control Action for KTR/Program Office: Safety assessment not provided to PSL. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

f. KTR/Program Office does not have the required technical data to assess safety.
g. KTR/Program Office does not have adequate technical experience to assess safety.
h. KTR/Program Office does not have sufficient funding to assess safety.
i. KTR/Program Office does not have sufficient manpower to assess safety.
j. KTR/Program Office does not have sufficient time to assess safety.

Scenario 2: KTR/Program Office does not provide safety assessment to the PSL.

b. KTR/Program Office does not effectively communicate safety assessment to the PSL.

Scenario 3: KTR/Program Office assumes that the PSL has incorporated adequate safety measures into the safety package.

d. PSL provides no feedback about safety measures incorporated causing KTR/Program Office to assume that the PSL has incorporated sufficient safety measures.
e. PSL provides incorrect feedback about incorporating sufficient safety measures causing KTR/Program Office to believe that the PSL has incorporated sufficient safety measures.
f. KTR/Program Office misinterprets feedback and believes that the PSL has incorporated sufficient safety measures.

Scenario 4: PSL does not incorporate safety assessment recommendations into the safety package.

e. PSL does not receive safety assessment recommendations.
f. PSL overlooks safety assessment recommendations.
g. PSL ignores safety assessment recommendations.
h. PSL misinterprets safety assessment recommendations.

Unsafe Control Action for KTR/Program Office: Incorrect safety assessment provided to PSL. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

f. KTR/Program Office does not have the required technical data to provide correct safety assessment.
g. KTR/Program Office does not have adequate technical experience to provide correct safety assessment.
h. KTR/Program Office does not have sufficient funding to correctly assess safety.
i. KTR/Program Office does not have sufficient manpower to correctly assess safety.
j. KTR/Program Office does not have sufficient time to correctly assess safety.

Scenario 2: KTR/Program Office provides inadequate safety assessment recommendations to the PSL.

b. KTR/Program Office communicates unsafe safety assessment recommendations to the PSL.

Scenario 3: KTR/Program Office assumes that incorrect safety assessment recommendations are adequate.

d. PSL does not provide feedback about the adequacy of safety assessment recommendations causing KTR/Program Office to assume that the PSL has incorporated sufficient safety measures.
e. PSL provides incorrect feedback about the adequacy of safety assessment recommendations causing KTR/Program Office to believe that the PSL has incorporated sufficient safety measures.
f. KTR/Program Office misinterprets feedback and believes that the safety assessment recommendations are adequate when they are not.

Scenario 4: PSL incorporates unsafe safety assessment recommendations.

b. PSL assume that the safety assessment recommendations are safe when they are not.

Unsafe Control Action for KTR/Program Office: Safety assessment provided late in or after review process. (CA: Provide Safety Assessment)

Controlled Process: Hazard analysis by PSL

Scenario 1: Policies do not require safety assessment from the KTR/Program Office prior to entering the safety review cycle.

b. The possibility of a safety constraint violation due to insufficient information provided to reviewers from the KTR/Program Office is not recognized and requirements for key information are not written into policy.

Scenario 2: KTR/Program Office provides safety assessment recommendations that lead to the violation of safety constraints or change assessed risk levels after reviewers have completed their review.

c. Due to other priorities, the KTR/Program Office is unable to provide a timely safety assessment but allows the safety package to enter planning and review.
d. Safety recommendations are provided after the safety package has been partially or completely reviewed.

Scenario 3: KTR/Program Office assumes that safety assessment recommendations will not adversely affect safety.

c. KTR/Program Office perceives that providing safety assessment recommendations out of sequence will increase safety rather than reduce safety.
d. Unsafe recommendations may go undetected and no feedback to the KTR/Program Office will be provided.

Scenario 4: PSL incorporates safety assessment recommendations that lead to the violation of safety constraints.

c. PSL incorporates safety assessment recommendations that lead to the violation of safety constraints from KTR/Program Office after safety reviewers have reviewed and approved.
d. PSL incorrectly interprets safety assessment recommendations from KTR/Program Office and incorporates them in a way that may lead to the violation of safety constraints after reviewers have reviewed and approved.

Unsafe Control Action for KTR/Program Office: Safe test point conditions not provided to PSL. (CA: Provide Safety Release)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

f. KTR/Program Office does not have the required technical data to determine safe test conditions.
g. KTR/Program Office does not have adequate technical experience to determine safe test conditions.
h. KTR/Program Office does not have sufficient funding to determine safe test point conditions
i. KTR/Program Office does not have sufficient manpower to determine safe test point conditions.
j. KTR/Program Office does not have sufficient time to determine safe test point conditions.

Scenario 2: KTR/Program Office does not provide safety release to the PSL.

b. KTR/Program Office does not effectively communicate safety release to the PSL.

Scenario 3: KTR/Program Office assumes that the PSL has incorporated safe test conditions into the safety package.

d. PSL provides no feedback about planned test conditions causing KTR/Program Office to assume that the PSL has incorporated sufficiently safe test points.
e. PSL provides incorrect feedback about planned test conditions causing KTR/Program Office to believe that the PSL has incorporated sufficiently safe test points.
f. KTR/Program Office misinterprets feedback and believes that the PSL safe test conditions when PSL has not.

Scenario 4: PSL does not incorporate safe test point conditions into the safety package.

e. PSL does not receive safe test point condition guidelines.
f. PSL overlooks safe test point condition guidelines.
g. PSL ignores safe test point condition guidelines.
h. PSL misinterprets safe test point condition guidelines.

Unsafe Control Action for KTR/Program Office: Unsafe test conditions provided to PSL. (CA: Provide Safety Release)

Controlled Process: Hazard analysis by PSL

Scenario 1: KTR/Program Office technical data and technical experience are insufficient.

f. KTR/Program Office does not have the required technical data to correctly determine safe test conditions.
g. KTR/Program Office does not have adequate technical experience to correctly determine safe test conditions.
h. KTR/Program Office does not have sufficient funding to correctly determine safe test point conditions
i. KTR/Program Office does not have sufficient manpower to correctly determine safe test point conditions.
j. KTR/Program Office does not have sufficient time to correctly determine safe test point conditions.

Scenario 2: KTR/Program Office provides unsafe test conditions to the PSL.

b. KTR/Program Office communicates unsafe test conditions to the PSL.

Scenario 3: KTR/Program Office assumes that unsafe test conditions are safe.

d. PSL does not provide feedback about the safety of the test conditions causing KTR/Program Office to assume that the PSL has incorporated sufficiently safe test points.
e. PSL provides incorrect feedback about the safety of the unsafe test conditions causing KTR/Program Office to believe that the PSL has incorporated sufficiently safe test points.
f. KTR/Program Office misinterprets feedback and believes that the test conditions are safe when they are not.

Scenario 4: PSL incorporates unsafe test conditions into the safety package.

b. PSL assumes that the test conditions are safe when they are not.

PSL

Unsafe Control Action for PSL: Potential safety constraint violations not analyzed and mitigated. (CA: Analyze and Mitigate Potential Safety Constraint Violations)

Controlled Process: Hazard analysis by PSL

Scenario 1: PSL technical data, technical experience, and guidance are insufficient.

d. PSL does not have the required technical data from the KTR/Program Office or the Technical Library to identify safety constraints, how they might be violated, and how to avoid violating them.
e. PSL does not have adequate technical experience to identify safety constraints, how they might be violated, and how to avoid violating them.
f. PSL does not have enough guidance from technical experts to identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 2: PSL does not identify safety constraints and how they might be violated.

c. The hazard analysis process is inadequate to identify safety constraints, how they might be violated, and how to avoid violating them.
d. The PSL has insufficient time to identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 3: PSL assumes that past testing is representative of current tests.

b. PSL applies identical or similar safety constraints and mitigating procedures as previous tests when the previous test safety planning is inadequate or does not apply to current testing.

Scenario 4: PSL does not identify potential safety constraint violations.

b. PSL overlooks potential safety constraint violations during analysis.

Unsafe Control Action for PSL: Incorrect analysis or mitigation of potential safety constraint limitations. (CA: Analyze and Mitigate Potential Safety Constraint Violations)

Controlled Process: Hazard analysis by PSL

Scenario 1: PSL technical data, technical experience, and guidance are insufficient.

d. PSL does not have the required technical data from the KTR/Program Office or the Technical Library to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
e. PSL does not have adequate technical experience to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
f. PSL does not have enough guidance from technical experts to correctly identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 2: PSL does not correctly identify safety constraints and how they might be violated.

c. The identification process is inadequate to correctly identify safety constraints, how they might be violated, and how to avoid violating them.
d. The PSL has insufficient time to correctly identify safety constraints, how they might be violated, and how to avoid violating them.

Scenario 3: PSL assumes that past testing is representative of current tests.

b. PSL applies identical or similar safety constraints and mitigating procedures as previous tests when the previous test safety planning is inadequate or does not apply to current testing.

Scenario 4: PSL does not correctly analyze potential safety constraint violations.

d. PSL overlooks potential safety constraint violations during analysis.
e. PSL misunderstands how safety constraints can be violated.
f. PSL applies mitigating procedures that cause safety constraint violations.

Contextual Factors Affecting Project Safety Planning

History: KTR/Program Office engineers and the PSL may employ techniques for safety analysis based on precedence however, they may be inadequate. Historical data may be used in determining safety constraints or mitigation measures but they may not be applicable to current testing.

Resources: Inadequate time, manpower, money, expertise, or information may be factors that cause KTR/Program Offices or the PSL to perform safety analysis and mitigation inadequately.

Tools and Interface: Inadequate tools for performing hazard analysis could result in potential safety constraint violations being overlooked or not sufficiently managed.

Training: KTR/Program Office engineers or the PSL may be inadequately trained on the systems under test or in safety analysis techniques leading to inadequately identified potential violations of safety constraints.

Pressures: Pressures to meet deadlines may limit KTR/Program Office engineer or PSL's ability to thoroughly analyze safety for test planning.

Safety Culture: A weak safety culture may cause the KTR/Program Office or the PSL to inadequately prioritize and perform safety analysis.

Communication: Inadequate communication and collaboration between the PSL and the KTR/Program Office could lead to misunderstandings about the existence of potential violations of safety constraints, appropriate ways to manage them, or whether they have been considered in safety planning. Inadequate communication of requirements and deadlines may also contribute to the KTR/Program Office engineers not providing safety analysis information on time.

APPENDIX D: COMPARISON OF AFFTCI 91-105 REQUIREMENTS TO STPA REQUIREMENTS

The following table provides a mapping between the AFFTCI 91-105 requirements and the STPA derived requirements. The comparison is not exact because in some cases, AFFTCI 91-105 provided requirements that were more specific. The STPA Step 2 analysis, based on the STPA requirements, can be easily used to derive a complete set of specific requirements that would be inclusive of the AFFTCI 91-105 requirements.

Process Under Control	**Controller**	**AFFTCI 91-105 Requirement**	**STPA Requirement**
Approval	Safety Reviewers (including approval authority)	Prior to delivering test package to the next official, all coordination comments should be answered to the satisfaction of the requestor	Reviewer must not provide approval for safety packages before prior reviewer feedback to the PSL is incorporated
Approval	Safety Reviewers (including approval authority)	Review and approve applicable test safety planning documentation	Reviewer must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
Approval	Unit/CC	Support AFTC test safety process in operations or for independent safety review	Unit/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items. Unit/CC must rescind approval to test if test has an unexpected result

Final Safety Review	AFTC/SET	Approve or disapprove safety reviewers	AFTC/SET must select qualified safety review board members to particpate in the safety review board meeting.
Final Safety Review	AFTC/SET	Ensure that final safety review prerequisites are complete	AFTC/SET must not conduct the safety review board meeting too early (before prerequisites are complete).
Final Safety Review	AFTC/SET	Provide opening remarks and expectations	AFTC/SET must provide safety review board meeting guidance to safety review board members. AFTC/SET must not provide safety review board meeting guidance that detracts from a focus on safety.
Final Safety Review	PSL	Develop list of proposed safety reviewers	Controlled by AFTC/SET

Final Safety Review	PSL	Brief test project and answer questions to safety review board	AFTC/SET must not provide approval for safety packages that have not met the requirements for safety planning and independent safety review. Tech Experts/Ops Reps must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
Final Safety Review	PSL	Update safety planning & resolve action items	Reviewers must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items
Final Safety Review	Safety Review Board	Perform risk assessment; assess overall risk of the test or activity	Tech Experts/Ops Reps must not understate the risk assessment provided to AFTC/SET.
Final Safety Review	Safety Review Board	Review applicable test & safety planning documentation	AFTC/SET must not provide approval for safety packages that have not met the requirements for safety planning and independent safety review. Tech Experts/Ops Reps must not provide approval

			for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
Final Safety Review	Safety Review Board	Provide action items, coordination comments, and other recommendations regarding safety planning	AFTC/SET must not provide approval for safety packages that have not met the requirements for safety planning and independent safety review. Tech Experts/Ops Reps must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
Project Safety Planning	AFTC/SE; AFTC/SET	Maintain administrative control of test safety planning resources	PSL must analyze and mitigate potential safety constraint violations (See Scenario 1 for this control action from STPA Step 2). PSL must not incorrectly analyze or mitigate potential safety constraint violations (See Scenario 1

			for this control action from STPA Step 2).
Project Safety Planning	AFTC/SE; AFTC/SET	Safety packages will be archived after approval	PSL must analyze and mitigate potential safety constraint violations (See Scenario 1 for this control action from STPA Step 2). PSL must not incorrectly analyze or mitigate potential safety constraint violations (See Scenario 1 for this control action from STPA Step 2).

Project Safety Planning	KTR	Supporting documents should be attached to safety package (provided by KTR)	KTR/Program Office must provide a safety assessment. KTR/Program Office must not provide an incorrect safety assessment. KTR/Program Office must not provide a safety assessment late in or after the safety package review process. KTR/Program Office must provide safe test conditions. KTR/Program Office must not provide unsafe test conditions.
Project Safety Planning	PSL	Evaluate risk and propose overall risk level	Controlled by Tech Experts/Ops Reps
Project Safety Planning	PSL; KTR; Test Team	Allocate sufficient time and resources to complete AFTC Test Safety Review process	"Just as in previous levels of control, inadequate time, manpower, money, expertise, or information may be factors that cause KTR/Program Offices or the PSL to perform safety analysis and mitigation inadequately."

Project Safety Planning	PSL; KTR; Test Team	Identify test unique hazards	KTR/Program Office must provide a safety assessment. KTR/Program Office must not provide an incorrect safety assessment. KTR/Program Office must not provide a safety assessment late in or after the safety package review process. KTR/Program Office must provide safe test conditions. KTR/Program Office must not provide unsafe test conditions. PSL must analyze and mitigate potential safety constraint violations. PSL must not incorrectly analyze or mitigate potential safety constraint violations.

Project Safety Planning	PSL; KTR; Test Team	Mitigate test unique hazards	KTR/Program Office must provide a safety assessment. KTR/Program Office must not provide an incorrect safety assessment. KTR/Program Office must not provide a safety assessment late in or after the safety package review process. KTR/Program Office must provide safe test conditions. KTR/Program Office must not provide unsafe test conditions. PSL must analyze and mitigate potential safety constraint violations. PSL must not incorrectly analyze or mitigate potential safety constraint violations.

Project Safety Planning	AFTC/SE; AFTC/SET	Provide test safety training courses	KTR/Program Office engineers or the PSL may be inadequately trained on the systems under test or in safety analysis techniques leading to inadequately identified potential violations of safety constraints.
Safety Package Preparation	Senior Leadership Reviewers	PSL should conduct approval briefing if required	Reviewer must provide action items to the PSL if safety planning is inadequate. Reviewer must not provide action items that lead to the violation of safety constraints to the PSL. Reviewer must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.

Safety Package Preparation	AFTC/SE; AFTC/SET	Provide guidance and assistance to project personnel	AFTC/SET must provide action items to the PSL if safety planning is inadequate. AFTC/SET must not provide action items that lead to the violation of safety constraints to the PSL. AFTC/SET must not provide action items that lead to the violation of safety constraints to the PSL after follow-on reviewers have reviewed the safety package.
Hazard Analysis	PSL	Prepare safety package	PSL must analyze and mitigate potential safety constraint violations. PSL must not incorrectly analyze or mitigate potential safety constraint violations

Hazard Analysis	PSL; KTR; Test Team	Consider test approach or build-up (mitigating procedure)	KTR/Program Office must provide a safety assessment. KTR/Program Office must not provide an incorrect safety assessment. KTR/Program Office must not provide a safety assessment late in or after the safety package review process. KTR/Program Office must provide safe test conditions. KTR/Program Office must not provide unsafe test conditions. PSL must analyze and mitigate potential safety constraint violations. PSL must not incorrectly analyze or mitigate potential safety constraint violations.

Safety Review Process Policy	AFTC/CC	Waive requirements of instruction if needed	AFTC/CC must not issue waivers to 412 TW/CC that violate safety constraints. AFTC/CC must not issue waivers to AFTC/SE that violate safety constraints.
Safety Review Process Policy	AFTC/SE; AFTC/SET	Set policy, provide updated policy information, and maintain integrity of test safety review process to ensure independent reviews	AFTC/SE must provide policy for safety risk mitigation and acceptance to 412 TW/CC. AFTC/SE must not provide inadequate policy for safety risk management and acceptance to 412 TW/CC. AFTC/SE must update existing safety policy for 412 TW/CC before it becomes obsolete. AFTC/SE must provide policy for safety risk mitigation and acceptance to AFTC/SET. AFTC/SE must not provide inadequate policy for safety risk management and acceptance to AFTC/SET.

			AFTC/SE must update existing safety policy for AFTC/SET before it becomes obsolete. AFTC/SE must not provide modified policy guidance that weakens the safety process to AFTC/SET. AFTC/SE must rescind modified policy guidance issued to AFTC/SET as soon as its use is no longer justified.
Safety Review Process Policy	AFTC/SE; AFTC/SET	Maintain AFFTCI 91-105	AFTC/SE must update existing safety policy for 412 TW/CC before it becomes obsolete. AFTC/SE must update existing safety policy for AFTC/SET before it becomes obsolete.

Safety Review Process Policy	AFTC/SE; AFTC/SET	Collect feedback on policy	AFTC/SE must update existing safety policy for 412 TW/CC before it becomes obsolete. AFTC/SE must update existing safety policy for AFTC/SET before it becomes obsolete.
Safety Review Process Policy	Unit/CC	Ensure test team compliance with safety policy	Unit/CC must not provide approval for safety packages without providing sufficient feedback to the PSL or verifying the closure of action items.
Safety Review Process Policy	Unit/CC	Allocate resources to support test safety review process	"Just as in previous levels of control, inadequate time, manpower, money, expertise, or information may be factors that cause KTR/Program Offices or the PSL to perform safety analysis and mitigation inadequately."

APPENDIX E: ACRONYM LIST

412 TW/CC – 412 Test Wing Commander

412 TW/CZ – 412 Test Wing Technical Director

AFFTCI – Air Force Flight Test Center Instruction

AFMC – Air Force Materiel Command

AFTC – Air Force Test Center

AFTC/CC – Air Force Test Center Commander

AFTC/CZ – Air Force Test Center Technical Director

AFTC/SE – Air Force Test Center Chief of Safety

AFTC/SET – Air Force Test Center System Safety Representative

CA – Control Action

KTR – Contractor

PSL – Project Safety Lead

SRB – Safety Review Board

STAMP – Systems-Theoretic Analysis and Processes

STPA – Systems Theoretic Process Analysis

Tech Experts/Ops Reps – Technical experts and operations representatives

Unit/CC – Test Unit Commander

Unit/CE – Test Unit Chief Engineer

UTSO – Unit Test Safety Officer

BIBLIOGRAPHY

[1] N. Leveson, *Engineering a safer world systems thinking applied to safety*. Cambridge, Mass: MIT Press, 2011.

[2] Air Force Test Center, "Air Force Test Center Fact Sheet." 07-Aug-2013.

[3] P. Checkland, *Systems thinking, systems practice*. Chichester [Sussex] ; New York: J. Wiley, 1981.

[4] H. W. Heinrich, *Industrial accident prevention: a safety management approach*, 5th ed. New York: McGraw-Hill, 1980.

[5] F. E. Bird and G. L. Germain, *Damage control; a new horizon in accident prevention and cost improvement, by Frank E. Bird, Jr. and George L. Germain*. [New York] American Management Association [1966], 1966.

[6] F. E. Bird, *Management Guide to Loss Control*. Intl Loss Control Inst, 1974.

[7] J. T. Reason, *Human error*. Cambridge [England] ; New York: Cambridge University Press, 1990.

[8] AF/SEF, "AFI 91-204 Safety Investigations and Reports." Air Force Safety Office, 08-Apr-2013.

[9] J. T. Reason, *Managing the risks of organizational accidents*. Aldershot, Hants, England ; Brookfield, Vt: Ashgate, 1997.

[10] AFFTC/SET, "AFFTCI 91-105: AFFTC Test Safety Review Process." Air Force Flight Test Center, 25-Jul-2012.

[11] M. V. Stringfellow and I. of T. Massachusetts, *Accident analysis and hazard analysis for human and organizational factors*. 2010.