Safety in US Air Force Tandem Seat Pilot Training Applying STAMP Processes

By

Adam Munekata

Bachelor of Science in Aeronautical Engineering
The United States Air Force Academy, 2020

Submitted to the Aeronautics and Astronautics Dept. in Partial Fulfillment of the Requirements for the Degree of.

Master of Science in Aerospace Engineering

At the
Massachusetts Institute of Technology

May 2022

© 2022 Adam Munekata
All rights reserved

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature of Author ______________________________
Department of Aeronautics and Astronautics
May 17, 2022

Certified by ______________________________
Nancy G. Leveson, Ph.D.
Thesis Supervisor
Department of Aeronautics and Astronautics.

Accepted by______________________________
Jonathan P. How
R. C. Maclaurin Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

Safety in US Air Force Tandem Seat Pilot Training Applying STAMP Processes

By

Adam T. Munekata

Submitted to the Department of Aeronautics and Astronautics on May 17, 2022 in partial fulfillment of the requirements for the degree of Master of Science in Aerospace Engineering.

ABSTRACT

The complexity and sophistication of modern systems pose many challenges for conventional accident and hazard analysis techniques. Although these methods have proven to be reliable on systems in the past, these methods often lack context, are subject to impartiality, and fail to approach systems holistically. System-Theoretic Accident Model and Process (STAMP) addresses these challenges and helps to identify how unsafe control actions can lead to hazards.

This thesis applies (STAMP) principles to an accident assessment and hazard analysis of tandem seat pilot training in the United States Air Force (USAF). The USAF Safety investigation board (SIB) process has gained valuable insight from accidents in the past; however, it suffers from the shortcomings mentioned above.

Northrup Grumman's T-38 Talon is the advanced jet trainer that has been used by the USAF since the 1960s, soon to be replaced by Boeing's T-7 Red Hawk as early as 2023. Causal Analysis based on Systems Theory (CAST) is an accident analysis technique based on STAMP. CAST is applied to the USAF SIB Report of the recent Vance T-38 crash on 21 November 2019. The findings of the SIB report are compared with the findings of CAST. Recommendations are provided to improve the SIB process by applying STAMP principles.

System Theoretic Process Analysis (STPA) is a hazard analysis technique based on STAMP principles. STPA is applied to a hypothetical Next Generation Trainer since the specifications of the T-7 are not known. Recommendations are generated to improve safety, focusing primarily on the conflict of control authority between the instructor and student pilots. Design recommendations and suggestions are provided for the next generation trainer to address concerns that may have been overlooked in preliminary hazard analysis.

Thesis Supervisor: Nancy G. Leveson, Ph.D.
Title: Professor, Department of Aeronautics and Astronautics

ACKNOWLEDGEMENTS

Far too many people deserve my gratitude for the unconditional support and guidance throughout the process. The following provided instrumental support to the completion of this work.

To Nancy Leveson, my thesis advisor and pioneer in the field: I cannot thank you enough for the continued patience and guidance throughout this thesis. Thank you so much for all your technical expertise, hours of feedback, and allowing me to pursue a topic I am passionate about. I'm beyond proud to say I was a student of yours.

The System Safety Lab Group gave instrumental feedback throughout the entire process. Many thanks to the past and present members of the group, specifically John Thomas, Bill Young, Michael Schmidt, Andrew Kopeikin, Elias Johnson, Alex Hillman, Justin Poh, Elizabeth Baker, Lawrence Wong, Sam Yoo, and Dro Gregorian.

To the Engineering Systems Lab, who provided incredible support and adaptation during the pandemic.

I would like to thank my mom and dad for the continued support throughout my time at MIT and always providing emotional support when times were tough. Making you both proud will always be my biggest motivation.

The author is an active-duty military officer and acknowledges that the views expressed in this thesis are our own and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

DEDICATION

This report is dedicated to the friends and families who have lost a loved one in an accident related to flight training.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AETC	Air Education and Training Command
AFI	Air Force Instruction
AFMAN	Air Force Manual
ASEC	Aircraft Software Enabled Controller
ATC	Air Traffic Control
CA	Control Action
CAST	Causal Analysis based on Systems Theory
CRM	Cockpit/Crew Resource Management
CS	Causal Scenario
DoD	Department of Defense
DOE	Department of Energy
EFIS	Electronic Flight Instrument System
ENJJPT	Euro-NATO Joint Jet Pilot Training
ETA	Event Tree Analysis
FAA	Federal Aviation Administration
FCP	Front Cockpit
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
FTG	Flying Training Group
FTS	Flying Training Squadron
FTW	Flying Training Wing
GLOC	G Induced Loss of Consciousness
GPS	Global Positioning System
HMA	Higher Mission Authority
IAW	In Accordance With
IP	Instructor Pilot
LMA	Lower Mission Authority
MA	Mishap Aircraft
MIL STD	Military Standard
MORT	Management Oversight, Risk Tree Analysis
MIP	Mishap Instructor Pilot

MSP	Mishap Student Pilot
NGT	Next Generation Trainer
NOTAM	Notice to Airmen
PF	Pilot Flying
PNF	Pilot Not flying
PRA	Probabilistic Risk Assessment
RCA	Root Cause Analysis
RCP	Rear Cockpit
RM	Recommended Mitigation or Risk Management
RMU	Radio Management System
SIB	Safety Investigation Board
SII	Special Interest Item
SP	Student Pilot
SRF	Squadron Read File
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TO	Technical Order
UCA	Unsafe Control Action
UPT	Undergraduate Pilot Training
USAF	United States Air Force

1. INTRODUCTION

This thesis applies System-Theoretic Accident Model and Process (STAMP) modeling to tandem seated pilot training in the United States Air Force (USAF) related to system safety and accident processes. This thesis outlines the current procedures and methods used in the USAF for safety practices and recommends STAMP augmentation to create a more comprehensive risk assessment approach. It applies STAMP to a hypothetical future tandem seated jet trainer as a test case.

Worldwide aviation is an immensely complex system. Current safety and accident investigation processes no longer have the scope necessary to handle them. A holistic approach is needed. Approaching USAF pilot training from a systemic perspective offers a deeper understanding of where safety improvements can be implemented. This chapter outlines the motivation, scope, research question, and structure of the thesis.

1.1. Scope

This thesis holistically analyzes the system and factors at play in the USAF's UPT. It includes the following:

1. A CAST analysis of the 2019 T-38 accident at Vance AFB compared to the USAF AIB's investigation published on 4 February 2020.
2. A dedicated System Theoretic Process Analysis (STPA) of a tandem seated jet trainer focusing on the unique interactions between pilot instructors and student pilots. The trainer will be a hypothetical next-generation jet trainer with improved software capabilities.
3. Recommendations for UPT. Recommendations will be tailored for a next-generation trainer, such as the soon-to-be commissioned T-7.

This thesis expands beyond the factors directly related to the accident. The effort is an independent analysis of the implications of the many sociotechnical pressures on the USAF at an organizational level, the mission and qualifications given at the Wing and Squadron levels, and exploration into the human factors regarding instructor and student pilots.

1.2. Problem Definition

The following question helps to frame the approach and define the scope of this thesis:

How can STAMP be applied to address the unique challenges faced in tandem seated pilot training?

The Air Force has taken many different approaches to mitigate risk in UPT. However, accidents continue to occur. This thesis introduces a systemic approach to safety in UPT. The goal is to help prevent accidents as military aviation becomes increasingly complex and automated.

> *AVIATION SAFETY. We will not compromise safety as we prepare our airmen and align resources for great power competition. Last year, the Air Force experienced an uncharacteristic increase in inflight mishaps and fatalities for manned aircraft. The safety of our Airmen remains a top priority, so we initiated several actions to bolster our mishap prevention programs, including additional safety training and operational pauses to discuss risk.*

SECAF Dr. Heather Wilson and Gen David L. Goldfein

USAF Posture Statement: Fiscal year 2020 [2]

Although there have been some independent approaches to address the Safety Investigation Board Process, there have not been many independent approaches attempting to investigate tandem seated pilot training. Existing analysis of the T-38C examines the aircraft's structural integrity (Finite Element Analysis) and aerodynamics (Computational Fluid Dynamics). Pilot training safety has been investigated in the commercial space, but although jet training has similarities, some glaring differences make it unique from commercial training. Furthermore, there has never been an analysis of the UPT program.

1.3. Thesis Structure

This thesis begins with defining the problem facing UPT and outlining the many sociotechnical pressures facing UPT and how that impacts many flight instructors. Chapter 2 provides an overview of pilot training, background on current analysis techniques, safety practices in the USAF, and STAMP. Chapter 3 is a Causal Analysis based on Systems Theory (CAST) of a recent tandem jet training accident. Chapter 4 is a System Theoretic Process Analysis (STPA) of a hypothetical next-generation tandem jet trainer. The thesis concludes with chapter 6, summarizing the research and suggesting areas of future work.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

2. BACKGROUND

2.1. Pilot Training in the USAF

Training takes many forms across different industries. However, training operators for sophisticated systems or heavy machinery distinguishes itself from other training modes. It frequently involves instructors immersing themselves in on-the-job training with students. Common examples include driver's education, heavy construction equipment, and flight training. This analysis will focus on tandem flight training for the USAF.

The USAF is known for its cutting-edge technology, where systems and aircraft are the most sophisticated and autonomous that they have ever been in history. As technology has evolved, the complexity behind each system has dramatically increased, and the human operator's role has evolved. Looking past the design choices of fourth-generation (Lockheed's F-16 Fighting Falcon and McDonnel Douglas's F-15 Eagle) and fifth-generation fighters (Lockheed's F-22 Raptor and F-35A Lightning II), the fifth-generation fighters apply a high degree of augmentation and autonomy never seen before in previous generations of aircraft. Highly augmented/autonomous systems are accompanied by equally dramatic shifts in the role of the human operator.

In 2018 the Department of Defense (DoD) reported to the congressional armed services committee on initiatives for mitigating military pilot shortfalls [1]. The report found that in 2018, the DoD faced a shortfall of more than 3,000 pilots, and all branches experienced pilot shortfalls due to underproduction in pilot training and reduced aircraft readiness. The report also found increased attrition of experienced pilots as the commercial aviation industry faced a global supply shortage for commercial pilots.

Pilot training reports have noted sub-par training volume for producing pilots and decreased aircraft material readiness—each factor contributing to the time required to train new aviators. Further concerns such as lack of sufficient flight time per pilot, extended and frequent deployments, and other quality of life concerns for aviators have added to pilot recruitment and acquisition difficulty. Once enough hours are accrued over their service commitment (a minimum of 10 years after pilot training ~1000 hours), they can then compete for a commercial job once their commitment is finished. This often leaves the Air Force understaffed in many aviation areas, including instructor pilots.

The pilot shortage extends beyond the military. The demand for pilots in the United States' commercial industry places a lot of pressure on the USAF. The report estimates that training for a mission-ready fighter pilot can take up to 5 years and cost between $3 and 11 million [1]. Around the 8-10-year commitment period, many military aviators analyze their alternatives for a civilian lifestyle. Airline compensation packages and greater control over one's work schedule seem to be the primary drivers of pilot attrition.

Air Education Training Command (AETC) is responsible for the pipeline that transforms civilians with little to no flying experience into capable operators of these highly complex systems. Although the USAF has continually adapted its training syllabus for years, the aircraft used to train pilots for fourth and fifth-generation fighters alike is decades old. Northrup's T-38 Talon has served in the Air Force as the premier supersonic jet trainer since the 1960s, before the development of the F-16 and F-15. The T-38 has actively been used through three different generations of fighter aircraft with numerous technological advancements. Although proven to stand the test of time, the asymmetric evolution of the aircraft these pilots are being trained to operate poses many problems going forward. The USAF's solution to this is the development of Boeing's T-7 Redhawk to be the next generation fighter trainer.

The USAF's UPT program is divided up into three phases. Phase 1 consists of academic classes that include aerospace physiology, altitude chamber training, ejection seat/egress training, parachute procedures, aircraft systems class, introductory instruments class, mission planning, navigation, aviation weather, and initial flight training in a DA-20.

Phase 2 initiates primary aircraft training, which includes approximately 90 hours of flight training in the T-6 Texan II, basic flying skills, instrument rating, and formation flying. By the end of Phase 2, students select an advanced track based on performance for phase 3.

Phase 3 consists of two fixed-wing tracks: the fighter/bomber track flown in the T-38, or the airlift/tanker track flown in the T-1 Jayhawk. There is a second flight training program called Euro-NATO Joint Jet Pilot Training, which consists of all the elements of UPT; however, the only phase 3 track is T-38s. Tandem seated pilot training occurs on the fighter/bomber track in the T-6 and T-38.

Flight training is inherently dangerous. Training for single-seat supersonic aircraft (e.g., fighters) adds an increased level of risk. The high speeds at which these aircraft operate require operators to make decisions faster and think 'further ahead' of the aircraft. This is further complicated by the increasing complexity and sophistication of the operated aircraft. These aircraft operate at higher Mach numbers, have increased maneuverability, and have high degrees of augmentation and autonomy.

Instructors of these aircraft have refined their technique over hundreds of flying hours and have learned the common tendencies of many students. In theory, these operators should never get into accidents; however, this is not the case. The typical designation is human error; however, this assumption requires a deeper dive.

Assigning causal factors to operator error masks other systemic factors and conditions that may have contributed to unsafe human control actions. The apparent mitigation would be to remove the operator entirely from the system, which prompts questions about the role of the human operator in the context of aviation.

Standard accident causality models explain why accidents happen primarily by assigning a root cause or exclusively looking at proximal events. In present times, accidents in complex systems can rarely be attributed to a single 'root cause,' and the idea of designating a root cause hides other factors that could also need improvement. Rather than focusing on a 'root cause' or 'human error,' this thesis is designed to look at the system as a whole and the causal factors of the tandem seated flight training based on the application of systems theory.

2.2. Root Cause Analysis

There is no universally accepted definition of Root Cause Analysis (RCA); however, it is often used to describe processes and tools—such as 5 Whys, fishbone diagrams, causal factor trees, and logic trees, with the end goal of identifying root causes of faults and problems [3] [4]. The USAF references the Department of Energy as a baseline for performing RCA. outlines five phases of root cause investigation and reporting: Data Collection, Assessment, Corrective Actions, Inform, and Follow-Up [5].

Phase I Data Collection involves information taken before, during, and after the event, including personnel involvement, environmental factors, and any other relevant data. Phase II Assessment includes identifying the problem, identifying causes (using RCA methods), and finally identifying why these causes were in the previous step. The DOE references Event and Causal Factor Analysis, Change Analysis, Barrier Analysis, Management oversight, Risk Tree (MORT) Analysis, Human Performance Analysis, and Kepner-Tregoe Problem Solving and Decision Making as the most common RCA methods. Note that almost all the methods mentioned are at least 50 years old and many even older. They were created when engineering was creating very simple systems compared to today’s highly sophisticated, software-intense products. The causes of accidents have changed as our technology has changed.

Phase III Corrective Action implements actions to reduce the probability that an accident will occur and improve reliability and safety. Phase IV Inform reports the accident to the proper authorities, and finally, Phase V Follow-up determines the efficacy of the corrective actions [5].

The DOE outlines several categories in which each causal factor must be fitted. These include equipment/material problems, procedure problems, personnel error, design problems, training deficiency, management problems, or external phenomenon [5]. Each category also has subsections to further refine what the causal factor is categorized as.

The DOE does not specify a particular RCA method to use however any method used must follow the following basic steps [5]:

1. Identify the problem: the DOE notes that the problem should be unwanted conditions or actions that resulted in actuation. The actuation itself is not the problem.
2. Determine the significance of the problem: Severity, likelihood of recurrence, presence within the program, impact on safety culture, etc.
3. Identify the causes (conditions or actions) immediately preceding and surrounding the problem (the reason the problem occurred).
4. Identify the reasons why the causes in the preceding identification step existed, working back to the root cause.

The DOE defines the root cause as “the fundamental reason that, if corrected, will prevent recurrence of this and similar occurrences of this event” [5]. The following are summaries of common RCA methods.

Table 2-1: Summary of Root Cause Methods [5]

METHOD	WHEN TO USE	ADVANTAGES	DISADVANTAGES	REMARKS
Events and Causal Factor Analysis	Use for multi-faceted problems with long or complex causal factor chain.	Provides visual display of analysis process. Identifies probable contributors to the condition.	Time-consuming and requires familiarity with process to be effective.	Requires a broad perspective of the event to identify unrelated problems. Helps to identify where deviations occurred from acceptable methods.
Change Analysis	Use when cause is obscure. Especially useful in evaluating equipment failures.	Simple 6-step process.	Limited value because of the danger of accepting wrong, "obvious" answer.	A singular problem technique that can be used in support of a larger investigation. All root causes may not be identified.
Barrier Analysis	Use to identify barrier and equipment failures and procedural or administrative problems.	Provides systematic approach.	Requires familiarity with process to be effective.	This process is based on the MORT Hazard/Target Concept.
MORT/Mini-MORT	Use when there is a shortage of experts to ask the right questions and whenever the problem is a recurring one. Helpful in solving programmatic problems.	Can be used with limited prior training. Provides a list of questions for specific control and management factors.	May only identify area of cause, not specific causes.	If this process fails to identify problem areas, seek additional help or use cause-and-effect analysis.
Human Performance Evaluations (HPE)	Use whenever people have been identified as being involved in the problem cause.	Thorough analysis.	None if process is closely followed.	Requires HPE training.
Kepner-Tregoe	Use for major concerns where all spects need thorough analysis.	Highly structured approach focuses on all aspects of the occurrence and problem resolution.	More comprehensive than may be needed.	Requires Kepner-Tregoe training.

2.2.1. Event Chain Analysis

Modeling accidents as event chains is a common practice in many accident causality models (such as RCA). The premise of event chain analysis is that accidents occur via a sequential combination of conditions and events. The system needs to break the “chain” of events before a loss occurs to prevent accidents.

Common event chain methods include Heinrich’s Domino Model, Bird and Loftus’ Domino Model, Reason’s Swiss Cheese Approach, and adaptations of the prior mentioned. Heinrich’s Domino model was of the first accident causality models and identified five stages in accident causality in the following order: social environment and ancestry, the fault of a person, unsafe act or condition, accident, and finally, injury. The underlying assumption behind Heinrich’s Domino model is that each “domino” (stage) automatically knocks down the next “domino” unless a domino is removed to break the chain [6] [7]. Heinrich’s model was criticized for being too human error/blame-focused. Bird and Loftus modified the Domino Model based on this criticism. With the same premise as Heinrich’s model, Bird and Loftus’ model involved Management structure (objectives, organization, and operations), operational errors (management or supervisory behavior), tactical errors (human error), accidents, and finally, injury in that order [7].

James Reason’s Swiss cheese model bases accident causality on slices of Swiss cheese, where each slice of cheese represents a step in a process. Each step in the process has the potential for failure, and losses occur when each step fails. In Reason’s model, active failures are defined as “unsafe acts that directly contribute to the accident,” and latent failures are “conditions that exist that may lay dormant for a period of time until it leads to an accident” [6]. For accidents to occur, the failures (holes) must line up.

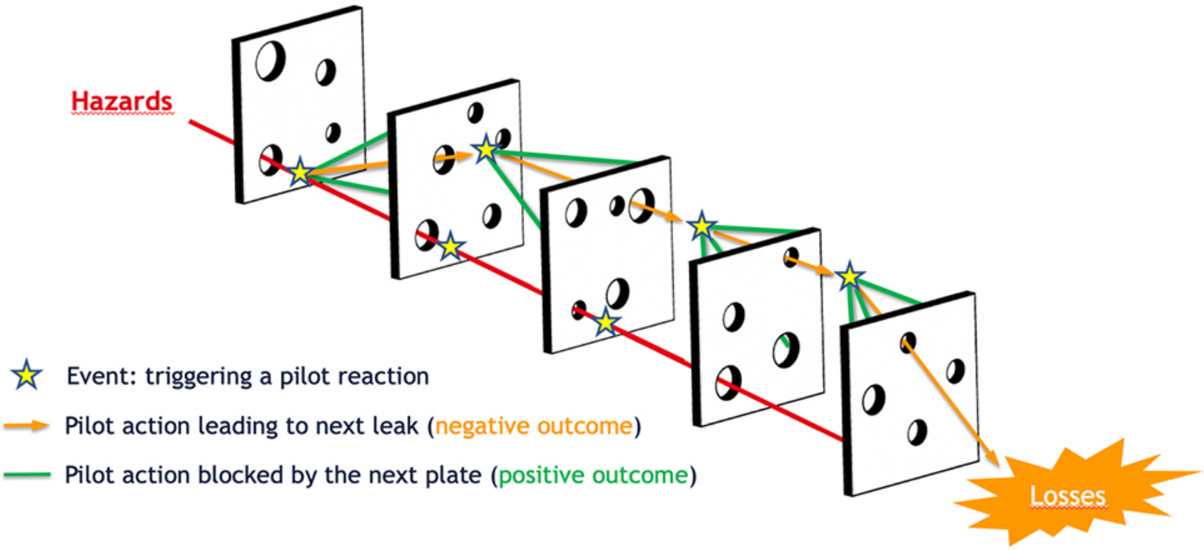


Figure 2-1: Swiss Cheese Model Applied to Aviation [8]

Note that all these models are really the same linear chain-of-events model with different analogies for the events (e.g., dominos or Swiss cheese slices). It goes back to a model of causality that is at least 100 years old.

2.2.2. Shortcomings of RCA and Event Chains

RCA attempts to establish the context necessary to determine why the actions or conditions lead to an accident. However, the premise of RCA inherently limits the scope of the analysis. Labeling a causal factor as a 'root cause' is subjective and contingent on the researcher's biases. Some causes can be labeled as direct, while others can be labeled as contributory with no real basis for the distinction [7]. Root causes can be selected due to familiarity, the event being the first in the chain that can be fixed or corrected, or for liability purposes.

This common practice omits causal factors further down in the sequence. And non-sequential events that lead to a loss are omitted altogether such as multiple events coming together randomly or circular causal loops, such as those involved in feedback.

In addition, the categorization in Phase II fails to account for the interaction between causal factors. The actual "cause" may lie in the interaction between two causes. Furthermore, an action or condition not considered a cause may be vital context to describe why another action or condition is deemed to be causal.

In Phase III, determining which RCA method to use is subject to bias. Figure 2-2 outlines the DOE's process in determining which RCA method to identify causal factors. By identifying the method to use before any causal factors have been identified, the researcher already has a preconception about what they think the causal factors will be. The DOE notes that multiple methods can be used depending on the issue's complexity. The selection of methods introduces foresight bias, which creates the context for the analysis and determines what will be considered. This practice ultimately limits the findings of the RCA.

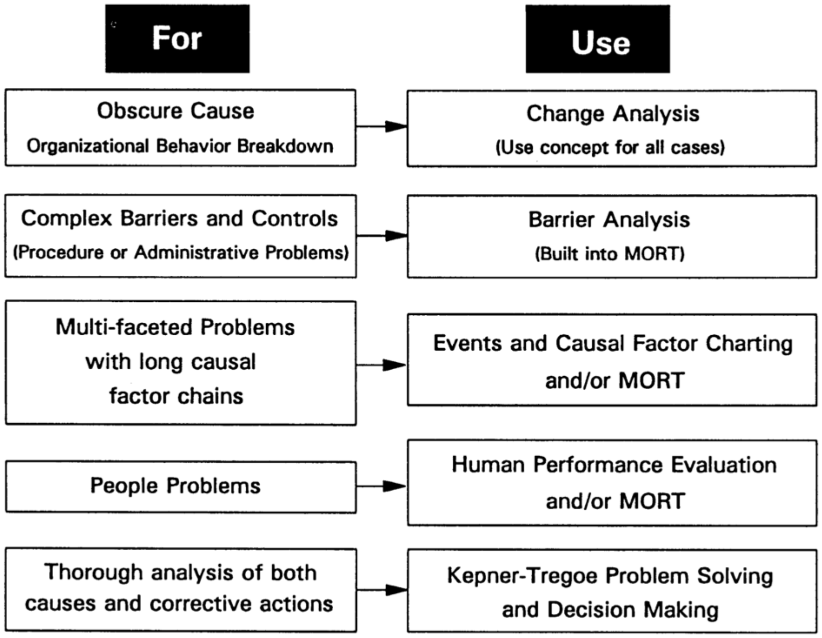


Figure 2-2: Summary of Root Cause Methods (Flow Chart) [5]

Event chains use a linear approach to accident causality; thus, nonlinear relationships are difficult to model [7]. Event chains specifically overlook system factors and are generally one-dimensional. Although Reason notes that each layer of protection involves a condition (context) and a latent or active failure, the model fails does not acknowledge control algorithms (decision-making processes for human operators), process models (mental models for human operators), feedback, or external influence amongst other considerations that add context to why decisions are made. The swiss cheese model also only propagates downstream the layers of protection. Feedback from downstream layers of protection may change a layer of protection's process model and thereby changing its action.

Neglecting the upstream flow of information is a symptom of a more significant concern with event chain causation models—the disregard of systemic factors. Systemic factors can include interactions between protection layers or influences of elements not deemed "protection layers" or part of the domino model that influences the behavior of system components. Although models such as the Swiss Cheese Model establish some context to determine accident causality, systemic factors and behavioral context cannot be ignored when dealing with modern and complex systems.

The assumption that accidents are caused by chains of events should be reshaped to reflect the "entire sociotechnical system" [7].

2.3. Accident Investigations in the United States Air Force

USAF safety and hazard reporting is conducted in accordance with (IAW) Air Force Instruction 91-204 [9]. AFI 91-204 defines the purpose of safety investigations as follows:

> *Safety investigations and reports are conducted and written solely to prevent future mishaps. Legal investigations are conducted for all other purposes. If initiated, criminal investigations*

> *take precedence over safety investigations until criminal activity, natural causes, and suicide have been ruled out as possible causes of damage, injury, or death.*

AFI 91-204, Section 1.1 [9]

Safety investigations fall into five categories: mishap, nuclear surety, incident, hazard, and safety study. For this analysis, the primary focus will be on mishap investigations.

Aviation-related mishaps [9], any mishap involving an aircraft or unmanned aerial system, follow IAW AFMAN 91-223 [10]. The aviation-related mishaps categories include flight, flight-related, and aviation ground operations. Flight mishaps are characterized by the intention of flight and damage to DoD aircraft during operation. Flight-Related involves the intent to fly and no reportable damage to the aircraft itself but consists of a fatality, injury, or property damage. Aviation Ground Operation mishaps include scenarios where the aircraft is the injury mechanism with no intent to fly.

A Safety Study is defined as:

> *… an in-depth analysis of two or more events to identify the root causes or hazards not previously identified utilizing AF safety investigation processes. Unlike other safety investigations, safety studies are not a single event. Any aggregate study, analysis, or aggregate safety investigation containing privileged safety information from other sources (privileged safety data and/or products of deliberative processes of safety investigators/ investigations) will be designated as a privileged safety product.*

AFI 91-204, Section 1.8 [9]

> *Aggregate studies use two or more similar events (mishaps, incidents, or hazards) to identify the root cause of a problem. Aggregate studies are used to make recommendations to mitigate hazards. Aggregate studies based on privileged safety data or products, or deliberative processes of the SIBs will be protected as privileged.*

AFI 91-204, Section 1.8.1 [9]

Privileged safety information is defined in Chapter 4 as “information that is exempt by case law from disclosure outside the DoD Safety Community” [9]. Only DoD personnel and certain contractors may access privileged information. Privileged safety information includes information given to investigators with a promise of confidentiality; any analysis, conclusions, or recommendations of the safety investigators; computer-generated animations, simulations, or reenactments used by a safety investigator or confidential witness statements that are incorporated; any graphics that reveal the deliberative process or analysis of the board; or any life sciences material that is a part of the analysis by a safety or life sciences investigator [9]. This analysis does **not** contain any privileged safety information.

Safety Investigations are conducted by Safety Investigation Boards (SIB) who “accomplish root cause analysis determining what factors led to an event, develop findings from those factors, and crafting recommendations” [9]. The information and evidence collected by the SIB are left exclusively for SIB uses. Determining and documenting factors involves weighing the investigator’s evidence, professional knowledge, and good judgment. These factors are shaped into recommendations to prevent future mishaps from happening again.

Section 8.5.1 defines a factor as “any deviation, out-of-the-ordinary or deficient action, or condition discovered in the course of an investigation that contributed to the eventual outcome” [9]. The investigator isolates determining factors (eliminating issues that were not factors) to focus the investigation on significant issues surrounding the event. The factors are “not mutually exclusive but often interrelated, and in some cases influence, each other” and are the basis for primary findings and help explain causes such as pilot error, supervision, or equipment failure [9]. This process is summarized in Figure 2-3.

Class A, B, and C mishaps must have at least one causal factor. SIBs are instructed to build a logical narrative of the event that includes specific references to technical orders (TO), publications, training, personnel actions, results of technical analysis, quotes from interviews, human factors, etc. [9]. AF 91-204 categorizes potential causal factors as actions, conditions, or publications. Actions are explained in the context of what an operator did during the mishap versus what should have been done. Conditions (weather or fatigue) are evaluated on how and why the condition influenced the accident. Finally, publications are analyzed for what guidance they provided at the time of the incident.

After analyzing the factors, the SIB decides whether an action was a factor or a causal factor. If a single factor cannot be defined as the most likely cause, the SIB identifies alternatives in the format “Action X most likely occurred due to one or more of the following reasons” in the order of the most probable to the least possible [9].

Non-Factors Worthy of Discussion include:

- Areas that were thoroughly investigated and subsequently ruled out as factors.
- Areas uncovered during the investigation that did not cause the event or influence the outcome but should be addressed to prevent future mishaps.
- Areas that may be considered an interesting item to the convening authority.

Section 8.5.3 states that the system’s program office should identify the hazard that played a role in the event sequence for system-related events. The program office should include an analysis of hazards that contributed to the mishap and recommendations for mitigations. In this context, the term ‘system’ refers to the aircraft (software and hardware included) used in the accident.

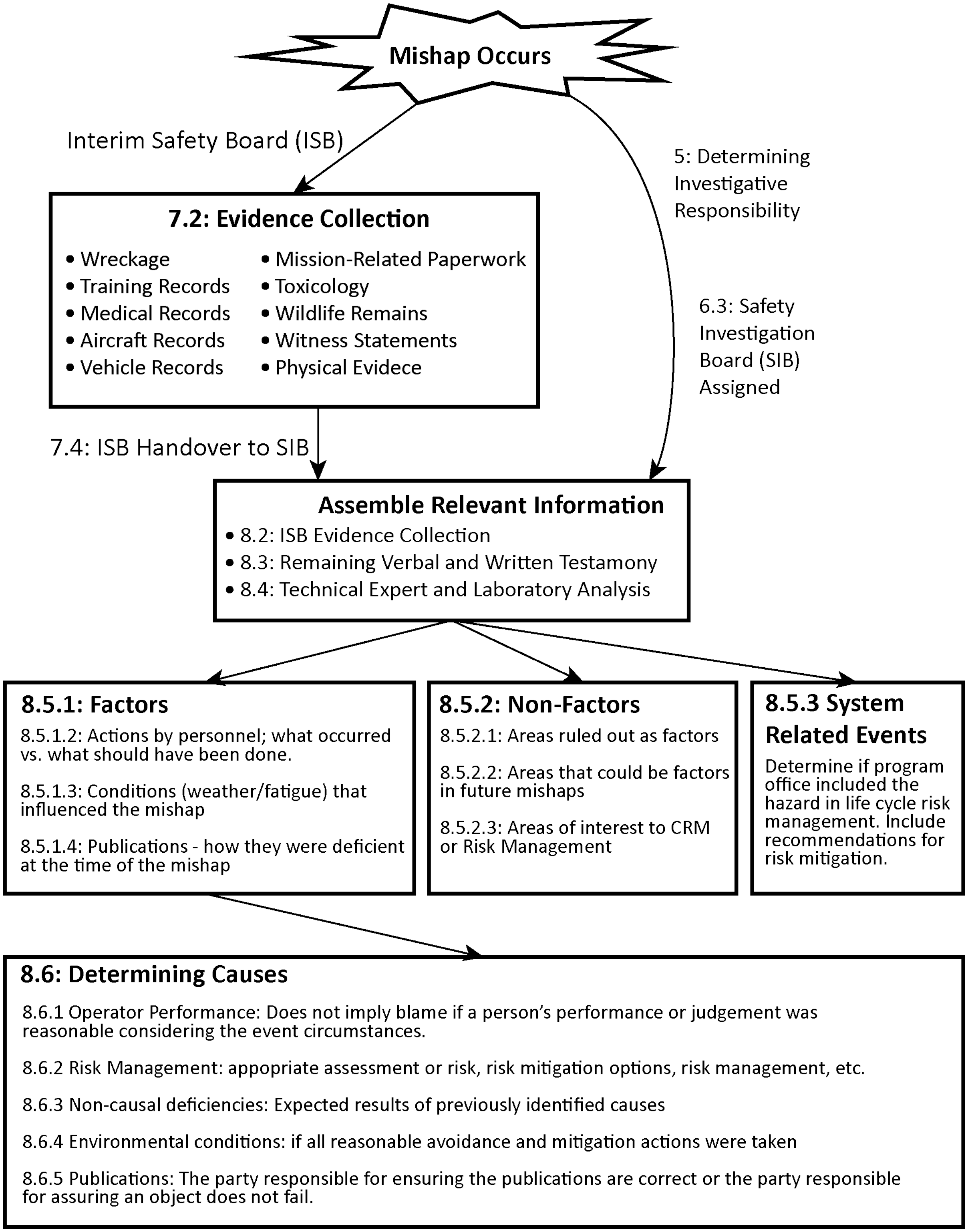


Figure 2-3: SIB Organization of Information and Causal Determination [9]

Section 8.6 defines a cause as "a deficiency which if corrected eliminated or avoided would likely have prevented or mitigated the event damage or injury" [9]. Most cases are correctable by human operators.

After factors and causes are documented, 'findings' summarize the event sequence of the mishap leading up to a cause in chronological order. Findings are written as single events or conditions relevant to the event sequence, supported by a factor (the factor which is backed by evidence).

Section 8.9 defines recommendations as "feasible and effective solutions to eliminate identified hazards, or if the hazard cannot be eliminated, to mitigate the hazard's potential consequences [9]. The recommendations should target one or more of the hazards identified during the investigation. The recommendations are then organized into an "order of precedence," prioritizing mitigations while providing alternatives. Other Recommendations of Significance are derived from Findings of Significance, derived from Non-Factors Worthy of Discussing [9]. Example outcomes of the SIB process are shown in Figure 2-4.

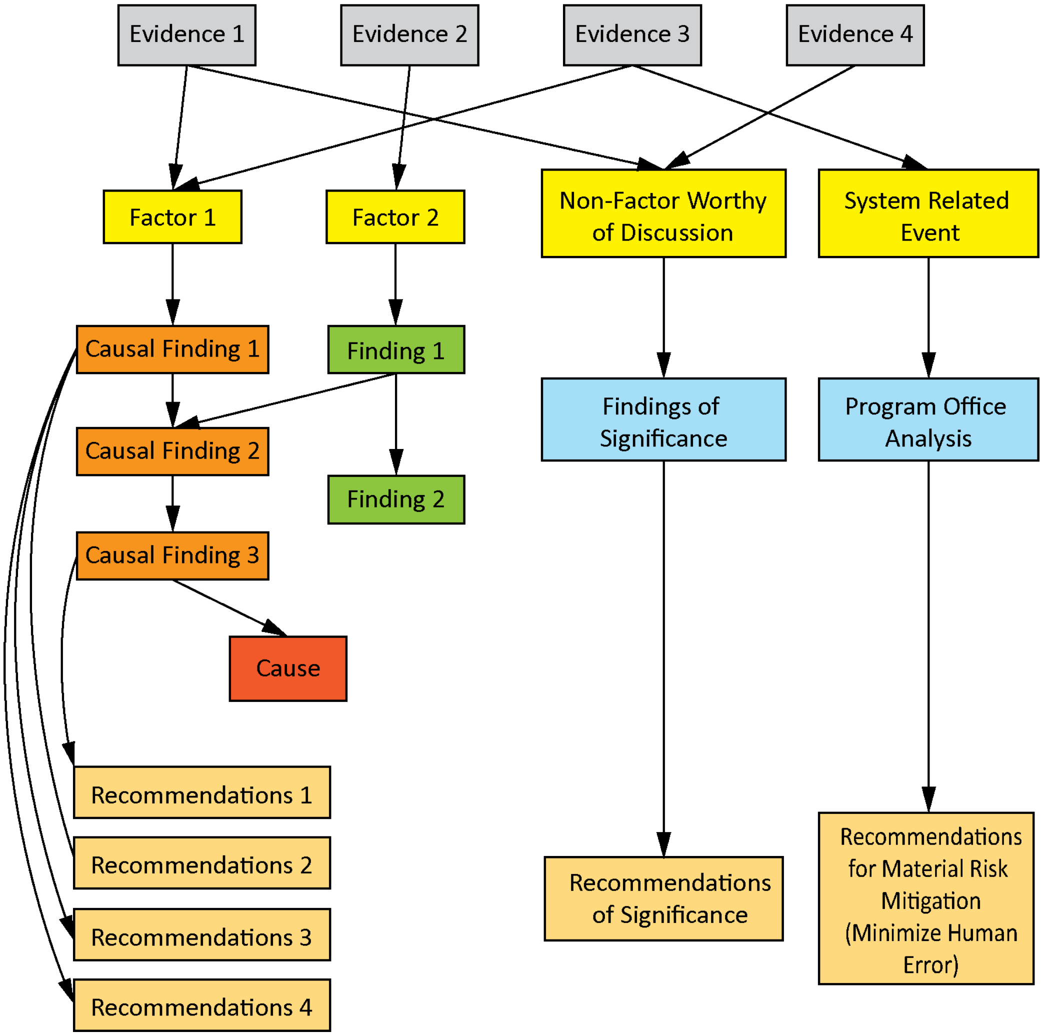


Figure 2-4: Example of Generating Recommendations in the USAF SIB Process

Follow-up actions are required by all appropriate parties and are independently evaluated to ensure program compliance. Safety offices are responsible for managing, updating, and closing recommendations [9]. Updates include any actions taken, results/problems of development or testing, delays, and any rationale supporting these decisions.

2.3.1. Shortcomings of the SIB Process

The USAF SIB process is an adaptation of RCA and modeling accident causation as event chains, thereby suffering from the same shortcomings as discussed in section 2.2.2. The SIB process has been influential for providing a straightforward approach to addressing mishaps in the USAF. Although the SIB process has served well in the past, weaknesses of the process have been brought to light in the past [11]:

- Impartiality: the board presidents conducting the investigations are Air Force Officers themselves. As a part of the Air Force, the board presidents are already subject to pre-existing organizational bias. The findings of the SIB process are also a direct reflection of what the individual has experienced in their career, which is subject to experience bias.
- Training: the senior officers conducting the safety investigations already have dedicated duties assigned to them. These officers lack time to be trained in safety practices and procedures. Lampela also notes that training for the SIB process takes away operational capacity from the responsibilities the officer was initially assigned to [11].

The SIB Process lacks clear traceability established from the stakeholders. Understanding the stakeholders is essential to identifying key losses or hazards in any safety analysis. Without establishing traceability from high-level hazards, recommendations have no basis for establishing a relationship to the stakeholders. Traceability also aids in adapting recommendations as the system changes or new systems are assimilated into procedures [7].

The SIB process excludes system-related events and the so-called ‘findings of significance’ from the recommendations in the final report. Because the recommendations of significance are not transferred to the final report, they are not tracked or held accountable for their improvements thereafter [12].

‘System’ in the context of the SIB process refers to the hardware and software associated with the mishap. This definition of a system excludes many factors that influence the outcomes of accidents. Hall and Fagan define a system as “a set of objects together with relationships between the objects and between their attributes” [13]. A system is characterized by a boundary that separates everything inside (the system) from everything outside (the environment) [14]. Even though the environment is outside the system, it still impacts system behavior in most cases. The objective of a system is to define the boundary such that the elements of the system serve the purpose of the analysis.

In the SIB’s definition of the system boundary, the exclusion of factors, such as regulation, management, human operators, software, etc., narrows the scope of the analysis and overlooks many essential interactions and relationships that influence software performance, human behavior, or even component failure. The inclusion of these elements is critical in handling the complexity of modern systems. In the context of accidents in aviation, the interaction between the operators and the aircraft has become more intricate with the inclusion of software-enabled controllers. The F-35 is commonly cited for having millions of lines of code both within the aircraft’s software controller and on the ground [15]. Software-human interfacing and integration are more relevant than ever in the history of the Air Force.

The SIB is vague and unspecific regarding how to determine if a human's actions are deemed 'causal.'. Section 8.6.1 specifies that a cause does not imply blame. If an operator's performance or judgment was reasonable in the context of the mishap, it is not appropriate to assign a cause [9]. This evaluation is highly subjective and contingent on the bias of the board president. The basis to which an individual's actions may seem reasonable in context is made more difficult due to the exclusion of 'non-factors worthy of discussion' and 'system-related events.' Eliminating context from the evaluation encourages the assignment of human error to the exclusion of a full explanation of why that error occurred and frequently overly narrows the scope of the analysis. Leveson writes that the old assumption that most accidents are caused by operator error must be reshaped to:

> *Operator behavior is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works.*

Leveson*, Engineering a Safer World pg. 47* [7]

In many systems, the role of software is to apply a predetermined set of rules and procedures to deal with a limited set of foreseen conditions [16]. If this were the case with humans, human error would be much more clear-cut. In contrast to software, humans primarily deal with unforeseeable conditions where predetermined rules and procedures may not apply. Humans have the capacity to adapt and be flexible (two essential attributes of instructor pilots). Although flexible judgment and decision making are the main benefits to humans as operators, human error is an inevitable side effect that occurs when attempts are made to diagnose and solve never before seen problems [16]. The SIB needs to shift the focus from the operators' actions to the contextual factors that shape operator behavior.

2.4. Hazard Analysis Techniques

Military Standard 882E (MIL-STD-882E) outlines the Department of Defense's approach to system safety. The standard defines a hazard as:

> *A real or potential condition that could lead to an unplanned event or series of events (i.e., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.*

MIL-STD-882E [17]

Eliminating or mitigating the hazards of a system to an acceptable amount of risk is the goal of system safety. Hazard analyses are used to identify the potential risks in a system by identifying hazards, hazard effects, and hazard causal factors [18]. Hazard analysis can be conducted at any stage of a system's development. The objective is to eliminate and mitigate hazards at each stage of development and operation, ranging from concept to operation and lifecycle management. Hazard analysis techniques are the different methods used to identify and mitigate hazards. Numerous hazard analysis techniques have been developed for various situations. Some of the more well-known hazard analysis techniques include fault tree analysis (FTA), event tree analysis (ETA), and failure mode and effects and criticality analysis (FMECA).

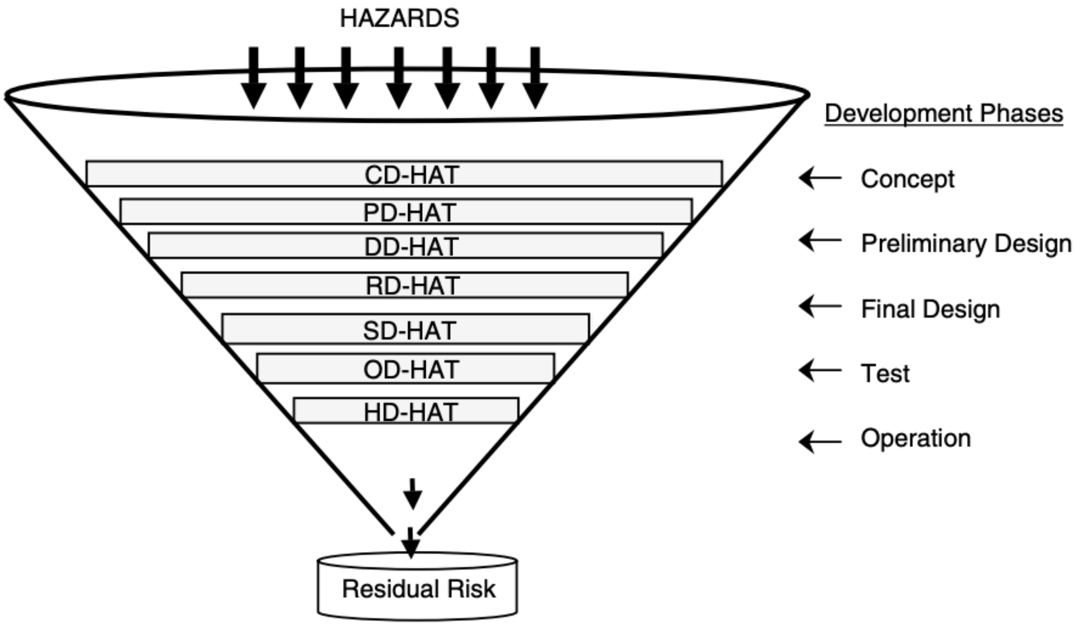


Figure 2-5: Hazard Analysis During Development [18]

FTAs and ETAs are probabilistic risk assessments (PRA) that use graphical models called fault trees to represent all combinations of possible events in a system that might lead to an undesired event. FTAs look at all possible event combinations that lead to a fault, while ETAs look at all possible outcomes from a single event. The probability of each event independently occurring is calculated, and the highest probability faults are addressed [18].

FMECA is a bottom-up analysis tool for evaluating how potential failure modes affect the reliability of the overall system and the probability that each mode will occur. FMECA is accomplished at the component level but can be used at any level of design detail—assembly, subsystem, etc. [18]. Ford identifies four types of functional failure modes that generally occur [19]:

1. No function: the system or component in question is non-functional or inoperative.
2. Partial/Over Function/Degraded over Time: Function has degraded over time and meets some of the functional requirements but not all.
3. Intermittent Function: Meets functional requirements but loses some functionality temporarily, often due to external factors.
4. Unintended Function: the interaction of several elements whose independent performance is correct adversely affects the product or process. Resulting in an unwanted outcome or 'unintended function.'

Ericson identifies "function does not fail safe" as a fifth functional failure mode that can occur [18]. Ericson also distinguishes between functional failure modes, hardware failure modes, and software failure modes. After failure modes are identified for each component[1], failure rates detail how likely the failure is predicted to occur. Then causal factors are determined, followed by the immediate

---

[1] Which is impossible for software because it can have an infinite number of "failure modes."

(proximate) effect of the failure and finally, the system effect of the failure. Recommendations are derived from the findings and adapted to current controls and detection methods.

2.4.1. Shortcomings of Current Hazard Analysis Techniques

FTAs and ETAs provide a good visualization of all possible failure event sequences but do not address the context in which events may happen. In isolation, the probability of an event occurring may be calculable if ***all*** events in the system are assumed to be independent. By treating each event occurrence independently, FTAs disregard systemic factors, dependent interaction (e.g., one event may increase the likelihood of another event occurring), and the context in which events occur. While this may be effective for physical failures, context plays a crucial role in human operators and software. Latent design errors may also be overlooked [7]. They also do not handle sophisticated software behavior, such as requirements errors, and the complex human decision making common in advanced systems today.

FMEA is effective for addressing the reliability of hardware. An important definition used by FMEA is the definition of a failure mode:

> *A design failure is defined as the manner in which as system, subsystem, or part fails to meet its intended purpose or function. A process failure is the manner in which a process fails to meet its intended purpose.*

Failure Mode and Effects Analysis Handbook [19]

A common issue with bottom-up approaches is that the analysis technique may overlook unintended system behavior even if individual components do not fail. A commonly cited example of this is the Mars Polar Lander loss. All the components met their intended purpose, including the software within the lander. The loss resulted from unintended and unsafe component interactions [7]. This accident is an example of a system where the components were incredibly reliable, yet the system was unsafe. Leveson writes that “high reliability is neither necessary nor sufficient for safety” [7].

Like FTAs and ETAs, FMEA assumes each part to act independently of each other and does not acknowledge the role that context plays in the probability of a failure. Component interaction, such as in the case of the Mars Polar Lander, could increase the likelihood of failure—as well as any other systemic factors.

2.5. Safety in Pilot Training

Safety is introduced in the first chapter of AETCMAN 11-248, the T-6 Primary Flying Manual. Safety is described as a “critical component of successful mission accomplishment” where each crew member “is responsible for minimizing risk to the people and assets under his or her control and identifying potential safety hazards” [20]. Ground safety and flight safety are discussed separately.

Flight Safety emphasizes a dynamic environment with “an aggressive disposition towards gaining and maintaining situational awareness (SA) [20]. The Cockpit/Crew Resource Management Training Program (AFI 11-290) defines SA as an “aircrew member’s continuous perception of self and aircraft in relation to the dynamic environment of flight, threats, and mission, and the ability to forecast, then execute, tasks based upon that perception” [21]. AETCMAN 11-248 outlines the following steps in maintaining SA:

1.4.2.1. Clearing the airspace

1.4.2.2. Monitoring aircraft systems

1.4.2.3 Establishing and maintaining an emergency recovery plan before an emergency.

AFI 11-290 further outlines positive and negative factors used to evaluate SA. After discussing safety, flight discipline is described as each operator's discipline to adhere to guidelines while "executing the mission in the presence of temptation to do otherwise" [20]. This involves appropriate mission preparation (including physical preparation, the pre-flight brief, knowledge of rules and procedures, etc.) and proper mission completion.

Each pilot is expected to be able to execute each checklist into 1T-6A-1CL, *The Pilot's Abbreviated Flight Crew Checklist,* for appropriate circumstances. Section 1.6 states that "the omission of a checklist item could lead to a dangerous situation. Therefore, positively confirm the completion of all checklists regardless of how they are accomplished" [20] [22].

The pilot controlling the aircraft is responsible for completing all checklists. When checklist items are marked 'BOTH,' both the PF and the pilot not flying (PNF) must complete and affirm the items. Affirmations are conducted as "challenge and response" items where the PF issues a verbal query requiring a response from the PNF. Section 1.6.5 states that if a checklist cannot be completed without interruption, "a good technique to get back on track includes restarting at the first step of the checklist or restarting two to three steps prior to the missed or interrupted step." It also states that the crew should not start a new checklist until completing the previous one.

In the case of an engine loss, 11-248 outlines two options, ejection or emergency landing pattern (ELP), depending on the circumstance.

Cockpit/Crew Resource Management (CRM) applies six skills outlined in AFI 11-290 to accomplish mission objectives safely and efficiently. The six skills outlined in AFI 11-290 are as follows:

3.2.2.1. Communication. Includes knowledge of common errors, cultural influences, and barriers (rank, age, experience, position, etc.). Skills will encompass listening, feedback, precision, and efficiency of communication with all members and agencies (crewmembers, wingmen, weather, air traffic control, intelligence, etc.). (T-2). Use precise terminology, acknowledge all communications, and ask questions/provide clarification when necessary.

3.2.2.2. Crew/Flight Coordination. Includes the knowledge and skills required within (internal) and outside the crew/flight members (external) for mission coordination, flight/mission integrity contracts, team building, leadership, command authority, responsibility, behavioral styles, assertiveness, persistence, conflict resolution, hazardous attitudes, legitimate avenues/methods of dissent, and solution driven statements. Adapt as situational demands require, focus attention on task, and ask for inputs.

3.2.2.3. Mission Analysis. Includes pre-mission analysis and planning, briefing, ongoing mission evaluation, and post mission debrief. Clearly define mission overview/goals. Analysis instruction will include specific threat and error management tools and techniques. (T-2). Debrief instruction will include aircrew responses and outcomes to threats and errors. (T-2).

3.2.2.4. Risk Management (RM)/Decision Making. Includes risk assessment, the risk management processes (deliberate, real time RM)/tools, breakdowns in judgment and flight *discipline, problem-solving, evaluation of hazards, and control measures. Identify contingencies and alternatives, gather all available decision data, and clearly state decisions.*

> *3.2.2.5. Situational Awareness. Includes knowledge and skill objectives for identifying errors, preventing the loss of situational awareness, recognizing the loss of situational awareness, and techniques for recovering from the loss of situational awareness. Recognize the need for action and verbalize/act upon unexpected events.*
>
> *3.2.2.6. Task Management. Includes establishing priorities; using available resources to manage workload, overload/under-load, and complacency; managing automation, checklist discipline and standard operating procedures; and stating problems and proposed solutions* [21].

Evaluators can reference AF Form 4031 "CRM Skills Criteria Training/Evaluation" as a reference for good CRM practices [23].

Section 1.14 outlines the challenges and limitations of tandem seating in the T-6. Limited visibility between each crewmember "makes it difficult to judge intentions, anticipate actions, and verify aircraft systems configurations" [20]. These communication challenges are a significant concern and are a primary focus of the analysis in this thesis.

Furthermore, some functions are only controllable from one cockpit (front or back). Table 2-2 shows functions exclusively controllable from either the front cockpit (FCP) or rear cockpit (RCP). ** indicates that the RCP can check the functionality

Table 2-2: T-6 Functions Exclusively Controlled by Either Cockpit [20]

Front Cockpit (FCP)	Rear Cockpit (RCP)
Activation of the auxiliary battery	Interseat Sequencing System (ISS)
Manual fuel balance left/right (L/R) switch	Interphone Hot/Cold mic switch
Environmental control system controls	
Parking brake position	
Emergency gear extension	
Power Management Unit (PMU)	
Firewall Shutoff handle	
Gust Lock.	
Bleed air inflow **	Check Bleed air inflow by pressing the G-suit test button.
On board oxygen-generating system (OBOGS) **	Confirm on board oxygen-generating system (OBOGS) is operating by momentarily turning off supply lever.
Defog operation **	Confirm defog operation by sound or temperature of the defog outlet valves along the canopy rail.
External light operations **	Confirm external light operations (on the ground) by looking for reflections from adjacent aircraft or other surfaces.

The manual also notes that if the RCP is operating with impaired visibility, the FCP pilot is responsible for landing. It also emphasizes the importance of the transfer of aircraft and systems control. Control of the aircraft is delineated by the pilot flying (PF) and the pilot not flying (PNF). A typical transfer of aircraft control consists of the PF relinquishing control by saying "You have the aircraft" and the PNF assuming control by saying "I have the aircraft" [20]. The PNF's assumption of control is paired with a noticeable shake of the control stick to verify that the PNF has assumed control of the aircraft. In tandem cockpits, the aircraft commander (AC) or instructor always retains the authority to take control of the aircraft.

In critical situations, the AC may reverse the order of transferring aircraft control by saying, "I have the aircraft" however the PF must still relinquish control by stating, "You have the aircraft." If intercoms fail, the PF can signal a desire to relinquish control by smoothly pushing the rudder pedals back and forth. To assume control, the PNF must vigorously shake the stick. It is also noted that the PF should never relinquish control until the PNF has positively assumed control of the aircraft. The PF should not hesitate to relinquish control when the AC directs a transfer of aircraft control.

It is also noted that the PF controls all dual aircraft systems to avoid inadvertent inputs. These systems include canopy, radio management system (RMU), global positioning system (GPS), and electronic flight instrument system (EFIS).

During emergencies in the aircraft, pilots abide by the following basic rules [20]:

1) Maintain Aircraft Control: Flying and recovering the aircraft takes precedence over other responsibilities. Pilots use the memory aid "Aviate, Navigate, Communicate" to order the priority of their actions. The AC is responsible for ensuring a safe recovery if the PF cannot safely recover the aircraft.
2) Analyze the Situation and Take Proper Action: Analyzing the situation includes analyzing aircraft performance for deviations, checking instrument readings, and warning systems, and confirming abnormalities with all crewmembers. Actions include executing boldface (time-sensitive procedures committed to memory), emergency checklists, additional noncritical actions, communication with ATC, and preparation for landing.
3) Land as Soon as Conditions Permit—if the aircraft cannot recover safely, ejection is the last contingency.

When practicing emergency procedures, students use the AABCDEF method outlined in Figure 2-6:

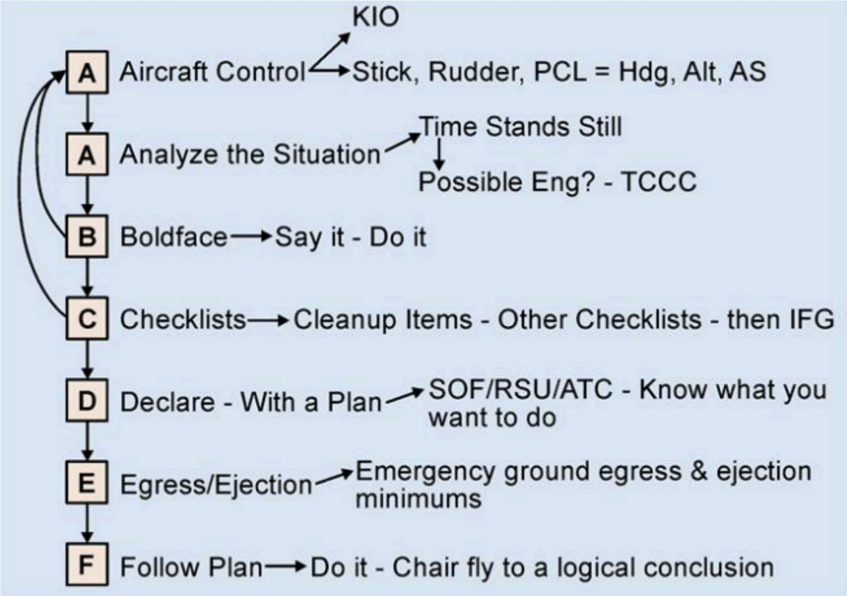


Figure 2-6: Method of Accomplishing Practice Emergency Procedures [20]

3. METHODOLOGY USED IN THIS THESIS

Systems theory provides the foundations for STAMP, which views systems as a hierarchy of controls and accidents as resulting from inadequate control over the behavior of the individual component and their interactions.

When using STAMP as the basis of analysis, the system model is organized into controllers and controlled processes in a control hierarchy where the highest control authority resides nearest to the top. Controllers can include high-level government legislation, regulatory agencies (the Federal Aviation Administration), human operators, software, and physical processes.

Controlled processes are defined by a goal condition, action conditions (e.g., the actions of the controller will influence an outcome of the system), observability condition (e.g., the state and any changes to the system must be observable by the controller), and model condition (e.g., the controller needs a model of the process within the control structure) [7]. Action conditions are typically met through actuators, and the observability condition is met through sensors.

Safety results or “emerges” as controllers interact with each other and their respective controlled processes. It is therefore an “emergent” property in the terminology of Systems Theory.

Safety can only be determined through the lens of the entire sociotechnical system. The emergence of safety is enforced by constraints imposed by higher control authorities. It is worth noting that control does not always imply compliance. One of the goals of STAMP-based methods is to analyze in what context a controller may not comply with a designated safety constraint from a higher authority. Control structures are drawn with information flowing to and from the control authority. As seen in Figure 3-1, a downward reference channel implies a safety constraint imposed by the control authority, and an upward reference channel indicates feedback from the controlled process. Note that this is simply a feedback control loop as used in engineering.

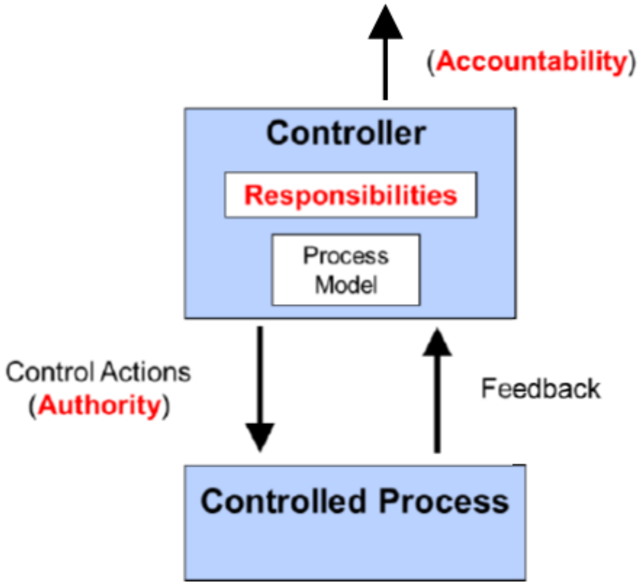


Figure 3-1: A Simple Control Loop [24]

Due to the complexity of modern systems, current accident and hazard analysis techniques do not provide the depth or sophistication required for addressing multi-faceted socio-technical systems and accidents. Systems Theory offers a different perspective, addressing many of the concerns of how safety has been looked at in the past.

Dr. Nancy Leveson pioneered STAMP to provide a more powerful accident causality model. STAMP addresses hindsight bias, component errors, software integration, and multiple interpretations when appropriate. Many accident models also exclusively define component failures and human error as the leading cause of accidents, whereas STAMP asks why certain safety constraints were not enforced in the system. It is much easier to blame the operators than to look at the confounding factors that may lead to human behaviors, which often provide the best opportunities for learning and improvement.

STAMP models safety as a control problem rather than the traditional view of safety as a reliability problem. STAMP is focuses on safety constraints—conditions designated and enforced by a control authority that will prevent the system from entering a hazardous state. Analysis tools based on STAMP identify where safety constraints come from, how they are derived, how they are enforced, what actions would lead to safety constraints not being enforced, and what scenarios would lead to unsafe control actions. These safety constraints are built into the hierarchical control structure. By analyzing these safety constraints within the context of the control structure, STAMP provides a foundation for both accident causality and hazard analysis.

4. CAUSAL ANALYSIS BASED ON SYSTEMS THEORY (CAST)

CAST is a causal analysis tool based on STAMP. This is an analysis method, **not** an investigation technique. CAST is used to help identify what questions should be asked and what system design recommendations can be implemented to prevent or mitigate future accidents. The goal of the CAST analysis is to investigate the control structure and identify why it was unable to enforce the safety constraints that were violated in the accident [24]. A primary goal of this analysis is to look past the role of human operators in the accident, analyze the system holistically, and determine the mechanisms and factors that shape human behavior.

> *"Most people are not malicious but are simply trying to do the best they can under the circumstances and with the information they have."*
>
> Dr. Nancy Leveson, *Engineering a Safer World* [7]

CAST has five parts, as depicted in Figure 4-1:

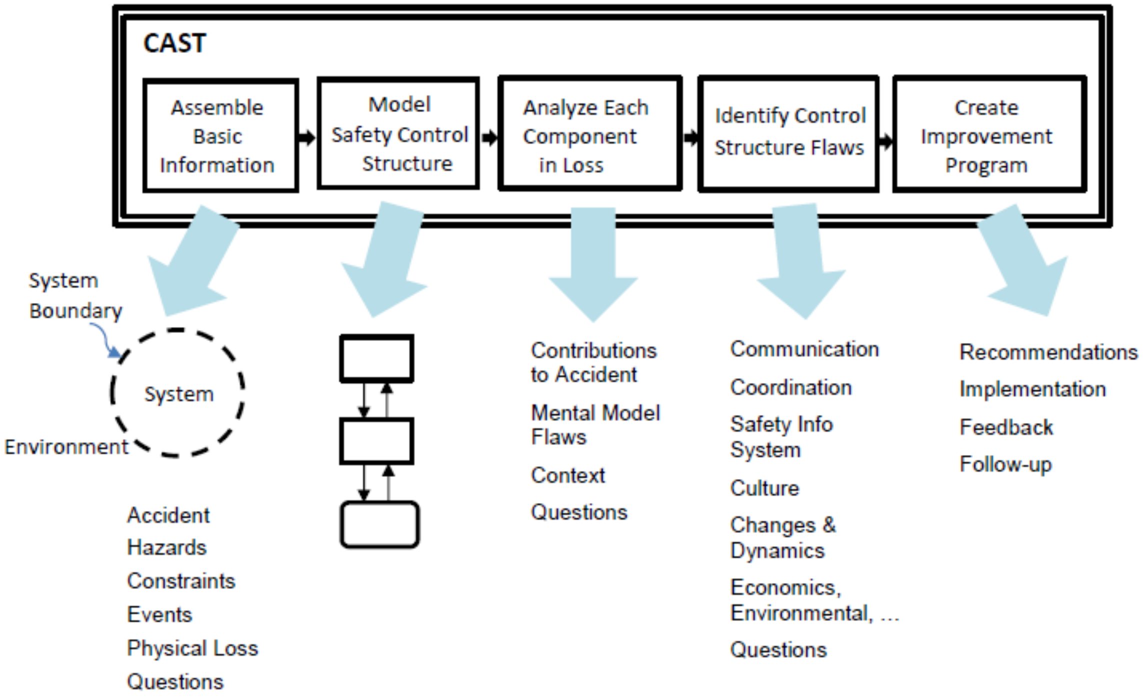


Figure 4-1: The Five Steps of a CAST Analysis [24]

The CAST process is illustrated using a real AF accident example. The results are then compared with the results of the official AF investigation.

4.1. Proximal Event Chain

On 21 November 2019, at approximately 1506Z, two T-38C Talons collided during an attempted formation landing at Vance AFB in Enid, OK. For the sake of the CAST analysis, the aircraft and personnel involved will be labeled in accordance with (IAW) the United States Air Force Aircraft Accident Investigation Board (USAF AIB) Report: Mishap student pilot 1 (MSP1) flew with mishap instructor pilot 1

(MIP1) in Mishap Aircraft 1 (MA1), and the adjacent aircraft will be referred to as mishap aircraft 2 (MA2) which was piloted by mishap student pilot 2 (MSP2) and mishap instructor pilot 2 (MIP2). Tail numbers can be referenced in the full USAF AIB Report. The report was conducted IAW Air Force Instruction (AFI) 51-307: *Aerospace and Ground Accident Investigations* [25] [26].

Both aircraft were assigned to the 25th Flight Training Squadron (25 FTS), part of the 71st Flying Training Wing. However, MIP1 was assigned to the 5th Flying Training Squadron as an Active Guard Reserve officer who flew with the 25 FTS.

The report first detailed the accident chronology:

Table 4-1: Proximal Event Chain as Defined by the Accident Report [26]

ID	Event
1	Immediately after touchdown, MA1, flying in the left-wing position, became briefly airborne, rolled rapidly to the right, then touched down once more in a right bank.
2	MA1 entered a skid and crossed the runway centerline from left to right toward MA2.
3	MA1 lifted off the runway again then struck MA2 with its right main landing gear.
4	The collision caused MA1 to roll over the top of MA2 then impact the ground in a nearly inverted attitude, fatally injuring MIP1 and MSP1.
5	MA1 slid approximately 700 feet before coming to a stop in a grassy area.
6	Following the collision with MA1, MA2 departed the prepared surface of the runway, remained upright, travelled through the grass, and came to a stop.
7	MIP2 and MSP2 shut down and safely egressed their aircraft.

4.2. Accident Investigation Board Findings

After detailing the proximal event chain, the AIB report then provided the Board President's evaluation of the evidence and the causes [26] as:

> *… the mishap were MIP1 failing to take control of MA1 as a precarious situation developed and MSP1 subsequently making an inappropriate flight control input. During the landing sequence, MSP1 prematurely initiated an aerodynamic braking maneuver (aerobrake) immediately after MA1 initially touched down, causing MA1 to lose contact with the runway surface. Almost simultaneously, MSP1 applied and held right rudder in an attempt to steer MA1 away from the left edge of the runway. MSP1's use of rudder under these conditions--airborne, configured for landing and at an increased angle of attack--caused MA1 to roll and yaw to the right and placed MA1 on a collision course with MA2. The Board President found MIP1 could not have successfully prevented a collision after MSP1's rudder input had taken effect, but that MIP1 would have already intervened to take control of MA1 had he made an accurate real-time risk assessment in the preceding moments. Additionally, the Board President found the following factor substantially contributed to the mishap: MSP1 lacked an effective visual scan during the formation approach. Due to his focus on MA2, MSP1 did not adequately crosscheck his runway alignment prior to touchdown. Instead, he used rudder in an attempt to steer MA1 as his premature aerobrake lifted the weight from MA1's wheels after MA1 initially touched down*.

Note that this describes the events but provides little information about why the events occurred beyond stating what the pilots did wrong.

The takeaways from the USAF SIB Report are that MSP1 did not make the proper maneuvers to execute a formation landing safely, and the MIP1 did not take action to prevent the aircraft from entering an unrecoverable state.

After the facts were gathered, the accident investigator provided a statement of opinion assuming the potential causes and contributing factors to the accident. AFI 51-307 paragraph 7.8.4 defines a cause as:

> *"an act, omission, condition, or circumstance that starts, sustains, or creates a condition permitting the mishap, without which the mishap could not have occurred. It may be an element of human environmental, mechanical performance or a combination thereof. A given act, omission, condition, or circumstance will be a cause' if correcting, eliminating, or avoiding it would have prevented the mishap. In other words, a factor is found causal if 'but for' that factor taking place, the mishap would not have occurred."*

Finally, the following were identified as causes in the statement of opinion in the report:

1. M1P1 made an inaccurate real-time risk assessment during the landing sequence. As a result, he did not take control of MA1 as a precarious situation developed. The investigator noted that MIP1 was one of Vance's most confident, capable, and dedicated T-38C IPs. More experienced IPs tend to let student errors progress further than other instructors to maximize learning. In application, the IP allows students to progress through their mistakes and make the necessary corrections while verbally coaching and cueing the student through the proper corrections. When an IP takes control of the aircraft during a student mishap, the student learns less from the interaction because they are not correcting their own mistake.

   Experienced and confident IPs will let students progress through their errors to facilitate better training. There was no evidence to suggest that MIP1 had any disregard for the safety of the flight. The accident investigator could not determine if MIP1 failed to notice the drift that led to the accident or if he elected not to intervene. MA1 remained on track to land on the prepared surface, and it was inferred that MIP1 elected not to interfere because he thought MSP1 could safely complete the landing sequence [26].

   The investigator noted that the T-38C IPs strongly discourage using the rudder during normal traffic pattern operations until both main tires are firmly planted on the ground. A typical student error is using the rudder in the traffic pattern. It is not expected beyond the early stages of the T-38C program, so the investigator noted that there would be no reason for MIP1 to expect such an error from a student with MSP1's experience during a normal landing (56th sortie).

   In the investigator's opinion, MIP1 did not assess the risk properly when MSP1 prematurely aerobraked near the runway's edge at touchdown. Compounded on top rudder input, the investigator concluded that the risk assessment made by MIP1 was inaccurate. MIP1 did not take control of MA1 as a precarious situation developed.

   a. These conclusions raise more questions than they answer. For example:
      - Why would MIP1 make an inaccurate risk assessment?
      - What factors could have shaped his behavior to make an inaccurate risk assessment?
      - How is "inaccurate" qualified in the case of pilot training?
      - Was the instructor providing appropriate verbal cues to the student?

    - Why would MIP1 not take control of the aircraft?
    - What factors could have shaped his behavior towards not taking control?
    - Was this a standard practice in the squadron?
    - Why would MIP1 fail to notice a drift that led to the accident when watching the events unfold?
    - What would prompt MIP1 to elect not to intervene?
    - Were there any factors that could have shaped this response?

2. MSP1 made an inappropriate flight control input during landing, placing MA1 on a collision course with MA2. The investigator notes that the evidence suggests MSP1 prematurely initiated an aerobrake to fall behind MA2. With sufficient airspeed to lift off, MSP1 pulled back on the stick to raise the nose, then less than a second later, applied the right rudder to steer towards the runway at which MIP1 directed a go around. At high AoA's, the yawing moment of the rudder is highly coupled with a complimentary rolling moment. Thus, on application, MA1 rolled to the right, the investigator believes that the collision with MA2 was inevitable. It is noted in Air Education and Training Command (AETCMAN) 11-251 that the T-38C's rudder is highly effective at rolling the aircraft in high AoA situations [27].
    a. Questions raised when reading this accident report but never answered in it:
        - If T-38 IPs strongly discourage the use of rudder, why would the student choose this as a control action?
        - What factors would have shaped MSP1's unsafe control action or behavior?
        - What would cause the student to think otherwise if the manual identified this?
        - Were there conflicting sources of feedback?
        - Are high AoA situations built into training?

MSP1 lacking an effective visual scan during the formation approach, was also identified as a substantial contributing factor. The investigator noted that M1P1 prompted MSP1 to tighten the formation a mile from touchdown. However, the spacing continued to widen as the formation approached the runway. The investigator claimed that because of MSP1's fixation on MA2, MSP1 failed to crosscheck the runway alignment and thus drifted left as they descended through 100 feet above ground level (AGL). When MSP1 finally realized MA1 was close to the edge of the runway, the abrupt rudder input was applied, leading to the ensuing accident. The investigator states that had MSP1 made a proper visual scan during the formation approach, the accident could have possibly been avoided [26].

The Board President concluded that the cause was MIP1 failing to take control of MA1 in a precarious situation developed and MSP1 subsequently making an inappropriate flight control input, where MSP1 lacked an effective visual scan during the formation approach [26]. This conclusion was drawn from the Board President's own opinion, cockpit video of both aircraft, a reconstructive animation of the mishap, engineering analysis, a replication of the mishap sequence in a T-38 Weapon System trainer (simulator), and consultation from a USAF Test Pilot and a T-38 expert who subsequently replicated the circumstances leading to the mishap during a live test flight.

While these conclusions do assign blame, they do not provide enough information to prevent similar occurrences in the future. Using CAST can provide that information.

4.3. CAST Step 1: Assemble Basic Information:

CAST starts by defining the boundary for the analysis and identifying the hazards that lead to the loss. The following are questions raised b ythe SIB report:

- How was the communication between the pilots during the touchdown?
- Was there something that prompted the pilot in control to become airborne?
- What was the rationale for the right rudder?
- Was this clear in the flight manuals?
- Was there any reason the instructor would say something different from what is in the manual?
- What were the limits of the instructor for taking control of the aircraft?
- Was there any way that this maneuver could have been recovered at this point in the accident?
- Was there external stress on the student or instructor?
- Did the aircraft have any warning mechanisms to alert the instructor/student?
- Were procedures consistent between the instructor and student?
- Was the aircraft designed in a way that helped the pilots clarify who has control of the aircraft?
- Was the aircraft designed in such a way that was conducive for the student to learn how to land?
- Were the operators' procedures incorrect or incomplete?
- Was there communication between the two aircraft as MA1 began to skid?
- Was the procedure for this type of emergency incorrect or incomplete?
- Was ATC providing any information to the operators of either aircraft during this event?
- Has it been conditioned that ATC relaxes standards during student training sorties?

4.3.1. Define system boundary

The system is focused on the operation of the mishap T-38 on the final approach to landing through the conclusion of the accident to include the following key actors: Air Traffic Control (ATC), Higher Mission Authority (HMA), Lower Mission Authority (LMA consisting of the 25th Flying training squadron, the 5th flying training squadron), the Instructor Pilot, the Student Pilot, and the T-38 and the physical processes associated with the aircraft.

4.3.2. Hazards

STAMP defines a hazard as a condition that leads to the loss. The hazard responsible for the loss is harder to identify, given the system's complexity. Identifying a single hazard reduces the scope of the analysis and is subject to hindsight bias. The constraints that must be enforced in the system design and operation are generated from the hazards. The following hazards are used in the analysis:

System Hazard 1: Aircraft is uncontrollable.

Safety Constraints:

a. Aircraft must remain controllable during the final approach.
b. Flight crew must communicate control authority and transfer of aircraft control.
c. A student pilot must be adequately trained in landing procedures during the final approach if in control.
d. Changing system states must be recognized and acknowledged by both pilots.
e. The controller's mental mode must reflect the true system state.
f. Aircraft structural integrity must be maintained during the final approach.

System Hazard 2: Aircraft violates minimum separation standards from other objects (Aircraft, approach)

Safety Constraints

a. Aircraft must remain controllable during the final approach.
b. Aircraft must remain in proper landing approach.
c. Aircraft must not violate minimum separation standards

System Hazard 3: Training limitations exceeded.

Safety Constraints:

a. The flight crew must stay within training limitations.
b. Instructors must recognize limitations.
c. The instructor must take control of the aircraft before exceeding limitations.

System Hazard 4: Student flies after training limitations are exceeded.

Safety Constraints:

a. Instructor Pilot must take control of aircraft before exceeding limitations.
b. Instructors must recognize limitations.
c. Instructor Pilot must recover the aircraft after exceeding limitations.
d. Student pilots must relinquish control of the aircraft when the instructor takes control.
e. Flight crew must communicate control authority and transfer of aircraft control.

4.4. CAST Step 2: Model Safety Control Structure:

In the second step of CAST, the system is modeled as a control hierarchy. This analysis will be high-level with generalized control actions. Each controller is responsible to uphold safety constraints to prevent a hazardous condition from arising in their controlled processes. Once the controllers are identified, they are analyzed to see why the safety constraints were ineffective.

The control structure can be broken down into a series of controlled processes in the form of feedback loops. As discussed in the overview of STAMP, control structures are drawn with information flowing to and from the control authority; a downward reference channel implies a safety constraint imposed by the control authority, and an upward reference channel indicates feedback from the controlled process. A complete control loop has a controller, control actions referenced downward, feedback referenced upward, and a controlled process. The controlled process can also be modeled such that there is external information given to the controller or the controlled process (e.g., cyber-attacks or interference). A generalized control loop is shown in Figure 3-1. These are instantiated for the system being analyzes and the relationships between the controlled is specified.

It is important to note that control authority does not mean compliance. Each controller has its respective process model or mental model of the controlled process. Process models represent the controller's internal beliefs about the system [28]. The controlled process may not always carry out the control action. Controllers use feedback from the controlled process to update their internal process model. A controller's control algorithm bases its following control action on the updated process model. Feedback is also used to facilitate accountability to the higher-level controllers.

Figure 4-2 is the high-level control structure for the T-38 accident. Trainer aircraft exhibit shared control between the FCP and RCP. A definition of shared control in the context of a trainer can be adapted from Abbink et al. [29]:

> *In shared control, human(s) and robots(s) are interacting congruently in a perception-action cycle to perform a dynamic task, that either the human or the robot could execute individually under ideal circumstances.*

Rather than robots, the shared control duty is between the instructor and student pilots. Both the instructor and student pilot exhibit the same controls over the aircraft (except for those listed in Table 2-2). However, for instructor-student shared control it is implied that the student cannot accomplish the same tasks as the instructor. The instructor aims to align his or her idealized process model about the operations of the aircraft with that of the student's through the process of instruction. The misalignment between the instructor's process model and the student's incomplete process model establishes a foundation for unsafe control actions that lead to hazards.

4.4.1. Control Structure

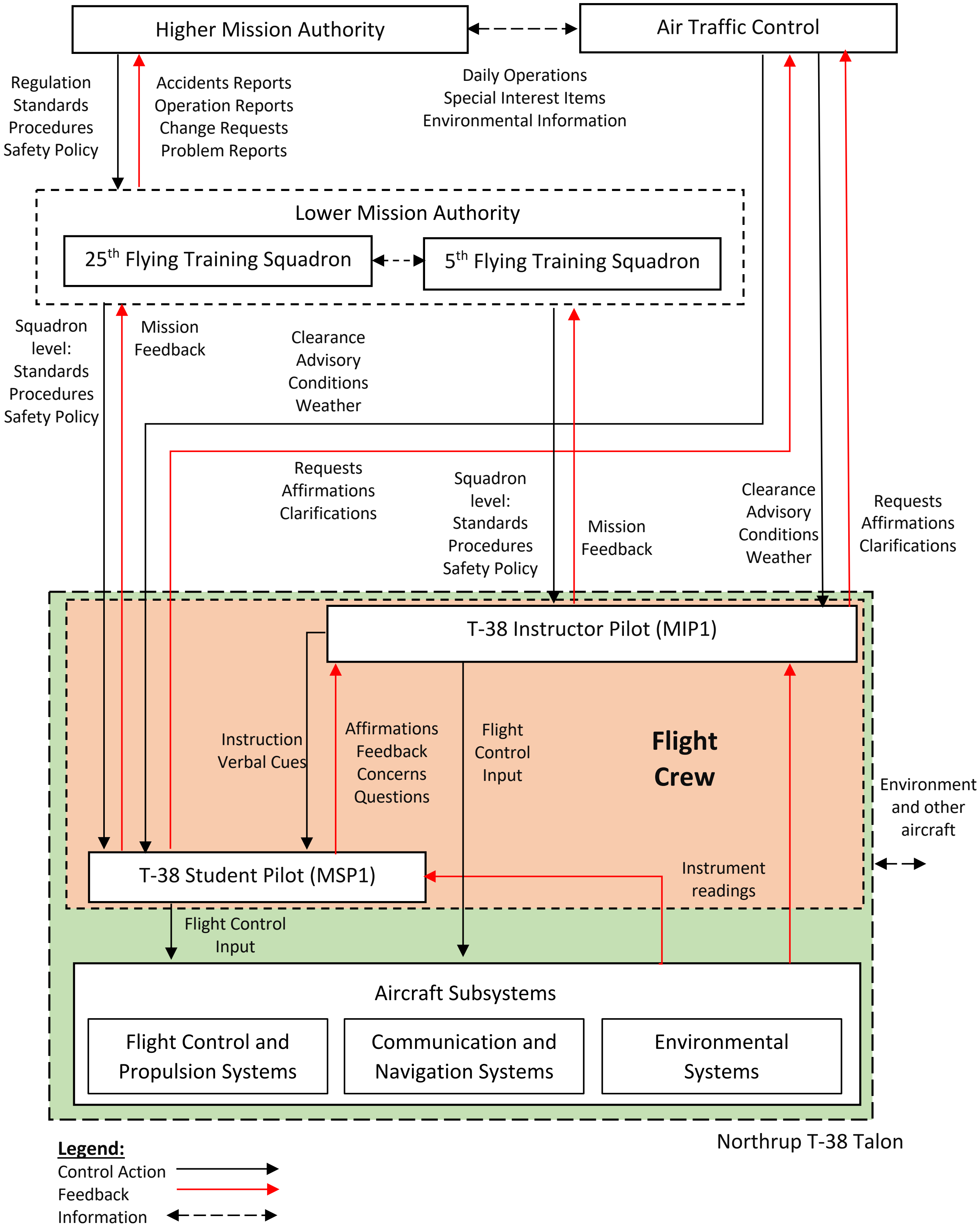


Figure 4-2: Control Structure for a Student Sortie in UPT

4.4.2. Controllers and Responsibilities

Each controller is responsible for enforcing safety constraints that keep the system from entering one of the hazardous states identified above. The controller responsibilities that do not contribute to the safety constraints are not included in the analysis. The following are the responsibilities required for hazard mitigation:

Higher Mission Authority: The highest command authority provides guidance and procedures for flying training groups and squadrons to follow and approve changes in procedures and operations. The higher mission authority encompasses Air Education Training Command (AETC), 71st Flying Training Wing (71 FTW), and the 340th Flying Training Group (340 FTG):

- R-1.1: Educate Squadrons on the policies and procedures passed down through ATC
- R-1.2: Define rules, regulations, and standards for squadrons.
- R-1.3: Approve additions and changes to the UPT syllabus (Fact check)
- R-1.4: Ensure the T-38 is equipped with the most up-to-date safety technology.
- R-1.5: Make appropriate changes to the recommendations from the squadrons.

Air Traffic Control: Coordinate aircraft movement to maintain safe distances between [30]. The following responsibilities are from the Bureau of Labor Statistics:

- R-2.1: Monitor and direct the movement of aircraft on the ground and in the air
- R-2.2: Control all ground traffic at airport runways and taxiways
- R-2.3: Issue landing and takeoff clearances to flight crews
- R-2.4: Inform pilots about the weather, runway closures, and other critical information
- R-2.5: Alert airport response staff in the event of an emergency

Lower Mission Authority (LMA) consisting of the 25th Flying Training Squadron and 5th Flying Training Squadron: Directly Implementing policy from the HMA

- R-3.1: Adhere to policy and procedures from the HMA
- R-3.2: Communicate changes to IPs and students
- R-3.3: Ensure consistent squadron level policies between the two squadrons
- R-3.4: Relay operator feedback to the HMA

T-38 Instructor Pilot (MIP1):

- R-4.1: Ensure Safety of Flight.
- R-4.2: Ensure adherence to flight training syllabus.
- R-4.3: Ensure an accurate mental model of the aircraft's status, mode, and position
- R-4.4: Adhere to HMA and ATC instructions.
- R-4.5: Ensure proper preflight mission analysis (to include pre-mission, ongoing mission, and post-mission)
- R-4.6: Conduct flight training sorties
- R-4.7: Stay within safe instructor limitations
- R-4.8: Report student progress to the student's grade card
- R-4.9: Ensure proper risk management and decision-making (to include general aircraft knowledge and emergency procedures).
- R-4.10: Ensure proper communication

- R-4.11: Ensure proper crew coordination and task management.
- R-4.12: Monitor aircraft descent profile
- R-4.13: Monitor aircraft airspeed, Aimpoint, and altitude
- R-4.14: Ensure aircraft is controllable
- R-4.15: Ensure accurate mental model of the student's capabilities.
- R-4.16: Maintain situational awareness

T-38 Student Pilot (MSP1):

- R-5.1: Adhere to the flight training syllabus
- R-5.2: Adhere to HMA, LMA, ATC, and IP instruction
- R-5.3: Ensure proper knowledge of general aircraft knowledge and emergency procedures
- R-5.4: Ensure an accurate mental model of the aircraft's status and position
- R-5.5: Communicate areas of focus to the instructor
- R-5.6: Relay affirmations of instruction to the instructor
- R-5.7: Communicate transfer of aircraft control to the instructor
- R-5.8: Operate and manage aircraft descent profile
- R-5.9: Operate and manage aircraft airspeed, aimpoint, and altitude

Aircraft Subsystems: The aircraft flight control systems (FCS) and propulsive systems, Aircraft Communication and Navigation Systems, and the aircraft's internal environmental systems. Because the T-38 is an older aircraft with less sophisticated systems, the aircraft's hydraulic and software controllers will be encompassed in the aircraft subsystems. The latter STPA will discuss the implications of adding additional and more sophisticated software controllers.

- R-6.1: Ensure proper communication between the flight crew
- R-6.2: Ensure adequate communication between the flight crew and ATC
- R-6.3: Provide salient alert for transfer of aircraft control
- R-6.4: Provide salient alert for critical aircraft feedback (stall warning, altitude warning, decent warning, etc.)
- R-6.5: Provide feedback on the aircraft's airspeed, position, and altitude (among other metrics)
- R-6.6: Conduct physical outputs of the operator's input

4.5. CAST Summary of Results:

The third step in CAST involves analyzing each component. After outlining the control structure and each controller's responsibilities to enforce safety constraints, the next step is to ask why the control structure was insufficient to enforce the safety constraints and then determine how each component contributed to the accident. These could be caused by flaws in the mental or process model of the controller or contextual factors explaining unsafe control actions.

The analysis starts at the lowest level of the control structure (the physical process), identifies the failure or unsafe interaction involved with the accident, and asks why the component behaved in such a manner that led to a hazardous condition. Then the analysis works up the control hierarchy to see how the roles of each controller contributed to the hazardous condition, specifically tying back to the controller's responsibilities, any unsafe control action, and then asking why they behaved unsafely. Finally, any other contextual factors contributing to the accident are considered (e.g., safety culture, external pressures, etc.). Recommendations are provided at every step.

The fourth step in CAST analyzes the interactions between each of the components. This step includes multiple controllers with authority over the same controlled process. The previous step analyzed each controller individually, whereas this step revisits the control structure and analyzes the interactions between controllers. This includes systemic factors stemming from the control structure, such as:

- Communication and coordination
- The safety information system
- Safety Culture
- Design of the Safety Management System
- Changes and dynamics over time: in the system and the environment ("CAST Handbook")

The fifth and final step in CAST involves creating an improvement program based on recommendations generated from the analysis of each component and the interactions between components. The following is a summary of this analysis:

4.5.1. Contributions to accident

Mishap Student Pilot 1:

Safety Requirements and Constraints:

The primary role of the student is to learn how to fly. The student must communicate control authority, transfer of aircraft control with the instructor, and update the instructor on the student's evolving process model. The student must also be receptive and responsive to the instructor's guidance during the flight. Because the student was struggling with formation flying and the maneuver was a formation landing, communication with the instructor is an extremely important safety constraint.

Unsafe Control Action:

MSP1 aligned too far to the left on their final approach. Upon touchdown, MSP1 needed to correct his heading and incorrectly inputted the right rudder on final approach, which led the aircraft to roll. This resulted in MIP1 taking control of the aircraft, which became airborne. With insufficient airspeed to obtain lift, the aircraft proceeded to roll over MA2 and then touch down inverted off the runway to the right.

Context in Which Decisions were Made:

- Environmental and Behavior-Shaping Factors:
  - Rudders on the T-38 are highly coupled at high angles of attack. The T-38 is only at high angles of attack during takeoff roll, final approach, and other maneuvers such as stalls or slow flight. The high coupling of the rudder and rolling moment contributed to the hazardous condition. Most jet aircraft are highly coupled at high angles of attack due to the high distribution of weight on the tail where the engine is placed. The aircraft used in the previous phase of pilot training, the T-6, is a turboprop aircraft where the aircraft's weight is centralized towards the turboprop engine in the front of the aircraft such that the aircraft is less coupled at higher angles of attack.

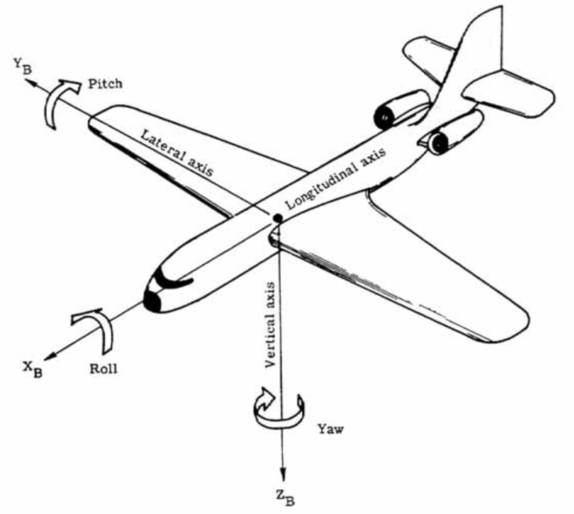


Figure 4-3: Body Axis System [31]

Dr. Thomas Yechout defines the three moment equations of motion in the body axis system as [32]:

$$\dot{P}I_{xx} + QR\left(I_{zz} - I_{yy}\right) - \left(\dot{R} + PQ\right)I_{xz} = L$$

$$\dot{Q}I_{yy} + PR(I_{zz} - I_{xx}) + (P^2 - R^2)I_{xz} = M$$

$$\dot{R}I_{zz} + PQ\left(I_{yy} - I_{xx}\right) + \left(QR - \dot{P}\right)I_{xz} = N$$

Angular Acceleration   Gyroscopic Precession   Coupling Terms

  - Where:
    - L, M, N = Moments about the x, y, z axis respectively
    - P, Q, R = Roll, Pitch, and Yaw rates respectively (angular velocity)
    - I_{xx}, I_{yy}, I_{zz} = Moments of Inertia (Resistance to rotation about that axis)
    - I_{xz}, I_{yz}, I_{xy} = Products of Inertia (Indications of symmetry about the aircraft)
  - In the context of this unsafe control action, the coupling terms in the rolling moment (L) equation is relevant in the context of the training program. Angular acceleration and velocity about the x-axis (P and $\dot{P}$) are assumed to be negligible

during a landing approach. The I_{zz} and I_{yy} are always positive; however with a constant pitch during an aerobraking maneuver, the gyroscopic procession term is negated. I_{xz} is notably different for the T-6 and the T-38; high-performance aircraft have higher concentrations of mass in the two negative quadrants of the xz plane.

Figure 4-4: The T-6 Texan II (Top) and the T-38C Talon (Bottom) [33] [34]

- The T-6 has a high concentration of mass towards the nose of the aircraft because of the turboprop engine, whereas the T-38 has a higher concentration of mass towards its turbojet near the tail. Isolating the coupling terms:

$$-(\dot{R})I_{xz} = L$$

    - Positive angular acceleration on the rudder results in a negative rolling moment—scaling to the product of inertia from each aircraft. In other words, the right rudder (negative angular acceleration) induces a positive roll (right-wing down).
    - The rolling moment is more prominent in the T-38 due to its higher I_{xz} and lower I_{xx} compared to the T-6. Furthermore, in this scenario, the T-38 inputs the right rudder at a higher angle of attack, further exacerbating the rudder-roll coupling. It is likely that during training for the T-6, students may have been able to use the rudder to correct centerline control on final approach with minimal consequences. In a high-stress scenario, students may fall back on their instincts learned from the T-6 to mitigate their actions.
  - In high-stress scenarios such as this accident, there is little time to abide by the conventional procedures of verbally and tactilely affirming transfer of aircraft control. In critical phases of flight, the transfer of aircraft control happens within seconds and sometimes with little communication between the pilots due to the criticality and timely nature of the situation. The student was likely unaware that the instructor was attempting to take control of the aircraft because in these circumstances, there is not enough time to verbally and haptically affirm a transfer of aircraft control, and there exist no other feedback redundancies in the aircraft which would establish a transfer of aircraft control.
  - The student had a series of unsatisfactory sorties beforehand and was likely stressed about the formation landing. Using rudder on the final approach is not a common practice taught by instructors. However, the AIB report states that the student excelled in the T-6 and was likely extremely well-versed in aircraft controls. Although the T-38 clearly outlines not to use the rudder during a final approach, the T-6 does encourage the use of the rudder "keep the fuselage aligned with the landing runway" [20]. This is a conflicting mental model derived from the structure of pilot training; because the student excelled in the T-6, it is likely that in the situations of high stress, the student reverted to the techniques that he used in the T-6 and thus used the rudder to try and correct the fuselage position.
  - The student likely had a conflicting mental model from different instructors he had flown with. As mentioned before, the limitations of instructors can vary based on experience. What the student may have thought was a safe position for one instructor pilot may not have been safe for another instructor pilot. By receiving conflicting feedback from various instructors over a series of many different sorties, the student likely had an inconsistent mental model throughout training on the ideal position/technique for the given maneuver.
- Control Structure Flaws:
  - The instructor did not provide appropriate cueing to the student as the student approached the training limitations. This could happen if the instructor's mental model of the student is flawed or incomplete.

Recommendations:

- UPT must emphasize the differences in flying qualities between the T-6 and T-38 as part of the training program. Making students more aware of old T-6 habits that do not translate to the T-38 would give students a foundation to reference during training. It might also be helpful for instructors to parallel maneuvers such as slow flight to landing approaches to demonstrate the rudder-roll coupling during landing. An alternative would be to use boldface or use emergency procedures to highlight the importance of not using the rudder on final approach.
- An alternative and redundant feedback mechanism must be implemented in the transfer of aircraft control procedure. There must be a clear way to communicate the transfer of aircraft control in these circumstances where there is neither time for verbal nor haptic confirmation. One option is to design a salient alert into the T-38 that can indicate a transfer of control authority redundantly through other means than purely through communication between the two pilots. A solution the program office could implement would be to install a button on the flight control stick that would alert the student that the instructor is attempting to control the aircraft.
- Students must be encouraged to constantly communicate their intentions and process model with the instructor even during critical phases of flight. One of the reasons the instructor may not have assumed control of the aircraft relates to the misalignment of the student's incomplete process model and the instructor's process model. An important safety constraint of the instructor is maintaining an updated process model of the student's capabilities. If the instructor is not receiving any feedback on the student's process model, the instructor cannot adequately assess if the student is acting on a flawed process model. Therefore, it is an equally important safety constraint for the student to communicate intentions and updates of the student's process model.
- Provide resources for students to manage stress. The student was placed on the Commanders Awareness Program (CAP), which is an indication that the student may be removed from pilot training with unsatisfactory performance. The added title of "CAP" may have added stress to the student that likely affected flight performance.

Mishap Instructor Pilot 1:

Safety Requirements and Constraints:

The instructor's primary role is to ensure the safety of the flight and properly instruct and guide the student through the training sortie. The instructor must communicate control authority and transfer of aircraft control with the student while also managing the mission profile and ensuring adherence to training limitations. The instructor must effectively communicate instruction and guidance to the student and must use safe judgment in assessing the risk of the profile and taking the flight controls when appropriate. As highlighted before, communication with the student is vital as a safety constraint. The instructor must keep an updated process model of the student's capabilities and correct the student's flawed process model when appropriate.

Unsafe Control Action:

As the aircraft was on final approach, MIP1 incorrectly assessed the situation and took control of the aircraft past the point where the situation was recoverable. When MIP1 took control of the aircraft, there was little he could do to recover the situation.

Context in Which the Decision was Made:

- Environmental and Behavior Shaping Factors
    - Experienced instructors may let students go past limitations to facilitate learning. It is important to recognize that these instructors are not negligent or overconfident. The instructor specifically is taught to be as hands-off as possible, allowing the student to control the aircraft as much as possible. If a correction still needs to be made, the instructor typically outlines exactly what the student needs to do to correct (e.g., "you are left of centerline, use a little right stick," "you are 20 knots slow, throttle up"). Finally, the instructor will take the stick and correct the aircraft if all else fails. Each of these is reflected in the grade card that the student receives at the end of the sortie; no correction or a slight hint is considered "Good" or a G on the grade card, and verbal consultation is regarded as a "Fair" or F on the grade card. Finally, if the instructor takes control of the aircraft during the accident, it is considered an "Unsatisfactory" or U.
    - The LMA and the HMA pressure the instructor to ensure that the student makes it through the program to meet the pilot demand. For most instructors, the intention is to let the student have as much flying time as possible and have as much opportunity to correct mistakes as possible. If the student's grade depends on the instructor not taking the stick, the instructor will be less motivated to take control of the aircraft in an attempt to keep the student in the program. In this scenario, the student was on CAP, which meant failing the student would likely remove him from the program entirely. In this scenario, the instructor has a conflicting mental model where he may let the student fly close to the limits of training with the impression that the student will be able to correct the error and stay in the program.
    - Instructors are bound by their squadrons and the HMA to limitations outlined in their regulations. However, each instructor has different experiences with students. Instructors also have different levels of tolerance as to when they find it appropriate to take the flight controls. This line gets blurred during critical phases of flight, and specifically in this circumstance—the student's progress check. This ties into the discussion of safety culture between the HMA and the flight training squadrons, as the mission is to get as many students through the program as fast as possible to meet the pilot demand—which further discourages instructors from taking appropriate actions. There were high stakes placed on the student to pass the sortie, which the instructor was completely aware of—and because of the culture built into the high pilot demand was likely discouraged from taking the stick from the student. It is possible that the instructor was doing everything he could to coach the student through the landing without taking the stick (such that the student would not fail out of pilot training).
- Control Structure Flaws:

  - The instructor’s mental model of the student was incomplete due to the lack of feedback from the student. The student did not provide adequate feedback to the instructor about his intentions and therefore, the instructor did not see a need to assume control of the aircraft early.
  - The flight crew lacked a redundant source of communication for the transfer of aircraft control. During the accident, the pilots had seconds to make critical decisions. The issue of coordination and communication here comes from there only being an auditory transfer of aircraft control. The transfer of aircraft control involves statements and affirmations from both pilots as well as a tactile shake of the control stick to confirm that one party has control of the aircraft. The time-sensitivity of critical phases of flight eliminates the redundancy of tactile confirmation. There is inadequate feedback to the student to relinquish control of the aircraft in critical phases of flight.
  - Different instructors may have different ways of communicating with the student. For instance, if the student needed to correct to centerline positioning, one instructor may have said, “use the right stick to get back on centerline.” In contrast, another instructor may have only given the student, “you are off centerline.” The student may react differently and make a different decision based on what different instructors say. The student may have conflicting mental models between different instructors that may affect decision-making during periods of high stress.

Recommendations:

- A possible mitigation for the disparity between instructor execution would be to perform more continuation training (CT) flights between experienced and inexperienced instructors. CT flights may slow down the rate of training, however it may be worth it to reduce the variation in training methods between instructors of varying experience.
  - An alternative to this mitigation would be to design different limitations for experienced instructors versus inexperienced instructors. However, this alternative would introduce further cognitive dissonance to students as they would be juggling two different mental models of experienced and inexperienced instructor limitations. It is recommended that the students are only presented with one mental model regarding instructors’ limitations.
- There is a lot of pressure on the Instructor Pilots to meet the demands of the Air Force. It may be worth exploring avenues to place less demand on the instructors and further emphasize safety culture regardless of the pilot demand. The USAF is exploring these avenues with programs such as UPT 2.5.
- Students must fly with different instructors so that students can experience a variety of different instructor techniques. However, it may be advantageous for students should stay with instructors with similar training limitations in situations where the student is on CAP or nearing a progress check. This would give students more consistency and reduce stress since they know that the instructor will have the same tolerance as the previous flight. This would also allow the instructor to build a more complete mental model of the student’s capabilities. When the student is not providing adequate feedback to the instructor (such as during critical phases of

flight), an instructor with precedent for the student's capabilities will have a more complete mental model to base safety critical decisions.

LMA (25th FTS and 5th FTS):

Safety Constraints and Requirements:

Each squadron must relay any procedures and safety protocol from the HMA down to the instructors and the students. The squadrons are responsible for pairing students and instructors to ensure the most effective training. Therefore, the squadrons must communicate feedback from other instructors on a student's performance, and squadrons must standardize procedures.

Unsafe Control Action:

The squadrons may have not effectively communicated all the information about the student's performance to the instructor, contributing to the instructor's incomplete mental model of the student.

Contextual Factors:

- Environmental and Behavioral Shaping Factors:
    - Students fly with a variety of instructor pilots during UPT. By flying with a wide variety of instructor pilots, they are exposed to a variety of different flying and training techniques that they can apply to their own practice. This inherently creates many different mental models for students based on whom they are flying with.
    - Because the instructor pilot was in a reserve squadron, it is possible that he cycled through recently and was only recently introduced to MSP1. With limited knowledge of the student, MIP1 did not have a complete mental model of the student's capabilities.

Recommendations:

- Aligning the schedule of the reserve squadrons to specific student rotations may help instructors get more exposure to students and learn about their training performance as they progress through the program. The AIB report does not explain how much MSP1 and MIP1 have flown together beforehand. Pairing MSP1 with an experienced instructor that he was comfortable with may have helped reduce stress during the flight and assure that the instructor flying with the student has a more complete mental model.

Higher Mission Authority:

Safety Constraints and Requirements:

The higher mission authority, which includes Air Education and Training Command (AETC), the 71st Flying Training Wing (71 FTW), 340th Flying Training Group (340 FTG), and the higher levels of USAF command, is responsible for the underlying safety culture in the squadrons. The HMA must not provide conflicting process models to the squadrons. The HMA must clearly outline its safety procedures and communicate any changes. The HMA is also responsible for equipping each squadron and must ensure that each training squadron is appropriately equipped for each training mission.

Unsafe Control Action:

The high demand for pilots forces the HMA produce pilots as fast as possible. The large-scale mission-driven pressures on the HMA have led to increased pilot production without systemic change to adjust for the demand.

Contextual Factors

- Environmental and Behavior Shaping Factors:
  - Every squadron in the Air Force holds safety as the number one priority. Considering the discussion above regarding the extremely high pilot demand, the HMA wants safety to be the number one priority. However, the HMA is also placing an increased emphasis on producing new pilots. This conflict of interest puts the highest stress on instructor pilots.
  - The USAF is experiencing an issue with retaining pilots, and instructor pilots are often overworked.
- Control Structure Flaws:
  - HMA is responsible for coordinating manning among all the flying training squadrons across all the UPT bases and pipelines. The high demand on pilots is problematic for the HMA, as their resources are spread thin and it is difficult to provide the proper manning for each squadron.

Recommendations

- Collect data on the maneuvers that lead to the most accidents and add additional training sorties specifically tailored toward the maneuver.
- Reduce the need for pilots by integrating more unmanned aircraft that can operate through teaming. This would allow the USAF to reduce the need for pilots while still maintaining a comparable projection of power.
- Reduce the need for instructors through the use of simulators. Although not a perfect substitute, simulators allow students to learn the basics of flying without placing such a demand on the instructors. Currently, the USAF is experimenting with simulators to find a proper balance between flight training in the aircraft and flight training with simulators.
- Programs in development such as UPT 2.5 should help reduce the workload of instructor pilots. STPA should be conducted on the new program to mitigate potential hazards.

Air Traffic Control

Safety Constraints and Requirements:

Air traffic control must give clearance and instruction for deconfliction for multiple aircraft looking for landing clearance.

Unsafe Control Action:

ATC also did not provide useful feedback to the flight crew that they were out of training limitations.

Contextual Factors

- Environmental and Behavior Shaping Factors:

    - ATC sees many training sorties in a day from the tower and likely knows what a safe and dangerous approach looks like. ATC may notify a flight crew if they see a deviation from a safe approach, however the responsibility is placed on the instructors.
- Control Structure Flaws:
    - Another factor in play was the communication between the HMA and ATC. It is likely that there was an operations supervisor in the tower with ATC during the accident. Although the contribution may have been minimal, HMA could have potentially relayed valuable information (e.g., “the aircraft is too low to make corrections” or “keep an eye out on this flight, student is on an elimination check”) to ATC who could then reach the pilots directly.

Recommendations:

- ATC could be trained to identify hazardous conditions from their perspective in the control tower and potentially relay information that is unclear to the flight crew (ATC does update conditions however they could contribute to training).
- Students on CAP should be treated as cautiously as possible and not put in a potentially hazardous condition.

It seems that the instructor knew that in the phase of training that the student was in, the student needed to get a good grade to stay in the UPT program. A good grade indicates that the instructor is only allowed to hint towards corrections and not take the stick. Thus, what likely happened is that the instructor was cueing the student all the way down to the extremely critical phase of the final approach. Within seconds, the instructor needed to make the critical decision whether to take the stick or not (removing the student from pilot training or having a hard landing). Ultimately it seems that the instructor took the stick too late. There are a lot of factors in this accident, but the instructor’s incomplete mental model of the student’s capabilities, inadequate feedback from the student to the instructor, the pilot demand coming from the HMA down to the squadrons, the safety culture embedded in experienced instructor pilots, and finally the communication and coordination between the student and the instructor are all relevant considerations in moving forward with improvement.

4.6. Improvement Program

4.6.1. Recommendations

On a grand scale, reducing the high demand for pilots would place less stress on the instructors. The 2018 report on the pilot training shortage focused on increasing the initiatives for pilots to use the Reserve Component in pilot training pipelines for pilot loss mitigation. The report also states that the long-term solution for the pilot shortage is increased production, which is noted that it will likely yield positive results in some forces (such as Mobility Air Forces), however for Combat Air Forces the same issue will likely be ever present. Based on these findings, there is an opportunity to reduce the pilot demand by making more flexible options for the reserve and guard components and potentially transitioning civilians into military aviation. The USAF must also consider incentives for retaining current pilots. STPA should be conducted with the development of new pilot training initiatives to help identify potential scenarios that may trace back to hazards.

As outlined above, there is a lot demanded on the instructor pilots in the USAF that creates a conflict of interest for instructor pilots. The most evident recommendation would be to reduce the demand for instructor pilots. The USAF is already moving towards this technique by experimenting with the use of simulators in UPT. These are not a perfect replacement for actual flying; however, there needs to be increased funding and effort towards moving students towards the use of simulators so that the demand placed on Instructor pilots can be reduced.

UPT must also work to eliminate conflicting mental models. Squadrons should consider clarifying and quantifying the training limitations and flying more continuation training (sorties flown between two instructors to compare instruction technique) between newer and more experienced instructors. This would reduce the mental model conflicts in students based on whom they fly with or what phase of training they are in.

Another useful consideration would be to implement an instructor anonymous feedback system, where students can anonymously give feedback to instructors. The anonymity would provide students protection when giving feedback about instructor techniques which can ultimately be used to help instructors better communicate to students.

HMA can also improve communications with ATC about the nature of certain training sorties. If HMA receives information from the squadrons that there is a training sortie involving a student struggling in the program, HMA can communicate that to ATC to help clear the airspace and take precautions before a hazardous situation develops.

Significant emphasis must be placed on assuring the instructor has a complete mental model of the student’s capabilities. This includes having previous instructors write in-depth notes of the student’s performance and areas where the student struggled. In the case of high-stress sorties such as progress checks, the student should fly with instructors that have flown with them before. This would ensure the instructor has a foundation of the student’s capabilities to influence decision-making. Having an evaluator fly with the student beforehand on an ungraded sortie would also provide a foundation of the student’s capabilities for the instructor. Students also need to communicate their intentions and thought processes to the instructor as much as possible to keep the instructor’s mental model of the student up to date.

In relation to the mental models of students flying the T-38 who have excelled in the T-6, instructors should note that the student will likely instinctually take from their mental model of the T-6 during high-stress environments and critical phases of flight. A more significant fix would be training students in the T-6 who plan to track T-38s to use less rudder on final approaches. Training should also emphasize aerodynamic and performance differences between the two aircraft to help broaden students’ situational awareness during their flight training.

Solutions to the lack of feedback regarding the transfer of aircraft control are discussed in the STPA portion of this thesis.

4.6.2. Implementation

On the operational side, training students to be less dependent on the rudder during their training in the T-6 could help change their mental model down the line as the students track T-38s. This would only apply to students who plan on tracking the T-38. This does not imply changing the syllabus. Early exposure to the consequences of rudder use in highly coupled aircraft at high angles of attack may help students down the line.

Squadrons could open discussion on implementing more CT flights for instructors during the program. Another possible implementation would be to emphasize safety culture over operations. This would help reduce the mental model conflict among instructors, who already have enough mental model conflicts as it is. CT sorties among instructors could be dedicated towards Pilot Instructor Training (PIT)—where one instructor acts as a student while the other takes the role of the instructor. Instructors would then compare instruction techniques and ideally standardize the most effective techniques. This would reduce the mental model conflicts among the student if they were hearing consistent information from the instructors.

4.6.3. Feedback

Feedback for pilot training would be largely subjective, however the most important feedback would be from the instructors and the students and vice versa. There needs to be a more open conversation over the conflicting mental models in both the instructors and the students, which needs to be relayed to the squadron level and the HMA. Students should also be able to anonymously submit feedback to instructors on what worked well for them and what could have been communicated better. This could be reviewed by the squadron leadership and evaluated for best practices.

4.6.4. Follow-Up

Squadrons should have a follow-up every month to discuss these matters. Any subsequent losses should be analyzed using CAST, and the recommendations should be compared with the recommendations found in this analysis.

4.7. A comparison with the AIB Findings:

On the surface, the SIB findings appear to be the factors that directly lead to the accident. However, the exclusion of system-related events, proclivity to assign human error, and subjectivity of the board president's analysis limit the findings of the SIB process. When the accident is placed in the context of the factors discussed above, more takeaways and improvements can be made to the program. Table 4-2 outlines the differences in perspective between the SIB and CAST.

As a reminder, the purpose of this analysis was not to place blame on more parties. Rather the intent is to look past the immediate causal factors and "root causes" to find areas of improvement that will better the UPT system as a whole and make the program safer going forward.

Table 4-2: Comparison of the SIB and CAST Perspectives

	SIB Perspective [26]	**CAST Perspective**
Mishap Instructor Pilot	• Inaccurate real-time risk assessment • Failed to take control of the aircraft as the situation developed—let students error progress further to maximize learning	• The instructor made an accurate risk assessment for the information available to him. • The instructor's mental model of the student's capabilities was flawed. • The instructor's believed the student could recover the aircraft and therefore did not intervene.

	• MIP1 elected to not intervene because he thought MSP1 could safely complete landing
	• Should have assumed control of the aircraft when the student prematurely aerobraked and lifted off the runway.
		• The instructor's incomplete mental model was influenced by:
		  ○ A conflict of interest where the instructor wanted the student to remain in the program and fix his mistake.
		  ○ The instructor did not receive adequate feedback from previous instructors regarding the student's capabilities. (Inadequate documentation in the student's grade cards)
		  ○ The instructor did not receive adequate feedback from the student regarding his capabilities.
		  ○ The instructor had not flown with the student before and therefore had no foundation for the student's capabilities.
		• The instructor likely attempted to assume control of the aircraft. However, there is no redundant source of feedback to inform the student to relinquish control of the aircraft.

Mishap Student Pilot	• Made inappropriate flight control input during landing—no reason for instructor to expect the rudder input. • Lacked visual scan during formation approach	• The student made a control input congruent with how he handled high stress scenarios in the previous phase of pilot training. • The student performed an appropriate visual scan during the formation approach and attempted to correct the approach using a flawed process model. ○ The student's flawed process model is based in the previous phase of training flying the T-6. It is common practice in the T-6 to use rudder for centerline control. In high stress situations, it is reasonable that the student would fall back on the habits developed in the T-6. For this reason, it should be emphasized to students the differences in flying qualities of the T-6 and T-38. • The student could not provide adequate feedback to the instructor due to the importance of the sortie.

		• The student could not determine when the instructor wanted the student to relinquish control of the aircraft.

5. SYSTEMS THEORETIC PROCESS ANALYSIS (STPA)

In contrast to CAST, which is used to analyze the causes of an accident that has already occurred, STPA is a proactive analysis method that is used to identify the causes of potential accidents that have no happened but could. The information obtained can be used to redesign or operate the system differently in order to prevent accidents before they occur.

The process consists of four steps seen in Figure 5-1:

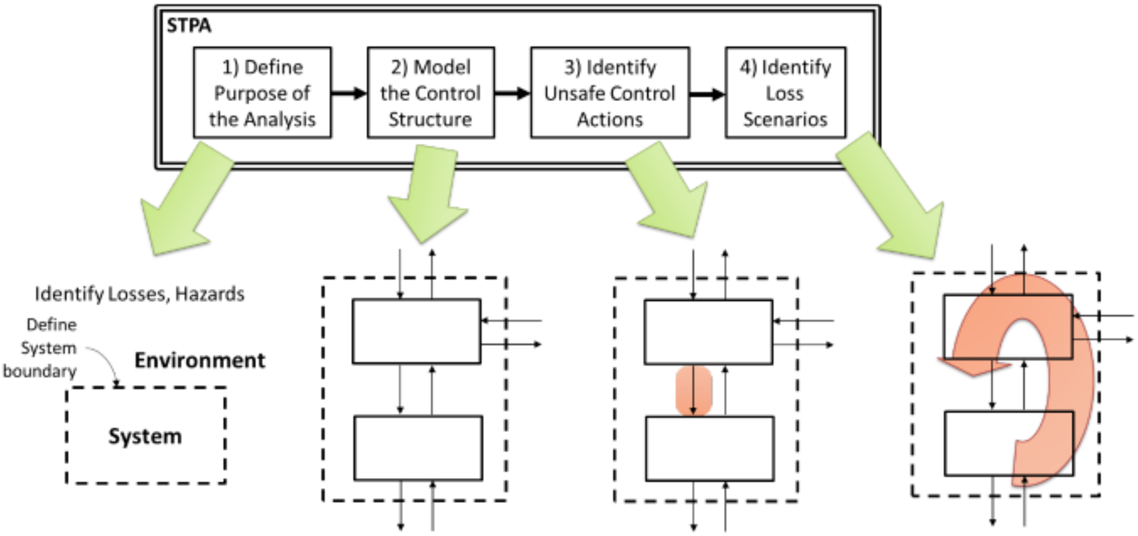


Figure 5-1: Overview of the Basic STPA Method [28]

5.1. STPA Step 1: Define Purpose of Analysis

In the first step of STPA, the stakeholders define losses that are deemed unacceptable. The following losses can be reasonably derived from the stakeholders (e.g., the higher mission authority, ATC, and the flight crew):

Table 5-1: System Losses

Loss ID	Loss Description
L01	Loss of life or injury
L02	Damage to aircraft or equipment
L03	Loss of training mission

5.1.1. System Hazards

A hazardous condition is defined as “a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss”—the loss in this case the accident—where the aircraft entered an unrecoverable state on final approach [28]. The system hazards are also linked to each loss to establish traceability. The system-level hazards are defined in Table 5-2:

Table 5-2: System Hazards

Hazard ID	Hazard Description	Loss Link

H01	The aircraft is uncontrollable	L01, L02, L03
H02	Structural integrity of aircraft is violated	L01, L02, L03
H03	Training limitations are exceeded (minimum separation from other aircraft, objects, or terrain, centerline control, airspeed, aimpoint, flight path)	L01, L02, L03
H04	Student pilot continues to fly aircraft after nearing instructor limitations	L01, L02, L03
H05	Aircraft environment is harmful to human health or not conducive to proper human control	L01, L03
H06	Training mission does not have proper guidance	L03

5.1.2. System Constraints

Table 5-3 details the system level safety constraints required to prevent the system hazards listed above. System constraints are also used to define how the system must respond in the case that hazards do occur [28]. Due to the nature of pilot training, the constraints need to serve the dual purpose of preserving the life of the flight crew and preventing the accident, while simultaneously not hindering the training mission.

Table 5-3: System Constraints

Constraint ID	**Constraint Description**	**Hazard Link**
C01	Aircraft must remain controllable	H01
C02	If Aircraft is uncontrollable, then the aircraft must have appropriate egress procedures and contingencies to mitigate further loss.	H01
C03	Flight crew must communicate who is controlling during the final approach	H01
C04	If flight crew cannot communicate, there must be procedures to establish responsibilities of each controller.	H01
C05	Student pilot must be properly trained in flight procedures	H01
C06	If student pilot is not properly trained in flight procedures, training and procedures must be in place to train the student and operate the aircraft safely	H01
C07	Aircraft structural integrity must maintain during the final approach	H01, H02
C08	If aircraft structural integrity is lost, the structural violation must be detected and properly communicated to the operators.	H01, H02
C09	If aircraft structural integrity is lost, there must be procedures in place to return safely to base or egress the aircraft.	H01, H02
C10	Flight crew must stay within training limitations	H01, H02, H03
C11	If flight crew breaks training limitations, their status must be communicated to other local controllers and operators.	H01, H02, H03

C12	If flight crew breaks training limitations, there must be procedures in place to return safely to base or egress the aircraft.	H01, H02, H03
C13	Instructor Pilot must be trained to recognize limitations	H01, H02, H03
C14	If the instructor pilot is not trained to recognize limitations, other controllers must be able to detect or recognize limitations.	H01, H02, H03
C15	Instructor Pilot must take aircraft before exceeding limitations	H01, H02, H04
C16	If the instructor pilot does not take aircraft before exceeding limitations, procedures must be in place to recover the aircraft or mitigate further loss.	H01, H02, H04
C17	Instructor Pilot must be able to recover the aircraft after exceeding limitations	H01, H02, H04
C18	If the instructor pilot cannot recover the aircraft after exceeding limitations, procedures must be in place to mitigate further loss	H01, H02, H04
C19	Aircraft environment must be suitable for human health	H05
C20	If the aircraft environment is not suitable for human health, the condition must be detected, and measures taken to prevent mission degradation.	H05
C21	Higher Authorities must provide guidance for the mission.	H06
C22	If higher authorities cannot give proper guidance, procedures must be in place to complete training mission and return safely.	H06

5.2. STPA Step 2: Model the Control Structure

The control structure follows the same model used in the CAST analysis except with the addition of a software enabled controller to account for advancements in future USAF Jet trainers. The T-7 is planned to be the next generation fighter trainer with increased autonomy. An aircraft software enabled controller (ASEC) will be implemented within the control structure. Because the T-7 is still in development, the model will be based off a hypothetical next-generation tandem supersonic jet trainer.

As seen in Figure 5-2, an additional controller and control action is added to the aircraft's actuation—indicating there are now three possible controllers for the aircraft's physical processes. The implications of multiple controllers were discussed in the CAST analysis; however, another controller adds another level of complexity, which will be revisited in STPA steps 3 and 4.

Like the CAST analysis, instructor-student shared control implies that the student is refining an incomplete process model with the instructor's assistance. The misalignment between the instructor's process model and the student's incomplete process model remains a foundation for unsafe control actions. The addition of the ASEC adds another process model that the instructor must ensure is complete.

5.2.1. Control Structure

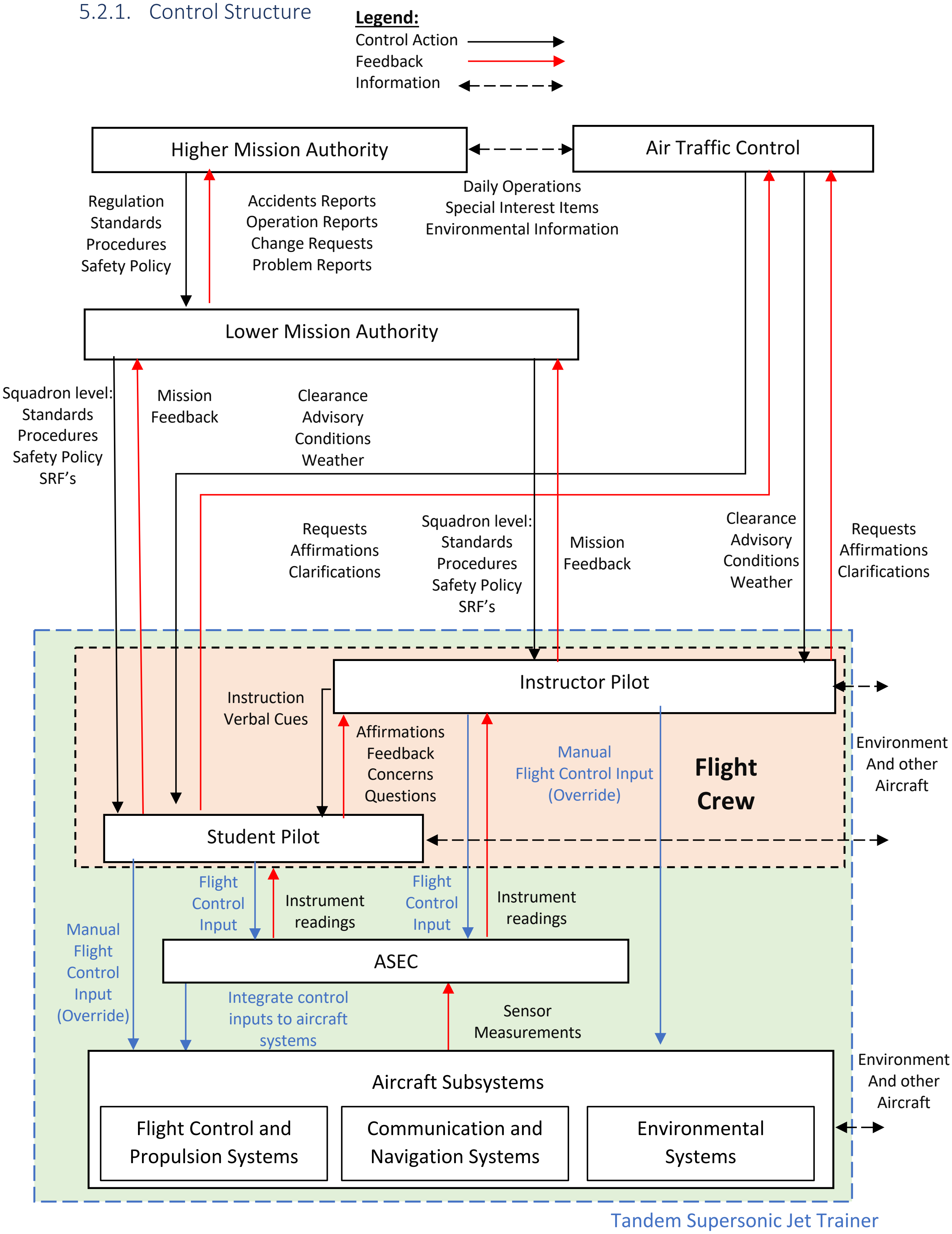


Figure 5-2: Control Hierarchy for a Student Sortie in UPT (Changes in Blue)

5.3. Responsibilities

Higher Mission Authority:

- R-1.1: Educate Squadrons on the policies and procedures passed down through ATC
- R-1.2: Define rules, regulations, and standards for squadrons
- R-1.3: Approve additions and changes to the UPT syllabus
- R-1.4: Ensure the T-38 is equipped with the most up-to-date safety technology
- R-1.5: Make appropriate changes from the recommendations from the squadrons

Air Traffic Control:

- R-2.1: Monitor and direct the movement of aircraft on the ground and in the air
- R-2.2: Control all ground traffic at airport runways and taxiways
- R-2.3: Issue landing and takeoff clearances to flight crews
- R-2.4: Inform pilots about weather, runway closures, and other critical information
- R-2.5: Alert airport response staff in the event of an emergency

Lower Mission Authority:

- R-3.1: Adhere to policy and procedures from the HMA
- R-3.2: Communicate changes to IP's and students
- R-3.3: Ensure consistent squadron level policies between the two squadrons
- R-3.4: Relay operator feedback to the HMA

Instructor Pilot:

- R-4.1: Ensure Safety of Flight.
- R-4.2: Ensure adherence to flight training syllabus.
- R-4.3: Ensure accurate mental model of the aircraft's status, mode, and position
- R-4.4: Adhere to HMA and ATC instruction.
- R-4.5: Ensure proper preflight mission analysis (to include pre-mission, ongoing mission, and post-mission)
- R-4.6: Conduct flight training sorties
- R-4.7: Stay within safe instructor limitations
- R-4.8: Clearly report student progress to student's grade card
- R-4.9: Ensure proper risk management and decision making (to include knowledge of general aircraft knowledge and emergency procedures).
- R-4.10: Ensure proper communication
- R-4.11: Ensure proper crew coordination and task management.
- R-4.12: Monitor aircraft decent profile
- R-4.13: Monitor aircraft airspeed, aimpoint, and altitude
- R-4.14: Ensure aircraft is controllable
- R-4.15: Ensure accurate mental model of the student's capabilities.
- R-4.16: Maintain situational awareness

Student Pilot:

- R-5.1: Adhere to flight training syllabus
- R-5.2: Adhere to HMA, ATC, and IP instruction

- R-5.3: Ensure proper knowledge of general aircraft knowledge and emergency procedures
- R-5.4: Ensure accurate mental model of the aircraft’s status, mode, and position
- R-5.5: Communicate areas of focus to the instructor
- R-5.6: Relay affirmations of instruction to the instructor
- R-5.7: Communicate transfer of aircraft control to the instructor
- R-5.8: Operate and manage aircraft decent profile
- R-5.9: Operate and manage aircraft airspeed, aimpoint, and altitude
- R-5.10: Control the aircraft

Aircraft Software Enabled Controller (ASEC): the autonomous control agent that takes operator input and uses specific control algorithm to actuate the aircraft’s physical processes.

- R-6.1: Integrate commands from the flight crew to the aircraft’s subsystems based on current aircraft mode selection.
- R-6.2: Enforce limitations on excessive commands from the flight crew.
- R-6.3: Provide assisted decision making to the operator

Aircraft Subsystems: Including the Aircraft flight control systems (FCS) and propulsive systems, Aircraft Communication and Navigation Systems, and the aircraft’s internal environmental systems.

- R-6.1: Ensure proper communication between the flight crew
- R-6.2: Ensure proper communication between the flight crew and ATC
- R-6.3: Provide salient alert for transfer of aircraft control
- R-6.4: Provide salient alert for critical aircraft feedback (stall warning, altitude warning, decent warning, etc.)
- R-6.5: Provide feedback on the aircraft’s airspeed, position, and altitude (among other metrics)
- R-6.6: Conduct physical outputs of the operator’s input

5.4. STPA Step 3: Identify Unsafe Control Actions (UCA’s)

The next step is to identify the conditions in which UCA’s can lead to a hazardous state from the control structure. There are four possible ways for a control action to be unsafe:

1. Not providing the CA causes a hazard
2. Providing the CA causes a hazard
3. CA is applied to early, too late, or out of order
4. CA is stopped too soon or applied too long

The resulting UCA’s are used to generate causal scenarios. UCA’s do not always guarantee that a hazard will always result; in the best-case scenario, the UCA can be avoided by the operator. STPA is a worst-case analysis method, and therefore under the worst conditions, the UCA will guarantee a hazard. This implies that even with safeguards in place, the worst-case scenario highlights the situations where the safeguards may not operate as intended. UCA’s contain five parts: the source or controller providing the control action, the type of unsafe control action (listed above), the control action itself, and finally, a link to the system hazards. The following are UCA’s related to the control structure. The instructor pilot and student pilot will be simplified down to ‘flight crew’ for organizational analysis except for the control action between the instructor and the student. Below are examples of potential UCA’s for the Instructor Pilot and the Aircraft Software Enabled controller (ASEC):

Table 5-4: UCAs from the Student to the Aircraft Subsystems

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Student Pilot overrides ASEC	10.01: Student does not override the ASEC when the instructor is unable to override.	H01, H02, H03, H04, H06	10.03: Student overrides the ASEC during a critical phase of flight without command from instructor.	H01, H02, H03, H04, H06	10.05: Student overrides the ASEC too early before being instructed.	H01, H02, H03, H04, H06	10.07: Student stops overriding ASEC too soon before the instructor can safely fly the aircraft.	H01, H02, H03, H04, H06
	10.02: Student does not override the ASEC when cued by the instructor.	H01, H02, H03, H04, H06	10.04 Student overrides the ASEC without enough experience on manual controls.	H01, H02, H03, H04, H06	10.06: Student overrides the ASEC too late after being instructed.	H01, H02, H03, H04, H06	10.08: Student overrides the ASEC for too long after the instructor cues the student to resume flight augmentation.	H01, H02, H03, H04, H06

Table 5-5: UCAs from the IP to the Student

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Flight Instructor verbally cues the student pilot	11.01: Flight Instructor does not cue the student pilot when the student is reaching the instructor's limits of training.	H01, H03, H04, H06	11.07: Flight Instructor cues the student when the student is not outside the instructor's training limitations.	H01, H03, H04, H06	11:10: Flight instructor cues the student out of order from intended procedure as the student approaches the instructor's limitations	H01, H03, H04, H06	11.16: Flight Instructor stops cues too early during critical phases of flight or aircraft deconfliction	H01, H03, H04, H06
	11.02: Flight Instructor does not cue the	H01, H03,	11.08: Flight Instructor cues the	H01, H03,	11.11: Flight instructor cues the student too early before the	H01, H03,	11.17: Flight Instructor takes too long to provide verbal	H01, H03,

	student during critical phases of flight.	H04, H06	student during critical phases of flight	H04, H06	student needs to make corrections.	H04, H06	cues during critical phases of flight or aircraft deconfliction	H04, H06
	11.03: Flight Instructor does not cue the student during aircraft deconfliction.	H01, H03, H04, H06	11.09: Flight instructor cues the student during aircraft deconfliction.	H01, H03, H04, H06	11.12: Flight instructor cues the student too late after the student has already exceeded the instructor’s limitations	H01, H03, H04, H06	11.18: Flight instructor stops cues too early as the student approaches training limitations	H01, H03, H04, H06
	11.04: Flight instructor cannot cue the student when the student is reaching the instructor’s limits of training.	H01, H03, H04, H06			11.13: Flight instructor cues the student out of order from the intended procedure during critical phases of flight or aircraft deconfliction.	H01, H03, H04, H06	11:19: Flight instructor takes too long to provide verbal cues as the student approaches training limitations.	H01, H03, H04, H06
	11.05: Flight instructor cannot cue the student during critical phases of flight	H01, H03, H04, H06			11.14: Flight instructor cues the student too early during critical phases of flight or aircraft deconfliction	H01, H03, H04, H06		
	11.06: Flight Instructor cannot cue the student during aircraft deconfliction.	H01, H03, H04, H06			11:15: Flight instructor cues the student too late during critical phases of flight or aircraft deconfliction.	H01, H03, H04, H06		

A complete list of UCA’s and STPA analysis is in Appendix A.

5.4.1. Requirements

The UCA's can be rewritten as constraints on the behavior of each controller. The following tables are the translated constraints from the UCA's derived above.

Table 5-6: Controller Constraints for the Student to the Aircraft Subsystems

Student Pilot Unsafe Control Actions	Controller Constraints
SP-UCA 10. 01: Student does not override the ASEC when the instructor is unable to override.	SP-C-10.01: Student must override the ASEC when the instructor is unable to override
SP-UCA 10.02: Student does not override the ASEC when cued by the instructor.	SP-C-10.02: Student must override the ASEC when cued by the instructor.
SP-UCA 10.03: Student overrides the ASEC during a critical phase of flight without command from instructor.	SP-C-10.03: Student must not override the ASEC during a critical phase of flight without command from instructor.
SP-UCA 10.04: Student overrides the ASEC without enough experience on manual controls.	SP-C-10.04: Student must not override the ASEC without enough experience on manual controls.
SP-UCA 10.05: Student overrides the ASEC too early before being instructed.	SP-C-10.05 Student must not override the ASEC too early before being instructed.
SP-UCA 10.06: Student overrides the ASEC too late after being instructed.	SP-C-10.06: Student must not override the ASEC too late after being instructed.
SP-UCA 10.07: Student stops overriding ASEC too soon before the instructor can safely fly the aircraft.	SP-C-10.07: Student must not stop overriding ASEC too soon before the instructor can safely fly the aircraft.
SP-UCA 10.08: Student overrides the ASEC for too long after the instructor cues the student to resume flight augmentation.	SP-C-10.08: Student must not override the ASEC for too long after the instructor cues the student to resume flight augmentation.

Table 5-7: Controller Constraints for the Instructor to the Student

Instructor Pilot Unsafe Control Actions	Controller Constraints
IP-UCA 11.01: Flight Instructor does not cue the student pilot when the student is reaching the instructor's limits of training.	IP-C-11.01: Flight Instructor must cue the student pilot when the student is reaching the instructor's limits of training.
IP-UCA 11.02: Flight Instructor does not cue the student during critical phases of flight.	IP-C-11.02: Flight Instructor must cue the student during critical phases of flight.
IP-UCA 11.03: Flight Instructor does not cue the student during aircraft deconfliction.	IP-C-11.03: Flight Instructor must cue the student during aircraft deconfliction.
IP-UCA 11.04: Flight instructor cannot cue the student when the student is reaching the instructor's limits of training.	IP-C-11.04: Flight instructor must be able to cue the student when the student is reaching the instructor's limits of training.
IP-UCA 11.05: Flight instructor cannot cue the student during critical phases of flight	IP-C-11.05: Flight instructor must be able to cue the student during critical phases of flight
IP-UCA 11.06: Flight Instructor cannot cue the student during aircraft deconfliction.	IP-C-11.06: Flight Instructor must be able to cue the student during aircraft deconfliction.
IP-UCA 11.07: Flight Instructor cues the student when the student is not outside the instructor's training limitations.	IP-C-11.07: Flight Instructor must not cue the student when the student is not outside the instructor's training limitations.

IP-UCA 11.08: Flight Instructor cues the student during critical phases of flight	IP-C-11.08: Flight Instructor must not cue the student during critical phases of flight [causing a hazard]
IP-UCA 11.09: Flight instructor cues the student during aircraft deconfliction.	IP-C-11.09: Flight instructor must not the student during aircraft deconfliction [causing a hazard].
IP-UCA 11:10: Flight instructor cues the student out of order from intended procedure as the student approaches the instructor's limitations	IP-C-11.10: Flight instructor must cue the student in the correct order of the intended procedure as the student approaches the instructor's limitations
IP-UCA 11.11: Flight instructor cues the student too early before the student needs to make corrections.	IP-C-11.11: Flight instructor must not cue the student too early before the student needs to make corrections.
IP-UCA 11.12: Flight instructor cues the student too late after the student has already exceeded the instructor's limitations	IP-C-11.12: Flight instructor must not cue the student too late after the student has already exceeded the instructor's limitations
IP-UCA 11.13: Flight instructor cues the student out of order from the intended procedure during critical phases of flight or aircraft deconfliction.	IP-C-11.13: Flight instructor must cue the student in the correct order of the intended procedure during critical phases of flight or aircraft deconfliction.
IP-UCA 11.14: Flight instructor cues the student too early during critical phases of flight or aircraft deconfliction	IP-C-11.14: Flight instructor must not cue the student too early during critical phases of flight or aircraft deconfliction
IP-UCA 11:15: Flight instructor cues the student too late during critical phases of flight or aircraft deconfliction.	IP-C-11.15: Flight instructor must not cue the student too late during critical phases of flight or aircraft deconfliction.
IP-UCA 11.16: Flight Instructor stops cues too early during critical phases of flight or aircraft deconfliction	IP-C-11.16: Flight Instructor must not stop cues too early during critical phases of flight or aircraft deconfliction
IP-UCA 11.17: Flight Instructor takes too long to provide verbal cues during critical phases of flight or aircraft deconfliction	IP-C-11.17: Flight Instructor must not take too long to provide verbal cues during critical phases of flight or aircraft deconfliction
IP-UCA 11.18: Flight instructor stops cues too early as the student approaches training limitations	IP-C-11.18: Flight instructor must not stop cues too early as the student approaches training limitations
IP-UCA 11:19: Flight instructor takes too long to provide verbal cues as the student approaches training limitations	IP-C-11.19: Flight instructor must not take too long to provide verbal cues as the student approaches training limitations

5.5. STPA Step 4: Identify Causal Scenarios

After identifying the UCA's of the system, causal scenarios can be derived by analyzing the situations that would lead to each UCS. This step looks at each different controlled process and analyzes where and how UCA's could arise in the controlled process. Figure 5-3 shows the two types of scenarios that can occur.

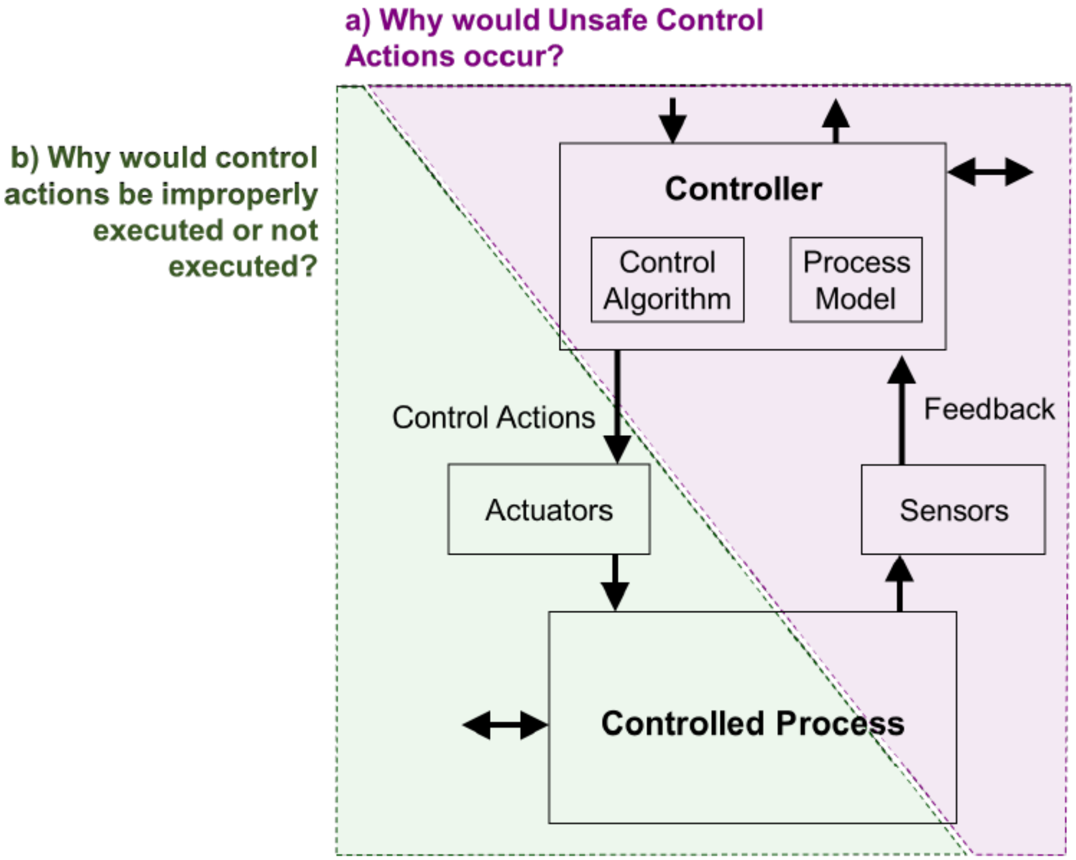


Figure 5-3: A Simplified Control Loop Subdivided into Different Reasons UCAs can Occur [28]

There are four general categories for where causal scenarios can be generated:

1. Unsafe Controller Behavior: including physical failures and failures related to the controller, inadequate control algorithms, unsafe control input, or inadequate process model.
2. Unsafe Feedback or Other Information: where the feedback/information leads to a hazardous situation. Feedback could not be received, or the feedback could be deemed inadequate for the controller.

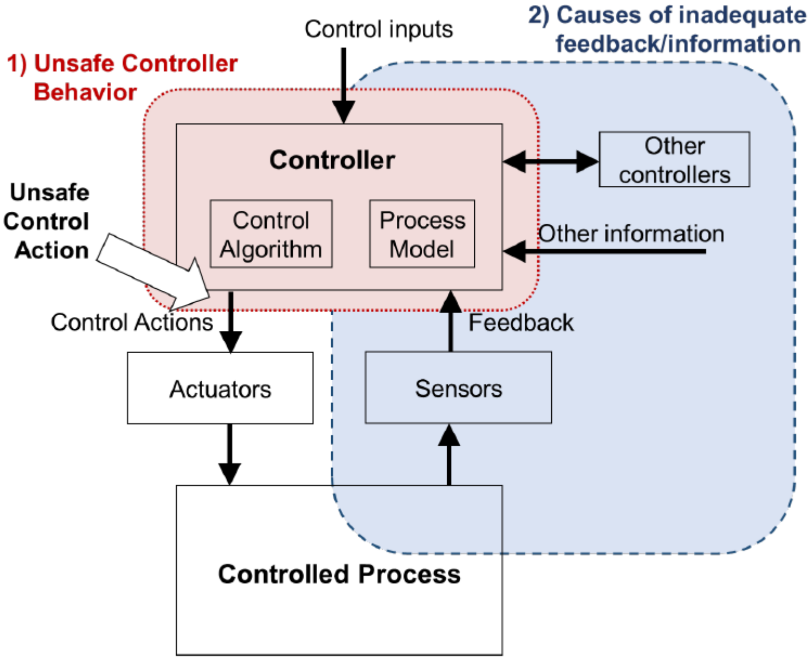


Figure 5-4: A Simplified Control Loop Illustrating Unsafe Controller Behavior and Inadequate Feedback [28]

3. Unsafe Controller Path: why a control action was not executed, or a control action was executed improperly based off the actuator's response.
4. Unsafe Process Behavior: why a control action was not executed, or a control action was executed improperly based off the controlled process.

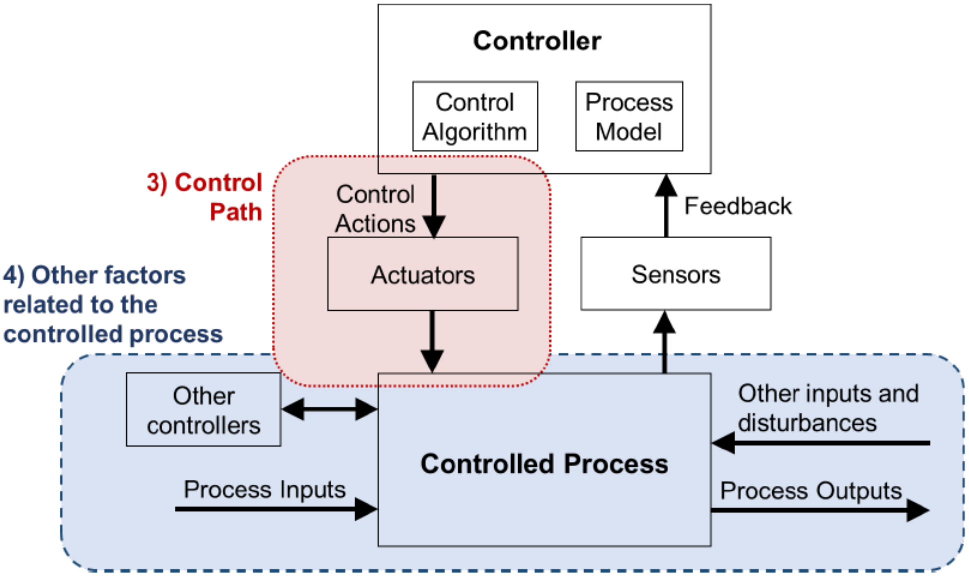


Figure 5-5: A Simplified Control Loop Illustrating Unsafe Control Paths and Controlled Processes [28]

In this case, the controlled process is the physical aircraft subsystems of the hypothetical next generation tandem supersonic jet trainer. Component failure of the physical subsystems is less of the focus of this analysis. External and environmental disturbances will be considered, but mostly in the context of a training scenario. The primary focus of the causal scenarios will be the breakdown of the controllers of the controlled processes.

The system is comprised of three types of controllers: organizational, automated, and human controllers. Organizational controllers consist of management, safety culture within the organization, and external factors contributing to how leadership influences operations.

Automated and human controllers are similar in the types of information that each requires and receive. An essential distinction between automated and human controllers is how each processes information. Automated control algorithms are responsible for generating control actions and maintaining an accurate process model. Maintaining an accurate process model requires information on the current state of the controlled process, the state of other controllers, the operational mode of the automation, and finally, the state of the human controller(s) [28]. Control algorithms directly receive information about the controlled process through sensors recording process variables. Even if a control algorithm issues a control action, the process model must still receive information about the process variables. Updating a process model based on control actions (rather than the actual state of the process) fails to account for latency, failed actuation, or execution. Operational modes are typically designated by a human controller and maintained by the control algorithm. In a flying context, the ASEC's model of the human controller is defined by the position of the flight controls. Many current systems use sensors to gauge other characteristics of human controllers, such as drowsiness or inattention. This will be discussed later in the causal scenarios.

Human controllers are also responsible for generating control actions and maintaining accurate process models. The distinction between a human controller's decision-making/mental processing and an automated controller's control algorithm is that human controllers are dynamic and decision-making can change based on the context of the scenario. Algorithms can be rewritten to reflect exactly what they were designed to do, whereas humans adapt their control actions based on the context of the situation. Verification and validation of control algorithms are also relatively straightforward. The closest comparable to verification and validation of human decision-making and proficiency is testing with evaluation criteria. In the context of flying, the human controller must maintain mental models of the control algorithm (ASEC), different operational modes of the ASEC, the controlled process (the aircraft), and other controllers (HMA/ATC). Inconsistencies in any of these mental models can lead to a UCA. In the context of tandem pilot training, the instructor must also maintain a mental model of the student pilot; this requires mental models of the student's own mental models. Inconsistencies in any of these mental models can also lead to a UCA. Figure 5-6 outlines the causal control model as described above.

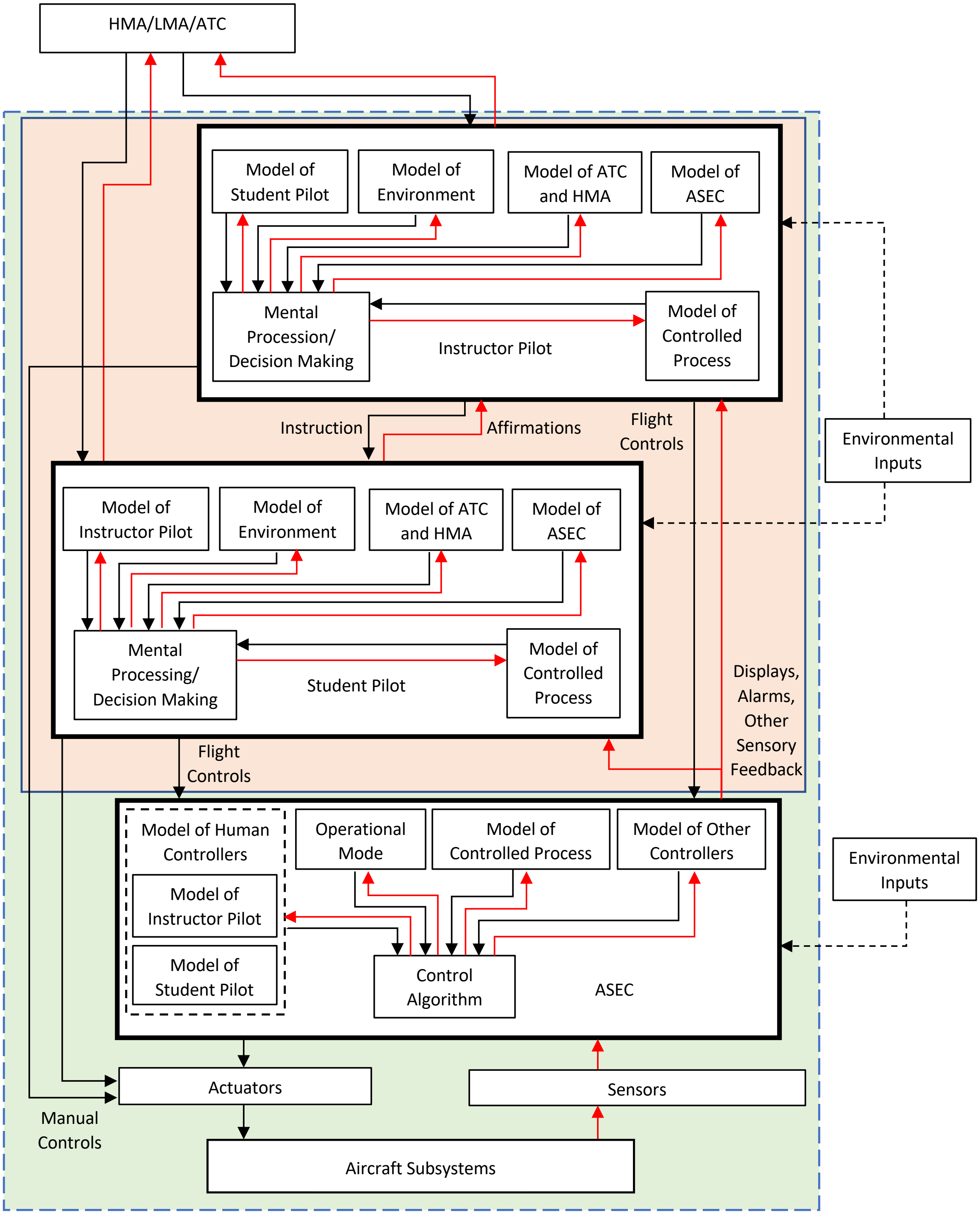


Figure 5-6: Causal Control Model of the Tandem Supersonic Jet Trainer

Because the instructor pilot's primary responsibility is the safety of flight and to teach the student, the instructor must construct the most accurate mental model of the student's abilities, general knowledge (GK), and experience with other instructors. The instructor's mental model can be isolated and further broken down in Figure 5-7:

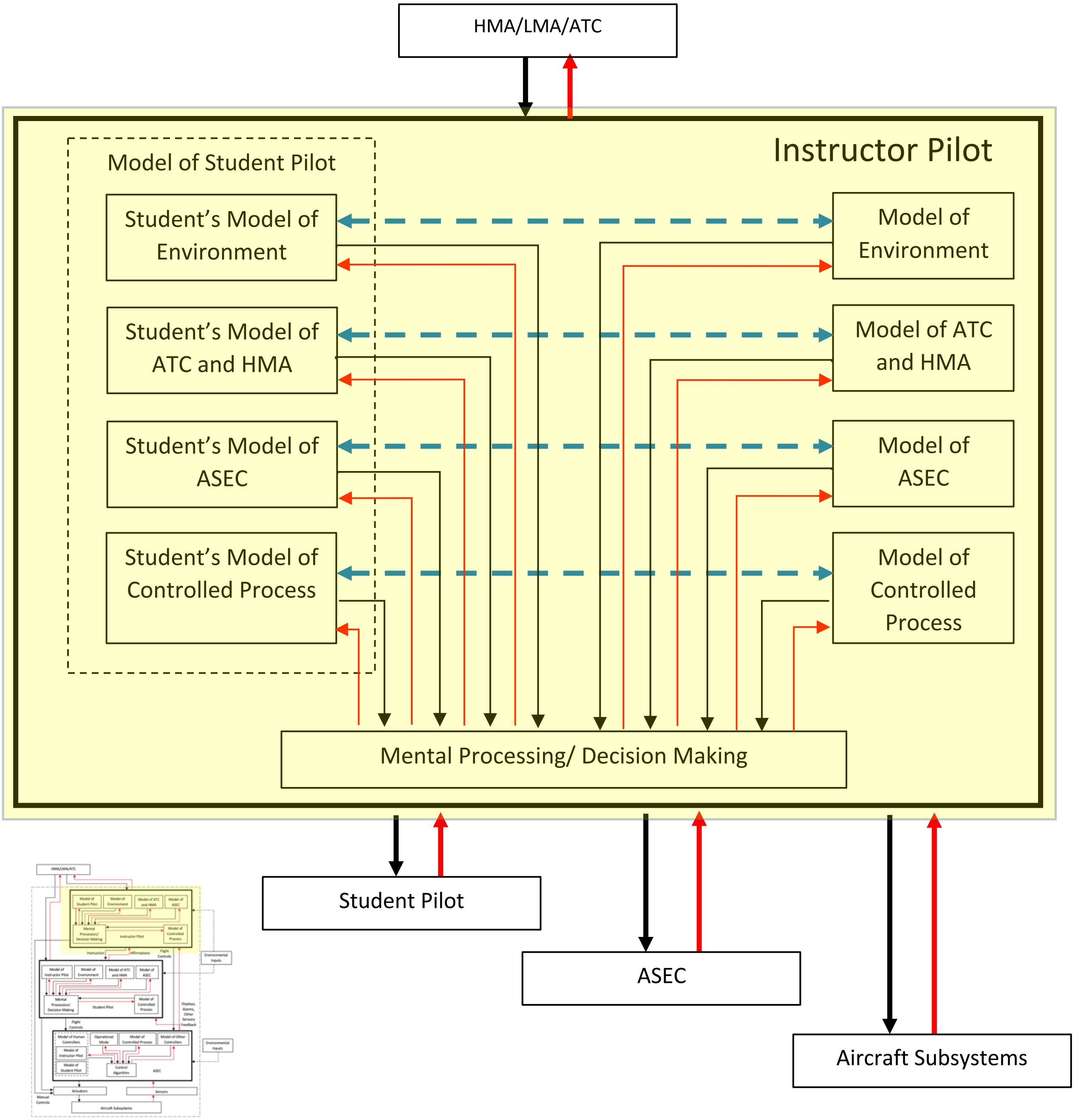


Figure 5-7: Breakdown of Instructor Pilot Mental Models and Decision Making

The instructor's mental processing and decision-making are heavily influenced by the interpretation of the student's mental models of the situation. Conflicting mental models between the instructor and the student can create many different causal scenarios that may lead to unsafe control actions. The following are some examples of how these scenarios are written:

Table 5-8: Causal Scenarios Derived from UCA ID 10 between the Student and the Aircraft Subsystems

CS ID	Causal Scenario	UCA Link	RM ID
10.01	The flight crew is recovering from an emergency that requires an override of the ASEC. The instructor cannot input the flight controls (IP is incapacitated). The student does not input the appropriate manual flight controls. This could happen if the student's mental model conflicts with the actual controlled process. Augmented flight controls must be designed to operate similarly to manual override. As a result, the aircraft becomes uncontrollable.	10.01	RM 9.01
10.02	The flight crew is recovering from an emergency and the instructor has been incapacitated. The student does not override the ASEC because the instructor's assumption of control is preventing the student from bypassing the ASEC. As a result, the aircraft becomes uncontrollable.	10.01	RM 10.02
10.03	The flight crew is recovering from an emergency and the instructor is cueing the student to override the ASEC. The student has a flawed mental model and does not override the ASEC when cued by the instructor because the student does not believe the override is necessary. As a result, the aircraft becomes uncontrollable.	10.02	RM 11.04
10.04	The student is recovering from a maneuver during training. The student is struggling to recover from the maneuver. As the flight crew loses altitude, the student decides that overriding the ASEC would aid the recovery. The student overrides the ASEC during a critical phase of flight without command from the instructor. As a result, training limitations are broken.	10.03	RM 11.04
10.05	The flight crew is recovering from an emergency that requires an override of the ASEC. The instructor cannot input the flight controls (IP is incapacitated). The student inputs manual flight controls without enough experience with manual controls. This could happen if augmented flight controls are not designed to operate similarly to manual override. As a result, the aircraft becomes uncontrollable.	10.04	RM 9.01
10.06	The student overrides the ASEC too early before being instructed. This could happen if manual flight controls are not practiced as part of an emergency procedure. As a result, the aircraft becomes uncontrollable.	10.05	RM 9.01
10.07	The student overrides the ASEC too late after being instructed. This could happen if the flight crew receives inadequate feedback and does not recognize the need to override the ASEC. As a result, the aircraft become uncontrollable.	10.06	RM 10.03
10.08	The student stops overriding the ASEC too soon before the aircraft is controllable. This could happen if the ASEC requires recalibration but does not provide adequate feedback to the flight crew that the recalibration is completed, or the recalibration does not address the problem with the ASEC. As a result, the aircraft is uncontrollable.	10.07	RM 6.01
10.09	The student overrides the ASEC for too long after flight augmentation is needed for safe operation. This could occur if there is no notification to alert the pilots that flight augmentation is recommended for safe flight. As a result, the aircraft becomes uncontrollable.	10.08	RM 6.01

5.6. Recommendations:

A full list of recommendations is listed in Appendix A derived from the causal scenarios. It is organized to provide recommendations to individual controllers. This section also includes operational and organizational implementation of the recommendation. Scenarios regarding the HMA, LMA, and ATC are highly generalized and are only visited to provide the framework for future analysis. HMA, LMA, and

ATC are unique in their own policies and procedures. STPA should be conducted for each organization to reflect their individuality.

5.6.1. Maintaining Accurate and Current Mental Models

A recurring theme throughout the analysis was the recurrence of maintaining and updating accurate mental models of other relevant controllers (RM 11.04). Misalignment of mental models specifically between the instructor and the student occurred in dozens of scenarios. Table 5-9 outlines the methods by which controllers maintain accurate mental and process models of other controllers and controlled processes in the system.

Table 5-9: Methods that Controllers Update their own Mental Models or Process Models

	Model of Student	**Model of Instructor**	**Model of Environment**	**Model of ATC/HMA**	**Model of ASEC**	**Model of Controlled Process**
State of Student	Student Reality	Instructor's expectation, Clarification of limits	SA on other aircraft, weather, etc.	Derived from regulations, training, NOTAMs, SII	Derived from flight manuals, publications, and experience.	Derived from flight manuals, publications, and experience.
Instructor's Beliefs about the Student's mental models ….	Student's reality	Student's mental model of Instructor's expectations, and training limits	Student's mental model of other aircraft, weather, etc.	Student's mental model of regulations, training, NOTAMs, SII	Student's mental model of ASEC	Student's mental model of the controlled process (flight controls, maneuvering, etc.)
State of Instructor	Student's Grade card, notes from previous instructors, experience from flying with the student	Instructor Reality	SA on other aircraft, weather, etc.	Derived from regulations, training, NOTAMs, SII	Derived from flight manuals, publications, and experience.	Derived from flight manuals, publications, and experience.
State of Environment	N/A	N/A	Environment Reality	N/A	N/A	N/A
State of ATC/HMA	Student's grade card, notes from instructors	Feedback sessions and performance reviews	SA on other aircraft, weather, etc.	ATC/HMA Reality	Derived from flight manuals, publications, and experience.	Derived from flight manuals, publications, and experience.
State of ASEC	Control Inputs	Control inputs	Sensor input	N/A	ASEC Reality	Software interfacing and actuation
State of Controlled Process	Manual Control Inputs	Manual Control Inputs	Sensor input	N/A	Control Inputs and interfacing with software	Controlled Process Reality

Each of the cells in

Table 5-9 can be rewritten as safety constraints for each controller. For example, the instructor's safety constraints can be written as:

Table 5-10: Safety Constraints of the Instructor's Mental Models

MENTAL MODEL	UPDATE MECHANISM	ASSOCIATED SAFETY CONSTRAINT
STUDENT	The student's grade card, notes from previous instructors, experience with flying with the student.	I-C-1: The instructor must maintain an accurate and current mental model of the student before the flight by assessing the student's grade card, notes from previous instructors, and experience from flying with the student.
INSTRUCTOR	N/A	N/A
ENVIRONMENT	SA on other aircraft, weather, etc.	I-C-2: The instructor must maintain an accurate and current mental model of the environment by maintaining SA on other aircraft in the area and staying up to date on changing weather.
HMA/ATC	Derived from regulations, training, NOTAMs, and SII	I-C-3: The instructor must maintain accurate and current mental models of the HMA/ATC by staying up to date on current and changing regulations, training, NOTAMs and SII.
ASEC	Derived from flight manuals, publications, and experience	I-C-4: The instructor must maintain accurate and current mental models of the ASEC by staying up to date on current flight manuals, publications, and experience.
CONTROLLED PROCESS	Derived from flight manuals, publications, and experience	I-C-5: The instructor must maintain accurate and current mental models of the controlled process. by staying up to date on current flight manuals, publications, and experience.

These safety constraints can help identify areas in systems that lack adequate feedback or understanding of relevant system components. The highlighted row in Table 5-9 is unique in the context of flight training, however the reasoning behind this row can be extended to ***any instructional, managerial, or leadership roles where the supervisory controller needs to keep accurate and updated mental models of the supervisee's mental models***. These supervisor-supervisee controller constraints are written in Table 5-11:

Table 5-11: Instructor-Student Mental Model Controller Constraints

MENTAL MODEL	UPDATE MECHANISM	ASSOCIATED SAFETY CONSTRAINT
STUDENT'S MENTAL MODEL OF THE INSTRUCTOR	Clarifying and asking questions about what the student expects from the instructor and where the instructor's limits are.	I-S-C-1: The instructor must maintain and accurate and current mental model of the student's beliefs about the instructor. This is accomplished by clarifying and asking questions about what the student expects from the instructor and where the instructor's limits are.

STUDENT'S MENTAL MODEL OF THE ENVIRONMENT	Clarifying and asking questions about the student's SA on other aircraft, weather, etc.	I-S-C-2: The instructor must maintain and accurate and current mental model of the student's beliefs about the environment. This is accomplished by clarifying and asking questions about the student's SA on other aircraft, weather, etc.
STUDENT'S MENTAL MODEL OF THE HMA/ATC	Clarifying and asking questions about the student's interpretation of regulations, training, NOTAMs, and SII	I-S-C-3: The instructor must maintain and accurate and current mental model of the student's beliefs about the HMA/ATC. This can be accomplished by clarifying and asking questions about the student's interpretation of regulations, training, NOTAMs, and SII.
STUDENT'S MENTAL MODEL OF THE ASEC	Clarifying and asking questions about the student's interpretation of flight manuals, publications, and experience with the ASEC.	I-S-C-4: The instructor must maintain an accurate and current mental model of the student's beliefs about the ASEC. This scan be accomplished by clarifying and asking questions about the student's interpretation of flight manuals, publications, and experience with the ASEC.
STUDENT'S MENTAL MODEL OF THE CONTROLLED PROCESS	Clarifying and asking questions about the student's interpretation of the flight controls, how to perform maneuvers, what to do in emergencies, etc.	I-S-C-5: The instructor must maintain an accurate and current mental model of the student's mental model of flying the aircraft. This scan be accomplished by clarifying and asking questions about the student's interpretation of the flight controls, how to perform maneuvers, what to do in emergencies, etc.

Table 5-11 helps develop significant controller constraints to prevent controllers from making unsafe control actions, however these constraints can also be used to help improve a student's training. By increasing the instructor's awareness of the student's mental models, the instructor can more accurately tailor instruction and training efforts to align the student's mental models with reality.

5.6.2. Mitigating Student Stress

As part of the instructor maintaining an accurate mental model of the student, the instructor should also note how the student responds to stressful situations (RM 11.01). This can also be documented in the student's notes on the grade cards. This can also be gauged during emergency procedures practice before the flight or during maneuvers in the area. Building situational awareness on how the student handles stress in situations where time is not a safety critical factor can provide context to the instructor for decision-making during critical phases of flight.

If a student is struggling with the program, their stress levels will likely be elevated higher than the average student. For high-stress progress checks, students should fly with instructors who have already flown with them in the past (RM 11.02). This is because instructors who have flown with struggling students in the past will already have a basis for the student's behavioral tendencies and how students handle stressful situations. Instructors who have flown with the struggling student will also have a basis for the student's mental models (addressing safety constraints described in Table 5-11).

When giving instruction, IPs must focus on the priority of instructions if multiple issues exist (RM 11.03). If more than one correction needs to be made during time-sensitive scenarios (e.g., critical phases of flight or aircraft deconfliction), the instructor should assume control rather than attempting to talk the student through multiple corrections and the precedence of each.

If a student is transitioning between phases of training or between separate aircraft, Instructors should emphasize the differences in flying and handling qualities between the two aircraft (RM 11.05). For example, the difference between rudder usage between the T-6 and T-38 during high AoA situations (as discussed in 4.5.1) can help students conceptualize their new control inputs. Instructors should still be aware of habits that may have been developed in previous training phases that could manifest in high-stress scenarios.

5.6.3. Recommendations for Student Pilots

Students can contribute to the IP's safety constraints by communicating the status of each mental model. This can include the student walking through their interpretation of a flight manual, publication, guidance from HMA or ATC, etc. During the flight, the student should communicate any changes to their mental models and walk the instructors through their process and control inputs to address specific corrections. The Federal Aviation Administration (FAA) ultimately places the full responsibility of flight training on the flight instructor; however that does not imply that the student does not influence the instructor's ability to uphold safety constraints [35].

5.6.4. Recommendations for the Next Generation Trainer Design

The hypothetical Next Generation Trainer (NGT) can mitigate many of the hazardous scenarios in the T-6 and T-38. However, introducing a software enabled controller presents new challenges that need to be considered.

Figure 5-2 illustrates how there are now 3 controllers that can provide conflicting control authority to the aircraft subsystems. The FCS must explicitly outline control priority (RM 6.09). Prioritizing control authority between the student and the instructor (e.g., providing an instructor override feature – RM 4.01) has the potential to address scenarios where there is no time for adequate transfer of aircraft control or where transfer of aircraft control may be unclear. Manual override of the ASEC needs to be the highest priority and should be considered in scenarios where augmented flight controls may be dysfunctional (5.01).

Another scenario that should be considered is if the ASEC assesses and determines that the aircraft is on a trajectory to violate structural integrity or collide with an object or other aircraft and overrides control to save the aircraft (RM 4.02, RM 6.07, RM 7.01). An example of how control priority may be designed is visualized in Figure 5-8. Flight crews must be trained on the final order of control priority and adequate feedback must communicate to both pilots who is controlling the aircraft at any specific moment.

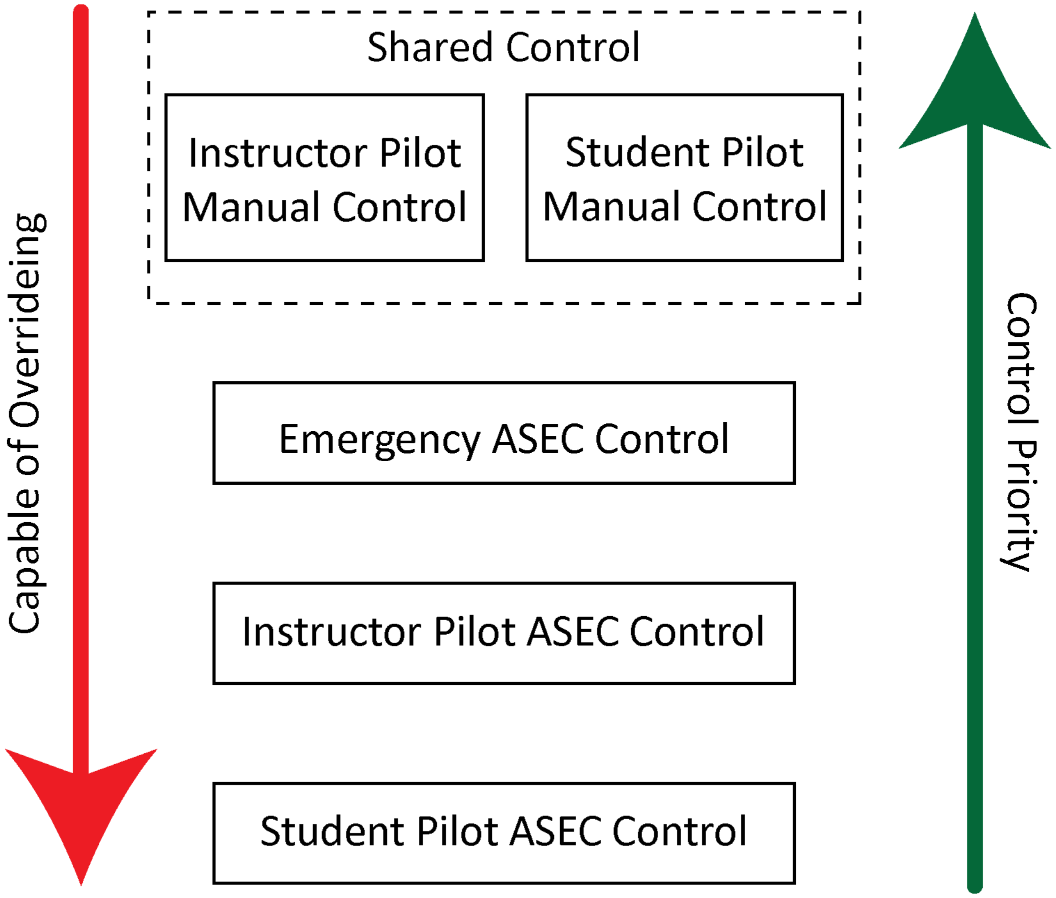


Figure 5-8: Example of Control Priority

The NGT must have all controls to any aircraft function accessible in both cockpits to address any scenarios where either pilot is incapacitated (11.06).

The NGT also needs to be designed with redundant feedback to all controllers. This is especially important for transfer of aircraft control between the instructor and the student. Redundant transfer of aircraft control feedback should include different sensory inputs (visual, audio, tactile/haptic). Biometric displays of the student are possible design features to aid the instructor in decision making. This option is explored in Chapter 8. Monitoring the pilot's biometric data could provide feedback if either of the pilots is incapacitated (from g induced loss of consciousness or other illness)—to which the ASEC could enter an emergency state.

The ASEC must be designed to self-regulate and detect when it has a flawed process model or any other malfunction (RM 10.03). If the ASEC is receiving inadequate feedback or the process model is flawed, the ASEC must have the ability to be recalibrated during the mission. The flight controls must default to a specified state or manual controls during recalibration. Feedback from sensors should be redundant, and sensors should be in different areas around the aircraft to cross-reference extreme readings. Feedback must also be provided about the status of sensors and if any are not functional. The ASEC must have different modes if the aircraft has violated limits of structural integrity. If the aircraft has violated structural integrity, flight controls limits must be increased. Some of the suggested recommendations are visualized in Figure 5-9.

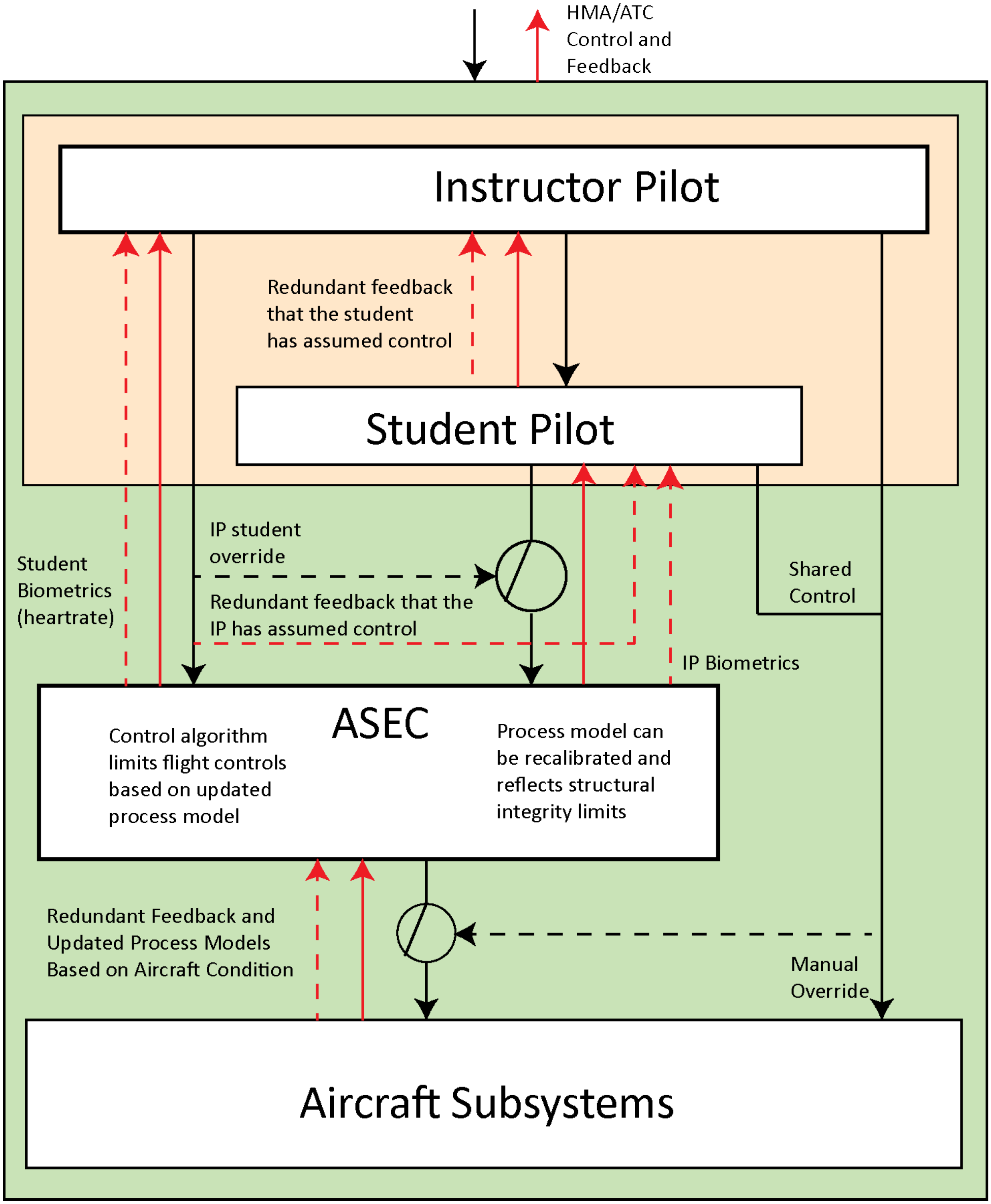


Figure 5-9: Recommendations Visualized on a Control Structure

5.6.5. Improvements to SIB Processes:

The shortcomings of the SIB process discussed in section 2.3.1 are generally concerned with not providing enough context for the findings. Other concerns include the lack of traceability, impartiality in selecting causal findings, exclusion of non-factors worthy of discussion and system-related events, and how human error is handled. The SIB would significantly benefit from adopting certain STAMP practices.

The CAST conducted in Section 4 begins by establishing traceability by reducing the events of the accident into hazards and constraints. Building a hierarchal control structure helps the analysts establish context by which each controllers' actions can be investigated in the context of the entire system. CAST also emphasizes the importance of mental models and how elements of the control structure can influence the decision-making of humans or control algorithms of software. By analyzing the system holistically, CAST incorporates factors (actions, conditions, and publications), non-factors worthy of discussion, and system-related factors.

The AFI 91-223 *Aviation Safety Investigations and Reports* detail specific aviation-related guidance for SIB [10]. Chapter 3 lists Aviation Specific Reporting Criteria for events that require a SIB. These criteria include physiological, propulsions related, flight control related, instrument related, miscellaneous, and hazardous air traffic report events. These event criteria can be reframed into elements of STPA and used to generate recommendations without an event occurring. Incorporating these elements into STPA can also help establish traceability to system-level losses and hazards. For example:

Table 5-12: AFI 91-223 Event/Conditions Conversion to STPA Scenarios [10]

AFI 91-223 Event/Condition	Loss/Hazard	Unsafe Control Action	Causal Scenario	Recommendation
Acceleration Effects—G-induced loss of consciousness (GLOC). [3.3.1 Physiological Events]	Loss of life/ Hazard: Aircraft environment is harmful to human health or not conducive to proper human control	Flight crew does not actuate flight controls.	Flight crew is executing a high g maneuver. The aircraft provides inadequate feedback to the flight crew about the load on the aircraft. As a result, the pilots lose consciousness.	The ASEC should limit control input when anticipating an over g.
Spatial Disorientation—Failure to correctly sense aircraft position, attitude, or altitude. [3.3.1 Physiological Events]	Loss of life/ Hazard: Aircraft is uncontrollable	[unspecified]	After flying into clouds, the pilot loses visual feedback.	The aircraft must have other means of feedback to validate the aircraft's orientation (e.g.., a gyro).
Loss of Thrust was sufficient to prevent maintaining level flight at a safe altitude	Loss of life/ Hazard: Aircraft is uncontrollable	Thrust is not increased.	There was inadequate feedback about the loss of thrust to the pilot	Engine needs to use redundant means of feedback

or which required the pilot to jettison stores. [3.3.2 Propulsion Related Events]				
Uncommanded Inputs to the Flight Controls (including stability augmenter, or trim system) whether it resulted in a dangerous situation nor not. [3.3.3 Flight Control Related Events]	Loss of life/ Hazard: Aircraft is uncontrollable	Actuating the flight controls causes the hazard	The ASEC determines the aircraft is on a hazardous course and inputs uncommanded flight controls.	ASEC must notify the flight crew and have the option to disapprove control actuation.
Near Mid-Air Collision: Aircraft took abrupt evasive action or would have taken such action if circumstance allowed, or aircraft was within 500' or inside "well clear" and presented a hazard to flight safety. [3.3.5 Miscellaneous Reportable Events]	Loss of life/ Hazard: minimum separation standards are violated	Flight crew evade the approaching aircraft too late after minimum separation has been broken.	This could happen if the flight crew have a flawed mental model regarding the other aircraft's intentions. This could happen if common procedures are not followed by the other aircraft (bank right)	Always communicate with other aircraft in uncontrolled airspace.

6. CONCLUSION

This thesis approaches tandem-seat pilot training by applying STAMP principles to an accident and a hypothetical next-generation trainer. Safety and incident investigations need to ask more questions beyond the proximal events and look at other systemic aspects of safety outside of human error. The USAF is at a pivotal point in its life where systems and aircraft are the most complex and autonomous that they have ever been in history. The USAF is on the forefront of next-generation technology, where a single operator may control many aircraft with high degrees of autonomy. The sophistication of future technology will require a system thinking approach to managing complexity.

6.1. Results and Insights

Revisiting the primary research question:

How can STAMP be applied to address the unique challenges faced in tandem seated pilot training?

STAMP can be applied retrospectively to identify context and areas of improvement by using CAST to analyze accidents in tandem seated pilot training. STAMP can also be applied proactively by using STPA to identify design recommendations for current and developing systems. CAST helps learn more from accidents and STPA helps design systems with safety built into the architecture.

6.2. Limitations and the Way Forward

Limiting the study was required to prevent scope creep beyond the time and resources available to the author. This section will summarize relevant limitations and propose future efforts to address these limitations.

A key limitation in the CAST was the omission of privileged information. The inclusion of privileged information may change or improve some of the recommendations derived from the CAST. A future area of work could involve applying STAMP to Air Force Safety Investigations. Using a system-theoretic approach to analyze past accidents can uncover potentially safety critical factors that need to be addressed. The USAF SIB process could also benefit from the application of STAMP. As discussed above, a key oversight in the USAF SIB process is the exclusion of system-related events. These 'system-related events' are essential to identifying UCA's as well as scenarios and recommendations thereafter. Reworking the USAF SIB process could help the USAF learn more from accidents. Another area of future work could be a comparison of how the current USAF SIB process stacks up against CAST.

A relevant generalization in the STPA analysis was not to specify a particular HMA, LMA, or ATC. At the highest level, the HMA may be the same for all flying operations in the Air Force (referring to relevant 11-series publications) and the general flying regulations across the FAA. However, the LMA can vary widely depending on the type of aircraft serviced at the base, the program or syllabus of the pilot training program, squadron composition, and total force integration, and any number of squadron or base-specific items.

ATC is also unique depending on the specific airfield, weather in the area, and general operations amongst other factors. Highly generalized UCA's and scenarios were created as examples for how each organization may begin to structure and think about their own unique STPA analysis. Due to their individual nature, it would serve each organization to have their own staff conduct an STPA. Using actual operators and personnel who function within each organization can provide better individualized insights to each mission authority.

The same sentiment can be extended to operators of both the T-38 and the T-6. Although the author had access to public training documents of each aircraft, the controlled unclassified information (CUI) relating to each aircraft's technical specifications would provide significantly more detail that can be used in STPA. The UCA's and scenarios generated in this report use a very high-level understanding of the potential function for the ASEC and subsystems. STPA could also be iterated on the same system at different levels of abstraction.

This analysis primarily focused on analyzing the interactions between the student and instructor pilots. A deeper dive into the technical specifications of each aircraft would bring to light specific recommendations that may be addressable in the aircraft's engineering. It would be in the best interest of the Air Force to conduct an STPA on the next-generation trainer, the T-7. The introduction of higher degrees of automation and more complex control makes a compelling argument for using STPA since software challenges are a strength of the tool.

STPA can also be applied to other areas of military aviation. Gregorian and Yoo's recent thesis demonstrates that the creation of risk matrices can be aided by using STPA [36]. This concept can be extended to aviation risk management. STPA could also be extended to commercial flight training or flight training in dual cockpits such as the T-1.

To revisit the purpose of the analysis, the author's objective was not to shift blame to other relevant parties. The benefit of the analysis is to examine decisions in the context that they were made to see how and where the system can be designed to minimize the likelihood for unsafe control actions going forward.

7. Appendix:

7.1. Full STPA Analysis

7.1.1. Define Purpose of the Analysis

Table 7-1: System-Level Losses

Loss ID	Loss Description
L01	Loss of life or injury
L02	Damage to aircraft or equipment
L03	Loss of training mission

Table 7-2: System-Level Hazards

Hazard ID	Hazard Description	Loss Link
H01	The aircraft is uncontrollable	L01, L02, L03
H02	Structural integrity of aircraft is violated	L01, L02, L03
H03	Training limitations are exceeded (minimum separation from other aircraft, objects, or terrain, centerline control, airspeed, aimpoint, flight path)	L01, L02, L03
H04	Student pilot continues to fly aircraft after nearing instructor limitations	L01, L02, L03
H05	Aircraft environment is harmful to human health or not conducive to proper human control	L01, L03
H06	Training mission does not have proper guidance	L03

Table 7-3: System-Level Constraints

Constraint ID	Constraint Description	Hazard Link
C01	Aircraft must remain controllable	H01
C02	If Aircraft is uncontrollable, then the aircraft must have appropriate egress procedures and contingencies to mitigate further loss.	H01
C03	Flight crew must communicate who is controlling during the final approach	H01
C04	If flight crew cannot communicate, there must be procedures to establish responsibilities of each controller.	H01
C05	Student pilot must be properly trained in flight procedures	H01
C06	If student pilot is not properly trained in flight procedures, training and procedures must be in place to train the student and operate the aircraft safely	H01
C07	Aircraft structural integrity must maintain during the final approach	H01, H02

C08	If aircraft structural integrity is lost, the structural violation must be detected and properly communicated to the operators.	H01, H02
C09	If aircraft structural integrity is lost, there must be procedures in place to return safely to base or egress the aircraft.	H01, H02
C10	Flight crew must stay within training limitations	H01, H02, H03
C11	If flight crew breaks training limitations, their status must be communicated to other local controllers and operators.	H01, H02, H03
C12	If flight crew breaks training limitations, there must be procedures in place to return safely to base or egress the aircraft.	H01, H02, H03
C13	Instructor Pilot must be trained to recognize limitations	H01, H02, H03
C14	If the instructor pilot is not trained to recognize limitations, other controllers must be able to detect or recognize limitations.	H01, H02, H03
C15	Instructor Pilot must take aircraft before exceeding limitations	H01, H02, H04
C16	If the instructor pilot does not take aircraft before exceeding limitations, procedures must be in place to recover the aircraft or mitigate further loss.	H01, H02, H04
C17	Instructor Pilot must be able to recover the aircraft after exceeding limitations	H01, H02, H04
C18	If the instructor pilot cannot recover the aircraft after exceeding limitations, procedures must be in place to mitigate further loss	H01, H02, H04
C19	Aircraft environment must be suitable for human health	H05
C20	If the aircraft environment is not suitable for human health, the condition must be detected, and measures taken to prevent mission degradation.	H05
C21	Higher Authorities must provide guidance for the mission.	H06
C22	If higher authorities cannot give proper guidance, procedures must be in place to complete training mission and return safely.	H06

7.1.2. Identify Unsafe Control Actions

Table 7-4: UCAs from the HMA to the LMA

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
HMA provides mission related procedure and regulations to the LMA.	1.01: HMA does not provide appropriate mission related guidance to the squadrons during squadron flight training operations.	H03, H06	1.02: HMA provides guidance to the squadrons during Flight Training Operations when the information is not accurate or misleading.	H03, H06	1.03: HMA provides mission related guidance to the squadrons too early before receiving updated information for the conditions or mission	H03, H06	N/A	
					1.04: HMA provides appropriate mission related guidance to the squadrons too late after the squadron has already completed training objectives	H03, H06		
					1.05: HMA provides appropriate mission related guidance to the squadrons out of order from other guidance that has already been rescinded from training.	H03, H06		

Table 7-5: UCAs from the LMA to the Flight Crew

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Training Squadron provides mission related regulations to the squadron	2.01: Squadron does not provide appropriate mission related guidance to the flight crew during training operations	H03, H06	2.02: Squadron provides misleading or contradictory guidance to the flight crew during Flight Training Operations	H03, H06	2.03: Squadron provides appropriate mission related guidance to the flight crew too early before the guidance is applicable	H03, H06	N/A	
					2.04: Squadron provides appropriate mission related guidance to the flight crew too late after the squadron has already completed training sorties	H03, H06		
					2.05: Squadrons provides appropriate mission related guidance to the flight crew out of order from other guidance that has already been rescinded from training.	H03, H06		

Table 7-6: UCAs from ATC to the Flight Crew

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
ATC provides instruction and clearance to the flight crew	3.01: ATC does not provide instruction or clearance during critical phases of flight	H03, H06	3.03: ATC provides clearance to the Flight crew when clearance is	H03, H06	3.05: ATC provides clearance to the flight crew too early before	H03, H06	N/A	

	(takeoff, landing, the pattern)		not available during critical phases of flight		the flight crew is cleared			
	3.02: ATC does not provide instruction or clearance during aircraft deconfliction	H03, H06	3.04: ATC provides instruction to the flight crew when the instruction will lead to airspace conflicts	H03, H06	3.06: ATC provides clearance or instruction to the flight crew too late after the flight crew needed clearance	H03, H06		
					3.07: ATC provides instruction to the flight crew too early before flight crew needs to deconflict	H03, H06		
					3.08: ATC Provides instruction to the flight crew too late after the flight crew have broken minimum separation standards with another aircraft	H03, H06		
					3.09: Provides instruction or clearance out of order so that the flight crew interprets the procedure incorrectly	H03, H06		

Table 7-7: UCAs from the IP to the ASEC

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Instructor Pilot controls ASEC	4.01: The instructor does not control the ASEC when the student is reaching the	H01, H03, H04	4.07: The instructor controls the ASEC without proper transfer of aircraft	H01, H03, H04	4.10: Instructor controls the ASEC too early before the student has reached	H06	4.18: Instructor stops control of ASEC too early before the student can confidently take	H01, H03, H04, H06

	instructor’s limits of training		control during training maneuvers		training limitations in a critical phase of flight		control of the aircraft during critical phases of flight	
	4.02: The Instructor does not control the ASEC during critical phases of flight.	H01, H03, H04	4.08: The instructor controls the ASEC without proper transfer of aircraft control during a critical phase of flight.	H01, H03, H04	4.11: Instructor controls the ASEC too late after the student has already exceeded the instructor’s limitations during a critical phase of flight.	H01, H03, H04, H06	4.19: Instructor takes control of the ASEC too long after an emergency has been averted during critical phases of flight	H06
	4.03: Instructor does not control the ASEC during aircraft deconfliction.	H01, H03, H04	4.09: Instructor controls the ASEC without proper transfer of aircraft control during aircraft deconfliction.	H01, H03, H04	4.12: Instructor controls the ASEC out of order from verbal cuing during a critical phase of flight.	H01, H03, H04, H06	4.20: Instructor stops ASEC control too early during aircraft deconfliction before aircraft are clear of the deconfliction	H01, H03, H04, H06
	4.04: Instructor cannot control the ASEC when the student is reaching the instructor’s limits of training	H01, H03, H04			4.13: Instructor controls the ASEC too early before the student can decide during aircraft deconfliction	H06	4.21: Instructor takes control of the ASEC for too long after aircraft deconfliction.	H06
	4.05: Instructor cannot make control inputs to the ASEC during critical phases of flight.	H01, H03, H04			4.14: Instructor controls the ASEC too late after the aircraft has broken minimum separation standards during aircraft deconfliction.	H01, H03, H04, H06		
	4.06: Instructor cannot make control inputs during aircraft deconfliction.	H01, H03, H04			4.15: Instructor controls the ASEC out of order from verbal cuing during aircraft deconfliction	H01, H03, H04, H06		

					4.16: Instructor controls the ASEC too early during training maneuvers.	H06		
					4.17: Instructor controls the ASEC too late after the aircraft exceeds training limitations	H01, H03, H04, H06		

Table 7-8: UCAs from the Student Pilot to the ASEC

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Student Pilot controls ASEC	5.01: Student does not control the ASEC when the student is reaching the instructor's limits of training	H01, H03, H04	5.07 Student controls the ASEC without proper transfer of aircraft control during training maneuvers.	H01, H03, H04	5.10: Student controls the ASEC too early before the instructor has cleared the student to fly in a critical phase of flight	H01, H03, H04, H06	5.17: Student stops control of ASEC too early before the instructor takes control of the aircraft during critical phases of flight	H01, H03, H04, H06
	5.02: Student does not control the ASEC during critical phases of flight (takeoff, landing, pattern)	H01, H03, H04	5.08: Student controls the ASEC without proper transfer of aircraft control during a critical phase of flight.	H01, H03, H04	5.11: Student controls the ASEC too late after the instructor has cleared the student to fly during a critical phase of flight.	H06	5.18: Student takes control of the ASEC too long after an emergency has been declared during critical phases of flight	H01, H03, H04, H06
	5.03: Student does not control the ASEC during aircraft deconfliction.	H01, H03, H04	5.09: Student controls the ASEC without proper transfer of aircraft control during aircraft deconfliction.	H01, H03, H04	5.12: Student controls the ASEC out of order from verbal cuing during a critical phase of flight.	H01, H03, H04, H06	5.19: Student stops ASEC control too early during aircraft deconfliction before the instructor can clear the deconfliction	H01, H03, H04, H06

	5.04: Student cannot control the ASEC when the student is reaching the instructor’s limits of training	H01, H03, H04			5.13: Student controls the ASEC too early before the instructor has cleared an aircraft deconfliction	H01, H03, H04, H06	5.20: Student takes control of the ASEC too long during aircraft deconfliction.	H01, H03, H04, H06
	5.05: Student cannot make control inputs to the ASEC during critical phases of flight.	H01, H03, H04			5.14: Student controls the ASEC too late after the aircraft has broken minimum separation standards during aircraft deconfliction.	H01, H03, H04, H06		
	5.06: Student cannot make control inputs during aircraft deconfliction.	H01, H03, H04			5.15: Student controls the ASEC too early before the instructor has transferred aircraft control during training maneuvers	H01, H03, H04, H06		
					5.16: Student Controls the ASEC too late after the instructor has transferred aircraft control during training maneuvers.	H01, H03, H04, H06		

Table 7-9: UCA's from the ASEC to the Aircraft Subsystems

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
ASEC change FCS	6.01: ASEC does not direct change in FCS when the FCS is needed to avoid breaking minimum separation standards with another object or aircraft.	H01, H03	6.03: ASEC directs change in FCS when the change in FCS breaks the minimum separation standards.	H01, H03	6.06: ASEC directs change in FCS too late after minimum separation standards have been broken.	H01, H03	6.10: ASEC directs change in FCS for too long that the aircraft enters another state where it is breaking minimum separation standards	H01, H03

	6.02: ASEC does not direct change in FCS when the aircraft is entering an uncontrollable state (Stall).	H01, H02	6.04: ASEC directs change in FCS when the change if FCS places the aircraft in an uncontrollable state (Stall).	H01, H02	6.07: ASEC directs change in FCS too late after the aircraft has entered an uncontrollable state.	H01, H02.	6.11: ASEC directs change in FCS for too long that the Aircraft enters a different uncontrollable state.	H01, H02
			6.05: ASEC directs change in FCS when the flight crew has not authorized a change in the FCS.	H01, H06, H07	6.08: ASEC directs change in FCS too early before the aircraft has entered an uncontrollable state.	H01, H06	6.12: ASEC directs change in FCS not long enough that the aircraft is still bound to break minimum separation standards	H01, H03
					6.09: ASEC directs change too early before proper FCS input has been assessed by the flight crew.	H01, H02, H03	6.13: ASEC directs change in FCS not long enough that the aircraft is not able to recover from an uncontrollable state.	H01, H02
ASEC limits FCS	7.01: ASEC does not limit change in FCS when the FCS input from the flight crew will violate the structural integrity of the aircraft.	H02	7.02: ASEC limits change in FCS when the FCS input is not violating the structural integrity of the aircraft	H01	7.04: ASEC limits change in FCS too early before the aircraft has approached the limits of structural integrity while performing a training maneuver.	H01, H06	7.06: ASEC limits change in FCS too short of a time that the aircraft violates structural integrity while performing a training maneuver.	H02
			7.03: ASEC limits change in FCS when the FCS input is needed for a safety critical maneuver.	H01, H06	7.05: ASEC limits change in FCS too late after the aircraft has violated structural integrity during a training maneuver.	H02	7.07: ASEC limits change in FCS too long of a time that the aircraft cannot perform a training maneuver.	H01
ASEC change internal environment	8.01: ASEC does not change the aircraft's environmental systems when the flight crew requests the change, and the aircraft internal	H01, H05	8.02: ASEC changes aircraft environmental systems when the flight crew does not request the change and the new environmental	H01, H02, H05	8.03: ASEC changes aircraft environmental systems too late after the aircraft environment has negatively impacted	H01, H02, H05	8.04: ASEC changes aircraft environmental systems for too long that the aircraft environment becomes hazardous to the flight crew/hardware.	H01, H02, H05

	environment is negatively impacting the flight crew or aircraft hardware's performance.		condition negatively impacts the flight crew or aircraft hardware's performance.		flight crew/hardware's performance.			
							8.05: ASEC changes aircraft environmental systems for too short that the aircraft environment is still hazardous to the flight crew/hardware.	H01, H02, H05

Table 7-10: UCA's from the IP to the Aircraft Subsystems

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Instructor Pilot overrides ASEC	9.01: The instructor does not override the ASEC when the student is reaching the instructor's limits of training during critical phases of flight	H01, H03, H04	9.07: The instructor overrides the ASEC without proper transfer of aircraft control during training maneuvers	H01, H03, H04	9.10: Instructor overrides the ASEC too early before the student has reached training limitations in a critical phase of flight	H06	9.16: Instructor stops override of ASEC too soon before the ASEC is controllable during critical phases of flight	H01, H03, H04, H06
	9.02: The Instructor does not override the ASEC during critical phases of flight.	H01, H03, H04	9.08: The instructor overrides the ASEC without proper transfer of aircraft control during a critical phase of flight.	H01, H03, H04	9.11: Instructor overrides the ASEC too late after the student has already exceeded the instructor's limitations during a critical phase of flight.	H01, H03, H04, H06	9.17: Instructor overrides ASEC for too long that the aircraft becomes uncontrollable.	H01, H03, H04, H06
	9.03: Instructor does not override the ASEC during aircraft deconfliction.	H01, H03, H04	9.09: Instructor overrides the ASEC without proper transfer of aircraft	H01, H03, H04	9.12: Instructor overrides the ASEC too early before the student can decide during aircraft deconfliction	H06		

			control during aircraft deconfliction.					
	9.04: Instructor cannot override the ASEC when the student is reaching the instructor’s limits of training	H01, H03, H04			9.13: Instructor overrides the ASEC too late after the aircraft has broken minimum separation standards during aircraft deconfliction.	H01, H03, H04, H06		
	9.05: Instructor cannot override the ASEC during critical phases of flight.	H01, H03, H04			9.14: Instructor overrides the ASEC too early during training maneuvers.	H06		
	9.06: Instructor cannot override the ASEC during aircraft deconfliction.	H01, H03, H04			9.15: Instructor overrides the ASEC too late after the aircraft exceeds training limitations	H01, H03, H04, H06		

Table 7-11: UCAs from the Student Pilot to the Aircraft Subsystems

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Student Pilot overrides ASEC	10.01: Student does not override the ASEC when the instructor is unable to override.	H01, H02, H03, H04, H06	10.03: Student overrides the ASEC during a critical phase of flight without command from instructor.	H01, H02, H03, H04, H06	10.05: Student overrides the ASEC too early before being instructed.	H01, H02, H03, H04, H06	10.07: Student stops overriding ASEC too soon before the aircraft is controllable.	H01, H02, H03, H04, H06
	10.02: Student does not override the ASEC when cued by the instructor.	H01, H02, H03, H04, H06	10.04 Student overrides the ASEC without enough experience on manual controls.	H01, H02, H03, H04, H06	10.06: Student overrides the ASEC too late after being instructed.	H01, H02, H03, H04, H06	10.08: Student overrides the ASEC for too long after flight augmentation is needed.	H01, H02, H03, H04, H06

Table 7-12: UCAs from the IP to the Student

Control Action	Not providing the control action causes hazard	Hazard Link	Providing the control action causes hazard	Hazard Link	Control action is applied to early, too late, or out of order	Hazard Link	Control action is stopped too soon or applied too long	Hazard Link
Flight Instructor verbally cues the student pilot	11.01: Flight Instructor does not cue the student pilot when the student is reaching the instructor's limits of training.	H01, H03, H04, H06	11.07: Flight Instructor cues the student when the student is not outside the instructor's training limitations.	H01, H03, H04, H06	11:10: Flight instructor cues the student out of order from intended procedure as the student approaches the instructor's limitations	H01, H03, H04, H06	11.16: Flight Instructor stops cues too early during critical phases of flight or aircraft deconfliction	H01, H03, H04, H06
	11.02: Flight Instructor does not cue the student during critical phases of flight.	H01, H03, H04, H06	11.08: Flight Instructor cues the student during critical phases of flight	H01, H03, H04, H06	11.11: Flight instructor cues the student too early before the student needs to make corrections.	H01, H03, H04, H06	11.17: Flight Instructor takes too long to provide verbal cues during critical phases of flight or aircraft deconfliction	H01, H03, H04, H06
	11.03: Flight Instructor does not cue the student during aircraft deconfliction.	H01, H03, H04, H06	11.09: Flight instructor cues the student during aircraft deconfliction.	H01, H03, H04, H06	11.12: Flight instructor cues the student too late after the student has already exceeded the instructor's limitations	H01, H03, H04, H06	11.18: Flight instructor stops cues too early as the student approaches training limitations	H01, H03, H04, H06
	11.04: Flight instructor cannot cue the student when the student is reaching the instructor's limits of training.	H01, H03, H04, H06			11.13: Flight instructor cues the student out of order from the intended procedure during critical phases of flight or aircraft deconfliction.	H01, H03, H04, H06	11:19: Flight instructor takes too long to provide verbal cues as the student approaches training limitations.	H01, H03, H04, H06
	11.05: Flight instructor cannot cue the student during critical phases of flight	H01, H03, H04, H06			11.14: Flight instructor cues the student too early during critical phases of flight or aircraft deconfliction	H01, H03, H04, H06		
	11.06: Flight Instructor cannot cue the student	H01, H03,			11:15: Flight instructor cues the student too	H01, H03,		

	during aircraft deconfliction.	H04, H06			late during critical phases of flight or aircraft deconfliction.	H04, H06		

7.1.3. Identify Loss Scenarios

Table 7-13: Causal Scenarios Derived from UCA's between the HMA and LMA

CS ID	Causal Scenario	UCA Link	RM ID
1.01	HMA believes that the information available to the LMA is complete, and thus the HMA does not provide mission related guidance to the LMA during flight operations. This could happen if information about LMA operations is not properly communicated back up to the HMA through appropriate reporting channels.	1.01	1.01
1.02	HMA believes that the information available to the LMA is incomplete, and thereby provides inaccurate or misleading guidance. This could also be a result of the LMA not properly communicating appropriate information about operations to the HMA. This could also happen if HMA is generalizing certain regulations and policies across all LMA's. While some regulations and policies may be generalized to all squadrons under the HMA, the HMA should be careful not to generalize squadron specific guidance to all LMA's	1.02	1.02
1.03	In this scenario, the HMA recently acquired new equipment to replace some old equipment. The equipment is in the process of being deployed at the squadron (LMA) level. HMA issues regulations and policies to each squadron regarding the new equipment. Squadrons experience delays in getting the equipment and furthermore, it takes time to onboard all relevant staff to the new equipment. Some of the regulations and policies regarding the new equipment are not suitable for the old equipment that is being replaced. This causes confusion among the LMA which causes problems for the operation of the new and old equipment.	1.03	1.03
1.04	The HMA recently investigated an accident that happened during flight training. At the time the system factors involved in the accident was unknown, so the HMA continued operations. The accident uncovered a critical flaw in the operation of the operation of the canopy during specific maneuvers. During the time between the accident and the discovery of this flaw many sorties have engaged in this maneuver. The HMA provides appropriate guidance to the LMA too late after the squadrons have already flown sorties with those same maneuvers.	1.04	1.04
1.05	The LMA recently encountered an unsafe situation where the LMA suspended the practice of certain maneuvers. Because this was accomplished at the squadron level, it was not relayed up to the HMA. The HMA thereby issues guidance pertaining to the mandatory training of this maneuver out of order from which the guidance issued by the squadron level. This confuses the LMA and impacts training.	1.05	1.01

Table 7-14: Causal Scenarios Derived from UCA's between the LMA and the Flight Crew

CS ID	Causal Scenario	UCA Link	RM ID
2.01	LMA believes that guidance directed down from the HMA was previously communicated to the flight crew and thereby the LMA does not give mission guidance directed from HMA down to the flight crew. This could happen if the LMA believes that a regulation was previously updated, or the guidance was given by ATC.	2.01	2.01

2.02	LMA gives misleading or contradictory guidance to the flight crew during the training operation. This could happen if the LMA receives conflicting mission feedback from different flight crews.	2.02	2.02
2.03	LMA provides mission related guidance to the flight crew too early before the guidance is applicable. This could happen during the unveiling of new equipment or implementation of novel procedures that the flight crew have not had a chance to use or learn yet.	2.03	1.03
2.04	LMA provides mission related guidance too late after the squadron has completed training sorties. This could happen if the squadron receives information about an aircraft or piece of equipment is already in use on a training sortie.	2.04	1.04
2.05	LMA provides mission related guidance to the flight crew out of order from other guidance that has already been rescinded from training. This could happen if HMA, ATC, and LMA are communicating effectively with the flight crew.	2.05	2.01

Table 7-15: Causal Scenarios Derived from UCA's between ATC and the Flight Crew

CS ID	Causal Scenario	UCA Link	RM ID
3.01	ATC has aircraft closing the runways due to emergencies. Other aircraft are still in the area and asking for status updates on the runway. ATC diverts most of the aircraft to nearby airports, however some aircraft are running low on fuel and do not have the capacity to get diverted to a nearby airport. ATC does not provide clearance or instruction to the flight crew during landing because of the emergencies occupying the runways. As a result, the flight crew of the aircraft are not able to land and enter a hazardous state.	3.01	RM 3.01
3.02	ATC is monitoring a saturated pattern due to a weather recall. Because ATC is busy clearing aircraft to land and deconflicting the pattern, ATC cannot provide guidance to other aircraft in the area for general deconfliction in holding patterns. ATC does not provide instruction or clearance during aircraft deconfliction. As a result, flight crews of aircraft in the holding patterns break minimum separation.	3.02	RM 3.01
3.03	ATC has aircraft closing the runways due to emergencies. Other aircraft are still in the area and asking for status updates on the runway. ATC diverts most of the aircraft to nearby airports, however some aircraft are running low on fuel and do not have the capacity to get diverted to a nearby airport. ATC provides clearance or instruction to the flight crew even though the emergencies are occupying the runways. As a result, the flight crew of the aircraft and the emergency on the runway enter a hazardous state.	3.03	RM 3.01
3.04	ATC is monitoring a saturated pattern during a weather recall. An emergency is declared by one of the aircraft in the pattern and ATC prioritizes landing the emergency. Amid the emergency, ATC redirects other aircraft into holding patterns. Due to the prioritization of the of the emergency, ATC provides instruction to aircraft that leads to airspace conflicts.	3.04	RM 3.01
3.05	ATC is monitoring a saturated pattern during a weather recall. As aircraft are lining up in the pattern, ATC is clearing each of them to land giving each aircraft enough room to land and taxi off the runway safe area. As one of the aircraft touches down, it blows a flat tire and is unable to taxi off the runway. ATC had already given clearance to the flight crew behind the aircraft that blew to flat, prompting a hazardous state for both aircraft.	3.05	RM 3.01
3.06	During flying operations on a day with impending weather ATC is communicating with the flight crew that they should clear the area because of inbound thunderstorms. As the flight crew heads back to the airfield, the storm closes faster than anticipated and the flight crew gets caught in the storm.	3.06	RM 3.01

3.07	ATC provides instruction too early before the flight crew needs to deconflict. This could happen in a scenario where ATC sees multiple aircraft needing to deconflict. By deconflicting one pair of aircraft, another pair of aircraft may need deconfliction or lead to aircraft breaking minimum separation.	3.07	RM 3.01
3.08	ATC provides instruction too late after the flight crew have broken minimum separation standards with another aircraft. This could happen if the aircraft in the airspace have already taken initiative to deconflict due to imminent collision, and the instruction provided by ATC is under the impression that neither aircraft has altered course. As a result, the instruction to deconflict from ATC is too late after the flight crew has broken minimum separation and could potentially lead to a more hazardous condition.	3.08	RM 3.01
3.09	ATC provides instruction or clearance out of order so that the flight crew interprets the procedure incorrectly. This could happen in scenarios where ATC is deconflicting multiple aircraft.	3.09	RM 3.01

Table 7-16: Causal Scenarios Derived from UCA's between the IP and the ASEC

CS ID	Causal Scenario	UCA Link	RM ID
4.01	IP receives inadequate or incorrect feedback from the ASEC and does not make a control input when the student is reaching training limitations. This could happen if the instructor has a flawed mental model and believes the maneuver is recoverable. As a result, the aircraft becomes uncontrollable.	4.01, 4.02, 4.03	RM 11.04
4.02	The student is approaching the instructor's limits of training (critical phases of flight, aircraft deconfliction, etc.). The student is frozen up due to fear or anxiety. The instructor cannot input appropriate flight controls to the ASEC. As a result, the aircraft becomes uncontrollable.	4.04, 4.05, 4.06	RM 11.06 RM 11.07
4.03	The instructor cannot input appropriate flight controls to the ASEC. This could happen if the ASEC is recalibrating to correct a previous error. As a result, the aircraft is uncontrollable.	4.04, 4.05, 4.06	RM 6.01
4.04	The instructor cannot input appropriate flight controls to the ASEC. This could happen if the student has manually overridden the ASEC, which has higher priority than the instructor's input to the ASEC.	4.04, 4.05, 4.06	RM 6.09
4.05	During a critical phase of flight, the IP cannot make appropriate flight inputs due to structural integrity limitations by the ASEC. As a result, the aircraft breaks the minimum safe altitude.	4.04, 4.05, 4.06	RM 5.01
4.06	The instructor controls the ASEC without proper transfer of aircraft control during training maneuvers. This could happen if the instructor believes that the student cannot recover and assumes control without adequate transfer of aircraft control. Because there was never a proper transfer of aircraft control, both the student and the instructor are competing for the shared control of the augmented flight controls. As a result, the aircraft is uncontrollable.	4.07, 4.08, 4.09	RM 6.09 RM 11.06
4.07	The instructor controls the ASEC too early before the student has reached training limitations in a critical phase of the flight. This could happen if the instructor is being overly cautious with the student. As a result, the training mission is not accomplished.	4.10, 4.13	RM 11.08

4.08	The instructor controls the ASEC too late after the student has exceeded the instructor's limitations during a critical phase of flight. This could happen if there is latency or issues with the augmented flight control path.	4.11, 4.14, 4.16	RM 4.01
4.09	The instructor controls the ASEC out of order from verbal cueing during a critical phase of flight. This could happen in time-sensitive situations where the instructor first attempts to cue the student but assumes control of the aircraft due to the lack of time.	4.12, 4.15, 4.27	RM 11.03
4.10	The instructor stops control of ASEC too early before the student can confidently take control of the aircraft during critical phases of flight. This could happen if the instructor believes the student is ready to assume control when the student is not prepared. The instructor preemptively relinquishes control and as a result, the aircraft is uncontrollable.	4.18	RM 4.04
4.11	The instructor takes control of the ASEC too long after an emergency has been averted during critical phases of flight. This could happen if the instructor feels that the student should not finish the sortie after recovering from an emergency. As a result, the training mission is not accomplished. [This scenario should ultimately be left to the discretion of the instructor.]	4.19	RM 11.08
4.12	Instructor stops ASEC control too early during aircraft deconfliction before aircraft are clear of the deconfliction. This could happen if the instructor is talking the student through the procedure and is confident that the student can take over. Upon relinquishing command, the aircraft breaks minimum separation.	4.20	RM 4.04
4.13	Instructor takes control of the ASEC for too long after aircraft deconfliction. This would occur if the instructor still believed there is a risk of aircraft deconfliction in the area. As a result, the training mission is not accomplished.	4.21	RM 11.08

Table 7-17: Causal Scenarios Derived from UCAs between the Student Pilot and the ASEC

CS ID	Causal Scenario	UCA Link	RM ID
5.01	The student receives inadequate or incorrect feedback from the ASEC and does not make a control input when approaching training limitations. As a result, the student does not control the ASEC, and the aircraft becomes uncontrollable.	5.01	RM 6.01
5.02	The student does not control the ASEC during critical phases of flight (takeoff, landing, pattern). This could happen if the instructor has overridden the student's control after realizing that the student was approaching training limits. [Although the student could not input controls to the ASEC, in this context this was the correct control action from the instructor. This is an example of the instructor assuming control to avoid a hazardous condition.]	5.02	N/A
5.03	The student does not control the ASEC during aircraft deconfliction. This could occur if the student has conflicting mental models about how to deconflict. If the instructor tells the student one instruction, this may conflict with what the student has read in a NOTAM, 11-publication, or otherwise.	5.03	RM 11.04
5.04	During a maneuver, the instructor has been incapacitated by injury or a health condition. The instructor recently overrode the student's ability to make control inputs to the ASEC. As a result, the student cannot make the appropriate flight controls to recover the aircraft. As a result, the aircraft becomes uncontrollable	5.04, 5.05, 5.06	RM 5.01
5.05	The student cannot make control inputs to the ASEC during critical phases of flight or aircraft deconfliction. This could occur if the student has unintentionally activated manual flight control.	5.05, 5.06	RM 6.01

5.06	The student controls the ASEC without proper transfer of aircraft control during training maneuvers. This would lead to an unsafe control action if the instructor attempted to assume control, but the student is fixated on recovering the maneuver.	5.07, 5.08, 5.09	RM 4.01
5.07	The student controls the ASEC too early before the instructor has cleared the student to fly in a critical phase of flight. This could occur if the student is anticipating the transfer of aircraft and takes control too early or misunderstands the instructor's relinquishment of control.	5.10, 5.13, 5.15	RM 11.04
5.08	The student controls the ASEC too late after the instructor has cleared the student to fly during a critical phase of flight. This could occur if there is latency or a delay in understanding from the instructor relinquishing control.	5.11, 5.14, 5.16	RM 11.04
5.09	The student controls the ASEC out of order from verbal cuing during a critical phase of flight. This could occur if the instructor has given a lot of instruction to the student that the student has a hard time remembering.	5.12	RM 11.08
5.10	The student stops control of ASEC too early before the instructor takes control of the aircraft during critical phases of flight. This could happen if the student relinquishes control too early before the instructor can assume control. As a result, there would be a period where the aircraft is uncontrollable.	5.17, 5.19	RM 4.04 RM 11.06
5.11	The student takes control of the ASEC too long after an emergency has been declared during critical phases of flight. This could happen if the student is not confident enough in relinquishing control in that moment. As a result, the student would be in conflict with the instructor.	5.18, 5.20	RM 4.01

Table 7-18: Causal Scenarios Derived from UCA's between the ASEC and the Aircraft Subsystems (ASEC Changes FCS)

CS ID	Causal Scenario	UCA Link	RM ID
6.01	ASEC receives a change in FCS from the flight crew to avoid breaking minimum separation with an object (other aircraft, environmental hazard, etc.) and uses a proper control algorithm. However, changes in the FCS make the specified control algorithm inadequate over time and do not change the FCS. This will occur if the object's location or orientation changes so that the new position makes the control algorithm inadequate. This could also happen if the object moves into a position that is unreadable by the system's sensors.	6.01	RM 6.01
6.02	ASEC receives FCS command from the flight crew but receives incorrect feedback about the FCS position and does not change the FCS. This would occur if the necessary feedback from the sensors is not sent or not received by the ASEC.	6.01	RM 6.01
6.03	ASEC receives correct feedback about the FCS orientation but interprets it incorrectly and does not change the FCS. This would occur if the software's control algorithm for the FCS is inadequate for the training maneuver or aircraft orientation.	6.01	RM 6.01
6.04	ASEC does not receive the necessary FCS orientation feedback because the information does not exist. The ASEC does not change the FCS in response. This would occur if the if the FCS were forcibly moved out of the typical range of motion in a high g maneuver and the software cannot account for where the FCS is. In a training environment the likelihood of over-g maneuvering is higher than experienced pilots.	6.01	RM 6.01 RM 6.04
6.05	FCS receives the command from ASEC to change orientation, however the FCS is not as sophisticated as the software, as a result the FCS is not changed. This could happen if the FCS and software controllers were manufactured separately, and the languages used in the software are incompatible with the FCS.	6.01	RM 6.08

*6.06	FCS receives command from the ASEC to change orientation but the process model of the FCS if flawed. As a result, the FCS does not change orientation. This would occur if the orientation of the FCS does not align with the process model of the ASEC. This could happen if there is a conflict in control authority with the flight crew and the ASEC (such as manual override from the flight crew). In this system there are two potential manual override commands from both the IP and the student.	6.01	RM 6.03 RM 6.09
6.07	FCS receives control input from the ASEC to change orientation but there are other objects interfering with the FCS movement. As a result, the FCS does not direct a change orientation, however the process model of the ASEC is under the impression that the change did happen. This could happen in the common occurrence of a bird strike.	6.01	RM 6.02
6.08	ASEC receives change in FCS from the flight crew and uses proper control algorithm, however changes in the aircraft's orientation makes the specified control algorithm inadequate over time and does not direct the FCS to return the aircraft to a stable state. This will occur if the ASEC's control algorithm is unfamiliar with the position that the aircraft is in and has no direct response to return the aircraft to a stable flying state. For instance, if the aircraft is hit by a projectile (e.g., bird strike) and places the FCS in an unfamiliar orientation.	6.02	RM 6.02
6.09	ASEC receives FCS command from the flight crew but receives incorrect feedback about the state of the aircraft and does not change the FCS. This would occur if the necessary feedback from the sensors is not sent or not received by the ASEC. For instance, if the aircraft is falling the aircraft's sensors may say that it is oriented correctly, however the aircraft's accelerometer will read negative or zero g forces.	6.02	RM 6.04
6.10	ASEC receives correct feedback about the aircraft's state but interprets it incorrectly and does not change the FCS. This would occur if the software's control algorithm were inadequate for controlling the FCS while the aircraft is in an uncontrollable state.	6.02	RM 6.03
6.11	ASEC does not receive the necessary parameters because the information does not exist. The ASEC does not change the FCS. This would occur if the if the aircraft is missing the proper sensors to detect the aircraft's state, potentially if the FCS is out of its standard ROM.	6.02	RM 6.02
6.12	FCS receives command from the ASEC to recover the aircraft from an uncontrollable state, but the process model of the FCS if flawed and does not recover from the position. This would occur the position the FCS does not align with the process model of the ASEC. This could happen if there is a conflict in control authority with the flight crew and the ASEC.	6.02	RM 6.03
*6.13	ASEC does not receive change in FCS from the flight crew, however the control algorithm from the ASEC commands a change in the FCS which guides the aircraft within minimum separation standards to an obstacle. This will occur if the ASEC has conflicting control authorities between the operators (autopilot from student, override from instructor).	6.03	RM 6.03 RM 6.09
6.14	ASEC does not receive FCS command from the flight crew but receives incorrect feedback about the orientation of the FCS and changes the FCS. As a result, the ASEC changes the orientation of the FCS. This will occur if the system incorrectly senses the orientation of the FCS.	6.03	RM 6.01
6.15	ASEC receives correct feedback about the FCS orientation but interprets it incorrectly and changes the FCS. This would occur if the software's control algorithm is inadequate for the orientation of the FCS. This would occur if turbulence knocked the FCS out of position from the ASEC’s calibrated orientation, or if a student over g’s the aircraft during a training maneuver.	6.03	RM 6.02
6.16	ASEC does not receives change in FCS from the flight crew and uses proper control algorithm, however changes in the aircraft's orientation makes the specified control algorithm inadequate over time (or through incorrect feedback), and the ASEC changes the FCS to position the aircraft in an uncontrollable state. This will occur if the ASEC's receives incorrect feedback from the sensors indicating that the aircraft needs FCS input to recover from an incorrectly assessed uncontrollable position. Another case is if	6.04	RM 6.01

	control algorithm is unfamiliar with the orientation of the FCS and has no direct response and then places the aircraft in an uncontrollable position.		
6.17	ASEC receives correct feedback about the aircraft's state but interprets it incorrectly and changes the FCS to position the aircraft in an uncontrollable state. This would occur if the software's control algorithm is inadequate for recovering the aircraft from an uncontrollable state.	6.04	RM 6.01 RM 6.04
6.18	FCS receives command from the ASEC to change the FCS, but the process model of the FCS is flawed and positions the aircraft in an uncontrollable position. This would occur the process model of the FCS does not align with that of the ASEC.	6.04	RM 6.05
6.19	ASEC receives change FCS command from the ASEC. A flawed process model leads to the FCS not changing in time such that minimum separation standards are broken. This could happen if the ASEC cannot properly communicate with the FCS and continues the previous flight profile regardless of the control action of the ASEC due to poor connection between the subsystems and the ASEC.	6.06	RM 6.03
6.20	ASEC receives change FCS command from the ASEC, but the control action is not received in time by the FCS. As a result, the aircraft breaks minimum separation standards. This could happen if the controlled process encounters interference, such as damage from severe turbulence interfering with the interfacing.	6.06	RM 6.08
6.21	ASEC receives change FCS command from the ASEC. A flawed process model leads to the FCS not changing in time such that the aircraft remains in an uncontrollable state. This would lead to the aircraft worsening the uncontrollable state by inputting the wrong control actions to the aircraft subsystems. This could happen during a training maneuver, where a high g maneuver interferes with the interfacing between the ASEC and the aircraft subsystems.	6.07	RM 6.06 RM 6.07
6.22	ASEC receives change FCS command from the ASEC. A flawed process model leads to the FCS not changing in time such that the aircraft remains in an uncontrollable state. This could happen if the ASEC encounters other disturbances, such as negative g forces due to inversion from a previous maneuver have interfered with the controlled process to the subsystems.	6.07	RM 6.06 RM 6.07
6.23	Flight crew does not approve of FCS change. The ASEC believes that the FCS need to be changed for flawed control algorithm in the autopilot. As a result, the FCS is changed without the flight crew's proper control authority.	6.08	RM 6.03
6.24	The flight crew is using the aircraft's autopilot to cruise and does not direct the ASEC to change the FCS. Due to outside information from another controller, the ASEC changes the FCS to reroute to a new location. This could happen if the systems of the trainer are not properly encrypted, and an adversary sends a control action to the system's ASEC.	6.08	RM 6.08
6.25	The flight crew does not input a flight control change. The ASEC recognizes feedback from sensors that the aircraft is nearing a hazardous condition (breaking minimum separation or close to stall). As a result, the ASEC directs a change in the FCS before the input has been assessed by the flight crew.	6.09	RM 6.02
6.26	The ASEC directs change in the FCS, however the control path to the aircraft subsystems is damaged and the aircraft subsystems encounter lag and apply the FCS for too long. As a result, the aircraft enters a hazardous condition. This could happen if the aircraft over g's, and the maneuver damages the control path.	6.10	RM 6.06 RM 6.07
6.27	The ASEC directs change in the FCS, the instructor notices the aircraft approaching the structural limits and overrides to manual control. Because of a lag in the override process, the ASEC changes the FCS for too long and the aircraft enters a hazardous condition.	6.11	RM 6.06
6.28	The Aircraft is entering near another aircraft. The ASEC receives correct feedback about the position of the other aircraft and correctly applies changes to the FCS to avoid the break in minimum separation. The ASEC's control algorithm incorrectly assumes	6.12	RM 6.02

	that the aircraft will avoid breaking minimum separation. This could occur if the control algorithm is predicting the course of the trainer, however the control algorithm is lacking the information to predict the course of the other aircraft. As a result, the ASEC applies the FCS change for too short of a time and the aircrew break minimum separation.		
6.29	The aircraft conducted a training maneuver that damaged the aircraft's sensors. The flight crew choose to activate the aircraft's autopilot, because the aircraft's hardware was damaged the ASEC attempts to modify the FCS but does not change the FCS for long enough and places the aircraft in a hazardous condition.	6.13	RM 6.01 RM 6.04
6.30	The aircraft bounced on a touch and go and damaged the wheel sensors and actuators. As a result, the flight crew command the ASEC to lower the landing gear for a landing, however the ASEC does not lower the landing gear enough and the aircraft remains in a hazardous condition during landing.	6.13	RM 6.04 RM 6.07

Table 7-19: Causal Scenarios Derived from UCA's between the ASEC and the Aircraft Subsystems (ASEC Limits FCS)

CS ID	Causal Scenario	UCA Link	RM ID
7.01	The flight crew is performing high g training maneuvers. As the flight crew approaches the g limit, a sudden gust of wind abruptly jerks the aircraft past the g limits. As a result, the ASEC does not limit the FCS, and the structural integrity of the aircraft is violated.	7.01	RM 7.01
7.02	The flight crew is performing high g training maneuvers. The flight crew is in a dive and as the flight crew approaches the g limit, the airspeed increases but their control actuation remains the same. As the airspeed increases, the load on the aircraft increases past the g limit. Because the control actuation was not increased, the ASEC did not limit in anticipation of the over-g. As a result, the structural integrity of the aircraft is violated.	7.01	RM 7.01
7.03	ASEC receives FCS change from the flight crew that will violate the structural integrity of the aircraft and uses proper control algorithm. However, changes in the aircraft's orientation make the specified control algorithm inadequate over time and the ASEC does not limit FCS input. This would occur if the student pilot is performing sporadic control inputs in training.	7.01	RM 7.01
7.04	The flight crew is performing high g training maneuvers. As the flight crew approaches the g limit, the ASEC cannot limit the control actuation because the necessary feedback needed by the control algorithm to make this control action does not exist. This could occur if turbulence damaged the aircraft's accelerometer or one of the necessary sensors needed by the ASEC's process model to determine if the aircraft is on a trajectory to violate the structural integrity of the aircraft.	7.01	RM 7.02
7.05	The flight crew is performing high g training maneuvers. As the flight crew approaches the g limit, the ASEC cannot limit the control actuation because the feedback received by the ASEC is incorrect. This could happen if one of the sensors is not calibrated properly and the ASEC's control algorithm bases its decision to limit control actuation off the incorrect sensor. As a result, the structural integrity of the aircraft is violated.	7.01	RM 7.03
7.06	ASEC receives correct feedback about the aircraft's structural limitations but interprets it incorrectly. As a result, the ASEC does not limit the FCS input from the flight crew. This would occur if the software's control algorithm is inadequate not calibrated or preflighted correctly.	7.01	RM 7.01 RM 7.03
7.07	The flight crew is performing training maneuvers. As the flight crew approaches an obstacle, they turn away from the obstacle and the FCS limits the control input in anticipation of structural integrity violation. As a result, the crew cannot turn away fast enough from the object and the aircraft breaks minimum separation with the object.	7.02	RM 7.06

7.08	ASEC receives FCS change from the flight crew that will not violate the structural integrity of the aircraft and uses proper control algorithm, however changes in the aircraft's orientation makes the specified control algorithm inadequate over time, and the ASEC limits FCS input. This would occur if there is lag in the sensors and actuators responsible for limiting excessive control.	7.02	RM 7.02 RM 7.03
7.09	The flight crew is recovering from an emergency in the area. The flight crew lost a lot of altitude when recovering and needs to pull up. The FCS limits the control input of the crew trying to pull up. As a result, the flight crew cannot pull up and breaks the minimum separation with the ground.	7.03	RM 7.06
7.10	The flight crew is in the area with another aircraft. As the aircraft approach each other, they both bank to the right however the FCS limits the control actuation too early before they can move away from other aircraft. As a result, the aircraft break minimum separation.	7.04	RM 7.06
7.11	The flight crew is performing high g training maneuvers. As the flight crew approaches the g limit, they continue the control actuation and violate the limits of structural integrity. This could happen if the control algorithm recognizes the need to limit control actuation too late.	7.05	RM 7.01
7.12	ASEC limits the FCS from flight crew input, however FCS limitations responds too late or applies too short of an FCS command. As a result, the ASEC does not limit input from the flight crew and the flight crew violates the aircraft's structural integrity. This would lead to the aircraft necessitating new emergency limitations after the aircraft has already broken structural limits. The old limits of flying would not be applicable in the scenario where the aircraft has already broken limitations and adhering to the old limitations could be hazardous to the aircraft. This could happen because changing conditions from violating aircraft structural integrity make the control algorithm inadequate or cause the process model to be flawed.	7.05	RM 7.04 RM 7.05
7.13	The flight crew is performing high g training maneuvers. The ASEC limits change in the FCS, however the control algorithm limits the control actuation for too short of a time that the aircraft still violates structural integrity limits.	7.06	RM 7.01
7.14	The flight crew is training in the area. As the flight crew make a turn, the ASEC limits control actuation. As the aircraft turns, the airspeed slows, and the control algorithm becomes inadequate to the changing conditions. AS a result, the ASEC limits the FCS for too long that the flight crew cannot perform a training maneuver.	7.07	RM 7.01 RM 7.05

Table 7-20: Causal Scenarios Derived from UCAs between the ASEC and the Aircraft Subsystems (ASEC Changes Internal Environment)

CS ID	Causal Scenario	UCA Link	RM ID
8.01	ASEC receives change internal environment command from the flight crew but does not recognize the need to activate internal climate control. This would occur if the ASEC has a flawed control algorithm or receives inaccurate feedback from the sensors that indicates there is no need to change internal environment (i.e., the internal environment is already at an unsafe state, or the internal environment is already at the requested temperature).	8.01	RM 8.01
8.02	ASEC does not receive the necessary internal climate feedback because the information does not exist. The ASEC does not change the internal environment conditions. This would occur if there were not appropriate climate sensors in all the vital locations for the flight crew or vital hardware. This would also occur if the sensors were damaged and there was not adequate feedback to inform the ASEC/Operators that the sensor readings are incorrect.	8.01	RM 8.01
8.03	ASEC sends the command to change internal climate, however the internal climate systems have already been damaged. This could happen if there is no factor of safety to prevent the internal climate from reaching extreme conditions. As a result, the internal	8.01	RM 8.02

	systems could already be damaged, and the sensors may be ineffective. At this point the internal climate my not be changeable because of damage to the internal systems.		
8.04	ASEC does not receive change internal environment command from the flight crew but uses flawed control algorithm which recognizes the hazardous condition for the flight crew and changes the internal environment. This would occur if the ASEC has a flawed control algorithm or receives inaccurate or misleading feedback from internal sensors.	8.02	RM 8.01
8.05	ASEC does not receive the necessary internal climate feedback because there is a delay in receiving internal climate sensing. The ASEC changes the internal environment conditions too late after the aircraft environment has damaged the aircraft's hardware. This would occur if there are not the appropriate sensors in all the vital locations for the flight crew or vital hardware.	8.03	RM 8.01
8.06	ASEC does not receive the necessary internal climate feedback because the necessary sensor has been damaged by the environment already. The ASEC changes the internal environment conditions too late after the aircraft environment has damaged the aircraft's hardware and negatively impacted the flight crew's performance. This would occur if the feedback path or hardware for a sensor is placed in a location that is downstream of the vital hardware components. Thereby the sensed temperature would be less extreme than what is being exhibited by the hardware.	8.03	RM 8.01
8.07	ASEC receives the necessary internal climate feedback, however there is a lag to what the flight crew experiences and what is measured on the sensor. As a result, the internal environmental systems are applied for too long and the flight crew's performance is negatively affected. This could occur if the internal environment sensors are placed in an arbitrary location away from the flight crew, where the flight crew would be closer to the internal environment actuators (heat/cooling vents) as compared to the environmental sensor.	8.04	RM 8.02
8.08	ASEC receives internal climate feedback, however one of the sensors is faulty and the control algorithm reads that sensor over the others. As a result, the internal environmental systems are applied for too long (or too short) and the flight crew's performance is negatively affected. This could occur if there are multiple internal environment sensors and ASEC's control algorithm abides by the most conservative estimates of the internal climate.	8.04, 8.05	RM 8.01
8.09	ASEC receives the necessary internal climate feedback, however there is a lag to what the is measured on the sensor and what the flight crew experiences. As a result, the internal environmental systems are applied for too short of a time, and the flight crew's performance is affected. This could occur if the internal environment sensors are placed too close to the internal environment actuators (heat/cooling vents) as compared to the operators.	8.05	RM 8.01

Table 7-21:Causal Scenarios Derived from the UCAs between the Instructor and the Aircraft Subsystems.

CS ID	Causal Scenario	UCA Link	RM ID
9.01	The flight crew is recovering from an emergency that requires an override of the ASEC. The instructor does not input the appropriate manual flight controls. This could happen if the instructor's mental model conflicts with the actual controlled process if augmented flight controls are too different from the manual override. As a result, the aircraft becomes uncontrollable.	9.01	RM 9.01
9.02	The instructor does not override the ASEC during critical phases of flight. This could happen if the instructor ASEC believes that the ASEC was corrected after recalibration when it was never corrected. As a result, the aircraft becomes uncontrollable.	9.02	RM 6.01

9.03	The instructor does not override the ASEC during aircraft deconfliction. This could happen if disabling the flight augmentation of the ASEC also disables instruments that are necessary for aircraft deconfliction (such as tracking other aircraft). As a result, the instructor does not override the ASEC, and the aircraft becomes uncontrollable.	9.03	RM 9.02
9.04	The instructor cannot override the ASEC as the student is nearing the limits of training. This could happen if the control to override the ASEC is sent by the instructor is sent but not received. As a result, ASEC control cannot be bypassed.	9.04	RM 5.01
9.05	The instructor cannot override the ASEC during critical phases of flight. This could happen if the ASEC senses that the aircraft is in an emergency state and enforces its own safety constraints over the pilots. As a result, the instructor cannot override the ASEC, and the aircraft becomes uncontrollable.	9.05	RM 6.09
9.06	The instructor cannot override the ASEC during aircraft deconfliction. This could happen if there is a faulty control path from the flight crew to the ASEC/Manual Flight controls. As a result, the aircraft becomes uncontrollable.	9.06	RM 5.01
9.07	The instructor overrides the ASEC without proper transfer of aircraft control during training maneuvers. This could happen if the instructor believes that the student cannot recover the maneuver with the ASEC and overrides to manual control. Because there was never proper transfer of aircraft control, both the student and the instructor are competing for the shared control of the manual flight controls. As a result, the aircraft is uncontrollable	9.07	RM 4.01
9.08	The instructor overrides the ASEC without proper transfer of aircraft control during critical phases of flight. This could occur if the ASEC prevents of flight augmentation too close to the ground. As a result, the aircraft becomes uncontrollable.	9.08	RM 6.09
9.09	The instructor overrides the ASEC without proper transfer of aircraft control during aircraft deconfliction. This could be a result of the ASEC shutting itself down which is possible if the software has any conditions where it shuts itself down under certain conditions or if the aircraft violates limits of structural integrity. The instructor is not prepared for this override and as a result the aircraft is uncontrollable.	9.09	RM 9.03
9.10	The instructor overrides the ASEC too early before the student has reached the limits during critical phases of flight. As a result, the shared control makes the aircraft difficult to control and as a result the flight crew break training limits.	9.10	RM 4.01
9.11	The instructor overrides the ASEC too late after the student has reached the limits during critical phases of flight. This could occur if there is a delay or latency in the override controls. As a result, the aircraft become uncontrollable.	9.11	RM 4.01 RM 5.01
9.12	The instructor overrides the ASEC too early before the flight crew needs to deconflict with an aircraft. This could occur if the student is frozen on the controls and the instructor needs to control over the aircraft. The instructor overrides the ASEC in attempt to gain control of the aircraft.	9.12	RM 4.01
9.13	The instructor overrides the ASEC too late after the flight crew has broken minimum separation. As a result, the ASEC cannot limit the flight control inputs from the flight crew. The proceeding maneuver violates structural integrity of the aircraft.	9.13	RM 6.03
9.14	The instructor overrides the ASEC too early during training maneuvers. As a result, the instructor needs to recalibrate the ASEC and flight augmentation. As a result, the flight crew cannot accomplish training mission objectives.	9.14	RM 6.03
9.15	The instructor overrides the ASEC too late after exceeding training limitations. This could happen if the ASEC does not limit control input and the flight crew exceed training limitations. If the ASEC does not acknowledge the aircraft structural integrity being violated, it will not appropriately limit control actions. Furthermore, if the structural integrity of the aircraft has been violated, augmented flight controls may be affected. As a result, the aircraft is uncontrollable.	9.15	RM 7.04

9.16	Instructor stops override of ASEC too soon before the ASEC is controllable during critical phases of flight. This could happen if the ASEC has completed a recalibration and the instructor believes it could benefit the critical phase of flight. As a result, the fast change from manual to augmented flight controls makes the aircraft uncontrollable.	9.16	RM 9.04
9.17	Instructor overrides ASEC for too long that the aircraft becomes uncontrollable. This could happen if the environment the flight crew are flying in would benefit from flight augmentation.	9.17	RM 6.01

Table 7-22: Causal Scenarios Derived from the UCAs between the Student and the Aircraft Subsystems

CS ID	Causal Scenario	UCA Link	RM ID
10.01	The flight crew is recovering from an emergency that requires an override of the ASEC. The instructor cannot input the flight controls (IP is incapacitated). The student does not input the appropriate manual flight controls. This could happen if the student's mental model conflicts with the actual controlled process. Augmented flight controls must be designed to operate similarly to manual override. As a result, the aircraft becomes uncontrollable.	10.01	RM 9.01
10.02	The flight crew is recovering from an emergency and the instructor has been incapacitated. The student does not override the ASEC because the instructor's assumption of control is preventing the student from bypassing the ASEC. As a result, the aircraft becomes uncontrollable.	10.01	RM 10.02
10.03	The flight crew is recovering from an emergency and the instructor is cueing the student to override the ASEC. The student has a flawed mental model and does not override the ASEC when cued by the instructor because the student does not believe the override is necessary. As a result, the aircraft becomes uncontrollable.	10.02	RM 11.04
10.04	The student is recovering from a maneuver during training. The student is struggling to recover from the maneuver. As the flight crew loses altitude, the student decides that overriding the ASEC would aid the recovery. The student overrides the ASEC during a critical phase of flight without command from the instructor. As a result, training limitations are broken.	10.03	RM 11.04
10.05	The flight crew is recovering from an emergency that requires an override of the ASEC. The instructor cannot input the flight controls (IP is incapacitated). The student inputs manual flight controls without enough experience with manual controls. This could happen if augmented flight controls are not designed to operate similarly to manual override. As a result, the aircraft becomes uncontrollable.	10.04	RM 9.01
10.06	The student overrides the ASEC too early before being instructed. This could happen if manual flight controls are not practiced as part of an emergency procedure. As a result, the aircraft becomes uncontrollable.	10.05	RM 9.01
10.07	The student overrides the ASEC too late after being instructed. This could happen if the flight crew receives inadequate feedback and does not recognize the need to override the ASEC. As a result, the aircraft become uncontrollable.	10.06	RM 10.03
10.08	The student stops overriding the ASEC too soon before the aircraft is controllable. This could happen if the ASEC requires recalibration but does not provide adequate feedback to the flight crew that the recalibration is completed, or the recalibration does not address the problem with the ASEC. As a result, the aircraft is uncontrollable.	10.07	RM 6.01

10.09	The student overrides the ASEC for too long after flight augmentation is needed for safe operation. This could occur if there is no notification to alert the pilots that flight augmentation is recommended for safe flight. As a result, the aircraft becomes uncontrollable.	10.08	RM 6.01

Table 7-23: Causal Scenarios Derived from the UCAs between the Instructor and Student Pilot

CS ID	Causal Scenario	UCA Link	RM ID
11.01	The student is performing adequately during training maneuvers. The student begins to approach the training limits of the instructor. The instructor does not provide any input to the student. This could happen as a result of a student's performance in the program. If the student is on a progress check, a subpar grade will remove the student from the program. If the instructor says anything to the student, it will lower the student's grade and thus remove the student from the program. The student is outside the training limits; however, the experienced instructor is confident that it is recoverable. As a result, the instructor does not cue the student, and the aircraft exceeds training limitations.	11.01	RM 11.01 RM 11.02
11.02	The student is performing adequately during training maneuvers, and the instructor recognizes the student is approaching the limits of training. The instructor incorrectly assumes that the student also recognizes that the flight crew is approaching training limits. This could happen if the student has flown with a different instructor with slightly different training limitations. As a result, the instructor does not cue the student pilot, and the aircraft enters exceeds training limits.	11.01	RM 11.01 RM 11.02
11.03	The student is performing adequately during training maneuvers, and the instructor recognizes the student is approaching the limits of training. The flight crew receives guidance from ATC or HMA, but the student interprets it differently than the instructor. The instructor incorrectly assumes that the ATC/HMA guidance is interpreted the same way. As a result, the student performs a maneuver under the assumption that ATC/HMA guidance will not exceed the instructor's training limitations. The student unexpectedly exceeds the limitations of the instructor.	11.01	RM 11.04
11.04	The student is performing adequately during training maneuvers, and the instructor recognizes the student is approaching the limits of flight. In this scenario, the student engages a certain mode of the ASEC. The student communicates this with the instructor however, the student has a different understanding of the mode than the instructor. This could happen if the student has not used a certain mode of the aircraft outside simulations. The instructor incorrectly assumes that the student's mental model of the ASEC mode is aligned with the instructor's mental model. As a result, the instructor has no reason to cue the student and the student inputs a control action that breaks the instructors training limitations.	11.01	RM 11.04
11.05	The student is performing adequately during training missions, and the instructor recognizes the student is approaching the limits of training. During a training maneuver, the student recognizes the maneuver to be similar to a maneuver that the student encountered in the last training phase (where a different aircraft was used). As a result, the student executes the maneuver equivalently to how it would be executed in the last training phase. As a result, the student unexpectedly reaches the instructor's limitations without the instructor being able to cue the student.	11.01	RM 11.05
11.06	The student is performing adequately during training missions, and the instructor recognizes the student is approaching the limits of training. The aircraft is approaching certain landmarks and the instructor notices that they are about to exceed the minimum	11.01	RM 11.04

	safe altitude over certain environments. The instructor incorrectly assumes that the student is aware of this and therefore does not cue the student. The student's mental model of the environment is different from the instructor's mental model of the environment. As a result, the instructor does not cue the student and the student exceeds the minimum safe altitude.		
11.07	The student is performing adequately during training missions, and the instructor recognizes the student is approaching the limits of training for a maneuver. The instructor has seen the student perform the maneuver up to a satisfactory grade on the maneuver item file (MIF) in past sorties. The instructor incorrectly assumes that the student will perform the same maneuver correctly as the student did in the past. Therefore, the instructor does not provide any cuing to the student. The instructor's mental model of the student is flawed, and the student exceeds training limitations.	11.01	RM 11.04
11.08	The student is performing adequately during the training mission, and the instructor recognizes that the student is approaching the limits of training for a maneuver with regards to the environment. In the past the student has recognized environmental limitation (such as crosswinds, minimum altitudes, minimum separations, etc.). As the training sortie has progressed, the environment changes (e.g., from an unpopulated rural area to an urban area) where the limits of training have changed. The instructor having seen the student demonstrate good discipline with regards to environmental limitations has no reason to believe that the student will exceed limitations in this new environment, and thus does not cue the student. The student does not respond to the changing environment and as a result the aircraft exceeds training limitations.	11.01	RM 11.04
11.09	The student is performing adequately during training maneuvers. The student begins to approach the training limits of the instructor. The student assures the instructor that the correct procedure for the maneuver is being followed and applied. The instructor does not provide any input to the student but notices the flight crew is still approaching the limits of training. This could happen because of a student's overconfidence. The student exceeds the limits of training; however, the student assures the instructor that the correct procedures are being followed. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft exceeds training limitations. This is an example of inadequate feedback from the student where the instructor is seeing conflicting feedback in the aircraft performance versus what the student is saying.	11.01	RM 11.04
11.10	The student is performing adequately during training maneuvers. The student begins to approach the training limits of the instructor. The maneuver in question requires checklist items. The student initiates all the necessary challenge and response items on the checklist. The student assures the instructor that the asterisked items are being executed. The instructor does not provide any input to the student. The instructor also receives no feedback that the student has completed the checklist item, other than the student's challenge and response. The student does not complete the item or incorrectly completes the checklist item. This could happen because of tandem training challenges. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft exceeds training limitations. This is an example of inadequate feedback from the student where the instructor is not receiving any feedback to validate what the student is saying.	11.01	RM 11.06
11.11	The student is performing adequately during training maneuvers. The student begins to approach the training limits of the instructor. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. In tandem cockpits, the instructor cannot directly see the student and therefore has no way to validate what the student is claiming. The last scenario outlines a lack of feedback mechanisms between the two cockpits whereas this scenario is highlighting the lack of visual feedback between tandem cockpits.	11.01	RM 11.06

	As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft exceeds training limitations. This is an example of inadequate feedback from the student where the instructor is not receiving any visual feedback to validate what the student is saying.		
11.12	The student is performing adequately during training maneuvers. The student begins to approach the training limits of the instructor. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the student gets nervous and tenses up. In tandem cockpits, the instructor cannot directly see the student and therefore has no way see if the student is panicking or tensing up. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft exceeds training limitations. This is an example of inadequate feedback from the student where the instructor is not receiving any visual feedback to validate the student's condition.	11.01	RM 11.01 RM 11.07
11.13	The student is performing adequately during training maneuvers. The student begins to approach the training limitations of the instructor. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the instructor notices the ASEC is giving inconsistent feedback to what the student is saying. This could happen if the student claims to follow the procedure but incorrectly does so. Given the conflicting feedback, instructor chooses to believe the student. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft exceeds training limitations.	11.01	RM 11.04 RM 11.06
11.14	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. This could happen on a student's progress check, where a subpar grade will remove the student from the program. If the instructor says anything to the student, it will lower the student's grade and thus remove the student from the program. As the student reaches training limitations, instructor believes that the student can still recover the aircraft. As a result, the instructor does not cue the student and aircraft enters a hazardous state during a critical phase of flight.	11.02	RM 11.02
11.15	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The instructor incorrectly assumes that the student also recognizes that the aircraft is approaching the limits of training. This could happen if the student has flown with a different instructor who has slightly different training limitations. As a result, the instructor does not cue the student and the aircraft enters a hazardous state during a critical phase of flight.	11..02	RM 11.04 RM 11.08
11.16	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The flight crew receives instruction from ATC or HMA regarding clearance to land, but the student interprets it differently than the instructor. The instructor incorrectly assumes that the student interprets ATC/HMA guidance the same. As a result, the instructor does not cue the student and student unexpectedly exceeds the limitations of the instructor.	11.02	RM 11.04
11.17	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. In this scenario, the student engages a certain mode of the ASEC. The student communicates this with the instructor however, the student has a different understanding of the mode than the instructor. This could happen if the student has not used a certain mode in context of a critical phase of flight. Some modes of the ASEC may require different control inputs at lower altitudes. The instructor incorrectly assumes that the student's mental model of the ASEC	11.02	RM 11.04

	mode is aligned with the instructor's mental model. As a result, the instructor has no reason to cue the student and the student inputs a control action that enters the aircraft into a hazardous state during a critical phase of flight.		
11.18	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. As the aircraft descends, the student recognizes a condition to be like a scenario that the student encountered in the last training phase (where a different aircraft was used). As a result, the student executes control actions equivalently to how it would be executed in the last training phase. As a result, the student unexpectedly enters a hazardous state without the instructor being able to cue the student.	11.02	RM 11.05
11.19	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The aircraft descends, the instructor notices that they are deviating from standard practice (off-centerline, high glidepath, low airspeed, etc.). The instructor incorrectly assumes that the student is aware of this and therefore does not cue the student. The student's mental model of the environment (or the student's situational awareness) is different from the instructor's mental model of the environment. As a result, the instructor does not cue the student and the aircraft enters a hazardous state during critical phases of flight.	11.02	RM 11.04
11.20	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The instructor has seen the student perform a landing up to a satisfactory grade on the maneuver item file in past sorties. The instructor incorrectly assumes that the student will perform the same landing correctly as the student did in the past. Therefore, the instructor does not provide any cuing to the student. The instructor's mental model of the student is flawed, and student enters a hazardous condition during a critical phase of flight.	11.02	RM 11.04
11.21	In this scenario, the flight crew is landing with reported wind shear on the final approach. The student is adequately performing the final approach. Winds suddenly shift direction 100 feet until touchdown. The instructor recognizes that the student is still on a good final approach even though the winds have shifted. The student however does not communicate the environmental changes with the instructor. The instructor having seen the student demonstrate good discipline with regards to environmental limitations has no reason to believe that the student will not adjust to the new environment, and thus does not cue the student. The student does not respond to the changing environment and as a result the aircraft enters a hazardous condition on final approach.	11.02	RM 11.01 RM 11.04
11.22	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The student assures the instructor that the correct procedure for the landing is being followed and applied. The instructor does not provide any input to the student but notices the flight crew is still approaching the limits of training. This could happen because of a student's overconfidence in their own flying ability. The student exceeds the limits of training; however, the student assures the instructor that the correct procedures are being followed. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft enters a hazardous state during a critical phase of flight. This is an example of inadequate feedback from the student where the instructor is seeing conflicting feedback in the aircraft performance versus what the student is saying.	11.02	RM 11.01 RM 11.04
11.23	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The maneuver in question requires checklist items. The student initiates all the necessary challenge and response items on the checklist. The student assures the instructor that the asterisked items are being executed. The instructor does not provide any input to the student. The instructor also receives no feedback that the student has completed	11.02	RM 11.06 RM 11.07

	the checklist item, other than the student's challenge and response. The student does not complete the item or incorrectly completes the checklist item. This could happen because of tandem training challenges. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft enters a hazardous condition during a critical phase of flight. This is an example of inadequate feedback from the student where the instructor is not receiving any feedback to validate what the student is saying.		
11.24	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. In tandem cockpits, the instructor cannot directly see the student and therefore has no way to validate what the student is claiming. The last scenario outlines a lack of feedback mechanisms between the two cockpits whereas this scenario is highlighting the lack of visual feedback between tandem cockpits. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft enters a hazardous condition during a critical phase of flight. This is an example of inadequate feedback from the student where the instructor is not receiving any visual feedback to validate what the student is saying.	11.02	RM 11.06 RM 11.07
11.25	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the student gets nervous and tenses up. In tandem cockpits, the instructor cannot directly see the student and therefore has no way see if the student is panicking or tensing up. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft enters a hazardous condition during a critical phase of flight. This is an example of inadequate feedback from the student where the instructor is not receiving any visual feedback to validate the student's condition.	11.02	RM 11.01 RM 11.07
11.26	The student begins to approach the instructor's limits during a critical phase of flight (e.g., landing). The instructor does not provide any instruction to the student. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the instructor notices the ASEC is giving inconsistent feedback to what the student is saying. This could happen if the student claims to follow the procedure but incorrectly does so. Given the conflicting feedback, instructor chooses to believe the student. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft enters a hazardous condition during a critical phase of flight.	11.02	RM 11.01 RM 11.06
11.27	The aircraft is on final approach and the instructor is cuing the student as they descend. As they rapidly approach the ground, the aircraft is hit with a gust of wind. As the instructor assesses the situation, he stops instruction. As a result, the student is confused on what to do in the critical phase of flight. As a result, the aircraft enters a hazardous condition.	11.02	RM 11.03
11.28	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. This could happen on an evaluation flight of the student. As the student approaches minimum separation, instructor believes that the student can still maneuver away from other aircraft. As a result, the instructor does not cue the student and aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.29	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The instructor	11.03	RM 11.04

	incorrectly assumes that the student also recognizes that the aircraft is approaching minimum separation. This could happen if the student has not seen how close minimum separation is in practice. As a result, the instructor does not cue the student and aircraft breaks minimum separation during aircraft deconfliction.		
11.30	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The flight crew receives instruction from ATC or HMA regarding aircraft deconfliction, but the student interprets it differently than the instructor. The instructor incorrectly assumes that the student interprets ATC/HMA guidance the same. As a result, the instructor does not cue the student and the aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.31	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The instructor notices that aircraft is getting closer to the other aircraft. The instructor incorrectly assumes that the student is aware of the closing aircraft and therefore does not cue the student. This could happen in scenarios where there is more than one aircraft to deconflict from. The student's mental model of the environment (or the student's situational awareness) is different from the instructor's mental model of the environment. As a result, the instructor does not cue the student and the aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.32	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The instructor has seen the student perform deconflict with other aircraft in past sorties. The instructor incorrectly assumes that the student will perform the same deconflicting practices as the student did in the past. Therefore, the instructor does not provide any cuing to the student. The instructor's mental model of the student is flawed, and the aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.33	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The student communicates intentions to deconflict with the instructor. The instructor approves of the students plan to deconflict however the instructor also notices that the environment has changed. The student's deconfliction plan will no longer be viable due to the changed environment. This could happen if the student's intended deconfliction would break minimum separation with other aircraft or objects in the environment. The student however does not communicate the environmental changes with the instructor. The instructor having seen the student demonstrate good discipline with regards to environmental limitations has no reason to believe that the student will not adjust to the new environment, and thus does not cue the student. The student does not respond to the changing environment and as a result the aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.34	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the student gets nervous and tenses up. In tandem cockpits, the instructor cannot directly see the student and therefore has no way see if the student is panicking or tensing up. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft breaks minimum separation during aircraft deconfliction. This is an example of inadequate feedback from the student where the instructor is not receiving any visual feedback to validate the student's condition.	11.03	RM 11.01 RM 11.07

11.35	During a training sortie, the flight crew encounters saturated airspace where aircraft deconfliction is necessary. The instructor helps the student clear but does not provide any instruction to the student to deconflict from the situation. The student assures the instructor that the appropriate procedures are being followed. The instructor does not provide any input to the student. After assuring the instructor, the instructor notices the ASEC (specifically the Traffic Collision Avoidance System) is giving inconsistent feedback to what the student is saying. This could happen if the student claims to follow the procedure but incorrectly does so. Given the conflicting feedback, instructor chooses to believe the student. As a result, the instructor does not believe instruction is necessary and does not cue the student. The aircraft breaks minimum separation during aircraft deconfliction.	11.03	RM 11.04
11.36	The flight crew are performing maneuvers in the area. The instructor is cuing the student on what to do when one of the pilots finds a rapidly approaching aircraft during their visual scan. As they approach the other aircraft, the instructor takes a second to assesses the situation, and thereby stops instruction. As a result, the student is confused on what to do in the deconfliction and breaks minimum separation standards.	11.03	RM 11.03
11.37	The student is performing adequately during a training maneuver. As the student approaches the instructor's limitations, the instructor provides verbal cues, but the student cannot hear the instructor. This could happen if the control path between the student and IP is severed without adequate feedback to inform the flight crew, or the ambient noise is too loud. The student does not acknowledge the control action and as a result, the aircraft enters an uncontrollable state.	11.04	RM 11.06
11.38	The student is performing adequately during a critical phase of flight (e.g., landing). On final approach the student is communicating with the instructor the process of landing. During the maneuver the student gets nervous and task saturated. Because of this, the student unable to receive instruction. As a result, the instructor cannot cue the student and the aircraft enters a hazardous state during a critical phase of flight.	11.05	RM 11.01 RM 11.07
11.39	The student is performing adequately during a critical phase of flight (e.g., landing), however as the aircraft approaches the ground the instructor provides verbal cues, but the student cannot hear the instructor. This could happen if the control path between the student and IP is severed without adequate feedback to inform the flight crew, or the ambient noise is too loud. The student does not acknowledge the control action and as a result, the aircraft enters a hazardous condition.	11.05	RM 11.06
11.40	During a training sortie, the instructor notices another aircraft in the vicinity on a course to collide. Upon noticing the impending collision, the student gets nervous and task saturated. Because of this, the student unable to receive instruction. As a result, the instructor cannot cue the student and the aircraft breaks minimum separation standards.	11.06	RM 11.01 RM 11.07
11.41	During a training sortie, the instructor notices another aircraft in the vicinity on a course to collide. The instructor provides verbal cues, but the student cannot hear the instructor. This could happen if the control path between the student and IP is severed without adequate feedback to inform the flight crew, or the ambient noise is too loud. The student does not acknowledge the control action and as a result, the aircraft breaks minimum separation standards.	11.06	RM 11.06
11.42	The student is performing training maneuvers. As part of the training the student must recover the aircraft from an uncontrolled state (e.g., stall or spin). As the flight crew initiates the maneuver, the instructor provides verbal cues, but the student is frozen from anxiety. This could happen early in the student's progression if the student has not been in such a position before. The student does not acknowledge the control action and as a result, the aircraft remains in an uncontrollable state.	11.07	RM 11.01 RM 11.07
11.43	The student is performing training maneuvers. As part of the training the student must recover the aircraft from an uncontrolled state (e.g., stall or spin). The instructor provides verbal cues, but the student does not completely understand the instruction and/or gets confused. This could happen on sorties early in the student's progression, or if the instruction is not well	11.04, 11.07	RM 11.08

	communicated and not easily understood by the student. This could also happen if the student has heard slightly different verbiage from a different instructor. The student does not acknowledge the control action and as a result, the aircraft remains in an uncontrollable state.		
11.44	The student is performing training maneuvers. As part of the training the student must recover the aircraft from an uncontrolled state (e.g., stall or spin). The instructor provides verbal cues but the verbal cues conflict with the student's mental model of the maneuver. This could happen if the instructor knows certain advanced techniques that are not regularly practiced by students. The student does not acknowledge the control action and as a result, the aircraft remains in an uncontrollable state.	11.07	RM 11.08
11.45	The student is performing adequately during a critical phase of flight (e.g., landing), however as the aircraft approaches the ground the instructor provides verbal cues, but the student is frozen from anxiety. This could happen on a high stakes sortie (a progress check) or a sortie early in the student's progression. The student does not acknowledge the control action and as a result, the aircraft enters a hazardous condition.	11.08	RM 11.01 RM 11.07
11.46	The student is performing adequately during a critical phase of flight (e.g., landing), as the aircraft approaches the ground the instructor provides verbal cues, but the student does not completely understand the instruction and gets confused. This could happen on sorties early in the student's progression, or if the instruction is not well communicated and not easily understood by the student. In high stress, the student could interpret "you are left of the runway" as instruction to bank left, when the student should bank right. The student does not acknowledge the control action and as a result, the aircraft enters a hazardous condition.	11.05, 11.08	RM 11.08
11.47	The student is performing adequately during a critical phase of flight (e.g., landing), as the aircraft approaches the ground the instructor provides verbal cues but the verbal cues conflict with the student's mental model of the phase of flight. This could happen if the instructor knows certain advanced techniques that are not regularly practiced by students. The student does not acknowledge the control action and as a result, the aircraft enters a hazardous condition.	11.08	RM 11.08
11.48	Student receives instruction during a critical phase of flight; however, the instructor's mental model of the student's control actions is flawed. The student's actual controls do not reflect what the instructor believes the student is inputting. This could happen if the instructor is receiving conflicting visual feedback in scenarios with extreme weather conditions. Control actions in high winds or turbulence may not accurately reflect the aircraft's position or attitude. As a result, the instructor gives incorrect instruction, and the student does not execute the appropriate control actions. In this scenario, there is not much that the instructor can do with conflicting feedback in extreme weather conditions. The instructor should be ready to take the aircraft and land safely.	11.08	RM 11.04
11.49	During a training sortie, the aircraft is alerted by the traffic collision avoidance system (TCAS) that another aircraft is on collision course with the training sortie. The instructor provides verbal cues, but the student is frozen from fear. The student does not acknowledge the control action and as a result, the aircraft remains on course to breach minimum separation standards.	11.09	RM 11.01 RM 11.04
11.50	During a training sortie, the aircraft is alerted by TCAS that another aircraft is on collision course with the training sortie. The instructor provides verbal cues, but the student does not completely understand the instruction and gets confused. This could happen if the instruction is given quickly due to the collision being imminent. The student does not acknowledge the control action and as a result, the aircraft remains on course to breach minimum separation standards.	11.06, 11.09	RM 11.03
11.51	During a training sortie, the aircraft is alerted by TCAS that another aircraft is on collision course with the training sortie. The instructor provides verbal cues but the verbal cues conflict with the student's mental model of aircraft deconfliction. This could happen if the aircraft on course to collide is positioned to the right off the aircraft's nose. The instructor may tell the student to	11.09	RM 11.03

	turn left to avoid the aircraft, however the student has been taught that aircraft on a head on course should each “alter its course to the right” (AETC 11-202v3, 3.24.3, [37]). The student does not acknowledge the control action and as a result, the aircraft remains on course to breach minimum separation standards.		
11.52	During a training sortie, the student has more than one issue with a specific maneuver (nose too low, too steep bank, etc.). The instructor cues the student on both issues in no specific order. As a result, the student corrects the errors in the wrong order which leads to a more hazardous state. This could happen in any maneuver that requires specific orders of recovery. For example, slow flight turns on a high aspect ratio aircraft requires a high pitch and primarily rudder movement. If student needs to nose down the aircraft and apply more rudder, applying the rudder first will induce the aircraft into a flat spin.	11.10	RM 11.03
11.53	During a training sortie, the student is in the process of recovering from a maneuver. The instructor notices another aircraft in the area and instructs the student that they need to deconflict. The student acknowledges and begins to deconflict but does not finish recovering from the maneuver. As a result, the maneuver is not recovered, and the aircraft enters a hazardous condition.	11.11, 11.13	RM 11.03
11.54	During a training sortie, the student is in the process of recovering from a maneuver. The instructor notices the student making control inputs to recover the aircraft; however, the student is missing some aspects of the recovery. Having seen the student recover the aircraft before, the instructor believes the student will make the adequate control inputs to recover the aircraft. The student does not apply the appropriate control inputs and the aircraft enters a hazardous state. The instructor gives cues too late after the student has attempted a recovery that as a result the condition worsened.	11.12	11.04
11.55	During a training sortie, the student is in the process of recovering from a maneuver. The instructor notices the student making control inputs to recover the aircraft; however, the student is missing some aspects of the recovery. Having seen the student recover the aircraft before, the instructor believes the student will make the adequate control inputs to recover the aircraft. The student does not apply the appropriate control inputs and the aircraft gets into a worse state. At this time the instructor gives cues too late after the aircraft’s condition has worsened, such that the cues are no longer relevant to the new condition of the aircraft.	11.12	RM 11.03 RM 11.04
11.56	The flight crew are in the pattern and need to deconflict with another aircraft already in the pattern. ATC tells the flight crew to deconflict with the aircraft in the vicinity, however after the instructor cues the student the instructor notices a condition that requires the student to land immediately. The student responds to the instructor’s cues out of order and as a result, the student proceeds back into the pattern where the other aircraft is without deconflicting and breaking minimum separation standards.	11.13	RM 11.03 RM 11.04
11.57	The flight crew are on final approach and the instructor tells the student that they are too high. As the student corrects their altitude, the aircraft drifts from centerline. The instructor responds by telling the student they are too far to the left. As a result, the student corrects for the centerline but disregards the altitude and is too high to land on that approach—responding to the instructor’s cues out of order. They must issue a go around.	11.13	RM 11.03
11.58	The flight crew are on their final approach and the instructor is cuing the student as they descend. As they rapidly approach the ground, the aircraft is hit with a gust of wind. As the instructor assesses the situation, he stops instruction for a second to assess. He gives instruction too late after the student need instruction. As a result, the student is confused on what to do in the critical phase of flight. As a result, the aircraft enters a hazardous condition.	11.15	RM 11.03
11.59	The flight crew are in highly active airspace, they see an aircraft close by that they need to deconflict from immediately. The instructor tells the student to bank right immediately. As they bank right, they realize they are now heading towards another	11.15	RM 11.03

	aircraft and the instructor does not have time to assess the situation and stops instruction. The instructor gives instruction too late and as a result, the aircraft breaks minimum separation.		
11.60	The flight crew are in a highly saturated airspace. The instructor is cuing the student on how to navigate the airspace when TCAS alerts the flight crew to an aircraft heading on course for collision. As a result, the instructor stops cuing too early and assumes control of the aircraft to avoid conflict.	11.16, 11.18	RM 11.03
11.61	The flight crew are in a highly saturated airspace. The instructor is cuing the student on how to navigate the airspace. The flight crew notices an aircraft on course to break minimum separation. While explaining to the student how to deconflict, the instructor takes too long to provide instruction. As a result, the flight crew break minimum separation.	11.17	RM 11.03 RM 11.08
11.62	The flight crew are training in the area. The instructor is teaching the student how to recover from a maneuver (e.g., a stall or spin). While the instructor is inducing the maneuver the instructor takes too long to explain the recovery. As a result, the flight crew does not recover in time and the aircraft becomes uncontrollable.	11.20	RM 11.08

7.1.4. Derived Recommendations

Table 7-24: Full List of Recommendations Derived from the Scenarios

RM ID	Recommended Mitigation	Related Causal Scenarios
1.01	Accurate reporting of the operations of each individual LMA (to include accident reports, operation reports, change reports, and problem reports) to the HMA is essential for the HMA to pass down accurate and pragmatic regulations and policies. This should also include certain discretionary LMA policies to avoid the HMA issuing guidance that directly conflicts with LMA guidance.	1.01, 1.05
1.02	While some regulations and policies may be generalized to all squadrons under the HMA, the HMA should be careful not to generalize squadron specific guidance to all LMA's	1.02
1.03	With the implementation of new policies, equipment, etc., the HMA should leave discretion for each LMA to implement the new changes at their own paces.	1.03, 2.03
1.04	During accident investigations, preventative measures need to be taken while analysis is being performed before continuing with normal procedures. For example, it one of the systemic factors involved with the accident related to the aircraft, the aircraft should be grounded until there is enough evidence to substantiate safe operation, or a recommendation is made to improve safe operation. The same applies to certain maneuvers, potentially hazardous environmental factors, software, or any other hardware associated with the accident.	1.04, 2.04
2.01	The LMA must communicate its operations to the HMA as feedback to limit conflicting guidance. The HMA and LMA must also be in constant communication to prevent conflicting control authority over the flight crew. The LMA must also provide timely updates to flight crews if there is any change in HMA policy. ATC must also be updated on changing HMA/LMA policies.	2.01, 2.05
2.02	The LMA must establish a culture of transparency among the Instructors and Students so that instances of conflicting mission feedback are uncommon and typically resolved in the squadron debrief.	2.02

3.01	Beyond general recommendations, STPA should be conducted for each individual airfield to identify what processes and procedures can be improved upon. Each individual ATC must have extensive contingencies in the cases of highly saturated airspaces. Beyond contingencies, ATC must have a considerable buffer of time before inclement weather moves in.	3.01-3.09
4.01	The ASEC in the next generation trainer (NGT) should feature a student override function. Where the instructor can immediately relinquish control authority from the student. This could be accomplished by disabling the student's ability to make control inputs to the ASEC. This would be a better option. This transfer of aircraft control needs to happen instantly, any latency would create hazardous conditions.	4.04, 4.07, 5.06, 5.11, 9.07, 9.10, 9.11 9.12
4.02	The ASEC in the NGT should include a level of autonomy that will recover assist the instructor in recovering from near-hazardous conditions. It is part of the instructor's responsibility to let the student approach the limits of the aircraft. Split-second decisions that can be tough for the instructor to process can be assisted through the proper use of autonomy automatically recover the aircraft. The recovery assist must come with an override in the case where it does not work as intended or is subject to a flawed control algorithm.	4.01
4.03	The ASEC in the NGT should include specific sensors and alerts that assist the instructor in assessing the training limitations. This could come in the form of Lidar detection of the distance an aircraft is away from another aircraft in formation and for detection of how close the aircraft is to the ground, or specific customizable alerts that instructors will set up before the training sortie to alert them of any areas of concern. These alerts could also help the student and reduce some of the task load of the instructor.	
4.04	The ASEC in the NGT needs to incorporate a feedback mechanism for transfer of control authority to assist with critical situations where control authority is hard to determine. This could come in the form of an auditory alert or a visual cue on the heads-up display/helmet mounted display (HUD/HMD). Another options would be to have pressure sensitive gauges on the control stick that would provide a salient alert to the other pilot if one pilot is applying pressure to the other control stick. This solution is expanded in section 8.	4.04, 9.07, 5.10
4.05	The ASEC in the NGT must provide a notification that requires acknowledgment from the pilots that the ASEC has changed modes, been bypassed for manual control, has entered an emergency state, or has made a control action without direction from either pilot.	
5.01	Manual override of the ASEC must be accessible in both cockpits. In the case where either pilot is incapacitated and impacting the augmented control, the other pilot must be able to disable augmented control. Both cockpits must be able to disable augmented control for both pilots. This would apply if the instructor cannot override the ASEC but would be better qualified to fly manual controls. The manual override must also have redundant control paths. Manual override needs to happen instantly and must not have any latency.	4.05, 5.04, 9.06
6.01	The ASEC's control algorithm as it pertains to FCS orientation must be able to sense changing conditions in the FCS and propulsive systems and adapt accordingly. The system's sensors must be able to recalibrate during operations and the ASEC must also be able to recalibrate in the cases where there is an inadequate process model. During recalibration of the ASEC, the flight controls must either	4.03, 5.01,

	be controllable by a default augmentation mode or by manual control inputs. Recalibration must give feedback to the pilots on the status of the recalibration and any issues the recalibration might have. Pilots should be notified when the recalibration is completed so that pilots do not resume augmented control without finishing recalibration. Pilots should be notified within a designated time frame if they are operating without flight augmentation.	5.05, 6.01-6.04, 6.14, 6.16, 6.17, 6.29, 9.02, 9.17, 10.08, 10.09
6.02	The process model and control algorithm in the ASEC must be able to work through interference. The aircraft subsystems must provide feedback if there is interference with the aircraft's FCS and provide feedback about the interference to the flight crew. The aircraft's FCS must also have a buffer to the registered range of motion. In the case where something damages the FCS and places them outside normal operating range, the flight crew needs to have the appropriate feedback about the updated process model and the ASEC must be able to adapt to this condition. If the control algorithm is using a TCAS software to avoid breaking minimum separation, feedback on other aircraft/objects must be interpreted and analyzed for the future position of other objects/equipment.	6.07, 6.08, 6.11, 6.15, 6.25, 6.28
6.03	The aircraft must have an operator override command in the cases where the ASEC need recalibration or the ASEC is operating on a flawed control algorithm. The ASEC must also be able to override the flight crew in cases where the flight crew are nearing the structural limits of the aircraft. Procedures must be set in place such that if the flight crew disable the limitations on control inputs, they must operate within a certain flight envelope. Then in the case of an emergency, they have adequate altitude to return to base or conduct an emergency landing within considerable margins. Pilots need to be properly trained of when and how the aircraft imposes limitations on the flight controls and how to disable those limitations in the case of an emergency. The ASEC's control algorithm must also be controllable when the process model of the aircraft is in an uncontrolled state. If the flight crew chooses to disable flight augmentation, adequate feedback must still be provided to the pilots if they are approaching the aircraft's structural limitations. The manual override should ask for confirmation from the flight crew to avoid inadvertently disabling flight control augmentation.	6.06, 6.10, 6.12, 6.13, 6.19, 6.23, 9.13, 9.14
6.04	The ASEC must receive more than one type of feedback so that it can properly assess the state and orientation of the aircraft. As part of the ASEC's control algorithm, it must be able to properly assess if the aircraft is in an uncontrollable state by assessing the control actions from the pilots and comparing the expected outcome with what is being sensed. The ASEC must also be able to detect when a feedback measurement is misleading or inaccurate based on readings from redundant or closely positioned sensors.	6.04, 6.09, 6.17, 6.29, 6.30
6.05	The ASEC's control algorithm must not account for the outcomes of a given control action and assure that the aircraft does not enter an unintended uncontrollable state. The ASEC must be able to take real-time sensor integration to effectively move the aircraft to prevent this causal scenario from happening.	6.18

6.06	The ASEC must have a seamless connection to the aircraft subsystems, and if the controlled process experiences lag, the ASEC must account for the lag in the feedback given to the operator. The ASEC must have a seamless connection to the aircraft subsystems, and if the controlled process experiences lag, the ASEC must be able to adapt real time to assess the situation and correct the uncontrollable state.	6.20, 6.21, 6.26, 6.27
6.07	The ASEC must have a set of limitations for the FCS, such that extensive FCS movement does not break the speed/altitude/g limits of the aircraft. This recommendation is implied; the fifth-generation fighters use a similar technology and thus should be incorporated into the trainer.	6.20, 6.21, 6.26, 6.30
6.08	System software designers must design each individual subsystem to be compatible with one another and the new highly automated ASEC. Software interfacing that is incompatible with each of the individual subsystems could raise many issues down the line.	6.05, 6.20, 6.24
6.09	The FCS needs to order the priority of control inputs from each of these controllers. The order of priority must also be a part of the IP and student's training. The aircraft subsystems must also order the priority of control inputs if conflicting control inputs are made. Manual flight control override from the pilots must be the top priority. When control authority is transferred, all controllers must update their process models of the system.	4.04, 4.06, 6.06, 6.13, 9.05, 9.08
7.01	The ASEC must implement a level of predictability such that it will anticipate the aircraft entering a position that could violate structural integrity of the aircraft or break the speed/altitude/g limits of the aircraft. The ASEC's process model must synthesize multiple variables (load, airspeed, attitude, control actuation, rates of change in these parameters, etc.), to estimate when the aircraft is on a trajectory to violate the limits of structural integrity. It must also incorporate a significant margin of safety such that in the case of a wind gust or turbulence, the aircraft will not violate the limits of structural integrity. After the ASEC determines that the aircraft is approaching a structural integrity violation, the pilots should be alerted with adequate time to respond	7.01, 7.02, 7.03, 7.06, 7.11, 7.13, 7.14
7.02	The ASEC must have redundant sensors ideally in different locations of the aircraft. This would allow the ASEC to limit excessive control inputs from the operator even if one of the sensors are damaged. The ASEC's control algorithm must also make decisions on the most conservative sensor in the case that one of the sensors is reporting incorrect information.	7.04 7.08
7.03	The ASEC must have the ability to change or calibrate the limitations to the FCS input in the cases of a changing mission profile (e.g., weather lowering g limits, or training near the g limit) or damage to the aircraft (also lowering g limits). The control algorithm must also have a default limit to control in the case that all feedback mechanisms are ineffective or inaccurate.	7.05, 7.06, 7.08
7.04	The ASEC must default to an emergency state, where it automatically increases control limitations on the flight crew in the case of a damage or destroyed sensor. If the aircraft has already violated its structural integrity, it will be more susceptible to damage with the same limitations. Therefore, an emergency state with tighter limits on structural integrity is necessary to protect the aircraft after it has been damaged. If the ASEC has determined that the aircraft is approaching a violation of structural integrity and the pilots have not acknowledged the condition or taken action, the ASEC must execute the appropriate control action. The ASEC must be able to	7.12, 9.15

	determine when the structural integrity of the aircraft has been violated. In the case where the ASEC does not have adequate feedback to determine that the structural integrity of the aircraft has been violated, the flight crew must be able to initiate the emergency state. The emergency state must be able to alert the flight crew of the tighter flight envelope with both augmented flight controls and manual flight controls.	
7.05	The ASEC needs to evaluate the condition of the aircraft in real time and assess the status of the aircraft. Based on the assessment of the aircraft, it must draw new limits based off the severity of how far the limits have been broken	7.12, 7.14
7.06	The flight crew must be able override the ASEC in the case where the flight crew will enter a hazardous situation if the ASEC limits their control inputs. If the aircraft is on course to crash or collide with another aircraft, overriding the ASEC and violating structural integrity is better than crashing. This may also be designed into the ASEC to recognize minimum separation as a higher priority hazard as compared to violating structural integrity.	7.07, 7.09, 7.10
8.01	Multiple sensors must be incorporated into the cockpit such that neither the flight crew nor the hardware in the aircraft are negatively impacted. Ideally the sensors will be placed as close as possible to vital systems and the flight crew, however if that is not pragmatic the sensors need to encompass both sides or surround of the vital system or pilot. The ASEC must be able to identify whether a sensor is faulty and exclude the outlier or ere on the side of caution and take the most conservative reading. Redundant sensors would help with this issue.	6
8.02	The aircraft subsystems must have a relevant margin of safety to the internal climate controls to ensure that the internal climate does not damage the hardware or negatively affects the flight crew's performance.	2
9.01	The aircraft's flight controls must be designed to operate similarly to manual flight controls. The manual flight controls must not be a far cry from the augmented flight controls so that the flight crew can adapt during emergencies where flight control augmentation need to be disabled. Instructors and students should also be trained on manual control operation.	9.01, 10.01, 10.05, 10.06
9.02	The pilots must be able to independently disable certain features of the ASEC without affecting the functionality of others. Certain functions may be deficient, but other functional features may be important to the flight crew. The ASEC should also incorporate a master switch that disables all ASEC functionality and augmentation. Flight crews should be trained to fly when certain features and modes are disabled from the ASEC.	9.03
9.03	The flight crew must be notified if the ASEC and flight augmentation is shut down for any reason. This could be a result of certain conditions that force the ASEC to shut down, violating the structural integrity of the aircraft forcing the ASEC to shut down, or any other case that would force the aircraft into manual control.	9.09
9.04	The flight crew must not be able to override of augmented flight controls from the ASEC or revert from manual flight controls to augmented flight controls below a specified altitude (e.g., pattern altitude) to prevent mental model issues during critical phases of flight.	9.16

10.01	The NGT's design should incorporate sensor that can monitor both pilots' biometric data. This may include heartrate and blood pressure so that the aircraft can alert the other pilot and engage appropriate emergency controls in the scenario that the pilot is incapacitated or has lost consciousness.	
10.02	The student must be able to access the manual override if the instructor has overridden student command over the ASEC. The aircraft need logic outlining the priority of control of all the controllers in the aircraft.	10.02
10.03	The ASEC and flight augmentation must be designed to self-regulate and recognize when it is not functioning currently. This information should be immediately communicated to both pilots in the case that the ASEC is dysfunctional. Other methods of feedback should be implemented to determine if the ASEC and flight augmentation is functioning as intended.	10.07
11.01	Instruction must be communicated clearly with the student at the student's level of proficiency. Because there is no time for hesitation in critical phases of flight, it is in the instructor's best interest to seize control of the aircraft at the earliest sign of the student's hesitation, confusion, or anxiety. The difficulty in this decision is knowing when the student is exhibiting hesitation, confusion, or anxiety. To assist in these safety critical decisions, the instructor can build SA on the student's habits and tendencies by gauging their responses in low-stakes scenarios. The instructor should gauge the student's propensity to respond under stress during emergency procedures (EP) practice before the flight, as well as during maneuvers in the area. The student's responses to the scenarios given in the EP practice can help the instructor gauge how the student will reason through live scenarios. It may be telling of the student's ability to handle stress if the student is having trouble responding to the EP. The instructor should also gauge the student's responses to instruction on other area maneuvers during the flight. These responses include but are not limited to • Affirmations—how fast the student affirms instruction, the verbiage used, the tone of voice used, how fast the student acknowledges the instruction, etc. • How quickly the student can apply corrections after receiving instruction. • How the student reacts to time-sensitive corrections. • How the student resolves confusion from instruction. • How the student responds to multiple corrections. • How the student responds to stress. For the most part, the benefit to EP practice and area maneuvering is that neither practice is time sensitive. In EP practice and area maneuvering, the student has time to listen, clarify, comprehend, and apply any instruction from the IP. Observing the student's natural tendencies and style of communication helps build the IP's situational awareness of the student which can be integral when time is not a luxury. The student's habits and tendencies observed by the IP during low-stakes situations can be applied during high stakes scenarios such as safety critical phases of flight, aircraft deconfliction, or other demanding maneuvers (such as formation flying). Because each student will likely handle stress differently and communicate in different ways, it is important that IP's treat every student independently and do not generalize instruction techniques across all students.	11.01, 11.02, 11.12, 11.21, 11.24 11.25, 11.26, 11.34, 11.38, 11.40, 11.42, 11.44, 11.45

11.02	When students begin the process of program elimination, nerves will already be a relevant factor in their flying ability. For this reason, it is essential that the IP that the student flies with already has an ample amount of situational awareness built. The IP should be someone that the student has flown with before and preferably is more comfortable with. Regardless, the IP who is flying the elimination/final progress check should also fly the preceding sorties or at least one preceding sortie to build SA on the student's behavioral tendencies. If the IP walks into the sortie without any grasp of how the student communicates or handles stress, the likelihood of all the causal scenarios from RM ID 11.01 increases as well as the likelihood of causal scenarios related to this recommendation.	11.01, 11.02, 11.14
11.03	When there is more than one correction needed to be addressed by the student, the instructor must make it clear to the student the order to which the corrections must be made. Some maneuvers will have checklists to aid in these orders, instructors must make this clear for all maneuvers to avoid applying corrections in the wrong order. If there is no order specified in the appropriate 11-series publications, the instructor should clarify the order of control actions required to recover the aircraft in the shortest period and restore positive control. The instructor should also assure that the student is aware of proper collision avoidance practices and aircraft right of way. **<u>If there is more than one correction needed during a critical phase of flight, or the situation is time sensitive, the instructor should assume control authority</u>**.	4.09, 11.27, 11.36, 11.50, 11.51, 11.52, 11.53, 11.55, 11.56, 11.57 11.58, 11.59
11.04	Instructors must constantly work to update their own mental models of the student's capabilities. This begins with previous instructors providing detailed notes on the student's behavioral tendencies on previous sorties and where the student seemed to be the most stressed (RM 11.01). Instructors must also work to align the student's incomplete mental models with their own mental models. Students should be encouraged to constantly communicate their mental models to instructors so that the instructors know where to focus their instruction. This would include updating any of the student's mental models and interpretation of instruction as they change over time. Instructors can ask leading questions to help fill in any gaps, while students can report their understanding of other controllers. Examples of this can include: • ATC and HMA guidance o Instructor: "Could you echo what ATC meant by that?" o Student: "As clarification, my interpretation of ATC instruction was ____"	4.01, 5.03, 5.07, 5.08, 11.03, 11.04, 11.06, 11.07, 11.08, 11.09, 11.13, 11.16, 11.17, 11.19,

	• Weather and the environment o Instructor: “What are you going to change about our approach with reported wind shear?” o Student: “Now that it has started to rain, I will change_____” • Other aircraft in the vicinity o Instructor: “Do you know if there is another aircraft in the area?” o Student: “As we approach the pattern, I remember hearing another aircraft get cleared for takeoff around a minute ago, I’m looking for where the aircraft is now.” • The ASEC and the current mode of the ASEC o Instructor: “Could you switch to the mode that displays ___?” o Student: “I’m switching to this mode which changes _____ about the flight controls?” • The aircraft subsystems (flight controls, propulsion, communications, navigation, environmental systems, etc.) o Instructor: “Please communicate with me your intended flight controls as we begin our approach” o Student: “I’m inputting right stick because we are left of centerline” • The instructor o Student: “We are approaching your limits on this maneuver” The student should also acknowledge how new information changes the interpretation of these mental models. New information can include: • Notices to Airmen (NOTAMs) and Special Interest Items (SIIs) • Changes to publications or manuals • ATC and HMA guidance during the sortie • Weather recalls • Declaration of emergencies Whenever the instructor notices a gap in the student’s mental model, the instructor must act to fill in the incomplete information in the student’s mental model in a timely manner. The student and the instructor should always aim to increase situational awareness, and the instructor should aim to help the student reason through changes in the environment. The benefit to ground ops, briefing, and debriefing is that the instructors can take time to fill in the gaps of their mental models of the students.	11.20, 11.28-11.33, 11.48, 11.49, 11.54, 11.55, 11.56
11.05	Differences in flying qualities should be emphasized upon transitioning between different phases of pilot training. Instructor should be aware of habits that have been developed in previous aircraft and what scenarios those habits may manifest in current training. For example, the rudder usage in the T-6 for centerline control may manifest in the next phase of training (T-38 or T-1).	11,05, 11.18

11.06	The next generation trainer should be designed to address many of the shortcomings of the T-38 ant the T-6. All controls should be accessible in both cockpits. This is critical for feedback to the other pilot and in the case that one of the pilots is incapacitated, there will be no issues actuating any controls. Feedback about the status of all controls needs to be routed to both cockpits. These include: • T-6 FCP Exclusive Controls: Activation of the auxiliary battery, Manual fuel balance left/right (L/R) switch, environmental control system controls, emergency gear extension, power management unit, firewall shutoff handle, gust lock, bleed air inflow, on board oxygen generating system, defog operation, external light operations • T-6 RCP Exclusive Controls: Interseat sequencing system, interphone hot/cold mic switch • T-38 FCP Exclusive Controls: engine start or shut down, crossbreed, boost pump one/off, environmental controls, pitot heating, and landing light • Tandem seat cockpits also have the unique challenge of no visual feedback between the two cockpits which is especially difficult for transfer of aircraft control. In critical phases of flight, there is not enough time for both pilots to verbally acknowledge control authority changes. The new design of the next generation trainer should incorporate an alternate method of feedback to indicate transfer of control authority. This could be a button or a trigger on the control stick that when pressed, sends an alert to the other cockpit that the other pilot is assuming control of the aircraft. This would help clarify when students need to relinquish control of the aircraft during critical phases of flight. An alternative option would be a complete override of the student cockpit. This may be possible with the addition of the ASEC; however, a button or trigger alert would be adequate to provide the necessary feedback for the student to relinquish control. This option is further explored in Chapter 8.	4.02, 4.06, 5.10, 11.10, 11.11, 11.13, 11.23, 11.24, 11.26, 11.37, 11.39, 11.41
11.07	The next generation trainer should incorporate a display that allows for the instructor to monitor the student's biometric data. At a minimum, the instructor being able to see the student's heartrate would provide valuable feedback to the condition of the student. If the student's heart rate gets dangerously high or low, the instructor could pre-maturely assume control of the aircraft before a hazardous situation develops. A proposed solution is explored in Chapter 8.	4.02, 11.12, 11.23, 11.24, 11.25, 11.37, 11.38, 11.40, 11.42, 11.44
11.08	HMAs and LMAs should require continuation training sorties regularly between instructors of different experience levels. The goal of these sorties would be to standardize practices, limits, and general instruction and communication techniques across all instructors.	4.07, 4.11, 4.13, 5.09, 11.15,

		11.43, 11.44, 11.46, 11.47, 11.61, 11.62

8. Appendix B: Human Factors Analysis

Stick control between students and pilots in tandem seated trainers provides a unique challenge to the flight crew as there is no visual feedback between the two seats. As of now, transfer of aircraft control is a verbal and tactile confirmation between the instructor and the student. When the student needs correction in a critical phase of flight, the verbal and tactile affirmation from the instructor is significantly more brief or completely non-existent depending on the criticality of the situation. Often, this transition is abrupt and confusing, and happens during critical phases of flight (e.g., takeoff and landing) when risk is the highest. This hands down mode is the most dangerous stage of flying but is also one of the most critical phases of learning for the student. For this reason, instructors often push the limits of safety when taking the aircraft. This analysis will look towards a solution to make the transfer of control authority in these critical phases of flight less dangerous and clearer to the flight crew.

This analysis approach will consist of a human factors analysis of the transfer of aircraft control system in single seat jet trainers. The key stakeholders that will use the system are:

1. Instructor Pilots: Instructors often take risks in critical phases of flight to facilitate the most conducive learning environment. The goal within the problem space would be to make a quick and salient transfer of aircraft control for the instructor to take the aircraft in the critical phases of flight.
2. Student Pilots: In a similar fashion, when students are terrified behind the stick, the stress might make it hard to concentrate on flying. Students may fixate on flying such that it is difficult to hear and feel when the instructor takes the stick. The goal would be to have a more salient transfer of control authority so that there would be no confusion going forward.
3. Higher Mission Authority (HMA): HMA oversees all UPT operations in the USAF and head all policy changes pertaining to pilot training. This will include the supervisory members of HMA overseeing flying operations.

Table 8-1: Persona for the Instructor Pilot

Instructor Pilot exemplar Personal	
User Goals	● Mission planning and preflight ● Ensure safety of flight during the training sortie ● Properly debrief the student after the flight ● Instruct the student on flying techniques ● Maintain situational awareness and accurate mental models in flight ● Ensure student has accurate mental models ● Clearly communicate with ATC and the student ● Stay up to date on changing squadron policies
Key Information Requirements	● Instructors have each been traditionally trained in the aircraft they are instructing ● Instructors go through additional training referred to as Pilot Instructor Training (PIT) where they learn techniques to be instructors ● Additional qualifications exist for certain instructors who qualify based on their hours flying and number of instructional sorties.

	● There exist instructors for different stages of training (e.g., the T-6, T-38, B course—specializing in each specific airframe, test pilot school, weapons school, etc.)
Pain Points	● Each student has their own individual strengths and weaknesses, and the instructor needs to be able to adapt to them on the fly. ● Each student communicates differently and is receptive to different styles of training. ● Instructors never have a complete mental model of the student's capabilities ● Transfer of aircraft control becomes risky as the altitude decreases
Outside Influences	● The demand for military and commercial pilots is at an all-time high ● Instructors are often overworked trying to meet this demand with training ● Pilot training is evolving, and instructors are forced to adapt and keep up to date with the constant changes. ● Instructor may push the limits of training to try and get students through the program

8.1. Proposed Solution:

The proposed solution is an improved transfer of aircraft control mechanism with improved feedback, integration into helmet mounted displays (HMD's) and supervisory capability to the HMA.

8.2. Use Case Definition:

Table 8-2: Five Main Use Cases

Use Case and Users Impacted	Description
Landing Instructor Pilot Intervention **All stakeholders impacted**	Use case begins when the student if off centerline and the Instructor Pilot needs to decide whether verbal instruction or taking control of the aircraft is appropriate. As the altitude decreases, the risk increases as the time to make a critical lifesaving decision decrease. The use case concludes when the instructor makes the decision to take control of the aircraft.
Takeoff Instructor Pilot Intervention **All stakeholders impacted**	Use case begins when the flight crew gets clearance from ATC for takeoff on the runway. The aircraft accelerates down the runway and if the student deviates from centerline or pitches up at an incorrect time, the instructor will need to make a critical decision to take control of the aircraft. As the speed Increases, the risk increases as the time to make critical decisions decrease. The use case concludes when the instructor makes the decision to take control of the aircraft.
Formation flying **All stakeholders impacted**	Use case begins when the flight crew begins a formation flying maneuver with a lead aircraft. With the student in control of the aircraft, the flight crew will slowly converge on the other aircraft getting as close as possible (fingertip formation). As the distance between the two aircraft decreases, the risk increases as the time to make a critical lifesaving decision decrease. The use case

	concludes when the instructor makes the decision to take control or formation flying is successfully performed without intervention.
Recovering the Aircraft from an Uncontrollable State (IP initiated) **All stakeholders impacted**	Use case begins where the instructor initiates a planned maneuver where the student needs to recover the aircraft from an uncontrollable state that the instructor initiated. As the instructor induces the uncontrollable state (e.g., a stall or upright spin), the instructor makes the decision that the aircraft is in in an appropriate state (within the limits of training) and transfers control to the student. As the altitude decreases and the scenario becomes dangerous, the instructor needs to make another decision whether to retain control from the student. The use case concludes when the instructor makes the decision to take control of the aircraft or not.
Recovering the Aircraft from an Uncontrollable State (SP initiated) **All stakeholders impacted**	Use case begins where the initiates an unplanned maneuver where the student needs to recover the aircraft from an uncontrollable state that the student unintentionally initiated. The student induces the uncontrollable state (e.g., a stall or upright spin) by incorrectly inputting the appropriate flight controls for a maneuver. The instructor assesses the situation and recognizes the appropriate controls to recover an aircraft. The first decision the instructor makes is whether to take the aircraft from the student upon the onset of the uncontrollable state. As the altitude decreases and the scenario becomes dangerous, the instructor needs to make another decision whether to retain control from the student. The use case concludes when the instructor makes the decision to take control of the aircraft or not.

All the use cases listed above incorporate the following theories:

- Sensory Processing Limitations
- Contrast sensitivity
- Depth perception
- Visual search and detection
- Temporal communication
- Tactile and haptic feedback
- Selective attention
- Working memory
- Situational awareness
- Problem solving and mental effort
- Task management and interruptions Decision making and bias
- SKR based behavior
- Recognition primed decision making
- Displays (heads up displays, head mounted displays)
- Control and time delays
- Environmental stress, psychological stress, level of arousal, life stress, workload overload, sleep deprivation and performance effects
- Safety and accident prevention, hazard analysis, human error, safety management, and risk taking

8.3. Use Case Deep Dive:

Referencing the preface, a combination of use case 1 (Landing IP Intervention) and use case 3 (Formation Flying) will be used for the potential solution particularly. The T-38 Accident referenced in Section 4 happened during a formation landing.

The SIB report references *AE105 Breakdown in Visual Scan* as a human factors' contribution to the accident [26] [9]. The SIB references that this was a factor because an individual failed to effectively execute visual scan patterns. In the 2nd Edition of *An Introduction to Human Factors Engineering* by Wickens et al., the topic of visual search and detection is discussed in Chapter 4: Visual Sensory Systems [38]. In this incident, the visual search occurred about the formation aspect of the landing. The eyes need to navigate the useful field of vision (UFOV) to detect and confirm that a signal is present. In a formation landing, the pilot must visually scan the cues for both a typical landing as well as formation flying. During a landing, the pilot must note the positioning, the altitude, the airspeed, as well as the flight controls while during formation flying the pilot must also note the positioning relative to the lead aircraft, the flight controls of their own aircraft, as well as the flight controls of the other aircraft.

This ties into situational awareness, task management, and workload also discussed by Wickens et al. A key aspect of flying is maintaining a high degree of situational awareness and being able to manage many tasks at once. IP's must manage all the previously discussed cues in visual scan, on top of instructing the student which adds to the workload and reduces the situational awareness of the IP. A common reason why IP's take control of the aircraft from students is task over-saturation of the student who does not have enough working memory to manage all the flight controls.

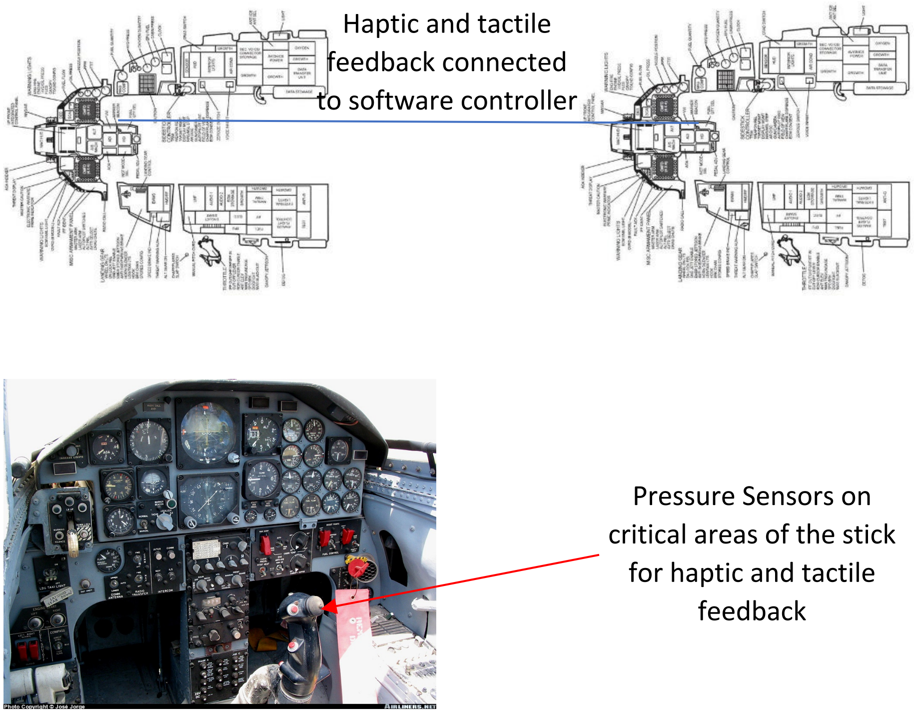
As a result of this accident, the USAF no longer conducts formation landings. Formation landings do not really serve too much of a purpose in combat operations and for that reason were removed from operations. In pilot training, there is a large emphasis on studying general knowledge and emergency procedures. This is because when a student placing mental effort trying to navigate through the correct procedure, it is taking away from their situational awareness and visual scan. This is emphasized to the students, and notably the students who have spent more time studying general knowledge and emergency procedures perform better in the cockpit than their peers who have not.

Instructors are trained to notice common mistakes of students, but generally they are still highly task saturated. Instructors must regularly make judgement calls based on the information available to them to assess the safety of the flight. On top of this, instructors of the T-38 cannot see exactly what the other pilot is doing with their flight controls. The aircraft is structured front so that one seat is in front of the other, so the instructor must heavily rely on SKR based decision making and recognition primed decision making to make their assessments without visually seeing exactly what is going on in the other seat. Other than noticing common trends in students and assuring that each instructor is highly trained in their craft, there has not been any significant solution to address the high task saturation of fighter jet trainers.

Although there are no studies specifically targeted towards fighter jet training instructor pilots, there is a wealth of literature on task management and crew coordination for aviation. Notably, a Military Medicine paper on found that task saturation commonly was associated with poor teamwork, communications, and mutual performance monitoring [39]. As it relates to flight instruction, teamwork, communication, and mutual performance monitoring are essential to safe operation. Task saturation issues between a student and instructor can be crippling to safe operation. If a student is task saturated, communication breaks down. Tasks are then offloaded onto the instructor who then needs to manage instruction and aircraft control. Because students may not know how to communicate effectively, instructors must ask the right questions and make assumptions about the student's capabilities during times of high stress.

8.4. Proposed Solution

The proposed is an integrated system that uses haptic and tactile sensors in the control stick to relay non-verbal communication to the instructor. The sensors would be ergonomically placed in the places where pressure is applied the most during control.



Haptic and tactile feedback connected to software controller

Pressure Sensors on critical areas of the stick for haptic and tactile feedback

Figure 8-1: Proposed Solution Infrastructure

The tactile and haptic feedback is relayed to the student and instructor's Helmet Mounted Display:

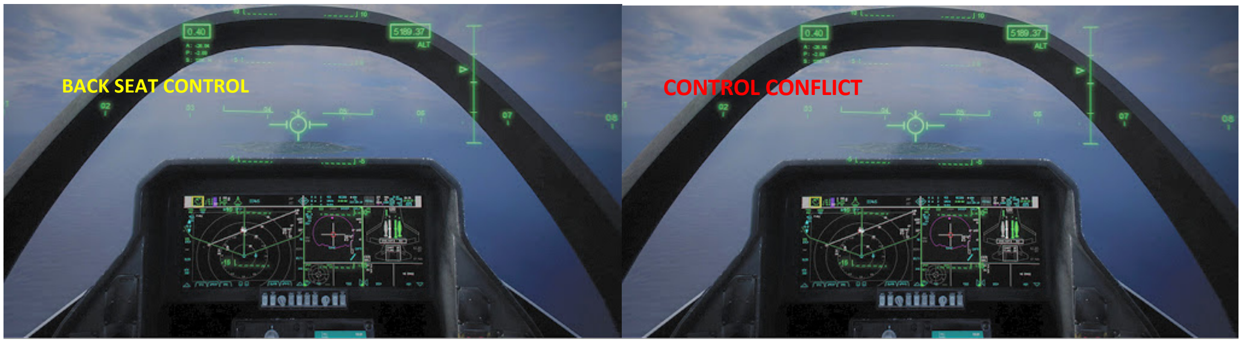


Figure 8-2: Helmet Mounted Display Visualization

The sensors would identify who is applying pressure to the control stick and relay that information to the HUD/HMD of both seats for who is hands-on with the control stick. The system would flash red if there is a conflict in control authority (or no control authority) and sound a small salient alarm.

The last element of the prototyped system will be a vitals display connected to a small wearable watch (e.g., apple watch or otherwise) that can track the student's heart rate and relay that feedback to the instructor. This would allow the instructor to make more educated decisions on when to take the aircraft controls during high stress situations.

Figure 8-3: HUD/HMD Instructor Display of Student Vitals

Table 8-3: System Function and Usability (definitions from Wickens et al. [38])

Function and Usability Categories	Proposed Solution
Learnability: The system should be easy to learn so that the user can rapidly start getting work done	The system requires little to no learning. All is self-explanatory on the HUD/HMD
Efficiency: The system should be efficient to use so that once the user has learned the system, a high level of productivity is possible	The system would relay instant feedback to the instructor
Memorability: The system should be easy to remember so that the casual user is able to return to the system after some period of not having used it, without having to learn everything all over again	The system is self-explanatory and would be easy to remember for future use
Errors: The system should have a low error rate so that users make few errors during the use of the system and so that if they do make errors, they can easily recover from them. Further catastrophic errors must not occur.	After flight testing and the optimal level of calibration is found for the pressure sensors, the system would be accurate to the degree of the pressure sensors.
Satisfaction: The system should be pleasant to use so that users are subjectively satisfied when using it; they like it	The system would add minimal clutter to the pilot's experience and provide a redundant source of communication for transfer of aircraft control

Table 8-4 is an example of how the system would work in a common flight training scenario.

Table 8-4: Task Analysis in a Scenario

Task Step	Sub-Steps
1. Flight Crew enter landing sequence with student in control	A. Student has control of the aircraft B. Instructor is giving proper cues towards landing.
2. As altitude decreases, instructor notices the student is approaching limits and their heart rate is decreasing (120 beats per minute)	A. Instructor notices the student is off center and is getting slow and provides the appropriate verbal instruction.
3. On the round out, student's heart rate jumps (150 beats per minute) and stops communication with the instructor.	A. Instructor is given seconds to act on the situation. B. Student has frozen up from stress and is no longer communicating.
4. The instructor assesses the student's high heart rate and lack of communication and take control of the aircraft.	A. Instructor takes the aircraft controls and activates the pressure sensors. B. Feedback in the form of "CONTROL CONFLICT" is displayed on the student's HUD/HMD and a salient alert is sounded.
5. Student sees "CONTROL CONFLICT" Indication and releases the stick	A. The student releases the controls.
6. Instructor lands the aircraft safely	N/A

8.5. System Evaluation Plan

After appropriate flight tests are conducted, an experimental evaluation would be used to evaluate the effectiveness of the system. The sample population would be a single training squadron chosen to implement the system such that could be directly compared to other bases. The squadron would implement the new system and conduct standard training operations. All training sorties involve takeoff, landing, and a pattern (e.g., critical phases of flight), which would allow the flight crews to complete up to three use case scenarios in a single sortie.

The initial results would be based off the subjective appraisal of the instructors. Instructors would be surveyed on how well the system operates, if the instructors find it useful, what improvements could be made, was the system easy to use, etc. The results of the assessment would help redefine the calibration of the system.

After implementation, results could be compared directly over a period where accident rates in pilot training are compared before and after the implementation of the technology. The system would be evaluated in 1-, 5-, and 10-year increments where the mishaps in training are compared year to year as a percentage of mishaps to training sorties. Furthermore, any subsequent accidents and incidents should be independently reviewed by a CAST analysis.

9. Bibliography

[1] Office of the Under Secretary of Defense for Personnel and Readiness, Report to Congressional Armed Services Committees on Initiatives for Mitigating Military Pilot Shortfalls, The Department of Defense, 2019.

[2] H. Wilson and D. Goldfein, "USAF Posture Statement Fiscal Year 2020," 2020.

[3] A. Khan, M. Sarwar, R. Hamid and R. U. H. Wani, "Root Cause Analysis".

[4] M. Latino, R. Latino and K. Latino, Root Cause Analysis | Improving Performance for Bottom-Line Results, vol. Fifth Edition, Boca Raton, FL: CRC Press, 2020, p. 24.

[5] Office of Nuclear Safety Policy and Standards, "Root Cause Analysis Guidance Document," Washington, D.C., 1992.

[6] W. DeCamp and K. Herskovitz, "5 - The Theories of Accident Causation," in *Security Supervision and Management*, Butterworth-Heinemann, 2015, pp. 71-78.

[7] N. Leveson, Engineering a Safer World | Systems Thinking Applied to Safety, Cambridge, MA: The MIT Press, 2011, pp. 6, 34-47, 273-279.

[8] P. Wannaz, "Safety-II: the brand new concept of the "complex" Swiss Cheese Model 2/2," CEFA Aviation, 9 April 2019. [Online]. Available: https://www.cefa-aviation.com/safety2-swiss-cheese-model-lessons-learned/. [Accessed 2 April 2022].

[9] Air Force Safety Center, "Safety Investigations and Reports," 2021.

[10] Air Mobility Command, "Aviation Safety Investigations and Reports," 2020.

[11] K. Lampela, "Air Force Safety Investigation Board Presidents: An Alternative Manning Source," Air Command and Staff College, 1997.

[12] R. Stewart, "USAF Aircraft Mishap Safety Investigation Boards | Are the Results Getting Published?," Air Command and Staff College, 1997.

[13] A. D. Hall and R. E. Fagen, "Definition of System," in *Modern Systems Reserach for the Behavioral Scientist*, Chicago, Aldine, 1968.

[14] G. M. Weinberg, "Breaking Down Observations," in *An Introduction to Systems Thinking*, New York, Dorset House Publishing, 2001.

[15] M. Şengöz and M. K. Topcu, "An Evaluation on F-35 Joint Strike Fighter: Turkish Perspective," in *The 11th International Scientific Conference "Defense Resources Mangement" in the 21st Century*, Braşov, 2016.

[16] N. G. Leveson, "Human Error and Risk," in *Safeware*, Addison-Wesley, 2020.

[17] Department of Defense, "Standard Practice System Safety MIL-STD-882E," 2012.

[18] C. A. Ericson, Hazard Analysis Techniques for System Safety, Fredericksburg: John Wiley & Sons, 2005, pp. 31-53, 183-220, 223-233, 235-258, 261-269, 271-284.

[19] Ford Motor Company, Failure Mode and Effects Analysis Handbook (with Robustness Linkages), Dearborn, MI: Ford Motor Company, 2011.

[20] Air Education and Training Command, "Flying Operations | T-6 Primary Flying," HQ AETC/A3VU.

[21] Air Force Global Strike Command, "Flying Operations | Cockpit/Crew Resource Management Program," 2021.

[22] 14th Flying Training Wing, "T-6 In-Flight Guide," Columbus AFB, 2021.

[23] Air Force Global Strike Command, "CRM Skills Criteria Training/Evaluation Form".

[24] N. Leveson, "CAST Handbook: How to Learn More from Incidents and Accidents," 2019.

[25] "Aerospace and Ground Accident Investigations," 2019.

[26] E. Pettus, "T-38C, T/N 65-0395 & T-38C, T/N 67-4950," Vance Air Force Base, 2019.

[27] Air Education and Training Command, "Flying Operations | T-38 Flying Fundamentals".

[28] N. Leveson and J. Thomas, STPA Handbook, 2018.

[29] D. A. Abbink, T. Carlson, M. Mulder, J. C. F. de Winter, F. Aminravan, T. L. Gibo and E. R. Boer, "A Topology of Shared Control Systems - Finding Common Ground in Diversity," 2017.

[30] U.S. Bureau of Labor Statistics, "Occupational Outlook Handbook | Air Traffic Controller," 22 October 2021. [Online]. Available: https://www.bls.gov/ooh/transportation-and-material-moving/air-traffic-controllers.htm.

[31] T. Talay, "Introduction to the Aerodynamics of Flight," Langley Research Center, 1975.

[32] T. Yechout, Introduction to Aircraft Flight Mechanics: Performance, Static Stability, Dynamic Stability, Classic Feedback Control, and State-Space Foundations, vol. 2nd Revised Edition, AIAA.

[33] United States Air Force, "T-6A Texan II," [Online]. Available: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104548/t-6a-texan-ii/.

[34] 560th Flying Training Wing, [Online]. Available: https://nara.getarchive.net/media/air-to-air-left-side-view-of-an-usaf-t-38-talon-aircraft-from-560th-flying-e9f6e2.

[35] Department of Transportation Federal Aviation Administration, "Airplane Flying Handbook," Flight Standards Service, Oklahoma City, 2021.

[36] D. Gregorian and S. Yoo, "A System-Theoretic Approach to Risk Analysis," MIT, 2021.

[37] Air Education and Training Command, "Flying Operations".

[38] C. D. Wickens, J. D. Lee, Y. Liu and S. E. Gordon Becker, An Introduction to Human Factors Engineering, Upper Saddle River: Pearson Education International, 2004, pp. 61-119.

[39] B. Davis, K. Welch, S. Walsh-Hart, D. Hanseman, M. Petro, T. Gerlach, W. Dorlac, J. Collins and T. Pritts, "Effective Teamwork and Communication Mitigate Tast Saturation in Simulated Critical Care Air Transport Team Missions," Military Medicine, 2014.