Systems-Theoretic Process Analysis of Small Unmanned Aerial System Use at Edwards Air Force Base

by

Sarah A. Folse

B.S. Aeronautical Engineering
United States Air Force Academy, 2015

B.S. Mathematics
United States Air Force Academy, 2015

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

Master of Science in Aeronautics and Astronautics
at the
Massachusetts Institute of Technology

June 2017

Signature of Author _____

Sarah Folse
Department of Aeronautics and Astronautics
May 25, 2017

Certified by _____

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

Accepted by _____

Youssef M. Marzouk
Associate Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

DISCLAIMER

The views expressed in this document are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense or the U.S. Government.

ACKNOWLEDGEMENTS

None of what I have done in my 23 years on this Earth has been done solely on my own. Everything I do is the work of God, and I have endeavored to live my life in a way that reflects that.

"Finally, brothers and sisters, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable—if anything is excellent or praiseworthy—think about such things. Whatever you have learned or received or heard from me, or seen in me—put it into practice. And the God of peace will be with you." Phil 4:8-9

To my parents, I owe you both for setting me up to be successful in life. Thank you for always providing encouragement and support, and never doubting that I can accomplish my goals – even when I doubted myself. You both have always been there to answer my questions, listen to my rants, and be my rock throughout all of the ups and downs. None of my accomplishments would have been possible without you.

Professor Leveson, thank you for taking the chance on a second year grad student who needed to move to a new lab. The research was meaningful and will have applications throughout my career, no matter what assignments I may receive. You pushed me to think about engineering in a new way, and given me the tools to succeed in my career, whatever it may be. At the heart of it all, you took a chance on me and for that I will always be grateful.

Pancho, Mirf, Matrix, and everyone at the ET CTF and USAF TPS, this thesis would not have been possible without your help and guidance. You answered all of the "stupid" questions that I had, gave me an operational perspective on things, and gave me all of the career advice that you could think of. You took the opportunity not only to work with me on this research, but also to set yourself up as mentors.

Systems-Theoretic Process Analysis of Small Unmanned Aerial System Use at Edwards Air Force Base

by

Sarah A. Folse

Submitted to the Department of Aeronautics and Astronautics
on May 25, 2017 in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Aeronautics and Astronautics

ABSTRACT

As the military moves forward with unmanned aerial vehicles, Edwards AFB must adjust its operations in order to accommodate testing these UASs in all stages of development. With a focus on Small UAS, this thesis applied Nancy Leveson's Systems-Theoretic Process Analysis to the problem to develop system requirements and recommendations.

Several portions of both the safety review process and flight operations were highlighted as a result of this analysis. Key features were identified and discussed. 74 potential unsafe control actions were found, along with numerous causal scenarios. 141 safety recommendations were made to mitigate potential causes of the UCAs.

After comparing this analysis to the existing guidance in AFTCI 91-202 and EAFBI 13-100, nine action items were identified that will enhance the safety of the system as it currently exists.

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

TABLE OF CONTENTS

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Recently, the United States Air Force (USAF) has shifted some of its focus towards the development of small unmanned aerial systems (SUAS). This shift increases the complexity of any airspace in which these SUAS operate; as such, a hazard analysis must be conducted in order to ensure that safe operations are maintained. Since Edwards Air Force Base (AFB) is host to the new Emerging Technologies Combined Test Force (CTF) that is tasked with the development and testing of new SUAS, the Edwards airspace is the subject of this thesis. Specifically, this thesis applies Nancy Leveson's Systems-Theoretic Process Analysis (STPA) method of hazard analysis to the use of SUAS in the Edwards AFB airspace.

MOTIVATION

Edwards AFB is responsible for a unique section of airspace, which must safely accommodate a diverse selection of aircraft in many different stages of development. As unmanned aerial systems (UAS) become more prevalent, this airspace must adapt in order to safely include the testing and operation of UAS in conjunction with the existing air traffic.

UAS in general are not able to follow one of the fundamental principles of the Edwards airspace: that "vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft (1)." This regulation is impossible for a UAS operator to accomplish when the unmanned aerial vehicle (UAV) that they are controlling is not within sight. For this reason, other controls must be in place in order to ensure that the UAV does not collide with other aircraft in the area.

Small UAS (SUAS), such as a RQ-11 Raven, present further challenges as they are operated at low altitudes and are often unequipped with communications equipment that is present on their larger brethren. While large UAVs, such as a MQ-1 Predator or a RQ-4 Global Hawk, are equipped with an Automatic Dependent Surveillance-Broadcast (ADS-B) transponder and have a radar return signature large enough to be visible, a small UAV (SUAV) may not carry an ADS-B transponder and can be confused with a bird or airborne debris on a radar screen. In recognition of these differences, the USAF has activated a new unit, called the Emerging Technologies CTF that focuses specifically on SUAS.

While Edwards Air Traffic Control (ATC) has developed procedures to handle large UASs, these procedures do not necessarily translate to the SUASs that will soon be operating in the airspace. With this new CTF beginning to conduct operations, the complexity of the Edwards ATC system increases significantly. This thesis applies STPA to the Edwards ATC system; the focus will be on modifications necessary to safely integrate SUAS operations into the existing infrastructure.

OBJECTIVE

The objective of this thesis is twofold; first, this thesis applies STPA to the current operations of the Edwards ATC system. This allows existing safety concerns to be addressed independently of the new SUAS operations. Second, STPA is used to generate recommendations on how SUAS can safely be integrated into the Edwards airspace.

ORGANIZATION

Chapter 2 examines several hazard analysis techniques to explain why STPA is used here. A detailed explanation of the STPA process is provided. A similar analysis that has been conducted on the Air Force Test Center's Safety Management system is also described. Chapter 3 provides a detailed description of the system that is being analyzed, and defines what a mishap, hazard, and control action is in the context of this thesis. The control structure for the Edwards AFB ATC system is presented. Chapter 4 applies STPA Step 1 to this system in order to determine what the unsafe control actions are for the system. Chapter 5 continues with STPA Step 2, which determines the causes of the unsafe control actions found in STPA Step 1. The results from this analysis are discussed in Chapter 6, which also includes recommendations for improvements to the Edwards ATC system. This thesis is concluded in Chapter 7, which provides a summary of the findings.

CHAPTER 2: LITERATURE REVIEW

Several different hazard analysis techniques may be used with various degrees of success in order to safely engineer a system. This chapter begins with a brief overview of the theory behind systems engineering, and continues with a discussion of various hazard analysis techniques that are available for use. Since STPA is selected to be the hazard analysis technique used, this chapter moves on to a discussion of previous STPA work that is relevant to this thesis.

SYSTEMS THEORY

Systems engineering differs from other forms of engineering by working from the big picture of the complete system down to the details, focusing on determining system requirements based on the goals of the system as a whole. By taking this holistic view of the system, interactions between multiple subsystems and components can be included in the analysis; other techniques rely primarily on pairwise analysis and cannot adequately capture the complex system interactions. According to Leveson, systems theory has two foundational concepts: emergence and hierarchy; and communication and control (2).

Looking at a system at a high level before delving into the details introduces the idea of a hierarchy. Systems theory embraces many levels of organization, starting at the top with the big picture, low detail level and delving into more complex, focused details in each subsequent level. The higher levels have properties of their own, called emergent properties. These properties have no meaning at lower levels, but take their meaning from a certain level of system interaction (2). Safety is a prime example of an emergent property; the safety of a nut or a bolt has no meaning. Instead, safety emerges from how the nut or bolt is used as a part of the larger system.

In order to exert influence on a system, controls must be used. These controls, which constrain the action of the system, can be built in to the design in order to ensure safe behavior, or can be the means by which a user or controller causes the system to operate in some capacity. In a perfectly closed system, which had no interaction with the outside world and no potential for interference or interruption, communication could not be necessary. Since it is virtually impossible to design such a system, communication is essential in order to keep the controller aware of the state of the system and capable of issuing the correct commands (2).

By using a systems-theoretic approach to safety engineering, it is possible to examine the interactions between different components and so determine the constraints that are necessary in order to ensure safe design and safe operation of the system.

HAZARD ANALYSIS TECHNIQUES

Several different hazard analysis techniques are used in safety engineering. In general, there are two types: forward search, which starts with some initiating event and determine the potential consequences of that event, and backward search, which starts with the consequence and attempts to identify the possible causes (3). Analysis techniques can also be classified based on whether or not they take a systems approach; those that start with the big picture and then delve into the effects on subsystems are called top-down techniques, while those that start with failures of

individual components and trace these failures to their effect on the system as a whole are called bottom-up techniques (3).

Most of the hazard analysis techniques were developed for use in a specific industry, such as chemical engineering or nuclear weapons development; however, some techniques can be applied to a broad range of problems outside of their original scope. Some of the most common hazard analysis techniques in use today are Fault Tree Analysis (FTA), Hazards and Operability Analysis (HAZOP), Failure Modes and Effects Analysis (FMEA), and Systems-Theoretic Process Analysis (STPA). Since HAZOP is used primarily for production facilities such as chemical plants, it would not be appropriate to use HAZOP for this problem. This section explains the concepts, strengths, and weaknesses of the other three approaches – FTA, FMEA, and STPA. Following an explanation of each, the three methods are compared and one is selected for use in this thesis.

Fault Tree Analysis and Event Tree Analysis

One hazard technique that is often used in aerospace, electronics, and nuclear safety analyses is a fault tree analysis (3). This analysis is conducted when the undesirable outcome event, or hazard, is known. It involves a top-down, backwards search method that determines what the necessary and sufficient conditions are that must exist in order for the event to occur. It can be used qualitatively, although most people assign probabilities to each causal event in order to perform a quantitative analysis.

After the system-level, undesired event is determined, the causal events are then determined and noted as branches below the top event using Boolean logic. Standard symbols note the relations between the branches and include Boolean operators such as “and” and “or” to combine events. The output can either be a qualitative list of necessary and sufficient conditions that will result in the hazard, or a quantitative probability derived from the individual probabilities of each causal event. Figure 1 gives an example of a Fault tree for a tank explosion.

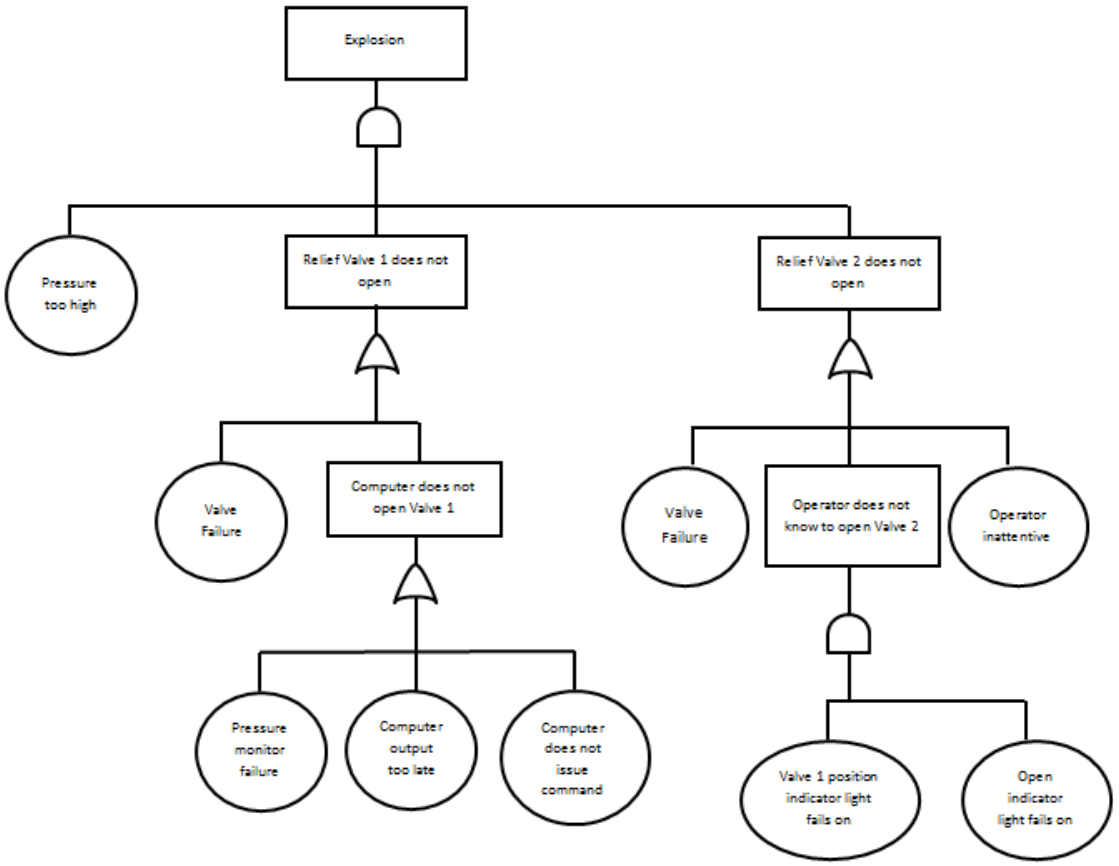

Figure 1. Example Fault Tree Analysis. (3)

The development of the fault tree results in a system-level view of the potential causal events. Identifying the minimum requirements for the hazard to occur can also provide information on the system's weaknesses and identify possible ways to eliminate the hazard. Using a FTA quantitatively, however, relies on the independence of the causal events, which may not be an accurate assumption to make. In addition, a FTA requires a certain level of design detail; as such, it is difficult to use FTA during concept design. Fault trees also can only capture one instant in time. For this reason, systems that have different mission phases or events that must occur in a certain time sequence are usually not able to be captured well by a FTA.

There is also a generalized version of this analysis called a Management and Oversight Risk Tree (MORT) Analysis. In effect, this is a FTA that also includes management, human behavior, and environmental factors as causal events (3). As defined, it is primarily a large checklist (1500 or so items) of questions that can be answered about the system.

Another similar analysis technique is called an Event Tree Analysis (ETA). It began when nuclear engineers needed a method to simplify the hopelessly complex FTA that resulted from applying the FTA technique to a nuclear power plant. The ETA differs from the FTA in that it begins from an initiating event and determines the possible outcomes, rather than starting at the outcome and determining causes. The protection systems each make up one level of the ETA, with branches from

the initiating event indicating the success or failure of that level. An example ETA is shown in Figure 2. This represents the same system as the Fault Tree shown in Figure 1.

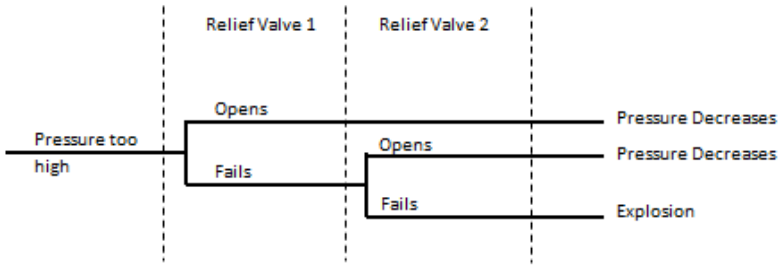

Figure 2. Example Event Tree Analysis. (3)

This technique is generally applied to a system where there are only two outcomes – success or failure. It also is generally used where there are separate layers of protection. While order is captured by an ETA, timing is not. It is also difficult to quantify the probability of failure when the failures of different protections may be based on a common cause or when there are multiple initiating events.

Since an ETA is a forward search, it starts with a single initiating event; as a result, ETAs must be developed for every possible initiating event. In order for this to occur, these initiating events must be known. There is no way for an ETA to predict the results of an unexpected initiating event or an event that is caused by several initiating events at once. All in all, it would be difficult to use a FTA or an ETA to analyze the problem of SUAS operation.

Failure Modes and Effects Analysis and Failure Modes, Events, and Criticality Analysis

While reliability and safety are very different qualities of a system, the two can be interrelated. A Failure Modes and Effects Analysis (FMEA) is used to help determine the reliability of a system based on its subsystems and components. It is a forward searching, bottom-up technique that is primarily used quantitatively.

Each component in the system is examined individually. The probability of a given component failing is usually taken from the manufacturer, based on empirical data. Then, the different types of failure, also known as failure modes, are listed for the component and the percent of failures that fall into each mode is also listed. The effect of each failure mode can be described qualitatively or is calculated quantitatively by multiplying the component failure rate of the part by the percent of times that component fails into each mode. This is repeated for every failure mode of every component in the system. The effects of each failure mode on the overall system is then determined.

Effects may be classified in many different ways, but in general, are at least divided into those that result in system failure, called critical, and those that do not, called noncritical. Other levels may be used as well. The critical effects can be summed to determine the probability of a critical failure for the system as a whole; the same can be done for each of the other categories as well. Extending the FMEA in this way - including the criticality of the effects - results in a Failure Modes, Effects, and

Criticality Analysis (FMECA). Table 1 shows an example FMECA for a railroad crossing boom gate. This gate is weighted in such a way that the weight of the boom gate will lower the gate in the event of a power failure.

Table 1. Example Failure Modes, Effects, and Criticality Analysis.

Component	Failure Modes	Cause(s) of Failure	Probability	Effects	Criticality Level	Possible Mitigations
Railroad Crossing Boom Gate	Up	Freezing Components, Obstructions	0.001	Cars on the tracks when a train is coming	Severe	Install system that indicates that the boom failed to lower completely
	Down	Motor failure, loss of power, obstructions	0.01	Cars cannot enter train crossing	Minimal	Acceptable as is

FMEAs and FMECAs are effective in determining the result of individual component failures on the system, but fail to capture the effects of multiple component failures or failures that originate from a common cause (3). It is useful for determining maintenance priorities and some improvements to the design; however, since a FMECA requires a very detailed level of design, it is generally used late in the design process. In addition, finding the probability of failure and failure modes is easiest with standard products that have been in use for some time (3). Therefore, a FMEA is difficult on an entirely new design.

Since the topic of this thesis relies on many interacting components that are organizations rather than standard parts, it would be difficult for a FMEA to provide any accurate, useful information about it.

Systems-Theoretic Process Analysis

The methods listed thus far are primarily used in reliability analyses, where components of a system may fail causing the system as a whole to operate in an unsafe state. Systems-Theoretic Process Analysis (STPA) treats safety as an emergent property of the system, based on Leveson's Systems Theoretic Accident Model and Processes (STAMP). STPA is a top-down analysis method, which treats safety as an emergent property of the higher levels.

STPA begins with defining accidents and hazards in the context of the system. Accidents are defined as loss events, while hazards are the conditions that may lead to an accident in a worst-case scenario. Once these are defined, the system is modeled using a hierarchical control structure where the controllers provide instructions or commands and receive feedback. The instructions, or control actions, that each controller may issue are identified at this point in the analysis.

Once the control structure for the system has been developed, STPA determines the conditions in which control actions result in a system hazard. Leveson lists four situations in which the control action may be unsafe, i.e., lead to a hazard. The four ways are:

- A necessary control action is not provided.
- An unsafe control action is provided.

- A control action is provided at the wrong time or in the wrong sequence.
- A control action is stopped too soon or applied too long. (2)

Each control action from the safety control structure is examined using these four categories and the context for each unsafe control action is identified. If there is a potential for the control action to result in a hazardous system state in the context of one or more of these four cases, a requirement may be written to ensure that the system design enforces that safety constraint. This is often done in table format, with the control actions listed by row and the four potentially unsafe types as column headings.

Once the first step of STPA has determined the potential unsafe control actions (UCAs) and system safety constraints, the next step is to determine potential scenarios in which the UCAs may occur (2).

The high-level scenarios sometimes lead to effective solutions that can be added to the system requirements. Otherwise, these high-level scenarios are then refined until an effective solution becomes apparent.

The overall goal of STPA is to provide engineers with a list of system functional and design requirements that can be incorporated early in the design process. These requirements put constraints on the system that enforce safe operation. This analysis technique does not provide a quantitative analysis of potential hazards. Overall, STPA allows a high-level safety analysis to be done early in the design process with a complex system, including mechanical components, software components, human operators, or even whole organizations. This flexibility makes it ideal to use for the analysis in this thesis.

PREVIOUS WORK

With the versatility of STPA in analyzing complex human systems, it has been applied to many problems. Nicholas Chung applied STPA to the Air Force Test Center's (AFTC) Safety Management System in his 2015 Master's Thesis and found some areas for improvement within the system (4).

The 13 areas for improvement that Chung found are discussed further in Chapter 6, where they are compared to the results of this analysis.

The AFTC Safety Management System plays an important role in the structure of the Edwards airspace system. Since Chung has already applied STPA to the Safety Management System organization itself, this thesis will not look into possible improvements internal to the AFTC Safety Management System.

CHAPTER 3: SUAS SYSTEM DEFINITION

The purpose of this chapter is to provide a brief overview of the SUAS control structure that will be examined in this thesis. The boundaries of the system, mishaps, and hazards are defined, and safety constraints are derived. Then, this chapter examines the current operations of SUAS in the Edwards AFB Airspace. A summary is included at the end of the chapter.

SYSTEM, MISHAP, AND HAZARD DEFINITION

SYSTEM DEFINITION

This analysis provides a high-level view of UAS test operations. As such, it does not go into detail regarding the internal workings of each organization. Detailed analyses should be, and in some cases have been, conducted to ensure that there are no breakdowns within each unit (i.e. one person receiving information and not passing it on). In order to narrow the scope of the analysis, only operations in the R-2515 airspace, coordinating with the High Desert Combined Control Facility (callsign JOSHUA) or the AFTC Military Radar Unit (callsign SPORT) will be considered. While manned aircraft are included in the system analysis due to their potential interactions with unmanned aircraft, they are not the main focus.

The Airspace

The R-2515 airspace, shown in Figure 3, is the busiest part of a much larger test range allocated to Edwards AFB. It operates under Visual Flight Rules (VFR) and requires pilots to "see and avoid" other aircraft in order to prevent collisions. All aircraft must obtain clearance before entering this area. Commercial and general aviation aircraft are not allowed within this airspace unless permission is specifically given. Some commercial test programs will request to use the airspace; in this case, Edwards AFB safety personnel will review the safety documentation of the test program and will provide approval. In addition, the general aviation Aeroclub on Edwards AFB operates out of the South Base runway; they are not allowed to stay in the airspace after takeoff unless they stay within the South Base pattern and they are only allowed to take one of two routes out of the airspace. Any pilot requesting access to the R-2515 airspace must have been briefed on the operating procedures within the airspace prior to access being granted. (5)

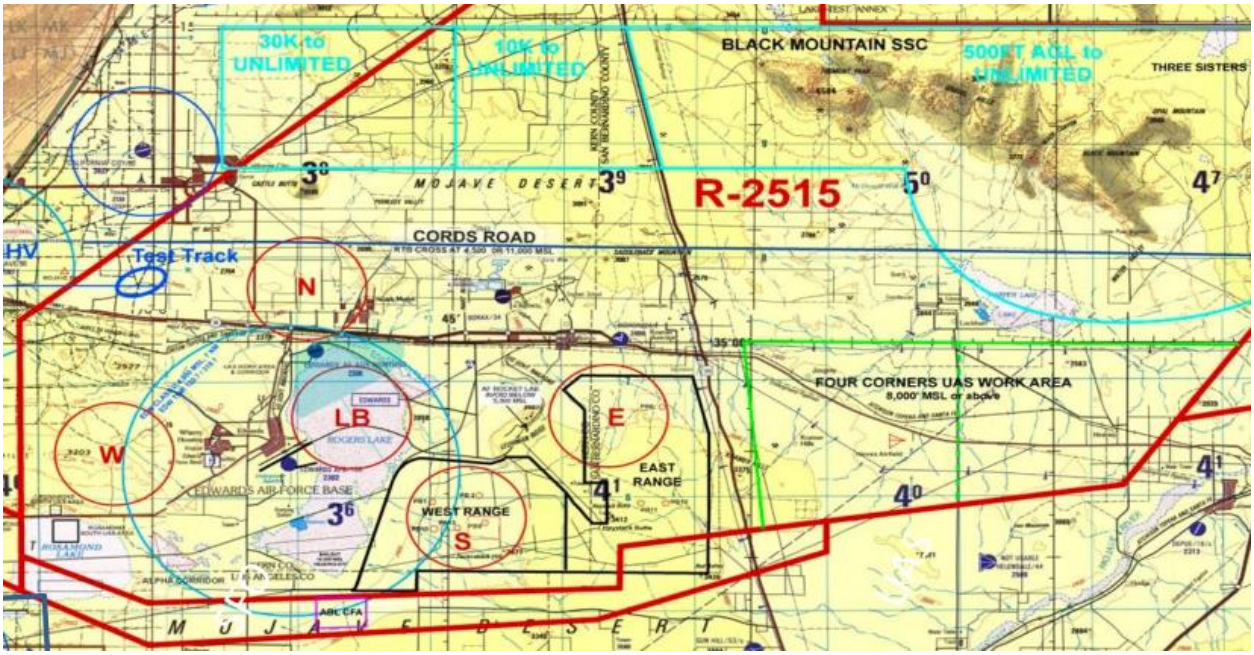

Figure 3. R-2515 Airspace.

There are areas within R-2515 that are often off limits due to particular tests or other activities. These include, but are not limited to:

- West & East Ranges – used for munitions, airdrop, and sensor testing
- Spin areas – used for departure from controlled flight testing
- Personnel drop zones – used for parachute testing
- Tower flyby – low-level high-speed flight parallel to the main runway
- Air Force Research Laboratory Rocket Propulsion Laboratory area – used for outdoor rocket testing
- Four Corners Work Area – reserved for RQ-9 flight test
- Rosamond Lakebed UAS Area – used for test or for RC aircraft hobbyists
- Small arms range – used for small arms proficiency activities
- Blackmountain Supersonic Corridor – used for supersonic flight

These areas are only off-limits if they are being actively used for the described purposes, otherwise they are available. (5)

Air Traffic Controllers

The test range as a whole falls under the control of JOSHUA. This air traffic control facility operates continuously and provides traffic advisories and boundary calls to the maximum extent possible. While JOSHUA may provide active monitoring of a specific flight, this is discouraged due to the high workload. (5)

Due to the large number of test operations being conducted in R-2515, SPORT assumes control of this area from JOSHUA during daytime hours and takes over primary controller duties. Any aircraft that is requesting an Instrument Flight Rules (IFR) clearance requires the SPORT controller to hand

off that aircraft, as well as that section of the airspace, to the JOSHUA controller. IFR clearances are generally not given in R-2515 unless weather conditions necessitate their use. (5)

Aircraft Being Analyzed

The Department of Defense (DoD) classifies UAS into groups based on their maximum weight, speed, and altitude. Table 2 shows how these groups are broken down.

UAS Group	Maximum Takeoff Weight (lbs)	Nominal Operating Altitude (ft)	Speed (kn)
Group 1	0-20	< 1,200 AGL	100
Group 2	21-55	< 3,500 AGL	< 250
Group 3	56-1,320	< FL 180	
Group 4	> 1,320	< FL 180	Any Airspeed
Group 5		> FL 180	

Table 2. UAS Groups. (6)

In order to align this analysis with the needs of the Emerging technologies CTF, this analysis will focus on UAS that fall into groups 1, 2, and 3. In order to distinguish the airborne vehicle itself from the ground control station, communications equipment, and other necessary components, the term UAV will be used to describe the vehicle only, while UAS will refer to the entire system.

MISHAP[1] DEFINITION

There are two main factors that need to be considered when SUAS are integrated into the controlled airspace: safety and efficiency, with safety having significantly higher priority. With these goals in mind, three events will be defined as mishaps for the purpose of this analysis.

A1: Aircraft Damage. Aircraft (including both manned and unmanned systems) in the air are damaged or destroyed.

The Aircraft Damage mishap was specifically defined to include only events that result in actual damage, rather than what the FAA terms a near mid-air collision (NMAC). These involve "an incident associated with the operation of an aircraft in which a possibility of collision occurs as a result of proximity of less than 500 feet to another aircraft, or a report is received from a pilot or a flight crew member stating that a collision hazard existed between two or more aircraft" (7). While a NMAC does constitute a violation of a FAA safety standard, it does not "result in a loss… of human life or human injury, property damage, environmental pollution, mission loss, etc." (2). Therefore, it is not defined as a mishap within the framework of STPA.

A2: Ground Damage. Ground structures are damaged or destroyed, or personnel on the ground are injured or killed.

[1] While the term "accident" is used for non-military systems, "mishap" (which is defined in a broad way to include any loss, as is done in STPA) is used for military systems.

The setup of Edwards AFB makes it difficult to ensure that a SUAV will never fly directly over a person or structure on the ground. Coupled with the possibility of the SUAV departing controlled flight, there is some risk to any ground personnel or structure in the vicinity of the test operations. While very small SUAS may not cause harm to an unprotected person, the Group 3 SUAS have the potential to injure or kill, as well as cause significant damage to structures. Since some SUAS are military in nature, the potential for an improper release of payload or munitions must also be taken into account.

A3: Inefficient Operations. Testing or flight operations are unable to be conducted.

The AFTC states that its mission is to "conduct Developmental Test and Evaluation of air, space, & cyber systems to provide timely, objective, and accurate information to decision makers" (8). For this reason, although flight operations, specifically test operations, inherently involve some form of risk, testing must still continue. While the safest option may be to forego any flight operations whatsoever, doing so runs counter to the mission of Edwards AFB. Therefore, the Edwards AFB seeks to avoid collisions and to maximize the airspace available for flight operations.

These mishaps are listed in order of priority, with A1: Aircraft Damage having the highest priority due to the potential damage such a collision may cause, A2: Ground Damage having the second highest priority since the scale of UAS being considered makes the potential damage to a ground object less, but still significant, and A3: Inefficient Operations being a distant third since it is a loss of mission, time, and money, but not damage or a potential loss of life.

Hazard Definition and Safety Constraints

Once the mishaps, or the events that must not occur, are defined for the system, the next step of the STPA process is to use these to derive hazards. These hazards consist of a "set of conditions that, together with a particular set of worst-case environmental concerns, will lead to a mishap" (2). From the three mishaps listed above, 5 hazards were found.

(A1) Aircraft Damage

The first mishap (A1) is when aircraft (including both manned and unmanned systems) in the air are damaged or destroyed. This can occur when one of two hazards occur.

H1: Air-to-Air Collision. Collision of two or more aircraft (including both manned and unmanned systems) in the air.

H2: Debris Impact in the Air. Debris from a SUAS impacts another aircraft (including both manned and unmanned systems).

The second hazard, H2: Debris Impact in the Air can be extended to include other objects, such as payload or munitions, being ejected from the SUAS and impacting other aircraft.

(A2) Ground Damage

The next mishap (A2) is when ground structures are damaged or destroyed, or personnel on the ground are injured or killed. This can occur when one of the following two hazards occur.

H3: Air-to-Ground Collision. Collision of a SUAS with a structure or person on the ground.

H4: Debris Impact on the Ground. Debris from a SUAS unintentionally impacts a structure or person on the ground.

The second hazard, H4: Debris Impact on the Ground can be extended to include other objects, such as payload or munitions, being ejected from the SUAS and impacting other aircraft. It only includes unintentional impacts; intentional impacts such as a munitions drop onto a structure intended for testing effectiveness are not a hazard.

(A3) Inefficient Operations

The next mishap (A3) is when testing or flight operations are unable to be conducted. In the context of SUAS use at Edwards AFB, this occurs when:

H5: Interference. SUAS testing or flight operations unnecessarily interfere with flight operations.

These five hazards together form the base system requirements; in the most general terms, the system must be constrained so that these hazards do not occur. The safety constraints, in the form of requirements that can be given to system designers, derived from the five hazards are:

(R1) SUAS must not collide with other aircraft (including both manned and unmanned systems) in the air.

(R2) Debris from a SUAS must not impact another aircraft (including both manned and unmanned systems).

(R3) SUAS must not collide with a structure or person on the ground.

(R4) Debris from a SUAS must not unintentionally impact a structure or person on the ground.

(R5) SUAS testing or flight operations must not unnecessarily interfere with flight operations.

SUAS Operations at Edwards AFB

Conducting a flight test of a SUAS can be informally broken down into four stages: planning, pre-flight, flight operations, and post-flight. These stages are discussed in the following sections.

Planning Stage

The test unit coordinates with the SUAS manufacturer in order to develop an understanding of the capabilities of the SUAS. The test unit then, with a specific goal in mind, structures a test plan that begins by testing basic capabilities, such as takeoff and landing, before moving on to more advanced capabilities, such as maneuvering. The specific buildup of the tests depends on the stage of the development that the SUAS is in, as well as the overall goals of the test unit. The buildup approach helps to establish specific goals for the individual flights. With these goals in mind, the test unit coordinates with the manufacturer to identify possible hazards and establish safeguards to prevent mishaps. These are documented in the test safety package, which is then presented to a Safety Review Board (SRB).

According to the Air Force Test Center Instruction (AFTCI) 91-202, "the purpose of the safety review phase is to allow an independent team to formally review the test unit's safety planning to ensure that all test hazards have been identified and sufficiently mitigated, then affirm or modify the residual risk." (9). The SRB examines the hazards identified, adding any that were missed, as well as the mitigations that the test unit will implement in order to prevent mishaps. Any feedback from the SRB must be addressed before the safety package will be approved. Once all of the concerns have been addressed, the safety package is submitted for approval. The final approval authority depends on the level of risk that the test will involve. The exact approval chain is outside of the scope of this analysis; however, it is important to note that the 412th Operations Group (which is responsible for operating both the JOSHUA and SPORT control facilities) is a part of the SRB and is able to provide feedback on the test in this way.

Pre-Flight Phase

Once the safety package has been approved, the test unit may conduct flight test operations subject to the conditions outlined in the package. Each individual flight, however, requires some coordination before it can take place.

During this phase, if necessary, special use areas such as drop zones or spin areas must be scheduled through the Resource Operations Center (ROC), which falls under the 412th Operations Group. (5) The SPORT prebrief must also be completed and sent to SPORT in order to convey the intentions of the aircraft during the flight, including entry/egress points, planned route, and any special considerations such as munitions drops or air-to-air refueling. This prebrief also lists the frequency that the aircraft will be operating on and the telephone number of the test unit. (10) An example prebrief is shown in Figure 4.

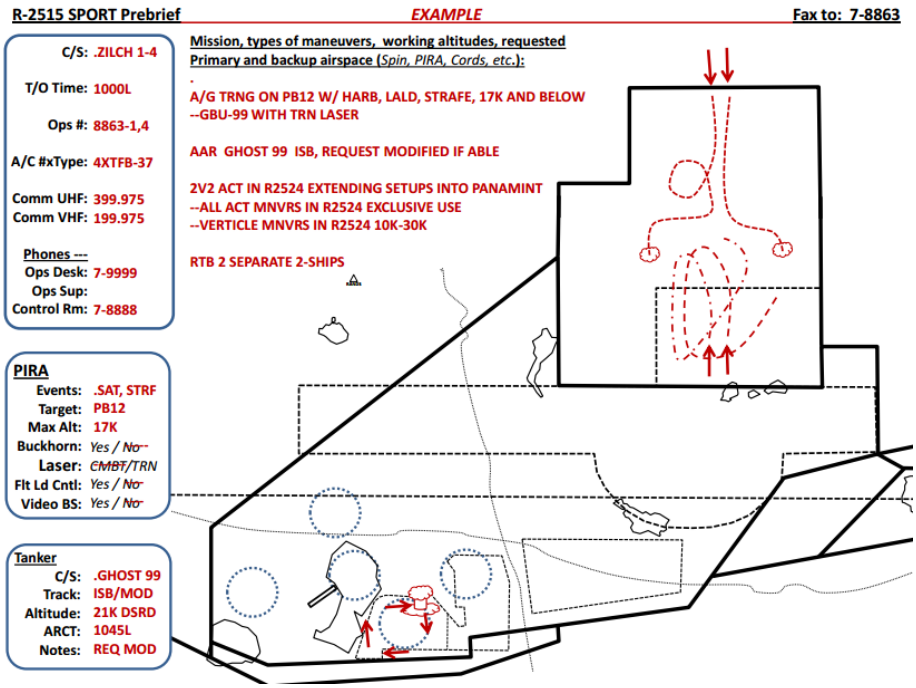

Figure 4. R-2515 Example SPORT Prebrief. (10)

If necessary, this phase also includes filing a flight plan, uploading an autopilot program to the SUAV, and any other steps needed to prepare for the actual test.

Flight Operations

This phase of testing includes the entire time between when the UAV begins to taxi and when the SUAV is back on the ground and clear of any taxi or runways. During this phase of flight, the SUAV taxis and takes off (if applicable) and requests clearance into R-2515 from SPORT. The pilot is controlling the SUAS in a manner that is appropriate for both the design of the system and the goals of the test. This control can be as rudimentary as roll, pitch, and yaw inputs or as complex as sending an entire route plan and monitoring the vehicle for any unexpected events. The pilot requests and SPORT grants (if conditions permit) airspace clearances and traffic advisories. The test is conducted according to the plans submitted and (if applicable) the SUAV lands and taxis to its final destination. While in many ways the simplest phase, as every step has already been planned, the flight operations phase is also the most dangerous. This phase is when the mishaps would most likely occur.

Should an unexpected event happen, the pilot, test unit, and controllers ensure that other aircraft, structures, or personnel are not endangered. If it is safe to resume the test, then this occurs; otherwise, the flight test concludes.

Post-Flight

Once the test, successful or otherwise, has been completed, the information gained is integrated into the planning of future tests. A successful test provides information that aids in planning the next buildup test, while an unsuccessful test is analyzed to find out how to improve future tests. If hazards are observed in the course of the test, the safety plan in place must be reevaluated to ensure that future tests are not subjected to the same faults.

Hierarchical Control Structure

In order to conduct a safety analysis using STPA, it is necessary to first construct a model of the system hierarchical control structure. This structure is shown in Figure 5. The control structure represents all of the key units, or controllers, in the system, as well as the feedback and control actions of each. Solid, black lines represent connections in place during the flight operations phase. Dotted, blue lines show the connections that are exclusively active during the planning, pre-flight, and post-flight phases. Since this analysis is meant to be a high-level view of the safety control structure, the diagram simplifies whole units into a single controller, and in some cases eliminates controllers that only pass on information. For example, the 412th Operations Group Staff pass on the safety packet to the 412th Operations Support Squadron, which passes on the information to SPORT and JOSHUA. In the interest of simplicity, this intermediate step is eliminated and the information is shown to flow from the Operations Group to SPORT and JOSHUA.

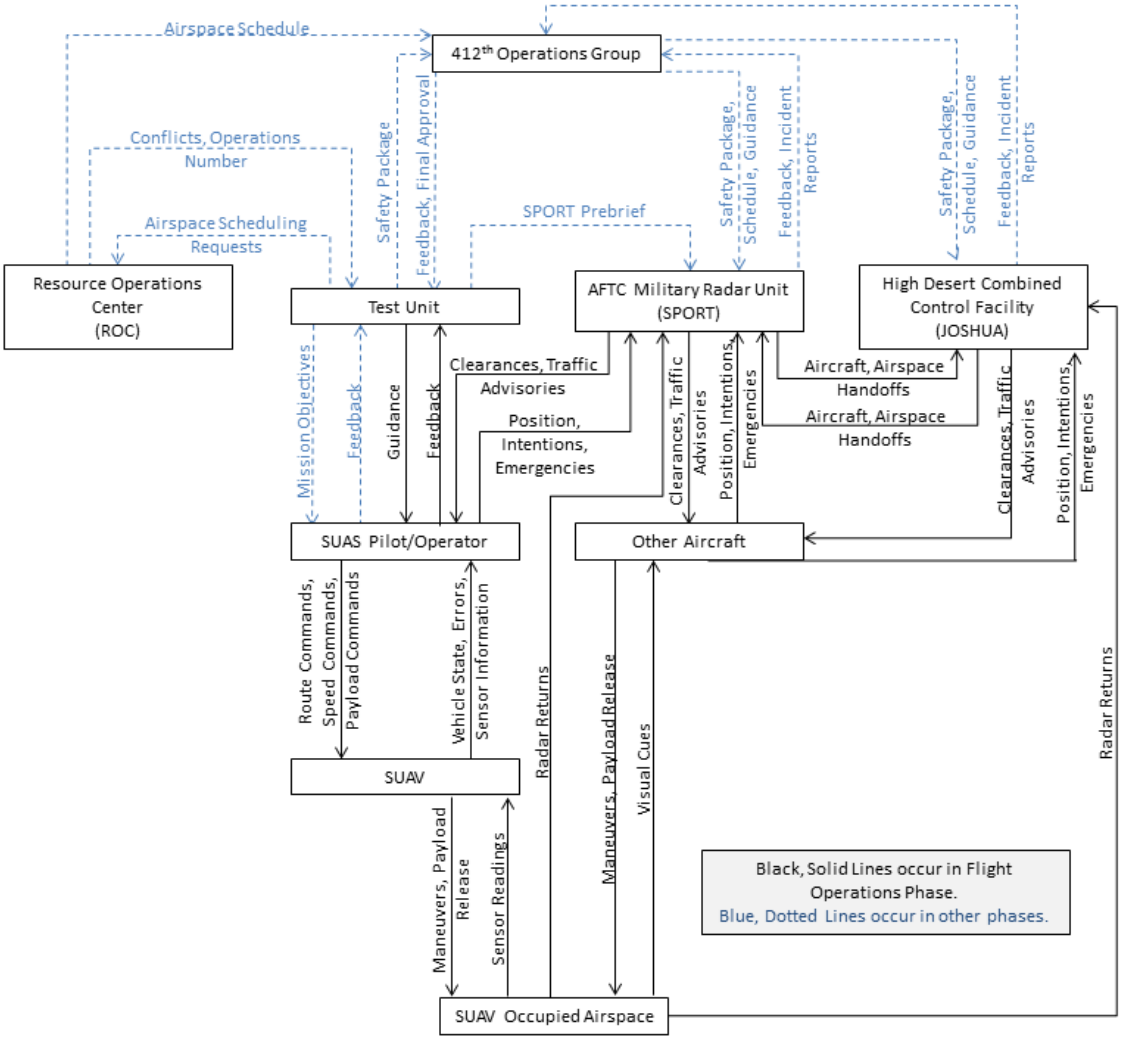

Figure 5. Hierarchical Control Structure.

Each controller and their respective control actions and feedback are described below. Additional details are available in Appendix A.

Planning, Pre-Flight, and Post-Flight Stages

In the following descriptions, the control actions and feedback responses occur during the Planning, Pre-Flight, or Post-Flight Stage. These phases will be referred to collectively as the Non-Flight Stage.

412th Operations Group (412 OG)

The 412th Operations Group includes many flight test squadrons, as well as the Operations Support Squadron (OSS). The OSS is responsible for all flight support aspects, including the Air Traffic Control Facilities and the Resource Operations Center (ROC). The group is responsible for ensuring that the ROC and ATC facilities receive proper training and are following all appropriate regulations. The 412 OG may also implement stricter regulations or guidance specific to operations at Edwards AFB if it is deemed appropriate.

The commander of the 412 OG or one of his or her representatives is present at the SRB to ensure that his or her safety concerns are addressed. If there are safety issues that the SRB does not address, the commander is able to direct the test unit to address the issue before submitting the final safety package by providing feedback. In some cases the 412 OG commander is authorized to give the final approval for the test. If this is not the case, the 412 OG commander's approval is still required, but the 412 OG passes the safety package to a higher level commander, who must also approve. In any case, the safety package must get approval from the 412 OG before the test may proceed.

Relevant issues from the safety package are passed on to subordinate units, including SPORT and JOSHUA, if needed. Once the ROC schedules and deconflicts all tests being conducted on any given day, that schedule is also passed on to ATC facilities.

The subordinate units are required to submit incident reports should a mishap occur; ideally, these will be used to modify the control measures in place to prevent further mishaps.

Resource Operations Center (ROC)

The Resource Operations Center receives a request from a test unit for operations in R-2515. This request indicates if a specific airspace is necessary, such as a specific altitude, spin or drop zones, etc. Since some of these areas cannot be used simultaneously, the ROC must make sure that there are no simultaneous requests. These conflicts are resolved according to a published priority list; the lower priority mission is required to reschedule or relocate in order to accommodate the other. Once these conflicts are resolved, the ROC assigns an Operations Number, which is required to enter the R-2515 airspace. The operations schedule that includes all requests is given to the 412 OG to distribute as necessary to subordinate units.

High Desert Combined Control Facility (JOSHUA)

During the non-flight phases, JOSHUA Control receives guidance, in the form of training, regulations, and other methods, from 412 OG that govern operations at Edwards AFB. In turn, JOSHUA provides feedback to the 412 OG regarding practices that are or are not working well.

Once the 412 OG receives the safety package, any aspects that need to be brought to JOSHUA's attention are passed on. JOSHUA also receives the airspace schedule from the ROC by way of the 412 OG and the combined supervisor of flying. This information is given to the controllers on shift so that they are aware of the flights that will be taking place.

In the event of an emergency as defined by Edwards Air Force Base Instruction (EAFBI) 13-100, an incident report is generated during the post-flight phase and sent to the 412 OG so that steps can be taken to prevent future occurrences.

AFTC Military Radar Unit (SPORT)

SPORT operates similarly to JOSHUA during the non-flight phases, providing feedback and incident reports as necessary and receiving the airspace schedule, relevant information from the safety package, and training and guidance from the 412 OG.

During the Pre-Flight Phase, SPORT also receives the Prebrief shown in Figure 4 above from each aircraft requesting access to R-2515. This provides additional information regarding each mission's intentions, special accommodations, and contact information that can be used in the event of an emergency. These SPORT Prebriefs are used to further deconflict flights and are available to the on-shift controllers.

Test Unit

Prior to flight operations, the Test Unit has several responsibilities. The overall mission objectives are formed and given to the team that is working on the safety package, which includes the SUAS Pilot. The project safety team receives feedback from many sources, including the SUAS pilot, project engineers, and safety experts in order to produce the test safety plan. Once this safety plan is deemed sufficient, a SRB is held at which point the 412 OG may provide feedback on items that were not sufficiently addressed. Once these items are fixed, the final safety package is presented to the 412 OG and final approval is received.

After the test plan receives approval, the Test Unit contacts the ROC to schedule their time in the airspace. If there are conflicts with other scheduled tests, these are resolved and the ROC provides an Operations Number for the mission. The SPORT Prebrief is also filled out and filed with SPORT.

SUAS Pilot

The SUAS Pilot's primary responsibility during the non-flight phases is to act as a member of the project safety team. He or she takes the mission objectives and provides feedback to the team from the point of view of the operator. Since this may be the only person on the team with flight experience, this feedback is necessary to the safety planning stage.

Flight Operations Stage

High Desert Combined Control Facility (JOSHUA)

Since JOSHUA operates continuously whereas SPORT only operates during the day, an airspace handoff must occur at the start and end of the SPORT operations period. In addition, any aircraft requiring an IFR clearance must be handed off to JOSHUA, along with the airspace that the aircraft is flying through. Once the aircraft has landed, cleared the airspace, or no longer needs an IFR clearance, that airspace is handed back to SPORT control.

JOSHUA is also in contact with any aircraft that it is controlling. This includes granting clearances for an aircraft to enter a specific airspace, and traffic advisories as necessary. The aircraft, in turn, provide JOSHUA with their position, intentions, and if conditions permit, alert JOSHUA of any emergencies that they experience. JOSHUA is equipped with a ground radar unit and a receiver so that it is able to monitor aircraft in the airspace by their radar returns and/or transponder signals.

In general, this analysis assumes that the SUAS is operating in SPORT controlled airspace.

AFTC Military Radar Unit (SPORT)

SPORT again acts similarly to JOSHUA in controlling other aircraft; however, SPORT controls the R-2515 airspace, where operations differ significantly. SPORT still issues airspace clearances and traffic advisories to aircraft in R-2515. Due to ongoing testing, however, the intentions of other

aircraft are not as clear cut. The constant maneuvering also makes the direction of flight difficult to gauge. This airspace will include SUAS operations as well as other test missions.

In addition to the SUAS Pilot reporting the SUAV's position, SPORT may be able to track the vehicle directly if the SUAV is large enough to appear on radar, or if it is equipped with a transponder.

Test Unit

During Flight Operations, a control room is set up at the Test Unit that includes many experts on the system. As the test progresses, this team monitors the flight and the information recorded and provides guidance to the pilot, including requests to run a particular test again or answering any questions that come up.

SUAS Pilot

The Flight Operations Phase revolves around the SUAS pilot. The pilot is sending route, speed, and payload commands to the SUAV. Depending on the nature of the vehicle's software, these commands may be the standard roll, pitch and yaw inputs, a complex flight plan that is preset, or anything in between. In any case, the pilot is monitoring the information that the SUAV is sending back, which includes information regarding the vehicle state, sensor information, and any errors that the system encounters.

The pilot is also communicating the SUAV's position, intentions, and any emergencies with SPORT, and receiving the clearances and traffic advisories that SPORT provides. The pilot is in communication with the control room should any additional guidance be needed.

SUAV

In the Flight Operations Stage, the SUAV is receiving and executing the route, speed, and payload commands, and sending the pilot the vehicle state and sensor information, as well as any errors that occur.

The SUAV acts on the airspace by maneuvering, as well as by dropping any payload that it may be carrying. The SUAV itself may be trackable by SPORT or other aircraft, which will then be able to receive the SUAV's position.

Other Aircraft

Any other aircraft operating within R-2515 will be conducting their own maneuvers, in collusion with their own control rooms. They will also be communicating their position, intentions, and any emergencies with SPORT or JOSHUA, and receiving the clearances and traffic advisories from SPORT or JOSHUA, depending on which controller they are currently under. If the SUAV is large enough to be visible to the pilot of the other aircraft, the position of the SUAV may be known. This is also possible if the SUAV is equipped with a transponder that is received by the other aircraft.

All other aircraft are also acting on the airspace by maneuvering, dropping payloads, or firing weapons.

SUAV Occupied Airspace

The controlled process in this system is the SUAV Occupied Airspace. This airspace will be defined to include only the SUAV's immediate surroundings and the area that the SUAV or its payload will occupy in the near future. How much of the surroundings are included will vary based on the proven accuracy of the SUAV's positioning. Initially, this airspace will be large as there is little to no proven accuracy, but once a vehicle is reliably maintaining its route and is accurately reporting its position, the SUAV Occupied Airspace will shrink.

In other words, it is assumed that any object that enters the SUAV Occupied Airspace is likely to collide with the SUAV. The SUAV Occupied Airspace is the portion of the R-2515 that the SUAV test is expected to occupy in the near future.

SUMMARY

The system that is being analyzed is composed of the R-2515 airspace, controlled by SPORT, and operations involving operations involving SUAS within these boundaries. A SUAS is defined by the DoD as having a maximum takeoff weight of less than 1,320 pounds, a Nominal Operating Altitude lower than flight level 180, and a maximum speed less than 250 knots. The term SUAV will be used to describe the vehicle itself, while the term SUAS will refer to the system as a whole.

Three types of mishaps were defined, in the context of this analysis:

- **A1: Aircraft Damage.** Aircraft (including both manned and unmanned systems) in the air are damaged or destroyed.
- **A2: Ground Damage.** Ground structures are damaged or destroyed, or personnel on the ground are injured or killed.
- **A3: Inefficient Operations.** Testing or flight operations are unable to be conducted.

These three mishaps were used to determine the five system hazards, which were also used to develop the high-level system requirements. The five hazards in this analysis are:

- **H1: Air-to-Air Collision.** Collision of two or more aircraft (including both manned and unmanned systems) in the air.
- **H2: Debris Impact in the Air.** Debris from a SUAS impacts another aircraft (including both manned and unmanned systems).
- **H3: Air-to-Ground Collision.** Collision of a SUAS with a structure or person on the ground.
- **H4: Debris Impact on the Ground.** Debris from a SUAS unintentionally impacts a structure or person on the ground.
- **H5: Interference.** SUAS testing or flight operations unnecessarily interfere with flight operations.

The flight testing process in place at Edwards AFB can be informally broken down into four phases: planning, pre-flight, flight operations, and post-flight. These can be further grouped into non-flight stages and the flight operations stage.

A hierarchical control structure was constructed to model the interactions of the system. The difference between the control structure in the non-flight stages and the control structure in the

flight operations stage makes breaking the analysis of the overall system down into two separate analyses a good choice.

The hierarchical control structure shows the controllers in the system as well as the control actions available to them. A description of the controllers and their control actions and feedback was provided. In the context of the flight operations analysis, the process that the system is controlling is the SUAV Occupied Airspace. This airspace is, essentially, a bubble enclosing the SUAV and separating it from other aircraft. While larger airspace allocations would lead to safer interactions, it would also significantly decrease the efficiency of the system.

CHAPTER 4: DETERMINING SAFETY REQUIREMENTS

Once the control structure has been generated and the control actions defined, the first step of STPA can be applied. This step takes the control structure and determines the potential unsafe control actions (UCAs) for each controller. These UCAs are then used to build system-level safety requirements that can be used as design requirements. In the case of people or organizations, these requirements may be better described as responsibilities. This chapter begins by describing STPA Step 1 and then applies this technique to the control structure found in Chapter 3. An example Step 1 Analysis is performed, and then interesting results are discussed. A summary concludes the chapter.

SPTA STEP 1

If the hierarchical control structure describes what actions the operators can take, then Step 1 of STPA describes when these actions are unsafe. It is important to remember that this step of the analysis does not explore why or how an UCA might occur; rather, this step focuses on identifying all of the possible UCAs. According to Leveson, a control action can be unsafe in one of four ways:

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long. (2)

This step examines every possible control action from every controller in the hierarchical control structure in each of these four contexts. If a hazard may occur, then the conditions under which the control action becomes an Unsafe Control Action (UCA) are annotated. This step is typically carried out using a table, where each control action is a row and the four ways that control action may become unsafe form the columns.

FULL STEP 1 ANALYSIS OF THE SUAV CONTROLLER

Referring back to the control structure, it can be seen that the SUAV has two control actions that act on the SUAV Occupied Airspace: Maneuver and Payload Release.

The Step 1 table, then, is generated using these control actions as the two rows. Each cell is filled in with the conditions that would make the control action unsafe, as shown in Table 3.

Control Action	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Maneuver	…when the maneuver takes the SUAV out of its assigned airspace. [H1, H3]	…when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]	…when the maneuver is applied too late. [H1, H3]	…stopped before the maneuver is complete. [H1, H3] …held after the maneuver is complete. [H1, H3]
Payload Release	…when the payload will exit	…when payload should be released	n/a	…stopped before payload can fully

	SUAV Occupied Airspace. [H2, H4]	[H5].		release. [H2, H4]

Table 3. SUAV Unsafe Control Actions.

The hazard associated with the UCA is also generally included. Here, the hazard is annotated in brackets. The table is turned into a list of the 8 potential UCAs for the SUAV:

- The SUAV maneuvers when then maneuver takes it out of its assigned airspace. [H1, H3]
- The SUAV does not maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]
- The SUAV maneuvers too late to stay in its assigned airspace. [H1, H3]
- The SUAV maneuver is stopped before the change in direction is complete. [H1, H3]
- The SUAV maneuver is held after the change in direction is complete. [H1, H3]
- The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]
- The SUAV does not release its payload when the payload should be released. [H5]
- The SUAV payload release is stopped before payload can fully release. [H2, H4]

These UCAs can then be turned into safety constraints, which can also be used as requirements in the design of a system. To transform an UCA into a Safety Constraint (SC), simply negate the sentence and make it an imperative sentence. The eight UCAs above become the following eight SCs:

Unsafe Control Action	Safety Constraint
The SUAV maneuvers when then maneuver takes it out of its assigned airspace. [H1, H3]	The SUAV must not maneuver when then maneuver takes it out of its assigned airspace. [H1, H3]
The SUAV does not maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]	The SUAV must maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]
The SUAV maneuvers too late to stay in its assigned airspace. [H1, H3]	The SUAV must maneuver in time to stay in its assigned airspace. [H1, H3]
The SUAV maneuver is stopped before the change in direction is complete. [H1, H3]	The SUAV maneuver must not stop before the change in direction is complete. [H1, H3]
The SUAV maneuver is held after the change in direction is complete. [H1, H3]	The SUAV maneuver must not hold after the change in direction is complete. [H1, H3]
The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]	The SUAV must not release its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]
The SUAV does not release its payload when the payload should be released. [H5]	The SUAV must release its payload when the payload should be released. [H5]
The SUAV payload release is stopped before payload can fully release. [H2, H4]	The SUAV payload release must not stop before payload can fully release. [H2, H4]

Table 4. SUAV Safety Constraints.

A full STPA Step 1 Analysis of control actions was performed, and is included in Appendix B. The above analysis for the SUAV Controller corresponds to UCAs (and SCs) 63 through 70.

UCAs in Non-Flight Stages

Twenty-five UCAs were found in the non-flight stages, from which twenty-five safety constraints were derived. Some of these UCAs are fairly obvious. For example, common sense could have derived the following safety constraints:

(SC 19) The Test Unit must not provide the safety package to the 412 OG when safety plan is not sufficient. [H1, H2, H3, H4]

(SC 21) The Test Unit must not provide the safety package to the 412 OG until feedback from the SRB has been addressed. [H1, H2, H3, H4]

Others, however, were less intuitive.

Safety Concerns

Feedback from the Safety Review Board

Unsafe Control Actions 1 and 2, which are presented below, deal with feedback given to the Test Unit during the SRB.

(UCA 1) 412 OG does not provide feedback to the Test Unit when the existing safety plan is not sufficient. [H1, H2, H3, H4]

(UCA 2) 412 OG stops providing feedback to the Test Unit before all of the concerns are addressed. [H1, H2, H3, H4]

This emphasizes the necessity of feedback as a control action by the 412 OG. This feedback must be given to the test unit in order to improve the safety plan, and this process must iterate until all of the 412 OG's safety concerns are addressed. The iterative nature of this feedback is an essential part of the test planning phase.

Final Approval

The feedback loop continues until Final Approval is given. UCAs 3 and 5 show when this final approval leads to a hazard.

(UCA 3) 412 OG provides final approval to the Test Unit when the safety plan is not sufficient. [H1, H2, H3, H4]

UCA 3 emphasizes that approval should not be conditional on the test unit addressing additional concerns; instead, final approval should only be given once the feedback loop has run its course.

(UCA 5) 412 OG provides final approval to the Test Unit before all of the concerns raised during the SRB are addressed. [H1, H2, H3, H4]

This UCA again emphasizes that the feedback must be incorporated into the safety package before final approval is given. In addition, since the commander may have sent a representative in his or her place to the SRB, it is important that the commander reviews the concerns raised during the SRB prior to granting final approval.

Rescinding Approval

One result of the step 1 analysis that is not immediately intuitive was UCA 6:

(UCA 6) 412 OG provides final approval to the Test Unit and does not rescind this approval if additional information indicates it should be. [H1, H2, H3, H4]

When final approval is granted, that is based on the information available at the time. As time progresses, however, other information may come to light and impact the safety plan of the test. For example, SPORT or JOSHUA may send feedback to 412 OG that the controller workload is too high for them to reliably provide traffic advisories during peak hours. If the safety plan is contingent on these traffic advisories, then it is no longer sufficient.

SPORT Prebrief

While much of the paperwork that must be filed prior to flight seems inefficient, the SPORT Prebrief is shown to be essential to system safety.

(UCA 23) The Test Unit does not provide the SPORT Prebrief when the mission is planned to fly. [H1, H2, H3, H4, H5]

This UCA can lead to any of the five hazards. SPORT may block off more airspace than the SUAS needs, leading to inefficient operations. More importantly, the SPORT controller does not have the Prebrief to reference and visualize where the SUAV will be operating. If the SUAV is not visible to radar and controller workload is high, the controller may inadvertently send another test mission into this same area without providing a traffic advisory. The quick, easy-to-reference nature of the SPORT Prebrief, in addition to the level of detail that it provides, is essential to safe operations in R-2515.

Efficiency Concerns

The Resource Operations Center

While the ROC has six potential unsafe control actions, all six only result in inefficient operations. This is because the schedule generated by the ROC is only used in the preliminary planning of the control operations. While it is available to reference and is useful in determining when the peak periods of activity will occur, the real-world conditions play a larger role.

In addition, while the Operations Number given by the ROC is necessary for a mission to enter R-2515, it is not sufficient. If a mission is given an operations number, then SPORT must still provide clearance before the aircraft enters R-2515. In the event of conflicts, SPORT can simply deny the aircraft clearance, resulting in inefficient (but safe) operations.

Mission Objectives

UCAs 24 and 25 dictate that the test unit must provide the test pilot and the rest of the safety planning team with mission objectives early in the test planning process.

(UCA 24) The Test Unit does not provide the SUAS pilot with the mission objectives. [H5]

(UCA 25) The Test Unit provides the SUAS pilot with the mission objectives too late in the test planning process. [H5]

If the test unit performs these UCAs, the safety planning team may begin to develop a plan for a test that is vastly different from the one that the test unit intended. Once this oversight is recognized, the safety planning process would have to start over, and all of the work that had been performed up to this point would have been for naught.

412 OG and Air Traffic Controllers

In most cases, the commander of the 412th Operations Group is a pilot, with little air traffic control background. UCAs 10 and 12, however, demonstrate that the 412 OG must find a way to think outside of the cockpit, and include other aspects of air operations in the decision-making process.

(UCA 10) 412 OG must provide information from the safety package to SPORT and JOSHUA when the information is relevant. [H1, H2, H3, H4]

(UCA 12) 412 OG must provide guidance (training) to SPORT and JOSHUA when specific guidance is necessary. [H1, H2, H3, H4, H5]

UCAs in Flight Operations Stage

Forty-nine additional UCAs and their corresponding safety constraints were found in the Flight Operations Stage. These include actions by air traffic controllers, pilots, the SUAV itself, and their interactions with the SUAV Occupied Airspace.

Air Traffic Controllers

JOSHUA Control Facility

This analysis assumes that SUAS Operations will only occur in SPORT airspace while SPORT is active. It seems redundant, then, to include another control tower in the analysis. JOSHUA was included due to its heavy interaction with SPORT and the SPORT controlled airspace. In general, SPORT controlled airspace is well-defined, but there are some cases where a portion of this airspace is handed off to JOSHUA, such as when an aircraft flying through R-2515 requires an IFR clearance.

The analysis found nine UCAs for JOSHUA; however, only one of these has a direct SUAS application.

(UCA 27) JOSHUA does not hand off aircraft to SPORT when aircraft is entering SPORT airspace. [H1, H2, H3, H4]

If an SUAS is operating in SPORT airspace and is not visible via radar or transponder, then JOSHUA would believe that the airspace is clear. The SUAS pilot is in communication with SPORT, however, so SPORT would be able to advise the aircraft of the location of the SUAV.

If SUAV operations are allowed to commence in R-2515 outside of the current UAV Work Areas, then a positive handoff to SPORT must occur before the aircraft crosses the airspace boundary into R-2515. This is the only way that SPORT will be able to advise the aircraft on the position of any active UAVs.

Handoffs

In addition to UCA 27, which is mentioned above, six additional UCAs involve airspace or aircraft handoffs. It is important during these handoffs that both controllers are aware of exactly which aircraft and airspace is being given or received, as well as the status of each.

It is possible, especially if the SUAS is not visible to SPORT, that the SUAV will be in or approaching the airspace involved. This must not be allowed to happen, because JOSHUA does not have contact with the SUAS Pilot; in effect, there is no way for JOSHUA to become aware of the SUAV in the airspace. The following two safety constraints are critical for the SPORT controller to confirm before the handoff occurs, especially if a SUAS is known to be operating in the area:

(SC 35) SPORT must not hand off an aircraft to JOSHUA when another SPORT controlled aircraft is encroaching. [H1]

(SC 38) SPORT must not hand off airspace to JOSHUA without handing off aircraft in the airspace. [H1]

Clearances

Similarly, it would be easy for a SPORT controller to issue a clearance to an aircraft assuming that the airspace is safe when it is, in fact, where a SUAS mission is occurring. This would result in UCA 39:

(UCA 39) SPORT provides an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]

Similarly, the airspace which was safe at the time the clearance may become unsafe if it is in the path of the SUAV. This would result in UCA 41:

(UCA 41) SPORT provides an aircraft with a clearance that is not rescinded when the airspace is no longer safe. [H1, H2, H3, H4]

UCAs 39 and 41 demonstrate that SUAS operations will need to involve more active monitoring from air traffic control facilities. If the SUAS is not visible to controllers, then the SUAS pilot should provide the route (in the form of the SPORT Prebrief) and continue to update the controller on the SUAV's progress; otherwise, the SUAV may need to operate in an airspace that is segregated away from other aircraft.

Traffic Advisories

As long as the SUAV's location is known, then traffic advisories would not change significantly. One of the major factors that SPORT would have to keep in mind, though, when controlling a SUAV, is the potential lag time between when the pilot commands a maneuver and when the SUAV responds. In order to enforce Safety Constraint 43, the controller must be aware of the degree of lag in the system.

(SC 43) SPORT must provide an aircraft with traffic advisories in time for corrective action. [H1, H2, H3, H4]

EXPECTED RESULTS

Test Unit Control Room

The four UCAs found for the Test Unit during flight operations all involve the control room. In normal test operations, this is where the test is monitored from the ground. UCAs 45-48 indicate a standard level of interaction between a test pilot and the control room.

Since the SUAS is being piloted remotely, some may believe that integrating the control room with the ground station would be wise; safety constraint 45, however, indicates that this may not be the best decision, as all of the control room activity may result in a UCA 45.

(UCA 45) The Test Unit provides guidance to the pilot that is excessive, redundant, or distracting. [H1, H2, H3, H4, H5]

SUAS Pilot

STPA has been applied extensively to flight operations. The 14 UCAs found for the SUAS pilot are consistent with those found in other analyses. This indicates that the actions themselves are the same regardless of whether the pilot is seated inside the aircraft or outside; however, the next step of this analysis indicates that the causes of the actions differ significantly.

SUAV OCCUPIED AIRSPACE

SUAV and Other Aircraft

The only two controllers that have the ability to directly influence the SUAV Occupied Airspace are the SUAV and the controller. In many ways, their UCAs are exact inverses of each other. Table 5 compares 4 of the SUAV UCAs to the 4 Other Aircraft UCAs.

SUAV Unsafe Control Action	Other Aircraft Unsafe Control Action
(UCA 63) The SUAV maneuvers when then maneuver takes it out of its assigned airspace. [H1, H3]	**(UCA 71)** The other aircraft maneuvers when the maneuver takes the other aircraft into SUAV Occupied Airspace. [H1, H3]
(UCA 64) The SUAV does not maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]	**(UCA 72)** The other aircraft does not maneuver when a maneuver is needed to keep the other aircraft out of SUAV Occupied Airspace. [H1, H3]
(UCA 65) The SUAV maneuvers too late to stay in its assigned airspace. [H1, H3]	**(UCA 73)** The other aircraft maneuvers too late to stay out of SUAV Occupied Airspace. [H1, H3]
(UCA 68) The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]	**(UCA 74)** The other aircraft releases its payload when the payload will enter SUAV Occupied Airspace. [H2, H4]

Table 5. Selected SUAV and Other Aircraft UCAs.

Essentially, the SUAV and the other aircraft are the same controller with different goals. The SUAV wishes to remain inside of the SUAV Occupied Airspace at all costs, while the Other Aircraft wishes to remain outside of the SUAV Occupied Airspace at all costs. Both are capable of maneuvering and not releasing the payload in order to avoid the boundary.

The nature of allowing SUAS test in R-2515, however, would result in the boundaries of the SUAV Occupied Airspace shifting with time as the SUAV continues along its route. The other aircraft must be kept aware of this boundary if it is expected to remain on the outside of it.

Payload Release

UCA 68 states:

(UCA 68) The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]

This wording may be somewhat confusing. If the SUAV Occupied Airspace is the area that the SUAV can influence, then the area surrounding the payload following a payload release would be included in the SUAV Occupied Airspace. This inclusion prevents H3: Debris Impact in the Air and H4: Debris Impact on the Ground. Other aircraft avoid this by remaining outside of SUAV Occupied Airspace.

SUMMARY

STPA Step 1 determines when the control actions shown in the hierarchical control structure may pose a hazard to the system. There are 4 possibilities as far as how a control action may become unsafe:

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long.

Once these unsafe control actions have been determined, they can be used to develop system constraints, or design requirements.

Step 1 was carried out for both stages of this system and is shown in its entirety in Appendix B. 25 UCAs were found for the non-flight stage, and 49 were found during the flight operations stage.

The non-flight stage UCAs emphasized the need for feedback to be checked as a part of the approval process, as well as the need to monitor operations and rescind approval if new information comes to light that casts doubt on a test safety plan. The SPORT Prebrief was also shown to be an essential part of the pre-flight planning. Some efficiency controls were also discovered, and include the requirement that the overall mission objectives be made clear early in the test planning process.

The flight operations stage yielded some expected results, such as the UCAs involving the control room at the Test Unit or the SUAS Pilot. It also generated several requirements for the air traffic control facilities, incorporating handoffs, clearances, and traffic advisories. The UCAs for the SUAV and the other aircraft were shown to be tied closely to one another.

CHAPTER 5: CAUSES OF UNSAFE CONTROL ACTIONS

After the potentially unsafe control actions have been identified, STPA then proceeds to systematically search out potential causes of each of these UCAs. The potential causes are evaluated and solutions are generated in order to prevent the UCA from occurring. If no solution is found, the cause is refined further until solutions are possible. This chapter starts by describing STPA Step 2 and then applies this technique to one of the UCAs found in Appendix B and discussed in Chapter 4. Following this example case, several of the causal scenarios and safety recommendations found in the full Step 2 Analysis are discussed. The chapter ends with a summary of the findings.

SPTA STEP 2

After STPA Step 1 has discovered the possible unsafe control actions that may occur, Step 2 then identifies potential causes of those UCAs. This is the step that determines how the UCAs may arise. This is done by generating scenarios through which a reasonable person would expect that the UCA may occur. Leveson uses a control loop to demonstrate possible factors that build a scenario, shown in Figure 6.

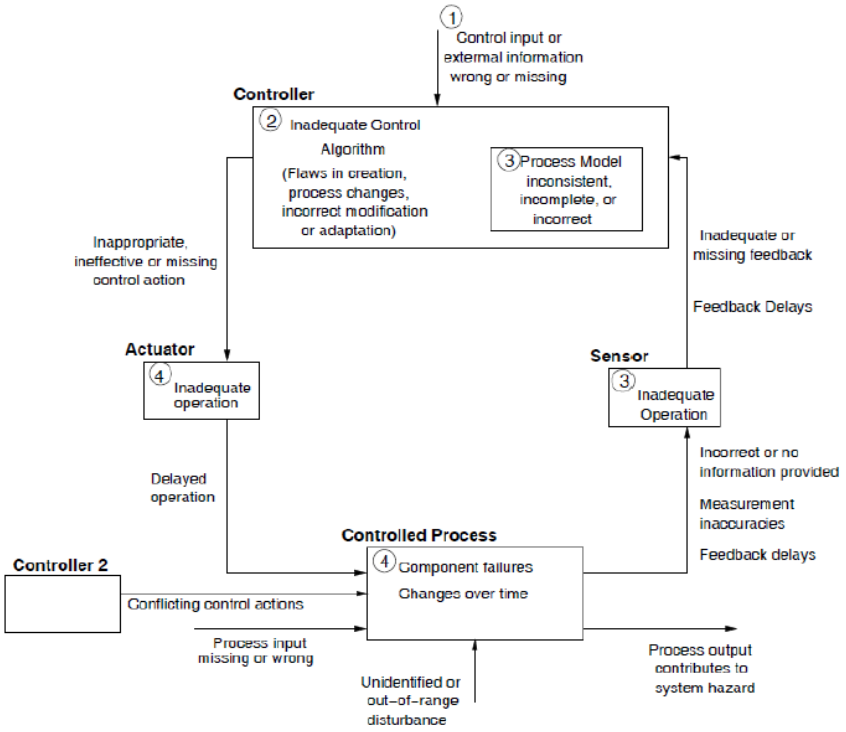

Figure 6. Causal Factors According to Leveson. (2)

This method, however, usually took an unstructured approach and was more similar to brainstorming than to systemically analyzing the potential causes of each UCA. In order to provide a step-by-step approach to STPA Step 2, John Thomas proposed an alternative approach (11). According to Thomas, there are four basic types of causal scenarios:

A. **Inadequate Control Execution**.

- Correct control action is given by the controller.
- Incorrect control action is received by the controlled process.

B. Inappropriate Decision

- Correct feedback is received by the controller.
- Incorrect control action is given by the controller.

C. Inadequate Feedback and Other Inputs

- Controlled process is behaving correctly.
- Incorrect feedback indicates to the controller that the controlled process is behaving correctly.

D. Inadequate Process Behavior

- Correct control action is received by the controlled process.
- Controlled process behaves incorrectly.

Each UCA is examined in the context of each of these basic scenarios. If a solution to prevent the high-level, basic scenario is readily apparent, then this solution serves as the end point of the analysis. Otherwise, the basic scenario is refined further into multiple lower level scenarios. In essence, a bullet is added between the two from the basic scenario that explains how this breakdown may occur. This iterates until solutions are found. Thomas's method has the additional advantage that scenarios from all parts of Leveson's feedback loop are considered, and solutions are able to be organized and traced. (11)

Thomas's method was used to complete a Step 2 Analysis for each of the 74 UCAs found in Step 1. The full analysis is found in Appendix C.

Full Step 2 Analysis of UCA 58

UCA 58: The SUAS Pilot provides payload commands when the payload should not be released. [H2, H4]

First, this UCA is examined in the context of each of the four basic scenarios:

A. Inadequate Control Execution: The SUAS pilot does not provide commands, but the SUAV receives commands.
B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate payload commands.
C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will incorrectly affect SUAV payload.
D. Inadequate Process Behavior: SUAS Pilot correctly does not provide payload commands, but the SUAS executes them. Solution: Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

Since there is a solution to basic scenario D, there is no need to further refine this scenario and discover additional causes. Scenarios A, B, and C, however, require further refinement. An intermediate step is added to clarify the cause of each of these scenarios, as shown below:

1. Inadequate Control Execution: The SUAS pilot does not provide commands, but the SUAV receives commands.
    i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
    ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.
2. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate payload commands.
    i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.
    ii. Refinement 2: Pilot is unaware of proper payload drop procedure(s). Solution: SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission.
3. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will incorrectly affect SUAV payload.
    i. Refinement 1: SUAS Pilot is unaware of the SUAV payload status. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
    ii. Refinement 2: SUAS Pilot is unaware of the appropriate drop zone or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
4. Inadequate Process Behavior: SUAS Pilot correctly does not provide payload commands, but the SUAS executes them. Solution: Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

At this point, solutions have been found for all of the causal scenarios so the STPA Step 2 analysis is complete. The 7 safety recommendations that result from this analysis are:

- Prior to flight testing, the command software should be tested on the ground.
- Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.
- The system has some sort of verification or check before sending any payload commands.
- SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission.
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
- SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
- Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

CAUSES OF UCAS IN NON-FLIGHT STAGES

126 causal scenarios were found for the 25 UCAs in non-flight stages. These scenarios generated a total of 66 Safety Design Recommendations. The causal scenarios generally fell into one of four categories: feedback, clarification, follow-up, and guidance/training, with 54 left over and not falling neatly into one of these categories.

The full list of causal scenarios and the solutions that were found is listed in Appendix C.

SCENARIO CATEGORIES

Lack of Feedback

Eleven of the causal scenarios can all be generalized as occurring due to a lack of feedback between the Test Unit and the 412 OG. These scenarios (except for 11.B and 11.C) are all related to the safety package approval, where the feedback also serves as a control action, or a way for the 412 OG to act on the test unit and influence the safety planning process. This further emphasizes that the safety planning process must be iterative and there must be an ongoing dialogue between the two levels of the organization, until a final safety plan has been agreed on. The safety recommendations that were found to alleviate these scenarios are:

- 412 OG must provide feedback on why safety plan was not approved. [UCA 3.D.ii, 5.D.ii]
- 412 OG must provide this feedback (on concerns other than safety, such as cost or resources) to the Test Unit so that they can adjust their test plan. [UCA 4.B.i, 19.D, 20.D]
- SPORT/JOSHUA inform 412 OG when the guidance becomes excessive or redundant. [UCA 11.B, 11.C]
- SPORT/JOSHUA provide this feedback (when the safety plan did not contain information that is relevant to air traffic controllers) to 412 OG, who can inform the appropriate Test Unit. [UCA 9.C]
- Test Unit must be made aware of the reason(s) the plan was not approved, and given the chance to provide an updated or corrected plan. [UCA 4.C.iii, 19.A, 21.A]

Lack of Clarification

Ten additional safety recommendations can be generalized as providing clarification, and alleviate an additional 19 causal scenarios. The clarification takes the form of questions in three of the solutions:

- 412 OG must ask questions until their concerns are addressed. [UCA 4.C.i, 19.D, 20.D]
- 412 OG must ask questions until they thoroughly understand the safety plan. [UCA 1.C.i. 2.C.i, 3.C.i]
- Test Mission Objectives are presented as a conversation, with the SUAS pilot able to ask clarifying questions. [UCA 24.A]

Four of the scenarios encourage that paperwork be clearly labeled, reducing confusion over which version is being received or reviewed.

- Safety package submitted for final approval should be clearly labeled as such. [UCA 19.B.ii]
- Schedule must be marked as a draft or complete when it is given to 412 OG. [UCA 18.C]
- SPORT/JOSHUA inform the ROC of what version of the schedule they are using. [UCA 18.A, 18.D]
- Schedule must be marked as a draft or complete when it is given to 412 OG. [UCA 8.C]

The final three clarification solutions attempt to clarify the intent behind the feedback and make it clear to the controller what the correct action should be.

- Test Unit must document reasons the SRB feedback has been addressed and is considered unimportant. [UCA 21.B.i]
- The ROC clearly indicates whether or not testing may proceed as requested. [UCA 13.A, 13.D, 16.A, 16.D]
- When the additional information is presented to the 412 OG, it should be in such a way that the safety implications are clear. [UCA 6.B.i, 6.C]

These 10 safety recommendations all attempt to present information in a way such that the recipient is left with no doubts about what information they have received and what actions they should take about it.

Lack of Follow-Up Checks

One of the simplest methods of solving a Type A causal scenario, where the correct control action is given by the controller but not received by the controlled process, is by conducting a follow-up check. This check ensures that the control action successfully reached the controlled process, and allows the controller to re-send the command immediately if it has failed to do so. The following five safety recommendations are all a form of follow-up check:

- The Test Unit periodically reviews the test and safety plan to ensure that mission objectives are being met. [UCA 24.D, 25.D]
- SPORT/JOSHUA inform 412 OG of what version of the schedule they are using. [UCA 8.D]
- Test Unit confirms that ROC received and acted on the schedule request. [UCA 22.A, 22.D]
- Test Unit confirms that SPORT reviewed the prebrief. [UCA 23.A, 23.D]
- Test Unit must follow up with 412 OG if approval is not received in an appropriate amount of time. [UCA 4.A, 4.B.ii, 19.D, 20.A, 20.D]

In some control process models, there are many inputs that must be considered before the correct action can be taken. When these controllers are human, it is easy for one of the inputs to be forgotten or remembered incorrectly. In these cases, the check acts as the controller gaining additional inputs to update their mental model, or process model, to ensure that the correct output is selected. Since the ROC has to handle a complex scheduling problem, it is recommended that the ROC check certain aspects before deciding. The following four safety recommendations address this.

- Before indicating that the Test Unit may proceed, the ROC must check the requested time and airspace. [UCA 14.C, 15.C]

- Before indicating that the Test Unit must reschedule or relocate, the ROC must check the requested time and airspace. [UCA 13.C, 16.C]
- The ROC must check which airspaces cannot be simultaneously active before scheduling missions. [UCA 14.B.i, 15.B.i]
- The ROC must check which mission has priority access, according to EAFBI 13-100. [UCA 13.B.ii, 16.B.ii]

Altogether, these checks address 20 of the causal scenarios that may lead to an UCA in the non-flight stages of the mission.

Lack of Guidance/Training

Another way to form a more correct process model is to provide the controller with additional guidance, training, or procedures. In this way, the controller is better able to recognize the correct action from the inputs and feedback that the controller receives. The following four recommendations, which alleviate a combined 10 causal scenarios, fall into this category.

- 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training. [UCA 1.C.ii, 2.C.ii, 3.C.ii, 4.C.ii, 5.C.ii, 19.D, 20.D]
- Test Unit representative(s) involved in the safety review process must undergo Hazard Analysis training. [UCA 21.C.ii]
- 412 OG must provide guidance on how to incorporate the airspace schedule into planning control operations. [UCA 7.D]
- 412 OG must provide guidance on how to incorporate the safety information into control operations. [UCA 10.D]

In the case of a human operator, having a set procedure or checklist also helps to prevent slips or lapses form occurring. Eight additional safety recommendations establish these procedures or checklists to ensure that steps are not skipped during flight planning. They address 12 more of the causal scenarios.

- 412 OG must always pass on the airspace schedule, regardless of its importance. [UCA 7.B.i]
- 412 OG must establish a standard procedure to ensure that the information is passed on. [UCA 10.B.ii]
- 412 OG must establish a standard procedure to ensure that the schedule is passed on (specific person, time of day, etc.). [UCA 7.B.ii]
- Ensure personnel are aware of all steps in pre-mission planning. [UCA 22.B.i, 23.B.i]
- The ROC must establish a standard procedure to ensure that the step (issuing an Operations Number) is not skipped. [UCA 16.B.iii]
- The ROC should develop a way to track what airspace each mission requested. [UCA 13.B.i, 16.B.i]
- The Test Unit designates a project representative who is kept aware of what stage the test planning is in. [UCA 22.C, 23.C]
- The Test Unit must establish a standard procedure or checklist to conduct all pre-mission scheduling. [UCA 22.B.ii, 23.B.ii]

UNIQUE CAUSAL SCENARIOS

While over half of the safety recommendations fall into one of the four categories above, 30 of the 66 safety recommendations, which account for 54 of the 126 causal scenarios in this stage, do not fit.

Outside Pressures

Six of the causal scenarios involve the test unit or the 412 OG knowingly approving a faulty test plan. This is most likely due to the influence of outside pressures, which are attempting to expedite testing. This can be mitigated by forming a safety culture, where safety remains a high priority, but cannot ever be truly eliminated as a potential cause of a UCA.

If outside influences are attempting to rush testing, both the test unit and the 412 OG must maintain vigilance and ensure that safety standards do not slip.

Iterative Safety Process

Four additional scenarios can occur if the safety review is not iterative. If the safety review stops after only one round, there is a potential for there to still be flaws that have not been addressed. A second review of the safety plan after the first round of feedback has been incorporated into the plan, these flaws have a better chance of being discovered and corrected.

412 OG Staffing

One of the recommendations in the guidance category above is

- 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training. [UCA 1.C.ii, 2.C.ii, 3.C.ii, 4.C.ii, 5.C.ii, 19.D, 20.D]

This is important because many members of the 412 OG staff may have little to no background in hazard analysis or engineering. Another recommendation regarding the staffing of 412 OG is

- A control facility representative is on hand to determine what information is necessary. [UCA 9.B.i, 10.B.i, 12.B.i]

This is necessary because, in most cases, the 412 OG commander is a pilot who may not have a thorough understanding of how air traffic control operations work. Since ATC operations are a critical part of any SUAS safety plan, having a control facility representative present will provide more feedback regarding the safety plan, and will be able to distinguish which aspects of the safety plan are important enough to pass on to SPORT or JOSHUA.

Airspace Scheduling

Some airspace, such as the impact range, may be scheduled for multiple simultaneous test missions on a regular basis. EAFBI 13-100 specifies the procedure for aircraft using these ranges; ultimately, the aircraft must maintain visual separation from one another.

Since this is not possible for the SUAS, the ROC should adjust their operations to ensure that a SUAS test mission is not scheduled in one of these areas concurrently with any other testing.

CAUSES OF UCAS IN FLIGHT OPERATIONS STAGE

The STPA Step 2 Analysis of the Flight Operations Stage discovered 284 causal scenarios and generated an additional 74 safety recommendations.

COMMUNICATION

A communications link can be a powerful tool in preventing several of the UCAs from occurring. 17 safety recommendations were found that involve ensuring that the lines of communication remain open, and fall into two categories: clarification and confirmation.

Used to Clarify

Communication, especially voice communication where immediate feedback is possible, serves as a way to reduce confusion and provide a better mental model to the controller. This communication must be conducted in such a way that it provides meaningful feedback and does not distract the controller from the task at hand. The following 6 safety recommendations address this aspect of communication, and address a total of 23 causal scenarios.

- Pilot asks for guidance, or if guidance is not available, uses his/her best judgement. [UCA 46.C, 47.C, 48.A, 48.B.ii, 48.C]
- Pilot has the authority to ask for less communication. [UCA 45.B, 45.C]
- Pilot is encouraged to ask questions. [UCA 46.A.ii, 47.A.ii]
- Pilots must contact SPORT/JOSHUA before transitioning to SPORT/JOSHUA airspace. [UCA 27.C, 36.C]
- SPORT/JOSHUA immediately contacts JOSHUA/SPORT to advise them of the situation. [UCA 26.D, 27.D, 28.D, 29.D, 35.D, 36.D, 37.D, 38.D, 39.D]
- Test Unit appoints one person to communicate directly with the pilot during the test If communication is not possible, pilot uses his/her best judgement. [UCA 45.A, 46.A.i, 47.A.i]

If a response is not received, then voice communication can easily be repeated in a second attempt to relay the necessary information or command. Five additional safety recommendations address 26 causal scenarios in which the control action is not received or acted upon by first repeating the radio call, then by taking other actions as appropriate.

Used to Confirm

Communication can also be used as a feedback tool, wherein the controller is able to receive confirmation that the command action was received correctly. This is often accomplished in the aviation community by a procedure called “read back,” which involves the recipient of a message repeating critical information verbatim. Six safety recommendations, solving 19 causal scenarios, make use of these read backs or verbal confirmation in order to ensure that the message was correctly received.

- Pilot is informed while the Test Unit works on the problem. In the interim, the pilot uses his/her best judgement. [UCA 46.B, 47.B, 48.B.i]
- Pilot must receive confirmation before changing radio frequency. [UCA 26.A, 35.A]
- Pilot must receive confirmation before entering the airspace. [UCA 29.A, 39.A]

- SPORT/JOSHUA confirms that both aircraft have the other in sight. [UCA 32.B.i, 33.B.i, 34.B, 42.B.i, 43.B.i, 44.B]
- SPORT/JOSHUA confirms that the aircraft is the one that requested access. [UCA 31.B.ii, 41.B.ii]
- When giving an airspace clearance, SPORT/JOSHUA specifies which airspace the clearance is for. [UCA 29.B, 30.B, 39.B, 40.B]

MONITORING

SUASs present unique challenges when it comes to monitoring the status of the vehicle. This difficulty can lead to 43 possible causal scenarios, posing difficulties for both the SUAS Pilot and the air traffic controllers.

Air Traffic Controllers

SPORT and JOSHUA are responsible for monitoring the airspace that they are controlling, which includes knowing the position and the intentions of the aircraft in that airspace. Since SUAS may not be large enough to carry a transponder, some other method must be developed that allows the ATC to check the location of the aircraft. This capability is tied to the following five safety recommendations:

- Airspace must be checked before providing or denying clearance. [UCA 29.C, 30.C, 39.C, 40.C]
- Before an airspace becomes unsafe, SPORT/JOSHUA checks to ensure that it is empty. [UCA 31.B.i, 41.B.i]
- SPORT/JOSHUA should continuously monitor any aircraft that is encroaching on another's airspace. [UCA 34.C, 44.C]
- SPORT/JOSHUA should periodically check the location and direction of all aircraft in their airspace (checks should occur more frequently as traffic increases). [UCA 32.C, 33.C, 42.C, 43.C]
- SPORT/JOSHUA should periodically check which sections of the airspace are off-limits, "active," or otherwise unsafe. [UCA 31.C, 41.C]

Flight Commands

Potentially more important than the ATC's ability to monitor the position of the SUAV is the ability of the pilot to monitor various aspects of the SUAV. In a manned aircraft, the pilot may be able to use visual or other sensory cues to detect things such as the aircraft's location, orientation, and approximate speed.

Operating a SUAS without having a direct line of sight to the vehicle robs the SUAS pilot of these sensory inputs. Essentially, the SUAS pilot is attempting to fly the SUAV using only his or her instruments. While this is possible, and indeed common for experienced pilots, it is not a safe method when the instruments themselves remain untested or unproven. This necessitates an outside source of feedback to the pilot, such as a spotter or a chase aircraft that has line of sight contact with the SUAV, a ground radar unit capable of detecting the vehicle, or other possible sources of information. These sources must be able to relay information that includes the SUAV's

location, orientation, speed, and payload status to the pilot. If the SUAV's reported sensor readings differ from the observer's report, the pilot must also have the ability to override the SUAS programmed route. 29 causal scenarios can be solved by this simple safety recommendation.

PROCEDURES

Handoff Procedures

Many of the JOSHUA and SPORT scenarios involve handoffs of aircraft or airspace. The step 2 analysis found four safety recommendations that should be incorporated into this procedure.

- Aircraft hand offs must happen before the aircraft crosses the boundary. [UCA 28.B.i, 38.B.i]
- Airspace hand offs must happen before the aircraft crosses the boundary. [UCA 27.B.i, 36.B.i]
- Nearby Traffic must be checked before conducting a hand off. [UCA 26.C, 28.C, 35.C, 38.C]
- Wait until traffic is deconflicted before conducting a hand off. [UCA 26.B, 35.B]

Necessary Guidance

Similarly, 17 of the causal scenarios generated 7 safety recommendations that should be incorporated into general R-2515 guidance.

- 412 OG provides guidance on what the acceptable distance between aircraft is. [UCA 32.B.ii, 33.B.ii, 42.B.ii, 43.B.ii]
- 412 OG provides training on IFR clearances. [UCA 37.B.i]
- 412 OG will enforce payload test guidance in EAFBI 13-100. When SUAV is undergoing payload drop testing, no other aircraft will be allowed into the impact range. [UCA 74.B, UCA 74.C]
- 412 OG will establish clear guidance for pilots in R-2515 that they should never enter SUAS occupied airspace, even when the SUAV is in sight. [UCA 71.B, 72.B]
- 412 OG will establish clear guidance for pilots in R-2515 that they should maneuver conservatively near the SUAS airspace boundaries. [UCA 73.B]
- Aircraft undergoing payload or drop testing will not overfly SUAV Occupied Airspace. [UCA 74.A, 74.D]
- ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests. [UCA 71.A, 71.D, 72.D, 73.A, 73.D]

SUAS TESTING

SUAS Programming

Each SUAS is unique, and this analysis left the specifics of the SUAS software as generic as possible. Even without the specific structure of the SUAS software, the Step 2 analysis found 11 safety recommendations that should be incorporated into the SUAS software.

As expected, the Step 2 analysis generated recommendations to establish lost link procedures and reduce software lag.

- Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot. These commands should not

involve deploying the payload. [UCA 50.A.ii, 52.A.ii, 53.A.ii, 55.A.ii, 56.A.ii, 57.A.ii, 61.A.ii, 62.A.ii]
- Attempt to reduce software lag. [UCA 65.B]

In addition, some of the critical commands should be verified either before they are sent or after they are received. Six recommendations for command verification were found.

- Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands. [UCA 49.B.ii, 51.A.ii, 54.A.ii, 58.A.ii, 59.A.ii, 60.A.ii]
- Do not allow payload drops without the location being confirmed by the pilot. [UCA 68.C.i]
- Ensure that the SUAS software allows the pilot to check the sensor status. [UCA 60.C]
- Have an inhibitor that keeps the pilot from dropping the payload when he/she does not intend to. [UCA 68.C.ii]
- The system has some sort of verification or check before sending complex commands. [UCA 49.B, 51.B, 52.B, 53.B, 54.B, 56.B, 57.B]
- The system has some sort of verification or check before sending any payload commands. [UCA 58.B.i, 59.B.i, 60.B.i, 61.B.i, 62.B.i]

Finally, the more complex SUAS programs have recommendations on how to handle airspace boundaries. When a SUAS incorporates any form of autopilot software, these three recommendations would apply.

- Prior to testing, ensure airspace boundaries are accurate. [UCA 63.B.i, 64.B.i]
- SUAV should be programmed not to cross an airspace boundary while in the process of deploying a payload, unless the pilot specifies this course of action. [UCA 61.D]
- SUAV should be programmed to never violate an airspace boundary without pilot authorization. [UCA 63.B.ii, 64.B.ii]

Altogether, 35 of the causal scenarios were due to flaws in the SUAS programming. These solutions help to alleviate those causes of UCAs.

Build Up Testing

One of the fundamental approaches to testing is to conduct build-up testing, where systems are tested in relatively simple, safe environments before proceeding to more complex tests. The STPA Step 2 analysis discovered 18 causal scenarios whose likelihood is significantly reduced it the build-up approach is used. The specific safety recommendations are:

- Payload drop hardware/connectors should be tested on the ground extensively before being tested inflight. [UCA 68.D, 69.D, 70.D]
- Payload drop software should be tested on the ground extensively before being tested inflight. [UCA 68.B]
- Prior to flight testing, the command software should be tested on the ground. [UCA 49.A.i, 50.A.i, 51.A.i, 52.A.i, 53.A.i, 54.A.i, 55.A.i, 56.A.i, 57.A.i, 58.A.i, 59.A.i, 60.A.i, 61.A.i, 62.A.i]

The software ground testing may also take on a build-up approach, with the program first running on a computer, then proceeding to communicate between two computers (with one simulating the ground control station and the other the SUAV), and finally between the actual ground control station and the actual SUAV on the ground before flight is attempted. The communications link between the ground control station and the SUAV should also be tested before flight is attempted.

Emergency Procedures

In some cases, prevention is not possible. If this is the case, steps should be taken to mitigate the effects. In flight operations, the steps taken following a mishap are sometimes referred to as emergency procedures (EPs). The STPA Step 2 found 9 suggested emergency procedures:

- Other aircraft pilot attempts to regain control of the aircraft and exit the airspace. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot. [UCA 71.A, 72.A, 73.A]
- Other aircraft pilot attempts to regain control of the aircraft and exit the airspace as quickly as possible. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot. [UCA 71.D, 72.D, 73.D]
- Send command a second time, then stop testing, minimize flight over structures or people, and land and modify software or hardware. [UCA 69.A, 69.D, 70.A, 70.D]
- Stop testing immediately and determine the cause of the deviation. [UCA 49.D, 50.D, 51.D, 52.D, 53.D, 54.D, 55.D, 56.D, 57.D, 60.D]
- Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people. [UCA 58.D, 59.D, 62.B.ii, 62.D]
- Have pilot send an overrule payload drop command. [UCA 69.B, 70.B]
- Stop testing immediately and modify hardware. [UCA 63.A.ii, 64.A.i, 66.A.ii, 67.A.ii]
- Stop testing immediately and modify software. [UCA 63.A.i, 64.A.i, 66.A.i, 66.B, 67.A.i, 67.B]
- Stop testing, minimize flight over structures or people, land and modify software. [UCA 69.B, 70.B]

These EPs are intended to rectify a situation that has already deviated from what is expected. These include loss of control of an aircraft/SUAV, payload drop malfunctions, and generally, any time that the vehicle is not able to be controlled. Since these must be able to be implemented when other aspects of the aircraft have failed, the programming must be able to handle these emergencies. For example, even if one of the control servos is stuck, the pilot should still be able to force the SUAV to land.

SUMMARY

STPA Step 2 finds potential causes of unsafe control actions and generates safety recommendations to combat the causal scenarios that were found. John Thomas states that there are 4 basic types of causal scenarios:

A. Inadequate Control Execution.
B. Inappropriate Decision
C. Inadequate Feedback and Other Inputs

D. Inadequate Process Behavior

If a solution to the basic causal scenario is not found, then that scenario may be further refined into a more detailed scenario, to the level where a solution is possible.

A full step 2 analysis was performed and is shown in its entirety in Appendix C. 141 safety recommendations were found.

In the non-flight stages, over half of the causal scenarios are due to a lack of feedback, lack of clarification, lack of guidance, and lack of follow-up checks. Additional causes of UCAs in the Non-Flight Stage include outside pressure to conduct the test and a lack of iteration in the safety planning process.

During the flight operations stage, the majority of the scenarios were due to a lack of communication, lack of monitoring, lack of guidance or procedures, or improper test planning. Although this analysis did not provide any specifications when it came to the SUAS software, 11 software safety recommendations were found. In addition, 9 suggested emergency procedures were found.

CHAPTER 6: DISCUSSION – STPA FINDINGS

With the results of the STPA analysis, the next step is to produce meaningful action items that can be implemented to improve the safety of the Edwards airspace. First, the results of the non-flight stages are compared to the current guidance in AFTCI 91-202 and the results of Nicholas Chung's STPA analysis of the AFTC Safety Management System. The results of the flight operations stage are then compared to the current guidance on UAS operations at Edwards AFB in EAFBI 13-100. A summary of the action items found concludes the chapter.

SAFETY PLANNING PHASE DISCUSSION

The official Air Force Test Center Test Safety Review Policy is presented in AFTCI 91-202. This analysis focuses on what AFTCI 91-202 calls the Review, Coordination and Approval, Execution, Revisions, Feedback, and Test Completion phases. Nicholas Chung performed a full SPTA analysis of the entire system in 2015; since Chung identified all of the requirements listed in 91-202, Chung's analysis will be the primary point of comparison with this thesis.

One of the common threads that ran through this analysis is the necessity that the safety review process be iterative and continues to iterate until all parties agree that the plan is sufficient. Then and only then should final approval be given. While Chung's control structure shows the presence of feedback loops, the importance of the iteration is not found. (4) AFI 91-202 also emphasizes the need for feedback following the SRB, but does not provide a structure for future iterations. (9) This leads to the first action item:

Action Item 1: *The Air Force Test Safety Center should revise the safety review documentation to clarify that this should be iterative. A structured way of iterating the safety plan should be developed.*

The analysis also shows the importance of clear communication in this phase. During the review and approval process, it is necessary for everyone present to have a full understanding of the safety plan and to ask questions if anything is unclear.

Communication can also apply to version control on the documents that are used to communicate. This was also discovered by Chung, who suggests that a formal way to track and close action items would be helpful. (4) The analysis that is presented here only serves to emphasize that this can be a safety concern, as some action items may be forgotten.

The analysis recommended that 412 OG representative(s) undergo hazard analysis training, and that a control facility representative be present to provide a controller's point of view. These findings are echoed by Chung, who recommends that hazard analysis training should be developed and provided, and that "reviewers have adequate subject matter knowledge" to review the safety plan. (4)

STPA identified that outside pressures may impact the safety project. AFI 91-202 states that the safety plan must be reviewed by independent reviewers, who are not subjected to the same pressures as the test unit. (9)

Pre-Flight Stage Discussion

This analysis led to several conclusions regarding the Resource Operations Center (ROC); however, the guidance available in EAFBI 13-100 is limited to "The Operations Number issued by the 412th Operations Support Squadron's (412 OSS) Resource Operations Center (ROC) authorizes crews to depart from, re-enter, and operate within R-2515 when the airspace has been scheduled for military use." (5) This analysis assumes that the ROC maintains some sort of record of missions requesting access and can provide this to the 412 OG. If this is not accurate, then the analysis still holds as all of the requirements and recommendations relating to the ROC only involve inefficient operations. Additional guidance for the ROC is no doubt available locally; however, its absence in EAFBI 13-100 leads to the second action item:

Action Item 2: *The 412th Operations Support Squadron should formalize the procedure to issue an Operations Number. The recommendations and requirements in this analysis should be incorporated in the procedure.*

Another pre-flight scheduling task is the SPORT prebrief. EAFBI 13-100 lists where to find this form and a fax number to which the completed form must be sent. According to the EAFBI, this should be accomplished "as early as possible." The EAFBI also indicates that these sheets are used by the watch supervisor to create a deconfliction plan for the day, which must be approved by the supervisor of flying (who oversees both SPORT and JOSHUA). This plan must be completed prior to the first takeoff, and is updated as required throughout the day. The combination of the prebrief sheet and the airspace clearance given prior to entering R-2515 are used to "proactively deconflict R-2515." (5) This guidance covers many of the SPORT requirements and recommendations found through STPA, but a modification to the form may be necessary for SUAS Operations.

Action Item 3: *SUAS Operations must indicate the SUAV's programmed lost link procedures on the SPORT prebrief sheet, as well as any other details from the safety plan that SPORT may need to be aware of.*

Action Item 4: *The watch supervisor must review relevant safety information passed from 412 OG while creating the day's deconfliction plan.*

Flight Operations Stage Discussion

EAFBI 13-100 divides UASs into five types, based on how they can interact with other aircraft, and specifies certain special handling procedures to be used with each type. An UAS is assigned a type designation in the course of the safety review process. (5) The primary factor that designates a specific type category is the ability of the UAS to avoid other traffic. EAFBI 13-100 specifies that any capabilities must be tested before they can be included in type categorization. The types are defined as follows:

Type 1: UAS has the ability to conduct sense and avoid to an equivalent level of capability as a manned aircraft.

Type 2: UAS is able to detect traffic that is at minimum broadcasting a transceiver code and take appropriate action in a timely manner. This process includes only the UAS and the UAS Operator, without any outside input.

Type 3: UAS is able to detect traffic that is at minimum broadcasting a transceiver code and communicating with ATC, but the UAS cannot react in a timely manner. This type of UAS usually relies on ATC monitoring and/or a chase aircraft to detect other aircraft in the area, but can also include UAS with a long delay in communications.

Type 4: UAS is unable to deviate from the flight path. ATC must detect the conflict and direct the conflicting traffic to maneuver. An ATC transponder is required in this type category.

Type 5: UAS is unable to deviate from the flight path and ATC cannot accurately track the UAS. (5)

The UAS is also labeled according to what stage of development the system is in. Depending on the type and development stage, EAFBI 13-100 directs that the UAS receive the special procedures listed in Table 6. A description of each mitigation technique follows the table. Mitigations relating to taxi, takeoff, and landing are not included.

	Type 1	**Type 2**	**Type 3**	**Type 4**	**Type 5**
Mature	No special procedures	(Airspace Bubble)	(Airspace Bubble) and (Traffic Avoidance)	(Airspace Bubble) and (Traffic Avoidance)	(Exclusive Use Airspace) Or (Airspace Bubble), (Chase Aircraft), and (Traffic Avoidance)
Provisional	(Airspace Bubble)	(Airspace Bubble)	(Airspace Bubble) and (Traffic Avoidance)	(Airspace Bubble) and (Traffic Avoidance)	(Exclusive Use Airspace) Or (Airspace Bubble), (Chase Aircraft), and (Traffic Avoidance)
Experimental	(Airspace Bubble), (Limited Ground Footprint), and (Flight Termination System)	(Airspace Bubble), (Limited Ground Footprint), and (Flight Termination System)	(Airspace Bubble), (Limited Ground Footprint), and (Flight Termination System)	(Airspace Bubble), (Chase Aircraft), (Limited Ground Footprint), and (Flight Termination System)	(Exclusive Use Airspace), (Limited Ground Footprint), and (Flight Termination System)
Unproven	(Exclusive Use Airspace) Or (Airspace Bubble), (Chase Aircraft), and (Sanitized Ground Footprint) And	(Exclusive Use Airspace) Or (Airspace Bubble), (Chase Aircraft), and (Sanitized Ground Footprint) And	(Exclusive Use Airspace) Or (Airspace Bubble), (Chase Aircraft), and (Sanitized Ground Footprint) And	(Exclusive Use Airspace), (Sanitized Ground Footprint), and (Flight Termination System)	(Exclusive Use Airspace), (Sanitized Ground Footprint), and (Flight Termination System)

	(Flight Termination System)	(Flight Termination System)	(Flight Termination System)		

Table 6. UAS Mitigation Matrix. (5)

The mitigation procedures are defined as follows:

Exclusive Use Airspace: Airspace dedicated to the sole use of the UAS mission. SPORT is responsible for directing non-participant traffic to avoid entering and advising the UAS pilot if there is an airspace incursion. UAS operations are required to remain within the confines of the airspace boundaries. (5)

Airspace Bubble: Aircrews shall remain clear of any UAS by 2000' vertical and 5 N< horizontal airspace bubble around the UAS. (5)

Traffic Avoidance: UAS pilot depends on ATC active monitoring to detect traffic and advise UAS pilot of all traffic conflicts and recommend avoidance maneuver. (5)

Chase Aircraft: Primary purpose may be to conduct see and avoid for both the UAS and the chase aircraft. If the chase aircraft is providing see and avoid functions, they will advise the UAS pilot of all traffic conflicts and recommend a course of action as appropriate. (5)

Flight Termination System: A fully redundant system that allows for control and/or flight termination of aircraft. (5)

Limited Ground Footprint: Geographic area on the ground with widely dispersed population and/or structures. Flight path is planned to minimize personnel risk exposure. (5)

Sanitized Ground Footprint: Geographic area on the ground actively cleared of all personnel. Risk is accepted to structures and vehicles remaining within the footprint in case of an aircraft crash. Flight path is planned to afford the maximum practical protection for personnel. (5)

EAFBI 13-100 addresses all of the guidance requirements found in the STPA analysis, and provides a standard set of responses that an aircraft pilot is expected to take in response to a UAS. By using a build-up approach, the UAS requires fewer safety mitigations as additional systems are proven to function correctly. All testing will help move the SUAS vertically in Table 6, and as sensors are proven, the UAS may achieve a lower type rating and move to the left as well.

What is not addressed in this instruction are the communication procedures between the aircraft and the air traffic controller. Standard communication procedures may be found elsewhere, such as FAA guidelines, but it should be reinforced in EAFBI 13-100.

Action Item 5: *Add guidance on read back requirements and other communication requirements between the Aircrew and SPORT to EAFBI 13-100.*

The current approach also takes a passive approach to monitoring the position of the aircraft. If the aircraft is not equipped with a transponder, then either a chase aircraft must be used or the UAS must be in exclusive use airspace. Other approaches to monitoring can be taken; for instance, if the

SUAS is reporting the UAV's location to the pilot, this can easily be relayed via a hardline link to the appropriate ATC facility.

Action Item 6: *Develop a way for SPORT to see the position that the SUAV is reporting to the pilot.*

This automatically shifts aircraft out of the Type 5 category. A final action item refines the exclusive use airspace in order to allow for more efficient operations.

Action Item 7: *Redefine Exclusive Use Airspace. For SUAS that have proven ability to hold a programmed route, other aircraft may enter the Exclusive Use Airspace if they (a) have the SUAV in sight and will maneuver to avoid a collision, and (b) are advised by SPORT on the SUAV's programmed/planned route.*

This allows a pilot to assume the burden of avoiding the SUAV, based on the fact that the SUAV's next series of maneuvers are known.

OTHER DISCUSSION

The 11 software requirements found are independent of SUAS type and how that particular vehicle's software functions. These requirements should serve as design requirements for any SUAS operating in the airspace; the flight termination system mentioned as a mitigation strategy is one method of providing pilot override capability.

Action Item 8: *Prior to any in-flight testing, the SUAS software should be tested to ensure that the 11 software requirements discussed in Chapter 5 are met.*

The emergency procedures should also be used to supplement any emergency procedures that are specific to the system. If the EPs for the system have not yet been developed, then the EPs discussed in Chapter 5 provide a good basis for development.

Action Item 9: *SUAS EPs must include those discussed in Chapter 5.*

SUMMARY

The following nine action items are proposed to better enhance Edwards AFB's ability to conduct SUAS operations:

Action Item 1: *The Air Force Test Safety Center should revise the safety review documentation to clarify that this should be iterative. A structured way of iterating the safety plan should be developed.*

Action Item 2: *The 412th Operations Support Squadron should formalize the procedure to issue an Operations Number. The recommendations and requirements in this analysis should be incorporated in the procedure.*

Action Item 3: *SUAS Operations must indicate the SUAV's programmed lost link procedures on the SPORT prebrief sheet, as well as any other details from the safety plan that SPORT may need to be aware of.*

Action Item 4: *The watch supervisor must review relevant safety information passed from 412 OG while creating the day's deconfliction plan.*

Action Item 5: *Add guidance on read back requirements and other communication requirements between the Aircrew and SPORT to EAFBI 13-100.*

Action Item 6: *Develop a way for SPORT to see the position that the SUAV is reporting to the pilot.*

Action Item 7: *Redefine Exclusive Use Airspace. For SUAS that have proven ability to hold a programmed route, other aircraft may enter the Exclusive Use Airspace if they (a) have the SUAV in sight and will maneuver to avoid a collision, and (b) are advised by SPORT on the SUAV's programmed/planned route.*

Action Item 8: *Prior to any in-flight testing, the SUAS software should be tested to ensure that the 11 software requirements discussed in Chapter 5 are met.*

Action Item 9: *SUAS EPs must include those discussed in Chapter 5.*

CHAPTER 7: CONCLUSION

The recent military climate places high stock in the use of unmanned systems, especially UAVs. Since UAVs are not able to operate under a standard VFR, "see-and-avoid" clearance, they must receive special treatment by air traffic controllers. A hazard analysis was conducted to ensure that the controllers are meeting all of the safety requirements necessary with SUAS operating in their airspace.

While many hazard techniques are available, Leveson's System-Theoretic Process Analysis was used. This technique was chosen because its systemic approach to safety was appropriate for the high level of analysis that was being conducted, and it also ensures that few, if any, safety requirements are missed. This thesis applied STPA to the current operations of the Edwards AFB airspace system. This helped to identify current potential issues with the system as well as the steps that must be taken to ensure that as testing shifts toward unmanned vehicles, flight operations remain safe.

The system is composed of the R-2515 airspace, controlled by the AFTC Military Radar Unit (SPORT), and operations involving SUAS as defined by the Department of Defense. Three mishaps and five hazards were defined in the context of this system. The flight testing was broken into two phases, both operating within a single control structure. The two phases were the non-flight phase and the flight operations phase.

The analysis proceeded for each of the two phases by first identifying the 74 possible UCAs. These UCAs were then transformed into system design requirements, or safety constraints. The constraints emphasized the need for an iterative feedback loop during the safety review phase, safety requirements for air traffic control operations, and other insights.

The 74 UCAs were each put through the next step of the STPA process, using Thomas's approach to scenario generation. This resulted in 141 safety recommendations, which again provided insights about the necessity of proper guidance to be in place and communication channels to be open during all phases of test planning. The ability to monitor the SUAV location also emerged as being one of the key components of system safety.

Even though the analysis was intentionally software-neutral when considering the SUAS, 11 software requirements were found. Additionally, 9 emergency procedures emerged. These should form the basis for any system that is attempting to test in the airspace, and should be confirmed well in advance of testing.

The results found in the STPA analysis were compared to the existing guidance in the form of AFTCI 91-202 for the safety review process and EAFBI 13-100 for flight operations. While the guidance in place addresses many of the safety requirements that were found, nine action items were listed that will better prepare Edwards AFB for SUAS operations.

Similar to how Chung performed a lower-level analysis of the AFTC Safety Management System, additional low-level analyses should be conducted to find more specific safety requirements. In particular, an analysis of the air traffic control system is encouraged, as this analysis was too high-

level to look into takeoff and landing operations, impact range operations, and other nuances of the R-2508 airspace. Use of STPA to conduct the hazard analysis portion of the safety review is also encouraged.

APPENDIX A: CONTROLLER DETAILS

The following sections describe the control actions and feedback received by each controller, as discussed in Chapter 3. The control structure is presented again below in Figure 7.

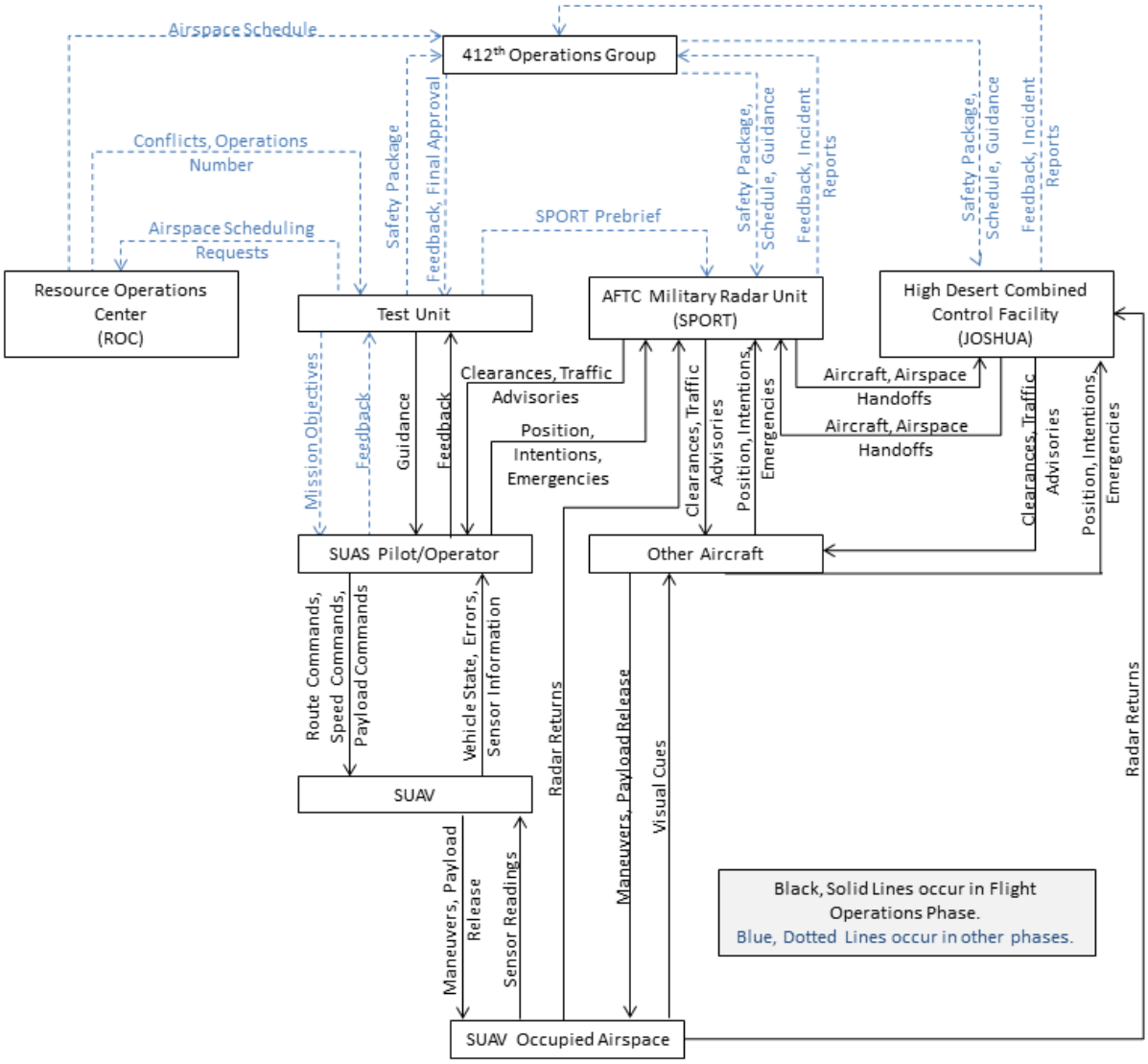

Figure 7. Hierarchical Control Structure.

NON-FLIGHT PHASE

412TH OPERATIONS GROUP (412 OG)

Control Action	Given To	Description
Feedback (Guidance)	Test Unit	The 412 OG has a representative present at the safety review board. If the safety package does not sufficiently address safety concerns, this representative raises the issue(s) and requires that the test unit address the issue(s) before the package can be submitted for approval.
Final Approval	Test Unit	The commander of the 412 OG receives the completed safety package

		and reviews it in order to ensure that safety has been sufficiently addressed. If so, the commander provides his approval. In some cases, higher approval is also needed.
Airspace Schedule	SPORT, JOSHUA	Once the test units have coordinated with ROC in order to schedule their tests in R-2515, the tentative schedule is passed to SPORT and JOSHUA, as well as other units.
Safety Package	SPORT, JOSHUA	If there are aspects of the safety plan that affect the air traffic control facilities, these details are passed to the appropriate control facility.
Guidance	SPORT, JOSHUA	The 412 OG provides guidance that elaborates on what the higher level regulations require in order to address issues specific to Edwards AFB. This guidance may come in the form of training, regulations, presentations, or other forms.

Table 7. 412th Operations Group Control Actions.

Feedback	Received From	Description
Feedback	SPORT, JOSHUA	The 412 OG is a military unit that is responsible for the SPORT and JOSHUA control facilities. As such, the 412 OG receives feedback regarding procedures that are or are not working, as well as possible improvements.
Incident Reports	SPORT, JOSHUA	EAFBI 13-100 lists 14 incidents which are considered an emergency. After these incidents are resolved, an incident report is submitted to the 412 OG so that procedures may be modified, if necessary.

Table 8. 412th Operations Group Feedback.

RESOURCE OPERATIONS CENTER (ROC)

Control Action	Given To	Description
Conflicts	Test Unit	The test units may require certain areas, such as spin zones or the supersonic corridor, to be active in order to successfully accomplish their test. These requests should be accommodated to the maximum extent possible, however, in some cases, requests may conflict. The lower priority mission will be notified of the conflict and have to reschedule or relocate.
Operations Number	Test Unit	Once the mission is scheduled, the ROC provides an Operations Number that is required to access R-2515.
Airspace Schedule	412 OG	The tentative schedule is given to the 412 OG to distribute as necessary.

Table 9. Resource Operations Center Control Actions.

TEST UNIT

Control Action	Given To	Description
Safety Package	412 OG	Once the test unit has completed its initial safety analysis of the mission, a safety review board is held. This provides the initial safety plan to 412 OG so that 412 OG can review the plan for completeness and provide feedback. This feedback is incorporated into the safety package, which is then submitted for final review.

Airspace Scheduling Requests	ROC	The test unit contacts the ROC with the approximate timing of the planned test and any specific airspace requirements that are a part of the test.
SPORT Prebrief	SPORT	According to EAFBI 13-100, aircrews are required to use the SPORT Prebrief sheet shown in Figure 4 to provide detailed information to the combined supervisor of flying and SPORT.
Mission Objectives	SUAS Pilot	The pilot is an active participant in the safety planning process. The pilot works in conjunction with the safety team to develop the safety package. In the process, the test unit conveys the mission objectives to the pilot. As a part of the safety planning, the test plan is also developed.

Table 10. Test Unit Non-Flight Stage Control Actions.

Feedback	Received From	Description
Feedback	412 OG	The 412 OG has a representative present at the safety review board. If the safety package does not sufficiently address safety concerns, this representative provides feedback and requires that the test unit address the issue before the package can be submitted for approval.
Final Approval	412 OG	The commander of the 412 OG receives the completed safety package and reviews it in order to ensure that safety has been sufficiently addressed. If so, the commander provides his approval. In some cases, higher approval is also needed.
Feedback	SUAS Pilot	As a member of the team developing the test safety plan, the pilot provides feedback to the unit regarding his or her concerns, the handling of the vehicle, and other operational insights.

Table 11. Test Unit Non-Flight Stage Feedback.

FLIGHT OPERATIONS PHASE

HIGH DESERT COMBINED CONTROL FACILITY (JOSHUA)

Control Action	Given To	Description
Aircraft Handoffs	SPORT	If an aircraft is transitioning from airspace under JOSHUA control to airspace under SPORT control, then an aircraft handoff occurs.
Airspace Handoffs	SPORT	At the beginning of the SPORT operations period, JOSHUA hands off the R-2515 airspace to SPORT. In addition, should any part of R-2515 be under JOSHUA control, it is handed back off to SPORT when conditions permit.
Airspace Clearances	Other Aircraft	JOSHUA provides airspace clearance into the larger Edwards AFB test range (R-2508), IFR clearances, and any other airspace blocks as necessary.
Traffic Advisories	Other Aircraft	JOSHUA will advise the pilot about traffic in the area and the route and intentions of that traffic.

Table 12. JOSHUA Flight Operations Stage Control Actions.

Feedback	Received From	Description
Radar Returns	SUAV Occupied Airspace	If an aircraft or SUAV is equipped with a transponder, is large enough to show up on radar, or both, then JOSHUA will receive the vehicle's position.
Position	Other Aircraft	The pilot relays the current position of the aircraft to JOSHUA as necessary. At minimum, the pilot informs JOSHUA when requesting access to R-2508.
Intentions	Other Aircraft	The pilot relays the intentions of the aircraft to JOSHUA as necessary. At minimum, the pilot informs JOSHUA when requesting access to R-2508.
Emergencies	Other Aircraft	In the event of an emergency, if conditions permit, the pilot relays information to JOSHUA regarding the nature of the emergency and their intentions. EAFBI 13-100 describes the information that the pilot should relay.

Table 13. JOSHUA Flight Operations Stage Feedback.

AFTC MILITARY RADAR UNIT (SPORT)

Control Action	Given To	Description
Aircraft Handoffs	SPORT	If an aircraft is transitioning from airspace under SPORT control to airspace under JOSHUA control, then an aircraft handoff occurs.
Airspace Handoffs	SPORT	At the end of the SPORT operations period, SPORT hands off the R-2515 airspace to JOSHUA. In addition, should an aircraft require an IFR clearance, that portion of airspace is handed off to JOSHUA.
Airspace Clearances	SUAS Pilot, Other Aircraft	According to EAFBI 13-100, "Prior to takeoff, local crews will contact SPORT to confirm airspace utilization and profile." SPORT provides aircraft clearance into R-2515, as well as into any specific airspace block that is necessary. If applicable, SPORT will call an area "active" or "hot," indicating to other pilots that it is in use.
Traffic Advisories	SUAS Pilot, Other Aircraft	SPORT will advise the pilot about traffic in the area and their route and intentions, as well as the status of the impact range, Alpha Corridor, Spin Areas, etc.

Table 14. SPORT Flight Operations Stage Control Actions.

Feedback	Received From	Description
Position	SUAS Pilot, Other Aircraft	The pilot relays the current position of the aircraft to SPORT as necessary. At minimum, the pilot informs SPORT when requesting access to R-2515.
Radar Returns	SUAV Occupied Airspace	If an aircraft or SUAV is equipped with a transponder, is large enough to show up on radar, or both, then SPORT will receive the vehicle's position.
Intentions	SUAS Pilot,	The pilot relays the intentions of the aircraft to SPORT as necessary. At minimum, the pilot informs SPORT when requesting access to R-2515.

	Other Aircraft	
Emergencies	SUAS Pilot, Other Aircraft	In the event of an emergency, if conditions permit, the pilot relays information to SPORT regarding the nature of the emergency and their intentions. EAFBI 13-100 describes the information that the pilot should relay.

Table 15. SPORT Flight Operations Stage Feedback.

TEST UNIT

Control Action	Given To	Description
Guidance	SUAS Pilot	During the test, the test squadron maintains a control room that monitors the test and provides guidance to the pilot as necessary.

Table 16. Test Unit Flight Operations Stage Control Actions.

Feedback	Received From	Description
Feedback	SUAS Pilot	During the test, the pilot relays feedback to the control room in the Test Unit regarding what is or is not working, any modifications to the test, and any questions or concerns that arise.

Table 17. Test Unit Flight Operations Stage Feedback.

SUAS PILOT

Control Action	Given To	Description
Route Commands	SUAV	The pilot provides route commands to the SUAV. These route plans may be as complex as a full flight plan or as rudimentary as standard roll, pitch, and yaw inputs.
Speed Commands	SUAV	The pilot provides speed commands to the SUAV. These commands may be as complex as preset target airspeeds or as rudimentary as a throttle increase or decrease.
Payload Commands	SUAV	If applicable, the pilot provides commands regarding the maneuvering of onboard cameras, electronic equipment, and dropping any payload or munitions.

Table 18. SUAS Pilot Flight Operations Stage Control Actions.

Feedback	Received From	Description
Vehicle State	SUAV	The SUAV relays information regarding the state of the vehicle, such as the speed, position of control surfaces, orientation, and software status to the pilot.
Errors	SUAV	In the event of an error, the SUAV relays this error to the pilot.
Sensor Information	SUAV	The SUAV relays information to the pilot from any applicable sensors, including camera, GPS, or other sensors.

Table 19. SUAS Pilot Flight Operations Stage Feedback.

SUAV

Control Action	Given To	Description
Maneuver	SUAV Occupied Airspace	The SUAV flight computer adjusts the control surfaces and motors to maneuver.
Payload Release	SUAV Occupied Airspace	The SUAV flight computer adjusts the servos to release the payload, if applicable.

Table 20. SUAV Control Actions.

Feedback	Received From	Description
Sensor Readings	SUAV Occupied Airspace	Sensors such as a camera, altimeter, GPS, etc. monitor the SUAV's location in the airspace.

Table 21. SUAV Feedback.

OTHER AIRCRAFT

Control Action	Given To	Description
Maneuver	SUAV Occupied Airspace	The aircraft pilot adjusts the control surfaces and engines to maneuver the aircraft.
Payload Release	SUAV Occupied Airspace	The aircraft pilot commands a payload release, if applicable.

Table 22. Other Aircraft Control Actions.

Feedback	Received From	Description
Visual Cues	SUAV Occupied Airspace	If the SUAV is equipped with a transponder, is large enough to be seen, or both, then the SUAV's position is visible to other aircraft by sight or other electronic tracking methods.

Table 23. Other Aircraft Feedback.

APPENDIX B: UNSAFE CONTROL ACTION ANALYSIS DETAILS

This section provides a complete STPA Step 1 Analysis as discussed in Chapter 4 for each controller based on the Control Actions listed in Appendix A. Each UCA is then translated into a safety requirement. Recall that the five hazards that are being considered in this analysis are:

H1: Air-to-Air Collision. Collision of two or more aircraft (including both manned and unmanned systems) in the air.

H2: Debris Impact in the Air. Debris from a SUAS impacts another aircraft (including both manned and unmanned systems).

H3: Air-to-Ground Collision. Collision of a SUAS with a structure or person on the ground.

H4: Debris Impact on the Ground. Debris from a SUAS unintentionally impacts a structure or person on the ground.

H5: Interference. SUAS testing or flight operations unnecessarily interfere with flight operations.

NON-FLIGHT PHASE

412TH OPERATIONS GROUP (412 OG)

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Feedback	Test Unit	n/a	…when the existing safety plan is not sufficient. [H1, H2, H3, H4]	n/a	…when the feedback does not address all of the concerns. [H1, H2, H3, H4]
Final Approval	Test Unit	…when the safety plan is not sufficient. [H1, H2, H3, H4]	…when the safety plan is sufficient. [H5]	…before all of the concerns raised during the SRB are addressed. [H1, H2, H3, H4]	…when approval is not rescinded if additional information indicates it should be. [H1, H2, H3, H4]
Airspace Schedule	SPORT, JOSHUA	n/a	[H5]	…before the schedule is complete. [H5]	n/a
Safety Package	SPORT, JOSHUA	…when the information is not relevant to SPORT/JOSHUA. [H5]	…when the information is relevant to SPORT/JOSHUA. [H1, H2, H3, H4]	n/a	n/a

Guidance	SPORT, JOSHUA	…excessively or redundantly. [H5]	…when specific guidance is necessary. [H1, H2, H3, H4, H5]	n/a	n/a

Table 24. 412th Operations Group Unsafe Control Actions.

The UCAs found in Table 24 are listed below:

1. 412 OG does not provide feedback to the Test Unit when the existing safety plan is not sufficient. [H1, H2, H3, H4]
2. 412 OG stops providing feedback to the Test Unit before all of the concerns are addressed. [H1, H2, H3, H4]
3. 412 OG provides final approval to the Test Unit when the safety plan is not sufficient. [H1, H2, H3, H4]
4. 412 OG does not provide final approval to the Test Unit when the safety plan is sufficient. [H5]
5. 412 OG provides final approval to the Test Unit before all of the concerns raised during the SRB are addressed. [H1, H2, H3, H4]
6. 412 OG provides final approval to the Test Unit and does not rescind this approval if additional information indicates it should be. [H1, H2, H3, H4]
7. 412 OG does not provide the Airspace Schedule to SPORT and JOSHUA. [H5]
8. 412 OG provides the Airspace Schedule to SPORT and JOSHUA before it is complete. [H5]
9. 412 OG provides information from the safety package to SPORT and JOSHUA when the information is not relevant. [H5]
10. 412 OG does not provide information from the safety package to SPORT and JOSHUA when the information is relevant. [H1, H2, H3, H4]
11. 412 OG provides guidance (training) to SPORT and JOSHUA excessively or redundantly. [H5]
12. 412 OG does not provide guidance (training) to SPORT and JOSHUA when specific guidance is necessary. [H1, H2, H3, H4, H5]

Safety Requirements

These 12 UCAs generate the safety requirements of the 412 OG. The safety requirements are listed below.

1. 412 OG must provide feedback to the Test Unit when the existing safety plan is not sufficient. [H1, H2, H3, H4]
2. 412 OG must not stop providing feedback to the Test Unit until all of the concerns are addressed. [H1, H2, H3, H4]
3. 412 OG must not provide final approval to the Test Unit when the safety plan is not sufficient. [H1, H2, H3, H4]
4. 412 OG must provide final approval to the Test Unit when the safety plan is sufficient. [H5]
5. 412 OG must not provide final approval to the Test Unit until all of the concerns raised during the SRB are addressed. [H1, H2, H3, H4]
6. 412 OG must rescind this approval if additional information indicates additional issues need to be addressed. [H1, H2, H3, H4]
7. 412 OG must provide the Airspace Schedule to SPORT and JOSHUA. [H5]

8. 412 OG must not provide the Airspace Schedule to SPORT and JOSHUA until it is complete. [H5]
9. 412 OG must not provide information from the safety package to SPORT and JOSHUA when the information is not relevant. [H5]
10. 412 OG must provide information from the safety package to SPORT and JOSHUA when the information is relevant. [H1, H2, H3, H4]
11. 412 OG must not provide guidance (training) to SPORT and JOSHUA excessively or redundantly. [H5]
12. 412 OG must provide guidance (training) to SPORT and JOSHUA when specific guidance is necessary. [H1, H2, H3, H4, H5]

RESOURCE OPERATIONS CENTER (ROC)

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Conflicts	Test Unit	…when no conflicts exist or deconflicting is possible. [H5]	…when conflicts exist. [H5]	n/a	n/a
Operations Number	Test Unit	…when conflicts exist. [H5]	…when mission is scheduled. [H5]	n/a	n/a
Airspace Schedule	412 OG	n/a	…when schedule is complete. [H5]	…before the schedule is complete. [H5]	n/a

Table 25. Resource Operations Center Unsafe Control Actions.

The UCAs found in Table 25 are listed below:

13. The ROC informs the Test Unit of conflicts when no conflicts exist or deconflicting is possible. [H5]
14. The ROC does not inform the Test Unit of conflicts when conflicts exist. [H5]
15. The ROC provides an Operations Number to the Test Unit when conflicts exist. [H5]
16. The ROC does not provide an Operations Number to the Test Unit when the mission is scheduled. [H5]
17. The ROC does not provide the Airspace Schedule to the 412 OG when the schedule is complete. [H5]
18. The ROC provides the Airspace Schedule to the 412 OG before the schedule is complete. [H5]

Safety Requirements

These 6 UCAs generate the safety requirements of the ROC. The safety requirements are listed below.

13. The ROC must not inform the Test Unit of conflicts when no conflicts exist or deconflicting is possible. [H5]
14. The ROC must inform the Test Unit of conflicts when conflicts exist. [H5]
15. The ROC must not provide an Operations Number to the Test Unit when conflicts exist. [H5]
16. The ROC must provide an Operations Number to the Test Unit when the mission is scheduled. [H5]
17. The ROC must provide the Airspace Schedule to the 412 OG when the schedule is complete. [H5]
18. The ROC must not provide the Airspace Schedule to the 412 OG until the schedule is complete. [H5]

TEST UNIT

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Safety Package	412 OG	…when safety plan is not sufficient. [H1, H2, H3, H4]	…safety plan is sufficient. [H5]	…before feedback from the SRB has been addressed. [H1, H2, H3, H4]	n/a
Airspace Scheduling Requests	ROC	n/a	…when mission is planned to fly. [H5]	n/a	n/a
SPORT Prebrief	SPORT	n/a	…when mission is planned to fly. [H1, H2, H3, H4, H5]	n/a	n/a
Mission Objectives	SUAS Pilot	n/a	[H5]	…too late in the test planning process. [H5]	n/a

Table 26. Test Unit Non-Flight Stage Unsafe Control Actions.

The UCAs found in Table 26 are listed below:

19. The Test Unit provides the safety package to the 412 OG when safety plan is not sufficient. [H1, H2, H3, H4]
20. The Test Unit does not provide the safety package to the 412 OG when safety plan is sufficient. [H5]
21. The Test Unit provides the safety package to the 412 OG before feedback from the SRB has been addressed. [H1, H2, H3, H4]

22. The Test Unit does not schedule their test with the ROC when the mission is planned to fly. [H5]
23. The Test Unit does not provide the SPORT Prebrief when the mission is planned to fly. [H1, H2, H3, H4, H5]
24. The Test Unit does not provide the SUAS pilot with the mission objectives. [H5]
25. The Test Unit provides the SUAS pilot with the mission objectives too late in the test planning process. [H5]

Safety Requirements

These 7 UCAs generate the safety requirements of the Test Unit during the Non-Flight Stages. The safety requirements are listed below.

19. The Test Unit must not provide the safety package to the 412 OG when safety plan is not sufficient. [H1, H2, H3, H4]
20. The Test Unit must provide the safety package to the 412 OG when safety plan is sufficient. [H5]
21. The Test Unit must not provide the safety package to the 412 OG until feedback from the SRB has been addressed. [H1, H2, H3, H4]
22. The Test Unit must schedule their test with the ROC when the mission is planned to fly. [H5]
23. The Test Unit must provide the SPORT Prebrief when the mission is planned to fly. [H1, H2, H3, H4, H5]
24. The Test Unit must provide the SUAS pilot with the mission objectives. [H5]
25. The Test Unit must provide the SUAS pilot with the mission objectives as early as possible in the test planning process. [H5]

FLIGHT OPERATIONS PHASE

HIGH DESERT COMBINED CONTROL FACILITY (JOSHUA)

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Aircraft Handoffs	SPORT	…when JOSHUA controlled aircraft is in encroaching. [H1]	…when aircraft is entering SPORT airspace. [H1, H2, H3, H4]	n/a	n/a
Airspace Handoffs	SPORT	...without handing off aircraft in the airspace. [H1]	n/a	n/a	n/a
Airspace Clearances	Other Aircraft	…when airspace is not safe. [H1, H2, H3, H4]	…when airspace is safe. [H5]	n/a	…not rescinded when airspace is no longer safe. [H1, H2]

Traffic Advisories	Other Aircraft	n/a	…when another aircraft is nearby or approaching aircraft. [H1, H2]	…too late for corrective action. [H1, H2, H3, H4]	…not rescinded when encroaching aircraft is no longer a factor. [H5]

Table 27. JOSHUA Flight Operations Stage Unsafe Control Actions.

The UCAs found in Table 27 are listed below:

26. JOSHUA hands off an aircraft to SPORT when another JOSHUA controlled aircraft is encroaching. [H1]
27. JOSHUA does not hand off aircraft to SPORT when aircraft is entering SPORT airspace. [H1, H2, H3, H4]
28. JOSHUA hands off airspace to SPORT without handing off aircraft in the airspace. [H1]
29. JOSHUA provides an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]
30. JOSHUA does not provide an aircraft with a clearance when the airspace is safe. [H5]
31. JOSHUA provides an aircraft with a clearance that is not rescinded when the airspace is no longer safe. [H1, H2, H3, H4]
32. JOSHUA does not provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]
33. JOSHUA provides an aircraft with traffic advisories too late for corrective action. [H1, H2, H3, H4]
34. JOSHUA provides an aircraft with a traffic advisory that is not rescinded when the encroaching aircraft is no longer a factor. [H5]

Safety Requirements

These 9 UCAs generate the safety requirements of JOSHUA. The safety requirements are listed below.

26. JOSHUA must not hand off an aircraft to SPORT when another JOSHUA controlled aircraft is encroaching. [H1]
27. JOSHUA must hand off aircraft to SPORT when aircraft is entering SPORT airspace. [H1, H2, H3, H4]
28. JOSHUA must not hand off airspace to SPORT without handing off aircraft in the airspace. [H1]
29. JOSHUA must not provide an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]
30. JOSHUA must provide an aircraft with a clearance when the airspace is safe. [H5]
31. JOSHUA must rescind a clearance when the airspace is no longer safe. [H1, H2, H3, H4]
32. JOSHUA must provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]
33. JOSHUA must provide an aircraft with traffic advisories in time for corrective action. [H1, H2, H3, H4]
34. JOSHUA must rescind a traffic advisory when the encroaching aircraft is no longer a factor. [H5]

AFTC MILITARY RADAR UNIT (SPORT)

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Aircraft Handoffs	SPORT	…when SPORT controlled aircraft is encroaching. [H1]	…when aircraft is entering JOSHUA airspace. [H1] …when aircraft is requesting IFR clearance. [H1, H3]	n/a	n/a
Airspace Handoffs	SPORT	...without handing off aircraft in the airspace. [H1]	n/a	n/a	n/a
Airspace Clearances	SUAS Pilot, Other Aircraft	…when airspace is not safe. [H1, H2, H3, H4]	…when airspace is safe. [H5]	n/a	…not rescinded when airspace is no longer safe. [H1, H2, H3, H4]
Traffic Advisories	SUAS Pilot, Other Aircraft	n/a	…when another aircraft is nearby or approaching aircraft. [H1, H2]	…too late for corrective action. [H1, H2, H3, H4]	…not rescinded when encroaching aircraft is no longer a factor. [H5]

Table 28. SPORT Flight Operations Stage Unsafe Control Actions.

The UCAs found in Table 28 are listed below:

35. SPORT hands off an aircraft to JOSHUA when another SPORT controlled aircraft is encroaching. [H1]
36. SPORT does not hand off aircraft to JOSHUA when aircraft is entering JOSHUA airspace. [H1]
37. SPORT does not hand off aircraft to JOSHUA when aircraft is requesting IFR clearance. [H1, H3]
38. SPORT hands off airspace to JOSHUA without handing off aircraft in the airspace. [H1]
39. SPORT provides an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]
40. SPORT does not provide an aircraft with a clearance when the airspace is safe. [H5]
41. SPORT provides an aircraft with a clearance that is not rescinded when the airspace is no longer safe. [H1, H2, H3, H4]
42. SPORT does not provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]
43. SPORT provides an aircraft with traffic advisories too late for corrective action. [H1, H2, H3, H4]
44. SPORT provides an aircraft with a traffic advisory that is not rescinded when the encroaching aircraft is no longer a factor. [H5]

Safety Requirements

These 10 UCAs generate the safety requirements of SPORT. The safety requirements are listed below.

35. SPORT must not hand off an aircraft to JOSHUA when another SPORT controlled aircraft is encroaching. [H1]
36. SPORT must hand off aircraft to JOSHUA when aircraft is entering JOSHUA airspace. [H1, H2, H3, H4]
37. SPORT must hand off aircraft to JOSHUA when aircraft is requesting IFR clearance. [H1, H3]
38. SPORT must not hand off airspace to JOSHUA without handing off aircraft in the airspace. [H1]
39. SPORT must not provide an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]
40. SPORT must provide an aircraft with a clearance when the airspace is safe. [H5]
41. SPORT must rescind a clearance when the airspace is no longer safe. [H1, H2, H3, H4]
42. SPORT must provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]
43. SPORT must provide an aircraft with traffic advisories in time for corrective action. [H1, H2, H3, H4]
44. SPORT must rescind a traffic advisory when the encroaching aircraft is no longer a factor. [H5]

TEST UNIT

Unsafe Control Action

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Guidance	SUAS Pilot	…when excessive, redundant, or distracting. [H1, H2, H3, H4, H5]	…when SUAS Pilot requests guidance. [H1, H2, H3, H4, H5]	…too late for corrective action. [H1, H2, H3, H4]	…stopped before the situation is resolved. [H1, H2, H3, H4]

Table 29. Test Unit Flight Operations Stage Unsafe Control Actions.

The UCAs found in Table 29 are listed below:

45. The Test Unit provides guidance to the pilot that is excessive, redundant, or distracting. [H1, H2, H3, H4, H5]
46. The Test Unit does not provide guidance to the pilot when the pilot requests guidance. [H1, H2, H3, H4, H5]
47. The Test Unit provides guidance to the pilot too late for corrective action. [H1, H2, H3, H4]
48. The Test Unit provides guidance to the pilot but stops before the situation is resolved. [H1, H2, H3, H4]

Safety Requirements

These 4 UCAs generate the safety requirements of the Test Unit during Flight Operations. The safety requirements are listed below.

45. The Test Unit must not provide guidance to the pilot that is excessive, redundant, or distracting. [H1, H2, H3, H4, H5]
46. The Test Unit must provide guidance to the pilot when the pilot requests guidance. [H1, H2, H3, H4, H5]
47. The Test Unit must provide guidance to the pilot in time for corrective action. [H1, H2, H3, H4]
48. The Test Unit must not stop providing guidance until the situation is resolved. [H1, H2, H3, H4]

PILOT

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Route Commands	SUAV	…in a direction that the SUAV should not go. [H1, H3]	…when the SUAV needs to change direction. [H1, H3]	…when the SUAV should not change direction. [H1, H3]	…stopped before the change in direction is complete. [H1, H3] …held after the change in direction is complete. [H1, H3]
Speed Commands	SUAV	…when a change in speed is not appropriate. [H1, H3]	…when a change in speed is appropriate. [H1, H3]	n/a	…stopped before the change in speed is complete. [H1, H3] …held after the change in speed is complete. [H1, H3]
Payload Commands	SUAV	…when payload should not be released. [H2, H4]	…when payload should be released [H2, H4] …when sensor reconfiguration is necessary. [H1, H2, H3, H4, H5]	n/a	…continues after SUAV exits payload drop zone [H2, H4]. …stopped before payload can fully release. [H2, H4]

Table 30. SUAS Pilot Flight Operations Stage Unsafe Control Actions.

The UCAs found in Table 30 are listed below:

49. The SUAS Pilot provides route commands in a direction that the SUAV should not go. [H1, H3]
50. The SUAS Pilot does not provide route commands when the SUAV needs to change direction. [H1, H3]
51. The SUAS Pilot provides route commands when the SUAV should not change direction. [H1, H3]
52. The SUAS Pilot provides route commands that are stopped before the change in direction is complete. [H1, H3]
53. The SUAS Pilot provides route commands that are held after the change in direction is complete. [H1, H3]
54. The SUAS Pilot provides speed commands to the SUAV when a change in speed is not appropriate. [H1, H3]
55. The SUAS Pilot does not provide speed commands to the SUAV when a change in speed is appropriate. [H1, H3]
56. The SUAS Pilot provides speed commands that are stopped before the change in speed is complete. [H1, H3]
57. The SUAS pilot provides speed commands that are held after the change in speed is complete. [H1, H3]
58. The SUAS Pilot provides payload commands when the payload should not be released. [H2, H4]
59. The SUAS Pilot does not provide payload commands when the payload should be released. [H2, H4]
60. The SUAS Pilot does not provide payload commands when sensor reconfiguration is necessary. [H1, H2, H3, H4, H5]
61. The SUAS Pilot provides payload commands that continue after the SUAV exits the payload drop zone [H2, H4]
62. The SUAS Pilot provides payload commands that stop before the payload can fully release. [H2, H4]

Safety Requirements

These 14 UCAs generate the safety requirements of the SUAS Pilot. The safety requirements are listed below.

49. The SUAS Pilot must not provide route commands in a direction that the SUAV should not go. [H1, H3]
50. The SUAS Pilot must provide route commands when the SUAV needs to change direction. [H1, H3]
51. The SUAS Pilot must not provide route commands when the SUAV should not change direction. [H1, H3]
52. The SUAS Pilot must not stop route commands before the change in direction is complete. [H1, H3]
53. The SUAS Pilot must not hold route commands after the change in direction is complete. [H1, H3]

54. The SUAS Pilot must not provide speed commands to the SUAV when a change in speed is not appropriate. [H1, H3]
55. The SUAS Pilot must provide speed commands to the SUAV when a change in speed is appropriate. [H1, H3]
56. The SUAS Pilot must not stop speed commands before the change in speed is complete. [H1, H3]
57. The SUAS pilot must not hold speed commands after the change in speed is complete. [H1, H3]
58. The SUAS Pilot must not provide payload commands when the payload should not be released. [H2, H4]
59. The SUAS Pilot must provide payload commands when the payload should be released. [H2, H4]
60. The SUAS Pilot must provide payload commands when sensor reconfiguration is necessary. [H1, H2, H3, H4, H5]
61. The SUAS Pilot must not provide payload commands that continue after the SUAV exits the payload drop zone [H2, H4]
62. The SUAS Pilot must not provide payload commands that stop before the payload can fully release. [H2, H4]

SUAV

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Maneuver	SUAV Occupied Airspace	…when the maneuver takes the SUAV out of its assigned airspace. [H1, H3]	…when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]	…when the maneuver is applied too late. [H1, H3]	…stopped before the maneuver is complete. [H1, H3] …held after the maneuver is complete. [H1, H3]
Payload Release	SUAV Occupied Airspace	…when the payload will exit SUAV Occupied Airspace. [H2, H4]	…when payload should be released [H5].	n/a	…stopped before payload can fully release. [H2, H4]

Table 31. SUAV Unsafe Control Actions.

The UCAs found in Table 31 are listed below:

63. The SUAV maneuvers when then maneuver takes it out of its assigned airspace. [H1, H3]
64. The SUAV does not maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]
65. The SUAV maneuvers too late to stay in its assigned airspace. [H1, H3]
66. The SUAV maneuver is stopped before the change in direction is complete. [H1, H3]

67. The SUAV maneuver is held after the change in direction is complete. [H1, H3]
68. The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]
69. The SUAV does not release its payload when the payload should be released. [H5]
70. The SUAV payload release is stopped before payload can fully release. [H2, H4]

Safety Requirements

These 8 UCAs generate the safety requirements of the SUAV. The safety requirements are listed below.

63. The SUAV must not maneuver when then maneuver takes it out of its assigned airspace. [H1, H3]
64. The SUAV must maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]
65. The SUAV must maneuver in time to stay in its assigned airspace. [H1, H3]
66. The SUAV maneuver must not stop before the change in direction is complete. [H1, H3]
67. The SUAV maneuver must not hold after the change in direction is complete. [H1, H3]
68. The SUAV must not release its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]
69. The SUAV must release its payload when the payload should be released. [H5]
70. The SUAV payload release must not stop before payload can fully release. [H2, H4]

OTHER AIRCRAFT

Unsafe Control Actions

Control Action	Given To	Providing Causes Hazard	Not Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Maneuver	SUAV Occupied Airspace	…when the maneuver takes the Other Aircraft into SUAV Occupied Airspace. [H1, H3]	…when a maneuver is needed to keep the Other Aircraft out of SUAV Occupied Airspace. [H1, H3]	…when the maneuver is applied too late. [H1, H3]	n/a
Payload Release	SUAV Occupied Airspace	…when the payload will enter SUAV Occupied Airspace. [H2, H4]	n/a	n/a	n/a

Table 32. Other Aircraft Unsafe Control Actions.

The UCAs found in Table 32 are listed below:

71. The other aircraft maneuvers when the maneuver takes the Other Aircraft into SUAV Occupied Airspace. [H1, H3]
72. The other aircraft does not maneuver when a maneuver is needed to keep the Other Aircraft out of SUAV Occupied Airspace. [H1, H3]
73. The other aircraft maneuvers too late to stay out of SUAV Occupied Airspace. [H1, H3]
74. The other aircraft releases its payload when the payload will enter SUAV Occupied Airspace. [H2, H4]

Safety Requirements

These 4 UCAs generate the safety requirements of Other Aircraft. The safety requirements are listed below.

71. The other aircraft must not maneuver when the maneuver takes the Other Aircraft into SUAV Occupied Airspace. [H1, H3]
72. The other aircraft must maneuver when a maneuver is needed to keep the Other Aircraft out of SUAV Occupied Airspace. [H1, H3]
73. The other aircraft must maneuver in time to stay out of SUAV Occupied Airspace. [H1, H3]
74. The other aircraft must not release its payload when the payload will enter SUAV Occupied Airspace. [H2, H4]

APPENDIX C: CAUSES OF UNSAFE CONTROL ACTIONS

This section provides a complete STPA Step 2 Analysis for each controller based on the Unsafe Control Actions listed in Appendix B. Each UCA is analyzed to determine possible causes. The four basic scenarios are listed and potential solutions are identified, if possible. If not, then the basic scenario is further refined.

NON-FLIGHT PHASE

412TH OPERATIONS GROUP (412 OG)

1. UCA: 412 OG does not provide feedback to the Test Unit when the existing safety plan is not sufficient. [H1, H2, H3, H4]

A. Inadequate Control Execution: 412 OG provides feedback to the Test Unit, but the feedback is not acted upon. Solution: 412 OG must follow up with Test Unit to ensure feedback is incorporated into the safety plan.

B. Inappropriate Decision: 412 OG understands the safety plan as briefed during the SRB is insufficient, but does not provide feedback.

   i. Refinement: 412 OG is under outside pressure to expedite testing. Solution: 412 OG should always operate with safety as their highest priority.

C. Inadequate Feedback and Other Inputs: 412 OG believes safety plan briefed during the SRB is sufficient, but it is not.

   i. Refinement 1: 412 OG believes safety plan briefed during the SRB is sufficient because 412 OG does not understand all aspects of the safety plan. Solution: 412 OG must ask questions until they thoroughly understand the safety plan.

   ii. Refinement 2: 412 OG believes safety plan briefed during the SRB is sufficient because 412 OG does not understand hazard analysis techniques. Solution: 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training.

D. Inadequate Process Behavior: Feedback is incorporated into the safety plan, but the safety plan remains insufficient. Solution: 412 OG must ensure that the review process is iterative, and continue to provide feedback until the safety plan is sufficient.

2. UCA: 412 OG stops providing feedback to the Test Unit before all of the concerns are addressed. [H1, H2, H3, H4]

A. Inadequate Control Execution: 412 OG continues to provide feedback, but the Test Unit stops updating the safety plan. Solution: 412 OG must ensure that feedback is incorporated in the safety plan.

B. Inappropriate Decision: 412 OG understands that the safety plan remains insufficient, but does not provide additional feedback. Solution: 412 OG always provides either final approval or feedback.

C. Inadequate Feedback and Other Inputs: 412 OG believes that the safety plan is now safe, but it is not.

i. Refinement 1: 412 OG believes safety plan is sufficient because 412 OG does not understand all aspects of the safety plan. Solution: 412 OG must ask questions until they thoroughly understand the safety plan.
ii. Refinement 2: 412 OG believes safety plan is sufficient because 412 OG does not understand hazard analysis techniques. Solution: 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training.

D. Inadequate Process Behavior: Feedback is incorporated into the safety plan, but the safety plan remains insufficient. Solution: 412 OG must ensure that the review process is iterative, and continue to provide feedback until the safety plan is sufficient.

3. UCA: 412 OG provides final approval to the Test Unit when the safety plan is not sufficient. [H1, H2, H3, H4]

A. Inadequate Control Execution: 412 OG does not provide approval, but the Test Unit proceeds with testing. Solution: 412 OG approval of the safety plan must be checked before test can proceed.

B. Inappropriate Decision: 412 OG understands that the safety plan remains insufficient, but provides approval.
i. Refinement: 412 OG is under outside pressure to expedite testing. Solution: 412 OG should always operate with safety as their highest priority.

C. Inadequate Feedback and Other Inputs: 412 OG believes that the safety plan is safe, but it is not.
i. Refinement 1: 412 OG believes safety plan is sufficient because 412 OG does not understand all aspects of the safety plan. Solution: 412 OG must ask questions until they thoroughly understand the safety plan.
ii. Refinement 2: 412 OG believes safety plan is sufficient because 412 OG does not understand hazard analysis techniques. Solution: 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training.
iii. Refinement 3: 412 OG receives incorrect safety plan, which is given approval. Solution: 412 OG must check that the safety plan is complete and correct before providing approval.

D. Inadequate Process Behavior: 412 OG does not provide final approval, and the test unit does not update the safety plan to incorporate changes.
i. Refinement 1: Test Unit has concerns about the test that are not safety related (cost, goals, resources). Solution: Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan.
ii. Refinement 2: Test Unit does not understand reasons why approval was not given. Solution: 412 OG always provides either final approval or feedback.

4. UCA: 412 OG does not provide final approval to the Test Unit when the safety plan is sufficient. [H5]

A. Inadequate Control Execution: 412 OG provides approval, but the Test Unit does not receive it. Solution: Test Unit must follow up with 412 OG if approval is not received in an appropriate amount of time.

B. Inappropriate Decision: 412 OG understands that the safety plan is sufficient, but does not provide approval.
    i. Refinement 1: 412 OG understands that the safety plan is sufficient, but has concerns about the test that are not safety related (cost, goals, resources). Solution: 412 OG must provide this feedback to the Test Unit so that they can adjust their test plan.
    ii. Refinement 2: 412 OG understands that the safety plan is sufficient, but forgets to provide approval. Solution: Test Unit must follow up with 412 OG if approval is not received in an appropriate amount of time.
C. Inadequate Feedback and Other Inputs: 412 OG believes that the safety plan is not sufficient, but it is.
    i. Refinement 1: 412 OG believes safety plan is not sufficient because 412 OG does not understand all aspects of the safety plan. Solution: 412 OG must ask questions until their concerns are addressed.
    ii. Refinement 2: 412 OG believes safety plan is not sufficient because 412 OG does not understand hazard analysis techniques. Solution: 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training.
    iii. Refinement 3: 412 OG receives incorrect or outdated safety plan, which is not given approval. Solution: Test Unit must be made aware of the reason(s) the plan was not approved, and given the chance to provide an updated or corrected plan.
D. Inadequate Process Behavior: 412 OG provides final approval, and the test unit does not proceed with testing.
    i. Refinement 1: Test Unit has concerns about the test that are not safety related (cost, goals, resources). Solution: Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan.

5. UCA: 412 OG provides final approval to the Test Unit before all of the concerns raised during the SRB are addressed. [H1, H2, H3, H4]

A. Inadequate Control Execution: 412 OG does not provide approval, but the Test Unit proceeds with testing. Solution: 412 OG approval of the safety plan must be checked before test can proceed.
B. Inappropriate Decision: 412 OG understands that the concerns were not addressed, but provides approval.
    i. Refinement: 412 OG is under outside pressure to expedite testing. Solution: 412 OG should always operate with safety as their highest priority.
C. Inadequate Feedback and Other Inputs: 412 OG believes that the concerns have been addressed, but they have not.
    i. Refinement 1: 412 OG believes concerns have been addressed because 412 OG does not know what concerns were raised in the SRB. Solution: Concerns raised in the SRB must be documented and accompany the final safety package for approval.
    ii. Refinement 2: 412 OG believes concerns have been addressed because 412 OG does not understand hazard analysis techniques. Solution: 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training.

D. Inadequate Process Behavior: 412 OG does not provide final approval, and the test unit does not update the safety plan to incorporate changes.
    iii. Refinement 1: Test Unit has concerns about the test that are not safety related (cost, goals, resources). Solution: Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan.
    iv. Refinement 2: Test Unit does not understand reasons why approval was not given. Solution: 412 OG must provide feedback on why safety plan was not approved.

6. UCA: 412 OG provides final approval to the Test Unit and does not rescind this approval if additional information indicates it should be. [H1, H2, H3, H4]

A. Inadequate Control Execution: 412 OG rescinds approval, but the Test Unit is not notified. Solution: 412 OG must immediately notify the affected test unit if approval is rescinded.
B. Inappropriate Decision: Additional information indicates that the safety plan is not safe, but 412 OG does not rescind approval.
    i. Refinement 1: 412 OG does not understand that the additional information affects the safety plan. Solution: When the additional information is presented, it should be in such a way that the safety implications are clear.
    ii. Refinement 2: 412 OG is under outside pressure to allow the test to continue. Solution: 412 OG should always operate with safety as their highest priority.
C. Inadequate Feedback and Other Inputs: The safety implications of the additional information are unclear. Solution: When additional information is presented, it should be in a way that the safety implications are clear.
D. Inadequate Process Behavior: 412 OG rescinds approval, but the Test Unit does not stop testing. Solution: 412 OG must follow up with the Test Unit to ensure testing has stopped.

7. UCA: 412 OG does not provide the Airspace Schedule to SPORT and JOSHUA. [H5]

A. Inadequate Control Execution: 412 OG provides the airspace schedule, but SPORT and/or JOSHUA do not receive it. Solution: 412 OG must receive confirmation that SPORT/JOSHUA has received the schedule.
B. Inappropriate Decision: 412 OG receives the airspace schedule, but does not pass it on.
    i. Refinement 1: 412 OG does not pass on the airspace schedule because they do not believe that it is important. Solution: 412 OG must always pass on the airspace schedule, regardless of its importance.
    ii. Refinement 2: 412 OG does not pass on the airspace schedule because they believe the schedule has already been passed on. Solution: 412 OG must establish a standard procedure to ensure that the schedule is passed on (specific person, time of day, etc.).
C. Inadequate Feedback and Other Inputs: 412 OG does not receive the airspace schedule. Solution: 412 OG must ask ROC to provide airspace schedule if it has not been received.
D. Inadequate Process Behavior: SPORT and/or JOSHUA receive the airspace schedule, but do not refer to it. Solution: 412 OG must provide guidance on how to incorporate the airspace schedule into planning control operations.

8. **UCA: 412 OG provides the Airspace Schedule to SPORT and JOSHUA before it is complete. [H5]**
   A. Inadequate Control Execution: 412 OG provides updated airspace schedule, , but SPORT and/or JOSHUA do not receive it. Solution: 412 OG must receive confirmation that SPORT/JOSHUA has received the schedule.
   B. Inappropriate Decision: 412 OG understands that the schedule is not complete, but passes it on to SPORT/JOSHUA. Solution: When updated schedule is available, 412 OG updates SPORT/JOSHUA.
   C. Inadequate Feedback and Other Inputs: 412 OG is not informed that this schedule is incomplete, and passes it on. Solution: Schedule must be marked as a draft or complete when it is given to 412 OG.
   D. Inadequate Process Behavior: SPORT/JOSHUA receive complete or updated schedule, but still use the incomplete one. Solution: SPORT/JOSHUA inform 412 OG of what version of the schedule they are using.

9. **UCA: 412 OG provides information from the safety package to SPORT and JOSHUA when the information is not relevant. [H5]**
   A. Inadequate Control Execution: 412 OG does not intend to provide irrelevant information, but SPORT/JOSHUA receives it. Solution: SPORT/JOSHUA ignores irrelevant information.
   B. Inappropriate Decision: 412 OG receives the safety information and provides it to SPORT/JOSHUA.
      i. Refinement 1: 412 OG does not understand what information is relevant to control facility operations. Solution: A control facility representative is on hand to determine what information is necessary.
   C. Inadequate Feedback and Other Inputs: 412 OG receives information that should be brought to the attention of SPORT/JOSHUA, but the information is incorrect or incomplete. Solution: SPORT/JOSHUA provide this feedback to 412 OG, who can inform the appropriate Test Unit.
   D. Inadequate Process Behavior: 412 OG provides information that is relevant to SPORT/JOSHUA, but SPORT/JOSHUA do not review or act on it. Solution: All safety information from 412 OG must be reviewed by one of the controllers on shift.

10. **UCA: 412 OG does not provide information from the safety package to SPORT and JOSHUA when the information is relevant. [H1, H2, H3, H4]**
   A. Inadequate Control Execution: 412 OG provides the information, but SPORT/JOSHUA does not receive it. Solution: 412 OG should ensure that the information is received and reviewed.
   B. Inappropriate Decision: 412 OG receives the information but does not pass it on to SPORT/JOSHUA.
      i. Refinement 1: 412 OG does not understand what information is relevant to control facility operations. Solution: A control facility representative is on hand to determine what information is necessary.
      ii. Refinement 2: 412 OG does not pass on the information because they believe the information has already been passed on. Solution: 412 OG must establish a standard procedure to ensure that the information is passed on.

C. Inadequate Feedback and Other Inputs: 412 OG receives incorrect safety plan, which does not include relevant control facility information. Solution: 412 OG must check that the safety plan is complete and correct before providing approval.
D. Inadequate Process Behavior: SPORT and/or JOSHUA receive the information, but do not refer to it. Solution: 412 OG must provide guidance on how to incorporate the safety information into control operations.

11. UCA: 412 OG provides guidance (training) to SPORT and JOSHUA excessively or redundantly. [H5]

A. Inadequate Control Execution: 412 OG provides specific training or guidance, but the training or guidance becomes excessive or redundant. Solution: 412 OG should periodically check on how much training or guidance is being implemented.
B. Inappropriate Decision: 412 OG believes that more training or guidance is needed, when it is not. Solution: SPORT/JOSHUA inform 412 OG when the guidance becomes excessive or redundant.
C. Inadequate Feedback and Other Inputs: 412 OG believes that more training or guidance is needed, when it is not. Solution: SPORT/JOSHUA inform 412 OG when the guidance becomes excessive or redundant.
D. Inadequate Process Behavior: 412 OG directs only specific training or guidance, but more is implemented by SPORT/JOSHUA. Solution: 412 OG should periodically check on how much training or guidance is being implemented.

12. UCA: 412 OG does not provide guidance (training) to SPORT and JOSHUA when specific guidance is necessary. [H1, H2, H3, H4, H5]

A. Inadequate Control Execution: 412 OG provides guidance, but SPORT/JOSHUA does not receive it. Solution: 412 OG must follow up with SPORT/JOSHUA to ensure guidance has been implemented.
B. Inappropriate Decision: 412 OG sees that guidance is necessary, but does not implement it.
    i. Refinement 1: 412 OG does not understand what guidance is relevant to control facility operations. Solution: A control facility representative is on hand to determine what guidance is necessary.
    ii. Refinement 2: 412 OG does not pass on guidance because they believe that it has already been accomplished. Solution: 412 OG should periodically check on what training or guidance is being implemented.
C. Inadequate Feedback and Other Inputs: 412 OG is not aware that guidance is needed. Solution: 412 OG must periodically check with SPORT/JOSHUA to determine what procedures are or are not working.
D. Inadequate Process Behavior: SPORT/JOSHUA receives guidance, but does not implement it. Solution: 412 OG must follow up with SPORT/JOSHUA to ensure guidance has been implemented.

Solutions

The above Step 2 Analysis has found the following 37 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- 412 OG must follow up with Test Unit to ensure feedback is incorporated into the safety plan. [UCA 1.A, 2.A]
- 412 OG always provides either final approval or feedback. [UCA 2.B, 3.D.ii]
- 412 OG must ask questions until they thoroughly understand the safety plan. [UCA 1.C.i. 2.C.i, 3.C.i]
- 412 OG representative(s) involved in the safety review process must undergo Hazard Analysis training. [UCA 1.C.ii, 2.C.ii, 3.C.ii, 4.C.ii, 5.C.ii, 19.D, 20.D]
- 412 OG must ensure that the review process is iterative, and continue to provide feedback until the safety plan is sufficient. [UCA 1.D, 2.D, 19.C, 20.C]
- 412 OG approval of the safety plan must be checked before test can proceed. [UCA 3.A, 5.A]
- 412 OG must check that the safety plan is complete and correct before providing approval. [UCA 3.C.ii, 10.C]
- Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan. [UCA 3.D.i, 4.D, 5.D.i]
- 412 OG must provide feedback on why safety plan was not approved. [UCA 3.D.ii, 5.D.ii]
- 412 OG must provide this feedback to the Test Unit so that they can adjust their test plan. [UCA 4.B.i, 19.D, 20.D]
- Test Unit must follow up with 412 OG if approval is not received in an appropriate amount of time. [UCA 4.A, 4.B.ii, 19.D, 20.A, 20.D]
- 412 OG must ask questions until their concerns are addressed. [UCA 4.C.i, 19.D, 20.D]
- Test Unit must be made aware of the reason(s) the plan was not approved, and given the chance to provide an updated or corrected plan. [UCA 4.C.iii, 19.A, 21.A]
- Concerns raised in the SRB must be documented and accompany the final safety package for approval. [UCA 5.C.i, 21.C.i]
- 412 OG must immediately notify the affected test unit if approval is rescinded. [UCA 6.A]
- When the additional information is presented, it should be in such a way that the safety implications are clear. [UCA 6.B.i, 6.C]
- 412 should always operate with safety as their highest priority. [UCA 1.B, 3.B, 5.B, 6.B.ii]
- 412 OG must follow up with the Test Unit to ensure testing has stopped. [UCA 6.D]
- 412 OG must receive confirmation that SPORT/JOSHUA has received the schedule. [UCA 7.A, 8.A]
- 412 OG must always pass on the airspace schedule, regardless of its importance. [UCA 7.B.i]
- 412 OG must establish a standard procedure to ensure that the schedule is passed on (specific person, time of day, etc.). [UCA 7.B.ii]
- 412 OG must ask ROC to provide airspace schedule if it has not been received. [UCA 7.C, 17.A, 17.B]
- 412 OG must provide guidance on how to incorporate the airspace schedule into planning control operations. [UCA 7.D]
- SPORT/JOSHUA inform 412 OG of what version of the schedule they are using. [UCA 8.D]
- When updated schedule is available, 412 OG updates SPORT/JOSHUA. [UCA 8.B]

- Schedule must be marked as a draft or complete when it is given to 412 OG. [UCA 8.C]
- SPORT/JOSHUA ignores irrelevant information. [UCA 9.A]
- A control facility representative is on hand to determine what information is necessary. [UCA 9.B.i, 10.B.i, 12.B.i]
- SPORT/JOSHUA provide this feedback to 412 OG, who can inform the appropriate Test Unit. [UCA 9.C]
- All safety information from 412 OG must be reviewed by one of the controllers on shift. [UCA 9.D]
- 412 OG should ensure that the information is received and reviewed. [UCA 10.A]
- 412 OG must establish a standard procedure to ensure that the information is passed on. [UCA 10.B.ii]
- 412 OG must provide guidance on how to incorporate the safety information into control operations. [UCA 10.D]
- 412 OG should periodically check on how much training or guidance is being implemented. [UCA 11.A, 11.D, 12.B.ii]
- SPORT/JOSHUA inform 412 OG when the guidance becomes excessive or redundant. [UCA 11.B, 11.C]
- 412 OG must follow up with SPORT/JOSHUA to ensure guidance has been implemented. [UCA 12.A, 12.D]
- 412 OG must periodically check with SPORT/JOSHUA to determine what procedures are or are not working. [UCA 12.C]

RESOURCE OPERATIONS CENTER (ROC)

13. UCA: The ROC informs the Test Unit of conflicts when no conflicts exist or deconflicting is possible. [H5]

A. Inadequate Control Execution: The ROC does not inform the Test Unit of conflicts, but the Test Unit believes that conflicts exist.
   i. Refinement 1: The ROC does not inform the Test Unit of conflicts, but indicates that the airspace will be active during the requested time. Solution: The ROC clearly indicates whether or not testing may proceed as requested.

B. Inappropriate Decision: No conflicts exist or deconflicting is possible, but the ROC indicates that the test cannot proceed as requested.
   i. Refinement 1: The ROC indicates that the test cannot proceed as requested because the ROC believes that two or more test missions need simultaneous access to the same airspace. Solution: The ROC should develop a way to track what airspace each mission requested.
   ii. Refinement 2: The ROC indicates that the test cannot proceed as requested because the ROC believes that the SUAS test mission is lower priority than another test mission. Solution: The ROC must check which mission has priority access, according to EAFBI 13-100.

C. Inadequate Feedback and Other Inputs: The ROC misunderstands the time or section of airspace that the Test Unit requests, and believes that a conflict exists. Solution: Before

indicating that the Test Unit must reschedule or relocate, the ROC must check the requested time and airspace.

D. Inadequate Process Behavior: The Test Unit is informed that no conflicts exist, but reschedule the mission. Solution: The ROC clearly indicates whether or not testing may proceed as requested.

14. The ROC does not inform the Test Unit of conflicts when conflicts exist. [H5]

A. Inadequate Control Execution: The ROC informs the Test Unit of conflicts, but the Test Unit does not reschedule. Solution: The ROC does not issue an Operations Number until conflicts are resolved.

B. Inappropriate Decision: Two or more missions conflict, but the ROC schedules both.
   i. Refinement 1: The ROC does not understand that the requested areas conflict. Solution: The ROC must check which airspaces cannot be simultaneously active before scheduling missions.
   ii. Refinement 2: The ROC believes that the aircraft can both use the airspace, using "sense-and-avoid" to prevent collisions. Solution: The ROC must never allow another aircraft to use the same airspace as an SUAS test mission.

C. Inadequate Feedback and Other Inputs: The ROC misunderstands the time or section of airspace that the Test Unit requests, and believes that no conflict exists. Solution: Before indicating that the Test Unit may proceed, the ROC must check the requested time and airspace.

D. Inadequate Process Behavior: The Test Unit is informed that a conflict exists, but does not reschedule the mission. Solution: The ROC does not issue an Operations Number until conflicts are resolved.

15. The ROC provides an Operations Number to the Test Unit when conflicts exist. [H5]

A. Inadequate Control Execution: The ROC does not issue an Operations Number, but the Test Unit does not reschedule. Solution: Aircraft cannot enter R-2515 without an Operations Number.

B. Inappropriate Decision: Two or more missions conflict, but the ROC provides an Operations Number.
   i. Refinement 1: The ROC does not understand that the requested areas conflict. Solution: The ROC must check which airspaces cannot be simultaneously active before scheduling missions.
   ii. Refinement 2: The ROC believes that the aircraft can both use the airspace, using "sense-and-avoid" to prevent collisions. Solution: The ROC must never allow another aircraft to use the same airspace as an SUAS test mission.

C. Inadequate Feedback and Other Inputs: The ROC misunderstands the time or section of airspace that the Test Unit requests, and believes that no conflict exists. Solution: Before indicating that the Test Unit may proceed, the ROC must check the requested time and airspace.

D. Inadequate Process Behavior: The Test Unit is informed that a conflict exists, but does not reschedule the mission. Solution: The ROC does not issue an Operations Number until conflicts are resolved.

16. The ROC does not provide an Operations Number to the Test Unit when the mission is scheduled. [H5]

A. Inadequate Control Execution: The ROC provides an Operations Number, but the Test Unit believes that conflicts exist. Solution: The ROC clearly indicates whether or not testing may proceed as requested.

B. Inappropriate Decision: No conflicts exist or deconflicting is possible, but the ROC does not issue an Operations Number.

   i. Refinement 1: The ROC indicates that the test cannot proceed as requested because the ROC believes that two or more test missions need simultaneous access to the same airspace. Solution: The ROC should develop a way to track what airspace each mission requested.

   ii. Refinement 2: The ROC indicates that the test cannot proceed as requested because the ROC believes that the SUAS test mission is lower priority than another test mission. Solution: The ROC must check which mission has priority access, according to EAFBI 13-100.

   iii. Refinement 3: The ROC indicates that there are no conflicts, but does not provide an Operations Number. The ROC must establish a standard procedure to ensure that the step is not skipped.

C. Inadequate Feedback and Other Inputs: The ROC misunderstands the time or section of airspace that the Test Unit requests, and believes that a conflict exists. Solution: Before indicating that the Test Unit must reschedule or relocate, the ROC must check the requested time and airspace.

D. Inadequate Process Behavior: The Test Unit is provided an Operations Number, but reschedules the mission. Solution: The ROC clearly indicates whether or not testing may proceed as requested.

17. The ROC does not provide the Airspace Schedule to the 412 OG when the schedule is complete. [H5]

A. Inadequate Control Execution: The ROC provides the airspace schedule, but the 412 OG does not receive it. Solution: Refer to UCA 7.C

B. Inappropriate Decision: The ROC completes the airspace schedule, but does not pass it on. Refer to UCA 7.C.

C. Inadequate Feedback and Other Inputs: The ROC does not receive all necessary information to complete the schedule. Solution: The ROC must not schedule a mission until all necessary information has been received.

D. Inadequate Process Behavior: 412 OG receives the airspace schedule, but does not pass it on. Solution: Refer to UCA 7.B.

18. The ROC provides the Airspace Schedule to the 412 OG before the schedule is complete. [H5]

A. Inadequate Control Execution: The ROC provides updated airspace schedule, but 412 OG passes on an out-of-date one. Solution: SPORT/JOSHUA inform the ROC of what version of the schedule they are using.
B. Inappropriate Decision: The ROC understands that the schedule is not complete, but passes it on to 412 OG. Solution: When updated schedule is available, The ROC updates 412 OG.
C. Inadequate Feedback and Other Inputs: The ROC is not aware that this schedule is incomplete, and passes it on. Solution: Schedule must be marked as a draft or complete when it is given to 412 OG.
D. Inadequate Process Behavior: 412 OG receives complete or updated schedule, but still passes on the incomplete one. Solution: SPORT/JOSHUA inform the ROC of what version of the schedule they are using.

The above Step 2 Analysis has found the following 15 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- The ROC clearly indicates whether or not testing may proceed as requested. [UCA 13.A, 13.D, 16.A, 16.D]
- The ROC should develop a way to track what airspace each mission requested. [UCA 13.B.i, 16.B.i]
- The ROC must check which mission has priority access, according to EAFBI 13-100. [UCA 13.B.ii, 16.B.ii]
- Before indicating that the Test Unit must reschedule or relocate, the ROC must check the requested time and airspace. [UCA 13.C, 16.C]
- The ROC does not issue an Operations Number until conflicts are resolved. [UCA 14.A, 14.D, 15.D]
- The ROC must check which airspaces cannot be simultaneously active before scheduling missions. [UCA 14.B.i, 15.B.i]
- The ROC must never allow another aircraft to use the same airspace as an SUAS test mission. [UCA 14.B.ii, 15.B.ii]
- Before indicating that the Test Unit may proceed, the ROC must check the requested time and airspace. [UCA 14.C, 15.C]
- Aircraft cannot enter R-2515 without an Operations Number. [UCA 15.A]
- The ROC must establish a standard procedure to ensure that the step is not skipped. [UCA 16.B.iii]
- 412 OG must ask ROC to provide airspace schedule if it has not been received. [UCA 7.C, 17.A, 17.B]
- The ROC must not schedule a mission until all necessary information has been received. [UCA 17.C]
- SPORT/JOSHUA inform the ROC of what version of the schedule they are using. [UCA 18.A, 18.D]
- When updated schedule is available, The ROC updates 412 OG. [UCA 18.B]
- Schedule must be marked as a draft or complete when it is given to 412 OG. [UCA 18.C]

TEST UNIT

19. The Test Unit provides the safety package to the 412 OG when safety plan is not sufficient. [H1, H2, H3, H4]

A. Inadequate Control Execution: The Test Unit provides the correct safety plan, but 412 OG reviews an old or outdated version. Solution: Refer to UCA 4.C.iii.

B. Inappropriate Decision: The Test Unit knows that the Safety Plan is not sufficient, but provides the safety package to 412 OG.
   i. Refinement 1: The Test Unit is under outside pressure to expedite testing. Solution: The Test Unit should always operate with safety as the highest priority.
   ii. Refinement 2: The Test Unit is seeking feedback rather than final approval. Solution: Safety package submitted for final approval should be clearly labeled as such.

C. Inadequate Feedback and Other Inputs: The Test Unit believes that the safety plan is sufficient, when it is not.
   i. Refinement 1: The Test Unit addressed the feedback from the SRB, but the safety plan is still insufficient. Solution: Refer to UCA 2.D

D. Inadequate Process Behavior: 412 OG receives the correct safety plan, but does not approve it. Solution: Refer to UCA 4.B, 4.C

20. The Test Unit does not provide the safety package to the 412 OG when safety plan is sufficient. [H5]

A. Inadequate Control Execution: The Test Unit provides the correct safety plan, but 412 OG does not receive it. Solution: Refer to UCA 4.A.

B. Inappropriate Decision: The Test Unit knows that the Safety Plan is sufficient, but does not provide the safety package to 412 OG.
   i. Refinement 1: Test Unit has concerns about the test that are not safety related (cost, goals, resources). Solution: Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan.

C. Inadequate Feedback and Other Inputs: The Test Unit believes that the safety plan is not sufficient.
   i. Refinement 1: The Test Unit addressed the feedback from the SRB, but unsure if there are additional issues. Solution: Refer to UCA 2.D

D. Inadequate Process Behavior: 412 OG receives the correct safety plan, but does not approve it. Solution: Refer to UCA 4.B, 4.C

21. The Test Unit provides the safety package to the 412 OG before feedback from the SRB has been addressed. [H1, H2, H3, H4]

A. Inadequate Control Execution: Test Unit submits safety plan with feedback addressed, but 412 OG reviews an old or outdated version. Solution: Refer to UCA 4.C.iii.

B. Inappropriate Decision: Test Unit understands feedback has not been addressed, but submits safety package.
   i. Refinement 1: Test Unit believes feedback is unimportant. Solution: Test Unit must document reasons the feedback is considered unimportant.

ii. Refinement 2: The Test Unit is under outside pressure to expedite testing. Solution: The Test Unit should always operate with safety as the highest priority.

C. Inadequate Feedback and Other Inputs: Feedback from the SRB is unclear.
   i. Refinement 1: Test Unit believes concerns have been addressed because Test Unit does not know what concerns were raised in the SRB. Solution: Refer to UCA 5.C.i.
   ii. Refinement 2: Test Unit believes concerns have been addressed because Test Unit does not understand hazard analysis techniques. Solution: Test Unit representative(s) involved in the safety review process must undergo Hazard Analysis training.

D. Inadequate Process Behavior: 412 OG reviews safety package before SRB feedback could be addressed. Solution: Test Unit does not send safety package to 412 OG until feedback has been addressed.

22. The Test Unit does not schedule their test with the ROC when the mission is planned to fly. [H5]

A. Inadequate Control Execution: The Test Unit sends the request, but ROC does not receive it. Solution: Test Unit confirms that ROC received and acted on the schedule request.

B. Inappropriate Decision: The Test Unit knows that the mission is planned, but does not schedule the test with the ROC.
   i. Refinement 1: The Test Unit is not aware that the ROC must be contacted to schedule the mission. Solution: Ensure personnel are aware of all steps in pre-mission planning.
   ii. Refinement 2: The Test Unit believes that the request has already been made. Solution: The Test Unit must establish a standard procedure or checklist to conduct all pre-mission scheduling.

C. Inadequate Feedback and Other Inputs: The Test Unit in not aware that the mission is ready to fly. Solution: The Test Unit designates a project representative who is kept aware of what stage the test planning is in.

D. Inadequate Process Behavior: The ROC receives the scheduling request, but does not process it. Solution: Test Unit confirms that ROC received and acted on the schedule request.

23. The Test Unit does not provide the SPORT Prebrief when the mission is planned to fly. [H1, H2, H3, H4, H5]

A. Inadequate Control Execution: The Test Unit sends the prebrief, but SPORT does not receive it. Solution: Test Unit confirms that SPORT reviewed the prebrief.

B. Inappropriate Decision: The Test Unit knows that the mission is planned, but does not provide a SPORT prebrief.
   i. Refinement 1: The Test Unit is not aware that the prebrief must be filed. Solution: Ensure personnel are aware of all steps in pre-mission planning.
   ii. Refinement 2: The Test Unit believes that the prebrief has already been sent. Solution: The Test Unit must establish a standard procedure or checklist to conduct all pre-mission scheduling.

C. Inadequate Feedback and Other Inputs: The Test Unit in not aware that the mission is ready to fly. Solution: The Test Unit designates a project representative who is kept aware of what stage the test planning is in.
D. Inadequate Process Behavior: SPORT receives the scheduling request, but does not review it. Solution: Test Unit confirms that SPORT reviewed the prebrief.

24. The Test Unit does not provide the SUAS pilot with the mission objectives. [H5]

A. Inadequate Control Execution: The Test Unit provides Mission Objectives, but the SUAS Pilot does not understand them. Solution: This is held as a conversation, with the SUAS pilot able to ask clarifying questions.
B. Inappropriate Decision: The Test Unit does not believe that the pilot needs the Mission Objectives. Solution: Incorporate the SUAS Pilot into the safety planning team.
C. Inadequate Feedback and Other Inputs: The Test Unit does not have mission objectives to pass on. Solution: The Test Planning Team, which includes the SUAS Pilot, begins by selecting mission objectives that the Test Unit can approve/disapprove.
D. Inadequate Process Behavior: The Test Unit provides Mission Objectives, but they are not used in the Test Planning Process. Solution: The Test Unit periodically reviews the test and safety plan to ensure that mission objectives are being met.

25. The Test Unit provides the SUAS pilot with the mission objectives too late in the test planning process. [H5]

A. Inadequate Control Execution: The Test Unit provides Mission Objectives, but the SUAS Pilot does receive them until late in the planning phase. Solution: Incorporate the SUAS Pilot into the safety planning team.
B. Inappropriate Decision: The Test Unit does not believe that the pilot needs the Mission Objectives. Solution: Incorporate the SUAS Pilot into the safety planning team.
C. Inadequate Feedback and Other Inputs: The Test Unit does not have mission objectives to pass on. Solution: The Test Planning Team, which includes the SUAS Pilot, begins by selecting mission objectives that the Test Unit can approve/disapprove.
D. Inadequate Process Behavior: The Test Unit provides Mission Objectives, but they are not used in the Test Planning Process until late. Solution: The Test Unit periodically reviews the test and safety plan to ensure that mission objectives are being met.

The above Step 2 Analysis has found the 15 solutions/recommendations, in addition to reinforcing six found in previous sections. The numbers in the bracket correspond to the scenarios that the solution addresses.

The six solutions that had been found previously are:

- 412 OG must ensure that the review process is iterative, and continue to provide feedback until the safety plan is sufficient. [UCA 1.D, 2.D, 19.C, 20.C]
- 412 OG must provide this feedback to the Test Unit so that they can adjust their test plan. [UCA 4.B.i, 19.D, 20.D]

- Test Unit must follow up with 412 OG if approval is not received in an appropriate amount of time. [UCA 4.B.ii, 19.D, 20.D]
- 412 OG must ask questions until their concerns are addressed. [UCA 4.A, 4.C.i, 19.D, 20.A, 20.D]
- Test Unit must be made aware of the reason(s) the plan was not approved, and given the chance to provide an updated or corrected plan. [UCA 4.C.iii, 19.A, 21.A]
- Concerns raised in the SRB must be documented and accompany the final safety package for approval. [UCA 5.C.i, 21.C.i]

The fifteen new solutions are:

- The Test Unit should always operate with safety as the highest priority. [UCA 19.B.i, 21.B.ii]
- Safety package submitted for final approval should be clearly labeled as such. [UCA 19.B.ii]
- Test Unit must re-evaluate the goals in light of the new information so that they can adjust their test plan. [UCA 20.B]
- Test Unit must document reasons the feedback is considered unimportant. [UCA 21.B.i]
- Test Unit representative(s) involved in the safety review process must undergo Hazard Analysis training. [UCA 21.C.ii]
- Test Unit does not send safety package to 412 OG until feedback has been addressed. [UCA 21.D]
- Test Unit confirms that ROC received and acted on the schedule request. [UCA 22.A, 22.D]
- Ensure personnel are aware of all steps in pre-mission planning. [UCA 22.B.i, 23.B.i]
- The Test Unit must establish a standard procedure or checklist to conduct all pre-mission scheduling. [UCA 22.B.ii, 23.B.ii]
- The Test Unit designates a project representative who is kept aware of what stage the test planning is in. [UCA 22.C, 23.C]
- Test Unit confirms that SPORT reviewed the prebrief. [UCA 23.A, 23.D]
- This is held as a conversation, with the SUAS pilot able to ask clarifying questions. [UCA 24.A]
- Incorporate the SUAS Pilot into the safety planning team. [UCA 24.B, 25.A, 25.B]
- The Test Planning Team, which includes the SUAS Pilot, begins by selecting mission objectives that the Test Unit can approve/disapprove. [UCA 24.C, 25.C]
- The Test Unit periodically reviews the test and safety plan to ensure that mission objectives are being met. [UCA 24.D, 25.D]

FLIGHT OPERATIONS PHASE

HIGH DESERT COMBINED CONTROL FACILITY (JOSHUA)

26. JOSHUA hands off an aircraft to SPORT when another JOSHUA controlled aircraft is encroaching. [H1]

A. Inadequate Control Execution: The pilot does not receive JOSHUA's radio call to stay on JOSHUA's radio frequency. Solution: Pilot must receive confirmation before changing radio frequency.
B. Inappropriate Decision: JOSHUA controller sees that the aircraft need to be maneuvered, but still hands off to SPORT.
    i. Refinement 1: JOSHUA believes that SPORT will advise aircraft. Solution: Wait until traffic is deconflicted before conducting a hand off.
    ii. Refinement 2: JOSHUA believes that the hand off aircraft does not need to adjust (will adjust the other aircraft). Solution: Wait until traffic is deconflicted before conducting a hand off.
C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that another aircraft is approaching the handoff aircraft. Solution: Nearby Traffic must be checked before conducting a hand off.
D. Inadequate Process Behavior: The Pilot changes to SPORT's radio frequency before the hand off occurs. Solution: JOSHUA immediately contacts SPORT to advise them of the situation.

27. JOSHUA does not hand off aircraft to SPORT when aircraft is entering SPORT airspace. [H1, H2, H3, H4]

A. Inadequate Control Execution: The pilot does not receive JOSHUA's radio call to contact SPORT. Solution: JOSHUA repeats radio call.
B. Inappropriate Decision: JOSHUA controller sees that the aircraft need to be handed off, but does not do so.
    i. Refinement 1: JOSHUA believes that SPORT will hand off the airspace. Solution: Airspace hand offs must happen before the aircraft crosses the boundary.
    ii. Refinement 2: JOSHUA's workload makes other tasks a priority. Solution: Provide feedback to 412 OG to ensure manpower is appropriate to the workload.
C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the aircraft is approaching SPORT airspace. Solution: Pilots must contact JOSHUA before transitioning to SPORT airspace.
D. Inadequate Process Behavior: The pilot remains on JOSHUA's radio frequency after the hand off occurs. Solution: SPORT immediately contacts JOSHUA to advise them of the situation.

28. JOSHUA hands off airspace to SPORT without handing off aircraft in the airspace. [H1]

A. Inadequate Control Execution: The pilot(s) do not receive JOSHUA's radio call to contact SPORT. Solution: JOSHUA repeats radio call.
B. Inappropriate Decision: JOSHUA controller sees that the aircraft need to be handed off, but does not do so.
    i. Refinement 1: JOSHUA is handing off both aircraft and airspace. Solution: Aircraft hand offs must happen before the aircraft crosses the boundary.
    ii. Refinement 2: JOSHUA's workload makes other tasks a priority. Solution: Provide feedback to 412 OG to ensure manpower is appropriate to the workload.

C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the aircraft is in the hand off airspace. Solution: Nearby Traffic must be checked before conducting a hand off.
D. Inadequate Process Behavior: The pilot remains on JOSHUA's radio frequency after the hand off occurs. Solution: SPORT immediately contacts JOSHUA to advise them of the situation.

29. JOSHUA provides an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]

A. Inadequate Control Execution: JOSHUA does not give clearance, but the pilot hears that they have clearance. Solution: Pilot must receive confirmation before entering the airspace.
B. Inappropriate Decision: JOSHUA controller sees that the airspace is unsafe, but provides clearance.
    i. Refinement 1: JOSHUA believes that aircraft is requesting clearance to a different airspace. Solution: When giving an airspace clearance, JOSHUA specifies which airspace the clearance is for.
C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the airspace is unsafe. Solution: Airspace must be checked before providing or denying clearance.
D. Inadequate Process Behavior: JOSHUA does not give clearance, but the pilot enters the airspace. Solution: JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

30. JOSHUA does not provide an aircraft with a clearance when the airspace is safe. [H5]

A. Inadequate Control Execution: JOSHUA gives clearance, but the pilot does not hear that they have clearance. Solution: JOSHUA repeats radio call.
B. Inappropriate Decision: JOSHUA controller sees that the airspace is safe, but does not provides clearance.
    i. Refinement 1: JOSHUA believes that aircraft is requesting clearance to a different airspace. Solution: When giving an airspace clearance, JOSHUA specifies which airspace the clearance is for.
    ii. Refinement 2: This airspace is about to become unsafe or occupied. Note: This is Acceptable.
C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the airspace is safe. Solution: Airspace must be checked before providing or denying clearance.
D. Inadequate Process Behavior: JOSHUA gives clearance, but the pilot does not enter the airspace. Solution: JOSHUA repeats radio call, and if necessary, rescinds clearance.

31. JOSHUA provides an aircraft with a clearance that is not rescinded when the airspace is no longer safe. [H1, H2, H3, H4]

A. Inadequate Control Execution: JOSHUA rescinds clearance, but the pilot does not hear the transmission. Solution: JOSHUA repeats radio call. If necessary, JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.
B. Inappropriate Decision: JOSHUA controller sees that the airspace is no longer safe, but does not rescind clearance.

i. Refinement 1: JOSHUA believes that aircraft is no longer in the airspace. Solution: Before an airspace becomes unsafe, JOSHUA checks to ensure that it is empty.
ii. Refinement 2: JOSHUA believes that this aircraft is the one requesting access (spin areas, drop zones, PIRA, etc.). Solution: JOSHUA confirms that the aircraft is the one that requested access.

C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the airspace is unsafe. Solution: JOSHUA should periodically check which sections of the airspace are off-limits, "active," or otherwise unsafe.
D. Inadequate Process Behavior: JOSHUA rescinds clearance, but the pilot does not exit the airspace. Solution: JOSHUA repeats radio call. If necessary, JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

32. JOSHUA does not provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]

A. Inadequate Control Execution: JOSHUA provides traffic advisories, but the pilot does not hear the transmission. Solution: JOSHUA repeats radio call. If necessary, JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.
B. Inappropriate Decision: JOSHUA controller sees that another aircraft is approaching, but does not provide traffic advisory.
    i. Refinement 1: JOSHUA believes that aircraft see one another and will avoid each other. Solution: JOSHUA confirms that both aircraft have the other in sight.
    ii. Refinement 2: JOSHUA believes that the aircraft are far enough apart to avoid a collision. Solution: 412 OG provides guidance on what the acceptable distance between aircraft is.
C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that another aircraft is nearby or approaching. Solution: JOSHUA should periodically check the location and direction of all aircraft in their airspace.
D. Inadequate Process Behavior: JOSHUA provides traffic advisories, but the pilot does not adjust course. Solution: JOSHUA repeats radio call. If necessary, JOSHUA provides new heading or altitude to avoid collision, or contacts other pilot to give them a new heading or altitude.

33. JOSHUA provides an aircraft with traffic advisories too late for corrective action. [H1, H2, H3, H4]

A. Inadequate Control Execution: JOSHUA provides traffic advisories, but the pilot does not hear the transmission. Solution: JOSHUA repeats radio call. If necessary, JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.
B. Inappropriate Decision: JOSHUA controller sees that another aircraft is approaching, but does not provide traffic advisory.
    i. Refinement 1: JOSHUA believes that aircraft see one another and will avoid each other. Solution: JOSHUA confirms that both aircraft have the other in sight.

ii. Refinement 2: JOSHUA believes that the aircraft are far enough apart to avoid a collision. Solution: 412 OG provides guidance on what the acceptable distance between aircraft is.

C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that another aircraft is nearby or approaching. Solution: JOSHUA should periodically check the location and direction of all aircraft in their airspace.

D. Inadequate Process Behavior: JOSHUA provides traffic advisories, but the pilot does not adjust course. Solution: JOSHUA repeats radio call. If necessary, JOSHUA provides new heading or altitude to avoid collision, or contacts other pilot to give them a new heading or altitude.

34. JOSHUA provides an aircraft with a traffic advisory that is not rescinded when the encroaching aircraft is no longer a factor. [H5]

A. Inadequate Control Execution: JOSHUA rescinds traffic advisory, but the pilot does not hear the transmission. Solution: JOSHUA repeats radio call.

B. Inappropriate Decision: JOSHUA controller sees that the encroaching aircraft is no longer a factor, but does not rescind traffic advisory.

i. Refinement 1: JOSHUA believes that aircraft see one another and are aware of the situation. Solution: JOSHUA confirms that both aircraft have the other in sight.

C. Inadequate Feedback and Other Inputs: JOSHUA is not aware that the aircraft is no longer nearby or approaching. Solution: JOSHUA should continuously monitor any aircraft that is encroaching on another's airspace.

D. Inadequate Process Behavior: JOSHUA rescinds traffic advisories, but the pilot does not adjust course. Solution: JOSHUA repeats radio call. Note: This is acceptable.

The Step 2 Analyses for JOSHUA and SPORT are very similar; therefore, the solutions found above will be listed with those found for SPORT.

AFTC Military Radar Unit (SPORT)

35. SPORT hands off an aircraft to JOSHUA when another SPORT controlled aircraft is encroaching. [H1]

A. Inadequate Control Execution: The pilot does not receive SPORT's radio call to stay on SPORT's radio frequency. Solution: Pilot must receive confirmation before changing radio frequency.

B. Inappropriate Decision: SPORT controller sees that the aircraft need to be maneuvered, but still hands off to JOSHUA.

i. Refinement 1: SPORT believes that JOSHUA will advise aircraft. Solution: Wait until traffic is deconflicted before conducting a hand off.

ii. Refinement 2: SPORT believes that the hand off aircraft does not need to adjust. Solution: Wait until traffic is deconflicted before conducting a hand off.

C. Inadequate Feedback and Other Inputs: SPORT is not aware that another aircraft is approaching the handoff aircraft. Solution: Nearby Traffic must be checked before conducting a hand off.

D. Inadequate Process Behavior: The Pilot changes to SPORT's radio frequency before the hand off occurs. Solution: SPORT immediately contacts JOSHUA to advise them of the situation.

36. SPORT does not hand off aircraft to JOSHUA when aircraft is entering JOSHUA airspace. [H1]

A. Inadequate Control Execution: The pilot does not receive SPORT's radio call to contact JOSHUA. Solution: SPORT repeats radio call.
B. Inappropriate Decision: SPORT controller sees that the aircraft need to be handed off, but does not do so.
    i. Refinement 1: SPORT believes that JOSHUA will hand off the airspace. Solution: Airspace hand offs must happen before the aircraft crosses the boundary.
    ii. Refinement 2: SPORT's workload makes other tasks a priority. Solution: Provide feedback to 412 OG to ensure manpower is appropriate to the workload.
C. Inadequate Feedback and Other Inputs: SPORT is not aware that the aircraft is approaching JOSHUA airspace. Solution: Pilots must contact SPORT before transitioning to JOSHUA airspace.
D. Inadequate Process Behavior: The pilot remains on SPORT's radio frequency after the hand off occurs. Solution: JOSHUA immediately contacts SPORT to advise them of the situation.

37. SPORT does not hand off aircraft to JOSHUA when aircraft is requesting IFR clearance. [H1, H3]

A. Inadequate Control Execution: The pilot does not receive SPORT's radio call to contact JOSHUA. Solution: SPORT repeats radio call.
B. Inappropriate Decision: SPORT controller sees that the aircraft is requesting IFR clearance, but does not hand off the aircraft.
    i. Refinement 1: SPORT believes that they can give IFR clearance. Solution: 412 OG provides training on IFR clearances.
    ii. Refinement 2: SPORT's workload makes other tasks a priority. Solution: Provide feedback to 412 OG to ensure manpower is appropriate to the workload.
C. Inadequate Feedback and Other Inputs: SPORT is not aware that the aircraft requires IFR clearance. Solution: Pilot repeats radio call.
D. Inadequate Process Behavior: The pilot remains on SPORT's radio frequency after the hand off occurs. Solution: JOSHUA immediately contacts SPORT to advise them of the situation.

38. SPORT hands off airspace to JOSHUA without handing off aircraft in the airspace. [H1]

A. Inadequate Control Execution: The pilot(s) do not receive SPORT's radio call to contact JOSHUA. Solution: SPORT repeats radio call.
B. Inappropriate Decision: SPORT controller sees that the aircraft need to be handed off, but does not do so.
    i. Refinement 1: SPORT is handing off both aircraft and airspace. Solution: Aircraft hand offs must happen before the aircraft crosses the boundary.
    ii. Refinement 2: SPORT's workload makes other tasks a priority. Solution: Provide feedback to 412 OG to ensure manpower is appropriate to the workload.

C. Inadequate Feedback and Other Inputs: SPORT is not aware that the aircraft is in the hand off airspace. Solution: Nearby Traffic must be checked before conducting a hand off.
D. Inadequate Process Behavior: The pilot remains on SPORT's radio frequency after the hand off occurs. Solution: JOSHUA immediately contacts SPORT to advise them of the situation.

39. SPORT provides an aircraft with a clearance when the airspace is unsafe. [H1, H2, H3, H4]

A. Inadequate Control Execution: SPORT does not give clearance, but the pilot hears that they have clearance. Solution: Pilot must receive confirmation before entering the airspace.
B. Inappropriate Decision: SPORT controller sees that the airspace is unsafe, but provides clearance.
    i. Refinement 1: SPORT believes that aircraft is requesting clearance to a different airspace. Solution: When giving an airspace clearance, SPORT specifies which airspace the clearance is for.
C. Inadequate Feedback and Other Inputs: SPORT is not aware that the airspace is unsafe. Solution: Airspace must be checked before providing or denying clearance.
D. Inadequate Process Behavior: SPORT does not give clearance, but the pilot enters the airspace. Solution: SPORT immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

40. SPORT does not provide an aircraft with a clearance when the airspace is safe. [H5]

A. Inadequate Control Execution: SPORT gives clearance, but the pilot does not hear that they have clearance. Solution: SPORT repeats radio call.
B. Inappropriate Decision: SPORT controller sees that the airspace is safe, but does not provides clearance.
    i. Refinement 1: SPORT believes that aircraft is requesting clearance to a different airspace. Solution: When giving an airspace clearance, SPORT specifies which airspace the clearance is for.
    ii. Refinement 2: This airspace is about to become unsafe or occupied. Note: This is Acceptable.
C. Inadequate Feedback and Other Inputs: SPORT is not aware that the airspace is safe. Solution: Airspace must be checked before providing or denying clearance.
D. Inadequate Process Behavior: SPORT gives clearance, but the pilot does not enter the airspace. Solution: SPORT repeats radio call, and if necessary, rescinds clearance.

41. SPORT provides an aircraft with a clearance that is not rescinded when the airspace is no longer safe. [H1, H2, H3, H4]

A. Inadequate Control Execution: SPORT rescinds clearance, but the pilot does not hear the transmission. Solution: SPORT repeats radio call. If necessary, SPORT immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.
B. Inappropriate Decision: SPORT controller sees that the airspace is no longer safe, but does not rescind clearance.
    i. Refinement 1: SPORT believes that aircraft is no longer in the airspace. Solution: Before an airspace becomes unsafe, SPORT checks to ensure that it is empty.

ii. Refinement 2: SPORT believes that this aircraft is the one requesting access (spin areas, drop zones, PIRA, etc.). Solution: SPORT confirms that the aircraft is the one that requested access.

C. Inadequate Feedback and Other Inputs: SPORT is not aware that the airspace is unsafe. Solution: SPORT should periodically check which sections of the airspace are off-limits, "active," or otherwise unsafe.

D. Inadequate Process Behavior: SPORT rescinds clearance, but the pilot does not exit the airspace. Solution: SPORT repeats radio call. If necessary, SPORT immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

42. SPORT does not provide an aircraft with traffic advisories when another aircraft is nearby or approaching. [H1, H2]

A. Inadequate Control Execution: SPORT provides traffic advisories, but the pilot does not hear the transmission. Solution: SPORT repeats radio call. If necessary, SPORT immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

B. Inappropriate Decision: SPORT controller sees that another aircraft is approaching, but does not provide traffic advisory.

i. Refinement 1: SPORT believes that aircraft see one another and will avoid each other. Solution: SPORT confirms that both aircraft have the other in sight.

ii. Refinement 2: SPORT believes that the aircraft are far enough apart to avoid a collision. Solution: 412 OG provides guidance on what the acceptable distance between aircraft is.

C. Inadequate Feedback and Other Inputs: SPORT is not aware that another aircraft is nearby or approaching. Solution: SPORT should periodically check the location and direction of all aircraft in their airspace (checks should occur more frequently as traffic increases).

D. Inadequate Process Behavior: SPORT provides traffic advisories, but the pilot does not adjust course. Solution: SPORT repeats radio call. If necessary, SPORT provides new heading or altitude to avoid collision, or contacts other pilot to give them a new heading or altitude.

43. SPORT provides an aircraft with traffic advisories too late for corrective action. [H1, H2, H3, H4]

A. Inadequate Control Execution: SPORT provides traffic advisories, but the pilot does not hear the transmission. Solution: SPORT repeats radio call. If necessary, SPORT immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment.

B. Inappropriate Decision: SPORT controller sees that another aircraft is approaching, but does not provide traffic advisory.

iii. Refinement 1: SPORT believes that aircraft see one another and will avoid each other. Solution: SPORT confirms that both aircraft have the other in sight.

iv. Refinement 2: SPORT believes that the aircraft are far enough apart to avoid a collision. Solution: 412 OG provides guidance on what the acceptable distance between aircraft is.

C. Inadequate Feedback and Other Inputs: SPORT is not aware that another aircraft is nearby or approaching. Solution: SPORT should periodically check the location and direction of all aircraft in their airspace.
D. Inadequate Process Behavior: SPORT provides traffic advisories, but the pilot does not adjust course. Solution: SPORT repeats radio call. If necessary, SPORT provides new heading or altitude to avoid collision, or contacts other pilot to give them a new heading or altitude.

44. SPORT provides an aircraft with a traffic advisory that is not rescinded when the encroaching aircraft is no longer a factor. [H5]

A. Inadequate Control Execution: SPORT rescinds traffic advisory, but the pilot does not hear the transmission. Solution: SPORT repeats radio call.
B. Inappropriate Decision: SPORT controller sees that the encroaching aircraft is no longer a factor, but does not rescind traffic advisory.
    ii. Refinement 1: SPORT believes that aircraft see one another and are aware of the situation. Solution: SPORT confirms that both aircraft have the other in sight.
C. Inadequate Feedback and Other Inputs: SPORT is not aware that the encroaching aircraft. Solution: SPORT should continuously monitor any aircraft that is encroaching on another's airspace.
D. Inadequate Process Behavior: SPORT rescinds traffic advisories, but the pilot does not adjust course. Solution: SPORT repeats radio call. Note: This is acceptable.

The above Step 2 Analysis has found the following 24 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- Pilot must receive confirmation before changing radio frequency. [UCA 26.A, 35.A]
- Wait until traffic is deconflicted before conducting a hand off. [UCA 26.B, 35.B]
- Nearby Traffic must be checked before conducting a hand off. [UCA 26.C, 28.C, 35.C, 38.C]
- SPORT/JOSHUA repeats radio call. [UCA 27.A, 28.A, 30.A, 34.A, 34.D, 36.A, 37.A, 38.A, 40.A, 44.A, 44.D]
- Airspace hand offs must happen before the aircraft crosses the boundary. [UCA 27.B.i, 36.B.i]
- Provide feedback to 412 OG to ensure manpower is appropriate to the workload. [UCA 27.B.ii, 28.B.ii, 36.B.ii, 37.B.ii, 38.B.ii]
- Pilots must contact SPORT/JOSHUA before transitioning to SPORT/JOSHUA airspace. [UCA 27.C, 36.C]
- SPORT/JOSHUA immediately contacts JOSHUA/SPORT to advise them of the situation. [UCA 26.D, 27.D, 28.D, 29.D, 35.D, 36.D, 37.D, 38.D, 39.D]
- 412 OG provides training on IFR clearances. [UCA 37.B.i]
- Pilot repeats radio call. [UCA 37.C]
- Aircraft hand offs must happen before the aircraft crosses the boundary. [UCA 28.B.i, 38.B.i]
- Pilot must receive confirmation before entering the airspace. [UCA 29.A, 39.A]
- When giving an airspace clearance, SPORT/JOSHUA specifies which airspace the clearance is for. [UCA 29.B, 30.B, 39.B, 40.B]

- Airspace must be checked before providing or denying clearance. [UCA 29.C, 30.C, 39.C, 40.C]
- SPORT/JOSHUA repeats radio call, and if necessary, rescinds clearance. [UCA 30.D, 40.D]
- SPORT/JOSHUA repeats radio call. If necessary, SPORT/JOSHUA immediately contacts the pilot(s) in the airspace, as well as any ground units (shooting range, etc.) to inform them of the encroachment. [UCA 31.A, 31.D, 32.A, 33.A, 41.A, 41.D, 42.A, 43.A]
- Before an airspace becomes unsafe, SPORT/JOSHUA checks to ensure that it is empty. [UCA 31.B.i, 41.B.i]
- SPORT/JOSHUA confirms that the aircraft is the one that requested access. [UCA 31.B.ii, 41.B.ii]
- SPORT/JOSHUA should periodically check which sections of the airspace are off-limits, "active," or otherwise unsafe. [UCA 31.C, 41.C]
- SPORT/JOSHUA confirms that both aircraft have the other in sight. [UCA 32.B.i, 33.B.i, 34.B, 42.B.i, 43.B.i, 44.B]
- 412 OG provides guidance on what the acceptable distance between aircraft is. [UCA 32.B.ii, 33.B.ii, 42.B.ii, 43.B.ii]
- SPORT/JOSHUA should periodically check the location and direction of all aircraft in their airspace (checks should occur more frequently as traffic increases). [UCA 32.C, 33.C, 42.C, 43.C]
- SPORT/JOSHUA repeats radio call. If necessary, SPORT/JOSHUA provides new heading or altitude to avoid collision, or contacts other pilot to give them a new heading or altitude. [UCA 32.D, 33.D, 42.D, 43.D]
- SPORT/JOSHUA should continuously monitor any aircraft that is encroaching on another's airspace. [UCA 34.C, 44.C]

TEST UNIT

45. The Test Unit provides guidance to the pilot that is excessive, redundant, or distracting. [H1, H2, H3, H4, H5]

A. Inadequate Control Execution: Multiple people attempt to provide guidance, which results in guidance that is excessive/redundant/distracting. Solution: Test Unit appoints one person to communicate directly with the pilot during the test.
B. Inappropriate Decision: Test Unit is aware that the pilot is receiving excessive guidance, but continues to provide it. Solution: Pilot has the authority to ask for less communication.
C. Inadequate Feedback and Other Inputs: Test unit is not aware that guidance is excessive/redundant/distracting. Solution: Pilot has the authority to ask for less communication.
D. Inadequate Process Behavior: n/a

46. The Test Unit does not provide guidance to the pilot when the pilot requests guidance. [H1, H2, H3, H4, H5]

A. Inadequate Control Execution: The Test Unit provides guidance, but pilot is unable to use it.
    i. Refinement 1: Pilot is not able to hear guidance. Solution: Test Unit appoints one person to communicate directly with the pilot during the test. If communication is not possible, pilot uses his/her best judgement.

ii. Refinement 2: Pilot is not able to understand guidance. Solution: Pilot is encouraged to ask clarifying questions.

B. Inappropriate Decision: Test Unit is aware that the pilot is requesting guidance, but does not provide it.
   i. Refinement 1: Test Unit does not know the answer. Solution: Pilot is informed while the Test Unit works on the problem.

C. Inadequate Feedback and Other Inputs: Test unit is not aware that guidance is required. Solution: Pilot asks for guidance, or if guidance is not available, uses his/her best judgement.

D. Inadequate Process Behavior: Test unit provides guidance, but the problem with the test remains. Solution: Continue to iterate or end the test.

47. The Test Unit provides guidance to the pilot too late for corrective action. [H1, H2, H3, H4]

A. Inadequate Control Execution: The Test Unit provides guidance, but pilot is unable to use it.
   i. Refinement 1: Pilot is not able to hear guidance. Solution: Test Unit appoints one person to communicate directly with the pilot during the test.
   ii. Refinement 2: Pilot is not able to understand. Solution: Pilot is encouraged to ask clarifying questions.

B. Inappropriate Decision: Test Unit is aware that the pilot is requesting guidance, but does not provide it.
   i. Refinement 1: Test Unit does not know the answer. Solution: Pilot is informed while the Test Unit works on the problem. In the interim, the pilot uses his/her best judgement.

C. Inadequate Feedback and Other Inputs: Test unit is not aware that guidance is required. Solution: Pilot asks for guidance, or if guidance is not available, uses his/her best judgement.

D. Inadequate Process Behavior: Test unit provides guidance, but the problem with the test remains. Solution: Continue to iterate or end the test.

48. The Test Unit provides guidance to the pilot but stops before the situation is resolved. [H1, H2, H3, H4]

A. Inadequate Control Execution: Pilot is no longer able to hear guidance. Solution: Pilot asks for guidance, or if guidance is not available, uses his/her best judgement.

B. Inappropriate Decision: Test Unit is aware that the situation is unresolved, but stops providing guidance.
   i. Refinement 1: Test Unit does not know the answer. Solution: Pilot is informed while the Test Unit works on the problem. In the interim, the pilot uses his/her best judgement.
   ii. Refinement 2: Test Unit believes that no more guidance is required. Solution: Pilot asks for guidance.

C. Inadequate Feedback and Other Inputs: Test unit is not aware that situation remains unresolved. Solution: Pilot asks for guidance, or if guidance is not available, uses his/her best judgement.

D. Inadequate Process Behavior: Test unit provides guidance, but the problem with the test remains. Solution: Continue to iterate or end the test.

The above Step 2 Analysis has found the following 6 safety recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- Test Unit appoints one person to communicate directly with the pilot during the test If communication is not possible, pilot uses his/her best judgement. [UCA 45.A, 46.A.i, 47.A.i]
- Pilot has the authority to ask for less communication. [UCA 45.B, 45.C]
- Pilot is encouraged to ask questions. [UCA 46.A.ii, 47.A.ii]
- Pilot asks for guidance, or if guidance is not available, uses his/her best judgement. [UCA 46.C, 47.C, 48.A, 48.B.ii, 48.C]
- Continue to iterate or end the test. [UCA 46.D, 47.D, 48.C]
- Pilot is informed while the Test Unit works on the problem. In the interim, the pilot uses his/her best judgement. [UCA 46.B, 47.B, 48.B.i]

PILOT

49. The SUAS Pilot provides route commands in a direction that the SUAV should not go. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides appropriate commands, but the SUAV receives different commands.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate route commands.
   i. Refinement 1: Pilot intends that the SUAV go in the correct direction, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will send the SUAV in an incorrect direction.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV position or orientation. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

D. Inadequate Process Behavior: SUAS Pilot provides correct route commands, but the SUAS goes in an incorrect direction. Solution: Stop testing immediately and determine the cause of the deviation.

50. The SUAS Pilot does not provide route commands when the SUAV needs to change direction. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides appropriate commands, but the SUAV does not receive them.
   i. Refinement 1: The software that translates and sends the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that blocked the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but does not provide route commands.
   i. Refinement 1: Pilot intends to send route commands, but does not. Solution: Ensure that SUAS pilot workload is appropriate so that attention can be focused on flying the test. Establish procedures and checklists as necessary.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands are needed.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV position or orientation. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

D. Inadequate Process Behavior: SUAS Pilot provides correct route commands, but the SUAS goes in an incorrect direction. Solution: Stop testing immediately and determine the cause of the deviation.

51. The SUAS Pilot provides route commands when the SUAV should not change direction. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot does not provide route commands, but the SUAV receives commands.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate route commands.
   i. Refinement 1: Pilot intends that the SUAV go in the correct direction, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will send the SUAV in an incorrect direction.

i. Refinement 1: SUAS Pilot is unaware of the SUAV position or orientation. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot.
ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

D. Inadequate Process Behavior: SUAS Pilot does not provide route commands, but the SUAS goes in an incorrect direction. Solution: Stop testing immediately and determine the cause of the deviation.

52. The SUAS Pilot provides route commands that are stopped before the change in direction is complete. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides route commands appropriately, but the SUAV receives a different transmission.
i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate route commands.
i. Refinement 1: Pilot intends that the SUAV go in the correct direction, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were stopped too soon.
i. Refinement 1: SUAS Pilot is unaware of the SUAV position or orientation, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot.
ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
iii. Refinement 3: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual orientation to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides route commands, but the SUAV stops executing them prematurely. Solution: Stop testing immediately and determine the cause of the deviation.

53. The SUAS Pilot provides route commands that are held after the change in direction is complete. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides route commands appropriately, but the SUAV receives a different transmission.

i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate route commands.
i. Refinement 1: Pilot intends that the SUAV go in the correct direction, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were held too long.
i. Refinement 1: SUAS Pilot is unaware of the SUAV position or orientation, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot.
ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
iii. Refinement 3: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual orientation to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides route commands, but the SUAV continues holding them for too long. Solution: Stop testing immediately and determine the cause of the deviation.

54. The SUAS Pilot provides speed commands to the SUAV when a change in speed is not appropriate. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides appropriate commands, but the SUAV receives different commands.
i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV speed, but provides inappropriate speed commands.
i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will incorrectly change the SUAV speed.

i. Refinement 1: SUAS Pilot is unaware of the SUAV speed. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.
ii. Refinement 2: SUAS Pilot is unaware of the appropriate speed or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

D. Inadequate Process Behavior: SUAS Pilot provides correct speed commands, but the SUAS executes them incorrectly. Solution: Stop testing immediately and determine the cause of the deviation.

55. The SUAS Pilot does not provide speed commands to the SUAV when a change in speed is appropriate. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides appropriate commands, but the SUAV does not receive them.
i. Refinement 1: The software that translates and sends the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
ii. Refinement 2: There was some sort of interference that blocked the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV speed, but does not provide speed commands.
i. Refinement 1: Pilot intends to send speed commands, but does not. Solution: Ensure that SUAS pilot workload is appropriate so that attention can be focused on flying the test. Establish procedures and checklists as necessary.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands are needed.
i. Refinement 1: SUAS Pilot is unaware of the SUAV speed. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.
ii. Refinement 2: SUAS Pilot is unaware of the appropriate speed or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

D. Inadequate Process Behavior: SUAS Pilot provides correct speed commands, but the SUAS executes them incorrectly. Solution: Stop testing immediately and determine the cause of the deviation.

56. The SUAS Pilot provides speed commands that are stopped before the change in speed is complete. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides speed commands appropriately, but the SUAV receives a different transmission.
i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.

ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV speed, but provides inappropriate commands.
   i. Refinement 1: Pilot intends to provide a speed command, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were stopped too soon.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV speed, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of the appropriate speed or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
   iii. Refinement 3: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides speed commands, but the SUAV stops executing them prematurely. Solution: Stop testing immediately and determine the cause of the deviation.

57. The SUAS pilot provides speed commands that are held after the change in speed is complete. [H1, H3]

A. Inadequate Control Execution: The SUAS pilot provides speed commands appropriately, but the SUAV receives a different transmission.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV speed, but provides inappropriate commands.
   i. Refinement 1: Pilot intends that the SUAV to change speed, but sends the wrong command(s). Solution: The system has some sort of verification or check before sending complex commands.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were held too long.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV speed, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source

(chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.

ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

iii. Refinement 3: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides speed commands, but the SUAV continues holding them for too long. Solution: Stop testing immediately and determine the cause of the deviation.

58. The SUAS Pilot provides payload commands when the payload should not be released. [H2, H4]

1. Inadequate Control Execution: The SUAS pilot does not provide commands, but the SUAV receives commands.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.
2. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate payload commands.
   i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.
   ii. Refinement 2: Pilot is unaware of proper payload drop procedure(s). Solution: SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission.
3. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will incorrectly affect SUAV payload.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV payload status. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of the appropriate drop zone or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
4. Inadequate Process Behavior: SUAS Pilot correctly does not provide payload commands, but the SUAS executes them. Solution: Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

59. The SUAS Pilot does not provide payload commands when the payload should be released. [H2, H4]

A. Inadequate Control Execution: The SUAS pilot provides commands, but the SUAV does not receive commands.
    i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
    ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.
B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but does not provide payload commands.
    i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.
    ii. Refinement 2: Pilot is unaware of proper payload drop procedure(s). Solution: SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission.
C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will incorrectly affect SUAV payload.
    i. Refinement 1: SUAS Pilot is unaware of the SUAV payload status. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
    ii. Refinement 2: SUAS Pilot is unaware of the appropriate drop zone or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
D. Inadequate Process Behavior: SUAS Pilot correctly provides payload commands, but the SUAS executes them incorrectly. Solution: Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

60. The SUAS Pilot does not provide payload commands when sensor reconfiguration is necessary. [H1, H2, H3, H4, H5]

A. Inadequate Control Execution: The SUAS pilot provides commands, but the SUAV does not receive commands.
    i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
    ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands.
B. Inappropriate Decision: SUAS pilot is aware of the SUAV location and sensor configuration, but does not provide sensor commands.
    i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.

ii. Refinement 2: Pilot is unaware of proper sensor configuration(s). SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands will be needed to affect SUAV sensors.
   i. Refinement 1: SUAS Pilot is unaware of the SUAV sensor status. Solution: Ensure that the SUAS software allows the pilot to check the sensor status

D. Inadequate Process Behavior: SUAS Pilot correctly provides payload commands, but the SUAS executes them incorrectly. Solution: Stop testing immediately and determine the cause of the deviation.

61. The SUAS Pilot provides payload commands that continue after the SUAV exits the payload drop zone [H2, H4]

A. Inadequate Control Execution: The SUAS pilot provides payload commands appropriately, but the SUAV receives a different transmission.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot. These commands should not involve deploying the payload.

B. Inappropriate Decision: SUAS pilot is aware of the SUAV location, but provides inappropriate commands.
   i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.
   ii. Refinement 2: Pilot is unaware of proper payload drop procedure(s). Solution: SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were held too long.
   i. Refinement 1: SUAS Pilot is unaware of the payload configuration, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of the appropriate direction or the airspace boundary. Solution: SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight.
   iii. Refinement 3: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides proper payload commands, but the SUAV continues holding them for too long. Solution: SUAV should be programmed not to cross an

airspace boundary while in the process of deploying a payload, unless the pilot specifies this course of action.

62. The SUAS Pilot provides payload commands that stop before the payload can fully release. [H2, H4]

A. Inadequate Control Execution: The SUAS pilot provides payload commands appropriately, but the SUAV receives a different transmission.
   i. Refinement 1: The software that translates the commands did not do so appropriately. Solution: Prior to flight testing, the command software should be tested on the ground.
   ii. Refinement 2: There was some sort of interference that affected the commands. Solution: Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot. These commands should return payload to a safe state.

B. Inappropriate Decision: SUAS pilot is aware that the payload has not fully released, but provides inappropriate commands.
   i. Refinement 1: Pilot sends the wrong command(s). Solution: The system has some sort of verification or check before sending any payload commands.
   ii. Refinement 2: Payload drop had to be aborted after the command was sent. Solution: Stop testing immediately and land as soon as conditions permit to deal with the payload on the ground. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

C. Inadequate Feedback and Other Inputs: SUAS Pilot is unaware that the commands were stopped too soon.
   i. Refinement 1: SUAS Pilot is unaware of the payload configuration, or system lag makes these readings unusable for real-time maneuvering. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.
   ii. Refinement 2: SUAS Pilot is unaware of how quickly the SUAV reacts to commands. Solution: Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot.

D. Inadequate Process Behavior: SUAS Pilot provides proper payload commands, but the SUAV stops executing them too soon. Solution: Stop testing immediately and land as soon as conditions permit to deal with the payload on the ground. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

The above Step 2 Analysis has found the following 16 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- Prior to flight testing, the command software should be tested on the ground. [UCA 49.A.i, 50.A.i, 51.A.i, 52.A.i, 53.A.i, 54.A.i, 55.A.i, 56.A.i, 57.A.i, 58.A.i, 59.A.i, 60.A.i, 61.A.i, 62.A.i]

- Command data package should include a checksum or similar feature that must be verified in order for the SUAV to follow the commands. [UCA 49.B.ii, 51.A.ii, 54.A.ii, 58.A.ii, 59.A.ii, 60.A.ii]
- The system has some sort of verification or check before sending complex commands. [UCA 49.B, 51.B, 52.B, 53.B, 54.B, 56.B, 57.B]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot. [UCA 49.C.i, 50.C.i, 51.C.i, 52.C.i, 53.C.i]
- SUAS Pilot reviews flight plan and airspace boundaries prior to testing, and has access to this information to reference during the flight. [UCA 49.C.ii, 50.C.ii, 51.C.ii, 52.C.ii, 53.C.ii, 54.C.ii, 55.C.ii, 56.C.ii, 57.C.ii, 58.C.ii, 59.C.ii, 60.C.ii, 61.C.ii]
- Stop testing immediately and determine the cause of the deviation. [UCA 49.D, 50.D, 51.D, 52.D, 53.D, 54.D, 55.D, 56.D, 57.D, 60.D]
- Ensure that SUAS pilot workload is appropriate so that attention can be focused on flying the test. Establish procedures and checklists as necessary. [UCA 50.B, 55.B]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual orientation to the pilot. [UCA 52.C.iii, 53.c.III]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual speed to the pilot. [UCA 54.C.i, 55.C.i, 56.C.i, 56.C.iii, 57.C.i, 57.C.iii]
- The system has some sort of verification or check before sending any payload commands. [UCA 58.B.i, 59.B.i, 60.B.i, 61.B.i, 62.B.i]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual payload status to the pilot. [UCA 58.C.i, 59.C.i, 61.C.i, 61.C.iii, 62.C.i, 62.C.ii]
- Stop testing immediately and determine the cause of the deviation. In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people. [UCA 58.D, 59.D, 62.B.ii, 62.D]
- SUAS Pilot must review the appropriate guidance from EABFI 13-100 and any relevant supplements prior to flying a payload test mission. [UCA 58.B.ii, 59.B.ii, 61.B.ii]
- Ensure that the SUAS software allows the pilot to check the sensor status. [UCA 60.C]
- Ensure that the SUAV is programmed with a set of commands that it defaults to when interference interrupts communication with the SUAS pilot. These commands should not involve deploying the payload. [UCA 50.A.ii, 52.A.ii, 53.A.ii, 55.A.ii, 56.A.ii, 57.A.ii, 61.A.ii, 62.A.ii]
- SUAV should be programmed not to cross an airspace boundary while in the process of deploying a payload, unless the pilot specifies this course of action. [UCA 61.D]

SUAV

63. The SUAV maneuvers when then maneuver takes it out of its assigned airspace. [H1, H3]

A. Inadequate Control Execution: SUAV maneuvers to remain in the airspace. Maneuver takes it out of the airspace.
   i. Refinement 1: SUAV software does not correctly maneuver. Solution: Stop testing immediately and modify software.

ii. Refinement 2: SUAV hardware does not correctly maneuver. Solution: Stop testing immediately and modify hardware.

B. Inappropriate Decision: SUAV flight software decides to leave the airspace.
   i. Refinement 1: Airspace boundaries are unclear. Solution: Prior to testing, ensure airspace boundaries are accurate.
   ii. Refinement 2: SUAV believes that it is appropriate to leave the airspace boundary. Solution: SUAV should be programmed to never violate an airspace boundary without pilot authorization.

C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
   i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
   ii. Refinement 2: Pilot commands are incorrect. Solution: Modify pilot commands to correctly maneuver.

D. Inadequate Process Behavior: SUAV does not attempt a maneuver. Wind blows the SUAV off course. Solution: Testing should not take place near the airspace boundary or during high winds.

64. The SUAV does not maneuver when a maneuver is needed to keep the SUAV in its assigned airspace. [H1, H3]

A. Inadequate Control Execution: SUAV sends maneuver commands to remain in the airspace. SUAV does not maneuver.
   i. Refinement 1: SUAV software does not correctly maneuver. Solution: Stop testing immediately and modify software.
   ii. Refinement 2: SUAV hardware does not correctly maneuver. Solution: Stop testing immediately and modify hardware.

B. Inappropriate Decision: SUAV flight software decides to leave the airspace.
   i. Refinement 1: Airspace boundaries are unclear. Solution: Prior to testing, ensure airspace boundaries are accurate.
   ii. Refinement 2: SUAV believes that it is appropriate to leave the airspace boundary. Solution: SUAV should be programmed to never violate an airspace boundary without pilot authorization.

C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
   i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
   ii. Refinement 2: Pilot commands are incorrect. Solution: Modify pilot commands to correctly maneuver.

D. Inadequate Process Behavior: SUAV attempts a maneuver. Wind blows the SUAV off course. Solution: Testing should not take place near the airspace boundary or during high winds.

65. The SUAV maneuvers too late to stay in its assigned airspace. [H1, H3]

A. Inadequate Control Execution: SUAV maneuvers to remain in the airspace. Maneuver is too late and takes it out of the airspace.
    i. Refinement 1: SUAV software has long lag. Solution: Test only at speeds where maneuvering to remain in the boundary is possible.
    ii. Refinement 2: SUAV hardware has long reaction time. Solution: Test only at speeds where maneuvering to remain in the boundary is possible.
B. Inappropriate Decision: SUAV flight software takes too long to decide to maneuver.
    i. Solution: Test only at speeds where maneuvering to remain in the boundary is possible.
    ii. Solution: Attempt to reduce software lag.
C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
    i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
    ii. Refinement 2: Pilot commands are incorrect. Solution: Modify pilot commands to correctly maneuver.
D. Inadequate Process Behavior: SUAV attempts to maneuver. Wind blows the SUAV off course. Solution: Testing should not take place near the airspace boundary or during high winds.

66. The SUAV maneuver is stopped before the change in direction is complete. [H1, H3]

A. Inadequate Control Execution: SUAV maneuvers to remain in the airspace. Maneuver command is cut off early.
    i. Refinement 1: SUAV software cuts off early. Solution: Stop testing immediately and modify software.
    ii. Refinement 2: SUAV hardware cuts connection early. Solution: Stop testing immediately and modify hardware.
B. Inappropriate Decision: SUAV flight software cuts the maneuver short. Solution: Stop testing immediately and modify software.
C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
    i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
    ii. Refinement 2: Pilot commands are incorrect. Solution: Modify pilot commands to correctly maneuver.
D. Inadequate Process Behavior: SUAV attempts to continue maneuver. Wind blows the SUAV off course. Solution: Testing should not take place near the airspace boundary or during high winds.

67. The SUAV maneuver is held after the change in direction is complete. [H1, H3]

A. Inadequate Control Execution: SUAV maneuvers to remain in the airspace. Maneuver command is held too long.

i. Refinement 1: SUAV software holds too long. Solution: Stop testing immediately and modify software.
ii. Refinement 2: SUAV hardware sticks or holds too long. Solution: Stop testing immediately and modify hardware.

B. Inappropriate Decision: SUAV flight software holds too long. Solution: Stop testing immediately and modify software.
C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
ii. Refinement 2: Pilot commands are incorrect. Solution: Modify pilot commands to correctly maneuver.
D. Inadequate Process Behavior: SUAV attempts to continue maneuver. Wind blows the SUAV off course. Solution: Testing should not take place near the airspace boundary or during high winds.

68. The SUAV releases its payload when the payload will exit SUAV Occupied Airspace. [H2, H4]

A. Inadequate Control Execution: SUAV does not command a payload release. Deploy payload command executed. Solution: In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.
B. Inappropriate Decision: SUAV flight software is aware of the airspace boundaries, and decides to release payload.
i. Solution: Payload should only be present when necessary for the test (payload drop tests, etc.).
ii. Solution: Payload drop software should be tested on the ground extensively before being tested inflight.
C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
i. Refinement 1: SUAV's sensors or software are incorrect. Solution: Do not allow payload drops without the location being confirmed by the pilot.
ii. Refinement 2: Pilot commands are incorrect. Solution: Have an inhibitor that keeps the pilot from dropping the payload when he/she does not intend to.
D. Inadequate Process Behavior: SUAV does not command a payload release. Payload deploys.
i. Solution: In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.
ii. Solution: Payload drop hardware/connectors should be tested on the ground extensively before being tested inflight.

69. The SUAV does not release its payload when the payload should be released. [H5]

A. Inadequate Control Execution: SUAV commands a payload release. Payload command not executed. Solution: Send command a second time, then stop testing, minimize flight over structures or people land and modify software or hardware.

B. Inappropriate Decision: SUAV flight software is aware of the location, and decides not to release payload.
    i. Solution: Have pilot send an overrule payload drop command.
    ii. Solution: Stop testing, minimize flight over structures or people, land and modify software.
C. Inadequate Feedback and Other Inputs: SUAV's assumed position differs from its actual position.
    i. Refinement 1: SUAV's location sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override.
    ii. Refinement 2: SUAV's payload sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to report on payload deployment to the pilot to override.
    iii. Refinement 3: Pilot commands are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to report on payload deployment.
D. Inadequate Process Behavior: SUAV commands a payload release. Payload does not deploy.
    i. Solution: In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.
    ii. Solution: Payload drop hardware/connectors should be tested on the ground extensively before being tested in flight.
    iii. Solution: Send command a second time, then stop testing, minimize flight over structures or people, and land and modify software or hardware.

70. The SUAV payload release is stopped before payload can fully release. [H2, H4]

A. Inadequate Control Execution: SUAV commands a payload release. Payload command interrupted. Solution: Send command a second time, then stop testing, minimize flight over structures or people land and modify software or hardware.
B. Inappropriate Decision: SUAV flight software does not fully open payload release servos/motors.
    i. Solution: Have pilot send an overrule payload drop command.
    ii. Solution: Stop testing, minimize flight over structures or people, land and modify software.
C. Inadequate Feedback and Other Inputs: SUAV's assumed configuration differs from its actual position.
    i. Refinement 1: SUAV's payload sensors or software are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to report on payload deployment.
    ii. Refinement 2: Pilot commands are incorrect. Solution: Have an external source (chase plane, ground radar unit, spotter, etc.) able to report on payload deployment.
D. Inadequate Process Behavior: SUAV commands a payload release. Payload does not deploy.
    i. Solution: In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people.

ii. Solution: Payload drop hardware/connectors should be tested on the ground extensively before being tested inflight.
iii. Solution: Send command a second time, then stop testing, minimize flight over structures or people land and modify software or hardware.

The above Step 2 Analysis led to the following 19 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- Stop testing immediately and modify software when SUAV software does not perform as expected. [UCA 63.A.i, 64.A.i, 66.A.i, 66.B, 67.A.i, 67.B]
- Stop testing immediately and modify hardware when SUAV hardware does not perform as expected. [UCA 63.A.ii, 64.A.i, 66.A.ii, 67.A.ii]
- Prior to testing, ensure airspace boundaries are accurate. [UCA 63.B.i, 64.B.i]
- SUAV should be programmed to never violate an airspace boundary without pilot authorization. [UCA 63.B.ii, 64.B.ii]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to give the SUAV's actual location to the pilot to override. [UCA 63.C.i, 64.C.i, 65.C.i, 66.C.i, 67.C.i, 69.C.i]
- Modify pilot commands to correctly maneuver when the pilot does not send the correct maneuver command. [UCA 63.C.ii, 64.C.ii, 65.C.ii, 66.C.ii, 67.C.ii]
- Testing should not take place near the airspace boundary or during high winds. [UCA 63.D, 64.D, 65.D, 66.D, 67.D]
- Test only at speeds where maneuvering to remain in the boundary is possible. [UCA 65.A, 65.B]
- Attempt to reduce software lag. [UCA 65.B]
- In tests that involve payloads, the SUAV occupied airspace should extend all of the way to the ground and minimize flight over structures or people. [UCA 68.A, 68.D, 69.D, 70.D]
- Payload should only be present when necessary for the test (payload drop tests, etc.). [UCA 68.B]
- Payload drop software should be tested on the ground extensively before being tested inflight. [UCA 68.B]
- Do not allow payload drops without the location being confirmed by the pilot. [UCA 68.C.i]
- Have an inhibitor that keeps the pilot from dropping the payload when he/she does not intend to. [UCA 68.C.ii]
- Payload drop hardware/connectors should be tested on the ground extensively before being tested inflight. [UCA 68.D, 69.D, 70.D]
- Send command a second time, then stop testing, minimize flight over structures or people, and land and modify software or hardware. [UCA 69.A, 69.D, 70.A, 70.D]
- Have pilot send an overrule payload drop command. [UCA 69.B, 70.B]
- Stop testing, minimize flight over structures or people, land and modify software when software does not execute a payload drop as expected. [UCA 69.B, 70.B]
- Have an external source (chase plane, ground radar unit, spotter, etc.) able to report on payload deployment to pilot to override. [UCA 69.C.ii, 69.C.iii, 70.C.i, 70.C.ii]

OTHER AIRCRAFT

71. The other aircraft maneuvers when the maneuver takes the Other Aircraft into SUAV Occupied Airspace. [H1, H3]

A. Inadequate Control Execution: Aircraft pilot attempts to maneuver, but the aircraft does not respond. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
   i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
   ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.

B. Inappropriate Decision: Other aircraft pilot decides to enter the airspace. Solution: 412 OG will establish clear guidance for pilots in R-2515 that they should never enter SUAS occupied airspace, even when the SUAV is in sight.

C. Inadequate Feedback and Other Inputs: SUAV's assumed airspace differs from its actual airspace.
   i. Refinement 1: Airspace boundaries are unclear. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.
   ii. Refinement 2: Aircraft is unaware of SUAV Operations. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.

D. Inadequate Process Behavior: The aircraft pilot attempts to avoid SUAV airspace, but the aircraft enters SUAV airspace. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace as quickly as possible. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
   i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
   ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.

72. The other aircraft does not maneuver when a maneuver is needed to keep the Other Aircraft out of SUAV Occupied Airspace. [H1, H3]

A. Inadequate Control Execution: Other aircraft pilot inputs maneuver to remain outside of the airspace. Aircraft does not respond. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
   i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
   ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.

B. Inappropriate Decision: Other aircraft pilot decides to enter the airspace. Solution: 412 OG will establish clear guidance for pilots in R-2515 that they should never enter SUAS occupied airspace, even when the SUAV is in sight.
C. Inadequate Feedback and Other Inputs: SUAV's assumed airspace differs from its actual airspace.
    i. Refinement 1: Airspace boundaries are unclear. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.
    ii. Refinement 2: Aircraft is unaware of SUAV Operations. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.
D. Inadequate Process Behavior: The aircraft pilot attempts to avoid SUAV airspace, but the aircraft enters SUAV airspace. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace as quickly as possible. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
    i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
    ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.

73. The other aircraft maneuvers too late to stay out of SUAV Occupied Airspace. [H1, H3]

A. Inadequate Control Execution: Other aircraft pilot inputs maneuver to remain outside of the airspace. Aircraft does not respond in time. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
    i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
    ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.
B. Inappropriate Decision: Other aircraft pilot underestimates space needed to maneuver. Solution: 412 OG will establish clear guidance for pilots in R-2515 that they should maneuver conservatively near the SUAS airspace boundaries.
C. Inadequate Feedback and Other Inputs: SUAV's assumed airspace differs from its actual airspace.
    i. Refinement 1: Airspace boundaries are unclear. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.
    ii. Refinement 2: Aircraft is unaware of SUAV Operations. Solution: SUAV airspace will be well defined (using major landmarks, when possible). SPORT will inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are.

D. Inadequate Process Behavior: The aircraft pilot attempts to avoid SUAV airspace, but the aircraft enters SUAV airspace. Solution: Other aircraft pilot attempts to regain control of the aircraft and exit the airspace as quickly as possible. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot.
    i. Mitigation: ROC/SPORT will not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests.
    ii. Mitigation: Flight operations take place away from airspace boundaries, when possible.

74. The other aircraft releases its payload when the payload will enter SUAV Occupied Airspace. [H2, H4]

E. Inadequate Control Execution: Payload release command is not given. Aircraft drops payload or munitions. Solution: Aircraft undergoing payload or drop testing will not overfly SUAV Occupied Airspace.
F. Inappropriate Decision: Aircraft pilot decides to drop its payload into SUAV Occupied Airspace. Solution: 412 OG will enforce payload test guidance in EAFBI 13-100.
G. Inadequate Feedback and Other Inputs: Aircraft believes that it is in DZ/PIRA/DAGRAG (payload test areas), but it is over the SUAV Occupied Airspace. Solution: 412 OG will enforce payload test guidance in EAFBI 13-100. When SUAV is undergoing payload drop testing, no other aircraft will be allowed into the impact range.
H. Inadequate Process Behavior: Payload release command is not given. Aircraft drops payload or munitions. Solution: Aircraft undergoing payload or drop testing will not overfly SUAV Occupied Airspace.

The above Step 2 Analysis has found the following 8 solutions/recommendations. The numbers in the bracket correspond to the scenarios that the solution addresses.

- Other aircraft pilot attempts to regain control of the aircraft and exit the airspace when the pilot enters the SUAS airspace inadvertently. Other aircraft immediately contacts SPORT, who notifies the SUAS pilot. [UCA 71.A, 71.D, 72.A, 72.D, 73.A, 73.D]
- ROC/SPORT must not schedule first flight, basic maneuvering, or "high risk" tests concurrent with SUAV tests. [UCA 71.A, 71.D, 72.D, 73.A, 73.D]
- Flight operations must take place away from airspace boundaries, when possible. [UCA 71.A, 71.D, 72.A, 72.D, 73.A, 73.D]
- 412 OG must establish clear guidance for pilots in R-2515 that they should never enter SUAS occupied airspace, even when the SUAV is in sight. [UCA 71.B, 72.B]
- SUAV airspace must be well defined (using major landmarks, when possible). SPORT must inform all aircraft operating in R-2515 of SUAV operations and where the airspace boundaries are. [UCA 71.C.i, 72.C.i, 72.C.ii, 73.C.i, 73.C.ii]
- 412 OG must establish clear guidance for pilots in R-2515 that they should maneuver conservatively near the SUAS airspace boundaries. [UCA 73.B]
- Aircraft undergoing payload or drop testing must not overfly SUAV Occupied Airspace. [UCA 74.A, 74.D]

- 412 OG must enforce payload test guidance in EAFBI 13-100. When SUAV is undergoing payload drop testing, no other aircraft will be allowed into the impact range. [UCA 74.B, UCA 74.C]

The STPA Step 2 analysis found a total of 141 safety recommendations.

APPENDIX D: ABBREVIATIONS

412 OG – 412th Operations Group

ADS-B – Automatic Dependent Surveillance-Broadcast

AFB – Air Force Base

AFTC – Air Force Test Center

AFTCI – Air Force Test Center Instruction

ATC – Air Traffic Control

CTF – Combined Test Force

DoD – Department of Defense

EAFBI – Edwards Air Force Base Instruction

EP – Emergency Procedure

ETA – Event Tree Analysis

FAA – Federal Aviation Administration

FL – Flight Level

FMEA – Failure Modes and Effects Analysis

FMECA – Failure Modes, Effects, and Criticality Analysis

FTA – Fault Tree Analysis

HAZOP – Hazards and Operability Analysis

IFR – Instrument Flight Rules

JOSHUA – High Desert Combined Control Facility (callsign)

MORT – Management Oversight Risk Tree

NMAC – Near Mid-Air Collision

OSS – Operations Support Squadron

ROC – Resource Operations Center

SC – Safety Constraint

SPORT – AFTC Military Radar Unit (callsign)

SRB – Safety Review Board

STAMP – Systems Theoretic Accident Model and Processes

STPA – Systems-Theoretic Process Analysis

SUAS – Small Unmannes Aerial System

SUAV – Small Unmanned Aerial Vehicle

UAS – Unmanned Aerial System

UAV – Unmanned Aerial Vehicle

UCA – Unsafe Control Action

USAF – United States Air Force

VFR – Visual Flight Rules

WORKS CITED

1. **Federal Aviation Administration.** 14 CFR 91.113 - Right-of-way rules. 2004.

2. **Leveson, Nancy G.** *Engineering a Safer World.* Cambridge : The MIT Press, 2011.

3. —. *Safeware: System Safety and Computers.* New York City : Addison-Wesley Publishing Company, 1995.

4. **Chung, Nicholas.** *Systems-Theoretic Process Analysis of the Air Force Test Center Safety Management System.* 2014.

5. **412 OG.** EAFBI 13-100 - Flying and Airspace Operations. s.l. : Edwards Air Force Base, 2014.

6. **UAS Task Force.** Unmanned Aircraft System Airspace Integration Plan. 2011.

7. **Federal Aviation Administration.** FAA Aeronautical Information Manual. s.l. : FAA, 2011.

8. AFTC Fact Sheet. *Edwards Air Force Base.* [Online] August 7, 2012. [Cited: November 21, 2016.] http://www.edwards.af.mil/About/Fact-Sheets/Display/Article/393903/air-force-test-center.

9. **AFTC.** AFTCI 91-202 - Air Force Test Center Safety Review Policy. s.l. : Air Force Test Center, 2016.

10. **AFTC Military Radar Unit.** AFD-160324-029 R-2515 SPORT Prebrief. s.l. : AFTC Military Radar Unit.

11. **Thomas, John.** A Process for STPA. 2017.