Systems Theoretic Process Analysis Applied to Air Force Acquisition Technical Requirements Development

by

Sarah E. Summers
Major, United States Air Force

B.S. Aerospace Engineering, Oklahoma State University, 2005
B.S. Mechanical Engineering, Oklahoma State University, 2005
M.S. Aeronautical Engineering, Air Force Institute of Technology, 2011
M.S. Flight Test Engineering, Air Force Test Pilot School, 2014

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

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2018

Signature of Author_____
Sarah E. Summers
System Design and Management Program
December 1, 2017

Certified by_____
Nancy G. Leveson, Ph.D., Professor
Department of Aeronautics and Astronautics
Thesis Supervisor

Accepted by_____
Joan Rubin
Executive Director, System Design and Management Program

This Page Intentionally Left Blank

Disclaimer

The views expressed in this document are those of the author and do not reflect the official position or policies of the United States Air Force, Department of Defense, or Government.

This Page Intentionally Left Blank

In memory of all of those who have given their life for our country, in particular:

Jolly 38:
Captain Gregg Lewis
Captain Philip Miller
Master Sergeant Matthew Sturtevant
Staff Sergeant Keven Brunelle
Staff Sergeant Kenneth Eaglin
Senior Airman Jesse Stewart

Jolly 39:
Lieutenant Colonel William Milton
Captain Carl Youngblood
Second Lieutenant Michael Harwell
Technical Sergeant Jeffrey Armour
Senior Airman Adam Stewart
Senior Airman Justin Wotasik

and
Captain Michael Geragosian

"These things we do that others may live"

Also in memory of Major Lee Berra.

This Page Intentionally Left Blank

Systems Theoretic Process Analysis Applied to Air Force Acquisition Technical Requirements Development

By

Sarah E. Summers
Major, United States Air Force

Submitted to the System Design and Management Program on 1 December 2017 in partial fulfillment of the requirements for the degree of Master of Science in Engineering and Management

Abstract

The Air Force experienced 12 Class A aviation mishaps in 2016, which resulted in 16 fatalities and 9 destroyed aircraft. So far in 2017, The Air Force has again experienced 12 Class A mishaps with 5 fatalities and 7 destroyed aircraft. (1) In addition to these mishaps, development of new aircraft or modifications to aircraft often take well over the planned duration. Developmental test identifies design deficiencies that must be addressed before the aircraft is fielded, which requires expensive and lengthy redesign cycles. A systems approach to design with humans included as part of the system can improve both the development process and aviation safety.

Such an approach was created by Professor Nancy Leveson at MIT and is called Systems Theoretic Process Analysis (STPA). STPA is shown to be applicable to the Air Force acquisitions process throughout the product lifecycle. STPA is also compliant with the airworthiness handbook, MIL-HDBK-516C, and STPA documentation is beneficial to the airworthiness certification inspectors.

STPA is applied to two use cases. One is a conceptual JSTARS aircraft, and the other is an unmanned aerial vehicle (UAV) that was modified from a general aviation aircraft. The Air Force is currently in source selection for a replacement to the JSTARS aircraft. The high-level STPA analysis is for a functional replacement to the JSTARS aircraft, as would be needed early in the acquisitions process. Additionally, accidents, hazards, and a safety control structure are developed for the JSTARS support system. The UAV analysis is more detailed, and provides information that is necessary during the Technology Maturation & Risk Reduction phase of an acquisition process.

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

This Page Intentionally Left Blank

Acknowledgements

I would like to acknowledge Professor Nancy Leveson for taking me on as a thesis advisee. I have learned an incredible amount in the last 18 months, and I am appreciative of your time and support. I would also like to thank Dr. John Thomas and the rest of the System Engineering Research Lab. Your help and insights during this journey has been incredible.

Thank you to the SDM faculty and staff for this amazing opportunity to come to MIT and learn what it means to be a systems thinker. This program has opened my eyes to a bigger picture and given me the tools to understand it and make a difference. The SDM 2016 Cohort has taught me just as much as the MIT faculty. Thank you to all those that have shared their knowledge and made this experience at MIT even better.

Thank you to all those who are currently serving in harm's way. The selflessness and professionalism of my fellow service members inspire me to do my best every day.

Thank you to my family and friends who have supported me throughout my life. You've cheered me on during life's good times and given me a shoulder during the hard times. You stimulate my creativity and encourage me to continue to question and learn.

Most of all, thank you to my wonderful wife. Thank you for sticking by my side while I drag you from coast to coast (to coast). Your endless support has enabled me to succeed in this endeavor. Every day I strive to be the person you deserve, and I am a better person for it. I look forward to many more adventures with you wherever the Air Force sends us.

This Page Intentionally Left Blank

Contents

Table of Figures

Table of Tables

Introduction

Motivation

On 2 September, 1998, twelve members of the 66th Rescue Squadron, flying with the callsigns Jolly 38 and Jolly 39, were killed in a midair collision at Nellis Air Force Base. My father was their squadron commander. On that day, a week after my 16th birthday, I decided to join the Air Force when I turned 18. The Air Force rescue motto is "These things we do that others may live". While I am not a member of the rescue community, I serve with that motto and those that have died living that motto in my heart. The safety of our men and women that serve in combat is the motivation behind my service and this thesis – that others may live.

As long as there is armed conflict, there will be military men and women that die in combat. Every death is a tragedy to family, friends, and their fellow service members. Those men and women who are killed in combat made a choice to serve and their sacrifice should be honored. Service members are also often killed during noncombat incidents. These incidents have an additional element of tragedy in that they are most often preventable. Military members should not die because their equipment does not operate as intended or the operating instructions do not provide correct information.

As a flight test engineer, I tested new aircraft and modifications to existing aircraft to ensure that the fielded product is safe to operate and operates as designed. We often find interactions between the operator and product or between the modifications and base aircraft are deficient for use in the field. Systems Theoretic Process Analysis (STPA) has the potential to predict these interactions during the development process in order to design out the flaws that can lead to accidents. I believe that STPA can also save the lives of flight test professionals and our men and women who utilize these systems in combat.

Objectives

The objective of this thesis is to determine the feasibility of implementing STPA within the Air Force acquisitions process. There are two main components of the thesis. One is to conduct case studies to illustrate the power of the STPA analysis to implement components of the acquisition process. The second component is to investigate how the STPA process can best be integrated into current Air Force acquisition processes.

Thesis Structure

Traditional hazard analysis methods will be researched, followed by an explanation of STAMP and STPA. The hazard analysis section is followed by explaining how STPA could be implemented into the AF acquisition and airworthiness processes and conclusions. Then, two cases studies using STPA are presented. The first case study is an example of a JSTARS used to manage battles that includes ground and air forces. The second case study is of a general aviation aircraft modified to become a UAV.

Hazard Analysis Methods

Fault Tree Analysis

Fault tree analysis (FTA) is a top down root cause hazard analysis tool that can be used for probabilistic risk assessments. Fault tree analysis was designed in the early 1960s for use on the Minuteman system, and has been adopted by several industries over the last 50 years including aerospace, nuclear, chemical processing, and software. FTA can be used throughout the design and lifecycle of the system to inform design, operations, and modifications to the system.

The analysis begins with an undesired event, and a fault tree is developed to determine what lower-level events (failures or faults) or combination of events could cause the undesired event. The relationship between the lower-level events are defined using logic gates. Once the model is developed, probabilities of each event are combined using Boolean logic and simple reliability calculations to compute the system reliability. (2)

The model also utilizes cut sets, which are a unique subset of all the lower-level events that would cause the undesired event to take place. There may be several cut sets for each undesired event, and evaluating each allows the designer to focus on specific design changes to avoid the undesired event along with calculating a probability for each cut set. Because the focus is on probability and reliability, the design changes suggested often involve adding redundancy so that the reliability calculations are increased.

An example of FTA is shown in Figure 1. The FTA is for a fire pump, which provides water to fire sprinkler systems. The question that necessitated the FTA below is whether or not the fire pump requires emergency power, such as a generator, or if it can use power from the utility provider. (3)

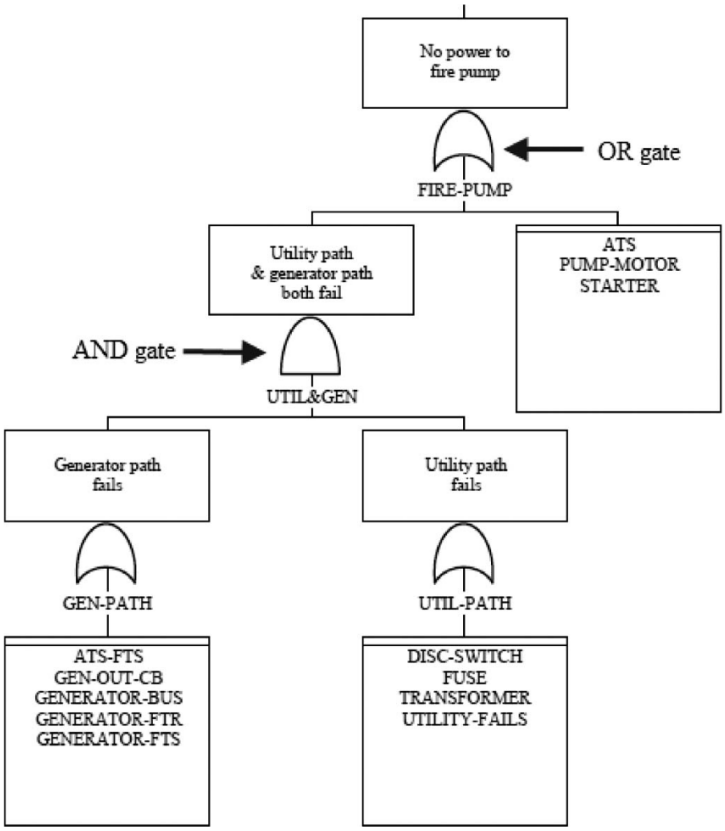


Figure 1 Fault Tree for Power to the Fire Pump (3)

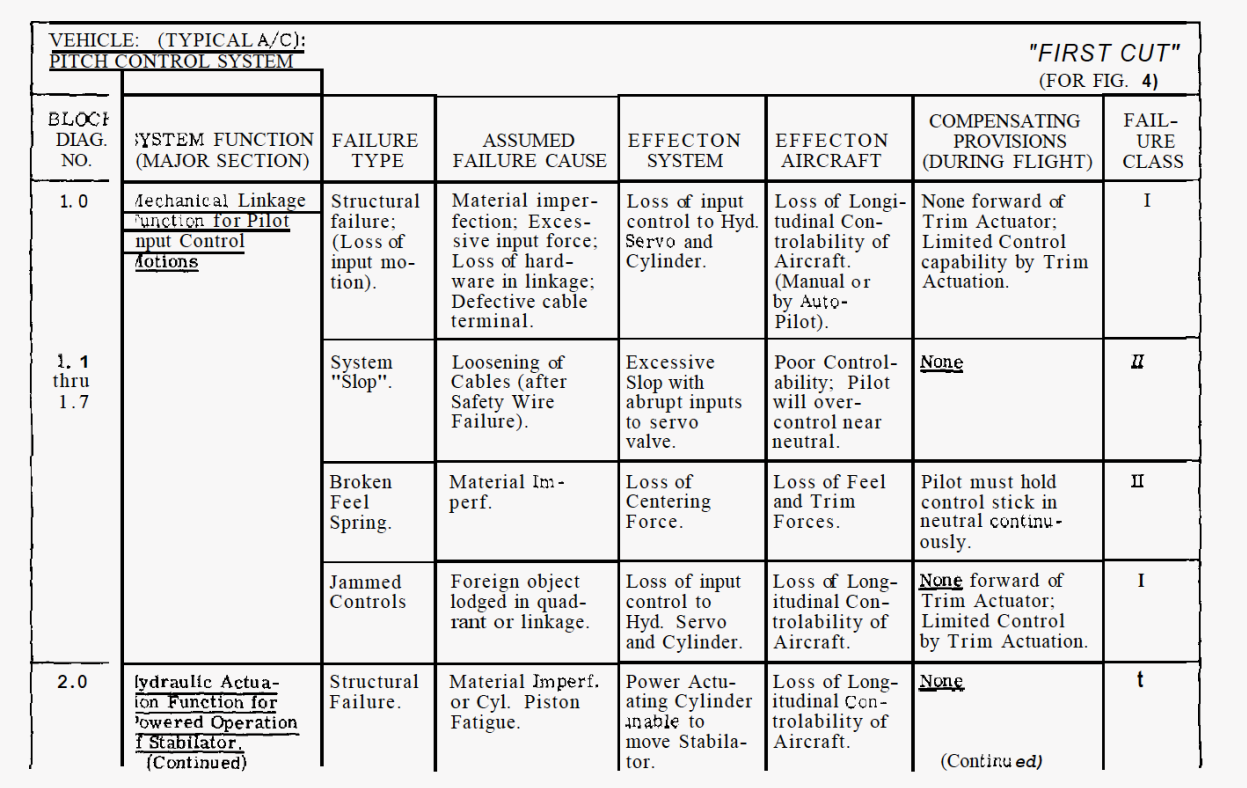
At the top of the example in Figure 1, the undesired event is 'no power to fire pump'. This could occur if the utility power and generator fails, or if the automatic transfer switch (ATS) fails. There are two paths below the utility power and generator fail element for each power source, and basic events that would cause each path to fail are listed in the bottom block. Probabilities for each basic event are estimated, which allows the user to determine the probability of the undesired event.

FTA is a powerful tool that can allow analysis of system reliability by evaluating component failures, however not all undesired events occur due to a component failure. Human and software-related system interactions will not be captured using FTA, nor can probabilities be assigned to such cases. Additionally, this type of analysis assumes that each of the failures are independent from each other. This assumption may not always be appropriate, and the results of the analysis will be inaccurate if the assumption is made when it should not be.

Failure Modes and Effect Analysis (FMEA)

FMEA is a bottom up hazard analysis tool. Rather than start with an undesired event, as with FTA, the analysis begins with a component. Each component or subsystem is analyzed for potential failures. The effect of the failure must be determined, and failure detection methods

and mitigations are determined. (4) Component failures may be determined by engineering judgement or statistical analysis. An example of FMEA is shown in the figure below.



VEHICLE: (TYPICAL A/C): PITCH CONTROL SYSTEM

"FIRST CUT" (FOR FIG. 4)

BLOCK DIAG. NO.	SYSTEM FUNCTION (MAJOR SECTION)	FAILURE TYPE	ASSUMED FAILURE CAUSE	EFFECTON SYSTEM	EFFECTON AIRCRAFT	COMPENSATING PROVISIONS (DURING FLIGHT)	FAIL-URE CLASS
1.0	Mechanical Linkage Function for Pilot Input Control Motions	Structural failure; (Loss of input motion).	Material imperfection; Excessive input force; Loss of hardware in linkage; Defective cable terminal.	Loss of input control to Hyd. Servo and Cylinder.	Loss of Longitudinal Controlability of Aircraft. (Manual or by Auto-Pilot).	None forward of Trim Actuator; Limited Control capability by Trim Actuation.	I
1.1 thru 1.7		System "Slop".	Loosening of Cables (after Safety Wire Failure).	Excessive Slop with abrupt inputs to servo valve.	Poor Controlability; Pilot will overcontrol near neutral.	None	II
		Broken Feel Spring.	Material Imperf.	Loss of Centering Force.	Loss of Feel and Trim Forces.	Pilot must hold control stick in neutral continuously.	II
		Jammed Controls	Foreign object lodged in quadrant or linkage.	Loss of input control to Hyd. Servo and Cylinder.	Loss of Longitudinal Controlability of Aircraft.	None forward of Trim Actuator; Limited Control by Trim Actuation.	I
2.0	Hydraulic Actuation Function for Powered Operation of Stabilator. (Continued)	Structural Failure.	Material Imperf. or Cyl. Piston Fatigue.	Power Actuating Cylinder unable to move Stabilator.	Loss of Longitudinal Controlability of Aircraft.	None (Continued)	t

Figure 2 FMEA Example Conceptual Design Review for Flight Control System (4)

As can be seen from the figure, the table is broken into systems, in this case the pitch control system, and further broken down by function, which is mechanical linkage function for pilot input control motions. Different possible failures are then listed for each function, along with what might cause the failure (assumed failure case), effect on the system, effect on the aircraft, any actions during flight to compensate for the failure, and finally the failure class with I being the most dangerous.

The failures can then be mitigated through design changes. The figure below shows the same system at preliminary design review.

VEHICLE: (TYPICAL A/C):
PITCH CONTROL SYSTEM

"SECOND CUT'
(FOR FIG. 6)

BLOCK DIAG. NO.	SYSTEM FUNCTION (MAJOR SECTION)	FAILURE TYPE	ASSUMED FAILURE CAUSE	EFFECT ON SYSTEM	EFFECT ON AIRCRAFT	COMPENSATING PROVISIONS (DURING FLIGHT)	FAIL-URE CLASS
1.0	Mechanical Linkage Function for Pilot Input Control Motion	Structural Failure; (Loss of input motion).	Same as "1st cut" (Ref. Fig. 5)	None if failure occurs within redundant cable	None if failure occurs within redundant cable section.	Redundant quadrant and cables up to Feel Device; More stringent Q.C., Preflight Ground Lnspec. and Maintenance Requirements.	II
1.1 thru 1.7		System "Slop".	Same as "1st cut" (Ref. Fig. 5)	None; redundant cables will maintain tension.	None	Redundant cables and quadrants; stringent Q.C. Inspec.	III
		Broken Feel Spring	Same as "1st cut" (Ref. Fig. 5)	Reduced Stick Centering Force	None	Redundant Feel Device Spring.	III
		Jammed Controls.	Same as "1st cut" (Ref. Fig. 5)	Loss of manual input control to Hyd. Servo and Act. Cylinder.	Partial Loss of Longitudinal Controllability of Aircraft.	Increased Limited Control of Trim Act., Enclose Components; Increase stringent Q.C. Inspec.	II
2.0					Reduction in Stabilator deflection at high velocity.	Dual-Tandem Servo Valves and Tandem Actuating Cyl. (Continued)	II

Figure 3 FMEA Example Preliminary Design Review for Flight Control System (4)

In Figure 3, the first 4 columns are the same, but now effect on system, effect on aircraft, compensating provisions have all changed. Additionally, the failure classes for all of the failure types has been reduced to II or III.

The main drawback to FMEA is that it requires the engineer to examine every component and potential failure to determine if there is a safety hazard associated with that failure. It can become incredibly time consuming compared to other methods. Additionally, just as with FTA, only single component failures are considered in this analysis. FTA considers component interaction to some degree, however FMEA does not at all. The case where two failures are required to produce an effect are not included. Theoretically they could be, but the amount of effort involved would be prohibitive except for the very simplest of systems. Additionally, this analysis does not consider the human, except to assume the human can enact the compensating provisions during flight, as seen in Figure 1 for the broken feel spring.

HAZOP

Hazard and operability study (HAZOP) was developed in the 1960s by Imperial Chemical Industries. (5 p. 1) it is "a structured analysis of a system, process, or operation for which detailed design information is available, carried out by a multidisciplinary team." (5 p. 2) HAZOP systematically goes through each of the system parameters and uses a set of

guidewords to determine whether or a not a deviation of the parameter would lead to a safety hazard.

Studies are carried out with a client and a facilitator. (5 p. 44) The facilitator is an expert in HAZOP, and the client is an expert in the particular system that to be studied.

According to the British Standard on HAZOP, the key features of a HAZOP analysis are:

- The examination is a creative process
- The examination is carried out under the guidance of a trained and experienced study leader
- The examination relies on specialists from various disciplines
- The examination should be carried out in a climate of positive thinking and frank discussion
- Solutions to identified problems are not a primary objective (6)

The HAZOP process, as shown in Figure 4, is broken into four main steps. Definition and Preparation are similar steps for any group based activity. Step 3, Examination, begins with dividing the system into parts. The division allows the HAZOP team to more specifically define the design intent of each part. According to the standard, the more complex the system, and the higher the standard, the smaller the divided parts will be. Each part is then broken into elements, which can range from steps or process stages to components. (6)

The elements all have characteristics associated with them, such as material properties, rates, or information. Each element is then examined using guide words. The generic list of guidewords are shown in Table 1.

Table 1 Basic Guidewords (6)

Guide word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN	Complete substitution

These guidewords are used to encourage the study participants to think creatively about the elements and parts under examination.

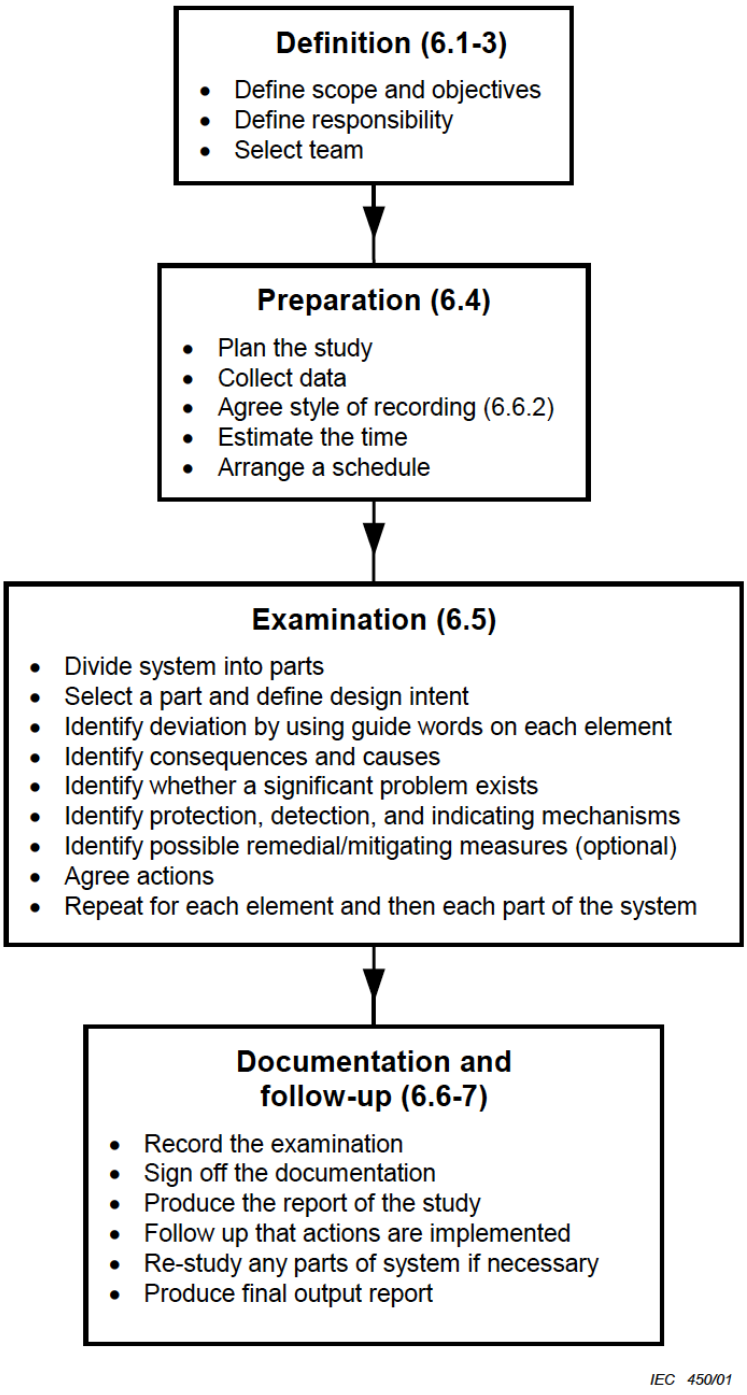


Figure 4 The HAZOP Study Procedure (6)

Drawbacks of Traditional Hazard Analyses

One drawback to HAZOP, Fault Trees, and FMEA, is the system must already have a detailed design (6). If hazards are identified, significant design rework may be required to mitigate or eliminate the hazards. Rework costs time and money, and there is a possibility that programs lacking one or both of those may choose not to implement all of the mitigations. Additionally,

solutions to hazards are not identified in these analyses, which means a second design study would be required to determine the best way to mitigate or reduce the identified hazards.

These analyses also focus on component failure, which is not the only cause of mishaps. Many mishaps such as the European Space Agency's Schiaparelli mishap on Mars, are not caused by component failure, but rather by software interactions due to design errors. (7) Other mishaps are caused due to human interaction within the system due to poor design. None of these analyses will identify these types of mishap causes.

The analyses only look at deviations from design intent, which assumes that design intent is safe. As discussed in the paragraph above this assumption may not be valid, leading to unidentified hazards associated with the design intent itself that will go into production.

The reason these analyses are deficient for modern technologies is because they were created during a time when systems were mainly electromechanical systems with no significant computers or software. As the timeline in Figure 5 shows, the traditional hazard analyses were all created before Man walked on the moon. Since then, humanity has experienced a giant leap in digital technologies. Efforts to adapt traditional methods to identify hazards not caused by a component failure cannot be successful, as the underlying theory for these analyses were not based on modern technologies.

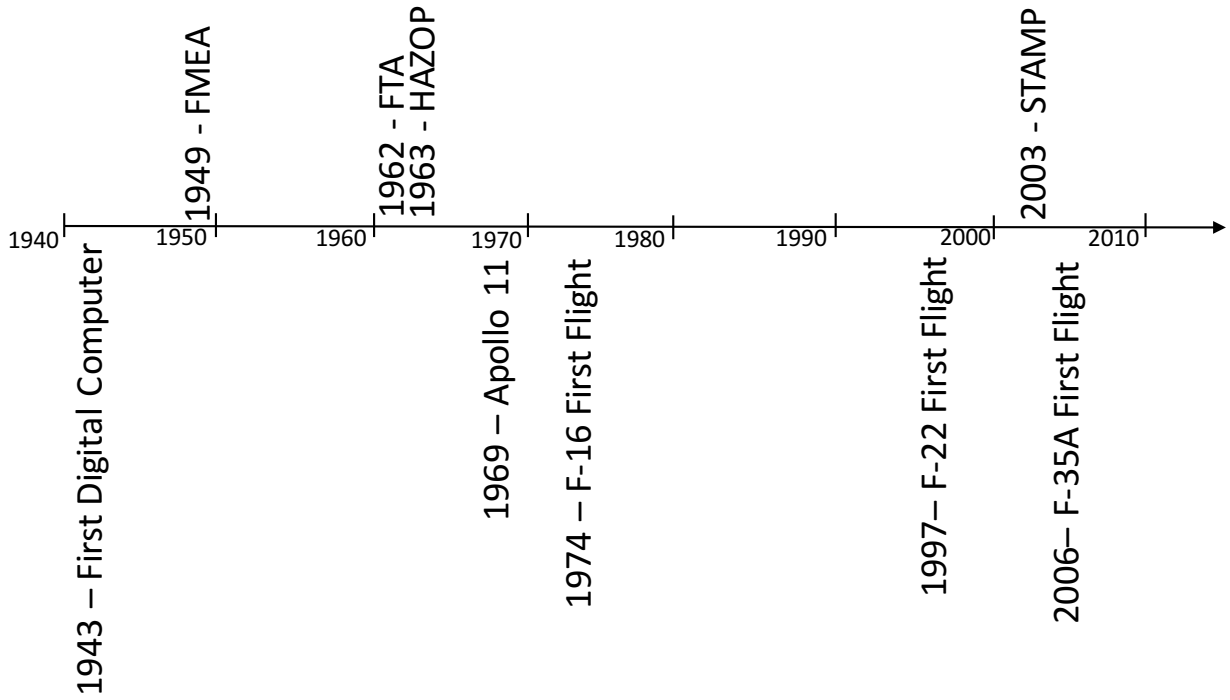


Figure 5 Hazard Analysis Timeline

A new hazard analysis is needed that is designed to capture both failure related and non-failure related hazards. The analysis should be able to consider humans and software as part of the system in addition to the electromechanical components traditionally evaluated.

STAMP

Systems-Theoretic Accident Model and Process (STAMP) is built on underlying systems theory and three concepts, "safety, constraints, a hierarchical safety control structure, and process models." Systems are 'viewed as interrelated components kept in a state of dynamic equilibrium by feedback control loops." (8) Accidents occur, therefore, due to a violation of the safety constraints. Safety constraints are initially defined at the system level, and are then broken down to "sub-requirements" as the design progresses and subsystems and components are developed.

The next concept, hierarchical safety control structure, is based off of hierarchical structures in systems theory. The lower levels are constrained by control processes from the higher levels. In turn, the lower levels provide feedback to the higher levels "about how effectively the constraints are being satisfied." (8) An example of a hierarchical safety control structure is shown in Figure 6. The left side is system development, and the right side is operations. This particular safety control structure has a large scope that includes legal bodies, regulators, and company management. Safety control structures can be scoped based on the objectives of the analysis. An important takeaway from this particular safety control structure is that a mishap may occur within the operating process (bottom right corner of the figure), however the inadequate safety constraints that led to the mishap could be well outside of the small operating process scope. Inadequate (missing, inappropriate, or unenforced) safety regulations, for example, could be a factor in a mishap. None of the other hazard analyses described in this section examine hazards that arise from outside of the system under design. The context in which the system operates should be input into the design. Context can include operating environment, company objectives and operating practices, or regulatory requirements. If these contextual inputs change, as they certainly will throughout the lifecycle of a product, the assumptions that went into the design are no longer valid. A system that may have been safe when it was first fielded becomes unsafe. This is why Leveson's sixth new assumption is: "Systems will tend to migrate towards states of higher risk." (8) If the context was not included as an input to the design, the system may be unsafe from the start.

Because the context of a designed system will change throughout its lifecycle, feedback in Figure 6 is just as important as the constraints that are applied to the lower levels. For example, problem reports provided by the controllers must be reported to both the system development and system operations chains. The operations management may have to alter work instructions or send out temporary notices regarding the problem reports. The project managers will evaluate the problem reports and take action to resolve the problem.

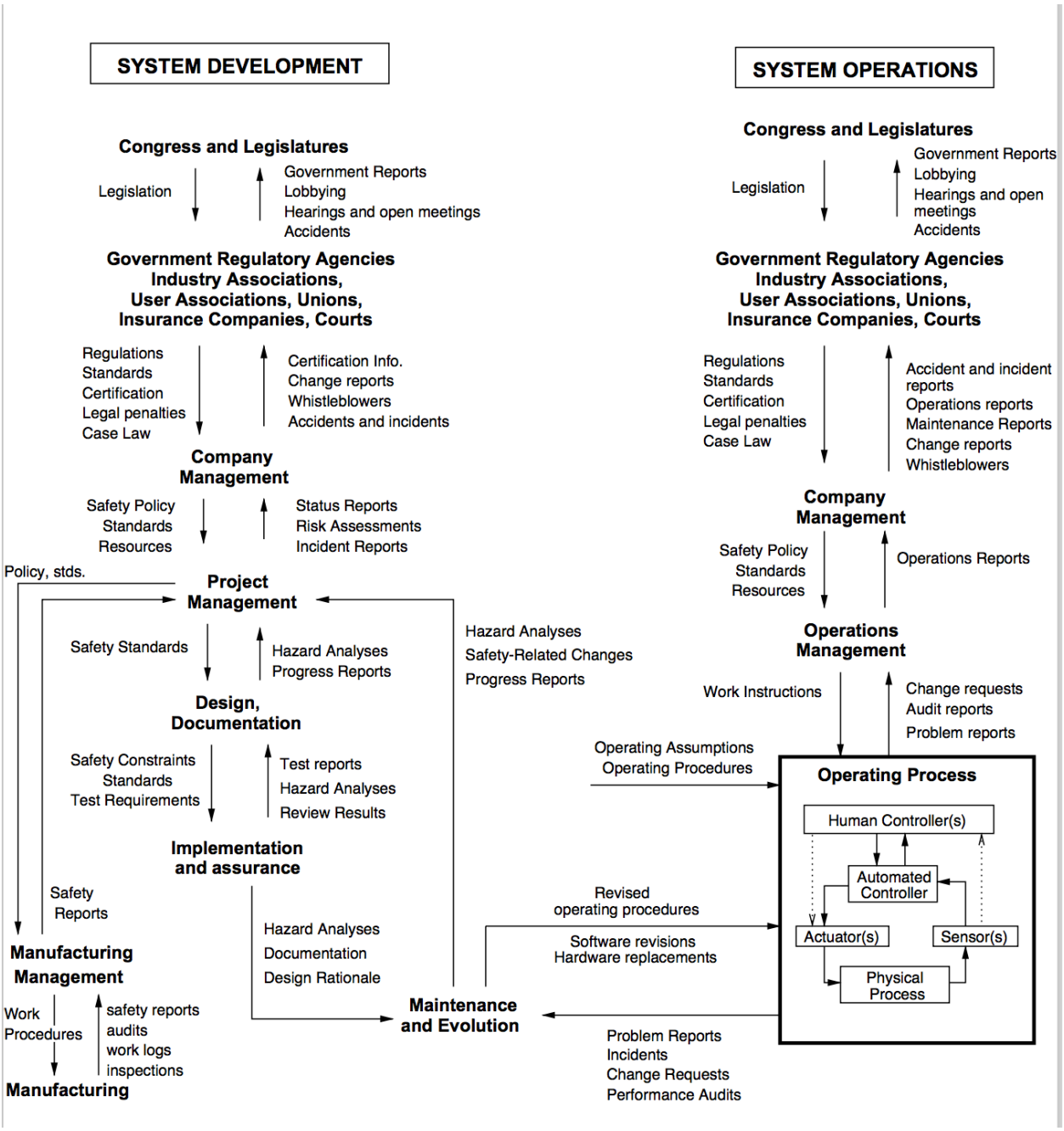


Figure 6 Example of a Hierarchical Safety Control Structure (8)

Often problems are not reported for a variety of reasons. The result is a system that is not operating as it should, operators creating work arounds by themselves or overlooking the problem, no hazard analysis to understand the safety implications of the problem, and no system redesign. Feedback, therefore, is essential to the safety of the system along with the safety constraints.

The last major component of STAMP is process models. The purpose of feedback is to inform the controller of the state of the process, which is a component of the process model. The process model, as described by Leveson, is a "model used to determine what control actions are needed, and it is updated through various forms of feedback." For example, an autopilot is set to maintain a heading. The autopilot must receive the current heading, aircraft attitude, and aileron deflections. Figure 7 illustrates the process model within a control structure. The controller then uses the process model to determine the control action.

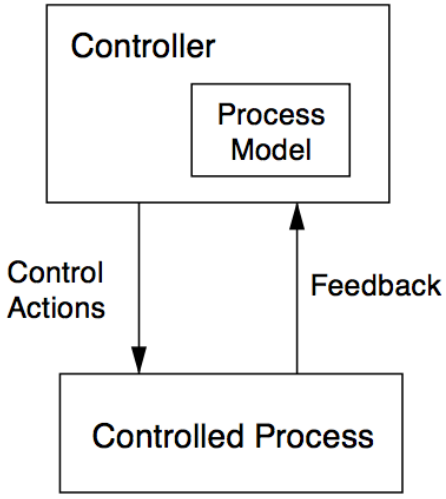


Figure 7 Simple Control Structure (8)

Even with accurate and adequate feedback, the controller still may not provide a safe control action. Therefore, as Leveson said, "process models play an important role (1) in understanding why accidents occur and why humans provide inadequate control over safety-critical systems and (2) in designing safer systems."

Leveson states that "systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback control loops." Safety is then "achieved when appropriate constraints on the behavior of the system and its components are satisfied." (8) Accidents occur when those constraints are violated. The violations are one or more of:

1. The safety constraints were not enforced by the controller.
    a. The control actions necessary to enforce the associated safety constraint at each level of the sociotechnical control structure for the system were not provided.
    b. The necessary control actions were provided but at the wrong time (too early or too late) or stopped too soon.
    c. Unsafe control actions were provided that caused a violation of the safety constraints.
2. Appropriate control actions were provided but not followed. (8)

Leveson illustrates control flaws with respect to the safety control structure in Figure 8 below.

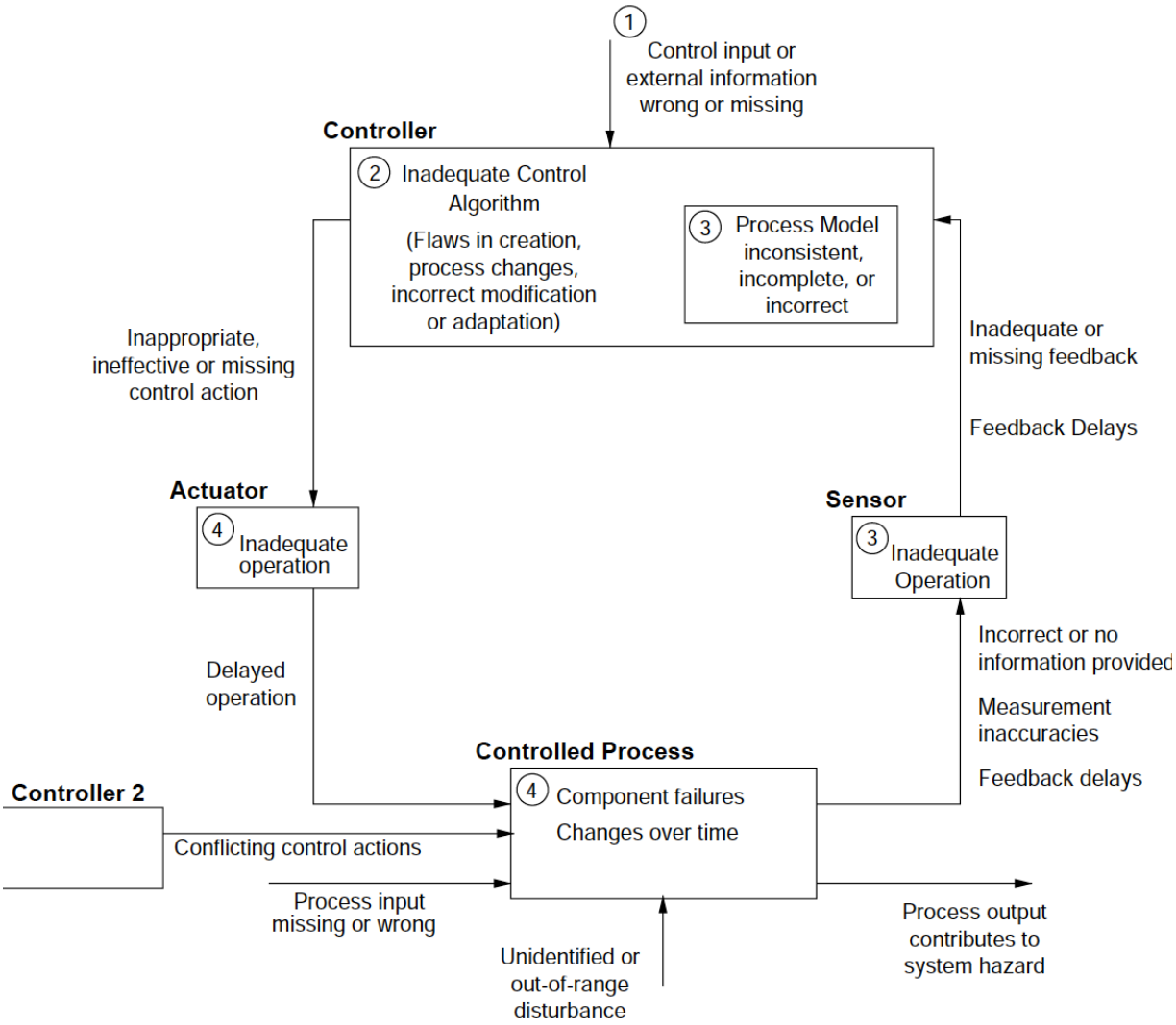


Figure 8 Control Flaws Leading to Hazards (8)

There are generally multiple controllers in each hierarchical control structures that either provide control inputs to lower level controllers (1), or provide control actions to the controlled process itself (controller 2). Within the controlled process (4), component failures will be identified. Feedback and control actions can be disrupted or altered by physical failures as well (such as actuator or sensor failures). These types of failures are what other hazard analyses previously described may identify. There are, however, many other causal factors beyond component failures in Figure 8 that will not be identified by the traditional hazard analysis techniques.

STPA (System Theoretic Process Analysis) is a hazard analysis technique built on the STAMP foundation. It starts with defining "accidents or losses, hazards, safety requirements and constraints, and the safety control structure." (8)

An accident (or mishap in military terminology) is defined as “An undesired or unplanned event that results in a loss including loss of human life or human injury, property damage, environmental pollution, mission loss, etc” (8) The project stakeholder should determine what the relevant losses are for the particular system being designed.

A hazard is defined as “A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).” (8) Each hazard should trace to an accident. As an example, an analysis of a new aircraft will likely include the accident of “loss of life”. A hazard might be “aircraft violates minimum separation requirements.” If an aircraft violates minimum separation requirements, it could cause a midair collision, which would possibly result in loss of life. Therefore, the hazard would trace to the accident loss of life.

Next, safety requirements are developed from the hazards. In the case of the example above, the requirement may be “aircraft must not violate minimum separation requirements.”

Once the high-level constraints have been developed, the safety control structure is created. The control structure must be designed based on the requirements previously defined, along with any other constraints associated with the organizations that are designing and operating the system, operational construct, and logistics support.

STPA has two steps. The first step is to identify unsafe control actions (UCAs). The safety control structure identifies each controller and their associated control actions. Each control action is then evaluated to determine under what circumstances that control action may lead to a hazardous state. In STAMP, UCAs happen because:

1. A control action required for safety is not provided or not followed.
2. An unsafe control action is provided.
3. A potentially safe control action is provided too early or too late, at the wrong time or in the wrong sequence.
4. A control action required for safety is stopped too soon or for too long. (8)

These UCAs are often put into a table with the control action in the first column and the four types of UCAs in the next 4 columns. An example of the UCA table can be seen below.

Table 2 Example UCA Table (9)

Control Action	Hazardous Control Actions			
	Not Providing Causes Hazard	**Providing Causes Hazard**	**Wrong Timing or Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
Open train doors	Door open command not provided when train is stopped at platform and person in doorway Door open command not provided when train is stopped and emergency exists	Door open command provided when train is moving and there is no emergency Door open command provided when train is moving and there is an emergency[14] Door open command provided when train is stopped unaligned with platform and there is no emergency	Door open command is provided more than X seconds after train stops during an emergency	N/A

In the table above, the control action is “open train doors”. Note that there are no UCAs in the “Stopped too soon or applied too long” category, which only applies to continuous actions. Discrete actions will not have UCAs in this column.

The second step is determining how the UCA might occur. This is typically accomplished by evaluating the control loop related to the particular controller and control action that is being examined. The causal scenarios that are generated in this step will provide information necessary to eliminate the hazard, or if elimination is impossible to control the hazard. This information is written as a safety requirement or constraint that should be included in design requirements or operational procedures.

Leveson gives an example of how to do this in Engineering a Safer World, which can be seen in Figure 9. Figure 9 is a modified version of Figure 8 for a high-power interlock. The interlock should cause the power to be disrupted when a door is open, so that someone can work in the area without being shocked. When the door is closed, power flows to the system again.

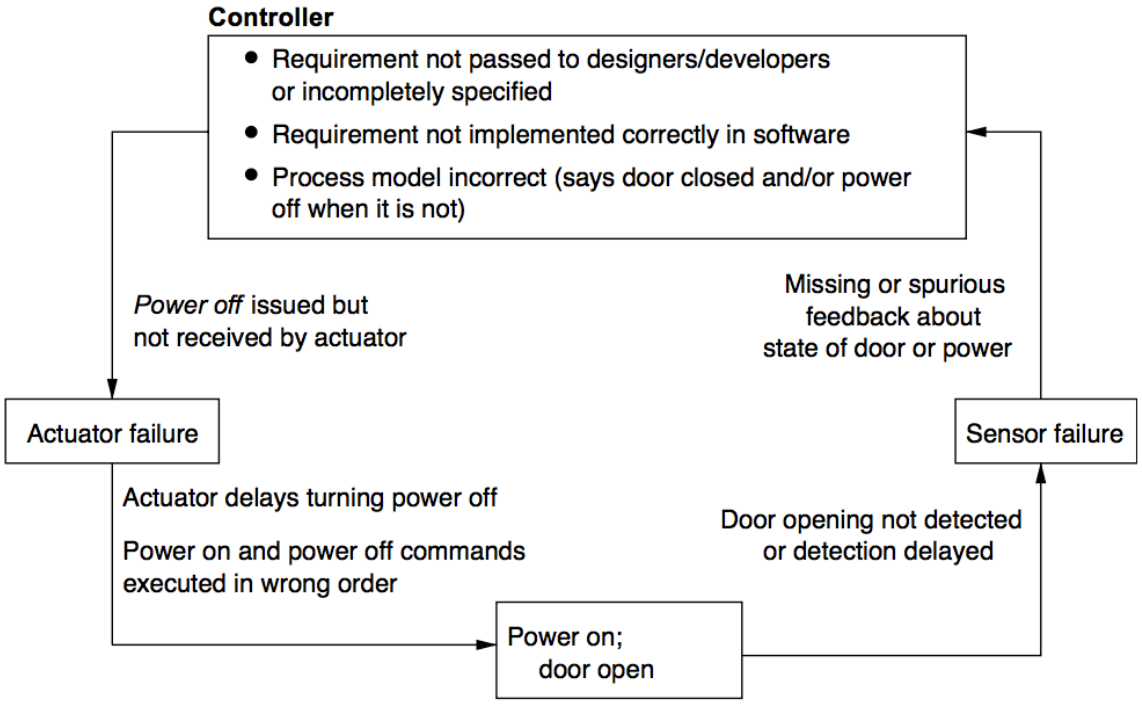


Figure 9 An Example of STPA Step 2: Scenario Generation (8)

Figure 9 shows general scenarios, such as "detection delayed." These scenarios are not yet detailed enough to determine how to eliminate the hazard. One must determine why the detection is delayed. Maybe vibrations in the environment causes the sensitive detector to give false door open feedback, so the sensor is programmed to only provide feedback once the detector indicates the door is open continuously for a certain period of time. If this is the case, the safety constraint might read "The detector must provide door open feedback within 0.1 seconds of opening", as an example. "Spurious feedback" is another general scenario. Along the lines of the previous example, the more detailed information might read "The detector is sensitive and detects small movements of the door, sending false open door feedback." A safety constraint may be "The detector must only detect the door opening, not door movement while still in the closed position." Now, design engineers can evaluate how to solve the spurious feedback, which will in turn solve the need for a delay in detection feedback. While this may seem obvious to the reader, system designs are often adjusted to 'fix' issues by resolving the symptoms of the issue rather than correcting a flawed design. The final design becomes a patchwork of 'solutions', instead of a thoughtful and cohesive design. The author has personally seen this type of patchwork engineering result in mishaps costing tens of millions of dollars.

STPA is a top down analysis, meaning that it starts with a high-level goal (accidents that need to be prevented), and the analysis progresses down into low-level details. The top down nature of

STPA can be seen in Figure 10. A handful of high-level accidents are followed by a slightly larger number of hazards that can each be traced to one or more accidents. Once the safety control structure is created, and the control actions in the system are understood, the UCAs can be examined. Each UCA is also traceable to one or more hazards. Scenarios for each UCA are then created. Because the analysis begins at the top, only scenarios that can actually cause an accident are investigated. Additionally, by starting with high-level accidents and hazards and working down into the detail, one can more easily tell if an accident or hazard is missing. Large lists of hazards are nearly impossible to inspect for completeness.

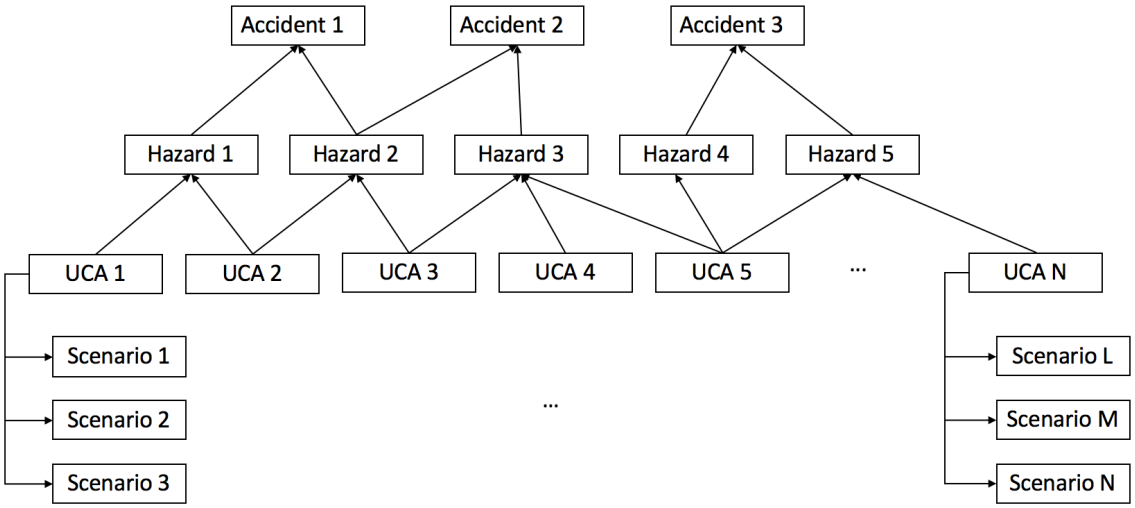


Figure 10 STPA Top Down Analysis

The traceability of an analysis is a key component of any system approach. The traceability provides multiple functions. First, when the analysis yields a safety constraint it is very easy to understand the origin of the constraint and the effect if the constraint is not considered in the design. Traceability, therefore, serves to document the analysis and justify the findings. This allows the analysis to be quickly understood by others, and provides documentation of the safety approach when the system requires safety certification. Second, if the design, associated support system, or operational context changes, updating the analysis becomes much easier.

Air Force Acquisitions and Systems Safety

Air Force Acquisitions Process

A simplified version of the Air Force acquisitions process is shown in Figure 11. The process consists of 6 phases.

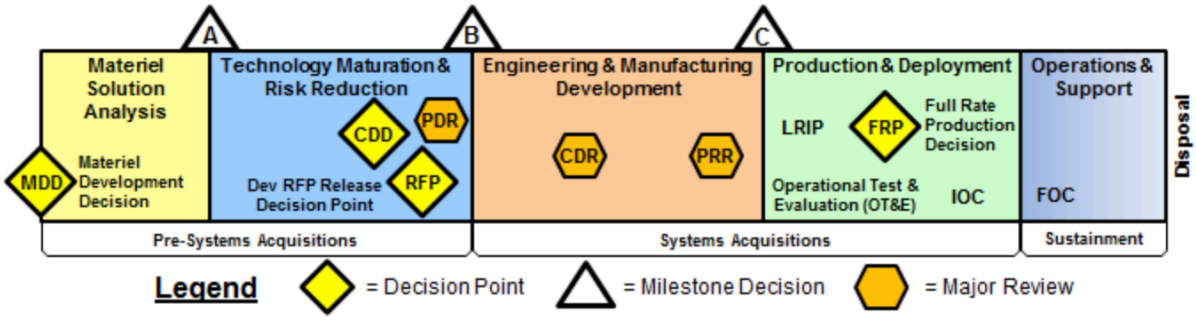


Figure 11 Acquisitions Process (10)

The first phase is the Material Solution Analysis phase. In this phase, an Analysis of Alternatives is conducted to determine the concept, or materiel solution, for the system. The activities in MSA and documents are shown in Figure 12.

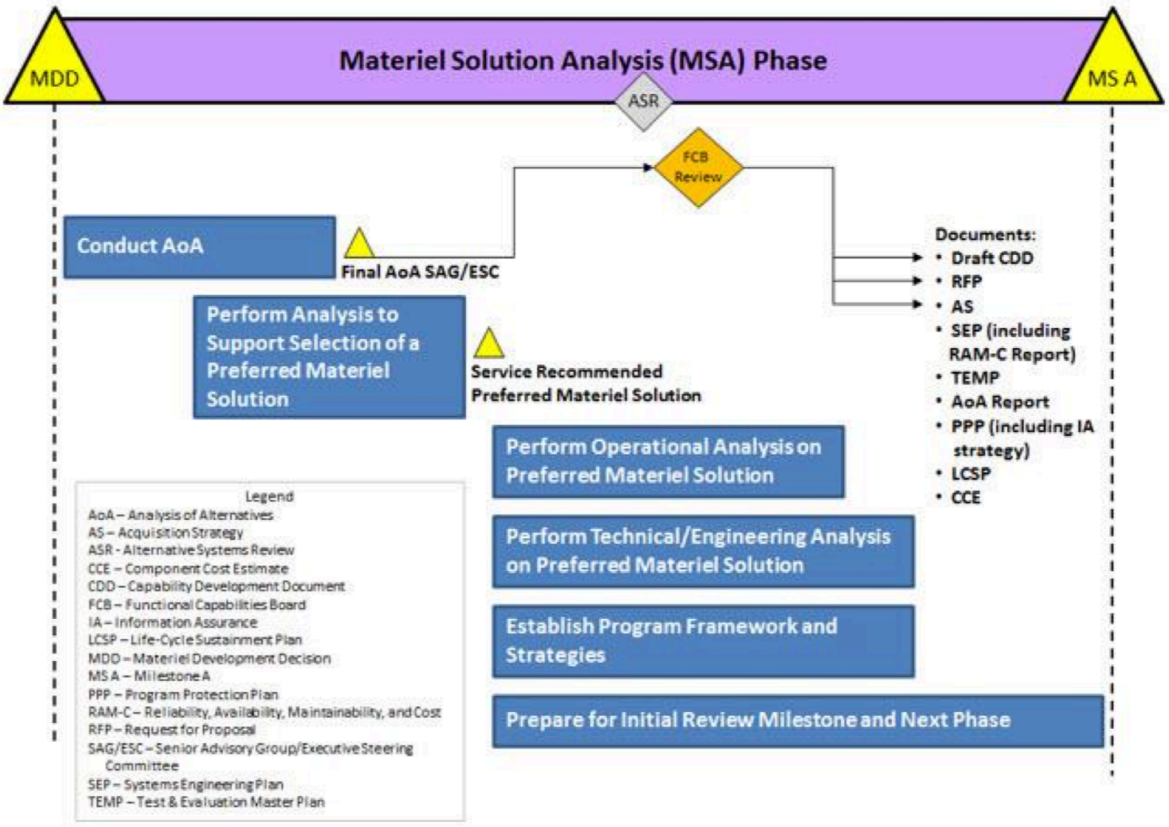


Figure 12 SE Activities in Materiel Solution Analysis Phase (11)

The second phase is the Technology Maturation and Risk Reduction phase. This phase's purpose is to "reduce technology, engineering, integration, and life cycle cost risk to the point that a decision to contract for Engineering and Manufacturing Development (EMD) can be made with confidence in successful program execution for development, production, and sustainment." (12) The activities associated with this phase are shown in Figure 13.

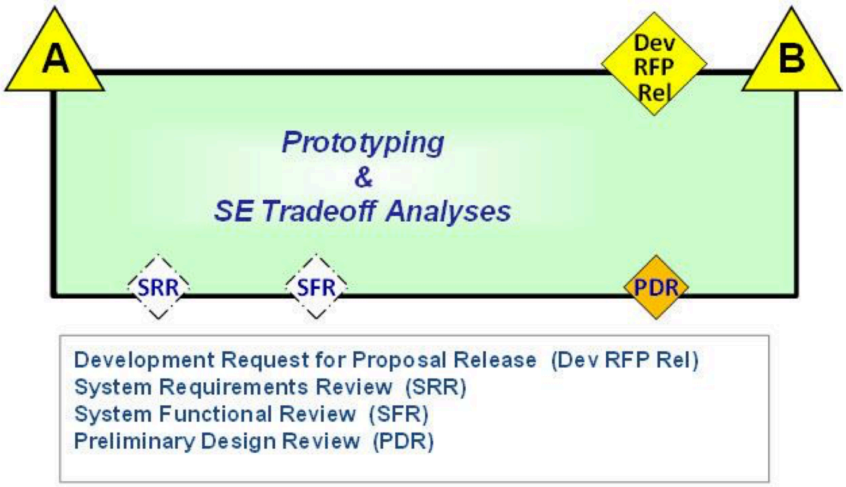


Figure 13 SE Activities in Technology Maturation and Risk Reduction Phase (11)

During this phase, trade studies to explore design options and reduce program risk are conducted. The Capability Development Document, Systems Engineering Plan, System Requirements Document, Test and Evaluation Master Plan, Request for Proposal and other documents are drafted. These documents are continually refined throughout the acquisitions process. The preliminary system design is developed in this phase, and safety engineers conduct a FMECA study on the design. Near the end of the phase the Preliminary Design Review will take place. PDR is typically required to proceed to Milestone B and enter the Engineering and Manufacturing Development phase.

During EMD, the design is further advanced and integrated, and the manufacturing process is developed. The Critical Design Review occurs during this phase. At the CDR, the PO determines whether or not the design meets requirements, if it is ready to build test articles, and if it is ready for DT to begin. These activities are illustrated in Figure 14.

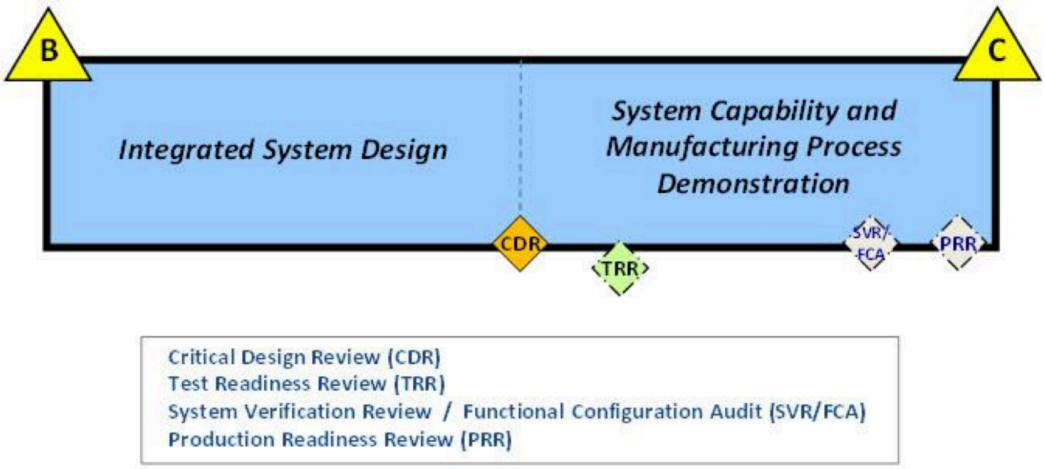


Figure 14 SE Activities in Engineering and Manufacturing Development Phase (11)

During this phase, the airworthiness certification basis, which consists of the suitable MIL-HDBK-516C criteria, must be approved by the TAA. Additionally, prior to DT, the TAA will approve the military experimental flight release (13). Near the end of EMD, the Production Readiness Review is conducted to determine if the system is ready for production.

After the Milestone C review, the program enters the Production and Deployment phase. In this phase, low-rate production begins and DT and OT perform the majority of their testing. The Full Rate Production Decision is made in this phase, which will mark the beginning of full production, as shown in Figure 15. Initial Operational Capability is typically declared during this phase, which indicates that the system has reached a minimum operational capability. The Military Type Certificate, issued by the TAA, must be obtained before OT&E begins or before the first delivery of aircraft for operational use.

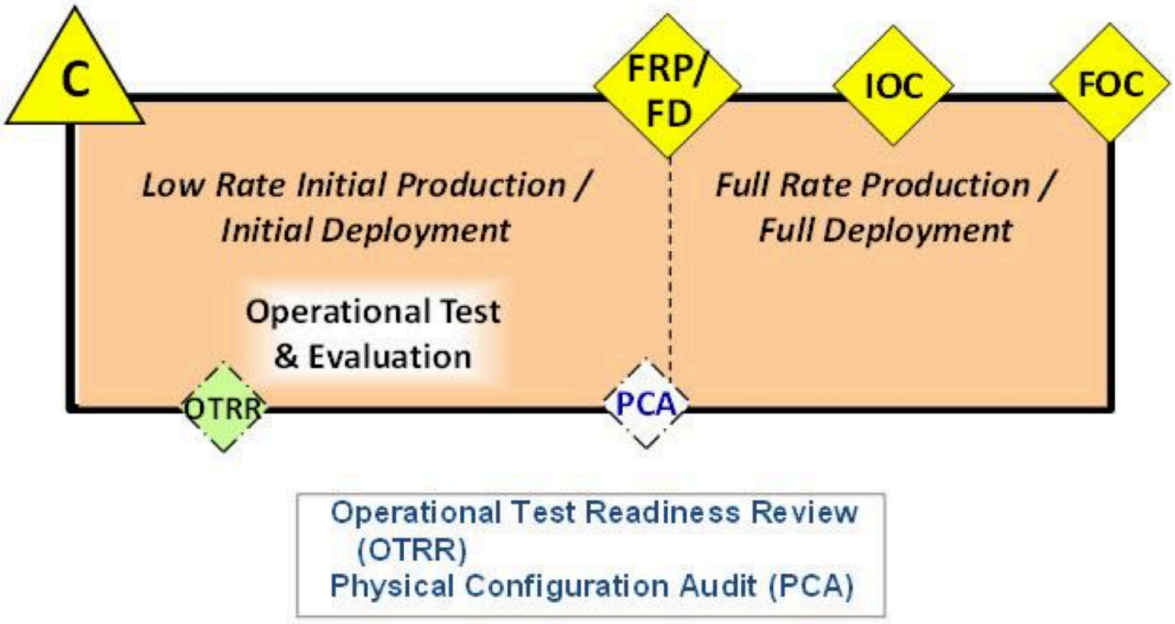


Figure 15 SE Activities in Production and Deployment Phase (11)

The longest phase of the acquisitions process is Operations and Support. In this phase, Full Operational Capability is declared, indicating that the operational units have received the system and are able to operate and maintain the system. If the system requires upgraded capabilities, the acquisitions process will be initiated for the operational requirement. The airworthiness process is repeated for system upgrades or any other modification to include issuing an updated MEFR for testing and MTC for fielding.

The last phase is the Disposal phase when the system. This phase includes demilitarizing the aircraft (removing weapons and hazardous materials), and either storing or destroying them.

STPA Implementation within the Air Force Acquisition Process

STPA in the Acquisitions Process

STPA can easily fit into this acquisitions process as it is currently conducted. Figure 16 shows the acquisitions process again, with numbers indicating where an STPA analysis would fit into the process. Below is a discussion of each number.

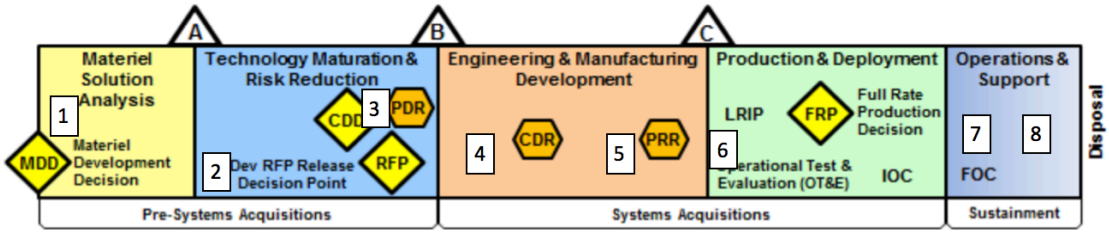


Figure 16 Acquisitions Process with STPA

(1) During the MSA, concept options can be evaluated using STPA. The concept of operations is one of the aspects of the concepts to be evaluated and will include the overarching function and the operational context, which are inputs to an STPA analysis. STPA would generate safety constraints for each of the concept options. The safety constraints, coupled with other aspects of the AoA will be used to support the Milestone A decision.

(2) After Milestone A, in the Technology Maturation and Risk Reduction phase, the system is further defined in more detail. Technical requirements for the RFP are developed, and source selection begins. As the technical requirements for the system are determined, so should the safety requirements. Continuing the STPA analysis will provide high-level safety constraints for input into the RFP. STPA will also provide inputs to the TEMP, SRD, and SEP during this phase.

(3) Once a contract is awarded and the contractor begins the design process, they will continue the STPA analysis for the system and guide the design. The PO should also begin STPA analysis on support functions, such as maintenance, logistics, infrastructure, technical orders, and training. Current airworthiness standards require that the support functions do not detract from the safety of the airframe, therefore these functions should also undergo the analysis. These analyses will also be continuously refined as the basing, maintenance, and logistic constructs are determined.

(4) In EMD, as the system is integrated, designs to achieve safety constraints identified by STPA will be verified by test. Some constraints may be tested in lab environments, such as software in the loop or hardware in the loop facilities. However, because the safety constraints are based on the system as a whole, some constraints will require the integrated system, and may even require the system in the operational environment for verification. This means that as the test plan is developed, each constraint will need to be categorized by how it will be verified. Options for these categorizations may include: inspection of design, software in the loop,

hardware in the loop, ground testing, developmental flight testing, or operational flight testing. If a safety constraint is verified early in the development, such as in a software in the loop facility, the contractor must ensure that further design changes do not affect the safety constraint, otherwise the testing will have to be redone. As the design is changed, the STPA analysis must be updated to ensure that constraints are still valid and identify new constraints associated with the design change.

(5) STPA can also be used to assist in manufacturing planning to ensure that the design can be safely manufactured, but also to ensure that the communication between the manufacturing team and design team is adequate.

(6) In Production and Deployment, the design is fixed unless DT or OT finds unacceptable deficiencies. Should such deficiencies be identified, the deficiencies should be added in the STPA analysis, which will help guide the redesign.

(7) Once the program reaches the Operations and Support phase and the system is FOC, the MAJCOMs will request capability upgrades or decide to use the system in new environments or in different ways than designed. The PO will maintain the STPA products and will modify the analysis with the upgrades to guide the design. The STPA analysis can also be modified with the different environment or utilization information to ensure continued system safety.

(8) If a mishap occurs during O&S, it means that a safety constraint was either missing or not enforced. Mishap investigators can use the STPA analysis on the system, along with evidence from the mishap, to determine what constraints were missing or unenforced and make changes as appropriate. This type of investigation is more powerful than current safety investigations, as it not only prevents the particular mishap from reoccurring, but it also updates the safety constraints to avoid mishaps in general. Methodology to do this already exists. Leveson built upon STAMP to create Causal Analysis based on STAMP, which is used to investigate mishaps from a systems perspective and implement constraints to avoid future mishaps. (8)

Integrating the STPA analysis performed during design with mishap investigation analysis would allow the Air Force, which already has an outstanding safety record, to prevent even more mishaps from occurring. Applying more resources to the current safety practices will have minimal returns – the safety record is as good as it can get without substantial change. A system theory-based approach should be that change. In addition to the fact that STPA covers more scenarios than just component failure, STPA is relatively low cost and takes less time compared to traditional hazard analyses. If STPA replaces FMECA in the development process the program will save time and money and improve safety.

STPA Study Execution and Personnel Composition

STPA studies will vary slightly by the purpose of the study and phase of the program. The description below is for the MSA and TMRR phases before the contractors are involved.

An STPA study can be performed similar to the HAZOP study with a facilitator and a client. Members of AFLCMC, whether they come from airworthiness (AFLCMC/EZ), or system safety (AFLCMC/SES), should be trained on the STPA process and act as facilitators. These facilitators would chair the STPA study and guide the STPA process for programs within LCMC. The program offices would act as the client. The members that should take part in the STPA study are:

- Engineers from each relevant engineering discipline
- System safety engineers
- System operators (either from within the PO, or from the MAJCOM)
- Representatives from DT
- Representatives from OT
- Airworthiness engineers
- Support functions, such as maintenance, logistics, facilities, etc

The study should be broken into the following components:

- Project preparation:
    - Facilitator assigned
    - PO develops accident lists with customer
- Study introduction
    - Introduction to STPA by facilitator
    - PO introduces project
- Hazard development
    - Facilitator leads group to develop hazards
- Safety control structure development
    - Group will create a high-level safety control structure
    - Safety control structure will include:
        - Operational context
        - System function
        - High-level system interactions (e.g. other systems it will interface with)
- UCA development
    - Group will create UCA table based on safety control structure
- UCA scenarios
    - Initial meeting starts scenario generation effort as a group
    - Each lead reviews scenarios after the initial meeting to ensure coverage and determine associated constraints
    - Conduct a final meeting to ensure everyone agrees with the scenarios and safety constraints
- STPA Out brief
    - During MSA, summary of safety constraints for each alternative should be presented along with recommendations
    - During TMRR, the safety constraints will be included in the RFP
        - Resolve any safety constraints that conflict with technical requirements

While the STPA analysis set up to be linear, it is often iterative—as the study proceeds, the group may find that they need to update their hazard list, safety control structure, or UCAs after they have finished that particular portion of the study. Additional meetings may be required as necessary to update previously completed steps.

Once the contract is awarded, the contractor will be responsible for continued analysis of the system. They should take the high-level analysis composed by the PO and develop it further during their design process.

System Safety Process

System safety is defined as "application of engineering and management principles, criteria and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time and cost throughout all phases of the system life cycle." (14) AFI 91-202, The US Air Force Mishap Prevention Program, mandates that each program office must initiate and maintain a System Safety Program that tracks hazards, mitigate risks, and formally accepts residual risks. (14) The document that defines the system safety process is MIL-STD-882E, DoD Standard Practice for System Safety. MIL-STD-882E "identifies the Department of Defense (DoD) Systems Engineering (SE) approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated." (15)

MIL-STD-882E identifies eight elements within the system safety process (15):

1. Document the System Safety Approach
2. Identify and Document Hazards
3. Assess and Document Risk
4. Identify and Document Risk Mitigation Measures
5. Reduce Risk
6. Verify, Validate and Document Risk Reduction
7. Accept Risk and Document
8. Manage Life-Cycle Risk

The system safety approach consists of describing the risk management effort and how it is integrated into the program management structure. Additionally, a hazard tracking system is developed. (15) Hazards are identified and documented in the hazard tracking system in the second element of the process. The standard states that "Hazards are identified through a systematic analysis process that includes system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment." It goes on to say that "mishap data; relevant environmental and occupational health data; user physical characteristics; user knowledge, skills, and abilities; and lessons learned from legacy and similar systems" can also be used to inform the hazard identification.

Hazards are then categorized by risk, which is defined by severity and probability. Risks are then assessed using the Risk Assessment Matrix, as shown in the figure below.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 17 Risk Assessment Matrix (15)

Element four involves identifying potential risk elimination or mitigation options for each identified hazard using system safety design order. Once potential options are identified, element five is to select and implement the risk elimination or mitigation options for each hazard. Next, the risk mitigation is verified and documented in element six, and any residual risk leftover is accepted and documented in element seven. Finally, the program office should continue to manage the risk throughout the lifecycle of the fielded.

Within each of these elements there are a set of tasks, which must be completed to be in compliance with the standard. Task 201 falls under element two, "Identify and Document Hazards". It requires the compilation of a Preliminary Hazard List (PHL) shortly after the materiel solution analysis begins. The PHL is based on historical and similar systems, and the system concept. Task 202 is Preliminary Hazard Analysis (PHA). The PHA consists of identifying hazards, assessing the initial risks, and identifying potential mitigation measures. (15) The risk matrix shown in Figure 17 is used when completing this task.

Recently, Leveson wrote a paper shown how STPA is complaint with MIL-STD-882E. In her conclusion, she states "STPA is totally compliant with MIL-STD-882 and, in fact, was created explicitly to support the tasks involving analysis in this standard." She goes on to say that STPA "is a top-down, system hazard analysis that can be used for the hazard analysis tasks (Tasks 201-209)." (16)

It is important to note that while MIL-STD-882E prescribes a process to conduct system safety, it does not prescribe what tools or methods to use to accomplish the tasks. MIL-STD-882E does call for probabilistic risk assessments, which STPA does not do. There are hazards that are impossible to provide a probability of occurrence. For instance, a recent F-16C mishap was caused by an improperly assembled engine. Two components were missing from the engine when it was built up at the maintenance depot. (17) There is simply no way to assess the probability that such an event may occur. Additionally, the probability, if evaluated based on historical data, may be so small that it is discounted or given a lower risk assessment that is accepted rather than mitigated. However, an STPA analysis of the maintenance organization and processes may have determined the potential hazard of improperly assembling the engine, and designed the safety control structure to avoid the hazard.

The airworthiness process is a subset of the systems safety process, and is discussed in further detail in the next section.

Air Force Airworthiness Process

Airworthiness is defined as "the verified and documented capability of an air system configuration to safely attain, sustain, and terminate flight in accordance with (IAW) the approved aircraft usage and operating limits." (13) The Air Force airworthiness process is determined by both Air Force Instruction (AFI) 62-601 and Air Force Policy Directive (AFPD) 62-6. These documents establish a Technical Airworthiness Authority (TAA) appointed by the Air Force Materiel Commander. (18) This position is responsible for issuing Military Type Certificates (MTC), Military Experimental Flight Releases (MEFR), Military Restricted Flight Releases (MRFR), and special flight releases. MTCs are issued when compliance of the certification criteria are met. MEFRs are issued to allow developmental flight test within a specified time period and flight envelope. MRFRs are issued for particular aircraft under specific conditions when there is a compelling military need and the AF cannot obtain design information in order to conduct an airworthiness assessment. (13) Special flight releases are issued when the certification criteria are not met, but the program managers prove that the aircraft is required for operational purposes.

The TAA chairs the Airworthiness Board (AB), which is comprised of "senior engineering functional organization representatives, an Air Force Safety Center (AFSC) representative, and a representative from the owning AFMC engineering organizations (as requested by the TAA)." (13) The board is responsible for providing airworthiness advice and recommendations to the TAA.

The program office is responsible for ensuring that the system meets airworthiness criteria. Airworthiness planning is included in the Life Cycle Management Plan, System Engineering Plan, and Integrated Master Plan. (13) in addition to providing certification, the TAA provides the guidance and standard processes to the program offices for airworthiness.

Military Handbook 516C (MIL-HDBK-516C), maintained by airworthiness office, contains the airworthiness criteria that must be met in order to be issued the MTC. Program offices do have

the latitude to tailor which criteria apply to their system by applying for an exemption from the criteria that are not applicable. (13) Each major section of MIL-HDBK-516C covers a specific discipline, such as systems engineering, structures, propulsion, avionics, maintenance, and others.

The risk matrices in MIL-STD-882E and MIL_HDBK-516C were updated in an airworthiness bulletin (AWB-150) for airworthiness assessments. (19) The updated risk matrix is shown in Figure 18.

USAF Airworthiness Risk Assessment Matrix			Severity Category			
Probability Level	Probability per FH or Sortie	Freq per 100K FH or 100K Sorties	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	$10^{-3} \leq$ Prob	100 ≤ Freq	1	3	7	13
Probable (B)	$10^{-4} \leq$ Prob < 10^{-3}	10 ≤ Freq < 100	2	5	9	16
Occasional (C)	$10^{-5} \leq$ Prob < 10^{-4}	1 ≤ Freq < 10	4	6	11	18
Remote (D)	$10^{-6} \leq$ Prob < 10^{-5}	0.1 ≤ Freq < 1	8	10	14	19
Improbable (E)	0 < Prob < 10^{-6}	0 < Freq < 0.1	12	15	17	20
Eliminated (F)	Prob = 0	Freq = 0	Eliminated			

High	CAE Risk Acceptance RAC = 1 - 5	Medium	PM Risk Acceptance RAC = 10 - 17
Serious	PEO Risk Acceptance RAC = 6 - 9	Low	Risk Acceptance as Directed RAC = 18 - 20

Figure 18 Updated Risk Matrix (19)

Prior to AWB-150, there were different probability scales with different exposure periods, which greatly altered the severity category assigned to the hazard. The standardized exposure periods will ensure that the probabilistic risk assessments represent the same amount of risk in all programs, which in turn ensures that the residual risk is accepted at the appropriate leadership level.

Just as with STAMP, in order to perform an airworthiness assessment, engineers must understand the system being analyzed and the context in which the system will perform. The context may include flight envelope, operating locations such as improved or unimproved runways, and logistics support. An initial airworthiness assessment will be provided to a program for a new system, however as the system is upgraded or operational context changes, so will the assessment. Airworthiness is therefore not a one-time determination of the safety of the aircraft, but rather continuously evolving.

STPA and Airworthiness

STPA provides a process that complies with the systems engineering and systems safety processes as defined in MIL-HDBK-516C. It is an approach that achieves the 'complete systems

view' and covers a range of criteria and expectations. An analysis of STPA's compliance with Chapters 4 and 14 of MIL-HDBK-516C can be found Appendix 3: STPA Compliance with MIL-HDBK-516C. This section reviews the overarching ideas and conclusions from the analysis.

Throughout the handbook, the verification of method of compliance is listed as "inspection." STPA provides a step-by-step process for analysis that will aid the inspection process. Otherwise, it is not possible to determine whether an inspection process is complete or adequate. Whether the inspection is complete and adequate is based on engineering judgement or checklists established by previous experience, which may be incorrect based on the experience of the engineer with the particular system that is undergoing an airworthiness certification. Additionally, new airframes or modifications may be different enough from legacy systems that basing inspection on historic data does not produce a complete safety analysis or inspection.

While this document only covers systems engineering and systems safety, STPA provides data for the entirety of the system. It provides a construct within which to conduct specific technical safety analyses such as materials or electromagnetic interference testing. STPA will not tell a designer that a material is appropriate for a particular component, but it will guide the designer to focus their energies on flight safety critical components and provide safety constraints as an input to the component or subsystem design. It gives system designers the ability to evaluate their system as a whole during the design phase and eliminate hazards that otherwise may not be identified until integration and testing. STPA will also provide safety constraints not associated with component failures at all, but rather how the human and software controllers interact with the system.

An important aspect of airworthiness certification is that it must be maintained throughout the lifecycle of the system, as the operational employment of the system changes and modifications are made to the system. STPA provides a construct to evaluate changes and ensure they do not introduce hazards to the system. If safety concerns are introduced by the modification, STPA will provide safety constraints for the design of the modification and integration with the baseline system. STPA also covers the support structure associated with the system to ensure that hazards are not introduced by factors outside of the system design.

System-based analysis allows the user to define scope of the system: it may be the specific aircraft being designed, the operational environment where it will be fielded, the maintenance depot that conducts programmed maintenance, or other options. The user can 'zoom' into specific subsystems and 'zoom' out to look at how the system will fit into the current operational and support structure.

The system analysis is meant to start high-level and work deeper into detail. When a program office is determining technical requirements to be included in an RFP, a high-level STPA may be completed to provide high-level safety constraints that must be included in the design. Once the contract bid is awarded and the design process begins, the STPA should be conducted as part of the design process to assist in decision-making about safety. As the design becomes

more detailed, so does the STPA analysis. The result is a system design that was guided by safety and documentation to show the airworthiness certification inspectors that the aircraft is safe to operate.

Reliability and Redundancy

Often when minimizing the risk associated with a component failure, redundancies are added such that even if one component fails the other will perform the safety critical function. Take for example a component that has a 20% probability of failure over a period of time. The reliability of that component is:

$$R = 1 - F$$

Where R is the probability the component will not fail, and F is the probability of failure. Therefore, R is 80%. If the component is flight critical, the design team may elect to use redundancy to increase reliability. In this case, reliability is:

$$R = 1 - (F_1)(F_2)$$

Which brings reliability up to 96%.

While this appears on the surface to be a logical and straightforward methodology, one must consider the assumptions that go into this analysis. In particular, the assumption of independence: the components must be completely independent of each other in order for the analysis to be valid.

The author flew on a test mission when a hydraulic pump failed in flight. The particular aircraft had two hydraulic systems that were usually tied together and includes four engine driven pumps. The systems can be isolated when required. The hydraulic pump's failure could cause metal contamination of the hydraulic system; therefore, the systems were isolated in response to the failure to prevent the additional pumps from failing. In this case, the pumps are not truly independent, as the pilots must take action to prevent the failure of one pump from causing the other pumps to fail. There are other dependencies between the pumps as well. the system was serviced by the same hydraulic mule, which if contaminated, would affect all the pumps. The same maintenance personnel inspect, repair, and replace the pumps, therefore if there is a deficiency in the maintenance practices all pumps could be at risk. If the components are exposed to harsh environments such as humidity, sand, or saltwater they will all deteriorate. Finally, if there is a manufacturing defect or incorrect specification being used, all components from the affected lots may have the same problem. So, in fact, the reliability would not be 96% in the case shown above, but rather something less. What that something is would be difficult if not impossible to quantify, as maintenance errors, manufacturing defects, and other dependencies are not probabilistically determined.

Therefore, using FMEA or FMECA cut sets to determine the probability of a failure will not yield accurate information. If design decisions are made based on the probabilistic assessment they will most likely be flawed. STPA, on the other hand does not rely on probabilities, making the results of STPA more actionable.

In addition, software flaws are design errors. Redundancy of flawed designs or software created from the same flawed requirements is not going to improve either reliability nor safety. What aircraft today are not built with extensive software components?

It should be noted that redundancy can be used to create a safe design, however it can be performed in more powerful ways such as dissimilar redundancies (i.e. power through batteries and an alternator), more accurately ensuring true independence of the components, and by not assuming that the reliability calculations above will yield an accurate answer that can be used to determine the risk level of the system. But all of these approaches apply only to hardware and ignore the software and the humans in the design. Software diversity does not work. (20)

An STPA analysis of the design will yield safety constraints that will minimize hazards associated with component failure, and also those created through design flaws and by unsafe interactions among components that have not failed.

Risk matrices

The two components of risk matrices are probability of occurrence and severity. The section above discusses ways in which probability of occurrence is not correct for redundant components. There are other reasons why probability of occurrence is impossible to predict: component interactions that are not failures, software related errors, and human interaction related errors all cannot be determined probabilistically. They are dependent on the quality of requirements development, how well the components are designed to work together, and how well the system is designed for human interaction. This is why STPA is so important – it provides safety constraints to better inform requirements and design.

What makes STPA unpalatable for some decision makers is there is no way to quantify residual risk that is accepted as part of the system design. People in technical fields such as engineering and acquisitions desire quantitative methods to make decisions. However, if the calculated values are wrong and lead to misunderstood residual risk, the decision will not result in a safe system. Using STPA rather than risk matrices will require a paradigm shift, but it will result in a more accurate understanding of the hazards associated with the design.

Systems Thinking in the AF: Effects-Based Approach to Operations

The greatest benefit of STPA is providing a systematic framework for evaluating the problem at hand that, if done right, is complete and considers the problem as a whole. It cannot be reduced down to a checklist. Doing so will negatively affect the benefits of STPA, and it will not work. This means that conducting STPA across a large, diverse, and dynamic workforce in dozens of different program offices presents a challenge. When thinking about how that challenge can be addressed in the Air Force, it was realized that systems thinking already exists in the Air Force in the form of EBAO.

EBAO provides a systematic framework to consider the problem of designing combat strategies. Annex 3-0 Operations and Planning discusses EBAO. In the opening paragraph, in bold letters,

the document states, "**EBAO is not a planning methodology; *it is a way of thinking about operations* that provides guidance for design, planning, execution, and assessment as an integral whole."** (21) STPA in this regard "provides the information and documentation necessary to ensure the safety constraints are enforced in system design, development, manufacturing, and operations, including the natural changes in these processes that will occur over time." (8)

Safety is an example of an emergent property. (22) Just because two components by themselves appear safe, does not mean that when you put the two together as part of a system their interaction will be safe.

Strategists understand the concept of emergent properties. An emergent property is a property that "arise from the interactions among the components." (22) Annex 3-0 refers to this concept as 'additivity' and says, "**Additivity** means that the whole equals the sum of its parts, but this is not true of living systems, which are more complex and often greater in output than the sum of their components, just as the joint force working as an integrated whole is more effective than its components working independently ("synergy"). The behavior of interactively complex systems often depends more upon the linkages between components than upon the components themselves. In fact, system-wide behavior often cannot be deduced from analysis of the component parts."

Annex 3-0 states, "**Reductionism** is the common scientific method of analyzing systems, by "pulling them apart" conceptually and examining how each component operates separately to determine overall system behavior. It has been the main technique behind machine design for centuries, as well as "nodal" methods of "systems analysis." However, reductionist methods may yield less insight than ways of examining systems as a whole—analyzing how the system behaves in relation to other systems in its environment, as well as how components of the system interact, and then trying to anticipate how the interaction of these systems may cause certain types of behavior, or allow new behaviors to emerge. Breaking a complex problem into constituent, structurally complex parts and solving each part will not necessarily solve the overarching problem, just as winning every battle does not guarantee winning a war."

The designers of EBAO also recognized that linear cause and effect relationships cannot be applied to strategic planning, stating "However, causes and effects are often hard to trace and harder to demonstrate, since common "linear" rules frequently do not apply—especially in cases involving human will" (21)

Similarly, in Engineering a Safer World, Professor Leveson says of reduction, "This assumption in turn implies that the components or events are not subject to feedback loops and other nonlinear interactions and that the behavior of the components is the same when examined singly as when they are playing their part in the whole." (8)

Therefore, when reduction and linear cause and effect analyses are used to analyze a complex system, such as an aircraft, component interactions are missed, which means safety constraints

for the system are not complete. STPA was purposely designed to analyze emergent properties.

Another commonality between EBAO and STPA is that "**EBAO focuses on behavior, not just physical changes."** (21) In other words, the analysis must be based on functionality. Strategists that employ EBAO seek to affect the function of opposing forces, just as STPA seeks to control the behavior of a design within specific safety constraints.

These systems-based ideas encompassing EBAO are accepted throughout all levels of Air Force leadership, and are taught to all officers in Air Force professional education. EBAO is an integral component of Air Force strategy, and affects the way the Air Force trains and executes combat operations.

System engineering methods are used by POs and contractors to design for emergent properties, such as safety, performance, reliability, or maintainability. Yet the AF still spends a decade or more of developmental testing *simply to understand what we built,* which causes schedule delays, cost overruns, and occasionally tragic loss of life. The program offices find themselves in a fly-fix-fly loop until the aircraft performs in a manner that is deemed acceptable enough to be fielded. This indicates that there is more to be done in the way that the AF applies systems engineering within programs.

The power of STPA is that it can lead to a transformation of how acquisitions professionals think about their systems, just as EBAO transformed the way the Air Force targets enemy forces. System engineers cannot be the only people in a program that think of the product and related support structure as systems. Other engineers don't necessarily need to be formally educated in SE, but they do need to learn SE concepts in order to make thoughtful design decisions that consider their program as a whole. They should also understand how emergent properties arise from the design – and more importantly inform the design to create the weapon system right the first time.

In order to demonstrate the use of STPA in the acquisitions process, two examples are provided of STPA analysis along with descriptions of how the information obtained can be used in acquisitions. The first example is of a high-level JSTARS analysis as might be completed during concept development. The second is of a UAV further in the design phase in TM&RR.

JSTARS Analysis

JSTARS System Definition

The E-8C JSTARS, or Joint Surveillance Target Attack Radar System provides multiple functions, to include airborne battle management, command and control, intelligence, surveillance, and reconnaissance. (23) According to the USAF's factsheet, the primary mission of the JSTARS is "to provide theater ground and air commanders with ground surveillance to support attack operations and targeting that contributes to the delay, disruption and distraction of enemy forces." (23)

The JSTARS is equipped an AN/APY-7 sensor that includes a side-looking, phased array radar, moving target indicator, and synthetic aperture radar modes. (24) The JSTARS collects data using this sensor, and then provides that data to ground personnel and aircraft supporting the ground war.

The USAF is currently in the process of recapitalizing the fleet, as the E-8Cs are aging Boeing 707-based aircraft. The intent is to acquire an aircraft that functionally replaces the current fleet, but with modern technologies that will reduce operational cost. (25) This analysis therefore examines a function that is the same as the current aircraft.

JSTARS System Mishaps, Hazards, and High-Level Safety Constraints

The mishaps associated with this system are:
M1. Loss of life
M2. Loss of property
M3. Loss of mission

The hazards for the system, which are all traceable back to a mishap, are:
H1. Aircraft violate minimum separation requirements (M1, M2)
H2. Friendly ground troops targeted (M1, M2)
H3. Unacceptable collateral damage (M1)
H4. Friendly forces not provided actionable data (M3)
H5. Aircraft engaged by enemy defenses (M1, M2, M3)
H6. Aircraft violates minimum altitude requirements (M1, M2)
H7. Support aircraft cannot provide support to ground troops (M1, M3)

Each hazard has an associated safety constraint:
SC1. Aircraft must not violate minimum separation requirements
SC2 Aircraft and ground troops must not target friendly ground troops
SC3. Aircraft and ground troops must not cause unacceptable collateral damage
SC4. JSTARS must provide actionable data
SC5. Aircraft must not be engaged by enemy defenses
SC6. Aircraft must not violate minimum altitude requirements

SC7. Support aircraft must provide support to ground troops

JSTARS Safety Control Structure

The safety control structure is based on the functionality discussed in the system description.

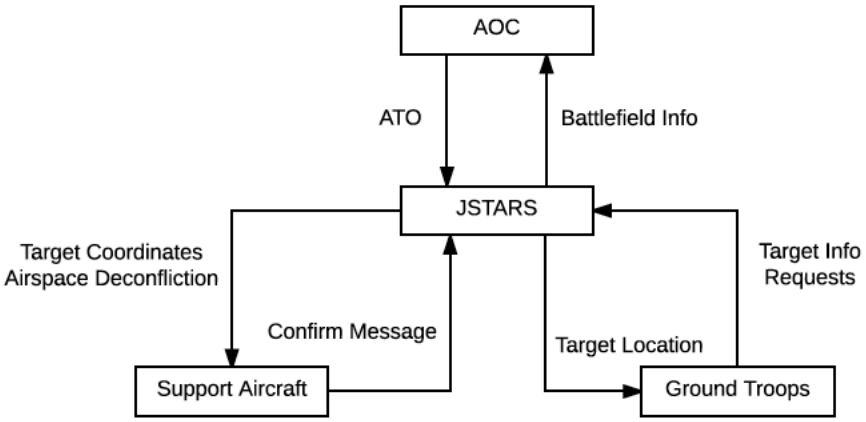


Figure 19 JSTARS Safety Control Structure

The Air Operations Center (AOC) is responsible for planning the air war and providing air assets with their tasking, known as an Air Tasking Order (ATO). JSTARS and other assets can provide feedback to the AOC in order for the AOC to understand the effectiveness of their planning and adjust as necessary.

The JSTARS, as previously described, provides target coordinates and airspace deconfliction to the support aircraft in the JSTARS area of responsibility.

The support aircraft confirms the messages received from the JSTARS and will engage targets as directed.

Ground troops will request target information, and use target information provided by the JSTARS to engage the enemy.

JSTARS Step 1: UCA Generation

The commands shown in the safety control structure are then used to the UCA table shown below.

Table 3 JSTARS UCAs

JSTARS	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/ Applied Too Long
Target Coordinates to Support Aircraft	JSTARS does not provide target coordinates to support aircraft when the target needs to be engaged (H4)	JSTARS provides target coordinates, but the coordinates are not where the enemy is located (H2, H3) JSTARS provides target coordinates to support aircraft that are within contested airspace (H6)	JSTARS provides target coordinates before the enemy forces are separated from civilians (H3) JSTARS provides target coordinates after the enemy leaves the target location (H2, H3) JSTARS provides target coordinates to support aircraft after friendly forces have moved towards and engaged enemy forces (H2) JSTARS provides target coordinates to support aircraft after support aircraft expends weapons (H7)	N/A
Airspace Deconfliction	JSTARS does not provide airspace deconfliction when support aircraft are co-altitude in the same airspace (H1)	JSTARS provides support aircraft deconfliction instructions that create a conflict (H1) JSTARS provides airspace deconfliction when the instruction causes the aircraft to fly too close to terrain (H5) JSTARS provides airspace deconfliction when the instruction causes the aircraft to enter into contested airspace (H6)	JSTARS provides aircraft deconfliction before support aircraft changes radio frequency to JSTARS frequency (H1) JSTARS provides aircraft deconfliction instructions after a midair collision (H1)	JSTARS provides partial aircraft deconfliction instructions (H1)

Target Coordinates to Ground Troops	JSTARS does not provide target coordinates to ground troops when a target needs to be engaged (H4)	JSTARS provides target coordinates, but they are not where the enemy is located (H2, H3)	JSTARS provides target coordinates after the enemy leaves the target location (H2, H3) JSTARS provides target coordinates to ground troops after friendly forces have moved towards and engaged enemy forces (H2)	N/A

Once the UCAs are generated, safety constraints can be developed to prevent the hazards.

Table 4 JSTARS UCAs and Safety Constraints

UCA Designator	UCA	Hazards	Constraint
J1	JSTARS does not provide target coordinates to support aircraft when the target needs to be engaged (H4)	H4	JSTARS must provide target coordinates to support aircraft when the target needs to be engaged
J2	JSTARS provides target coordinates, but the coordinates are not where the enemy is located (H2, H3)	H2, H3	JSTARS must provide target coordinates where the enemy is located
J3	JSTARS provides target coordinates to support aircraft that are within contested airspace (H6)	H6	JSTARS must not provide target coordinates that are within contested airspace
J4	JSTARS provides target coordinates before the enemy forces have separated from civilians (H3)	H3	JSTARS must not provide target coordinates if the enemy is in close proximity with civilians
J5	JSTARS provides target coordinates after the enemy leaves the target location (H2, H3)	H2, H3	JSTARS must not provide target coordinates after the enemy leaves the target location
J6	JSTARS provides target coordinates to support aircraft after friendly forces have moved towards and engaged enemy forces (H2)	H2, H3	JSTARS must not provide target coordinates to support aircraft after friendly forces have moved within close proximity of enemy forces

J7	JSTARS provides target coordinates to support aircraft after support aircraft expends weapons (H7)	H7	JSTARS must provide target coordinates to support aircraft with the appropriate weapons payload
J8	JSTARS does not provide airspace deconfliction when support aircraft are co-altitude in the same airspace (H1)	H1	JSTARS must provide airspace deconfliction when support aircraft are co-altitude in the same airspace
J9	JSTARS provides support aircraft deconfliction instructions that create a conflict (H1)	H1	JSTARS must not provide deconfliction instructions that create a conflict
J10	JSTARS provides airspace deconfliction when the route is too close to terrain (H5)	H5	JSTARS must not provide airspace deconfliction when the route is too close to terrain
J11	JSTARS provides airspace deconfliction when the new route is through contested airspace (H6)	H6	JSTARS must not provide airspace deconfliction when the new route is through contested airspace
J12	JSTARS provides aircraft deconfliction before support aircraft changes radio frequency to JSTARS frequency (H1)	H1	JSTARS must not provide aircraft deconfliction before support aircraft changes radio frequency to JSTARS frequency
J13	JSTARS provides aircraft deconfliction instructions after a midair collision (H1)	H1	JSTARS must provide aircraft deconfliction to aircraft when the aircraft has time to take action
J14	JSTARS provides partial aircraft deconfliction instructions (H1)	H1	JSTARS must provide complete deconfliction instructions
J15	JSTARS does not provide target coordinates to ground troops when a target needs to be engaged (H4)	H4	JSTARS must provide target coordinates to ground troops when a target needs to be engaged
J16	JSTARS provides target coordinates, but they are not where the enemy is located (H2, H3)	H2, H3	JSTARS must provide target coordinates where the enemy is located
J17	JSTARS provides target coordinates after the enemy leaves the target location (H2, H3)	H2, H3	JSTARS must not provide target coordinates after the enemy leaves the target location

J18	JSTARS provides target coordinates to ground troops after friendly forces have moved towards and engaged enemy forces (H2)	H2	JSTARS must not provide target coordinates to support aircraft after friendly forces have moved within close proximity of enemy forces

JSTARS Step 2: Scenario Generation

Finally, the scenarios for each UCA are developed. The table of all scenarios can be found in Appendix 1.
Several safety constraints identify the need for interoperability between JSTARS, support aircraft, and ground troops. Interoperability amongst joint forces has been an issue in previous program acquisitions, therefore highlighting interoperability early is incredibly important, especially for a program such as JSTARS.

Other scenarios indicated the need for data that JSTARS itself may not be able to detect, such as location of all aircraft within the area of responsibility, and location of enemy threats. The data would then have to come from other sources. These sources must be identified early so that the inputs into the JSTARS system are well understood and incorporated into the design.

Another important safety constraint that was discovered is the need for communication within the JSTARS aircrew. At this early stage of development, the number and function of aircrew likely has not been decided. Critical crew communication constraints must be considered in the design of the system and determination of aircrew complement.

JSTARS STPA Summary

This analysis was completed with a concept of function and operational context. There is no detail about the actual system under design. This type of analysis would occur during concept development in the MSA phase of the acquisitions process. It can also be used to provide safety constraints to be included in the RFP in the TMRR phase.

Recently, it was announced that the JSTARS Recapitalization program may not go forward as expected. The Air Force is considering whether or not we really need an aircraft to do this mission at all, or if it could be accomplished through a distributed network of sensors with the battle managers located away from the war. (26) The Air Force is concerned that JSTARS would not survive in a large-scale war against an enemy with significant anti-air capabilities. A large aircraft such as the JSTARS may not survive highly contested airspace, whereas other aircraft are designed for survivability in contested environments. The Air Force is attempting to determine if, rather than put an expensive asset with relatively few numbers in harm's way, a non-airborne JSTARS replacement system could receive data from airborne assets and perform the function of the current JSTARS. The analysis performed above is mostly agnostic to such decisions. It does not matter if the JSTARS is airborne in theater or in a building located in the US. The function will remain the same. Where one finds a difference between airborne and

non-airborne analyses is in the scenarios. For instance, non-airborne JSTARS replacement would be entirely dependent on assets external to the JSTARS system for sensor data and communications. Airborne JSTARS missions are limited in duration based on fuel and crew duty day and limited in range by the airfield location and enemy threats. Scenarios based on these differences could be developed to determine what constraints are required given the two options. In this way, different concepts or alternatives may be evaluated early in the acquisition process.

JSTARS Support STAMP Analysis

Early in the acquisition process, the program office will begin determining the support structure required for the fielded system. This will include the maintenance and supply structure, required ground equipment, suitable airbases to base operations, aircrew and maintenance procedures and training, technical order support, and others. STPA can support this decision as well.

JSTARS Support Mishaps

M1. Loss of life
M2. Loss of JSTARS or other property
M3. Loss of mission

JSTARS Support Hazards

H1. JSTARS is not mission capable (M3)
H2. JSTARS maintenance procedures are unsafe (M1, M2, M3)
H3. JSTARS operational procedures are unsafe (M1, M2, M3)
H4. JSTARS aircraft does not meet operational requirements (M3)

JSTARS Support Safety Control Structure

The safety control structure shown in Figure 20 is not all inclusive, but it gives the reader an idea of what the support structure might look like for the JSTARS.

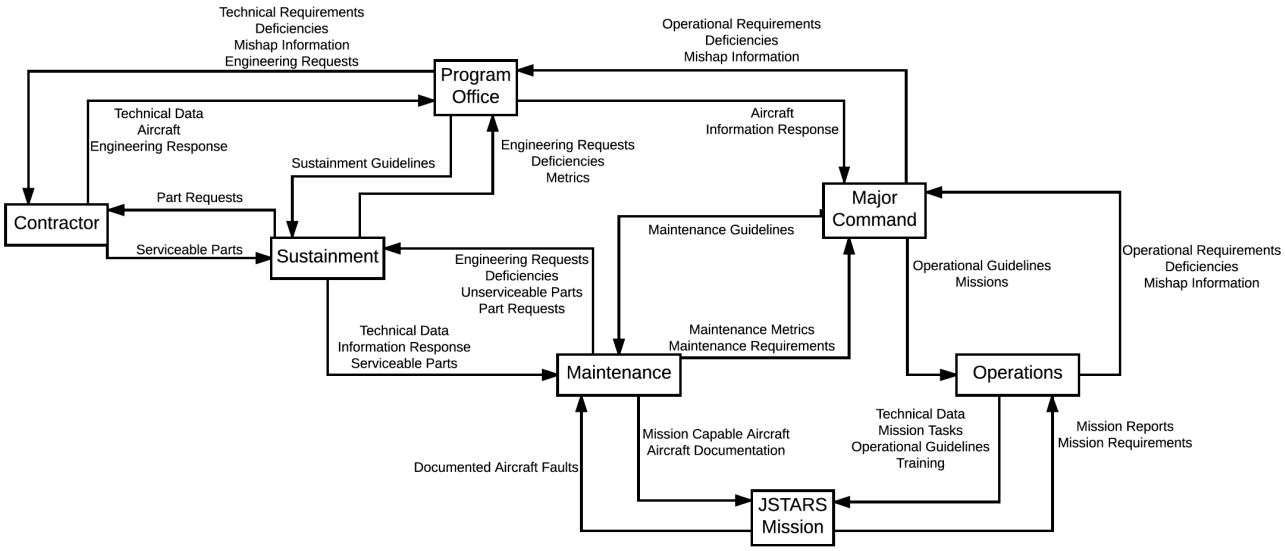


Figure 20 Simple JSTARS Support Safety Control Structure

There are critical decisions within this support structure that the program office must decide upon. For instance, who is responsible for repairing unserviceable parts? It could be at a sustainment center by Air Force personnel, or it could be a contracted service. Who will be responsible for answering engineering technical requests and maintaining technical data? Again, it could be Air Force engineers or the contractor. Each decision has ramifications to maintaining the safety of the system, and an STPA analysis of safety control structures defined by the potential choices assists the program manager in the decision. Any safety constraints identified by the analysis of the winning solution must be incorporated into program planning.

STPA Step 1 and 2 were not completed for this example, as the purpose was to illustrate how STPA is used in decision-making beyond the design of the system itself.

UAV STPA Analysis

UAV System Definition

Recently, a group modified a general aviation aircraft to create an unmanned aerial vehicle (UAV). The modifications included a vehicle management system (VMS) with autopilot linked to actuators which control the engine throttle and control surfaces, an engine control module, alternators, a lipstick camera to allow the operator to see in front of the UAV, and radio and payload additions.

The operational context for the UAV is a takeoff, climb, and cruise at altitude for several hours before returning to the airfield. A ground station at the airfield controls the UAV using line of sight (LOS) communications. Once the UAV is at cruise, the ground station operator will transition the UAV to beyond line of sight (BLOS) communications. The BLOS ground station is not located at the airfield, and communicates with the UAV via satellite.

The UAV does not taxi during ground operations. It is towed to the engine run-up area, to the runway for take-off, and off the runway to parking after landing.

Lost link procedures are set such that when the link is lost the UAV will continue along the path for a certain period of time. If the link is not reestablished, the UAV will return to the airfield via the latest lost link procedure provided to the UAV.

UAV Accidents, Hazards, and High-Level Safety Constraints

The accidents for the UAV operation are:
A1. Loss of life/injury
A2. Loss of or damage to UAV aircraft
A3. Loss of mission

The hazards for the UAV operation are:
H1. UAV too close to ground/building/person (A1, A2)
H2. UAV violates minimum separation requirements (A1, A2)
H3. UAV does not complete mission (A3)
H4. UAV departs controlled flight (A1, A2)
H5. UAV departs apron, taxiway, or runway during ground operations (A1, A2)
H6. Loss of UAV airframe integrity (A1, A2)

Each hazard is traceable back to an accident. Each hazard has an associated high-level safety constraint:

SC1. UAV aircraft must not collide with the ground, buildings, or people (H1)
SC2. UAV aircraft must not violate minimum separation requirements with other aircraft (H2)
SC3. UAV must complete assigned mission (H3)
SC4. UAV must not depart controlled flight (H4)

SC5. UAV must not depart the apron, taxiway, or runway during ground operations (H5)
SC6. UAV must not lose airframe integrity (H6)

Each of these high-level safety constraints will be achieved if lower level safety constraints are achieved. The lower level safety constraints will be explored during Step 1 and Step 2 of STPA.

UAV Safety Control Structure

The UAV safety control structure is shown in Figure 21. The ground station consists of the operator and the user interface (UI). The user interface is loaded onto a computer, and communicates with the UAV via radios. The operator provides commands through interaction with the UI. Feedback regarding the state of the UAV is displayed on the UI.

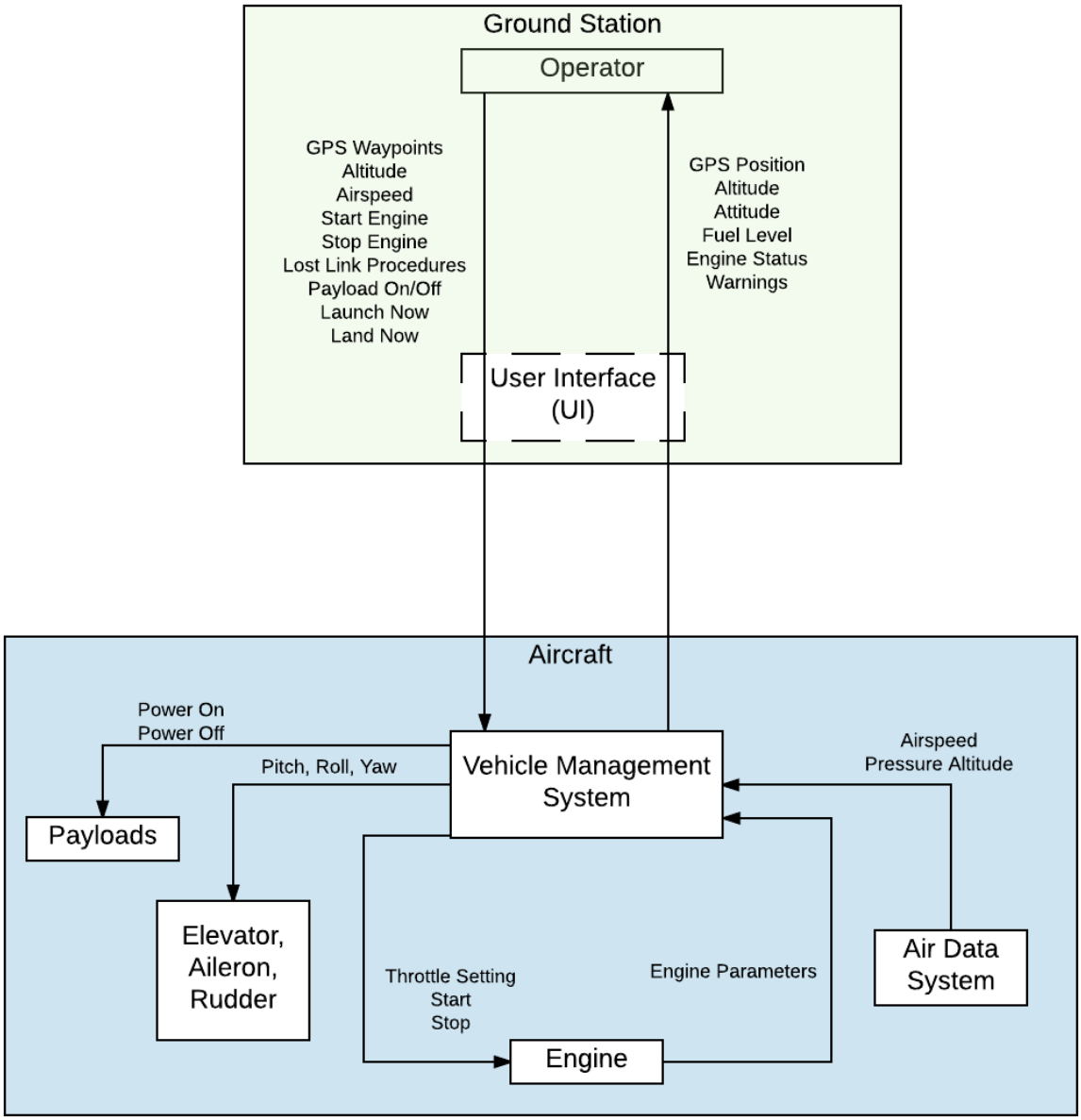


Figure 21 UAV Safety Control Structure

The aircraft consists of the VMS, payloads, control surfaces, engine, and air data system. The VMS is a pass through for the payload power and engine start/stop commands: it provides the command when the operator sends the command to the VMS. The pitch, roll, yaw, and throttle setting commands are determined by the VMS based on the GPS waypoint altitude, and airspeed commands given by the operator. The VMS uses location data, engine parameter data, and airspeed and altitude data to determine the appropriate pitch, roll, yaw, and throttle commands.

STPA Step 1: UCA Generation

The first step of the analysis is to define the UCAs and the associated requirements. As stated previously, control actions are hazardous if:

1. A control action required for safety is not provided or not followed.
2. An unsafe control action is provided.
3. A potentially safe control action is provided too early or too late, at the wrong time or in the wrong sequence.
4. A control action required for safety is stopped too soon or for too long. (8)

The UAV UCAs were divided into operator UCAs and aircraft UCAs. The UCAs are not written in sentence format in Table 5 and Table 6, but they can be written in sentence format using the information in the table. For instance, the first UCA in row 2, column 2 in Table 5 is written as "The operator does not provide the GPS waypoints during prelaunch operations."

Table 5 UAV Operator UCAs

Operator	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
GPS Waypoints	…during prelaunch operations (H3) …when mission changes (H3)	…when GPS waypoints do not align with the mission (H3) …when the waypoints present a conflict with other aircraft (H2) …when the route length exceeds the fuel on board (H4) ...when the route is outside of LOS radius and BLOS is not being used (H3, H4)	…after LOS is lost, but before BLOS radio link is established (H3, H4) …after the UAV reaches bingo fuel (H4)	…when the number of waypoints exceed the storage capacity of the autopilot (H3) …when the list of waypoints is not complete for the entire mission (H3)

Altitude	…when the GPS waypoints are updated (H1, H2, H3)	…when the altitude, coupled with the programmed waypoints are not above minimum obstacle clearance altitude (MOCA) (H1) …when the altitude conflicts with other traffic's altitude blocks (H2) …when the altitude is above icing level and the UAV flies through clouds (H4)	…after LOS is lost due to terrain masking, but before BLOS radio link is established (H3)	…when the altitude assignments exceed the number of GPS waypoints (H3) …when there are fewer altitude assignments than waypoints and it does not include the entire mission (H3)
Airspeed	…during a change in flight or environmental conditions (H1, H4, H6)	…when the airspeed provided is at or below stall speed (H4) …when the airspeed is above VNE (H6) …when flight planning fuel duration was based on auto (max endurance) airspeed, but a higher airspeed is set (H3, H4) …with an airspeed value that will create a conflict with other aircraft (H2)	…after the UAV stalled due to slow flight (H4) …after structural damage from flying above VNE (H6)	…when the airspeed assignments exceed the number of GPS waypoints (H3) …when the airspeed assignments are fewer than the number of GPS waypoints (H3)
Engine Start	…during prelaunch engine run-up (H3) …during before takeoff procedure (H3) …when the engine fails in flight and the engine needs to be restarted (H4)	…when ground personnel are near the propellers (H1)	…when the engine fails in flight, but after the UAV is committed to landing (H1)	N/A

Launch Now	…during takeoff (H3)	…when the runway is not clear (H2) …when the UAV is not on the runway (H5)	…before ground personnel have cleared the area (H1) …after the UAV is airborne (H4)	N/A
Land Now	…when the UAV is in the pattern and at minimum fuel (H4) …when the UAV is at the airfield and other aircraft are attempting to enter the pattern (H2)	…when the runway is not clear (H2) …when the UAV is not at the airfield (H1)	…before the UAV completes the airfield arrival procedure (H1, H2)	N/A
Lost Link Procedure	…during flight operations (H1, H2)	…when the lost link procedure waypoints conflict with other aircraft (H2) …when the lost link procedure is not at or above MOCA (H1)	…before terrain, conflicting traffic, or weather necessitate a lost link procedure update (H1, H2)	…when the waypoints exceed the storage capacity of the autopilot (H1, H2)
Payload Power On	…when UAV is over the target area (H3)	…when the alternator fails (H4)	N/A	N/A
Payload Power Off	…when the alternator fails (H4)	…when the UAV is over the target area (H3)	N/A	N/A

Table 6 UAV VMS UCAs

Vehicle Management System	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/Order	Stopped Too Soon/Applied Too Long
Roll, Pitch, Yaw	…when the UAV is off course (H1, H2, H3)	…when the roll, yaw, or pitch command exceeds aircraft attitude limits (H4) …when the roll, pitch, yaw command steers the UAV off course (H1, H2, H3)	…when the throttle is reduced in order to descend, but the subsequent pitch down command is delayed (H4) …when the throttle is increased for a climb, but the subsequent nose up command is delayed (H6)	…the actuator displacement is not brought back to neutral when the aircraft reaches the target heading/descent/ascent (H1, H2, H3) …the actuator displacement is brought back to neutral before the UAV reaches the target heading/descent/ascent (H1, H2, H3)
Throttle Setting	…when environmental conditions change (H4, H6) …when the UAV is in a sustained turn, which reduces lift (H1, H2)	…when the throttle setting is not enough to maintain an airspeed above stall speed (H4) …when the throttle setting accelerates the aircraft above VNE (H6)	…reduces throttle too late after the UAV flares for landing (H1, H5)	…when the accelerates to a target speed, but the throttle is not reduced before reaching VNE (H6) …when the UAV decelerates to a target speed, but the throttle is not increased before reaching stall speed (H4)

Once the UCA tables are populated, safety constraints to prevent each of the UCAs must be identified. An example of the safety constraints for the GPS waypoints control action are shown in Table 7. The entire table of safety constraints can be found in Appendix 2.

Table 7 Example of Safety Constraints Derived from UCAs

UCA Designator	UCA	Hazards	Constraint
C1	The operator does not provide the GPS waypoints during prelaunch operations	H3	The operator must provide GPS waypoints during prelaunch operations

C2	The operator does not provide updated GPS waypoints when mission changes	H3	The operator must provide GPS waypoints during the mission when the mission changes
C3	The operator provides the GPS waypoints when they do not align with the mission	H3	The operator must not provide GPS waypoints that do not align with the mission
C4	The operator provides the GPS waypoints when they present a conflict with other aircraft	H2	The operator must not provide GPS waypoints that present a conflict with other aircraft
C5	The operator provides GPS waypoints and the route length exceeds the fuel on board	H4	The operator must not provide GPS waypoints for a route that exceeds the fuel on board
C6	The operator provides GPS waypoints that create a route outside of LOS radius and BLOS is not being used	H3, H4	The operator must not provide GPS waypoints that create a route outside LOS radius if BLOS is not being used
C7	The operator provides GPS waypoints after LOS is lost, but before BLOS radio link is established	H3, H4	The operator must provide waypoints while the UAV is in LOS
C8	The operator provides GPS waypoints after the UAV reaches bingo fuel	H4	The operator provides GPS waypoints to bring the UAV back to the airfield before the UAV reaches bingo fuel
C9	The operator provides GPS waypoints and the number of waypoints exceed the storage capacity of the autopilot	H3	The operator must not provide GPS waypoints for a route that exceeds the fuel on board

STPA Step 2: Scenario Generation

The second step of STPA is to generate the scenarios. The majority of the actionable data that can be implemented into the system design will come from this step. It is not enough to just understand what can happen, but to understand how it could happen. Once the 'how' is known, constraints are developed to prevent the hazard from occurring.

The scenarios were generated using a new method recently developed by Dr. John Thomas. The method divides the scenarios into types by their location on the safety control structure. The four types are:

1. Command not followed or followed inadequately

2. Inappropriate decision
3. Inadequate feedback or other inputs
4. Inadequate process behavior (27)

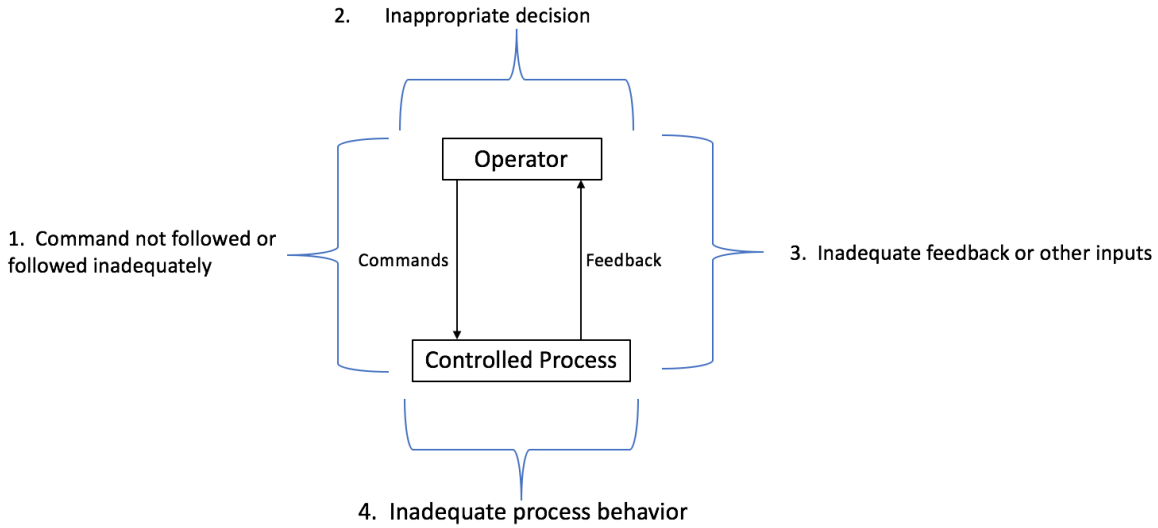


Figure 22 Scenario Types on Control Structure

Previously, when generating scenarios, a person (or people) would examine the safety control structure and come up with scenarios, in a brainstorming type of manner. While this produces good results, it does not necessarily ensure coverage of the entire control structure. Just as bucketing UCAs into four categories ensures each type of UCA is considered, bucketing scenarios ensures coverage across the control structure. The type of scenario and corresponding location on the control structure is shown in Figure 22.

UCA V2 states, "The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits." The hazard associated with this UCA is H4 "UAV departs controlled flight." The following scenarios were generated using the new procedure:

V.2.1 The VMS does not provide the roll, pitch, or yaw command, but the aileron, elevator, and rudder receive the command. *A shorted wire provides power to the actuator causing the aileron, elevator, or rudder to move.* The aileron, elevator, and rudder receive the command even though the VMS did not command it. (Type 1)

V.2.2 The VMS provides the roll, pitch, or yaw command and exceed limits for the current flight condition. *The VMS was programmed with one set of attitude limits, rather than a set of attitude limits for different flight conditions (altitude & speed).* The command did not exceed the programmed limits, but it did exceed actual limits for that particular flight condition. (Type 2)

V.2.3 The VMS provides a roll, pitch, or yaw command that it believes will result in an attitude within limits, however the attitude is actually out of limits. *The aeromodelling*

of the system was not validated, and the magnitude of the command is too large. The commanded attitude is actually out of limits. (Type 2)

V.2.4 The VMS provides a roll, yaw, or pitch input to correct an invalid attitude indication it is receiving and exceeds attitude limits. *The invalid feedback is due to a vacuum pump failure that renders the attitude indicator inoperative.* The command exceeds attitude limits, but the VMS does not recognize the exceedence due to the invalid attitude indication. (Type 3)

V.2.5 The VMS provides a roll, pitch, or yaw command that is appropriate for staying within the UAV attitude limits. *The actuator was connected to the cables backwards, and the VMS input has the opposite effect (roll left input rolls UAV right).* The VMS continues to command in the same direction in an attempt to correct the attitude eventually exceeding aircraft limits. (Type 4)

Note that, just as with UCAs, there can be more than one scenario for each type. In fact, that should be expected.

In the examples above the italicized font is the refined scenario and the regular font is the general scenario. The scenario type informs the general scenario. The refined scenario is based on knowledge of the system and the operational context. There may be more than one refined scenario per general scenario. Dividing up the scenarios assists facilitation of an STPA analysis. An STPA expert can derive the general scenarios, then work with the system and operational experts to determine the refined scenarios that are applicable to the specific use of the system.

This process also reveals additional hazards associated with the UCAs that might not be apparent during UCA development. In the example above, the UCA is associated with the hazard H4. Scenario V.2.5 is associated with an additional hazard, H5, "UAV departs apron, taxiway, or runway during ground operations." In 1995, a mishap similar to this scenario occurred. The longitudinal and lateral controls were crossed, resulting in pitch inputs causing roll outputs. (28) The aircraft was unable to takeoff, and ran off the runway, killing the pilot.

The scenario generation process serves to help stimulate ideas when developing scenarios, resulting in more scenarios and coverage across the control structure. The rest of the scenarios are found in Appendix 2.

Once the scenarios are generated, safety constraints must be identified to prevent the scenario from occurring. These scenarios provide actionable information that can be implemented into the system design or operations/maintenance procedures.

The safety constraints for the scenarios shown above are as follows:

SC.V.2.1 Wiring must be designed to withstand the flight environment, and inspected before flight.

SC.V.2.2 The VMS must be programmed with limits at all flight conditions.

SC.V.2.3 The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations

SC.V.2.4 A secondary attitude indicator must be included in the UAV design as a backup to the main attitude indicator. The VMS must receive feedback of a vacuum pump failure so that it can switch to the secondary attitude feedback

SC.V.2.5 After any control surface related maintenance, a controls check must be accomplished. A controls check must also be accomplished during preflight. Consider different connectors for the different directions so that it cannot physically be connected backwards.

UAV STPA Summary

The STPA analysis on the UAV resulted in 211 scenarios and associated safety constraints for the operator, and 65 scenarios and safety constraints for the VMS for a total of 276 scenarios. Several of the safety constraints are applicable to more than one scenario. Many of the safety constraints are also already implemented in the program through operational procedures or design decisions. Constraints, along with their associated UCA and scenario, that may be of interest to the program. These scenarios are highlighted to illustrate coverage across design, testing, maintenance, and operations.

Design constraints:

V12. The VMS provides a reduced throttle setting too late after the UAV flares for landing.

Scenario V.12.3. The VMS provided the command late due to incorrect system feedback. The laser altimeter is malfunctioning and providing incorrect altitude data. The VMS believes the UAV is too high for a reduced throttle setting.

Safety Constraint SC.V.12.3. The UAV must be designed to detect laser altimeter malfunctions. The laser altimeter must be inspected regularly for proper function, and the exterior must be clean before flight.

V14. The VMS provides a throttle setting to decelerate to a target speed, but the throttle is not increased before reaching stall speed.

Scenario V.14.5. The VMS provided the command to increase the throttle once target airspeed was reached, however the throttle was not increased. The power system did not provide power to the actuator due to a power system failure.

Safety constraint SC.V.14.5. Flight critical components such as actuators must have backup power so that the aircraft may be landed after a power system failure.

The UAV program has experienced two mishaps associated with power loss. The first mishap was due to an alternator belt failure. The UAV was redesigned with two alternators to provide redundant power after the mishap. The second mishap was due to a wiring error. Both alternators were wired to a supply wire that connected to the VMS. The supply wire either broke, or had a loose connector which resulted in VMS power loss. The UAV has been since redesigned again to provide a supply wire from each alternator to the VMS, and the battery stores enough power for 5 hours of flight with only flight essential systems powered on. While this scenario doesn't directly discuss these specific design issues, it does cover ensuring that flight critical components are powered. As the detailed design is developed, the STPA analysis would also become more detailed and address these specific issues.

Testing constraints:

V6. The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is not brought back to neutral when the aircraft reaches the target heading/descent/ascent

Scenario V.6.2. The VMS provides a command to return the aileron, elevator, or rudder back to neutral, however the aeromodel is incorrect and the aircraft did not take as long as expected to reach the desired heading/descent/ascent.

Safety constraint SC.V.6.2. The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations.

The most recent UAV mishap was due to an engine failure after takeoff. The UAV was at an altitude that allowed the operator to turn the UAV back towards the airfield for a deadstick landing. The autopilot did not account for the lack of thrust and was commanding thrust (even though thrust commands had no effect). Deadstick flight was never tested, therefore the aeromodel was not validated. The UAV landed hard, resulting in repairable damage. Engine out aeromodelling was never validated because of the risk associated with the test. It is recommended that abnormal conditions are tested exactly because of the associated risk. It is much better to find out that the aeromodel is incorrect in controlled test conditions rather than a busy operational airfield where the potential to strike people and equipment is greater. It is not necessary to land the aircraft in an engine out condition. Rather, the test should occur higher altitudes so that the engine may be restarted before landing. If there are other abnormal conditions that were not validated it is recommended that the program validates those conditions.

C11. The operator does not provide altitude when the GPS waypoints are updated

Scenario C.11.4. The operator provides a new altitude assignment with the updated GPS waypoints. The altitude is not attained by the UAV, however because the additional alternators reduce max engine RPM, thus decreasing the service altitude of the UAV.

Safety constraint SC.C.11.4. Simulation and flight test must be accomplished to validate the limitations of the baseline aircraft or validate new limitations due to modifications

Maintenance constraints:

V6. The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is not brought back to neutral when the aircraft reaches the target heading/descent/ascent.

Scenario V.6.1. The VMS provides a command to return the aileron, elevator, or rudder back to neutral, however the command was not received due to a power system fault. Wiring or connections to the actuator are broken, keeping the actuator from receiving the signal. Or, a system power failure (such as an alternator failure) occurs, and the actuators are not on battery power.

Safety constraint SC.V.6.1 Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight. The power system must be designed such that a power system failure does not result in loss of actuator power

If a hazard is not controlled by design, it must be controlled through operations or maintenance procedures. Hence, any flight critical components such as wiring must be inspected before flight.

> **Scenario V.6.4.** The VMS provided a command to return the control surface actuator to neutral, however the control surface did not move as expected. The actuator linkage or cable is broken, and the aileron, elevator, or rudder is no longer controllable
> **Safety constraint SC.V.6.4.** Actuators and cable linkages must be inspected on a regular basis and during preflight inspections.

Operational constraints:

C1. The operator does not provide the GPS waypoints during prelaunch operations.

> **Scenario C.1.1.** The operator provides the GPS waypoints. A second UAV sortie is beginning at the same time, and the GPS waypoints are sent to the wrong UAV. The intended UAV does not receive the waypoints
> **Safety constraint SC.C.1.1.** Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct.

Current operations may not be of a high enough tempo that more than one aircraft is operated at a time, however considerations for higher tempo operations are important to identify in order to easily and safely scale up if it is required. The interference may also come from an aircraft or ground station undergoing maintenance checkouts or training, so those operations must also be accounted for. Additionally, other UAV programs using similar equipment may interfere with this UAV's operation. Currently, the operator verifies that they are linked to the correct UAV by using autopilot identification. Therefore, the program must also consider the possibility of maintenance replacing the autopilot, or switching it to another aircraft for troubleshooting, and not documenting it correctly.

C31. The operator provides engine start command when the engine fails in flight, but after the UAV is committed to landing.

> **Scenario C.31.3.** The engine quits because the operator does not switch fuel tanks, and the currently selected fuel tank is empty. The operator attempts to restart the engine, but is unsuccessful. During the landing sequence, the operator realizes the fuel feed error, switches tanks, and successfully restarts the engine. However, the UAV is too close to the ground, and the autopilot does not transition safely from engine off performance to engine on performance.
> **Safety constraint SC.C.31.3.** The operator must verify fuel state and switch tanks during engine failure emergency procedures if the UAV is above safe restart altitude. The UAV autopilot must be designed to transition smoothly between engine off and engine on performance.

In most general aviation aircraft that require the pilot to switch between tanks, engine out emergency procedures call for switching the fuel tank to ensure that fuel starvation was not a

cause of the engine failure. This UAV's manual does not have a such a step. It is recommended that the program investigates adding the step to their emergency checklist.

> **Scenario C.31.4.** The operator attempts to restart the engine, but the engine does not restart. The operator continues to attempt a restart as time permits, in accordance with the checklist. The UAV is flying far from the airfield, and the exact height above ground is not known. The operator continues to attempt restart and finally does restart the engine, but the UAV descended too low and impacts terrain
> **Safety constraint SC.C.31.4.** During mission planning, operators must determine minimum restart attempt altitudes for each leg of the route that is based on a safe pressure altitude, since exact altitude above ground may not be known. The laser altimeter must be on battery power for use to determine height above terrain.

The emergency procedures appear to assume that the operator will always be aware of the UAV's height above the ground in order to make a determination of whether to continue to restart the engine, or begin ditching/landing or aerodynamic termination procedures. However, when the UAV is over uneven terrain, such as hills or mountains, far away from the airfield that information might not always be readily available. Therefore, it is recommended that during mission planning the operators choose some minimum altitude where they will stop attempting a restart for each leg of the route. The altitude would be based on the highest obstacle within the particular leg.

C41. The operator does not provide lost link procedures during flight operations.

> **Scenario C.42.2** The operator does not believe that the lost link procedure needs to be updated because the procedure was recently updated per a regular schedule. However, terrain, weather, or conflicting traffic between the UAV and airfield have changed along the route since the schedule update. The operator does not provide the lost link procedures because it isn't time, yet.
> **Safety Constraint SC.42.2.** The lost link procedures must be updated based on route of travel and obstacles between the UAV and the airfield rather than timing. If timing remains the preferred method, consider continuing the route of flight to a point known to be free of obstacles and then return to the airfield – timing for lost link updates & timing for return to base doesn't work. One needs to be based on geography/obstacles.

The current procedures require the operator to update lost link procedures at regular time intervals. If the UAV is flying over uniformly low terrain for the entire flight with no other obstacles such as conflicting traffic or weather between the UAV and the airfield, time intervals may be appropriate. However, for any situation where terrain, traffic, and weather are considerations for lost link procedures it is not appropriate. Recommend reevaluating lost link flight planning procedures based on the safety constraint above.

A full list of the safety constraints is found in Appendix 2.

This UAV use case illustrates how STPA would be used during system design. The safety control structure does not contain all the details of a finished product, yet a significant of amount information was generated. Safety constraints covered areas such as maintenance, operations, design, and test. Were this program still in the design phase, the constraints would be incorporated in the system design, and test and operations planning. Once the next level of design detail is created, the STPA analysis is extended to include that detail. In Engineering a Safer World, Leveson refers to this process as safety guided design. (8) Figure 23 shows that design decisions feed into the hazard analysis, which in turn feeds back safety constraints to be implemented in the design.

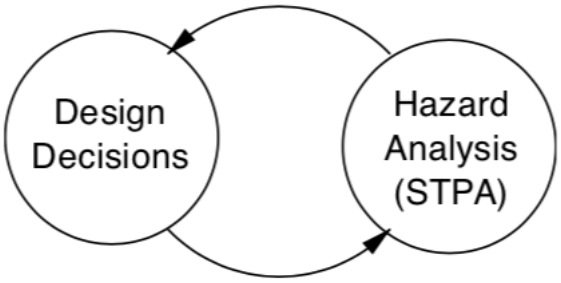


Figure 23 Safety-guided design (8)

The more tightly coupled this feedback loop is, the faster designers will identify safety constraints that must be incorporated in the design requiring less rework.

Conclusions

This thesis shows that STPA is not only useful, but that a more developed systems-based safety process is necessary to ensure that the systems provided to the warfighter are safe. A systems-based process ties the safety analysis together through the entire lifecycle of the system from concept development to operations. The process also not only informs the design of the physical system, but also of the entire system to include support and operations constructs.

If STPA is to have a meaningful impact on aircraft safety in the Air Force, it cannot simply be implemented on top of current safety processes. Program offices do not need more work, as they are very busy as it is. What they need is a cohesive systems-based safety strategy that promotes thoughtful system design and maintains safety throughout the lifecycle of the system.

Initial adoption may prove challenging. It may be difficult to convince AFLCMC to switch from current probabilistic assessments to STPA. Likely, STPA will initially be done in conjunction with current processes on a trial basis. In the short-term, this means more work for the PO that decides to try STPA. In the long-term, once the new approach to safety is proven, then workload will decrease. In fact, in comparisons with fault trees, FMEAs, and other traditional hazard analysis techniques, STPA has been found in every case to be orders of magnitude cheaper.

One method to introduce STPA to the acquisitions process is through airworthiness. The system safety process flows from airworthiness certification requirements. If the airworthiness office accepts STPA, system safety processes will adjust to match the new certification standard. In fact, the FAA is currently looking into allowing STPA to be used as an alternative method to the SAE ARP standards.

It is often thought that safety is at odds with design and program efficiency. However, this is not the case with STPA because it is a systems-based analysis. Not only is STPA cheaper to perform than current hazard analysis techniques, but using STPA during the design process will save system program offices time and money in rework that is discovered after the design process is complete during developmental testing.

Acronym Listing

AF – Air Force
AoA – Analysis of Alternatives
BLOS – Beyond Line of Sight
CAST – Causal Analysis based on STAMP
CDR – Critical Design Review
COTS – Commercial off the shelf
DT – Developmental Test
EBAO – Effects-Based Approach to Operations
EMD – Engineering, Manufacturing, and Development
FMEA – Failure Modes and Effects Analysis
FMECA – Failure Mode, Effects, and Criticality Analysis
FOC – Full Operational Capability
FTA – Fault Tree Analysis
GPS – Global Positioning System
HAZOP – Hazard and Operability Study
JSTARS – Joint Surveillance Target Attack Radar System
LOS – Line of Sight
LRIP – Low-Rate Initial Production
MAJCOM – Major Command
MEFR – Military Flight Release
MOCA – Minimum Obstacle Clearance Altitude
MRFR – Military Restricted Flight Release
MTC – Military Type Certificate
OT – Operational Test
O&S – Operations and Support
OT&E – Operational Test and Evaluation
PM – Program Manager
PO – Program Office
RFP – Request for Proposal
SE – Systems Engineering
SEP – System Engineering Plan
SRD – System Requirements Document
STAMP – Systems-Theoretic Accident Model and Processes
STPA – System Theoretic Process Analysis
TAA – Technical Airworthiness Authority
TEMP – Test Evaluation Master Plan
TO – Technical Order
UAV – Unmanned Aerial Vehicle
UCA – Unsafe Control Action
UI – User Interface
VMS – Vehicle Management System

VNE – Velocity Not to Exceed

Appendix 1: JSTARS STPA Analysis

Table 8 JSTARS Scenarios

UCA	Hazards	Number	Main Scenario Description	Safety Constraint
JSTARS does not provide target coordinates to support aircraft when the target needs to be engaged (H4)	H4	J.1.1	JSTARS provides target coordinates, but the support aircraft did not receive them. The communication was jammed by enemy forces	JSTARS must be able to overcome communications jamming by enemy forces
		J.1.2	JSTARS provides target coordinates, but the support aircraft did not receive them. The support aircraft does not have compatible communications capabilities	JSTARS must be designed to communicate with all potential support aircraft
		J.1.3	JSTARS does not provide target coordinates to the support aircraft because JSTARS does not believe the target needs to be engaged. The JSTARS believes either the enemy does not currently pose a threat to friendly forces.	JSTARS must be able to determine threats to friendly forces and provide target coordinates to support aircraft to prevent the enemy from engaging friendly ground troops
		J.1.4	JSTARS does not provide target coordinates to the support aircraft. The JSTARS does not know that the support aircraft has the appropriate munitions to engage the target	JSTARS must be provided weapons stores information for support aircraft in the area

		J.1.5	JSTARS does not provide target coordinates to the support aircraft. The JSTARS does not know that the support aircraft is in the area	JSTARS must be aware of support aircraft in the area
		J.1.6	JSTARS does not provide target coordinates to the support aircraft. JSTARS cannot detect the location of enemy forces	The JSTARS must be able to detect enemy forces and determine their location
		J.1.7	Ground troops requested that the target be engaged to the JSTARS controller coordinating with ground troops, but that message was not relayed to the controller coordinating with support aircraft	JSTARS must be designed to provide coordination between ground troops and support aircraft
		J.1.8	JSTARS provides target coordinates, but the support aircraft does not engage the enemy. The support aircraft detects enemy air defenses that the JSTARS does not, and decides not to engage	JSTARS must either detect all enemy air defenses, or receive air defense data from other sources. JSTARS must then provide target coordinates to the support aircraft outside enemy air defense capabilities
JSTARS provides target coordinates, but the coordinates are not where the enemy is located (H2, H3)	H2, H3	J.2.1	The JSTARS provided accurate target coordinates via a datalink to the support aircraft, however enemy forces were able to corrupt the transmission	The JSTARS datalinks must be secured from enemy disruption

		J.2.2	JSTARS provides coordinates, but they are not were the enemy is located. JSTARS is unable to differentiate between enemy forces, friendly forces, and civilians in the area.	JSTARS must either be able to differentiate between enemy, friendly, and civilians or use other sources to provide target differentiation
		J.2.3	The JSTARS sensor data is inaccurate, and the coordinates provided do not match the actual location of the enemy	JSTARS sensor data must be accurate in order to determine the location of the enemy
		J.2.4	The JSTARS provided coordinates of an area to avoid, due to presence of civilians or friendly forces, but the support aircraft believed these were target coordinates	JSTARS must be able to provide areas to avoid without those areas being misinterpreted as target coordinates
JSTARS provides target coordinates to support aircraft that are within contested airspace (H6)	H6	J.3.1	The target is located on the edge of enemy air defenses. JSTARS provides coordinates and a vector to the target that will avoid the defenses, however the vector is 180 degrees off, causing the support aircraft to travel through contested airspace	JSTARS must ensure that vectors to target coordinates are such that the support aircraft will not travel through contested airspace
		J.3.2	JSTARS provides target coordinates to support aircraft that are within contested airspace. JSTARS does not believe the radius of the air defenses is large enough to endanger support aircraft that engage the target	JSTARS must have accurate information regarding enemy capabilities

		J.3.3	JSTARS does not detect the enemy air defenses, and therefore does not recognize that the target coordinates are within contest airspace	JSTARS must either be able to detect enemy air defenses or be provided enemy air defense data prior to the operation
		J.3.4	The air defenses were supposed to be disrupted, however they were not. JSTARS did not receive feedback that efforts to destroy/disrupt the defenses were unsuccessful and provided target coordinates to the support aircraft that are within contested airspace	Feedback must be provided to the JSTARS if efforts to disrupt enemy air defenses are unsuccessful
JSTARS provides target coordinates before the enemy forces have separated from civilians (H3)	H3	J.4.1	JSTARS provides target coordinates to a support aircraft with instructions to wait until the civilians are no longer in proximity of the enemy forces. The communication is disrupted, and the instruction to delay was not received	JSTARS must have undisrupted communications with support aircraft
		J.4.2	JSTARS misinterprets the rules of engagement and believes that the collateral damage is acceptable and does not wait for the civilians to no longer be in proximity of enemy forces	JSTARS must understand the rules of engagement and must communicate questions regarding the rules to AOC if there are concerns regarding civilian safety
		J.4.3	JSTARS is not aware of civilian presence, and therefore does not know to wait until enemy and civilians are not longer in proximity	JSTARS must either be able to detect a civilian presence near enemy forces or be provided the data from other sources

		J.4.4	After JSTARS provides target coordinates civilians move into proximity with civilian forces. JSTARS does not have time to call off the attack	JSTARS must monitor area around enemy forces and be able to determine if civilians may move into the area (for instance, driving on a road in the direction of enemy forces)
		J.4.5	JSTARS provides target coordinates to a support aircraft, however that aircraft is unable to engage the target. The aircraft's wingman engages the target instead. The first aircraft had smaller munitions that would result in more localized damage, but the second aircraft had larger munitions with a larger effective radius that included the civilian position	If the original aircraft is unable to engage the target and a second aircraft is utilized, JSTARS must determine the suitability of the second aircraft's weapons before allowing the engagement to continue
JSTARS provides target coordinates after the enemy leaves the target location (H2, H3)	H2, H3	J.5.1	JSTARS provides target coordinates after the enemy leaves the target location. The JSTARS does not detect that the enemy has moved away from the target coordinates.	The JSTARS must be able to detect enemy forces and determine their location
		J.5.2	JSTARS provides target coordinates while the enemy is still in the location, however the support aircraft is delayed in engaging the target due to maintenance issues.	JSTARS must be able to track target and provide the support aircraft with updated coordinates as the target moves

JSTARS provides target coordinates to support aircraft after friendly forces have moved towards and engaged enemy forces (H2)	H2, H3	J.6.1	JSTARS provides target coordinates through datalink system. Due to the high volume of traffic across the links, the message was queued and receipt was delayed by the support aircraft	JSTARS must have capability to handle large amounts of communication traffic such that all messages are sent as soon as possible or prioritize high value information.
		J.6.2	JSTARS cannot detect the movement of friendly forces, and does not recognize that they are within close proximity of enemy forces	JSTARS must be able to track friendly forces
		J.6.3	JSTARS provides target coordinates before friendly forces have engaged the enemy, however the support aircraft is delayed in engaging the target due to maintenance issues	JSTARS must be informed of or able to track friendly positions and provide the support aircraft with updated instructions
JSTARS provides target coordinates to support aircraft after support aircraft expends weapons (H7)	H7	J.7.1	JSTARS does not receive feedback on weapons status of support aircraft, and does not realize that the support aircraft tasked to engage the enemy has expended weapons	JSTARS must receive feedback when support aircraft are out of weapons
		J.7.2	The support aircraft has some weapons onboard, but not weapons that are appropriate for the task. JSTARS does not receive feedback on type of weapons loaded on the aircraft	JSTARS must receive feedback indicating what type of weapons the support aircraft are carrying

JSTARS does not provide airspace deconfliction when support aircraft are co-altitude in the same airspace (H1)	H1	J.8.1	JSTARS provides deconfliction instructions to the support aircraft, however the communications are disrupted	JSTARS communications with support aircraft must be secure and not able to be disrupted
		J.8.2	JSTARS believes that even though the aircraft are co-altitude, they are horizontally deconflicted. However their orbits intersect	If aircraft are in holding patterns awaiting instructions, those patterns must not intersect. JSTARS must be designed to assist JSTARS controllers with deconfliction
		J.8.3	JSTARS does not receive feedback regarding the location and altitude of support aircraft	JSTARS must receive feedback regarding location and altitude of support aircraft in order to deconflict them
		J.8.4	JSTARS provides deconfliction instructions to separate the aircraft at different altitudes, however one of the aircraft has not switched from airfield altimeter setting to the current altimeter setting in theater and the aircraft are still co-altitude	JSTARS must provide a standard altimeter setting for all aircraft that are in the JSTARS area of responsibility
JSTARS provides support aircraft deconfliction instructions that create a conflict (H1)	H1	J.9.1	JSTARS provides deconfliction instructions that do not conflict with other traffic, however the support aircraft aircrew either mishear or misread the instructions and fly a different route than instructed that causes a conflict	JSTARS must require instruction feedback to ensure oral instructions are understood. If instructions are given via a datalink the JSTARS must be designed to provide the data such that it can be directly input into the support aircraft system

		J.9.2	JSTARS provides support aircraft deconfliction instructions to one aircraft that puts it in conflict with another aircraft. Aircrew on the JSTARS are responsible for controlling different support aircraft and have no way of deconflicting instructions	JSTARS must be designed so to ensure mission deconfliction among multiple JSTARS controllers for both air assets and ground assets
		J.9.3	JSTARS is not aware of all aircraft in the vicinity, and deconflicts support aircraft, but puts support aircraft in conflict with other aircraft	JSTARS must be aware of all aircraft in the area
		J.9.4	JSTARS provides deconfliction instructions that do not conflict with other traffic, however the support aircraft also receive instructions from other controllers such as AWACS or ground controllers and follow those instructions	JSTARS must be designed to operate with other controlling functions to prevent conflicting instructions to support aircraft
JSTARS provides airspace deconfliction when the route is too close to terrain (H5)	H5	J.10.1	JSTARS does not provide a route too close to terrain, but the support aircraft receives the route from another source.	JSTARS must be designed such that communication between JSTARS and support aircraft is secure.
		J.10.2	JSTARS is not provided with detailed terrain data, and does not realized that the route is too close to terrain	JSTARS must be designed to provide terrain data to controllers and warn controllers if a proposed route is too close to terrain

		J.10.3	JSTARS provides deconfliction instructions that are above the terrain, however the standard altimeter setting provided to the support aircraft was incorrect resulting in a lower altitude above ground than intended	JSTARS must provide a standard altimeter setting that is appropriate given the atmospheric conditions of the area at the time. The setting must be updated when conditions change
JSTARS provides airspace deconfliction when the new route is through contested airspace (H6)	H6	J.11.1	JSTARS does not provide a route through contested airspace, but the support aircraft receives the route from another source.	JSTARS must be designed such that communication between JSTARS and support aircraft is secure
		J.11.2	JSTARS does not detect the enemy air defenses, and therefore does not recognize that the new route is through contest airspace	JSTARS must either be able to detect enemy air defenses or be provided enemy air defense data prior to the operation
		J.11.3	JSTARS provides a route that is not through contested airspace, however the support aircraft's navigation is inaccurate or disrupted, causing the support aircraft to fly into contested airspace	JSTARS must either be able to detect the location of aircraft relative to contested airspace or be provided the information in order to correct the support aircraft's heading before it enters contested airspace
JSTARS provides aircraft deconfliction before support aircraft changes radio frequency to JSTARS frequency (H1)	H1	J.12.1	JSTARS instructed an aircraft to maintain an orbit near the entry point into the JSTARS controlled airspace. The incoming aircraft is being handed off to the JSTARS and switching frequencies when the deconfliction call is made	JSTARS must not instruct an aircraft to maintain an orbit near an identified entry point into the airspace.

		J.12.2	The combat operation is very busy, and JSTARS is overtasked. The JSTARS provides the deconfliction to the aircraft that just entered the airspace, but does not receive a response from the aircraft. Due to the high volume of radio calls, JSTARS does not realize they did not get a response from the aircraft	JSTARS must receive confirmation of instructions. The JSTARS must be designed to ensure safety-critical tasks such as airspace deconfliction are not overlooked
JSTARS provides aircraft deconfliction instructions after a midair collision (H1)	H1	J.13.1	JSTARS provides deconfliction instructions before the aircraft is involved in a midair, but communications were disrupted and the aircraft did not receive the instructions	JSTARS communications with support aircraft must be secure and not able to be disrupted
		J.13.2	JSTARS did not recognize that in order for a support aircraft to engage a target it would travel through another aircraft's orbit until the aircraft was in proximity of the other aircraft	JSTARS must be designed to assist the controllers with airspace deconfliction and warn controllers when one aircraft's route will intersect with another aircraft's route or orbit
		J.13.3	JSTARS provides aircraft deconfliction instructions to aircraft after it is involved in a midair collision. JSTARS does not receive timely positon reports from aircraft within the area of responsibility	JSTARS must receive real-time or near real-time feedback of support aircraft position and altitude
JSTARS provides partial aircraft deconfliction instructions (H1)	H1	J.14.1	JSTARS provides complete deconfliction instructions, however the communication is disrupted and the aircraft does not receive the entire procedure	JSTARS communications with support aircraft must be secure and not able to be disrupted

		J.14.2	JSTARS controllers are not aware of all aircraft within the airspace, and believe that just altitude or vectors are required to deconflict the aircraft, but both are actually needed due to multiple conflicting aircraft	JSTARS must be aware of all aircraft in the area
		J.14.3	JSTARS controllers provide complete aircraft deconfliction instructions, however the support aircraft only comply with part of the instructions. The support aircraft pilot is unable to comply with the entire procedure	JSTARS must be designed to provide controllers with aircraft location information so that if an aircraft does not follow deconfliction instructions the JSTARS controllers may correct the situation
JSTARS does not provide target coordinates to ground troops when a target needs to be engaged (H4)	H4	J.15.1	JSTARS provides the target coordinates to ground troops, however the communication is disrupted or the ground troops do not have interoperable communications capability	JSTARS must communicate with ground troops, and the communication must be secure and not able to be disrupted
		J.15.2	One JSTARS controller coordinates with ground troops and another coordinates with support aircraft. The ground troop controller believed that the support aircraft controller would have a support aircraft engage the target	JSTARS must be designed to provide communication and coordination between controllers
		J.15.3	JSTARS does not provide target coordinates to ground troops when a target needs to be engaged. The JSTARS does not receive ground troop request for target coordinates	JSTARS must be designed to receive ground troops requests

		J.15.4	JSTARS provides target coordinates to ground troops, but they do not engage the enemy. They do not have capability to engage the enemy at the current distance	JSTARS must be aware of ground troops capability
JSTARS provides target coordinates to ground troops, but they are not where the enemy is located (H2, H3)	H2, H3	J.16.1	JSTARS provides accurate target coordinates, but the communication is disrupted and the ground troops receive incorrect data	JSTARS communication must be secure and not able to be disrupted
		J.16.2	JSTARS detects personnel presence and determines the personnel are enemy forces, but misinterprets location data. JSTARS provides the information to ground forces, however the coordinates are incorrect	JSTARS must be designed to provide accurate coordinate information
		J.16.3	JSTARS sensors detect personnel presence and movement, but cannot determine whether they are civilians, enemy forces, or friendly forces	JSTARS must be able to determine if personnel present are civilians, enemies, or friendlies, or JSTARS must be provided that data from other sources
		J.16.4	JSTARS provides accurate target coordinates, but the ground troops misinterpret the coordinates and target a different location	JSTARS must be designed to provide target coordinates consistent with ground troop procedures and equipment so that they do not have to translate the data. JSTARS should be able to communicate directly with ground troop equipment.

JSTARS provides target coordinates after the enemy leaves the target location (H2, H3)	H2, H3	J.17.1	JSTARS provides the target coordinates to ground troops, however the communication is disrupted and delayed until after the enemy has moved	JSTARS communication must be secure and not able to be disrupted
		J.17.2	JSTARS does not detect enemy movement, either due to the sensor scan rate or sensitivity of sensor, and therefore believes that the original target location is still accurate	JSTARS sensors must be able to detect enemy movement
		J.17.3	JSTARS provides the target coordinates before the enemy leaves the target location, however the ground troops delay engagement of the enemy. JSTARS does not continue to monitor the enemy location due to other sensor requests and does not provide ground troops with updated information	JSTARS must be designed to be able to monitor known enemy locations while performing other sensor functions
JSTARS provides target coordinates to ground troops after friendly forces have moved towards and engaged enemy forces (H2)	H2	J.18.1	JSTARS provides target coordinates to ground troops before friendly troops have engaged enemy forces, however the communication is disrupted. JSTARS troubleshoots the problem and resends the coordinates, but by this time friendly forces have moved within close proximity of the enemy	JSTARS communication must be secure and not able to be disrupted. If communication is disrupted, JSTARS must have procedures in place to determine whether or not the commands are still appropriate once communications are reestablished

		J.18.2	JSTARS recognizes that friendly forces are moving towards the enemy forces in order to engage the enemy, but still provides target coordinates to the ground troops. JSTARS believes that the friendly forces are far enough away from the enemy to allow the ground troops to attack the enemy	JSTARS must be aware of ground ordnance radius and ensure friendly troops are not within that radius.
		J.18.3	JSTARS provides target coordinates to ground troops after friendly forces have engaged the enemy. The friendly forces do not provide feedback to either JSTARS or the ground troops in contact with JSTARS indicating they are in proximity of enemy forces	JSTARS must be designed to detect friendly forces in order to prevent providing target coordinates that result in friendly fire. In addition, procedures must be in place to ensure ground troops inform JSTARS of troop movements.

Appendix 2: UAV STPA Analysis

Table 9 UAV Operator Safety Constraints

UCA Designator	UCA	Hazards	Constraint
C1	The operator does not provide the GPS waypoints during prelaunch operations	H3	The operator must provide GPS waypoints during prelaunch operations
C2	The operator does not provide updated GPS waypoints when mission changes	H3	The operator must provide GPS waypoints during the mission when the mission changes
C3	The operator provides the GPS waypoints when they do not align with the mission	H3	The operator must not provide GPS waypoints that do not align with the mission
C4	The operator provides the GPS waypoints when they present a conflict with other aircraft	H2	The operator must not provide GPS waypoints that present a conflict with other aircraft

C5	The operator provides GPS waypoints and the route length exceeds the fuel on board	H4	The operator must not provide GPS waypoints for a route that exceeds the fuel on board
C6	The operator provides GPS waypoints that create a route outside of LOS radius and BLOS is not being used	H3, H4	The operator must not provide GPS waypoints that create a route outside LOS radius if BLOS is not being used
C7	The operator provides GPS waypoints after LOS is lost, but before BLOS radio link is established	H3, H4	The operator must provide waypoints while the UAV is in LOS
C8	The operator provides GPS waypoints after the UAV reaches bingo fuel	H4	The operator provide GPS waypoints to bring the UAV back to the airfield before the UAV reaches bingo fuel
C9	The operator provides GPS waypoints and the number of waypoints exceed the storage capacity of the autopilot	H3	The operator must not provide GPS waypoints for a route that exceeds the fuel on board
C10	The operator provides GPS waypoint, but the list of waypoints is not complete for the entire mission	H3	The operator must provide a complete set of GPS waypoints for the entire mission
C11	The operator does not provide altitude when the GPS waypoints are updated	H1, H2, H3	The operator must provide updated altitude assignments when the GPS waypoints are updated
C12	The operator provides altitude when the altitude, coupled with the programmed waypoints are not above minimum obstacle clearance altitude (MOCA)	H1	The operator must not provide altitudes that are below the MOCA
C13	The operator provides altitude when the altitude conflicts with other traffic's altitude blocks	H2	The operator most not provide altitude assignments that conflict with other aircraft
C14	The operator provides altitude when the altitude is above icing level and the UAV flies through clouds	H4	The operator must not provide an altitude above the icing level if the UAV flies through clouds

C15	The operator provides altitude after LOS is lost due to terrain masking, but before BLOS radio link is established	H3	The operator must provide an altitude assignment before LOS is lost
C16	The operator provides altitude when the altitude assignments exceed the number of GPS waypoints	H3	The operator must provide the same number of altitude assignments as waypoints
C17	The operator provides altitude when there are fewer altitude assignments than waypoints and it does not include the entire mission	H3	The operator must provide the same number of altitude assignments as waypoints
C18	The operator does not provide airspeed during a change in flight condition or environmental conditions	H1, H4, H6	The operator must provide airspeed during a change in flight phase or environment
C19	The operator provides airspeed when the airspeed provided is at or below stall speed	H4	The operator must not provide an airspeed below stall speed
C20	The operator provides airspeed when the airspeed is above VNE	H6	The operator must not provide an airspeed above VNE
C21	The operator provides airspeed when flight planning fuel duration was based on auto (max endurance) airspeed, but a higher airspeed is set	H3, H4	The operator must monitor the fuel state and not provide airspeed significantly different than the flight planned airspeed for substantial portions of the cruise phase
C22	The operator provides an airspeed value that will create a conflict with other aircraft	H2	The operator must not provide an airspeed value that conflicts with other aircraft
C23	The operator provides airspeed after the UAV stalled due to slow flight	H4	The operator must provide an airspeed above stall speed before the UAV departs controlled flight

C24	The operator provides airspeed after structural damage from flying above VNE	H6	The UAV airspeed must never exceed VNE. If there is an excursion above VNE, the operator must provide an airspeed below VNE as soon as possible and return to base.
C25	The operator provides airspeed when the number of airspeed assignments exceed the number of GPS waypoints	H3	The operator must provide the same number of airspeed assignments as waypoints
C26	The operator provides airspeed when the number of airspeed assignments are fewer than the number of GPS waypoints	H3	The operator must provide the same number of altitude assignments as waypoints
C27	The operator does not provide engine start during prelaunch engine run-up	H3	The operator must provide the engine start command during prelaunch engine run-up
C28	The operator does not provide engine start during before takeoff procedure	H3	The operator must provide engine start command during before takeoff procedure
C29	The operator does not provide engine start command when the engine fails in flight and the engine needs to be restarted	H4	The operator must provide engine start command when the engine fails in flight
C30	The operator provides the engine start command when ground personnel are near the propellers	H1	The operator must not provide the engine start command when ground personnel are near the propellers
C31	The operator provides engine start command when the engine fails in flight, but after the UAV is committed to landing	H1	The operator must not provide the engine start command when the engine fails if the UAV is committed to landing
C32	The operator does not provide the launch now command during takeoff	H3	The operator must provide the launch now command during takeoff
C33	The operator provides the launch now command when the runway is not clear	H2	The operator must not provide the launch now command if the runway is not clear

C34	The operator provides the launch now command when the UAV is not on the runway	H5	The operator must not provide the launch now command when the UAV is not on the runway
C35	The operator provides the launch now command before ground personnel have cleared the area	H1	The operator must not provide the launch now command before ground personnel have cleared the area
C36	The operator provides the launch now command after the UAV is airborne	H4	The operator must not provide the launch now command after the UAV is airborne
C37	The operator does not provide the land now command when the UAV is in the pattern and at minimum fuel	H4	The operator must provide the land now command when the UAV is above the airfield and at minimum fuel
C38	The operator does not provide the land now command when the UAV is at the airfield and other aircraft are attempting to enter the pattern	H2	The operator must provide the land now command when the UAV must provide the land now command when the UAV is in the pattern and other aircraft are attempting to enter the pattern
C39	The operator provides the land now command when the runway is not clear	H2	The operator must not provide the land now command when the runway is not clear
C40	The operator provides the land now command when the UAV is not at the airfield	H1	The operator must not provide the land now command when the UAV is not at the airfield
C41	The operator provides the land now command before the UAV completes the airfield arrival procedure	H1, H2	The operator must not provide the land now command before the UAV has completed the airfield arrival procedure
C42	The operator does not provide lost link procedures during flight operations	H1, H2	The operator must provide the lost link procedures during flight operations
C43	The operator provides lost link procedure, and the lost link procedure waypoints conflict with other aircraft	H2	The operator must not provide lost link procedures that are in conflict with other aircraft

C44	The operator provides lost link procedures, and the lost link procedure is not at or above MOCA	H1	The operator must not provide lost link procedures that are below the MOCA
C45	The operator provides lost link procedures before terrain, conflicting traffic, or weather necessitate a lost link procedure update	H1, H2	The operator must not provide updated lost link procedures before terrain and airspace changes necessitate the update
C46	The operator provides lost link procedures when the waypoints exceed the storage capacity of the autopilot	H1, H2	The operator must not provide lost link procedures that contain more waypoints than the storage capacity
C47	The VMS does not provide the payload power on command when UAV is over the target area	H3	The VMS must provide payload power on command when UAV is over the target area
C48	The VMS provides the payload power on command when the alternator fails	H4	The VMS must not provide power on command when there is not enough power for payload and VMS operation
C49	The VMS does not provide the payload power off command when the alternator fails	H4	The VMS must provide payload power off command when there is not enough power for both the payload and VMS
C50	The VMS provides the payload power off command when the UAV is over the target area	H3	The VMS must provide the power off command when the UAV is over the target area

Table 10 UAV VMS Safety Constraints

UCA Designator	UCA	Hazards	Constraint
V1	The VMS does not provide roll, pitch, or yaw commands when the UAV is off course	H1, H2, H3	The VMS must provide roll, pitch, or yaw commands to correct the UAV course when it is off course
V2	The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits	H4	The VMS must not provide roll, pitch, or yaw commands that exceed attitude limits

V3	The VMS provides roll, pitch, or yaw when the command steers the UAV off course	H1, H2, H3	The VMS must not provide roll, pitch, or yaw commands that steer the UAV off course
V4	The VMS provides the pitch down command when the throttle is reduced in order to descend, but the command is delayed	H4	The VMS must provide the pitch down command after the throttle is reduced for a descent before the UAV decelerates to stall speed
V5	The VMS provides a pitch up command when the throttle is increased for a climb, but the command is delayed	H6	The VMS must provide the pitch up command after the throttle is increased for a climb before the UAV accelerates to VNE
V6	The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is not brought back to neutral when the aircraft reaches the target heading/descent/ascent	H1, H2, H3	The VMS must provide a roll, pitch, or yaw command to return to neutral such that the aircraft attains the target attitude
V7	The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is not brought back to neutral before the UAV reaches the target heading/descent/ascent	H1, H2, H3	The VMS must provide a roll, pitch, or yaw command to return to neutral such that the aircraft attains the target attitude
V8	The VMS does not provide a throttle setting command when environmental conditions change	H4, H6	The VMS must provide a throttle setting when the environmental conditions change
V9	The VMS does not provide a higher throttle setting when the UAV is in a sustained turn, which reduces lift	H1, H2	The VMS must provide a higher throttle setting during sustained turns to maintain target altitude
V10	The VMS provides a throttle setting, but the throttle setting is not enough to maintain an airspeed above stall speed	H4	The VMS must provide a throttle setting high enough to maintain an airspeed above stall speed
V11	The VMS provides a throttle setting that accelerates the aircraft above VNE	H6	The VMS must provide a throttle setting low enough to maintain an airspeed below VNE

V12	The VMS provides a reduced throttle setting too late after the UAV flares for landing	H1, H5	The VMS must not provide a reduced throttle setting too late after the UAV flares for landing
V13	The VMS provides a throttle setting to accelerate to a target speed, but the throttle is not reduced before reaching VNE	H6	The VMS must reduce the throttle setting before reaching VNE during an acceleration
V14	The VMS provides a throttle setting to decelerate to a target speed, but the throttle is not increased before reaching stall speed	H4	The VMS must increase the throttle setting before reaching stall speed when decelerating

Table 11 UAV Operator Scenarios

UCA	Hazard	Number	Main Scenario Description	Safety Constraint
The operator does not provide the GPS waypoints during prelaunch operations	H3	C.1.1	The operator provides the GPS waypoints. A second UAV sortie is beginning at the same time, and the GPS waypoints are sent to the wrong UAV. The intended UAV does not receive the waypoints	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct
		C.1.2	The operator provides the GPS waypoints to the UAV. A signal interferes with the command, and the UAV does not receive it.	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.
		C.1.3	The operator does not send the GPS waypoints even though they are need to carry out the sortie. The operator is told that a new customer route request is forthcoming, and the operator decides to wait for the waypoints and continue on with the preflight. The operator forgets that the GPS waypoints were never provided to the UAV after the preflight is complete.	The operator must either delay the sortie if new customer requirements are expected, or provide the current GPS waypoints with a plan to update them once the new request is provided
		C.1.4	The operator does not send the GPS coordinates. The operator receives warnings from the UAV indicating there is a problem. The warnings are inaccurate, and the systems are operating correctly, but the operator stops prelaunch operations to troubleshoot the problem.	The UAV must not provide nuisance warnings

	H2	C.1.5	The operator sends the GPS waypoints to the UAV. They were not saved by the autopilot, and older waypoints already loaded were not overwritten.	The autopilot must save the GPS waypoints received by the UAV
The operator does not provide updated GPS waypoints when mission changes	H3	C.2.1	The operator provides the GPS waypoints, but the UAV does not receive the waypoints due to interference along the route of flight	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.
		C.2.2	The operator receives accurate fuel state feedback, but incorrectly believes the fuel state of the UAV will not allow for the new route because the operator miscalculated the current UAV fuel duration or miscalculated the duration of the updated route. The operator does not provide the GPS waypoints to the UAV to avoid running out of fuel.	The operator must be able to quickly and accurately calculate fuel duration and route duration to make the correct determination for route changes inflight
	H2	C.2.3	The customer request for a route change during the sortie was not brought to the operator at the ground station. The request was delivered to the operator's unit, which is not collocated with the ground station. The operator does not provide the GPS waypoints to the UAV because the operator is unaware of the mission change	Customer change requests during the mission must be delivered as quickly as possible. Consider having the change requests delivered directly to the ground station
	H2	C.2.4	The operator sends the GPS waypoints to the UAV. They were not saved by the autopilot, and older	The autopilot must save the GPS waypoints received by the UAV

			waypoints already loaded were not overwritten.	
The operator provides the GPS waypoints when they do not align with the mission	H3	C.3.1	The operator does not provide GPS waypoints. The step is accidentally skipped during preflight. GPS waypoints from the last sortie are stored in the memory and the UAV uses those	The GPS waypoints stored in the autopilot must be verified with the mission plan
	H2	C3.2	The operator sends the GPS waypoints to the UAV however they do not align with the mission. During mission planning the requested route was changed, however that information did not make it to the mission planners.	Customer change requests during the mission must be delivered as quickly as possible to mission planners
	H2	C.3.3	The operator sends the GPS waypoints to the UAV however they do not align with the mission. The mission planners copy an old mission plan and update it, however they miss the waypoint updates	The operator must verify the mission plan with the customer request
	H1, H2, H3	C.3.4	The operator provided coordinates that aligned with the mission, but a BLOS operator doing a ground station checkout accidentally linked with the UAV and sent new coordinates. These coordinates overrode the previous coordinates and did not align with the mission	Ground station checks must be either deconflicted with the UAV flying schedule, or be conducted with radios off to avoid transmitting commands
	H1, H2, H3	C.3.5	The operator provided GPS waypoints that aligned with the mission, however the UAV did not fly the waypoints. The GPS solution along the route is such that the navigation is not accurate	The operator must receive feedback when the accuracy of the GPS solution is below a minimum threshold, additionally other navigation solutions

				such as INS or VOR should be considered as a backup system
The operator provides the GPS waypoints when they present a conflict with other aircraft	H2	C.4.1	The operator provides GPS waypoints that do not conflict with other traffic, but there is interference along the route. The waypoints are not received by the UAV, and autopilot uses waypoints from the previous sortie, which conflict with present traffic	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.
	H3	C.4.2	The operator provides waypoints to the UAV. The operator or mission planners used an old flight plan as a template for the current mission, but did not copy over all the data., The waypoints do not match the approved route from the airspace traffic operator (ATC).	The operator must verify the mission plan with the customer request and approve ATC route
		C.4.3	The operator provides waypoints which do not conflict with air traffic, but the waypoints are far apart from each other, and travel between the waypoints do present a conflict with other aircraft	Waypoints must be sufficiently close together to control the behavior of the UAV and prevent it from conflicting with other traffic
		C.4.4	The operator provides waypoints which do not conflict with the air traffic as reported by the air traffic operator, however the air traffic changes after planning or during the sortie. The operator does not receive the updated information in order	The operator must be provided with and air traffic changes to ensure the UAV is properly deconflicting from other traffic

			to provide a different set of waypoints	
		C.4.5	The operator sends the GPS waypoints to the UAV. They were not saved by the autopilot, and older waypoints already loaded were not overwritten.	The autopilot must save the GPS waypoints received by the UAV
The operator provides GPS waypoints and the route length exceeds the fuel on board	H4	C.5.1	The operator does not provide GPS waypoints. The step is accidentally skipped during preflight. GPS waypoints from the last sortie are stored in the memory and the UAV uses those. The previous sortie was longer, and the UAV was fueled with more fuel.	The GPS waypoints stored in the autopilot must be verified with the mission plan
		C.5.2	The operator provides the GPS waypoints and the route length exceeds the fuel on board. The operator fat fingered a GPS waypoint resulting in the UAV flying further from the airfield than anticipated. The error was not discovered until the UAV traveled significantly off course and no longer had the fuel to return to the airfield	The GPS waypoints stored in the autopilot must be verified with the mission plan
		C.5.3	The operator provides GPS waypoints to create a route based on a larger than standard takeoff fuel weight of the aircraft, however ground personnel fueled the aircraft the standard amount.	The operator must provide nonstandard fuel requests to the ground personnel, and ground personnel must document the fuel status of the aircraft for

			There was not enough fuel to complete the sortie.	the operator to verify during preflight
		C.5.4	The operator provided the GPS waypoints and believed based on the reported fuel state that the UAV that the sortie duration was appropriate, however the fuel state feedback was incorrect due to fuel system modifications	The UAV must provide accurate fuel state feedback to the operator
		C.5.5	The operator provided the GPS waypoints based on the expected fuel consumption, however, the fuel consumption was higher than expected. The operator monitors the fuel consumption and recognizes that that the duration of the sortie will be longer than fuel duration and provides a new set of waypoints, but the fuel state is too low to make it back to the airfield	The operator must have joker and bingo fuel states that can be adjusted if the fuel is consumed faster than expected to ensure the aircraft can return to the airfield before running out of fuel
The operator provides GPS waypoints that create a route outside of LOS radius and BLOS is not being used	H3, H4	C.6.1	The operator sent GPS waypoints, however the waypoints were not received due to interference and the UAV used previously stored waypoints for a BLOS sortie	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.

		C.6.2	The operator sent GPS waypoints that are within the LOS radio radius, however terrain between the antenna and the aircraft masks the signal. The operator did not recognize that areas of high terrain in the area could mask the signal, LOS is lost	UAV operators using an LOS ground station must research potential terrain masking areas in the area of operations and flight plan accordingly
		C.6.3	The operator provides GPS waypoints that are known to be outside LOS, but believed that radio signal repeaters would carry the signal to the UAV beyond ground station LOS. The repeaters are not functioning, and the status of the repeaters was not verified during preflight operations. Once the UAV was outside of the ground station's LOS radius, it lost the link	UAV operators using LOS ground stations and repeaters must include repeaters status during preflight checks
		C.6.4	The operator provides GPS waypoints within LOS radius. The lost link procedures were not updated from a previous BLOS sortie, and lost link occurs resulting in the aircraft to departing the LOS radius.	Lost link procedures must be updated prior to every flight
The operator provides GPS waypoints after LOS is lost, but before BLOS radio link is established	H3, H4	C.7.1	The GPS waypoints were provided by the operator after LOS is lost, but before BLOS radio link is established. The operator provided GPS waypoints just before the LOS transition to BLOS near the LOS radius limit, however the limit was less than expected due to terrain, atmospherics, or other effects and the LOS was lost before the BLOS transition.	LOS/BLOS transition must occur well within LOS radius to ensure the transition occurs before the UAV loses communication with the LOS ground station.

	H2	C.7.2	The operator provides the GPS waypoints late outside of the LOS radius, but has not completed BLOS transition. Heavier traffic than normal causes several changes to the departure procedures for the UAV, and the operator gets behind creating the new flight plan and uploading it to the UI. BY the time the new flight plan is ready for upload, the UAV is outside the LOS radius.	The UI must provide feedback to the LOS operator when the UAV is near the LOS radius limit if BLOS has not yet been established. The operator must have established procedures with ATC to keep the UAV in the LOS radius of BLOS is not established as planned
		C.7.3	The operator does not recognize that LOS was lost, and believes the UI still has a link to the UAV. The operator provides waypoints, but they are not received due to the lost link.	The UI must provide feedback to the operator when the link is lost.
	H1, H2, H3	C.7.4	The operator provides GPS waypoints to the UAV, however the UAV does not fly the waypoints provided. Significant winds push the UAV off course, and the UAV does not adjust the heading to maintain the correct ground track	The UAV must adjust the target heading to account for winds to maintain a safe ground track.
The operator provides GPS waypoints after the UAV reaches bingo fuel	H4	C.8.1	The operator provides GPS waypoints to update the route after the UAV reaches bingo fuel. The operator recognizes that the UAV is nearing bingo fuel, and provides GPS coordinates, but lost link occurs and the UAV does not receive the coordinates. Per lost link procedures, the UAV continues to fly the last route provided. When the link is reestablished, the operator provides waypoints to return	The operator must not wait until bingo to replan the flight. Once the UAV reaches joker, replanning must begin

			to the airfield, but the UAV is past bingo and no longer has enough fuel to return.	
		C.8.2	The operator provides GPS waypoints after the UAV reaches bingo fuel. The operator believed based on the fuel state and distance that the UAV could make it back to the airfield with less fuel than bingo. However, headwinds cause the return trip to take longer than expected	The operator must consider winds when conducting flight planning
		C.8.3	The operator provides GPS waypoints after the UAV reaches bingo fuel. The operator did not recognize that the fuel state was at bingo until reviewing the fuel state at the regular status check. The operator immediately provides GPS coordinates to return to the airfield, but the UAV no longer has enough fuel to return home.	The operator must enter joker and bingo fuel states in the UI, and the UI must alert the operator when the UAV is at joker and bingo
		C.8.4	The operator provides GPS waypoints to return home before the UAV reached bingo, however the waypoints were not saved in the autopilot, and the UAV continued to travel on the original route. By the time the operator recognized that the UAV was not returning to the airfield, the UAV was past bingo and did not have enough fuel to return home.	The GPS waypoints stored in the autopilot must be verified with the mission plan

The operator provides GPS waypoints and the number of waypoints exceed the storage capacity of the autopilot	H3	C.9.1	The operator provides waypoints that were within the storage capacity of the autopilot. The message received by the UAV is delimited incorrectly due to translation from the UI to the radios to the UAV, which exceeds storage capacity	The ground station radios must send commands accurately
		C.9.2	The operator provides a large number of waypoints to ensure that the UAV flies a route that aligns with the mission, however the operator uses too many waypoints that exceeded the storage	The operator must send a number of waypoints that are less than the autopilot storage. The autopilot storage must be large enough to store enough waypoints for the length of mission
		C.9.3	The operator provides the waypoints, but does not receive feedback that the waypoints were received, so the operator provides the waypoints again. The second set of waypoints are concatenated rather than replacing the first set of waypoints	The UAV must provide feedback that the waypoints were received, and the autopilot must replace old waypoints with new waypoints
	H1, H2	C.9.4	The operator provides waypoints that were within the storage capacity of the autopilot, but the waypoints are delimited incorrectly taking up more storage space than the autopilot's capacity	The UAV must save provided waypoints into the autopilot accurately
The operator provides GPS waypoint, but the list of waypoints is not complete for the entire mission	H3	C.10.1	The operator provided a complete set of GPS waypoints, however the transmission was cut short due to a ground station radio power failure, and the UAV did not receive the entire set of waypoints.	The ground station and associated equipment must be connected to emergency power, and the ground station power must transition without delay to emergency power if the main power supply is cut

		C.10.2	The operator provides an incomplete set of waypoints that did not include the entire mission. The operator does not translate the flight plan completely into the UI due to distraction or other factors during the preflight preparations. The operator does not verify the waypoints after entering them, so the error was not caught	The GPS waypoints stored in the autopilot must be verified with the mission plan
		C.10.3	The operator provides an incomplete set of waypoints that did not include the entire mission. The customer request was incomplete, and the customer is not required to approve the mission plan, therefore the incomplete plan was not caught	The customer must provide a complete request to the operator, and must review the plan to ensure it aligns with the mission
		C.10.4	The operator provides a complete set of waypoints, however the autopilot did not save all of the waypoints.	The GPS waypoints stored in the autopilot must be verified with the mission plan
The operator does not provide altitude when the GPS waypoints are updated	H1, H2, H3	C.11.1	The operator provides the altitude after assigning new GPS waypoints, but the UAV begins a turn to the next waypoint causing aircraft masking and the altitudes are not received by the aircraft.	The operator must ensure that altitude commands are accepted, monitor altitude, and correct altitude as needed
		C.11.2	The operator believes that the previously assigned altitudes would be safe with the new GPS coordinates. The operator misreads the sectional, and the previous altitudes are not above MOCA.	The UI must be programmed to include terrain data (at least highest obstacle in each section), and provide feedback if the UAV will fly below MOCA

		C.11.3	The operator receives an air traffic briefing and believes that the previously assigned altitude will be deconflicted from other air traffic. The air traffic briefing is outdated, and there are now air traffic conflicts with the previously assigned altitude.	The operator must confirm with ATC that the altitude block is deconflicted if GPS waypoints are updated
		C.11.4	The operator provides a new altitude assignment with the updated GPS waypoints. The altitude is not attained by the UAV, however because the additional alternators reduce max engine RPM, thus decreasing the service altitude of the UAV.	Simulation and flight test must be accomplished to validate the limitations of the baseline aircraft or validate new limitations due to modifications
The operator provides altitude when the altitude, coupled with the programmed waypoints are not above minimum obstacle clearance altitude (MOCA)	H1	C.12.1	The operator provides an altitude above the MOCA as the UAV flies towards mountainous terrain, however the link is lost due to terrain or aircraft masking during maneuvering and the UAV does not receive the altitude assignment	The operator must provide safe altitude as part of the entire flight plan such that if lost link occurs the UAV will not collide with terrain
		C.12.2	The operator misreads the sectional charts and provides an altitude that the operator believes is above MOCA, but it is actually not	The UI must be programmed to include terrain data (at least highest obstacle in each section), and provide feedback if the UAV will fly below MOCA

		C.12.3	The operator receives incorrect or outdated sectional charts, and assigned an altitude that was above the MOCA on the chart but there are obstacles higher than listed on the chart	The operator must ensure charts are updated during mission planning and obtain updated information prior to flight
		C.12.4	The operator provides an altitude above the MOCA, however the region of flight has a significantly different pressure compared to the field, and the UAV is flying an altitude lower relative to the ground	The operator must receive ambient pressure reports throughout the route of flight and update the altimeter as appropriate
The operator provides altitude when the altitude conflicts with other traffic's altitude blocks	H2	C.13.1	The operator provides an altitude that deconflicts with traffic, however the command is not received due to masking	The operator must ensure that altitude commands are accepted, monitor altitude, and correct altitude as needed
		C.13.2	The operator believes that the traffic will no longer be in conflict by the time the UAV arrives at that waypoint, however the conflicting traffic stays in the airspace for longer than expected	The operator must request updated information as the UAV progresses through route of flight to ensure traffic deconfliction
		C.13.3	The operator receives information that conflicting traffic is at a particular altitude, so the operator climbs or descends to deconflict. The traffic has an altitude block within which it can maneuver, and while the UAV is above or below the current position, it is not outside the maneuvering block	The operator must confirm the assigned altitude is outside of the altitude block of conflicting aircraft

		C.13.4	The operator provides an altitude that is deconflicted, however the pitot-static system is partially blocked resulting in the aircraft flying a different altitude than assigned	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
The operator provides altitude when the altitude is above icing level and the UAV flies through clouds	H4	C.14.1	The operator recognizes by viewing the onboard camera that the UAV is heading towards a cloud and provides a change in altitude to stay below the clouds and icing level, but the message is not received due to interference or masking	The operator must monitor altitude to make sure commands are accepted and reattempt command as needed
		C.14.2	The operator knows that there are icing conditions forecasted and knows the icing level, but assigns an altitude above the icing level anyway to avoid terrain. The operator believes that by using the camera the operator can avoid the clouds and therefore not fly through icing conditions, however the clouds are too thick along the route, and the operator cannot stay out of the clouds	The operator must fly below the icing level as terrain permits and consider returning to the airfield if the clouds are too thick to fly at altitude
		C.14.3	The operator is aware of the icing forecast, but intends to stay out of the clouds, however the onboard camera fails and the operator can no longer detect whether or not the UAV is flying through clouds	If the weather is such that camera use is required for safety, and the camera fails, the UAV must return to the airfield or another closer airfield below the icing layer if terrain permits

		C.14.4	The icing forecast was incorrect, and the icing level was lower than predicted, so the operator intended to stay below the level, but in fact was above the level. The clouds are not very thick, so they are hard to see to avoid	The UAV operator must monitor indications of icing anytime icing conditions are possible, and remove the UAV out of the conditions as soon as they are detected
		C.14.5	The operator provided altitudes that were below the icing level, however the UAV flew above the icing level. The operator provided the correct altitudes and the UAV properly stored them, however the pitot static system failed resulting in inaccurate information sent to the VMS and the UAV different altitudes than planned	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
The operator provides altitude after LOS is lost due to terrain masking, but before BLOS radio link is established	H3	C.15.1	The departure route includes travel over a rising terrain that masks the ground station antenna signal. The operator recognized that the terrain would mask the signal causing the UAV to lose LOS link earlier than normal and provided a higher altitude command, but the link was lost before the command was received.	Terrain masking from the LOS ground station must be identified during site planning and incorporated in flight planning for each sortie
		C.15.2	The operator recognizes that the UAV flight path will put terrain between the ground station and the UAV, but provides an altitude per the normal climb procedures. The operator believes that the terrain is not high enough to mask the signal. The UAV loses the link and does not	Terrain masking from the LOS ground station must be identified during site planning and incorporated in flight planning for each sortie

			receive the command to continue the climb.	
		C.15.3	Heavier traffic caused ATC to provide the operator with an abnormal departure route. The operator does not recognize that the new route has rising terrain that would mask the LOS signal, and the operator sent the climb altitude at the normal time, but the LOS link was lost.	The UAV must provide altitude feedback relative to ground for takeoff/climb and landing flight phases
	H1	C.15.4	The operator recognizes the rising terrain and provides an altitude to ensure that the terrain does not mask the LOS signal until the BLOS transition. However, the UAV does not fly the assigned altitude. The altimeter was not set to airfield altitude, and the UAV flies lower than it should.	The altimeter must be set to the airfield altitude during preflight and verified before launch.
The operator provides altitude when the altitude assignments exceed the number of GPS waypoints	H3	C.16.1	The operator provides more altitude assignments than GPS waypoints. The initial message containing altitude assignments was cut off due to lost link. The operator resends the altitude assignments, but rather than replace the incomplete message, the second message is added onto it.	The autopilot must replace previously provided altitudes with the most recently provided altitudes.

		C.16.2	During mission planning the operator creates too many altitude assignments, and does not realize that there are more altitude assignments than waypoint assignments.	The mission planning process must provide feedback to the operator when number of waypoints and altitude assignments do not match
		C.16.3	The operator accidentally inputs one (or more) altitudes twice into the UI. The UI does not provide feedback to indicate that the number of altitude assignments is different from the number of waypoint assignments. The UI assigns an incorrect altitude for each of the subsequent waypoints after the duplication, and never assigns the altitudes that do not have a corresponding waypoint.	The UI must provide feedback when the number of altitude and waypoints do not match.
	H1, H2	C.16.4	The operator provides the same number of altitudes as waypoints, but the UAV does not fly the altitudes matched with each waypoint. The altimeter is incorrect, and the UAV does not fly the assigned altitude.	The altimeter must be set in flight based on atmospheric conditions reported by ATC.
The operator provides altitude when there are fewer altitude assignments than waypoints and it does not include the entire mission	H3	C.17.1	The operator provides the same number of altitude assignments as waypoints, but the message is cut off due to lost link.	If lost link occurs after the operator provides a command, the operator must resend the command when the link is established to ensure that command was received

		C.17.2	The operator provides the same number of altitude assignments as waypoints, but there are too many waypoints, and not all the altitude assignments are not saved because the autopilot runs out of storage capacity.	The operator must know how many waypoints and associated altitude and airspeed assignments the autopilot can store and provide less than that amount. Additionally, the autopilot must be able to store enough data for the operator to provide the entire flight plan
		C.17.3	The operator misses an airspeed when inputting the altitudes from the mission plan into the UI. The UI does not provide feedback to indicate that the number of altitude assignments is different from the number of waypoint assignments. The UI assumes that the last altitude assignment in the list is the altitude assignment for the remainder of the flight.	The mission planning process must provide feedback to the operator when number of waypoints and altitude assignments do not match
	H1, H2	C.17.4	The operator provides the same number of altitudes as waypoints, but the UAV does not fly the altitudes matched with each waypoint. The altimeter is incorrect, and the UAV does not fly the assigned altitude.	The altimeter must be set in flight based on atmospheric conditions reported by ATC.
The operator does not provide airspeed during a change in flight condition or environmental conditions	H1, H4, H6	C.18.1	The operator provides the airspeed, but it is not received due to interference with nearby UAV operations.	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.

		C.18.2	The operator does not provide the airspeed command because the operator believes that the current airspeed is appropriate for the new situation. The operator is near an airspeed limit, and the new conditions reduce the limit such that the UAV has exceeded airspeed limits	The operator must know the effects of flight conditions on the airspeed limits and adjust airspeed when commanding a climb or descent as appropriate
		C.18.3	The operator does not recognize the change in flight condition. The UAV is programmed to automatically descent and climb per the flight plan, and the UAV operator does not receive feedback that the climb or descent will cause the UAV to exceed airspeed limits.	The UI must provide feedback when climbing or descending, and provide feedback if currently assigned airspeed will violate a limit at the new altitude
		C.18.4	The operator does not recognize the change in environmental conditions. Gusts cause the UAV to exceed airspeed limits, however the operator does not receive adequate feedback to realize that the UAV is in gusty conditions.	The UAV must be able to detect gusty conditions and provide feedback to the operator.
		C.18.5	The operator provides an airspeed appropriate for gusty, turbulent conditions, however the conditions are variable with various gust speeds and direction. The UAV receives variable airspeed feedback from the pitot static system due to the winds, and is constantly providing throttle settings to maintain the provided airspeed. The UAV's reaction to changes in airspeed cause	When flying in gusty, turbulent conditions the UAV must not 'chase' the provided airspeed so aggressively that it exceeds an airspeed limit.

			the UAV to exceed airspeed limits.	
The operator provides airspeed that is at or below stall speed	H4	C.19.1	The operator provided an airspeed above stall speed, but the UAV did not receive the command. The UAV is on final approach when the operator has to abort the landing due to an obstruction on the airfield. The operator immediately provides a command to level off at the current altitude. The UAV throttle setting is low, and the operator sends a command to increase airspeed, however the command is not received due to masking at the low altitude	The UI must be designed with an abort procedure that sends altitude and airspeed commands simultaneously. Additionally, the ground station and associated antennas must be located such that they have clear LOS to the UAV during landing and takeoff phases
		C.19.2	The operator provides a slow airspeed above stall to maintain a slow ground track in an orbit around the target area. The initial portion of the orbit has a significant headwind, but when the UAV turns the headwind becomes a tailwind reducing airspeed below stall speed	The operator must account for headwinds during slow flight and adjust the airspeed accordingly

		C.19.3	The operator provides an airspeed below stall speed by accidentally inputting the wrong numbers (fat fingering). There was no feedback that the airspeed the operator input into the UI was out of limits, and the incorrect airspeed was sent to the UAV	The UI must provide feedback to the operator if the operator enters a command that is outside of UAV limits
		C.19.4	The operator provides airspeed that higher than stall speed, but the engine fails in flight. The operator does not immediately recognize the state of the UAV, and the UAV autopilot is programmed to maintain altitude, such that airspeed bleeds off below stall speed.	The UAV must provide engine indicators to the operator, and the UI must be programmed to alert the operator when the engine is not functioning properly or has failed
		C.19.5	The operator provides an airspeed above stall speed, however the pitot-static system malfunctions, and the actual airspeed decreases. The operator recognizes that the UAV is decelerating based on the ground track and expected waypoint timing, but cannot intervene by directly commanding a throttle setting.	The operator must have the ability to directly command a throttle setting
The operator provides airspeed that is above VNE	H6	C.20.1	The operator commands an airspeed near VNE, and the UAV enters airspace with gusty wind conditions. The operator recognizes that the airspeed should be reduced to ensure that the airspeed does not exceed VNE. The operator commands a lower airspeed, but the command is not received due to masking or interference.	The operator must not command airspeed near VNE if gusty conditions are forecasted or expected.

		C.20.2	The operator provides an airspeed that is just below VNE, however the wind conditions are variable with significant gusts. A wind gust causes the airspeed exceed VNE	In gusty conditions, the operator must assign an airspeed far enough below VNE that the winds will not cause the UAV to exceed VNE
		C.20.3	The operator provided an airspeed that is within limits at lower altitudes, but the UAV then climbs and violates the airspeed limit.	The UI must be programmed to identify changes in limits based on flight conditions and alert the operator.
		C.20.4	The operator provides an airspeed above VNE by accidentally inputting the wrong numbers (fat fingering). There was no feedback that the airspeed the operator input into the UI was out of limits, and the airspeed is sent to the UAV	The UI must provide feedback when the operator provides an airspeed outside of the limits.
		C.20.5	The operator provides an airspeed below VNE, however the pitot-static system malfunctions, and the autopilot commands a higher throttle setting to maintain the airspeed, causing the UAV to exceed VNE	The UAV autopilot must have a secondary method of measuring airspeed in case of a pitot-static system failure, such as GPS
The operator provides airspeed when flight planning fuel duration was based on auto (max endurance) airspeed, but a higher airspeed is set	H3, H4	C.21.1	The operator commands a higher airspeed for a fixed duration that will get the UAV to the target area faster. After the duration the operator provides an airspeed to auto (max endurance) command, however it is not received by the UAV due to interference or masking	The operator must command a return to max endurance airspeed early enough that if the command is not received immediately the UAV will still have enough fuel endurance to complete the sortie

		C.21.2	The operator provides a cruise airspeed higher than max endurance, which was the flight planning airspeed. The UAV took off late, and the operator wants to make up time by cruising at a faster airspeed to get back on the original flight plan. The operator believes there is enough fuel in the UAV to fly the route with a higher airspeed (and therefore higher fuel flow), but does not do the calculations to verify.	The operator must verify with new flight plan calculations if the airspeed will differ significantly from max endurance airspeed
		C.21.3	The operator provides a cruise airspeed higher than max endurance, which was the flight planning airspeed. The UAV took off late, and the operator wants to make up time by cruising at a faster airspeed to get back on the original flight plan. The operator uses the fuel flow rate feedback provided by the UAV to calculate the endurance of the UAV at the higher cruise altitude, however the fuel flow rate is inaccurate	The UAV flight manual must include fuel consumption charts for the operator to calculate UAV endurance
		C.21.4	The operator commands airspeed on auto (max-endurance), however the pitot-static system malfunctions and the UAV actually flies faster, burning fuel at a faster rate	The UAV autopilot must have a secondary method of measuring airspeed in case of a pitot-static system failure, such as GPS

The operator provides an airspeed value that will create a conflict with other aircraft	H2	C.22.1	The operator provides an airspeed command to deconflict with the traffic, but the airspeed change was not sufficient to avoid the traffic.	The operator must command a change in airspeed that is sufficient to deconflict with traffic
		C.22.2	The operator provides an airspeed command to accelerate in order to avoid traffic. The other aircraft also accelerates, resulting in a continued conflict.	The operator must communicate deconfliction actions with ATC or the aircrew of the aircraft In conflict. Otherwise, deconfliction actions must be standardized to allow deconfliction actions without communication
		C.22.3	The operator receives feedback from ATC that the traffic is no longer in conflict, and resumes max endurance speed. The feedback was based on current rate of speed, but the new airspeed causes a conflict.	The operator must turn off engine start command when the engine start command does not work until the operator is ready to try again.
		C.22.4	The operator provides an airspeed, but the winds change, causing the airspeed to change and no longer deconflict with the traffic.	The operator must consider winds when conducting flight planning and deconflicting with traffic
The operator provides airspeed after the UAV stalled due to slow flight	H4	C.23.1	The operator recognizes that the UAV is about to stall, and provides a higher airspeed so that the UAV will accelerate. The link is lost, and the UAV does not receive the airspeed command. The operator provides higher airspeed when the link is reestablished, but the UAV has already stalled.	The UAV must not fly near stall speed during appropriate phases of flight, such as touchdown

		C.23.2	The operator provides an airspeed that is above stall speed, but a tailwind or decreased headwind results in a stall. The operator does not immediately recognize that the aircraft is in a stall, and delays commanding a higher airspeed.	The UI must provide feedback to the operator when the airspeed approaches stall speed. The UAV must be programmed with a stall recovery procedure.
		C.23.3	The operator provides an airspeed below stall speed due to a pitot-static system malfunction. The airspeed feedback is higher than actual airspeed. The operator commands an airspeed that is above stall speed, but the resulting speed is less than stall speed. The operator receives attitude feedback indicating a stall, and commands a higher airspeed, but aircraft has already stalled.	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
		C.23.4	The operator provides an airspeed that is above stall speed, however a tailwind causes the airspeed to decrease and the UAV to stall. The operator provides an airspeed command, but the aircraft has already stalled.	The operator must fly an airspeed high enough above stall speed to avoid a stall if the headwind/tailwind changes occur
		C.23.5	The operator provides an airspeed that is above stall speed, however the engine fails, and the UAV does not adjust the UAV attitude to stop the deceleration below stall speed. The operator restarts the engine and commands a higher airspeed, but the UAV has already stalled.	The UAV must recognize when the engine has failed and fly an attitude that results in an airspeed above stall speed

The operator provides airspeed after structural damage from flying above VNE	H6	C.24.1	The operator recognizes that the UAV is about to exceed VNE and provides a lower airspeed. The link is lost, and the UAV does not receive the airspeed command. The operator provides higher airspeed when the link is reestablished, but the UAV already exceeded VNE.	The UAV must not fly near VNE.
		C.24.2	The operator provides an airspeed that is below VNE, but a decreased tailwind or an increased headwind results in exceeding VNE. The operator does not immediately recognize that the aircraft has exceeded VNE because the operator was not on the main UI page, and delays commanding a lower airspeed.	The UAV must not fly near VNE. Safety critical alerts, such as nearing an airspeed limit must be provided to the operator regardless of what UI screen the operator is on.
		C.24.3	The operator provides an airspeed that is above VNE due to a pitot-static system malfunction. The airspeed feedback is lower than the actual airspeed. The operator commands an airspeed that is below VNE. There is no feedback other than airspeed to indicate the VNE exceedance until the UAV airframe integrity is lost.	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
		C.24.4	The operator provides an airspeed that is below VNE, however a headwind causes the airspeed to increase above VNE. The operator commands a lower airspeed, but the UAV already exceeded VNE.	The UAV must not fly near VNE.

The operator provides airspeed when the number of airspeed assignments exceed the number of GPS waypoints	H3	C.25.1	The operator provides more airspeed assignments than GPS waypoints. The initial message containing airspeed assignments was cut off due to lost link. The operator resends the airspeed assignments, but rather than replace the incomplete message, the second message is added onto it.	The autopilot must replace previously provided airspeeds with the most recently provided airspeeds.
		C.25.2	During mission planning the operator creates too many airspeed assignments, and does not realize that there are more airspeed assignments than waypoint assignments.	The mission planning process must provide feedback to the operator when number of waypoints and airspeed assignments do not match
		C.25.3	The operator accidentally inputs one airspeed twice into the UI. The UI does not provide feedback to indicate that the number of airspeed assignments is different from the number of waypoint assignments. The UI assigns an incorrect airspeed for each of the subsequent waypoints after the duplication, and never assigns the airspeeds that do not have a corresponding waypoint.	The UI must provide feedback when the number of airspeed and waypoints do not match.
	H4, H6	C.25.4	The operator provides the same number of airspeeds as waypoints, but the UAV does not fly the assigned airspeeds. A pitot-static system malfunction causes the UAV to fly different airspeeds than assigned.	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch

The operator provides airspeed when the number of airspeed assignments are fewer than the number of GPS waypoints	H3	C.26.1	The operator provides the same number of airspeed assignments as waypoints, but the message is cut off due to lost link.	If lost link occurs after the operator provides a command, the operator must resend the command when the link is established to ensure that command was received
		C.26.2	The operator provides the same number of airspeed assignments as waypoints, but there are too many waypoints, and not all the airspeed assignments are not saved because the autopilot runs out of storage capacity.	The operator must know how many waypoints and associated altitude and airspeed assignments the autopilot can store and provide less than that amount. Additionally, the autopilot must be able to store enough data for the operator to provide the entire flight plan
		C.26.3	The operator misses an airspeed when inputting the airspeeds from the mission plan into the UI. The UI does not provide feedback to indicate that the number of airspeed assignments is different from the number of waypoint assignments. The UI assumes that the last airspeed assignment in the list is the airspeed assignment for the remainder of the flight.	The mission planning process must provide feedback to the operator when number of waypoints and airspeed assignments do not match

	H4, H6	C.26.4	The operator provides the same number of airspeeds as waypoints, but the UAV does not fly the assigned airspeeds. A pitot-static system malfunction causes the UAV to fly different airspeeds than assigned.	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
The operator does not provide engine start during prelaunch engine run-up	H3	C.27.1	The operator provides the engine restart command, however the battery is either depleted or not producing enough power to restart the engine.	The battery must provide enough power to start the engine during engine run-up. The battery charge must be checked during preflight, and external power must be used to start the engine as needed.
		C.27.2	The operator clicks on the engine start icon on the UI, however the engine start command is not sent because the operator clicked just outside the area that sends the command.	The operator must be able to click anywhere on an icon to send a command.
		C.27.3	The operator does not provide the engine start command because the operator believes that there are people in the propeller area. The ground personnel are actually clear of the area, but did not announce they were clear.	The ground personnel must provide an all clear call when personnel are out of the propeller area.
		C.27.4	The operator provides the command, but the engine does not start. The engine underwent maintenance, and the wiring was disconnected for maintenance, but not reconnected post maintenance.	The maintenance personnel must perform a post maintenance engine run-up after engine maintenance. Additionally, after maintenance the work area must be inspected to ensure the UAV has

				been returned to a flight ready state.
The operator does not provide engine start during before takeoff procedure	H3	C.28.1	The operator provides the engine restart command, however the battery is either depleted or not producing enough power to restart the engine.	Ground power must be available to start the engine as required. If battery is not charging, the flight must be cancelled.
		C.28.2	The operator clicks on the engine start icon on the UI, however the engine start command is not sent because the operator clicked just outside the area that sends the command.	The operator must be able to click anywhere on an icon to send a command.
		C.28.3	The operator receives inaccurate engine feedback indicating that the engine should not be started. The operator provides the information to the ground crew, who troubleshoot the problem, delaying the flight.	The engine health feedback parameters must be calibrated and regularly maintained to ensure accuracy.
		C.28.4	The operator provides the command, but the engine does not start. The engine start wire was loose, and when the aircraft was taxied to the engine run-up area, the wire became completely disconnected.	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight

The operator does not provide engine start command when the engine fails in flight and the engine needs to be restarted	H4	C.29.1	The operator provides the engine restart command, however the battery is either depleted or not producing enough power to restart the engine.	The battery must provide enough power to restart the engine if the engine fails in flight.
		C.29.2	The operator attempts to restart the engine, but the UAV is above the restart airspeed limit. The aircraft attitude is such that the airspeed does not decrease below the limit, and the engine is not restarted.	The UAV must be flown at an airspeed below the engine restart limit before engine restart is attempted.
		C.29.3	The operator provides the restart engine command, however the airspeed feedback is incorrect and the UAV is still above the restart airspeed limit and does not restart.	If airspeed feedback is incorrect the UAV must be able to fly attitude/throttle setting combinations to achieve a safe airspeed. Airspeed errors must be detected in order for the UAV to update the method of controlling flight.
		C.29.4	The operator provides the restart engine command, but the engine does not restart. The engine has failed such that it cannot be restarted, or the engine is no longer receiving fuel.	The operator must attempt to cycle fuel tanks before engine restart attempt. If there are indications that an engine restart is not possible, the operator must immediately begin preparation for landing

The operator provides the engine start command when ground personnel are near the propellers	H1	C.30.1	The operator does not provide the engine start command, however the UAV receives an engine start command from a second ground station while ground personnel were near the propellers	Either UAV operations must be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft.
		C.30.2	The operator does not provide the engine start command because there are people in the propeller area. The UAV is configured to start engines, but the operator is waiting for an area clear call. The operator puts the mouse over the engine start button on the UI and waits for the all clear call. The mouse is accidentally clicked before the all clear call starting the engine.	The operator must not put the mouse over a safety critical command until the command is safe to perform. Additionally, consider a secondary prompt for safety critical commands or other designs to prevent accidentally sending command.
		C.30.3	The operator is told that ground personnel are clear of the propeller area, but a technician reenters the area because the individual sees an issue that must be corrected before engine start	The ground personnel must inform the operator if personnel reenter the propeller area after the clear signal
	H5	C.30.4	The operator provides the engine start command, however the brakes failed and did not keep the aircraft from moving, and it taxis towards the personnel	Ground personnel must stand in a position such that if the UAV does inadvertently taxi after engine start it does not hit anyone.
The operator provides engine start command when the engine fails in flight, but after the UAV	H1	C.31.1	The operator attempts to restart the engine, but the engine start command is not received by the UAV due to terrain masking as it descends. The operator begins troubleshooting the lost link and leaves the engine start command on. When the	The operator must turn off engine start command when the engine start command does not work until the operator is ready to try again.

is committed to landing			link is established the UAV receives the engine restart command and restarts the engine.	
		C.31.2	The operator attempts to restart the engine, but the engine does not restart. The operator then begins checklist actions for landing. The operator does not disable the starter, and the engine starts near touchdown	The operator must turn off engine start command when the engine start command does not work until the operator is ready to try again.
		C.31.3	The engine quits because the operator does not switch fuel tanks, and the currently selected fuel tank is empty. The operator attempts to restart the engine, but is unsuccessful. During the landing sequence the operator realizes the fuel feed error, switches tanks, and successfully restarts the engine. However, the UAV is too close to the ground, and the autopilot does not transition safely from engine off performance to engine on performance.	The operator must verify fuel state and switch tanks during engine failure emergency procedures if the UAV is above safe restart altitude. The UAV autopilot must be designed to transition smoothly between engine off and engine on performance.

		C.31.4	The operator attempts to restart the engine, but the engine does not restart. The operator continues to attempt a restart as time permits, in accordance with the checklist. The UAV is flying far from the airfield, and the exact height above ground is not known. The operator continues to attempt restart and finally does restart the engine, but the UAV descended too low and impacts terrain	During mission planning, operators must determine minimum restart attempt altitudes for each leg of the route that is based on a safe pressure altitude, since exact altitude above ground may not be known. The laser altimeter must be on battery power for use to determine height above terrain.
		C.31.5	The operator determines based on the altitude that an engine restart is not appropriate and begins checklist actions for landing. A loose wire provides power to the engine starter, and the engine restarts without the engine start command	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight
The operator does not provide the launch now command during takeoff	H3	C.32.1	The operator provided the launch now command, however the command was not received due to interference with concurrent UAV operations	UAV operators must be aware of EM usage in operating area and deconflict operations to avoid interference.
		C.32.2	The operator does not provide the launch now command because the operator did not receive ATC's clear for takeoff call	The ground station must be equipped to communicate with ATC, and radio and internal communications must be kept to a minimum during launch operations to ensure all ATC instructions are received

		C.32.3	The operator does not provide the launch now command because the controller receives incorrect engine parameter feedback and believes the engine is not operating within limits. The operator aborts the takeoff to allow ground personnel to tow the aircraft back to park and troubleshoot the problem.	The engine health feedback parameters must be calibrated and regularly maintained to ensure accuracy.
		C.32.4	The operator provides the launch now command, which was received by the UAV, however the UAV did not launch. The UI launch sequence is not programmed correctly, and the UAV does not accelerate enough to rotate and takeoff	The UI launch sequence must be verified before flight and adjusted for atmospheric conditions at the airfield.
The operator provides the launch now command when the runway is not clear	H2	C.33.1	The operator does not provide the launch now command, however another LOS ground station on site is conducting checks and does provide the launch command	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct
	H1	C.33.2	The operator receives a clear for takeoff call from ATC, but the ground personnel did not provide a personnel clear call. The operator commands launch now after the ATC call.	The operator must not provide the launch now command until the operator receives calls from both ATC and ground personnel

	H1	C.33.3	The operator is waiting on a clear for takeoff call from ATC, and rests the mouse cursor over the launch now button on the UI. While waiting, the operator or another person in the ground station accidentally clicks the mouse, launching the UAV.	The operator must not put the mouse over a safety critical command until the command is safe to perform. Additionally, consider a secondary prompt for safety critical commands or other designs to prevent accidentally sending command.
		C.33.4	The operator receives a clear for takeoff call from ATC and a personnel clear call from the ground personnel supporting the launch. Visibility is low, and the tower cannot see the entire runway. The lipstick camera also does not provide a view of the entire runway due to low visibility. There is either an aircraft or a vehicle on the runway that cannot be seen by ATC, ground personnel, or the UAV operator.	The UAV must be able to abort a launch attempt once the operator recognizes that the runway is not clear.
	H5	C.33.5	The operator does not provide the launch now command, however the parking brake fails and the UAV travels down the runway.	The UAV should maintain an idle or near idle throttle setting until the launch command is provided. Additionally, the UAV must be able to quickly stop if the UAV moves inadvertently
The operator provides the launch now command when the UAV is not on the runway	H5	C.34.1	The operator does not provide the launch now command, however another LOS ground station on site is conducting checks and does provide the launch command	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be

				verified to ensure it is correct
		C.34.2	During the engine run-up, the operator accidentally clicks the launch now button on the UI. The thrust overcomes the parking brake and the UAV travels over the chocks.	A secondary prompt for safety critical commands or other designs to prevent accidentally sending command.
		C.34.3	The operator provides the launch now command when the UAV is on the runway, however the UAV runs off the runway during the launch procedure. The crosswinds are out of limits, however the latest weather report indicated crosswinds were within limits.	The weather support organization must provide up to date weather information and alert the UAV operator if the wind is out of limits during the before takeoff procedures.
		C.34.4	The operator provides the launch now command when the UAV is on the runway, however the UAV runs off the runway during the launch procedure. The UAV does not compensate for the crosswinds.	The UAV must be designed to compensate for crosswinds during takeoff.
The operator provides the launch now command before ground personnel and equipment are clear of the area	H1	C.35.1	The operator does not provide the launch now command, however another LOS ground station on site is conducting checks and does provide the launch command	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.35.2	The operator received a takeoff clearance from ATC and did not see anyone through the camera. The operator assumed the runway was clear and provided the launch now command	The operator must receive an area clear message from the ground personnel before providing the launch now command
		C.35.3	The ground personnel state that the area is clear, however it is not actually clear. The ground personnel are still walking out of the path of the UAV and believe they have time to clear the area before launch.	The area clear call must only be given when all personnel are out of the path of the aircraft
		C.35.4	The ground personnel state that the area is clear, and believe the ground equipment is out of the path of the aircraft, however the equipment is still within the path of the aircraft.	All ground equipment used to tow the aircraft to the runway must be completely off the runway before takeoff
	H5	C.35.5	The ground personnel and equipment are to the side of the aircraft out of the path, however when the aircraft launches, it does not move in a straight line down the runway, and instead rolls towards the ground personnel and equipment	All personnel and ground equipment must be placed behind the aircraft to avoid being hit by the aircraft if the launch is not successful
The operator provides the launch now command after the UAV is airborne	H4	C.36.1	The operator does not provide the launch now command, however another LOS ground station on site is conducting checks and does provide the launch command	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.36.2	The operator accidentally clicks the launch now button. The operator intended to click a different button. The UAV immediately reduces throttle to the starting throttle position during the launch sequence, causing the UAV to stall.	A secondary prompt for safety critical commands or other designs to prevent accidentally sending command.
		C.36.3	The operator provides the launch now command, but the pitot static system is not working. The UAV accelerates and goes airborne, but the operator believes the command was not received and provides the launch now command again.	The operator must use visual confirmation of launch, either from the camera or from ground personnel. Additionally if the UAV does not appear to working as expected, the launch or sortie must be aborted and the issue resolved before continuing the mission.
		C.36.4	The operator provides the launch now command. A headwind gust causes the UAV to become airborne earlier than expected, and when the gust or ground effect ends the UAV no longer has enough lift to maintain flight and lands back on the runway.	During takeoff in gusty conditions, the rotate speed must be increased, if runway length allows, to prevent early rotation.
The operator does not provide the land now command when the UAV is in the pattern and at minimum fuel	H4	C.37.1	The operator provides the land now command, but the UAV does not receive the command. Interference from another UAV prevents the signal reception.	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.37.2	The operator believes that the UAV has enough fuel to last until landing, even though the UAV is fuel state is low. The operator decides to wait for the UAV's turn to land rather than declaring a fuel emergency and landing as soon as possible.	The operator must declare a fuel emergency when the fuel state is low in order to land as soon as possible
		C.37.3	The UAV provides inaccurate fuel state data and the operator believes that the UAV has more fuel than it actually has. There are other aircraft in the pattern ahead of the UAV, and the UAV waits to land instead of declaring an emergency in order to land ahead of the other aircraft.	The UAV must provide accurate fuel state feedback to the operator
	H1	C.37.4	The operator recognizes that the fuel is low and declares an emergency. The operator then provides the land now command, but it takes longer to land than expected due to traffic and winds. The UAV runs out of fuel and crash lands off the runway.	The operator must include winds and the time it takes to deconflict traffic when determining when to declare an emergency
The operator does not provide the land now command when the UAV is at the airfield and other aircraft are attempting to enter the pattern	H2	C.38.1	The operator provides the land now command, but the UAV does not receive the command. Interference from another UAV prevents the signal reception.	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.38.2	The operator does not provide the land now command. The operator believes that the winds are out of limits for landing, and decides to remain in the pattern to see if the winds decrease in order to land. There are other aircraft with higher wind limits that are attempting to land at the same time, and the pattern is busy.	If the UAV cannot land, but other aircraft can enter the pattern and land the UAV must maintain a hold away from the pattern to avoid traffic congestion
		C.38.3	The operator does not hear the clear to land call from ATC. The operator is coordinating with the ground personnel for the tow and providing aircraft status information when ATC's call was made.	During critical phases of flight, such as takeoff, climb, and landing, the ground station must be clear of nonessential personnel and the operator must maintain a 'sterile cockpit' environment.
	H1	C.38.4	The operator provides the land now command, but the GPS solution is not accurate, and the UAV does not fly the pattern as published or land on the runway	The VMS must receive feedback when the accuracy of the GPS solution is below a minimum threshold, additionally other navigation solutions such as INS or VOR should be considered as a backup system
The operator provides the land now command when the runway is not clear	H2	C.39.1	The operator does not provide the land now command, but the UAV executes the landing procedure. Another ground station provides the land now command for another UAV in the pattern, but both UAVs receive the command.	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.39.2	The operator heard ATC provide a landing clearance to another aircraft and mistakenly thought the clearance was for the operator's UAV. The operator reads back the clearance at the same time as the other pilot, and ATC only hears the read back for the correct aircraft. The operator provides the land now command as the other aircraft is landing.	During critical phases of flight, such as takeoff, climb, and landing, the ground station must be clear of nonessential personnel and the operator must maintain a 'sterile cockpit' environment.
		C.39.3	ATC provides a landing clearance even though an aircraft is on the runway because the controller believes that the aircraft will be off the runway by the time the UAV lands. The aircraft on the runway is not able to clear the runway in time, and the UAV lands on the runway while the other aircraft is also on the runway.	The operator must be able to abort the landing procedure if the landing is not longer considered safe. Ground personnel must provide feedback if there is an aircraft on the runway, as the UAV operator may not see the runway through the camera.
	H5	C.39.4	The operator provides the land now command, but the UAV does not compensate for crosswinds during final approach and does not land on the runway	The UAV must be designed to compensate for crosswinds during landing
The operator provides the land now command when the UAV is not at the airfield	H1	C.40.1	The land now command is not provided, but the UAV receives a land command from a different ground control station	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct

		C.40.2	The operator does not intend to click the land now button. The button is near another button that the operator meant to press. The operator does not immediately realize that the UAV is trying to land, and does not recover the aircraft before it flies into terrain.	A secondary prompt for safety critical commands or other designs to prevent accidentally sending command.
	H2	C.40.3	The UAV provides a GPS position indicating that the UAV is in the pattern, however the GPS solution is inaccurate and the UAV is not in the pattern.	The VMS must receive feedback when the accuracy of the GPS solution is below a minimum threshold, additionally other navigation solutions such as INS or VOR should be considered as a backup system
		C.40.4	The operator provides the land now command, but provides a GPS landing waypoint that is not at the airfield. The landing point was for an emergency off field landing, and was mistakenly provided to the UAV prior to landing.	The UI must provide feedback if the landing waypoint is not at the runway.
The operator provides the land now command before the UAV completes the airfield arrival procedure	H1, H2	C.41.1	The land now command is not provided, but the UAV receives a land command from a different ground control station	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct
		C.41.2	The operator sets up the landing procedure, and places the mouse over the land now button. The operator accidentally presses the	A secondary prompt for safety critical commands or other designs to prevent

			mouse, commanding the UAV to land.	accidentally sending command.
		C.41.3	The operator receives incorrect GPS location and believes the UAV has finished the approach.	The VMS must receive feedback when the accuracy of the GPS solution is below a minimum threshold, additionally other navigation solutions such as INS or VOR should be considered as a backup system
		C.41.4	The operator provides the command, which is to be executed once the arrival is complete, but instead the UAV executes the landing procedure as soon as the command is received. The command overwrites the current flight plan.	The landing sequence must not overwrite the current plan, or the landing sequence must not be provided until the UAV is in a position to land.
The operator does not provide lost link procedures during flight operations	H1, H2	C.42.1	The operator provides the lost link procedure, but it is not received due to interference or masking. The procedure is then not updated as terrain, weather, or conflicting traffic changes along the route of flight	The UAV most provide feedback indicating the lost link procedures were received. If the feedback is not received by the operator, the operator must resend the procedures
		C.42.2	The operator does not believe that the lost link procedure needs to be updated because the procedure was recently updated per a regular schedule, and does not provide updated lost link procedure. However, terrain, weather, or conflicting traffic have changed along the route since the schedule update.	The lost link procedures should be updated based on route of travel and obstacles between the UAV and the airfield rather than timing.

		C.42.3	The operator does not provide an updated lost link procedure because the operator was not aware that the airspace that the UAV would fly through if a lost link occurred is no longer safe.	ATC must provide the operator with up to date information if airspace is no longer safe. The operator must also provide ATC with the current lost link procedure so that if lost link should occur ATC can ensure other aircraft are clear of the path.
		C.42.4	The operator provides lost link procedures, but the same signal that is jamming communications also jams the GPS signal, and the UAV flies off course	The UAV must be able to detect when the GPS signal is lost and use backup navigation methods. Additionally, the communications system must have a backup system that is fully independent of the main communications system.
The operator provides lost link procedure, and the lost link procedure waypoints conflict with other aircraft	H2	C.43.1	Lost link procedures are updated by another ground station. The procedures were intended for another UAV.	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct
		C.43.2	The operator is aware that there are other aircraft in the airspace, but provides the lost link procedure anyway. The operator believes that should lost link occur, the operator can update ATC so that they can deconflict the other aircraft. However, the lost link is due to communications failure at the ground station,	The operator must not provide a lost link procedure that conflicts with other traffic.

			and the operator cannot inform ATC of the lost link.	
		C.43.3	The operator does not receive feedback from ATC that the airspace the UAV will fly through if lost link occurs is now occupied by aircraft.	ATC must provide the operator with up to date information if airspace is no longer safe. The operator must also provide ATC with the current lost link procedure so that if lost link should occur ATC can ensure other aircraft are clear of the path.
		C.43.4	The lost link procedures do not conflict with other traffic, but winds blow the UAV off course, and the UAV does not correct the course deviation	The UAV must compensate for winds and maintain the course between waypoints.
The operator provides lost link procedures, and the lost link procedure is not at or above MOCA	H1	C.44.1	Lost link procedures are updated by another ground station. The procedures were intended for another UAV that is flying over lower terrain.	Either UAV operations should be deconflicted, or procedures put in place to ensure the control station is linked to the correct aircraft. If an incorrect link takes place all data must be verified to ensure it is correct
		C.44.2	The lost link procedures are based off of the current position of the UAV, but when the UAV loses the link later in the flight there is higher terrain between the airfield and the UAV.	If lost link procedures are provided based on timing rather than expected terrain, the lost link procedure must be safe for the entire time until the next

				scheduled lost link update.
		C.44.3	The operator has inaccurate charts, and believes that the lost link procedure is safe, but the altitude is actually too low compared to the terrain.	The operations support organization must provide updated and accurate charts.
		C.44.4	The lost link procedures are of an appropriate altitude for the course, however the winds blow the UAV off course, and it does not correct the course deviation.	The UAV must be programmed to correct course deviations.
The operator provides lost link procedures before lost link procedures needed to be updated	H1, H2	C.45.1	It is almost time to update the lost link procedures, so the operator decides to go ahead and send the update. Shortly after the update, the UAV experiences a lost link and executes the procedures for the upcoming leg rather than the current leg.	The lost link procedure update must not be provided until the UAV is flying the leg associated with the updated procedure
		C.45.2	The operator received position feedback that indicated the UAV was at the next leg, so the operator provided the lost link procedure. The position feedback was incorrect, and the update was not yet needed.	Once the UAV has entered the leg associated with the updated lost link procedure, the operator must send the procedure.
The operator provides lost link procedures when the waypoints exceed the storage	H1, H2	C.46.1	The operator provides lost link procedures that were within the storage capacity of the autopilot. The message received by the UAV is delimited incorrectly due to translation from the UI to the radios to the UAV, which exceeds storage capacity	The ground station radios must send commands accurately

capacity of the autopilot				
		C.46.2	The operator provides a large number of lost link waypoints to ensure that the UAV flies a safe route, however the operator uses too many waypoints that exceeded the storage	The operator must send a number of waypoints that are less than the autopilot storage. The autopilot storage must be large enough to store enough waypoints for the length of mission
		C.46.3	The operator provides the lost link procedures, but does not receive feedback that the procedures were received, so the operator provides them again. The second set of procedures are concatenated rather than replacing the first set of procedures	The UAV must provide feedback that the procedure are received, and the autopilot must replace old procedures with new procedures
		C.46.4	The operator provides lost link procedures that are within the storage capacity of the autopilot, but the procedures are delimited incorrectly taking up more storage space than the autopilot's capacity	The UAV must save procedures into the autopilot accurately
The operator does not provide the payload power on command when UAV is over the target area	H3	C.47.1	The operator provided the payload power on command, however the signal is jammed, and the UAV does not receive the command.	The operator must provide payload power on early to ensure that the command is received before the UAV is over the target area

		C.47.2	The operator does not provide the payload on command because the operator misinterpreted the flight plan and did not believe the UAV was over the target area	The UI must provide feedback indicating when the UAV is over the target area
	H1, H2	C.47.3	The operator does not provide the payload on command because the operator believes the UAV is not at the target area. A GPS navigation malfunction, inaccurate solution, or jamming of the navigation signal causes the operator to get incorrect or no position feedback.	The GPS must provide feedback when the solution is below the minimum accuracy threshold. Additionally, a secondary navigational system such as VOR or INS must be considered in the design
		C.47.4	The operator provides the power on command when the UAV is over the target area, however the payload does not turn on. The payload was installed before the flight, and the wiring was not installed to provide the payload with power	After conducting payload maintenance, the payload must undergo a functional checkout to ensure it works as expected
The operator provides the payload power on command when the alternator fails	H4	C.48.1	The operator does not provide the payload power on command because the operator recognizes that there is an alternator failure, and the UAV is operating on battery power. A shorted wire provides the payload power, anyway, draining the battery.	Wiring must be checked during preflight and should be designed to withstand vibrations associated with flight
		C.48.2	The operator recognizes that the alternator has failed, but the aircraft is heading towards the airfield (on a return leg), and the operator believes that there is enough power for the payload to be turned on for a short time.	The payload must not be powered on if the alternator is not functioning

		C.48.3	The operator does not receive power system feedback from the UAV, and does not recognize that the alternator has failed. The operator is using a main screen, and unless the operator checks the electric power status screen is unaware of the power system state.	Subsystem faults must be displayed on the UI regardless of what screen the operator is actively looking at. Additionally, consider an electrical system screen check prior to turning on the payload.
		C.48.4	The operator provides the payload power on command. The payload uses more power than expected, causing the battery to drain. The alternator fails, but there is no battery power to power the UAV	The payload must not consume any more power than what the alternator provides
The operator does not provide the payload power off command when the alternator fails	H4	C.49.1	The operator cannot turn the payload power off when the alternator fails because the radio is not on battery power. The UAV executes lost link procedures, but is not programmed to turn off the payload power and does not have enough battery power to return home.	The radio must be on battery power in case of an alternator failure. In case of lost link, the VMS must be programmed to turn off the payload power if the alternator fails or wiring must be designed to prevent emergency power to the payload.
		C.49.2	The operator recognizes that the alternator is not producing power, but the UAV is over the target area, and the operator decides to continue operating the payload until the UAV has left the target area	The operator must power off the payload and return to the airfield if the alternator fails.
		C.49.3	The operator recognizes that the alternator is not producing power, the operator sends a command to turn the power off, however the power system feedback	Subsystem faults must be displayed on the UI regardless of what screen the operator is actively looking at. Additionally, consider an alert to ensure that

			was delayed, and the battery is significantly depleted	the operator sees the feedback as soon as it is provided.
		C.49.4	The operator recognizes that the alternator is not producing power and clicks the button on the UI to turn off the payload. The operator clicked just outside the button, and the operator did not notice that the command to the payload power was not sent.	The status of the payload power must be distinguishable between on and off.
		C.49.5	The operator provides the payload power off command to conserve power once the alternator fails, however even with the payload power off the UAV does not have enough battery power to return to base	The battery must have enough power to return to base safely
The operator provides the payload power off command when the UAV is over the target area	H3	C.50.1	The operator provides the payload power on command, however another ground station is being used for a post maintenance check or training, and the ground station sends a payload power off signal that the UAV receives, and the UAV turns off payload power.	Ground stations must not send signals out when they are not actively controlling an aircraft.
		C50.2	The operator misinterprets the flight plan, and believes that the UAV has exited the target area. The operator turns the payload power off while the UAV is still over the target area.	The UI must provide feedback indicating when the UAV is over the target area

		C.50.2	The operator believes the UAV has left the target area. A GPS navigation malfunction, inaccurate solution, or jamming of the navigation signal causes the operator to get incorrect or no position feedback and provide the payload power off command	If the operator is unsure of the position of the UAV, the operator must not provide the payload off command
		C50.3	The operator does not provide the payload power off command, however the payload was not designed for the flight environment it is being subjected to, and fails inflight	The payloads must be designed and tested for the UAV flight conditions

Table 12 UAV VMS Scenarios

UCA	Hazard	Scenario Designator	Main Scenario Description	Safety Constraint
The VMS does not provide roll, pitch, or yaw commands when the UAV is off course	H1, H2, H3	V.1.1	The VMS provides the roll, pitch, or yaw, however the actuator does not receive the command. A broken wire or connection prevents the signal from getting to the actuator.	Wiring must be checked during preflight and should be designed to withstand vibrations associated with flight
		V.1.2	The VMS knows the position of the aircraft relative to the waypoint, however it does not command roll, pitch, or yaw in order to fly to the waypoint. Winds are blowing the UAV off course. The waypoints are spread out, and the UAV autopilot is programmed to fly to the next waypoint, not maintain	The UAV must fly the desired course. In windy conditions, the waypoints may have to be closer together to maintain the track. Or, the UAV must be programmed to follow the course, not just fly to the waypoint from present position

			the course from the previous waypoint.	
		V.1.3	The VMS receives incorrect UAV position feedback, and therefore does not recognize that it needs to provide roll, pitch, or yaw commands to fly to the waypoint. The position is inaccurate because the GPS navigation malfunctions or has an inaccurate solution.	The VMS must receive feedback when the accuracy of the GPS solution is below a minimum threshold, additionally other navigation solutions such as INS or VOR should be considered as a backup system
	H4	V.1.4	The VMS provides the roll, pitch, or yaw, but the control surface does not deflect. An actuator or cable linkage is broken not allowing the aircraft roll, pitch or yaw	Actuators and cable linkages must be inspected before each flight. A control check should also be performed during preflight.

The VMS provides roll, pitch, or yaw when the command exceeds aircraft attitude limits	H4	V.2.1	The VMS does not provide the roll, pitch, or yaw command, but the aileron, elevator, and rudder receive the command. A shorted wire provides power to the actuator causing the aileron, elevator, or rudder to move. The aileron, elevator, and rudder receive the command even though the VMS did not command it.	Wiring must be designed to withstand the flight environment, and inspected before flight.
		V.2.2	The VMS provides the roll, pitch, or yaw command and exceed limits for the current flight condition. The VMS was programmed with one set of attitude limits, rather than a set of attitude limits for different flight conditions (altitude & speed). The command did not exceed the programmed limits, but it did exceed actual limits for that particular flight condition	The VMS must be programmed with limits at all flight conditions
		V.2.3	The VMS provides a roll, pitch, or yaw command that it believes will result in an attitude within limits, however the attitude is actually out of limits. The aeromodelling of the system was not validated, and the magnitude of the command is too large. The commanded attitude is actually out of limits.	The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations

		V.2.4	The VMS provides a roll, yaw, or pitch input to correct an invalid attitude indication it is receiving and exceeds attitude limits. The invalid feedback is due to a vacuum pump failure that renders the attitude indicator inoperative. The command exceeds attitude limits, but the VMS does not recognize the exceedence due to the invalid attitude indication.	A secondary attitude indicator must be included in the UAV design as a backup to the main attitude indicator. The VMS must receive feedback of a vacuum pump failure so that it can switch to the secondary attitude feedback
	H5	V.2.5	The VMS provides a roll, pitch, or yaw command that is appropriate for staying within the UAV attitude limits. The actuator was connected to the cables backwards, and the VMS input has the opposite effect (roll left input rolls UAV right). The VMS continues to command in the same direction in an attempt to correct the attitude eventually exceeding aircraft limits.	After any control surface related maintenance, a controls check must be accomplished. A controls check must also be accomplished during preflight. Consider different connectors for the different directions so that it cannot physically be connected backwards.
The VMS provides roll, pitch, or yaw when the command steers the UAV off course	H1, H2, H3	V.3.1	The VMS provided the roll, pitch, or yaw correctly to maintain the course, however the command was received incorrectly . The wiring to the actuator was backwards, commanding the UAV to move in the opposite direction.	After any control surface related maintenance, a controls check must be accomplished. A controls check must also be accomplished during preflight. Consider different wiring connectors so that it is impossible

				to wire the actuator backwards
	H5	V.3.2	The UAV provides a roll, pitch, or yaw command that is insufficient to maintain the course. The control algorithm is designed to make small, slow corrections to avoid overcontrol. The corrections are too small to correct course deviations, and the UAV flies off course	The control algorithm in the autopilot must be designed to make both small corrections when deviations are small, and larger corrections for greater deviations.
	H5	V.3.3	The UAV provides roll, pitch, or yaw command that steers the UAV off course. The UAV receives incorrect position data indicating that the UAV is off course. The UAV commands roll, pitch, or yaw to return to the course, but actually causes the UAV to go off course	The GPS must provide feedback when the solution is below the minimum accuracy threshold. Additionally, a secondary navigational system such as VOR or INS must be considered in the design
		V.3.4	The UAV does not provide roll, pitch, or yaw command, but the UAV goes off course. Wind blows the UAV off course, and the VMS is programmed to fly towards a waypoint, not maintain a course.	The autopilot must be programmed to maintain the course between waypoints to avoid airspace conflicts or CFIT

The VMS provides the pitch down command when the throttle is reduced in order to descend, but the command is delayed	H4	V.4.1	The VMS provided the pitch command, however the actuator did not receive the command at the appropriate time. An intermittent wiring issue delays the command to the actuator	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight
		V.4.2	The VMS provided the pitch command late. The autopilot was programmed incorrectly with too long of a delay between throttle and elevator commands	The autopilot must be programmed to minimize delay between two correlated control surface or throttle commands
		V.4.3	The VMS received incorrect feedback which resulted in delaying the pitch command. The VMS did not receive feedback that the throttle was reduced therefore it did not command the nose down to avoid an overspeed	The VMS must receive accurate feedback of the throttle position
		V.4.4	The VMS received incorrect feedback which resulted in delaying the pitch command. The VMS received incorrect feedback that the elevator was already at the appropriate position	The VMS must receive accurate feedback of the control surface deflections
		V.4.5	The VMS provided the control surface actuator command correctly, but the elevator did not deflect as expected. The actuator linkage or cable is broken, and the elevator is no longer controllable	Actuators and cable linkages must be inspected regularly before flight

		V.4.6	The VMS provided the pitch command correctly, but the control surface did not deflect as expected. The power system did not provide power to the actuator due to a power system failure	Flight critical components such as actuators must have backup power so that the aircraft may be landed after a power system failure
The VMS provides a pitch up command when the throttle is increased for a climb, but the command is delayed	H6	V.5.1	The VMS provided the pitch command, however the actuator did not receive the command at the appropriate time. An intermittent wiring issue delays the command to the actuator	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight
		V.5.2	The VMS provided the pitch command late. The autopilot was programmed incorrectly with too long of a delay between throttle and elevator commands	The autopilot must be programmed to minimize delay between two correlated control surface or throttle commands
		V.5.3	The VMS received incorrect feedback which resulted in delaying the pitch command. The VMS did not receive feedback that the throttle was increased therefore it did not command the nose up to avoid a stall	The VMS must receive accurate feedback of the throttle setting
		V.5.4	The VMS received incorrect feedback which resulted in delaying the pitch command. The VMS received incorrect feedback that the elevator was already at the appropriate position	Actuators and cable linkages must be inspected regularly before flight

	H4	V.5.5	The VMS provided the control surface actuator command correctly, but the elevator did not deflect as expected. The actuator linkage or cable is broken, and the elevator is no longer controllable	Actuators and cable linkages must be inspected regularly before flight
	H4	V.5.6	The VMS provided the pitch command correctly, but the control surface did not deflect as expected. The power system did not provide power to the actuator due to a power system failure	Flight critical components such as actuators must have backup power so that the aircraft may be landed after a power system failure
The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is not brought back to neutral when the aircraft reaches the target heading/descent/ascent	H1, H2, H3	V.6.1	The VMS provides a command to return the aileron, elevator, or rudder back to neutral, however the command was not received due to a power system fault. Wiring or connections to the actuator are broken, keeping the actuator from receiving the signal. Or, a system power failure (such as an alternator failure) occurs, and the actuators are not on battery power.	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight. The power system must be designed such that a power system failure does not result in loss of actuator power
	H4	V.6.2	The VMS provides a command to return the aileron, elevator, or rudder back to neutral, however the aeromodel is incorrect and the aircraft did not take as long as expected to reach the desired heading/descent/ascent	The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations

	H4	V.6.3	The VMS received incorrect attitude data, and believed that the aileron, elevator, or rudder needed to stay deflected for longer than actually needed to attain the desired heading/descent/ascent	Attitude indicators must be inspected during preflight, and must be flight tested to ensure accuracy
	H4	V.6.4	The VMS provided a command to return the control surface actuator to neutral, however the control surface did not move as expected. The actuator linkage or cable is broken, and the aileron, elevator, or rudder is no longer controllable	Actuators and cable linkages must be inspected on a regular basis and during preflight inspections
The VMS provides a roll, pitch, or yaw command, but the aileron, elevator, or rudder is brought back to neutral before the UAV reaches the target heading/descent/ascent	H1, H2, H3	V.7.1	The VMS does not provide a command to return the aileron, elevator, or rudder back to neutral, however the command was received due to a power system fault. Wiring or connections to the actuator are broken, removing power to the actuator and causing the aileron, rudder, or elevator to return to neutral.	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.

	H4	V.7.2	The VMS provides a command to return the aileron, elevator, or rudder to neutral, but the UAV has not yet achieved the desired heading/descent/ascent. The aeromodel was incorrect, and aircraft took longer than expected to reach the desired heading/descent/ascent.	The aeromodel must be validated for the entire flight envelope and flight configurations to include abnormal configurations
	H4	V.7.3	The VMS receives incorrect attitude data, and believes that the aileron, elevator, or rudder does not need to stay deflected to attain the desired heading/descent/ascent	Attitude indicators must be inspected during preflight, and must be flight tested to ensure accuracy
	H4	V.7.4	The VMS does not provide a command to return the aileron, elevator, or rudder to neutral, but it returned anyway. The actuator linkage or cable is broken, and the aileron, elevator, or rudder is free floating	Actuators and cable linkages must be inspected on a regular basis and during preflight inspections
The VMS does not provide a throttle setting command when environmental conditions change (turbulence, gusts)	H4, H6	V.8.1	The VMS provides a throttle setting, but the engine throttle does not receive the command. The wires or connectors to the throttle actuator are broken	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.

		V.8.2	The VMS receives vertical speed and airspeed data that indicate the UAV is in an area of turbulence or gusts, however it is not programmed to change the throttle setting.	The VMS must be able to either determine when environmental conditions change, or provide feedback to the operator such that the throttle can be set for a safe airspeed in the conditions
		V.8.3	The VMS does not receive vertical speed feedback, and does not recognize that the UAV is in turbulent conditions	The VMS must receive feedback to determine when it is in turbulent or gusty conditions so that it can set a safe airspeed
		V.8.4	The VMS recognizes that the UAV is flying through gusty conditions, and commands the throttle lower the airspeed to less than maximum safe velocity in rough air (VNO). The throttle setting does not change. The cable or actuator connection is broken, and the throttle is no longer controllable	Actuators and cable linkages must be inspected on a regular basis and during preflight inspections
The VMS does not provide a higher throttle setting when the UAV is in a sustained turn, which reduces lift	H1, H2	V.9.1	The VMS provides a throttle setting, but the engine throttle does not receive the command. The wires or connectors to the throttle actuator are broken	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.

		V.9.2	The VMS enters a turn and the airspeed subsequently decreases. The VMS commands a higher throttle setting to maintain airspeed, which in turn increases the turn radius, causing the aircraft to no longer be on course. The VMS responds by increasing bank angle, which again necessitates an increased throttle setting causing the turn radius to increase again. This cycle occurs until the UAV reaches the bank angle limit, causing the payload to point away from the target area the UAV is orbiting	The UAV must be programmed to pitch up in an orbit to maintain the turn radius with the higher throttle setting.
	H4	V.9.3	The VMS enters a turn and the airspeed subsequently decreases. The VMS commands a higher throttle setting to maintain airspeed, which in turn increases the turn radius, causing the aircraft to no longer be on course. The VMS responds by increasing bank angle, which again necessitates an increased throttle setting causing the turn radius to increase again. This cycle continues, but attitude indicators are inoperative, and the UAV exceeds attitude limits	The UAV must have a secondary attitude indicator, and the primary attitude indicator must provide feedback when it is inoperative

	H4	V.9.4	The VMS recognizes that the UAV is descending in the turn and commands an increased throttle setting. The throttle setting does not change. The cable or actuator connection is broken, and the throttle is no longer controllable	Actuators and cable linkages must be inspected on a regular basis and during preflight inspections
The VMS provides a throttle setting, but the throttle setting is not enough to maintain an airspeed above stall speed	H4	V.10.1	The VMS did not provide a throttle setting below stall speed, however a short in the wiring provided the command to the actuator, and the throttle setting decreased	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.
		V.10.2	The UAV provides a throttle setting for a slow airspeed above the programmed stall speed. The programmed stall speed is incorrect: it is for lower altitudes, but at higher altitudes the stall speed increases. The higher stall speed is not programmed into the autopilot, and the UAV is actually below stall speed	The VMS must be programmed with limits at all flight conditions
		V.10.3	The UAV receives inaccurate throttle feedback and believes that the throttle is in an appropriate position to maintain an airspeed above stall. The actuator was replaced, and not calibrated to ensure the position feedback is correct.	After any throttle related maintenance, an engine run must be accomplished, to include calibrating the position of the actuator with the throttle setting

		V.10.4	The UAV provided a throttle setting that should have resulted in a higher airspeed, but the airspeed is below stall. Slack in the cables caused the throttle to not reach a the commanded setting	Cables must be inspected on a regular basis, and during the preflight inspection
The VMS provides a throttle setting that accelerates the aircraft above VNE	H6	V.11.1	The VMS did not provide a throttle setting below stall speed, however a short in the wiring provided the command to the actuator, and the throttle setting increased	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.
		V.11.2	The UAV provides a throttle setting for a high airspeed just under VNE The programmed VNE speed is incorrect: it is for lower altitudes, but at higher altitudes VNE decreases The lower VNE speed is not programmed into the autopilot, and the UAV is actually above VNE	The VMS must be programmed with limits at all flight conditions
		V.11.3	The UAV receives inaccurate throttle feedback and believes that the throttle is in an appropriate position to maintain an airspeed below VNE. The actuator was replaced, and not calibrated to ensure the position feedback is correct.	After any throttle related maintenance, an engine run must be accomplished, to include calibrating the position of the actuator with the throttle setting

		V.11.4	The UAV provided a throttle setting that should have resulted in a lower airspeed, but the airspeed is above VNE. Cable maintenance resulted in an initial throttle setting at a neutral actuator position that is higher than designed. Therefore, when the throttle increased the actual throttle setting was higher than expected	After any throttle related maintenance, an engine run must be accomplished, to include calibrating the position of the actuator with the throttle setting
The VMS provides a reduced throttle setting too late after the UAV flares for landing	H1, H5	V.12.1	The VMS provided the throttle command at the right time, but the actuator received the command late. An intermittent wiring issue delays the command to the actuator	Wiring must be inspected during preflight and must be designed to withstand vibrations associated with flight.
		V.12.2	The VMS provided the command late due to incorrect programming. The UAV is programmed to wait a certain amount of time after the flare to reduce the airspeed, however flight conditions required an earlier throttle reduction	The VMS autopilot must be programmed to land using airspeed and altitude feedback rather than timing. The UAV must be tested in nominal and off nominal conditions
		V.12.3	The VMS provided the command late due to incorrect system feedback. The laser altimeter is malfunctioning and providing incorrect altitude data. The VMS believes the UAV is too high for a reduced throttle setting	The UAV must be designed to detect laser altimeter malfunctions. The laser altimeter must be inspected regularly for proper function, and the exterior must be clean before flight

		V.12.4	The VMS provided the command late due to incorrect system feedback. The pitot static system is malfunctioning, and the VMS believes the UAV is slower than it actually is.	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
		V.12.5	The VMS provided the command, but the actuator performed the throttle reduction late. A mechanical malfunction of the actuator, such as a jam, prevented the throttle actuator from operating at the commanded time.	Actuators and cable linkages must be inspected regularly before flight. Additionally, there should be no loose items, or items that could become loose in flight, left in the aircraft that could interfere with operation of the UAV
The VMS provides a throttle setting to accelerate to a target speed, but the throttle is not reduced before reaching VNE	H6	V.13.1	The VMS provides the command to reduce the throttle, however it is not reduced. The wiring to the throttle actuator from the VMS is broken, preventing the actuator from receiving commands	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight
		V.13.2	The VMS recognized that the target airspeed was reached, however it did not provide the command to reduce the throttle. The autopilot is programmed with a large deadband around target airspeed to avoid overcontrol and the associated induced oscillations, however the target airspeed is near VNE, and the deadband	If target airspeed is not tightly controlled, the target airspeed must be sufficiently below VNE to avoid overspeeds

			allows the UAV to exceed VNE	
		V.13.3	The VMS received incorrect airspeed feedback due to a pitot-static system fault and did not recognize that target airspeed was reached	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
	H4	V.13.4	The VMS provided the command to reduce the throttle once target airspeed was reached, however the throttle was not reduced. The actuator linkage or cable is broken, and the throttle is no longer controllable	Actuators and cable linkages must be inspected regularly before flight
		V.13.5	The VMS provided the command to reduce the throttle once target airspeed was reached, however the throttle was not reduced. The power system did not provide power to the actuator due to a power system failure	Flight critical components such as actuators must have backup power so that the aircraft may be landed after a power system failure
The VMS provides a throttle setting to decelerate to a target speed, but the throttle is not increased before reaching stall speed	H4	V.14.1	The VMS provides the command to increased the throttle, however it is not increased. The wiring to the throttle actuator from the VMS is broken, preventing the actuator from receiving commands	Wiring and connections must be checked during preflight and should be designed to withstand vibrations associated with flight

		V.14.2	The VMS recognized that the target airspeed was reached, however it did not provide the command to reduce the throttle. The autopilot is programmed with a large deadband around target airspeed to avoid overcontrol and the associated induced oscillations, however the target airspeed is near stall speed, and the deadband allows the UAV to decelerate below stall speed	If target airspeed is not tightly controlled, the target airspeed should be sufficiently above stall speed to avoid stalls
		V.14.3	The VMS receives incorrect airspeed feedback due to a pitot-static system fault and does not recognize that target airspeed was reached	The pitot static system must be regularly inspected and the pitot tube should be clear of obstructions before launch
		V.14.4	The VMS provided the command to increase the throttle once target airspeed was reached, however the throttle was not increased. The actuator linkage or cable is broken, and the throttle is no longer controllable	Actuators and cable linkages must be inspected regularly before flight
		V.14.5	The VMS provided the command to increase the throttle once target airspeed was reached, however the throttle was not increased. The power system did not provide power to the actuator due to a power system failure	Flight critical components such as actuators must have backup power so that the aircraft may be landed after a power system failure

		V.14.6	The VMS provided the command to increase the throttle once target airspeed was reached, however the throttle was not increased. Engine failure occurred, not allowing the aircraft to accelerate	If engine failure occurs, the VMS must recognize the failure and provide attitude commands to avoid a stall

Appendix 3: STPA Compliance with MIL-HDBK-516C

Chapter 4 of MIL-HDBK-516C discusses the systems engineering criteria for airworthiness certification. This paper examines how STPA would provide the information required for each of the SE airworthiness criteria listed in the handbook, and more importantly ensure a safe aircraft design.

4.1 Design criteria.
4.1.1 Requirements allocation.
Criterion: Verify that the design criteria, including requirements and ground rules, adequately address airworthiness and safety for mission usage, full permissible flight envelope, duty cycle, interfaces, induced and natural environment, inspection capability, and maintenance philosophy.
Standard: Allocated high level airworthiness and safety requirements down through the design hierarchy are defined. Allocated design criteria for all system elements and components result in required levels of airworthiness and safety throughout the defined operational flight envelope, environment, usage and life.
Method of Compliance: Inspection of process documentation verifies allocation of airworthiness and safety requirements and design criteria. Traceability is documented among requirements, design criteria, design and verification. Consistency between design criteria and airworthiness and safety requirements is confirmed by inspection of documentation.

One of the inputs into an STPA analysis is the context within which the system operates. The context includes mission set, flight phases, operating environment, and maintenance and logistics support. Once the context is determined, the requirements generated by STPA for safe operation within that context flow from high level requirements to the subsystem and component levels. Traceability is a key component of STPA and flows through the analysis and products to operations. This traceability coupled with the systematic approach of STPA also ensures that critical safety requirements are not missed during the airworthiness certification inspection.

4.1.2 Safety critical hardware and software.
Criterion: Verify that airworthiness and safety design criteria are adequately addressed at component, subsystem and system levels, including interfaces, latencies, software and information assurance.
Standard: Safety critical software and hardware (including Critical Safety Items (CSIs)) are identified. Design criteria and critical characteristics of safety critical software and hardware are defined, substantiated and documented in sufficient detail to provide for "form, fit, function and interface" replacement without degrading system airworthiness. Design criteria and critical characteristics of safety critical software and hardware incorporate relevant security requirements and mitigation techniques needed to ensure safety of flight.
Method of Compliance: Inspection of documentation verifies that a process is in place to adequately identify safety critical software and hardware, CSIs, and associated design criteria and critical characteristics at the component, subsystem and system levels. Inspection of documentation verifies that safety critical software and hardware, CSIs, and associated design criteria and critical characteristics resulting from this process are documented. Inspection of documentation verifies that security requirements and mitigation techniques that affect flight safety are incorporated into safety critical software and hardware and CSIs.

Critical safety items are easier to identify with STPA because of the top-down approach. Rather than looking at all components to determine which ones are safety critical, STPA starts with the accidents and associated hazards and generates the scenarios that could cause the hazardous state to occur. These scenarios would illustrate which components or subsystems are most safety critical. Additionally, an STPA analysis provides information regarding the interfaces between the component and other elements in the system. If the safety constraints are implemented in the design, the system will be safe. As long as the new component meets the

same safety constraints as the previous component, the component will not degrade airworthiness. If the new component provides upgraded functionality, the original STPA analysis can be modified to determine safety of the upgraded component. STPA can also be used for software and information assurance. Another important and often overlooked interface is between the operator and the automation. STPA is designed to account for human and software interactions as well as component-level interactions.

4.1.3 Commercial derivative aircraft.
Criterion: Verify that, for commercial derivative air vehicles, the air vehicle's certification basis addresses all design criteria appropriate for the planned military usage.
Standard: Commercial derivative aircraft has been assessed for its suitability for the intended military application and determined to be airworthy and safe. Limitations appropriate to the intended military usage and environment are identified.
Method of Compliance: Inspection of certification data and analyses substantiates that the military air vehicle is airworthy and safe for its intended military usage and environments. Military air vehicle airworthiness certification data addresses all equipment, usage, and environments not covered by the commercial certification.

An STPA analysis can be completed using the commercial aircraft within the new operational context. In addition, the analysis will determine the safety of the integrated design of the commercial airframe with military mission systems.

Military missions are usually much more stressful on the aircraft and involve pushing the envelope more than the missions for which commercial aircraft are certified. The expected environment and stresses used during the commercial certification process may be different than that for military missions. STPA would consider the change in operations in the analysis.

In addition, commercial airworthiness standards like SAE ARP 4761 assume that pilots and maintainers do the right thing and do not consider the implications of human error on the design of the aircraft itself (not just the interface between the aircraft and the humans). STPA includes human behavior in airworthiness certification.

4.1.4 Failure conditions.
Criterion: Verify that safety of flight related failure conditions have been adequately addressed in the design criteria.
Standard: Safety of flight failure conditions (including applicable single point failures) have been identified. No single safety of flight failure condition results in a "Catastrophic" severity (i.e., death, permanent total disability, monetary loss equal to or exceeding $10 million or loss of air vehicle) with a frequency greater than "improbable" (i.e., a rate of less than one event per one million flight hours).
Method of Compliance: Inspection of the hazard analysis verifies that safety critical hazards have been identified and that catastrophic failures are no more frequent than improbable. Analysis of the design verifies that the required level of safety is achieved. Operating limitations are defined. The analysis includes ground rules and assumptions.

While STPA does not assign probabilities to safety conditions, if all of the requirements and constraints found via the analysis are implemented, either through system design or operational requirements, the safety of flight related failure conditions is adequately addressed.

Mishaps may occur when multiple failure conditions exist. In addition, particularly when software is involved, mishaps may result when nothing has failed and instead unsafe

interactions occur among functioning components. Commercial aircraft certification standards (such as SAE ARP 4761) do not include such considerations. STPA does.

4.1.5 Operating environment.
Criterion: Verify that the air system is designed to operate in the natural and induced environments for which it is intended.
Standard: The air system design criteria includes the intended natural and induced environments. The air system, including the air vehicle and control station equipment, is qualified to operate in the intended natural and induced environments (e.g., temperature, humidity, precipitation, icing, fungus, salt fog, particulate and liquid contamination, shock and vibration, and explosive atmosphere).
Method of Compliance: Inspection of documentation verifies that the air system intended natural and induced environments are documented. Analysis, demonstration and test verify that equipment provides required function and performance within the envelope of intended natural and induced environments without imposing a safety of flight risk. Inspection of qualification test results verifies that equipment is qualified for its intended environments.

STPA provides a procedure for identifying the operational context of the system and identifying the safety constraints associated with that environment. Additionally, STPA provides information to determine design tradeoffs as there may be some competing interests such as engine takeoff power and cruise performance or the location of displays. With STPA, the safety considerations for the decision are evaluated and once a decision is made, STPA can be used to minimize any induced safety concerns.

4.1.6 Flight and safety critical functions.
Criterion: Verify that the air systems design criteria identify flight and safety critical functions, and their degraded and failed modes and states. Verify that the air system and air vehicle detect and respond appropriately, predictably, safely and in a timely manner to flight and safety critical function degraded states or failures.
Standard: The design criteria identify flight and safety critical functions, modes and states for the air system, including the air vehicle.
The air system design criteria identify flight and safety critical function degraded states and failures.
The air system detects and responds appropriately, predictably, safely and in a timely manner to flight or safety critical function degraded states or failures.
The air vehicle detects and responds appropriately, predictably, safely and in a timely manner to air vehicle flight or safety critical function degraded states or failures, with or without operator intervention.
The air vehicle detects and responds appropriately, predictably, safely and in a timely manner to loss of flight and safety critical command and control data link(s) between the operator and air vehicle.
The air vehicle response to loss of command and control data link is appropriate and safe for the airspace in which the air system will be operated.
The air system detects and responds appropriately, predictably, safely and in a timely manner to the sense and avoid function for the airspace in which the air system will be operated, with or without operator intervention.
The air system (including air vehicle) responses to flight and safety critical function normal and degraded states or failures, and loss of flight and safety critical command and control data link(s):
a. Activate appropriately and in a timely manner,
b. Activate only when needed,
c. Safely transition to pre-determined modes and states (see also 6.2.2.4 of this document),
d. Activate pre-determined procedure(s) for restoring functionality,
e. Alert airspace control or air traffic control, as necessary, and
f. Prevent entry into pre-defined keep-out airspace or over-flight of pre-defined surface regions (see also 11.1.1.5 of this document).
(For information, see also 6.2; 8.3.10; 11.1.1 and 11.2.3; Section 15; and 17.2.9 of this document.)
Method of Compliance: Verification methods include analysis, test, simulation, demonstration, and inspection of documentation.
Inspection of documentation verifies that design criteria and processes identify flight and safety critical functions, modes and states; flight and safety critical functions degraded states and failures; and loss of flight and safety critical command and control data link(s).
Inspection of documentation verifies that design criteria and processes ensure air system responses are appropriate for the intended airspace.
Analysis verifies that flight and safety critical functions, modes and states for the air system, including the air vehicle, are identified.
Analysis verifies that flight and safety critical function degraded states and failures are identified.
A combination of ground testing and simulation verifies that the air system (including air vehicle) detects and responds appropriately, predictably, safely and in a timely manner to: (1) flight or safety critical function normal and degraded states or failures, with or without operator intervention, (2) loss of flight and safety critical command and control data link(s), and (3) sense and avoid function, with or without operator intervention. This testing and simulation verifies that the air system (including air vehicle) responses:
a. Activate appropriately and in a timely manner,

b. Activate only when needed,
c. Safely transition to pre-determined modes and states,
d. Activate pre-determined procedure(s) for restoring functionality,
e. Alert airspace control or air traffic control, as necessary, and
f. Prevent entry into pre-defined keep-out airspace or over-flight of pre-defined surface regions.

As aircraft systems become more complex, it is more difficult to fully understand all of the hundreds or thousands of potential failure states that are possible. This means that designing an aircraft to detect and appropriately respond to these failure states is equally difficult. STPA was designed for just this problem. STPA allows the designers to evaluate the emergent properties of the system as they design it to eliminate failure states or minimize the hazardous condition associated with system failures. This airworthiness criterion does not account for hazardous aircraft states that do not result from a component failure but rather, for example, missing cases or missing requirements or system engineering deficiencies. These properties are not identified by current bottom up hazard analysis techniques, but they are identified using STPA.

Additionally, flight and safety-critical functions are identified by STPA, and information from the STPA analysis will feed into the verification process for the safety-critical functions.

4.1.7 Flight termination system.
Criterion: Verify that the flight termination function, if incorporated into the design, is safe, secure and reliable.
Standard: Design criteria ensure that the flight termination function operates reliably and in a timely manner when commanded. The flight termination function results in a defined air vehicle flight state (e.g., zero lift, zero thrust). The likelihood of uncommanded flight termination is remote. A minimum of two operator actions is required to execute the flight termination function.
Method of Compliance: Inspection of documentation verifies that design criteria are in place to ensure that the flight termination function operates reliably and appropriately, and only when required. Inspection of test and simulation data verifies that the flight termination function operates appropriately, only when required, and results in the expected defined flight state(s). Inspection of analysis documentation indicates that the flight termination function operates reliably.

An STPA analysis of the flight termination function provides safety constraints to ensure safe function, which would include uncommanded flight termination and accidental flight termination by the operator. STPA does not determine likelihood of an uncommanded flight termination, however it would provide information to design a flight termination system with design constraints to prevent an uncommanded flight termination. The analysis will also verify the effectiveness of the two-operator action requirement. An STPA analysis provides data to the developmental test organization in order to properly test the functionality of the flight termination system. The analysis would also consider unintentional flight termination (commanded by pilot or operator, but did not intend to) and provide safety constraints to prevent such an occurrence.

4.2 Tools and databases.
4.2.1 Tool and database processes.
Criterion: Verify that all tools, methods, and databases used in the requirements management, design, risk control and assessments of safety are applied appropriately and exhibit accuracy commensurate with their application.
Standard: Processes are in place to ensure that all analysis, modeling and simulation tools and databases are of appropriate accuracy and fidelity, are validated for the intended applications, and are configuration controlled. Requirements definition/traceability, design and performance analysis tools, prediction methods, models and simulations are applied appropriately, and exhibit accuracy commensurate with their applications.

Method of Compliance: Inspection of documentation verifies that processes are in place to ensure that tools and databases are validated and under configuration control. Inspection of documentation verifies that analysis tools, models, simulations and databases are applied appropriately. Inspection of documentation verifies that analysis, modeling and simulation tools and databases are of appropriate accuracy and fidelity for the intended applications. Inspection of documentation verifies the validation basis of design analysis, models and simulations is substantiated and based on actual hardware/software test data.
Inspection of documentation verifies that the design analysis, modeling and simulation tools are substantiated by and based on actual test data (when available). Actual system verification results are compared with design analysis, modeling and simulation tool results and databases for validation purposes.

An STPA analysis of the tools and methods ensures that the correct information is provided to the system designers. Additionally, STPA will ensure that safety requirements definition and traceability are appropriate and accurate.

4.3 Materials selection.
4.3.1 Selection of materials.
Criterion: For Army and Navy air systems, verify that the material selection process uses validated and consistent material properties data, including design mechanical and physical properties such as material defects, and corrosion and environmental protection requirements (see also Section 19, Materials; Section 5, Structures; and Section 7, Propulsion; Section 8, Air Vehicle Subsystems of this document).
Standard: Material selection process uses materials covered by an industry specification, government specification (Military or Federal) or other specifications as approved by the procuring agency.
Method of Compliance: Inspection of documentation confirms that materials are adequately covered by either:
a. An Aerospace Materials Specification (AMS) issued by the SAE Aerospace Materials Division,
b. An ASTM standard published by ASTM International (formerly the American Society for Testing and Materials),
c. A government (Military or Federal) specification, or
d. Other specifications as approved by the procuring agency.
If an approved specification for the product is not available, an acceptable draft specification has been prepared.

An STPA analysis does not directly affect this requirement, however an STPA analysis may determine the critical areas for materials that require more attention.

4.4 Manufacturing and quality.
4.4.1 Key characteristics.
Criterion: Verify that key product characteristics (including critical characteristics) have been identified.
Standard: Physical characteristics which are key to the successful function of critical safety items (CSIs) and flight critical components are defined and documented. Tolerance allowances for each characteristic and traceability through the design hierarchy are defined, and the effects of adverse tolerance accumulation at higher (e.g., above the CSI) levels of product assembly are analyzed and reflected in the design documentation.
Method of Compliance: Key product characteristic (including critical characteristics) and tolerance definitions are verified by inspection and analysis of program design documentation at the applicable levels of the product hierarchy. Manufacturing process controls for specific key product characteristics identified as Critical to Safety (CTS) and manufacturing process parameters necessary to achieve and maintain acceptable process indices are verified by inspection and analysis of manufacturing process control documentation for the applicable stages of manufacture and assembly.

STPA will not determine the tolerances, but it will determine critical safety items and flight critical components. Additionally, STPA constraints will feed directly into the manufacturing process requirements.

4.4.2 Critical processes.
Criterion: Verify that all critical process capabilities exist to meet key product characteristic requirements (including critical characteristics).
Standard: All key characteristics (including critical characteristics) are mapped to corresponding critical processes. Critical process capabilities are characterized, process capability indices (Cpk) are calculated and acceptable limits established. Process control plans for critical processes are defined and implemented throughout the supply chain. For Army and Navy only, quality control procedures for critical processes are defined and implemented throughout the supply chain.

Method of Compliance: Critical process capabilities and control plans are verified by inspection of design documentation and process control documentation and if applicable, on-site audit documentation, throughout the supply chain.

The system's key product characteristic requirements can be analyzed via STPA to ensure that the processes are adequate to maintain safety.

4.4.3 Critical process controls.
Criterion: Verify that all critical process controls exist to assure key product characteristic requirements (including critical characteristics) are met.
Standard: Work and inspection instructions are defined, documented and implemented for all critical manufacturing processes. A process capability index (Cpk) of at least 1.67 is maintained for processes Critical to Safety (CTS) or processes that produce Critical Safety Items (CSI). Quantitative product quality criteria (i.e., product acceptance criteria) are defined and used for product acceptance at all levels of the product hierarchy up to and including the air system level.
Method of Compliance: Work and product inspection instructions, product acceptance criteria are verified by inspection. Cpk is verified by analysis and inspection of design documentation and manufacturing process capability data. Design conformance (i.e., "as built" configuration is in accordance with design requirements) is verified by first article inspections or first article tests, review of manufacturing process control data, and/or periodic hardware quality audits.
4.4.4 Quality system.
Criterion: Verify that the as-built configuration matches the as-designed configuration.
Standard: The quality system is effective in assuring conformance to product design and realization, including production allowances and tolerances. The quality system addresses defect prevention and achieving stable, capable processes. The quality system employs methods sufficient for conducting root cause analyses and implementing effective corrective actions.
Method of Compliance: Compliance is determined by inspection of the Quality System's policies, processes and procedures and examples of Material Review Board records.

The output of an STPA analysis are process controls. STPA can be used to ensure that process controls are adequate to maintain safety.

4.4.5 Nondestructive inspections.
Criterion: Verify that nondestructive inspection (NDI) processes have been validated to assure conforming parts.
Standard: Nondestructive inspection (NDI) methods and equipment have been qualified to suitable standards and meet the requirements of the applicable specification and application. The specification being used ensures any non-conformance adversely affecting the part will be detected. Accept and reject criteria for safety and flight critical hardware are based on validated models and data.
Method of Compliance: Compliance is determined by inspection of NDI process, selection criteria, operator certification and method validation documentation. For new applications of specifications, test and inspection data confirms the inspection method is valid for the application.

The STPA analysis will feed into the NDI processes. It will identify flight critical hardware and will be used to ensure that the NDI processes provide the adequate feedback to maintain flight safety. Specific methods and equipment may be identified based off of the safety constraints.

4.4.6 Control of Safety-Related Articles.
Criterion: Verify that safety-related items (Critical Safety Items, flight critical components, and components containing critical characteristics that impact safety) conform to their approved design.
Standard: The quality of safety-related items, whether furnished by the prime contractor, supplier, or sustainment organization, is controlled to ensure conformance with design. The manufacturers of the items have instituted manufacturing process controls inspections, and testing procedures to ensure each safety-related product or part conforms to its approved design.
Method of Compliance: For safety-related items, initial design conformance is verified by inspection of First Article Inspection reports, First Article Test reports, and other manufacturing records that prove design conformance. Controls for ensuring the quality of safety-related items are verified by inspecting manufacturing process control plans (including work instructions) and inspection and test procedures.

An STPA analysis of the manufacturing process will identify appropriate controls and ensure that they are in place and that the communication between the design team and the manufacturer is adequate to make sure that the manufacturer has the correct technical data. The STPA analysis will also analyze feedback channels from the manufacturer to the design team.

4.5 Operator's and maintenance manual/technical orders.
4.5.1 Procedures and limitations.
Criterion: Verify that processes are in place to identify and document normal and emergency procedures, limitations, restrictions, warnings, cautions and notes.
Standard: Operator handbooks or manuals identify all normal and emergency procedures, limitations, restrictions, warnings, cautions and notes. Warnings, cautions and notes are identified in such a manner as to attract attention and set them apart from normal text. When an unsafe condition is detected and annunciated, the operator's manual has clear and precise corrective procedures for handling the condition.
Method of Compliance: Inspection of operator handbooks or manuals process documentation describes procedures for developing normal and emergency procedures, limitations, restrictions, warnings, cautions and notes from system technical data. Process descriptions include methods for updating this information as needed. For Army and Navy, inspection of operating handbooks and manuals verifies that they include all normal and emergency procedures, limitations, restrictions, warnings, cautions and notes. The USAF confirms operator manual accuracy and completeness through other sections contained within this document.

STPA provides inputs to the technical orders (TOs) for the system. If a potential safety hazard is not designed out of the system, STPA can provide operational or maintenance constraints that would be included in the TO as a procedure or as a caution/warning.

4.5.3 Maintenance of safety.
Criterion: Verify that procedures are in place for establishing and maintaining air system flight safety, as affected by product design changes, safety issues, changes in operations, maintenance, transportation or storage.
Standard: Processes are defined, documented, and implemented to establish and accomplish timely updates to operator and maintenance manuals as made necessary by product design changes, identified safety issues (e.g., Category I Deficiency Reports), changes in operational concepts, usage, maintenance concepts, transportation, or storage. Current updated technical data are used to effect technical manual revisions. Maximum timelines to incorporate changes in manuals are based on the effect of the change and the severity of the identified hazard.
Method of Compliance: The adequacy of establishment and change processes for operator and maintenance manuals is verified by inspection of process documentation. Inspection of examples of revised operator and maintenance manuals (i.e., change pages) verifies traceability to change events.

All systems that are in operation for a significant amount of time undergo changes either to the system itself or to the context in which it operates. These changes, without an accompanying change to the safety control structure, can lead to accidents. An organizational safety control structure for the operational phase will model the support system, but must be updated to ensure continued control. An STPA analysis of the support system will verify that the procedures in place for maintaining flight safety are appropriate. As changes are made to either the system itself (upgrades) or to the operational environment (new mission set, new operating location) the analysis will be modified to ensure that the safety controls are still adequate, or determine new safety constraints to meet the updated needs of the system. The traceability inherent in the STPA process assists with identifying the safety impacts of changes.

Another output of STPA is an operational safety management plan. This plan "is used to guide the operational control of safety".

Additionally, STPA has been used to identify leading indicators of increasingly risky behavior so that they are monitored and used to avoid mishaps as changes occur.

4.6 Configuration management (CM).
4.6.1 Functional baseline.
Criterion: Verify that the functional baseline is established and under configuration control to preclude unauthorized changes.
Standard: The functional baseline is properly documented, approved and brought under control by a Configuration Management Process.
Method of Compliance: The Configuration Management Plan (CMP) is defined and implemented in accordance with the contract. Inspection of documentation verifies that the functional baseline has been documented and approved.

The STPA analysis would be controlled through the CMP along with all other models. An STPA analysis can provide data to the CMP to ensure that the configuration is properly controlled.

4.6.2 Allocated baseline.
Criterion: Verify that the allocated baseline is established and under configuration control to preclude unauthorized changes.
Standard: The allocated baseline is properly documented, approved and brought under control by a Configuration Management Process.
Method of Compliance: The Configuration Management Plan is defined and implemented in accordance with the contract. Inspection of documentation verifies that the allocated baseline has been documented and approved. Inspection of the engineering release documentation verifies adequate capture of the allocated baseline.

The STPA analysis would be controlled through the CMP along with all other models. An STPA analysis can provide data to the CMP to ensure that the configuration is properly controlled.

4.6.3 Product baseline.
Criterion: Verify that the product baseline is established and under configuration control to preclude unauthorized changes.
Standard: The product baseline is properly documented, approved and brought under control by a Configuration Management Process.
Method of Compliance: The Configuration Management Plan is defined and implemented in accordance with the contract. Inspection of documentation verifies that the product baseline has been documented and approved. Inspection of the approved engineering documentation and engineering release system verifies adequate capture of the product baseline.

An STPA analysis of the Configuration Management Process will identify if the process is adequate to control the configuration of the system. Additionally, the STPA models should be controlled by the CMP.

4.6.4 Safety critical item configuration management.
Criterion: Verify that all safety-critical items are tracked and under configuration control.
Standard: A configuration status accounting (CSA) system is adequately documented and maintained and tracks the configuration of safety-critical items.
Method of Compliance: CSA process documentation is verified by inspection. Inspection of CSA records and reports for CI/CSCIs verifies accuracy of the configuration status accounting system and that the system is able to track and record changes to the configuration.

STPA can be used to identify safety-critical items. Any changes to the items or how they are used in the aircraft system can be easily analyzed with updated data to ensure that the results of the changes are fully understood and that the safety control structure still adequately controls system safety.

Chapter 14 of MIL-HDBK-516C covers system safety.

14.1.1 System safety process.
Criterion: Verify that an effective system safety program is implemented that mitigates risks/hazards attributed to hardware, software, and human system integration and that the safety program documents and tracks the risks/hazards of the design/modification.
Standard: The system safety program meets the minimum mandatory requirements of MIL-STD-882 (e.g., system safety approach has been documented; hazards have been identified; hazards have been assessed; hazards have been mitigated; residual risks are at an acceptable level; residual risk has been accepted by appropriate authority; and hazards and residual risk have been tracked), and the system safety requirements are incorporated into the technical and programmatic documents. The Programmatic Environmental Safety and Health Evaluation (PESHE) includes all hazards identified for the program.
Method of Compliance: Verification method includes inspection of documentation. Effectiveness of the system safety program is verified by inspection of technical and programmatic documents to verify: system safety approach has been documented; hazards have been identified; hazards have been assessed; hazards have been mitigated; residual risks are reduced; residual risk has been accepted by appropriate authority; and hazards and residual risk have been tracked. Inclusion of Environmental Safety and Occupational Health (ESOH) hazards in PESHE is verified by inspection.

STPA documentation would provide the inspector all of the information needed to ensure compliance with the system safety process. Additionally, the inspector would able to tell quickly that appropriate hazards have been identified because STPA refines hazards from a small set of high-level hazards (compared to dozens or hundreds of hazards that are found in some analyses) so that review is optimized. STPA has been shown to comply with MIL-STD-882 and, in fact, was created with that goal in mind.

14.1.1.1 System safety requirements.
Criterion: Verify that the system safety program incorporates system safety into all aspects of systems engineering throughout all acquisition phases.
Standard: System safety requirements are incorporated into the system technical and programmatic documents. System safety requirements, analyses, time lines and other milestones are in synchronization with the rest of the program schedules.
Method of Compliance: Verification method includes inspection of documentation. Incorporation of system safety requirements into the systems technical documents, programmatic documents and operating procedures is verified by inspection. Integration of system safety requirements,

A high-level STPA analysis on a proposed new system can be conducted by the program office and that information should be incorporated into system requirements along with the technical requirements. The lower-level analyses can be synchronized with the lower-level design of the system once the contract has been awarded and the contractor develops the system. The timelines of the safety analysis would therefore match the design timelines.

As stated previously in the analysis of Chapter 4, an output of STPA is a set of operational constraints (safety requirements) that will affect operating procedures. Additionally, any known operating procedures should feed into the scenario generation portion of STPA, verifying the safety of those procedures. For instance, a new refueling aircraft most likely will be expected to conduct procedures similar to refueling aircraft currently in the inventory.

14.1.1.2 System safety analysis and assessment.
Criterion: Verify that appropriate system safety analysis and assessment tasks are accomplished for all programs, including temporary and permanent modifications.
Standard: System, subsystem, component and software safety analyses and assessments are accomplished for all programs, including temporary and permanent modifications. Design and operational/maintenance procedures do not have an unacceptable negative effect on system safety or on the mishap risk baseline.
Method of Compliance: Verification method includes inspection of documentation. Accomplishment of appropriate system, subsystem, component and software safety analyses and assessments for all programs, including temporary and permanent modifications is verified by inspection, and any change

STPA works very well for modifications to the system and for operational and maintenance procedures. A completed STPA analysis can be updated for system modifications in order to understand the effects of the modification on the system and design the modification to avoid introducing hazards to the system.

If a modification is a COTS product, the integration of the product with the airframe will be analyzed to ensure that it is safe. The product itself most likely will not be redesigned based on the STPA results, but safety constraints for the integration or for the airframe will be identified. Additionally, if PO does not want to implement the safety constraints, they may determine that the COTS product is unsuitable and look for other options.

14.1.1.3 Hazard/risk tracking and risk acceptance.
Criterion: Verify that hazards/risks are tracked and residual risks documented.
Standard: Hazard/risk tracking and residual risk documentation and acceptance are planned, documented and accomplished in accordance with MIL-STD-882. Risks are presented and accepted at the appropriate level and risk acceptances are documented in a hazard tracking system.
Method of Compliance: Evidence of the closed loop hazard tracking system

A hazard list is the second step of a STAMP analysis. Further analysis builds off of the hazard list. In current AF practice, the level of risk acceptance is based on residual risk level (low, medium, high). STPA does not provide probability of occurrence, therefore risk acceptance level must be addressed differently. If the safety constraints for an associated hazard are addressed, the hazard will be appropriately mitigated.

14.1.1.4.1 Flight safety.
Criterion: Verify that the system safety program addresses flight safety.
Standard: Single point failures that result in loss of aircraft or system do not occur at an unacceptable rate (e.g., improbable or lower probabilities in accordance with MIL-STD-882). Safety design deficiencies uncovered during flight mishap investigations or in deficiency reports (e.g., Materiel Deficiency Reports (MDRs), Quality Deficiency Reports (QDRs)) are assessed and residual risks identified. Flight hazard risks for the system do not exceed threshold limits that are established for the program.
Method of Compliance: Verification methods include analysis and inspection of documentation. Evidence of a flight safety process is verified by: review of all hazards associated with single point failures to document their elimination or reduction of risks to an acceptable level; by inspection of design deficiencies identified in flight safety reports and deficiency reports (e.g., MDRs, QDRs) to assure they are assessed and resolution actions are tracked to closure; by analysis that actual flight mishap rates comply with pre-set program threshold limits.

STPA inherently address flight safety. Single point failures will be identified in the analysis and eliminated with safety constraints. Deficiency reports must feedback into the STPA analysis. These reports may provide additional scenarios that were not considered in the original analysis, or even a hazard that was not originally included. The analysis must be modified to include the deficiencies discovered during flight test or operations once the system is fielded. STPA will identify more than single point failures and even hazards that do not arise from component failures but from unsafe interactions among components.

14.1.1.4.2 Foreign Object Damage (FOD) prevention.
Criterion: Verify that the system safety program addresses ground/industrial safety (foreign object damage prevention).
Standard: Ground/Industrial safety requirements are established for activities at the plant to minimize the risk of Foreign Object Damage (FOD) or undetected damage to the assembled air vehicle and all required support equipment.

Method of Compliance: Verification method includes inspection of documentation. Evidence of an established FOD prevention program is verified by review of FOD program documents and inspection of reports, or on-site certification by the Defense Contract Management Agency (DCMA) that an acceptable FOD program exists.

An STPA analysis of the FOD program may yield additional safety constraints to prevent FOD. Additionally, the STPA analysis on the aircraft should consider FOD in the scenarios to ensure that if an aircraft is damaged by FOD, the damage does not result in an accident.

14.1.1.4.3 Explosives and ordnance safety; non-nuclear munitions.
Criterion: Verify that the system safety program addresses explosives and ordnance safety; non-nuclear munitions.
Standard: Requirements for system safety processes and analyses are established in accordance with MIL-STD-882 to support weapons testing, certification, and obtainment of explosive hazard classifications.
Method of Compliance: Verification method includes inspection of documentation. Safety program requirements for explosives and ordnance safety are verified by inspection of system safety program analysis data.

STPA does not directly support explosives safety, however an STPA analysis of the explosives safety program may provide additional constraints to prevent an accident.

14.1.1.4.4 Range safety.
Criterion: Verify that the system safety program addresses range safety.
Standard: The system safety program is responsive to test range safety requirements and official requests for safety analysis information.
Method of Compliance: System safety program support for range safety is verified by inspection of system safety process documentation.

STPA can include range safety requirements as an input into the analysis. STPA will provide additional constraints as necessary to prevent an accident.

14.1.1.4.5 Nuclear safety.
Criterion: Verify that the system safety program addresses nuclear safety.
Standard: The nuclear safety program adheres to the four key DoD Nuclear Weapon System Safety Design Standards for hardware and software.
Method of Compliance: Verification method includes inspection of documentation. Evidence that a process is in place to incorporate the four key nuclear safety design requirements into the safety analyses, program functional baselines and other design requirements is verified by inspection of program safety documents and functional baselines.

STPA starts from hazards and system behavioral constraints, which can be the four nuclear safety standards. These requirements are then a direct part of the STPA analysis.

14.1.1.4.6 Radiation/LASER (light amplification by stimulated emission of radiation) safety.
Criterion: Verify that the system safety program addresses radiation/laser safety.
Standard: Key design requirements for radiation/laser safety are established including: protective housing; safety interlocks; remote interlock connector; key control/arming device; emission indicator; beam stop/attenuator; location of controls; viewing optics; scanning safeguard; manual reset; labeling requirements; laser classification; hazard evaluation; protective eyewear; laser area control; and informational requirements.
Method of Compliance: Verification method includes inspection of documentation. Evidence of a process to establish the key safety design requirements for radiation/laser safety is verified by inspection of safety analyses, design specifications and program functional baselines.

STPA can include radiation and laser design requirements in the analysis. The effectiveness of the design requirements will also be evaluated, and additional constraints may be found.

14.1.1.4.7 Test safety and support.
Criterion: Verify that the system safety program addresses test safety and support.
Standard: System safety organization actively participates in test planning and post-test reviews to analyze all test-related hazards and recommended corrective actions to ensure hazard closeout or mitigation. Appropriate system safety requirements criteria are incorporated into the test program for validation and verification.
Method of Compliance: Verification method includes inspection of documentation. System safety support of the test and evaluation process and incorporation of safety requirements criteria are verified by inspection of the system safety program plan, test-related hazard analyses and the Test and Evaluation Master Plan (TEMP).

The STPA results directly apply to test safety planning. Additionally, the developmental test program will verify that the safety constraints identified are met by the designed system. Any safety findings will be provided to the designers to update the STPA analysis.

The Air Force Test Center is currently undergoing a trial using STPA for test planning. Utilizing STPA in the design process and developmental test will provide synergy to the entire acquisitions development process.

14.1.1.4.8 Software safety.
Criterion: Verify that the system safety program addresses software safety.
Standard: See 14.3 (this document) and subparagraphs.
Method of Compliance: Methods of Compliance for Software Safety are contained in 14.3 (this document) and subparagraphs.

Most software safety programs focus on assurance of the implementation of the software requirements. However, virtually all accidents involving software stem from flawed (unsafe) requirements and not from the implementation. STPA identifies the safety-critical software requirements that need to be implemented in the software. See 14.3 below.

14.1.1.4.9 Material changes/deficiencies.
Criterion: Verify that the system safety program addresses materials.
Standard: Risks associated with use of new/alternate/substituted/hazardous materials or material deficiencies do not exceed the hazard baseline set for the program.
Method of Compliance: Verification method includes inspection of documentation. Evidence of a material safety process is verified by inspection of program safety documentation and safety analyses. Cumulative risks of identified hazards do not exceed the program's hazard baseline.

STPA does not directly address materials, as explained in the discussion of 4.3, but the analysis would identify critical safety components that require specific attention.

14.1.1.4.10 Failure Modes and Effects Testing (FMET) and Built-In-Test (BIT).
Criterion: Verify that the system safety program addresses FMET and BIT.
Standard: System safety participates in all tests/test planning on parts and assemblies that establish failure modes and rates, and conducts safety analyses on all built-in test equipment to assure that integration into a system does not induce hazards which exceed the hazard baseline set for the program.
Method of Compliance: Verification method includes inspection of documentation. Evidence of system safety support of FMET and BIT evaluations is verified by inspection of the system safety program documents, test documents and the hazard tracking data base.

Complex systems often have more potential failure modes than can be tested in a timely manner, and not all failure modes will be understood during the design phase, meaning they cannot be tested until they are discovered. Discovery may not occur until the system is fielded and has been operating for a significant amount of time. The undiscovered failure mode (often

called an “unknown unknown”) may cause an accident resulting in loss of life and property. The late discovery may also result in standing the system down until the failure is investigated and expensive modifications to prevent future mishaps.

STPA will provide safety constraints to design the system such that if a failure occurs it does not result in the realization of a hazard. The safety constraints will also mitigate potential failures. STPA essentially provides a way to discover “unknown unknowns” during the development process.

The safety constraints provided by STPA will also be an input into the FMET procedures. System failures will be tested and safety constraints verified.

STPA scenarios will also consider BIT in the system design and provide safety constraints to prevent BIT from inducing hazards.

14.1.1.4.11 Fail-safe design.
Criterion: Verify that the system safety program addresses fail-safe design.
Standard: Design ensures that the system remains inherently safe. A single failure causes the system to revert to a state which will not cause a mishap. Flight hazard risks for the system do not exceed threshold limits that are established for the program.
Method of Compliance: Verification method includes inspection of documentation (e.g., safety analyses, technical documentation, testing documentation, hazard tracking data base). Design documentation verifies: inherent system safety; that a single failure will not cause the system to revert to a state which will result in unacceptable risk of a mishap; and that flight hazard risks for the system do not exceed the threshold limits established for the program.

STPA will provide safety constraints to reduce or eliminate system states that result in a hazard. The STPA documentation will provide the airworthiness inspector with the information required to verify compliance.

STPA also evaluates hazards that occur without a failure. Many incidents occur when the system operates as designed – STPA should be used during the design process to ensure that it is designed to operate safely.

14.1.1.4.12 Safety assessment of support equipment.
Criterion: Verify that the system safety program addresses support equipment.
Standard: Design related hazards and interfaces of support equipment with aircraft and control stations are included in system safety analyses. Identified safety hazards are resolved or risks reduced to an acceptable level before first test use or first operational use of the support equipment.
Method of Compliance: Verification method includes inspection of documentation. The incorporation of design safety requirements for support equipment into technical document baselines/safety documents and the elimination or control of their associated safety risks is verified by inspection of technical documents baselines, safety process documentation, safety analyses and the closed loop hazard tracking system.

The support structure can be analyzed using STPA to include support equipment, maintenance and logistics practices. Just as with the actual system under design, test results regarding the support equipment must be fed back to the program office to ensure the support equipment is safe and meets the requirements for the system.

14.2 Safety design requirements.
14.2.1 Hazard identification/control/resolution process

Criterion: Verify that a systematic process is employed that provides for hazard identification, hazard control requirement generation and implementation, and residual risk assessment.
Standard: A process is in place to identify and characterize hazards, devise corrective actions, and assess residual risks. A System Safety Group is established to implement the process
Method of Compliance: Verification method includes inspection of documentation. Evidence of a hazard identification/control/resolution process is verified by inspection of safety process documentation and review of safety analyses and system safety group proceedings.

STPA is a systematic process that identifies hazards and devises corrective actions (safety constraints). Residual risk is not calculated, but if a constraint is not implemented there will be risk inherent in the design.

14.2.2 Mitigation of mishap risks.
Criterion: Verify that the design is free from unacceptable mishap risk, including risks to third parties.
Standard: Unacceptable risks to personnel or equipment are eliminated or controlled in accordance with MIL-STD-882. Mishap risk determination, including risk to third parties, reflects the current configuration and maturity of the system. Mishap risk acceptability is based on the intended airspace operations, including rules and restrictions for such airspaces.
Method of Compliance: Verification method includes inspection of documentation. Evidence of a process to mitigate hazards with "unacceptable" mishap risk is verified by inspection of system safety documents, technical documents, test documents, programmatic documents, safety hazard tracking database and the residual risk acceptance process.

STPA will identify risks based on intended operations and system design. Rather than provide a probability, STPA generates the causal scenarios leading to a mishap so that they can be eliminated or controlled in accordance with good safety engineering practices (and MIL-STD-882). Probabilities do not provide the information needed to eliminate or control hazards. “Unacceptable” risk is most likely determined by probabilistic risk assessment, which is not a component of STPA. However, any scenario that is found by STPA must be resolved otherwise there is residual risk associated with the design. The inspector would use the STPA documentation to verify the safety of the design. There is no way, with any hazard analysis method, to verify that the system is completely free from mishap risk, however STPA will provide more complete coverage across potential mishap risks such as component failure, software requirements and interactions, human interaction, and support structure.

14.2.3 Single point failure assessment.
Criterion: Verify that no single-point failure unacceptably affects the safety of the system.
Standard: The risks of all hazards associated with single point failures do not exceed the hazard baseline set for the program. Residual risk is accepted in accordance with MIL-STD-882.
Method of Compliance: Verification method includes inspection of documentation. Evidence that the risks of all single point failure hazards do not exceed the hazard baseline set for the program and that the residual risk has been accepted is verified by inspection of the safety analyses for single point failures and the relevant data in the closed loop hazard tracking system.

An STPA analysis includes component failures, and would identify potential scenarios for a single point failure to cause a hazard. The scenarios would then be used to determine safety constraints to prevent the hazard. However, STPA handles more than just single-point failures.

14.2.4 Subsystem protection.
Criterion: Verify that the design adequately protects the power sources, controls, and critical components of redundant subsystems.
Standard: Power sources, controls, and critical components of redundant subsystems are separated/shielded per the general safety requirements of MIL-STD-882.

Method of Compliance: Verification method includes inspection of documentation. Inspection of safety analyses/assessments and associated documentation verifies that power sources, controls, and critical components of redundant subsystems are separated/shielded per the general safety requirements of MIL-STD-882.

STPA examines component and subsystem interactions. The analysis will identify any hazards associated with power sources, controls, or redundant subsystems. The analysis will also assist in determining how the subsystems should be designed for redundancy, or if other methodologies to protect the subsystems are appropriate.

14.2.5 Human factors.
Criterion: Verify that all aspects of human factors are addressed and unacceptable human factors safety issues/risks are resolved in the design process.
Standard: Establish human factors design requirements interface with system safety to minimize the probability of human error and satisfy the intent of MIL-STD-882.
Method of Compliance: Verification method includes inspection of documentation. The standard to establish human factors requirements and identify safety issues/risks related to human factors and reduce them to an acceptable level is verified by inspection of safety documentation, safety analyses and program functional baselines.

STPA provides human factors safety constraints. Human operators are included in the analysis so that the system is designed for the human operator to provide safe commands and receive accurate and adequate feedback in order to determine what commands are safe.

14.2.6 Human error.
Criterion: Verify that the system is produced/manufactured ensuring risk reduction of failures or hazards potentially created by human error during the operation and support of the system.
Standard: System design minimizes risk created by human error in the operation and support of the system.
Method of Compliance: Verification method includes inspection of documentation. Evidence that a process is in place to reduce the mishap risks associated with human error to acceptable levels is verified by inspection of safety documents and analyses and review of the closed loop hazard tracking system.

The human factors safety constraints provided by STPA would reduce the potential for human error to cause a hazard.

14.2.7 Environmental conditions.
Criterion: Verify that the system design is within acceptable risk bounds over worst-case environmental conditions.
Standard: Safety risks due to system exposure/operation in required environmental conditions are defined and verified to be within acceptable limits.
Method of Compliance: Verification method includes inspection of documentation. Evidence that the safety risk minimization process addresses effects of worst-case environmental conditions on the design is verified by review of safety analyses and environmental/climatic test results/reports.

STPA considers the context of the system, which includes how the system is to be operated and the operational environment. The analysis will ensure that the environmental limits are appropriate and if the system is exposed to severe or worst case environmental conditions, the result is not a mishap.

If the environment of the system changes, for instance it deploys to an area of the world not initially intended, a revised analysis considering the new environmental changes should be conducted.

14.2.8 Assembly/installation hazards.
Criterion: Verify that personnel exposure to hazards during the installation process, including hazards due to locations of systems in the air vehicle, is at an acceptable risk level.
Standard: A safety process is in place to prevent errors in assembly, installation, or connections which could result in a safety hazard or mishap for the system.
Method of Compliance: Verification method includes inspection of documentation. Design and procedural safety requirements acceptability is verified by inspection and approval of system safety documentation and requirements. Evidence of acceptability/approval is provided by inspection of equipment installation, operation and maintenance process documentation.

STPA can be directly applied to the manufacturing, operation, and maintenance of a system. The system design can provide a safer process for manufacturing, operation and maintenance. Additionally an analysis of the organizational structure surrounding the design, manufacturing, operation, and maintenance functions will ensure that the interactions between the functions are safe.

14.2.9 Safety design process.
Criterion: Verify that the system design isolates hazardous substances, components, and operations from other activities, areas, personnel, and incompatible material.
Standard: A safety design process is in place to isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.
Method of Compliance: Verification method includes inspection of documentation. The standard to assure that hazardous substances, components and operations have been identified and corrective measures taken (e.g., separation, shielding, isolation), and/or risks reduced to an acceptable level for the program, is verified by review of safety analyses and program technical documentation.

STPA analysis would provide safety constraints to meet this criterion. Exposure to hazardous substances or processes would be considered a hazard in the analysis and safety constraints identified to prevent the hazard.

14.2.10 Analysis of changes or modifications.
Criterion: Verify that a system safety change analysis is accomplished on changed or modified equipment or software.
Standard: All changes/modifications to existing systems do not:
a. create new hazards;
b. affect a hazard that had previously been resolved;
c. increase the risk of any existing hazards;
d. adversely affect any safety-critical component.
Method of Compliance: Verification method includes inspection of documentation. Inspections of system safety change analyses on changed or modified equipment or software. Verify that no changes/modifications to existing systems will cause any of the following:
a. create new hazards;
b. affect a hazard that had previously been resolved;
c. increase the risk of any existing hazards;
d. adversely affect any safety-critical component.

STPA can be used to design the modification to prevent introducing new hazards to the system. If the modification is already designed (such as a COTS product), an analysis of the modification will determine if it introduces safety hazards and provide interface or system redesign recommendations to mitigate the hazard. The traceability inherent in the STPA results will minimize the amount of effort to analyze changes and modifications.

14.2.11 Assess safety of operational contingencies.
Criterion: Verify that the system provides and implements operational contingencies in the event of catastrophic, critical and marginal failures or emergencies involving the system.
Standard: In the event of catastrophic, critical and marginal failures or emergencies the system provides and implements operational contingencies by transitioning to a pre-determined and expected state and mode.

Method of Compliance: Verification method includes inspection of documentation. Inspections of safety analyses *v*erify which catastrophic, critical, marginal failures, and other system emergencies require operational contingencies. Inspections of design documentation *v*erify that, in the event of the identified failures or emergencies, the system provides and implements operational contingencies by transitioning to a pre-determined and expected state and mode. Inspection of system safety documentation verifies that operational contingencies have been approved.

An STPA analysis of the transition to backup modes during system emergencies can ensure safe continued operation of the system during contingencies. It will include more than just failures, i.e., it also considers design errors. Implementing safety constraints during the system design will therefore minimize the occurrence of system emergencies.

14.2.12 Safety assurance for special military modes of operation.
Criterion: Verify that special military modes of operation when inactive do not reduce the UAS below threshold safety levels.
Standard: Special military modes of operation of UAS (e.g., weapons or stores arming and release or operation of electromagnetic spectrum emitters) when inactive (e.g., a jammer in standby mode) meet probability of failure and design and development assurance requirements through physical/functional segregation and design.
Method of Compliance: Verification method includes inspection of documentation. Inspections of programmatic, system safety and software safety documents.
Criterion: Verify that special military modes of operation of UAS (e.g., weapons or stores arming and release or operation of electromagnetic spectrum emitters) when inactive (e.g., a jammer in standby mode) meet probability of failure and design and development assurance requirements through physical/functional segregation and design.

STPA will identify safety hazards associated with military modes on UAS and provide safety design constraints to mitigate the hazards.

14.3.1 Comprehensive approach to software safety.
Criterion: Verify that a comprehensive software safety program is integrated into the overall system safety program.
Standard: A comprehensive software safety program is integrated into the system safety program by ensuring the following:
a. Adequate planning for software safety tasks;
b. Adequate planning for analysis, traceability and testing is documented in safety management plans and test plans;
c. Active participation of software safety in engineering processes/events (i.e., peer review, change boards, deviation processing etc.);
d. Inclusion of software safety in the software development process and products;
e. System safety allocates safety requirements to software safety in a timely manner;
f. System/software hazard analyses substantiate that no single point failure caused by software results in loss of aircraft or system;
g. Software causes of and mitigations for the system hazards are identified and integrated into the system safety process (i.e., hazard reports, hazard tracking system etc.);
h. Software safety recommends system safety requirements to system safety in a timely manner;
i. Systems engineering receives the final software safety input from system safety in a timely manner;
j. Software integrity levels are established and enforced for the program in accordance with prescribed industry standards;
k. Safety designated functions and their associated safety designated software are identified and analyzed;
l. Test plans and procedures include testing of software safety functional requirements and design requirements.
NOTE: The preceding should not be considered to be an all-encompassing exclusive list, and may be expanded depending on program scope and complexity.
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of program safety, software safety, and software documentation that the comprehensive software safety program has been integrated into the system safety program in a manner which meets the standard.

STPA provides software safety requirements. These requirements are traceable and the STPA artifacts serve as documentation of the analysis. The data from the analysis should feed into test plans. The STPA software safety requirements will be determined during the analysis along with all other safety requirements and meet criteria such as reducing single point failures, and tracking software hazards recommending safety requirements.

STPA does not differentiate between hardware and software hazards, and in fact they are related as the software often controls hardware. Treating hardware hazards and software hazards as two different problems to solve reduces the likelihood of solving software/hardware interaction hazards.

14.3.2 Planning/accomplishing software safety analyses and assessments.
Criterion: Verify that the software safety program requires that appropriate software safety-designated analyses be performed as part of the software development process and *v*erify accomplishment of related assessment tasks.
Standard: A tailored set of analyses and assessments (or equivalent) required by the references of 14.3 (this document) is planned for and accomplished.
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of system safety, software safety, and software documentation that the tailored set of analyses and assessments (or equivalent) required by the references of 14.3 (this document) are planned for and accomplished.

The STPA artifacts will provide documentation that a software safety analysis is accomplished.

14.3.2.1 Performance of software safety analyses.
Criterion: Verify that the required software safety analyses preparation is accomplished.
Standard: The types and quantities of required software safety analyses are prepared and provided in accordance with planning for software safety. Software safety analyses and assessments include the tailored documentation required by the references of 14.3 (this document).
Method of Compliance: Verification method includes inspection of documentation.
Criterion: Verify by inspection that the delivered software safety analyses for the program have a complete systems view, including identification of software hazards, and associated software risks.

An analysis using STPA will be in compliance with this criterion. Additionally, STPA artifacts will provide documentation for the airworthiness certification inspector to verify that the program is in compliance.

14.3.2.2 Performance of software safety traceability analyses.
Criterion: Verify that the required software safety traceability analyses are accomplished.
Standard: System safety requirements allocated to software are refined using appropriate analyses to allocate the system safety requirements to the software requirements, and bi-directional traceability to the identified hazard(s) is accomplished. Appropriate analyses include the tailored documentation required by the references of 14.3 (this document).
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of system safety, software safety and program documentation that the bi-directional software safety traceability analyses amongst requirements, design, implementation, verification, and hazard have been accomplished.

A key component of STPA is traceability. Each safety constraint is directly tied to a hazard and is documented in the analysis. Traceability in STPA goes from the system-level hazards down to the specific design techniques used to mitigate those hazards.

14.3.3 Evaluation of software for elimination of hazardous events.
Criterion: Verify that the design/modification software is evaluated to ensure controlled or monitored functions do not initiate hazardous events or mishaps in either the on or off (powered) state.
Standard: The software as designed or as modified does not initiate hazardous events in either the on or off (powered) state.
Method of Compliance: Verification methods include analysis, test, and inspection of documentation. Verify that a system safety assessment is accomplished which includes evaluation of software and identification of anomalous software control/monitoring behavior to assure the software as designed or as modified does not initiate relevant hazardous events.

This criterion describes what STPA is designed to do: identify hazards and control the function of the system to avoid those hazards.

14.3.4 Commercial off-the-shelf software integrity level confirmation.
Criterion: Verify that Commercial Off-the-Shelf (COTS) and reuse software (which includes application software and operating systems) are developed to the necessary software integrity level.
Standard: The software criticality level for COTS and reuse software functions has been determined and their development has been confirmed to be at the required software integrity level as defined by software and/or safety planning.
Method of Compliance: Verification methods include inspection of documentation. Verify by inspection of program, system safety, software safety and software engineering documentation that the software criticality level for COTS and reuse software by function is determined. Verify that the software is developed to the required software integrity level as defined by software and/or safety planning.

STPA does not support confirmation of COTS software integrity level. In fact, software components are not safe or unsafe; they can be either depending on the system design in which they are used. Therefore, software integrity level has no relation to safety.

14.3.5 Identification of safety designated/significant software.
Criterion: Verify that software elements which perform functions related to system hazards have been identified and handled as safety designated/significant software.
Standard: Safety functions identified as system hazards are allocated to software functions. Software elements (e.g., CSCI, CSC, CSU, data, interfaces) related to each of those software functions are identified and assigned an appropriate safety criticality as defined by the system safety planning documentation. The software elements are handled (labeled, tracked, implemented, tested, etc.) as defined by the system safety planning documentation.
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of system safety and software safety documentation that safety related software functions have been identified. Verify by inspection of program, system safety and software safety documentation that the identified safety related software elements are handled (labeled, tracked, implemented, tested, etc.) as required by software/safety planning based on their safety criticality levels.

Through the scenarios generated by STPA, safety critical systems and software will be identified.

14.3.5.1 Assignment of criticality levels.
Criterion: Verify that each safety designated software function is assigned an appropriate criticality level.
Standard: For each of the software elements (e.g., CSCI, CSC, CSU, data, interfaces), the software functions implementing those elements are assigned an appropriate criticality level. If a software function contains multiple software elements, the function is assigned a criticality level equal to the criticality level of the highest element.
Method of Compliance: Verification method includes analysis and inspection of documentation. Verify that the appropriate level of criticality is assigned to each software function.

STPA will not directly assign criticality levels, however by identifying safety critical systems the analysis may help determine these levels.

14.3.5.2 Testing to criticality levels.
Criterion: Verify that each safety designated software function is tested commensurate with its assigned criticality level.
Standard: Each safety designated software function is tested to the level required by its assigned criticality level. The testing requirements for the software criticality levels are documented in the system safety planning documents.
Method of Compliance: Verification method includes inspection of documentation. Verify that the appropriate level of testing for designated safety software has been performed and required results were achieved.

STPA will provide safety constraints which can be used as an input to testing. Hazards can be prioritized in STPA, however STPA treats all hazards and associated safety constraints the same.

14.3.6 Software safety test analyses.
Criterion: Verify that the appropriate software safety test analyses have been planned and performed.

Standard: Software safety test analyses (e.g., nominal and functional requirements base testing/analysis, structural coverage analysis, hazard mitigation testing analysis, failure modes and effects testing analysis) planning and other documentation are formally documented and are kept under configuration management control. Software safety test analyses activities are also executed; results are recorded using formal procedures and are kept under configuration control.
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of the safety plans that software safety testing and test analyses have been adequately documented and planned. Verify by analysis of the documented hazards that the hazards associated with software and computer components have been eliminated or controlled to the acceptable level of risk as required by the system/software safety plan. Verify by inspection of the test reports that the software safety test results have been analyzed and approved/accepted.

STPA provides safety constraints that should be used as an input into the test plan, just as technical requirements are evaluated during developmental test.

14.3.7 Structural coverage analysis.
Criterion: Verify that software safety planning adequately plans for structural coverage analysis and that the planned analysis is accomplished.
Standard: Adequate structural coverage analysis for the software criticality level is accomplished; results are recorded using formal procedures and are kept under configuration management.
Method of Compliance: Verification method includes inspection of documentation. Verify by inspection of the test plans that adequate structural coverage analysis is planned for and documented. Verify by inspection of structural coverage analysis results that adequate structural coverage testing and analysis were achieved.

If the safety constraints determined by STPA are verified, the testing should be complete from a safety perspective.

Bibliography

1. **Air Force Safety Center.** Aviation Statistics. *Air Force Safety Center.* [Online] 2017. [Cited: 11 27, 2017.] http://www.safety.af.mil/Portals/71/documents/Aviation/End%20of%20Year%20statistics/FY17.pdf.

2. *Fault Tree Analysis.* **Ericson, Clifton.** Orlando : System Safety Conference, 1999.

3. *Reliability Analysis for Power to Fire Pump Using Fault Tree and RBD.* **Anthony, Michael, et al.** 2, s.l. : IEEE, March/April 2013, IEEE Transactions on Industry Applications, Vol. 49.

4. *Failure Mode and Effect Analysis: A Powerful Engineering Took for Component and System Optimization.* **Arnzen, Harry.** Forest Park : Symposium on Deep Submergence Propulsion and Marine Systems.

5. **Crawley, Frank and Tyler, Brian.** *HAZOP: Guide to Best Practice.* 3rd. s.l. : Elsevier, 2015.

6. **Institution, British Standards.** *BS IEC 61882: 2001 Hazard and Operability Studies (HAZOP Studies) - Application Guide.* 2001.

7. **Tolker-Nielsen, Toni.** *EXOMARS 2016 - Schiaparelli Anomaly Inquiry.* s.l. : European Space Agency, 2017.

8. **Leveson, Nancy.** *Engineering a Safer World: Systems Thinking Applied to Safety.* Cambridge : The MIT Press, 2011.

9. **Thomas, John.** Extending and Automating a Systems-Theroetic Hazard Hanalysis for Requirements Generation and Analysis. 2013.

10. **Acquisitions Process.** ***AcqNotes.*** **[Online] 8 5, 2017. [Cited: 11 13, 2017.] http://acqnotes.com/acqnote/acquisitions/acquisition-process-overview.**

11. Department of Defense. Defense Acquisition Guide. 2017.

12. Defense Acquisition Glossary. ***Technology Maturation and Risk Reduction (Phase of the Defense Acquisition System).*** **[Online] [Cited: 11 14, 2017.] https://www.dau.mil/glossary/pages/3193.aspx.**

13. ***AFI 62-601. USAF Airworthiness.*** **11 June 2010.**

14. ***AFI 91-202. The US Air Force Mishap Prevention Program.*** **24 June 2015.**

15. MIL-STD-882E System Safety. s.l. : Department of Defense, 2012.

16. Leveson, Nancy. STPA Compliance with Army Safety Standards and Comparison with SAE ARP 4761. 2017.

17. Losey, Stephen. Air Force report finds faulty engine assembly caused F-16 crash in April. ***Air Force Times.*** **[Online] October 26, 2017. [Cited: November 2, 2017.] https://www.airforcetimes.com/news/your-air-force/2017/10/26/air-force-report-finds-faulty-engine-assembly-caused-f-16-crash-in-april/.**

18. ***AFPD 62-6. USAF Airworthiness.*** **11 June 2010.**

19. USAF Airworthiness Office. USAF Airworthiness Bulletin (AWB)-150. ***Memorandum.*** **Wright-Patterson AFB, OH : s.n., 2017.**

20. ***A Large Scale Experiment in N-Verion Programming.*** **Knight, J. and Leveson, N. Ann Arbor, MI : s.n., 1985. Fifteenth International Symposium on Fault-Tolerant Computing.**

21. ***Annex 3-0 Operations and Planning The Effects-Based Approach to Operations.*** **Curtis E. Lemay Center for Doctrine Development and Education. Maxwell AFB : United States Air Force, 2016.**

22. Leveson, Nancy. Rasmussen's Legacy: A Paradigm Change in Engineering for Safety.
23. Air Combat Command. E-8C Joint Stars Fact Sheet. [Online] 9 23, 2015. [Cited: 11 18, 2017.] http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104507/e-8c-joint-stars/.
24. Northrop Grumman. Joint Stars. *Northrup Grumman.* [Online] 2012. [Cited: 11 18, 2017.] http://www.northropgrumman.com/Capabilities/JointSTARSReCap/Documents/MissionDocs/A_GlimpseJSTARS.pdf.
25. General Services Administration. Federal Business Opportunities. *JSTARS Recapitalization-EMD.* [Online] 1 13, 2017. [Cited: 11 18, 2017.] https://www.fbo.gov/index?s=opportunity&mode=form&id=fe71ff06a1af42be5ee7e63cef761151&tab=core&_cview=1.
26. Insinna, Valerie. Future of JSTARS recap program in question as Air Force explors other options. *DefenseNews.* [Online] September 12, 2017. [Cited: November 18, 2017.] https://www.defensenews.com/air/2017/09/12/future-of-jstars-recap-program-in-question-as-air-force-explores-other-options/.
27. *A Process for STPA.* Thomas, John. 2017.
28. Tillery, Jackie. *Accountability: Inconsistent, Situation Dependent and Subjective.* Maxwell AFB : Air War College, 1997.