The Use of System Theoretic Process Analysis (STPA) on Novel Tiltrotor Aircraft to Prevent Mode Confusion

by

Natalie Ann Basnight

B.S. Mechanical Engineering
United States Military Academy, 2016

Submitted to the Department of Mechanical Engineering
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN MECHANICAL ENGINEERING

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2025

Authored by: Natalie Ann Basnight
Department of Mechanical Engineering
December 12, 2024

Certified by: Nancy G. Leveson
Jerome C. Hunsaker Professor in Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Nicolas Hadjiconstantinou
Department of Mechanical Engineering
Chairman, Department Committee on Graduate Theses

Disclaimer

Any and all opinions, findings, conclusions, or recommendations expressed in this publication constitute views of the author and do not reflect the views of the U.S. Government, its Department of Defense, or the United States Army. All sources used in this work were publicly available.

The use of System Theoretic Process Analysis (STPA) on Novel Tiltrotor Aircraft to Prevent Mode Confusion

by

Natalie Ann Basnight

Submitted to the Department of Mechanical Engineering
on December 12, 2024 in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Mechanical Engineering

ABSTRACT

Initiatives are underway to develop tiltrotor and vertical take-off and lift (VTOL) aircraft that enhance commercial and military aviation's autonomy, capability, and survivability. These designs integrate rotary and fixed-wing elements, introducing distinct safety considerations. These safety concerns are largely due to the differing mental models of operators trained in either rotary or fixed-wing aviation, alongside the rising reliance on autonomy. The traditional hazard analysis techniques (e.g., Fault Tree Analysis and Failure Models and Effects Criticality Analysis) do not adequately account for system component interactions or human factors in complex new aircraft designs.

System Theoretic Process Analysis (STPA) is a powerful new hazard analysis technique for novel tiltrotor aircraft that includes their unique safety requirements. It is a top-down system hazard analysis technique that identifies loss scenarios (N. G. Leveson and J. Thomas Mar2018). It satisfies the tasks described in MIL-STD-882E (Department of Defense 2023). This research demonstrates the use of STPA to identify and mitigate potential instances of mode confusion between the operator's mental model and the autonomy's decision logic in the uniquely dynamic tilt-rotorcraft environment.

Two previous tiltrotor aircraft accidents are analyzed utilizing Causal Analysis based on System Theory (CAST) to help set a framework for the importance of human and machine collaboration in systems. These accidents show a trend in the dangers of aircraft system mismanagement between various controllers. The CAST results for these accidents help provide information about how to prevent these types of incidents in the future, setting the stage for the use of STPA on novel tiltrotor aircraft, as demonstrated in this thesis. STPA can be used before design, implementation, and fielding, allowing for better early design of systems and reducing the cost of later redesign or modification.

Thesis Supervisor: Nancy G. Leveson
Title: J. C. Hunsaker Professor in Aeronautics and Astronautics

Acknowledgments

My time at MIT and the production of this thesis were made possible by my family, friends, peers, and mentors. I want to recognize and thank them all for their contributions and encouragement throughout my research and thesis development.

First, I would like to thank my research advisor, Nancy Leveson, whose work and dedication to safety have inspired me as an academic and an aviator. Our world is better and safer because of Nancy, and I am grateful and honored for her mentorship and wisdom during my time at MIT. Nancy, thank you for your commitment to your students and for your support as I ventured back into the academic world. Your support as I navigated graduate school and simultaneously became a mother will not be forgotten. I hope that my thesis work will inspire change as yours has throughout industry.

Peter, my husband, your unwavering support and love have empowered me to grow and become a better person. Thank you for constantly uplifting me and for being an incredible father to our favorite little guy, Michael. Formulating this thesis involved many conversations and deliberations with you, and I owe you immense gratitude.

I would like to thank and recognize my parents, whose twenty years of military service to the nation and expertise in human factors have inspired my efforts across multiple life domains. They are the ultimate role models and have always encouraged my paths in the military, academia, and now as a parent myself. Thank you for always believing in me and loving me through all the joys and challenges.

To my friend Julie Johnston, crossing paths with you in the Army aviation community and here at MIT has been an incredible blessing. Our shared journey into motherhood while re-entering the engineering field has been both exciting and demanding. I'm truly grateful that we supported each other along the way.

To the Future Long Range Assault Aircraft (FLRAA) team, Zach Zimmerman and Sam Clark, and from the NASA Ames Research Center, Tom Berger, thank you for including me in your work toward optimizing Army aviation and for the expertise of tiltrotor aircraft required for this thesis. Your dedication to the FLRAA mission gives me confidence in the Army's efforts toward creating safe, powerful aircraft that will prioritize the survivability of our aviators, crew chiefs, and soldiers.

Finally, I am immensely grateful to the entire Engineering Systems Lab, specifically those in the Systems Safety group, for the teamwork, encouragement, and inspiration. To John Thomas, thank you for your expertise and your advice as I formulated my thesis. To Alex Hillman and Justin Poh, thank you for your continued mentorship and for helping me formulate ideas to improve my work. To Polly Harrington, Lauren Gutierrez, Braden Brower, Brittany Bishop, Rodrigo Rose, Chris Tommila, and Elizabeth Baker, thank you for your discussions, friendship, and advice throughout the graduate school experience.

Table of Contents

List of Figures

List of Tables

Glossary of Acronyms and Symbols

AC	Advisory Circular
ACAH	Attitude Command / Attitude Hold
ADC	Air Data Computer
AFCS	Automatic Flight Control System
AGL	Above Ground Level
AM	Aircraft Manufacturer
AOA	Angle of Attack
ARP	Aerospace Recommended Practice
ASA	Aircraft Safety Assessment
ATC	Air Traffic Control
A/P	Autopilot
A/T	Autothrottle
$\boldsymbol{\alpha}$	Tip-Path-Plane Angle of Attack
CAD	Computer Aided Design
CAST	Causal Analysis based on Systems Theory
CF	Contextual Factor
CLAW	Control Law
DOD	Department of Defense
DSR	Derived Safety Requirements
EASA	European Union Aviation Safety Agency
EENT	End Evening Nautical Twilight
EP	Emergency Procedure
EVTOL	Electric Vertical Take-Off and Lift
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FC	Flight Crew
FCB	FAA Certification Branch

FCC	Flight Control Computer
FD	Flight Director
FHA	Fault Hazard Analysis
FHA	Functional Hazard Analysis
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
FLCH SPD	Flight Level Change Speed
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FMRI	Final Mishap Risk Index
GPS	Global Positioning System
IEL	Indentured Equipment List
IFR	Instrument Flight Rules
IGE	In ground effect
IMRI	Initial Mishap Risk Index
JAG	Judge Advocate General
KIAS	Knots Indicated Airspeed
LZ	Landing Zone
NAVAIR	Naval Air Systems Command
NTSB	National Transportation Safety Board
NVG	Night Vision Goggle
OGE	Out of ground effect
PASA	Preliminary Aircraft Safety Assessment
PC	Pilot in Command
PF	Pilot Flying
PFCS	Primary Flight Control System
PFD	Pilot Function Display
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PI	Pilot
PM	Pilot Monitoring
PMB	Process Model Belief
PMF	Process Model Flaw
PSSA	Preliminary System Safety Assessment
RBS	Retreating Blade Stall
RCAH	Rate Command / Attitude Hold
RPM	Revolutions per minute
SAE	Society of Automotive Engineers
SFHA	System Functional Hazard Assessment
SIS	Safety Information System

SSA	System Safety Assessment
SSHA	Subsystem Hazard Analysis
SSR	System Safety Requirement
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TCL	Thrust Control Lever
TLM	Top-Level Mishap
θ	Collective Blade Pitch
UCA	Unsafe Control Action
UE	Undesired Top Event
UL	Unit Leadership
UM	Unit Maintenance
VFR	Visual Flight Rules
VRS	Vortex Ring State
$\mathbf{V_{tip}}$	Rotor Tip Speed
$\mathbf{V/V_{tip}}$	Advance Ratio
VTOL	Vertical Take-Off and Lift
WOW	Weight on Wheels

Chapter 1 Introduction

1.1 The Problem

The development of novel military helicopter systems has been slow due to the intrinsic nature of helicopter aerodynamic complexity and constantly changing mission requirements. The helicopters used in the field for decades have proven to be robust, reliable, and survivable. Specific to the United States Army Aviation rotary fleet, the UH-60 Black Hawk, AH-64 Apache, and Ch-47 Chinook have been the primary helicopters in use for the past forty years because of their ability to perform the required missions safely and efficiently. Despite these platforms' reliability, the Army created the Future Vertical Lift (FVL) initiative to develop new aircraft that can compete in highly complex and dangerous environments in Large Scale Combat Operations (LSCO).

Various companies have produced rotorcraft prototypes over the past three decades, but they have all failed to pass the approval for final full-scale production with the government. Their inability to guarantee the safe delivery of combat power, whether in the form of troops, ammunition, or reconnaissance, has resulted in canceled projects and contracts. In addition, the exponential growth of autonomy in technology outpaces the development process for these novel rotorcraft projects. Therefore, the defense industry has focused on tiltrotor technology to meet these demands.

Tiltrotor aircraft combine rotary and fixed-wing components, allowing for high airspeeds and hover capability. Although this type of aircraft meets mission demand, it also creates unique safety requirements. Most pilots are trained in rotary or fixed-wing flight, and how those pilots interact with potential autonomy on tiltrotor aircraft requires in-depth safety analysis. As automation becomes more prevalent in aircraft, the pilot must share the decision-making with that automation. This shared decision-making can lead to the potential of mode confusion, where the different controllers of a system, either human or computer, develop a misunderstanding of the current mode of the aircraft.

The current safety processes used in aircraft development typically fail to account for these interactions between all system components. They also do not consider the unique feedback and control paradigms involved in autonomy. STPA provides a way forward.

1.2 Research Objectives

The primary objectives of this research are to apply CAST to two previous tiltrotor accidents and STPA to novel tiltrotor aircraft, helping to identify system-level hazards associated with mode confusion and creating safety-related design requirements. By applying STPA for hazard analysis early in the design process, aircraft developers can better guarantee the entire system's survivability by considering controller relationships and their interactions with the aircraft. In contrast, other traditional hazard analysis techniques used for aircraft development are typically applied after the design is complete or in a mature phase. Modifications then require expensive and sometimes unachievable adaptations that are time-consuming and inefficient. The use of STPA, with a focus on the mission environment and the tiltrotor aerodynamic functionality, provides useful early information to the developer about the critical considerations of the human-automation relationship.

1.3 Thesis Approach

The thesis approach applies CAST to two previous accidents. STPA is then applied to a novel two-rotor tiltrotor aircraft, focusing on the aerodynamic complexities that make it unique from other, more traditional helicopters and airplanes. The results are compared to those of traditional hazard analyses, highlighting how these traditional approaches yield inefficient data for hazard prevention. By conducting STPA at multiple levels of abstraction, the results help identify multiple instances of mode confusion between the operator's mental model and the autonomy's decision logic. The results are used to recommend design requirements to improve the safety of future tiltrotor or VTOL aircraft.

1.4 Structure of this Thesis

The thesis is organized as follows: Chapter 2 provides the necessary background information on traditional hazard analysis methods, human factors, mode confusion, aircraft aerodynamics, pilot training, and the System Theoretic Accident Model and Processes (STAMP) causality model. Chapter 3 presents the findings from the application of CAST to two Osprey V-22 tiltrotor accidents. Chapter 4 provides the results from STPA applied to a two-tiltrotor aircraft to demonstrate the method's capability in identifying mode confusion early in the design process. The results are compared with traditional hazard analyses from a NASA study. Chapter 5 presents conclusions, describes the study's limitations, and suggests directions for future research.

Chapter 2 Literature Review

Chapter 2 provides relevant background information about current systems safety processes used in novel aircraft development as well as general information about aircraft functionality. Section 2.1 summarizes the current safety regulations and practices used in commercial and military aircraft development and section 2.2 highlights the traditional hazard analysis techniques recommended by those regulations. Section 2.3 defines and explains human factors considerations in the aviation industry to show the importance of including human operators in hazard analyses for aircraft. Section 2.4 explains the differences between fixed-wing, rotary wing, and tiltrotor aircraft functionality and operability to set a framework for the possibility of mode confusion, whereby the pilots and automation share a misunderstanding of the system's mode of operation. The literature review concludes with section 2.5, which presents an overview of the Systems-Theoretic Accident Model and Processes (STAMP) as ways forward to identify important safety considerations for tiltrotor aircraft that are currently not adequately addressed in standard practice.

2.1 Current Safety Regulations Used in Aircraft Development

There are two applicable documents used for safety regulation in military and civil aircraft development leveraged for this thesis: MIL-STD-882E and SAE ARP 4761. The military and Department of Defense (DOD) require MIL-STD-882E for aircraft development and can use other industry standards such as SAE ARP 4761 to satisfy Federal Aviation Administration (FAA) requirements. For civil aircraft, developers can use SAE ARP 4761 to fulfill higher regulatory requirements outlined by the FAA and the European Union Aviation Safety Agency (EASA).

2.1.1 MIL-STD-882E

Military Standard 882E is a DOD systems safety approach for identifying hazards and mitigating associated risks for defense systems. The DOD created this standard to make risk management a preemptive system safety methodology rather than addressing hazards as operational considerations. It is organized into two main sections: general/detailed requirements and the following tasks: management, analysis, evaluation, and verification. This Standard may be required in solicitation or contract and if not addressed otherwise, is only mandated to include the "General Requirements" section.

The general requirements section includes information and guidance on systems safety requirements, the systems safety process, documentation guidance, hazard identification, risk assessment and mitigation measures, and software risk contributions. There are associated probability and severity tables for reference as well as a risk assessment matrix. Figure 1 shows the general process required but can include additional tasks per the specified contract.

The detailed requirements section includes information on the tasks that can be tailored to a specific system per the contract. This section mentions recommended hazard analyses for use but does not mandate them. It says, rather, to identify the desired analysis method and provides options such as the Preliminary Hazard Analysis (PHA), Subsystem Hazard Analysis (SSHA), Fault Tree Analysis (FTA), and Failure Modes and Effects Criticality Analysis (FMECA). The DOD tends to use one or more of these analysis methods for their systems, which do not always

produce effective hazard identification and mitigation. It is important to understand the outlines of MIL-STD-882E because the later proposed safety analysis tools from STAMP satisfy this standard.

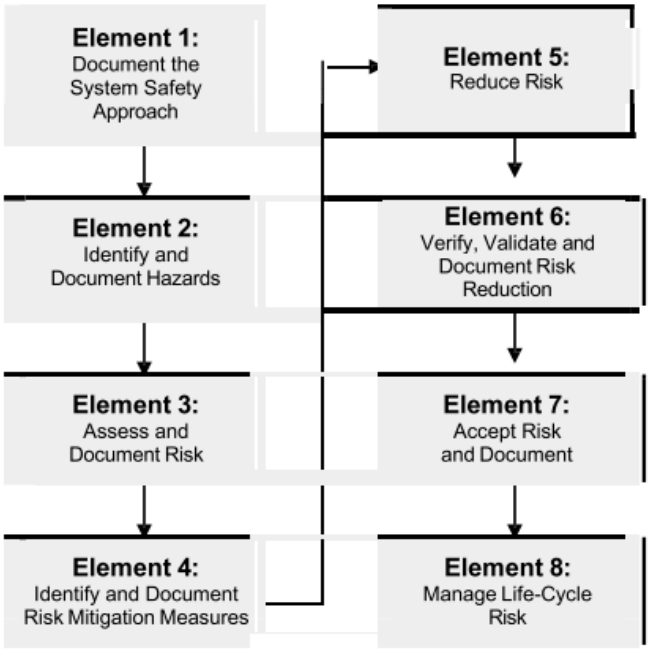

Figure 1: Eight Elements of the System Safety Process (Department of Defense 2023, 10)

2.1.2 SAE ARP 4761

The following safety regulations recommend the use of safety analysis methods that are inadequate in identifying necessary hazardous outcomes. The Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761 provides guidelines for conducting safety assessment processes on civil aircraft, systems, and equipment. This ARP supports a larger aircraft and system development regulation, SAE ARP 4754. Advisory Circular (AC) 20-174 recommends the use of both ARPs to satisfy FAA or EASA regulations for certification of aircraft systems. These regulations include the Federal Aviation Regulation (FAR) 25.1309 and Certification Specification (CS) 25.1309.

SAE ARP 4761 identifies safety program plan options and mentions that all projects vary in size and scope; therefore, different programs will have varying safety process outputs at multiple levels by multiple stakeholders. Figure 2 shows the different safety assessment processes and hazard analysis methods at the system and aircraft levels all of which can feed information into the development process. This figure shows the relationship between different assessment processes and how the use of multiple processes can provide different value or output to the overall development process for aircraft systems. The figure is modified to emphasize the assessment levels that require the use of hazard analysis methods, which are highlighted.

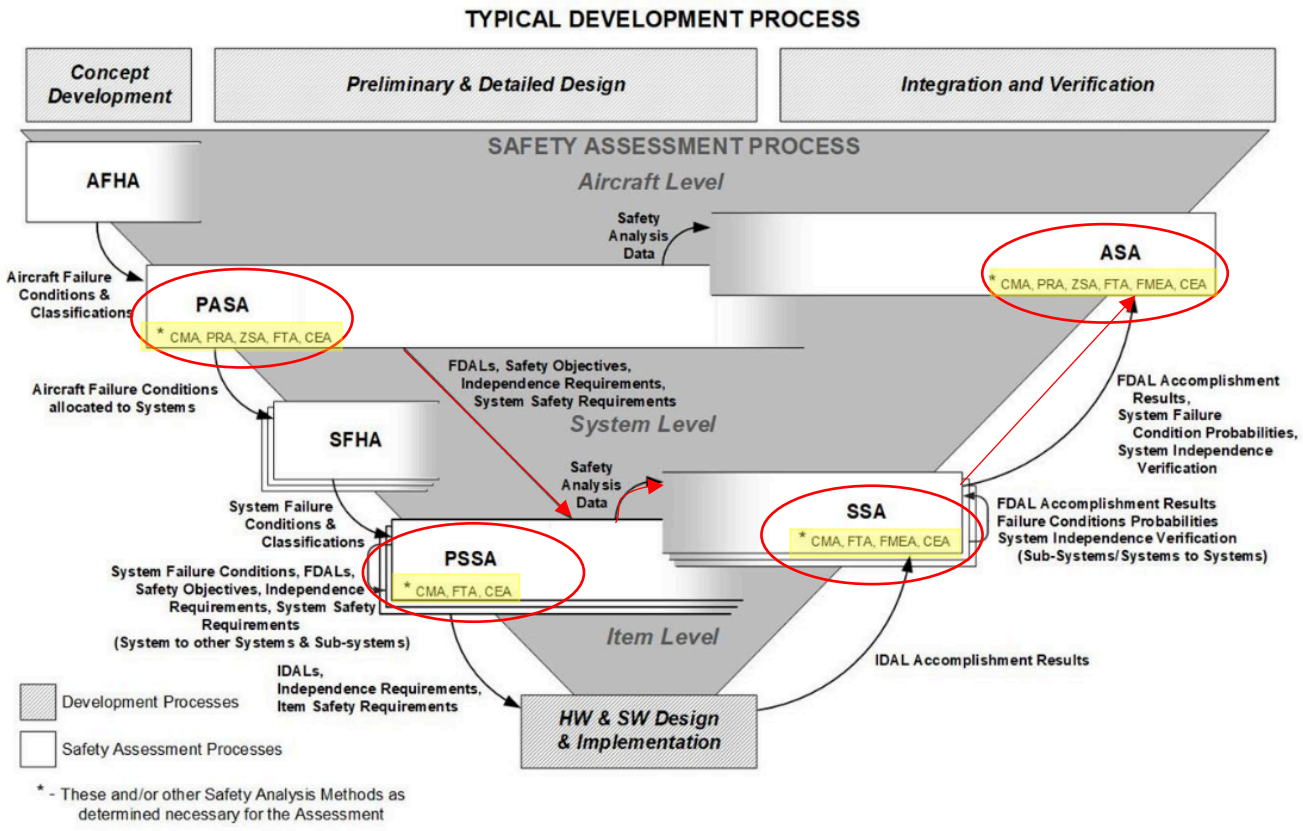

Figure 2: General Safety Assessment Process (SAE International 2023, 19)

2.1.2.1 Preliminary Aircraft Safety Assessment (PASA)

The Preliminary Aircraft Safety Assessment (PASA) is a systematic safety evaluation of the aircraft architecture. Its primary objective is to address the aircraft failure conditions compiled from the Aircraft Functional Hazard Assessment. The PASA assesses the interactions between multiple component-level failure conditions to identify system safety requirements. ARP4761 recommends various hazard analysis techniques to complete this assessment, which are depicted in Figure 2 in the PASA box. The most commonly used technique is Fault Tree Analysis, which is defined in more detail in section 2.2. The FTA provides the information necessary for the PASA to continue the aircraft development process, feeding its analysis to the Preliminary System Hazard Analysis.

2.1.2.2 Preliminary System Safety Assessment (PSSA)

The Preliminary System Safety Assessment (PSSA) is similar to the PASA but evaluates the system-level architecture as opposed to the aircraft architecture. It applies system-level failure conditions and classifications from the System Functional Hazard Assessment to hazard analysis techniques, like FTA, to determine if the proposed architecture can meet designated safety objectives. The output from the hazard analysis provides redesign feedback, architectural constraint requirements, and quantitative probabilistic requirements necessary for the System Safety Assessment.

2.1.2.3 System Safety Assessment (SSA)

The System Safety Assessment (SSA) verifies that the system design satisfies the qualitative and quantitative safety objectives from the previous assessments. It applies a hierarchical approach of hazard analysis for different levels of the system to cover the specific safety requirements identified earlier. The analyses are completed at the system, subsystem, equipment, or part of equipment levels to provide further assumptions, safety requirements, and system independence verification for the final step in the assessment process, the Aircraft Safety Assessment.

2.1.2.4 Aircraft Safety Assessment (ASA)

The Aircraft Safety Assessment (ASA) is a systematic evaluation of aircraft implementation at the most mature stage of the development process. It is designed to consider the hazard analysis and assessment results at each level of the entire process to make final confirmation of safety conclusions. Similar to earlier assessment levels, it uses traditional hazard analysis techniques like FTA and FMEA to confirm final aircraft architecture for the system.

2.2 Traditionally Used Hazard Analyses

SAE ARP 4761 recommends various hazard analysis techniques from systems safety theory for use in aircraft development and assessment. Historically, these analyses were used when systems were simpler and had less autonomous or software intensive functionality. While these analyses can provide useful information for hazard development and mitigation, they do not synthesize component level interaction within a system or include the human as an important component. They also do not include software. It is therefore unlikely that they would account for the potential of mode confusion in aircraft operation.

2.2.1 Preliminary Hazard Analysis (PHA)

The Preliminary Hazard Analysis (PHA) is a technique used for identifying hazards in the early design stage of a system. The basic architecture of the analysis involves developing and synthesizing the initial system design, hazard sources, system design tools, and top-level mishaps (TLMs) to generate causal sources, risks, and mitigation methods. Information development for this analysis uses data from similar systems, legacy systems, and other lessons learned (Ericson 2005). It requires a preliminary hazard list (PHL), among other sources, which is a brainstorming type of generation of potential hazards from a conceptual design of an early system. The results are then formulated onto a worksheet consisting of the hazards, causes, effects, system mode, initial mishap risk index (IMRI), recommended action final mishap risk index (FMRI), additional comments, and status of the hazard (open or closed). The IMRI and FMRI use recommendations from MIL-STD-882 that combine severity and probability into qualitative measures. This analysis does not provide a final, wholistic coverage of hazards for an overall system because it is meant to be an initial compilation to feed further analyses. There is also no structured technique for identifying the results and therefore no assistance is provided in ensuring completeness.

2.2.2 Subsystem Hazard Analysis (SSHA)

The SSHA is used when a system design is more detailed and has modifications from the PHA. This analysis method uses similar techniques from the PHA but helps identify additional, detailed causal factors, hazards, and ultimately system safety requirements (SSRs). This analysis requires expert knowledge of the system to identify and produce subsystem-level hazard information. It uses an indentured equipment list (IEL), initially formed in the PHA, to ensure complete coverage of all components in the system. The following list is recommended when developing subsystem hazards:

1. Performance of the subsystem hardware
2. Performance degradation of the subsystem hardware
3. Inadvertent functioning of the subsystem hardware
4. Functional failure of the subsystem hardware
5. Common mode failures
6. Timing errors
7. Design errors or defects
8. Human error and the human system interface design
9. Software errors and the software–machine interface
10. Functional relationships or interfaces between components and equipment comprising each subsystem

(Ericson)

Although this list includes human consideration and component interactions, it does not provide tools for how to identify, analyze, or mitigate these types of hazards.

2.2.3 Fault Tree Analysis (FTA)

FTA is a top-down approach that is used to identify the causal factors of a hazard. It is structured as a diagram of failure events that may lead to an undesired, top event (UE) as depicted in Figure 3. There are four steps when using FTA: define the system, construct the fault tree, conduct qualitative analysis, and conduct quantitative analysis (N. Leveson 2023, 284).

Step 1, defining the system, requires an in-depth understanding of all aspects of the system to account for all potential top events. It is also important to identify if the system has multiple states and how that top event has different meaning with those states. For example, a top event may be inadvertent pitch angle change of a tiltrotor. The hazardous state may have different outcomes if the aircraft is on the ground, at a hover, or at cruising altitude. Step 2, constructing the fault tree, involves developing all causal events that could lead to the top event and using logic symbols to connect them. This development is at the whim of the analyst's decision making on when is the appropriate stopping point for the causal events. Figure 4 shows the symbology used to create the fault tree. Step 3, the qualitative analysis, involves reducing the fault tree into its minimum top event and primary events based on cut sets. A cut set is defined as the set of events that can, together, cause the top event. Step 4 is the quantitative analysis that involves calculating the probability of occurrence of the top event through the multiplication of the minimal cut sets shown in Figure 3.

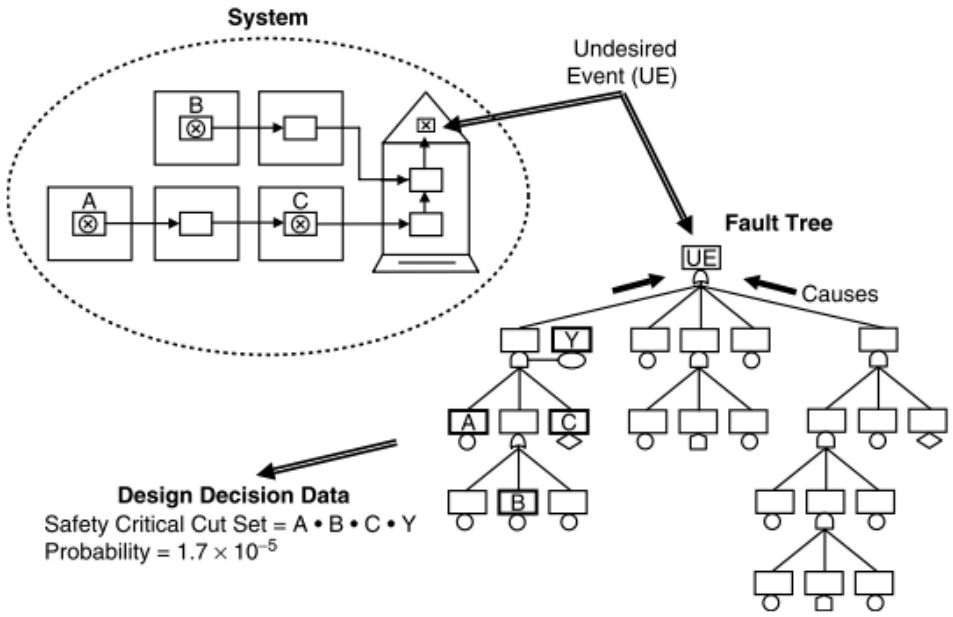

Figure 3: FTA Overview (Ericson 2005, 199)

FTA requires completed design information to have detailed results. It also requires expert knowledge of a system to produce accurate information about causal, failure-based events that could lead to the UE. Also, its primary focus on only component or system failures does not account for other potential hazardous outcomes for non-failures. It also does not typically account for time-based situations in which chronology of events is important for the determination of a hazardous event. Aircraft development does not benefit from solely using FTA due to these disadvantages.

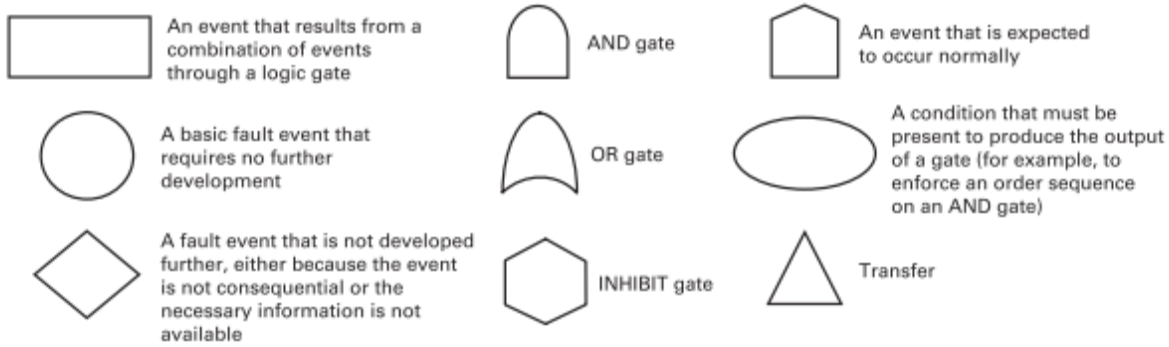

Figure 4: Fault Tree Symbols (N. Leveson 2023, 286)

2.2.4 Failure Modes and Effects Criticality Analysis (FMECA)

FMECA is a bottom-up process that focuses on reducing the likelihood of failure in system components. It is a more detailed version of Failure Modes and Effects Analysis (FMEA) by including the criticality and detection of potential failure modes. Although it is classified as a hazard analysis, it is more accurately described as a reliability analysis since it focuses solely on the successful functioning of components (N. Leveson 2023, 279). FMECA involves listing out

all components of a system and their failure modes, the cause of failure, the effects on the overall system, the probability and severity levels, and actions to reduce the failure. Table I includes a sample of a FMECA result. Probabilities associated with failure are based on averages from similar systems. This does not always provide accurate or usable information for all components on a system especially if it is comprised of new hardware not used before or extensive software. Humans and human error as well as software are generally excluded from this analysis, or their behavior oversimplified because assigning probability to this type of failure is immeasurable.

For FMECA to be complete, in aircraft systems today, would mean applying this theory to potentially millions of components. It also does not typically account for multiple or combinations of failures, which can be lacking in hazard analysis for aircraft. Finally, FMECA requires a completed design of a system, which could lead to costly design modifications once failure modes are analyzed.

Table I: FMECA sample (N. Leveson 2023, 280)

FAILURE MODES AND EFFECTS CRITICALITY ANALYSIS Subsystem_____ Prepared by_____ Date_____						
ITEM	FAILURE MODES	CAUSE OF FAILURE	POSSIBLE EFFECTS	PROB.	LEVEL	POSSIBLE ACTION TO REDUCE FAILURE RATE OR EFFECTS
Motor case	Rupture	a. Poor workmanship b. Defective materials c. Damage during transportation d. Damage during handling e. Overpressurization	Destruction of missile	0.0006	Critical	Close control of manufacturing processes to ensure that workmanship meets prescribed standards. Rigid quality control of basic materials to eliminate defectives. Inspection and pressure testing of completed cases. Provision of suitable packaging to protect motor during transportation.

2.2.5 Fault Hazard Analysis (FHA)

FHA is similar to FMECA but focuses on system functions and their reliability as opposed to only hardware component failures. It includes function failures that can lead to accidents and includes human error, procedural deficiencies, environmental conditions, and time-based hazardous system states as potential sources. The FHA uses the function, failure condition, phase of operation, effect of the failure condition, severity classification, and other applicable information. Disadvantages of the FHA are similar to those from FMECA. FHA also includes best-case assumptions for human and environmental reactions to failures, which are not always reflective of reality.

2.3 Human Factors in Aviation

Human factors consideration in system design originated because of aviation accidents. Design of aircraft initially factored in little to no analysis of human cognitive processes. When early investigations found human error as the main cause of aviation mishaps, experts realized that further analysis was needed to better understand the human-machine interface.

"Human error" alone does not provide guidance for prevention of future mishaps or solutions for design improvement. Rather, human behavior responds in accordance with the design of a system, and errors can result from performance considerations (workload, experience, distractions, conflicting interfaces) or inadequate process models. As something human factors scientist Iulia Dumitru explains, "understanding the predictable dimensions of human capabilities and limitations and applying this knowledge in operational environments is the main concern of human factors," (Dumitru and Boşcoianu 2015).

While systems engineering has shifted towards including human factors into its processes, traditional hazard analyses still do not wholistically include human factors. When "human error" is assumed to be the cause of many aviation accidents, it is a clear indication that the hazard analyses performed on aircraft must include consideration of human performance and their mental/process models. Humans are not operating in isolation in these incidents, but rather in conjunction with machines. It is crucial, therefore, to specifically identify where this interaction goes awry.

2.3.1 Human Performance

According to the FAA human factors engineering branch, human performance is measured through the following considerations:

- Physical: size, strength, and anthropometrics
- Physiological: flight physiology, fatigue, noise, and vibration throughout a duty cycle
- Sensation and perception: visual, auditory, haptic, and other sensory elements used for flight tasks
- Cognition: Memory, mental function, perception, and information processing
- Behavior: Decision-making, human error, and crew interactions

The optimal system approach to human factors involves the analysis of how humans process information, from the list mentioned above, with the interface system design and the tasks to be performed. This ensures that information is clearly presented to the human, the system is designed for usability, workloads are manageable, and potential for error is minimized or controlled. Workloads are measured through subjective and objective means. Subjective information is based upon an individual's personal experience, human bias, and memory. Objective information is measured both overtly, through task performance, and covertly, through physiological measurements.

While both objective and subjective measurements of human performance provide valuable insights into operator efficiency and cognitive load, these metrics also highlight areas where human-machine interaction can become problematic.

One such issue is mode confusion, a phenomenon that occurs when an operator misinterprets or is unaware of the current state or mode of an automated system. This breakdown in situational awareness is particularly critical in complex environments, such as aviation, where the consequences of such errors can be severe.

2.3.2 Mode Confusion, Mental Models, and Process Models

A mode is defined as a "mutually exclusive set of automation behaviors" (N. G. Leveson 2012, 310). There are four general types of modes including controller operating modes,

supervisory modes, display modes, and controlled process modes. Controller operating modes define a controller's set of behaviors. Supervisory modes include system components that can be controlled by multiple supervisors with the same control responsibilities. Display modes include the various information presented to the user by the system display. Controlled process modes are the current or operating modes of the controlled process. The combination of modes and increased complexity in mode design in a system can contribute towards the potential breakdown of mode awareness for controllers. Leveson defines mode awareness as keeping the controlled-system operating mode in the controller's process model consistent with the actual controlled system mode (N. G. Leveson 2012, 311).

A human error known as mode confusion occurs when the operator may misunderstand or misdiagnose what mode a system is operating under at a given point in time. The human user may act with the understanding of one mode when the system could be operating on another mode.

As automation becomes more prevalent in systems and the number of modes of automation increases, the chance for disconnect between different controllers in systems will grow. More specifically, the human controller's mental model must contain an accurate model of the current state of the process/automation. A process model contains an automated understanding of a mode whereas a mental model applies specifically towards a human controller's understanding of a system (N. G. Leveson 2012, 88).

When the various controllers have a misunderstanding of what mode the system is operating on, there is a chance for mode confusion, mismanagement of the system, and potential hazards. Sarter and Woods breakdown the definition of mode confusion into two categories: errors of commission, when the operator takes an inappropriate action, and errors of omission, when the operator fails to take a required action (Sarter and Woods 1995, 9). Pilots can also experience an atrophy in their skills due to increased reliance on automation or augmentation, potentially leading to delayed reaction times in hazardous scenarios that require immediate and appropriate pilot intervention. The aircraft design should provide the appropriate cueing mechanisms for automation or augmentation to prevent inappropriate pilot action or mode confusion.

Figure 5 represents a generic control structure to model the potential for mode confusion between human operators and the automation. A control structure is a system model that captures different controllers and their functional relationships through feedback loops. This example depicts the feedback relationships between operators, automation, and the controlled process through the upward and sideways arrows. The downward arrows indicate the process model decisions and actions based on the feedback received. The human controller updates mental models from direct system feedback and from feedback from the automated controller. The automated controller updates process models from system sensors, human input, or previous control actions (Bishop et al. 2023, 4). When multiple modes exist for multiple controlled processes or systems, the human controller may become oversaturated with feedback and could have an incorrect understanding of the process model.

An important form of mode confusion can arise from indirect mode changes. These happen when the automation changes mode without direct instruction or demand from the human controller. This is seen more in modern systems as automation is given more autonomy. In aviation, specifically for tiltrotor aircraft, the automatic mode of the rotor system tilting is based off the airspeed. However, there may be other modes for the tiltrotor including approach or take-off modes, rotor RPM changes, or deceleration to hover modes, which may ignore or not

consider input from the pilot based on its logic. Gaps in the controller's mental model of this automated control could impact the controller behavior.

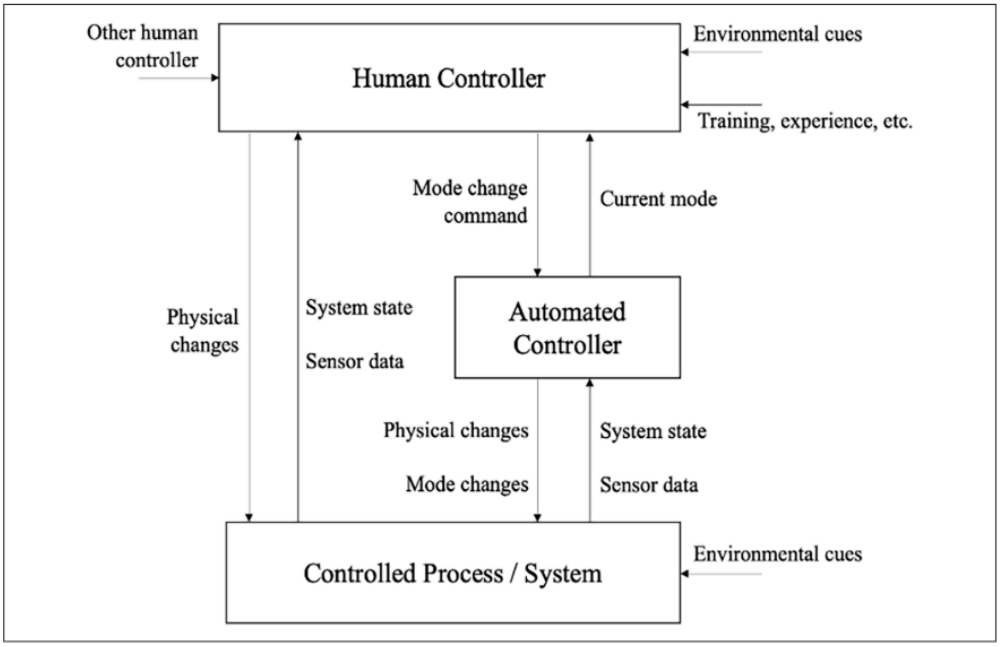

Figure 5: Generic Control Structure for Mode Confusion Analysis (Bishop et al. 2023, 5)

2.3.3 Mode Confusion Case Studies in Aviation Accidents

As future aircraft continue to have more autonomy and increased software complexity, it is important to ensure that human controllers understand the process models and behavior of the various automatic systems. The following aircraft case studies involve a misalignment of that understanding between controllers.

2.3.3.1 Joby Aero Incorporate JAS4-2 eVTOL

Joby Aero Inc. conducted a remotely piloted flight test on its electric vertical take-off and lift (eVTOL) aircraft JAS4-2 in 2022. During an airspeed and altitude envelope expansion flight test, the aircraft entered a dive speed of 181 knots indicated airspeed (KIAS), beyond that of the expected operating conditions of the aircraft. A propeller blade on station 3 experienced bending failure, released from its station, and impacted other station propellers, causing the aircraft to depart controlled flight and impact the ground.

The aircraft was a pre-production prototype configured of six tilting propellors designed to perform hover and forward flight, depicted in Figure 6. The aircraft is capable of remote or manned flight but was remotely controlled during the mishap. Although this was an experimental test flight designed to push and test the structural capabilities of the aircraft, propeller station 3 contained a tiltrotor actuator linkage that allowed its propeller blades to be at a steeper angle than commanded (National Transportation Safety Board (NTSB) 2014, 2).

Unbeknownst to the remote operator, the anomalous behavior of the tiltrotor mechanisms of station 3 allowed for rapid growth in vibration and resonant responses, which at a high diving airspeed of 181 knots, pushed the physical capabilities of this propellor station to failure. A form

of mode confusion existed between the operator and the computer programming, which allowed unsafe angles of blade pitch on propellor station 3. The remote operator was unaware of the computer's ability to set the blade pitch at angles outside of its limitations.

It is unknown whether this mode was intentionally programmed to operate at angles outside of the structural capability, and the investigation did not make any conclusions or recommendations into this matter.

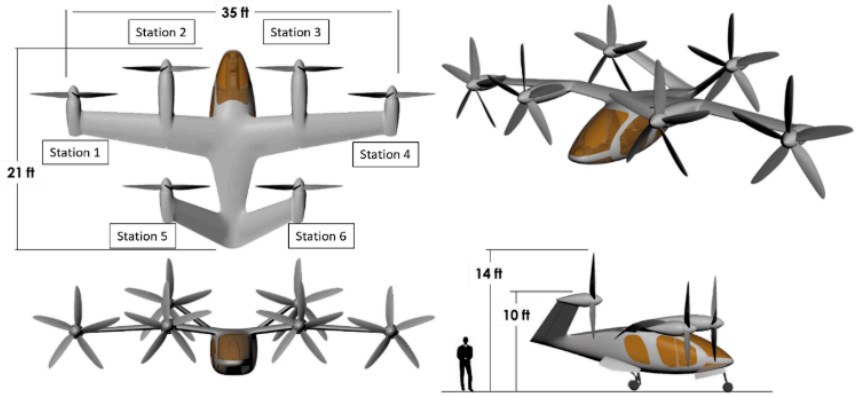

Figure 6: Depiction of a JAS4-2 aircraft (Haley Davoren 2024)

2.3.3.2 Asiana Airlines Flight 214 Descent Below Visual Glidepath

On July 6, 2013, a Boeing 777-200ER aircraft operating under Asiana Airlines crashed at San Francisco International Airport when it stalled during a routine landing approach. The flight crew was slightly above the desired glidepath during its straight-in visual approach and mismanaged the automation when trying to remedy the aircraft's descent.

> "In an attempt to increase the airplane's descent rate and capture the desired glidepath, the pilot flying (PF) selected an autopilot (A/P) mode (flight level change speed [FLCH SPD]) that instead resulted in the autoflight system initiating a climb because the airplane was below the selected altitude. The PF disconnected the A/P and moved the thrust levers to idle, which caused the autothrottle (A/T) to change to the HOLD mode, a mode in which the A/T does not control airspeed. The PF then pitched the airplane down and increased the descent rate. Neither the PF, the pilot monitoring (PM), nor the observer noted the change in A/T mode to HOLD" (NTSB, Descent Below Visual Glidepath and Impact With Seawall, p. 14).

The aircraft slowed considerably and descended at a rate of 1,200 ft per minute. When the aircrew realized the aircraft could not be landed safely, they attempted a Go Around but did not have the performance capability to accomplish the maneuver. The aircraft crashed on the runway resulting in three fatally injured passengers and numerous injuries.

The aircrew did not have a complete and wholistic mental model of the various modes in the autopilot function of the aircraft. The autopilot process model did not contain the information necessary to determine the aircrew's intent when they disconnected the A/P at certain points in the approach.

2.3.3.3 V-22 Osprey Burst Hydraulic Line ("Osprey Aircraft Crash" 2000)

On December 11, 2000, a V-22 experienced a leak in a hydraulic line that fed its primary side swashplate actuators. The leak caused a Primary Flight Control System (PFCS) alert, prompting the aircrew to press the PFCS reset button to remedy the multiple cautions.

In response, the flight control computer reset the blade pitch angles to zero and initiated an unexpected thrust increase. The aircraft became uncontrollable and was unable to produce the necessary lift for continued flight.

The aircrew pressed the PFCS reset button nine times, and each time the computer reset the blade pitch angles and thrust factor. The aircraft crashed from 1,600 feet. The aircrew's misunderstanding of what mode the computer switched to when they pressed the button led to the aircraft entering an uncontrollable state, despite what their training manuals advised.

Mode confusion existed between the aircrew's mental model of the PFCS reset functionality and the actual operation of the computer controller. This case study is further analyzed in Chapter 3.

2.4 Rotary, Fixed-Wing, and Tiltrotor Characteristics

Identifying the potential for hazards when the characteristics of rotary and fixed wing aircraft are combined in tiltrotors requires understanding (1) the applicable aerodynamic considerations for each of these types of aircraft and (2) the training provided to pilots to fly these aircraft types.

2.4.1 Aerodynamic Considerations

2.4.1.1 Vortex Ring State

All rotary wing aircraft, including tiltrotor, are susceptible to an aerodynamic phenomenon known as Vortex Ring State (VRS). Vortex Ring States have led to accidents in tiltrotor aircraft.

VRS occurs during vertical descent or high decent angle flight. The pressure differential between the top and bottom of the rotor disk plane in a descending profile causes a highly unstable and turbulent flight regime. "Descending into the downwash of a rotor beyond a certain point causes the stable helical wake vortex structure to collapse into a single strong vortex ring that encompasses the rotor tips" (McQuaid et al. 2020, 1). This phenomenon can also be referred to as "settling with power."

Figure 7 shows stable, airflow velocity along a blade span for a helicopter in hovering flight. Figure 8 depicts the flow velocity for a blade span in descending flight where an upflow towards the center of the rotor overcomes the effective lift. When the rotor tips do not provide angle of attack effectiveness, the thrust forces of the entire rotor disk decrease and oscillations increase. The resultant aircraft state can lead to insufficient lift for a safe flight profile. Figure 9 shows an example of a quadcopter in a descent profile and the resulting increased vorticity magnitude near the rotor tips. Helicopter pilots can mitigate the possibility for VRS by limiting descent rate at low airspeeds, but there is limited research completed on aircraft automation detecting and mitigating VRS.

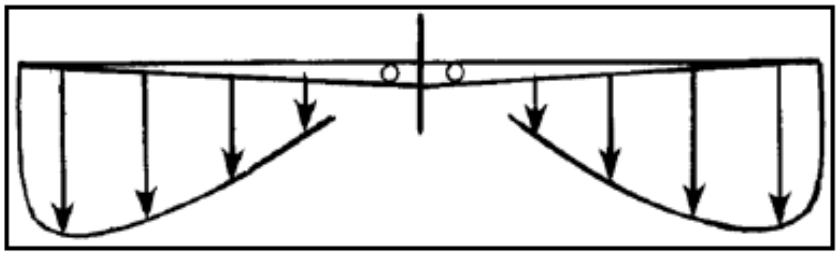

Figure 7: Induced flow velocity during hovering flight ("Fundamentals of Flight" 2022, 59)

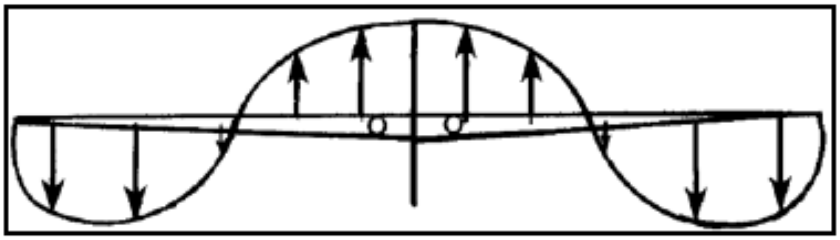

Figure 8: Induced flow velocity before vortex ring state ("Fundamentals of Flight" 2022, 59)

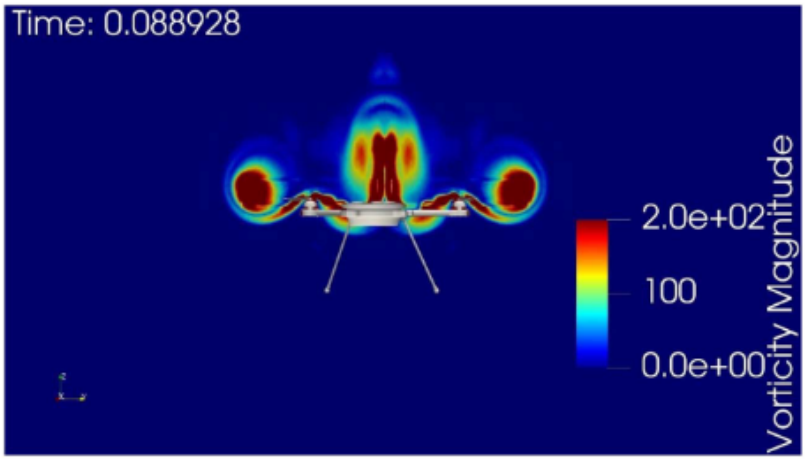

Figure 9: Vorticity contour around quadrotor at 5-m/s descent rate, V Z=V h ¼ −1.08 (McQuaid et al. 2020, 7)

NASA Ames Research Center conducted an experimental investigation into the possible implications of VRS in a tiltrotor aircraft. The experiment was conducted in a Wind Tunnel and used a smaller scale model of the left-hand rotor of a V-22 Osprey. This test only modeled one tiltrotor hub as opposed to two side-by-side rotor hubs like that on the V-22. By varying the advance ratios (V/Vtip), the collective blade pitch (θ), and the tip-path-plane angle-of-attack (α) and keeping the rotor tip speed (Vtip) constant, the experiment tested the effect of VRS on the mean rotor thrust and power and oscillatory rotor thrust.

The data showed that mean rotor thrust reduces at a high descent angle (20 – 45 deg) because of the recirculation of the rotor wake and development of VRS. The power remains unchanged and unaffected by VRS and is determined by the aircraft's collective pitch angle (Betzina, p. 1). The oscillatory rotor thrust fluctuations increase in accordance with the parameters from the

mean rotor thrust reduction, and they can cause low frequency roll oscillations in a two-rotor configuration.

This study concludes that further research is needed to determine the requirements for an automatic control system that can respond to these low-frequency roll oscillations.

Tiltrotor aircraft require a higher rate of descent to enter VRS because of higher disk loading and more thrust generated than traditional helicopters. However, once the aircraft enters VRS it can be significantly more difficult to exit because of a lack of power to initiate forward flight. The two rotor systems may also lose lift at different times causing a tendency to roll.

Tiltrotor engineers must consider VRS when designing new aircraft and conducting hazard analysis.

2.4.1.2 Retreating Blade Stall

An aerodynamic phenomenon known as retreating blade stall (RBS) exists in helicopters in forward flight. Velocity of airflow on the retreating blade decreases in forward flight and demands higher Angle of Attack (AOA) to generate the same lift as the advancing blade. RBS is depicted in Figure 10. As airspeed increases, the "no-lift area" on the retreating blade side of the wing-span increases until eventually the blade tip stalls. Tip stall results in the aircraft rolling left or right, depending on the rotational direction of the rotor system, and pitching the nose up. RBS is possible for single or tandem rotor systems like that in a tiltrotor aircraft.

As automation has increasing authority in aircraft flight and maneuvering, it is important for the system to have limits or mitigation in place that avoid increasing the AOA to the point of critical stall. Aviators can reduce the effects or recover a helicopter from retreating blade stall by reducing the collective (or reducing AOA), reducing airspeed, descending to lower altitude, increasing rotor RPM to normal limits, or reducing the severity of their maneuvering ("Fundamentals of Flight" 2022, 85).

In tiltrotor aircraft, maneuverability requires more reaction time, so the possibility of recovery from retreating blade stall could be impossible in certain contexts.

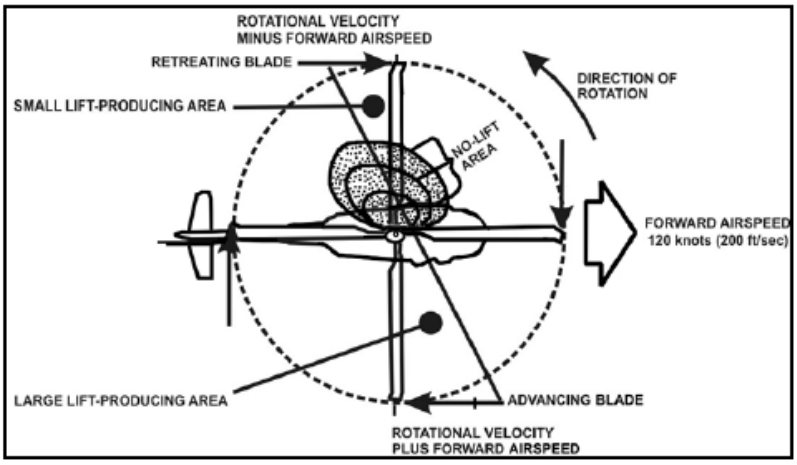

Figure 10: Retreating Blade Stall (Normal Cruise Lift Pattern) ("Fundamentals of Flight" 2022, 64)

2.4.1.3 Aerodynamic Stall

A fixed-wing aerodynamic stall occurs when an increase in the airfoil AOA reaches a critical point and no longer produces lift. Most common in take-offs and landings, stalls occur during low airspeed flight envelopes, which require higher AOA to produce lift. When the AOA increases, the pressure differential between the top and bottom of the airfoil creates boundary layer separation and turbulent airflow. Figure 11 shows this boundary-layer separation and depicts an increase in turbulence on the 20-degree airfoil. A stall can occur in tiltrotor aircraft when the nacelles are operating at a forward angle and unable to produce enough lift for slow airspeeds or hover.

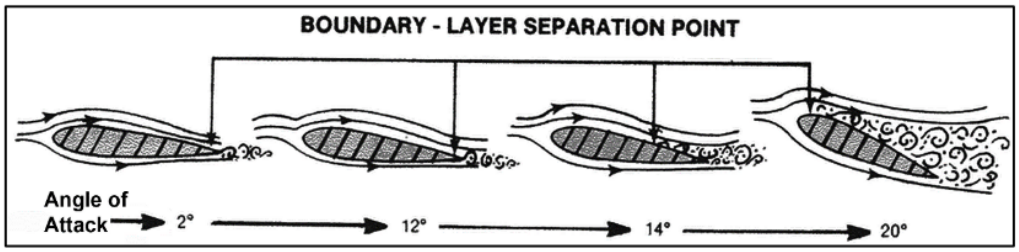

Figure 11: Boundary Layer Separation Point for Various Angles of Attack ("Fundamentals of Flight" 2022, 253)

2.4.1.4 Tiltrotor Conversion Corridor

It is important to identify a conversion corridor for tiltrotor aircraft, which displays the conversion angle of the pylon, or nacelle, tilt versus the true airspeed. Conversion corridors highlight the operating envelope for safe flight through avoidance of aircraft wing stall and breaching cruise torque limits.

Figure 12 shows a typical conversion corridor for a tiltrotor aircraft and includes different gross weights for reference (Appleton 2020, 26). The appropriate terminology for pylon angle moving up or more perpendicular with the ground is "conversion." For a pylon moving down, or more parallel with the ground, the term is "transition." At a hover, or zero forward airspeed, the optimal pylon angle will be around 90°, and for the most efficient forward airspeed the pylon angle will be at 0°.

When the aircraft pylons undergo a conversion or transition, the flight controls change modes, and the pilots must alter their operational techniques. These control changes are described in section 2.4.2 Pilot Training. When a tiltrotor aircraft falls within the conversion mode, it is at risk for more hazardous states because it operates without the full benefits of vertical lift or forward thrust and can result in unpredictable aerodynamic behavior that jeopardizes flight stability.

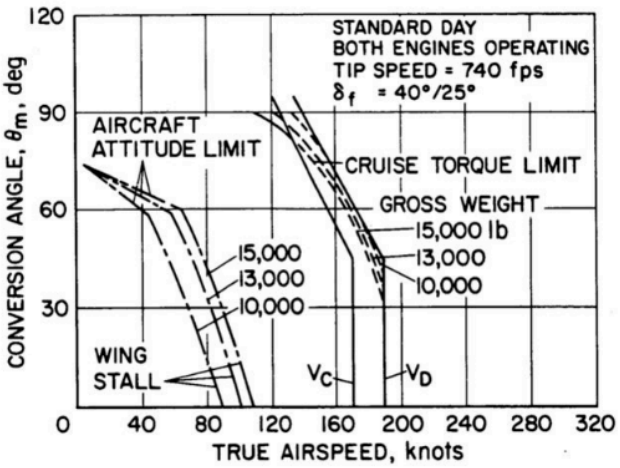

Figure 12: Illustration of a typical conversion corridor highlighting the operating envelope as a function of the airspeed and rotor tilt. The conversion angle is 90° for rotors vertical and 0° for rotors horizontal (Appleton 2020, 26)

2.4.1.5 Unique versus Displacement Trim

Trim is a flight vehicle control that neutralizes forces on aircraft to maintain steady flight paths without constant input from the pilot. While trim is a feature of all types of aircraft, its application is different on rotary, fixed-wing, and tiltrotor aircraft.

In a helicopter or tiltrotor, trim refers to how the cyclic control behaves in response to the aircraft's automatic adjustments for aerodynamic forces like rotor torque, asymmetric lift, or environmental factors. In unique trim, when the pilot makes an input on the cyclic to change the flight attitude, the cyclic temporarily adjusts to the new position but then returns to its original center point once the input is released. Unique trim is different from displacement trim, where the cyclic's center point changes after an input.

Unique trim ensures that, while the flight control system automatically handles minor corrections, the pilot retains precise control over the aircraft without permanently altering the cyclic's neutral position, thereby maintaining a steady flight path.

The operational differences between unique and displacement trim can cause mode confusion for pilots who may have an incorrect, inaccurate, or limited process model of them.

2.4.1.6 Fly-by-wire versus Mechanical Control

Fly-by-wire and mechanically controlled aircraft represent two distinct approaches to flight control systems. In mechanically controlled aircraft, pilots use direct, physical linkages such as cables and rods to operate control surfaces and mechanisms. For tiltrotor aircraft, control surface operation includes controlling the rotor blade pitch angle with the collective or TCL, adjusting the rotor disk tilt with the cyclic, and adjusting the nacelle or pylon angle for transitioning between vertical and horizontal flight. This traditional method offers a direct connection between pilot inputs and aircraft responses but can be limited in terms of automation and adaptability.

In contrast, fly-by-wire systems utilize electronic controls instead of mechanical linkages. Pilots enter commands via electronic interfaces, which are then interpreted by computer systems that send precise signals to the control surfaces or mechanisms. This design allows for greater automation and augmentation, including advanced flight management features and stability control.

Fly-by-wire systems offer the flexibility to implement sophisticated control laws and assist with handling characteristics that would be challenging with purely mechanical systems. However, it requires a pilot's thorough understanding of how physical inputs are interpreted and implemented by the computer to avoid mismanagement. It also demands a system design that provides a clearly understood interface of how the computer interprets the pilot's control inputs.

2.4.2 Pilot Training

Rotary, fixed-wing, and tiltrotor flight training regiments require different techniques and knowledge bases. A pilot solely trained on rotary wing flight will not have the knowledge to fly a fixed-wing or tiltrotor aircraft and vice-versa. It is important to recognize the differences between the three training regimens when analyzing tiltrotor aircraft because pilots must operate three different modes of flight: helicopter, conversion, and airplane. This raises the question: should tiltrotor pilots be trained first on rotary or fixed-wing flight before tiltrotor operation? Does the order have any effect on pilot efficiency? Lapses in knowledge between the different flight regimes can contribute towards mode confusion when the automation may act in helicopter, conversion, or airplane modes.

2.4.2.1 Rotary

Rotary wing flight training begins with learning how to hover the aircraft with zero forward airspeed. The student pilot develops the skills necessary to hover by using three different controls: the collective (pitch), cyclic (roll), and the pedals (yaw). Although the three different controls directly contribute towards and alter the indicated angular motions (pitch, roll and yaw), they can each indirectly influence one another through simultaneous manipulation. The student pilot is then trained on the transition from hover to forward airspeed and back to hover. The collective is primarily used for altitude adjustments while the cyclic is used for airspeed manipulation. When the pilot pulls up on the collective, the aircraft altitude increases. This distinction is important when considering the differences in control inputs between fixed-wing and tiltrotor aircraft.

Rotary wing flight students also learn how to avoid settling with power resulting from Vortex Ring State. They must conduct descents to the ground from various altitudes in-ground-effect (IGE) and out-of-ground effect (OGE). Ground effect occurs when the airflow from a rotor system impacts the ground, resulting in a reduction in induced drag and a more horizontal relative wind. IGE occurs, for most helicopters, at one length of its rotor-disk in vertical height. OGE occurs anywhere above the rotor-disk height ("Fundamentals of Flight" 2022, 34).

Understanding and performing aircraft hover and approaches-to-land from IGE and OGE heights is required. This training prepares rotary-wing pilots to avoid settling with power and vortex ring state effects by understanding the power requirements necessary to fly the aircraft. Fixed-wing pilots are not trained on VRS because airplanes are not susceptible to it.

2.4.2.2 Fixed-Wing

In fixed-wing training, a pilot learns how to manipulate the primary controls including the yoke or stick, throttle, and rudder pedals. A pilot-in-training will learn the basics of take-off, cruise flight, landing, stall avoidance, unusual attitude recovery, and other emergency

procedures. Most standard, fixed-wing aircraft do not have the ability to hover so that task is not included in fixed-wing training.

When the pilot pulls the yoke back, it raises the aircraft's elevators (the horizontal stabilizers on the tail), increasing the pitch angle and causing the plane to climb. Pushing the yoke forward lowers the elevators, decreasing the pitch angle and leading to a descent.

Adjusting the throttle changes engine power, which affects airspeed. Increasing power results in higher airspeed and a steeper climb, while decreasing power reduces airspeed and results in a shallower climb or descent.

The pedals control the aircraft's rudder, a vertical stabilizer located at the tail that adjusts yaw, or the side-to-side movement of the nose. Pressing the left pedal moves the rudder to the left, causing the nose to yaw left, while pressing the right pedal moves the rudder to the right, causing the nose to yaw right ("Fundamentals of Flight" 2022, 249).

The throttle in a fixed-wing aircraft is manifested and operated differently than the collective in a helicopter, although they both control the torque of the engine. The yoke or stick of airplanes versus the cyclic in a helicopter have more similarities in terms of pilot operation and aircraft reaction. The pedals in both, while they control different aircraft parts (rudders versus anti-torque rotor), are operated in a similar fashion. A tiltrotor pilot must learn and manage all of these differences for safe operation.

2.4.2.3 Tiltrotor

A tiltrotor student pilot's flight training regimen typically begins with fixed-wing training, where they learn the fundamentals of flying airplanes. Once proficient in fixed-wing flying, the student transitions to rotary-wing training, where they learn to control helicopters in hover, low-speed flight, and vertical takeoffs and landings. This phase emphasizes the unique aspects of rotary-wing flight, such as the use of collective, cyclic, and anti-torque pedals and handling the aircraft in confined spaces or during low-speed maneuvers.

After completing both fixed-wing and rotary-wing training, the student moves into a tiltrotor simulator, where they practice transitioning between airplane and helicopter modes. The simulator training includes emergency procedures such as engine failures and autorotations, where the pilot practices descending safely in the event of engine loss, simulating the rotor auto-rotating to maintain control.

Finally, the student flies the actual tiltrotor aircraft. In this phase, they combine their fixed-wing and rotary-wing skills, focusing on smooth transitions between hover and forward flight and learning to manage the tiltrotor's unique aerodynamics.

The controls in a tiltrotor aircraft include a Thrust Control Lever (TCL), commonly seen in fixed-wing aircraft, a cyclic similar to that in a helicopter, and pedals. At a hover or with the rotors in the vertical position (90° pylon), the TCL adjusts the aircraft's altitude by modifying power to the rotors, effectively functioning like the collective in a helicopter. However, as the aircraft transitions forward into airplane mode, the TCL's function changes to primarily control airspeed, while altitude is adjusted through pitch (cyclic) control, just as in a fixed-wing aircraft.

This change in control function can sometimes lead to what is commonly referred to as "collective dyslexia," where pilots inadvertently attempt to use the TCL as they would a helicopter collective, leading to incorrect handling. In helicopter mode, pushing the TCL forward increases torque and power, which results in a climb, but this is the opposite of the input used in traditional helicopters, where pulling up on the collective increases altitude and pushing down

reduces it. This inversion of control inputs during mode transitions can create confusion for pilots who are not fully adapted to the tiltrotor's unique control system.

While traditional hazard analyses account for component and system failures on tiltrotor aircraft, they do not consider the unique relationship, handling qualities, and potential for mismanagement between the pilot, the automation, and augmentation. Systems Theory and STAMP provide a way forward to account for all of these controllers.

2.5 Systems Theory Approach to Safety

Systems theory focuses on the whole system as opposed to analyzing its individual parts. The interaction of smaller components at various hierarchical complexities in a system can create greater system properties through the idea of emergence. For example, the properties of an aircraft engine and rotor system operating on their own are different than the interactions and dependencies they have with one another when put together in an aircraft. Their operations affect and depend upon one another. Reliability, the probability that an individual part will perform its specification over time, is a component level property whereas safety is an emergent property due to its dependence on the analysis of an entire system plus its component's interactions. Emergent properties of a system can be seen in Figure 13.

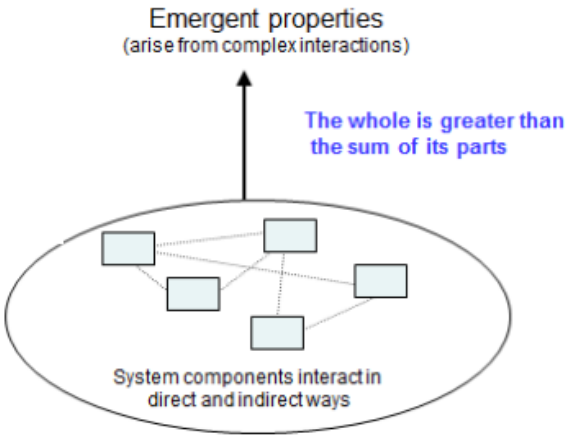

Figure 13: Emergent Properties in System Theory (N. G. Leveson 2019, 28)

2.5.1 STAMP Accident Model

A causality model based on systems theory called STAMP (Systems-Theoretic Accident Model and Processes), focuses on enforcing system behavioral constraints as hazard prevention as opposed to solely analyzing and preventing component level failures. Traditional hazard analyses utilize and depend upon linear chain of events to identify potential accident causation and component failures. The result for hazard prevention is then redundancy in system components to serve as mitigation for failure (N. G. Leveson 2012, 75).

As systems grow in complexity, have more software components, and have higher dependence on automation, these traditional hazard analyses are no longer sufficient in ensuring safety. STAMP, in contrast, looks at a larger vantage point of entire systems including the human and sociotechnical interfaces. Non-failure interactions, indirect or non-linear causes, and design flaws are all considered in this accident model, which make it a unique and more encompassing approach.

STAMP is built on three primary concepts – safety constraints, hierarchical safety control structure, and process models.

Identifying safety constraints for the design and operation of a system includes not only component failures but also the interactions between components that could be potentially hazardous. Once a constraint is identified, a control must be created to enforce that constraint.

A hierarchical safety control structure represents the controls in a system that manage its constraints. "Control processes operate between levels to control the processes at lower levels in the hierarchy" (N. G. Leveson 2012, 103). Accidents occur when there are inappropriate or missing constraints as well as inadequate control of constraints. Figure 14 shows a generic control structure in the aviation industry. It includes the physical aircraft and the human component.

The third concept required in STAMP is the process model, which is a human or automated controller's understanding of the process being controlled. The process model must include, at a minimum, the required relationship among system variables, the current state of the system, and the possible ways the process state can change.

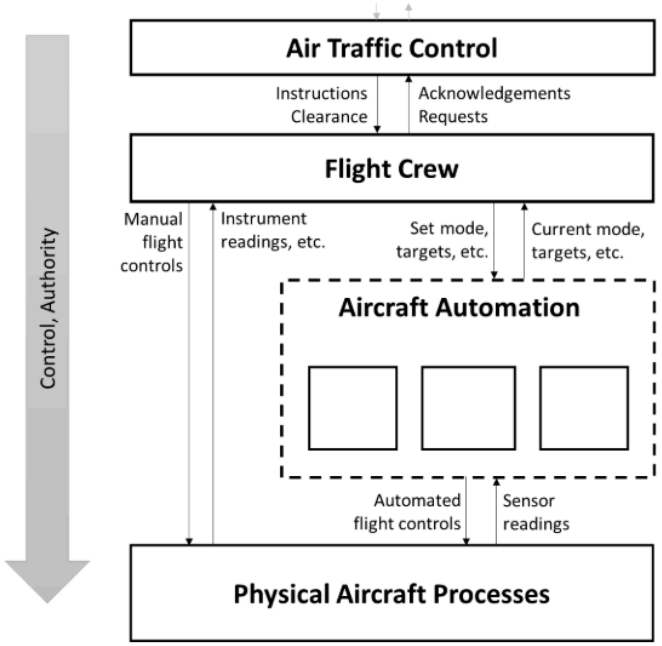

Figure 14: Aviation example of a hierarchical control structure (N. G. Leveson and J. Thomas Mar2018, 24)

2.5.2 CAST Overview – Causal Analysis Based on Systems Theory

Causal Analysis Based on Systems Theory (CAST) is an accident focused analysis based on STAMP. Instead of solely identifying root causes or causal factors in an accident like most traditional post-accident analyses, CAST identifies weaknesses in a system's control structure and systematic design flaws. It ultimately looks for why an accident occurred and how to prevent it from happening in the future through comprehensive recommendations for design improvement. An accident is defined as an undesired, unacceptable, and unplanned event that results in a loss (N. G. Leveson 2019, 9). A loss is anything of value to the stakeholder of a particular system.

CAST has five parts depicted in Figure 15. The first step is to collect basic information for not only the accident that occurred but the entire system. This includes the environment, hazardous states that led to the specific loss, system constraints that should exist based on the hazards, events surrounding the accident, questions that remain unanswered about the events, and missing or inadequate physical controls of the system.

Step 2 involves modeling the existing hierarchical safety control structure. This provides an abstraction of the controls and feedback loops of the system.

Step 3 examines the control structure components to determine how and why they were ineffective and did not prevent hazardous states or losses.

Step 4 then examines the entire control structure for more wholistic, systematic factors that may have contributed towards the loss. This portion focuses on component interactions and why together they did not satisfy system safety constraints.

The fifth and final step in CAST is to provide recommendations for control structure changes needed to prevent system losses in the future.

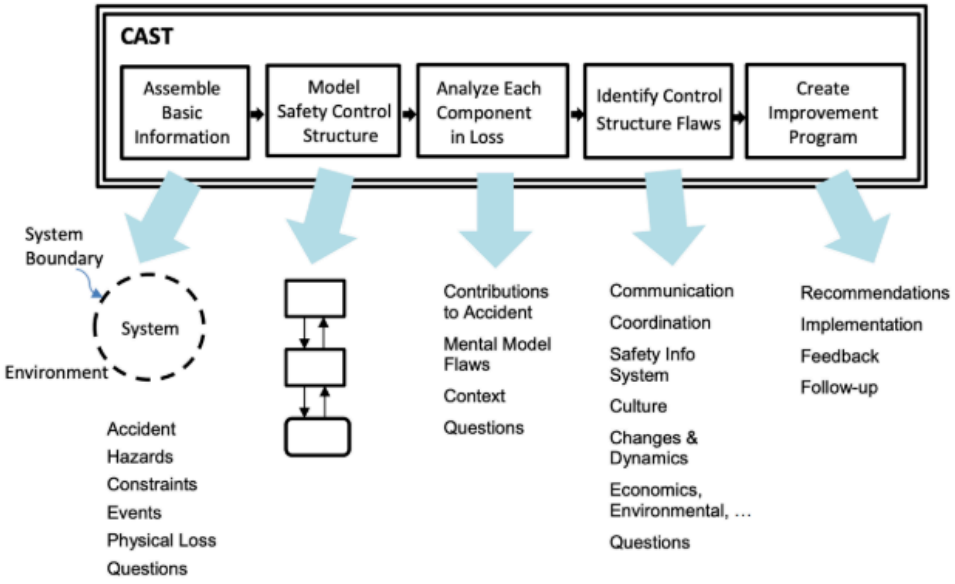

Figure 15: Five steps of CAST (N. G. Leveson 2019, 34)

2.5.3 STPA Overview – System Theoretic Process Analysis

System Theoretic Process Analysis (STPA) is a top-down hazard analysis technique based on the STAMP causality model. Unlike traditional hazard analyses, the goal of this relatively new technique is to identify scenarios that can lead to accidents based on design errors, component interactions, human decision-making errors, and socio-technical contributions. Further information about STPA can be found in the STPA Handbook (N. G. Leveson and J. Thomas Mar2018).

STPA is unique in that it can be used at any point in a system design process and provides necessary remedying information for system design, manufacturing, and development. Figure 16 shows the 4-step process of STPA.

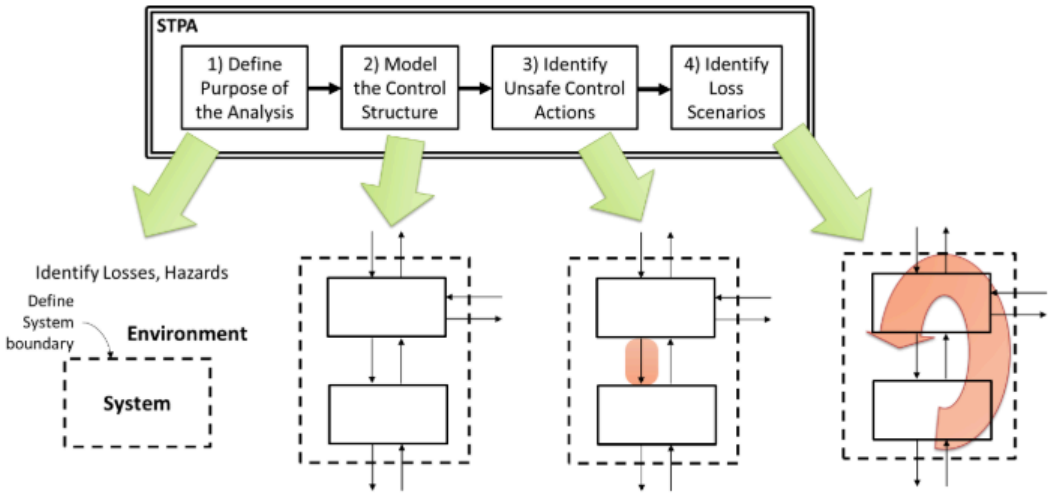

Figure 16: Overview of the STPA Method (N. G. Leveson and J. Thomas Mar2018, 14)

The first step in STPA is to define the purpose of the analysis in terms of the system boundary, its surrounding environment, and the undesirable losses and hazards. The boundary and environment of the system are determined by the analyst and should aim to include elements of the system that the designers can control. A loss is something valuable to the stakeholder (producer, owner, customer). Examples of losses include loss of life, loss of mission, or loss of property. Hazards are defined as "system states or sets of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" (N. G. Leveson and J. Thomas Mar2018, 17). It is important to identify hazards at the system level as opposed to component-level causes or environmental states that are outside of the designer's control.

Step 2 in STPA is to model the hierarchical control structure, as defined earlier. A generic control structure is shown in Figure 17, modeling the relationship between a controller and the controlled process through actions and feedback. The control actions exist to enforce constraints on the controlled process, and the feedback allows the controller to update its process models. Control structures are not only physical or executable models of systems but rather functional or relationship models. Control structures are created and adjusted at varying levels of abstraction deemed applicable for the purposes of the analysis.

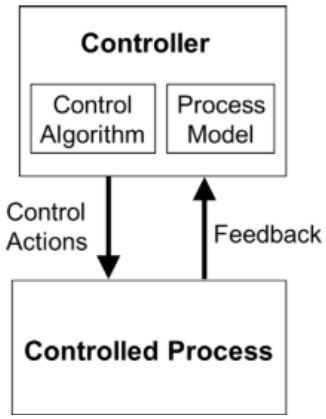

Figure 17: Generic Control Structure (N. G. Leveson and J. Thomas Mar2018, 23)

The third step in STPA is to identify Unsafe Control Actions (UCA), which are control actions that, in a worst-case environment or context, will lead to a hazard. Control actions may be considered unsafe through the following four ways: not providing the control action leads to a hazard, providing the control action leads to a hazard, providing the control action too early, too late, or in the wrong order is potentially unsafe, or the control action lasts too long or is stopped too soon. A UCA is modeled in the five-part format: <Source> <Type> <Control Action> <Context> <Link to Hazards>. Once UCAs are identified, the analyst will translate them into constraints on the controller behavior.

The fourth and final step of STPA is to identify the causal factors that can lead to UCAs, otherwise known as loss scenarios. Areas that may involve loss scenarios include controller faults, flawed control algorithms, unsafe control inputs, or inadequate process models. Scenarios highlight situations that could result in hazardous states for systems, and this allows developers to identify specific software, hardware, and human factors considerations for development improvements.

A scenario development technique developed by John Thomas provides a formal, top-down process for performing step 4 (Thomas 2024). Figure 18 shows this technique, which is broken down into four classes of scenarios. Class 1 involves a controller receiving the correct feedback or input but making an unsafe control action based on either an incorrect process model or inadequate control algorithm. Class 2 occurs when the feedback from a sensor, the controlled process, or another controller is inadequate, missing, or delayed and the resulting controller's action is then unsafe. Class 3 includes correct feedback to the controller and an intended "safe" control action, but the control path acts as if a UCA was provided to the controlled process. Class 4 involves correct feedback to the controller and a safe control action sent and received by the controlled process; however, the controlled process behaves in a way that is deemed unsafe potentially from component failures, outside disturbances, or changes over time.

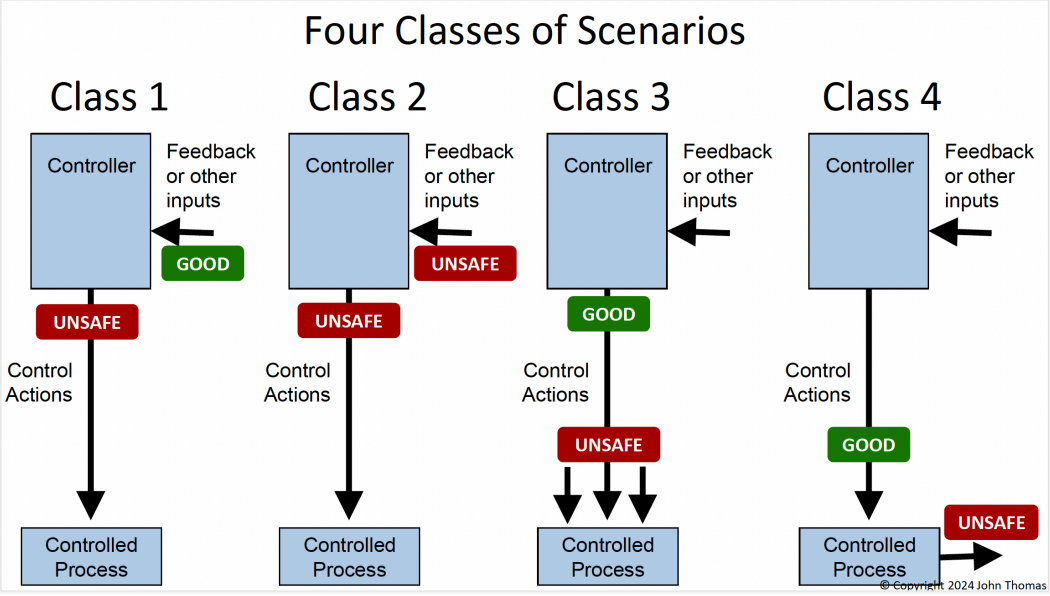

Figure 18: Classes of Loss Scenarios (Thomas 2024)

STPA differs from traditional and widely used hazard analyses as it does not generate or use probabilistic assessments Instead, STPA provides a thorough, in-depth analysis of the potential causes of mishaps so they can be eliminated or mitigated in the system design.

Chapter 3 CAST Applied to Two Tiltrotor Aircraft Accidents

This chapter presents a summary of the CAST results from two accidents, illustrating how current aircraft safety hazard analyses fall short in identifying and mitigating the risk of mode confusion during the early design phase of tiltrotor aircraft.

3.1 Summary of MV-22B Osprey Tiltrotor Hydraulic Line CAST Results

All information used for this analysis is from public sources ("Osprey Aircraft Crash" 2000) (Richard Whittle 2010) (General John R. Dailey et al. 2001). On December 11, 2000, an MV-22B Osprey tiltrotor aircraft, callsign Crossbow 08, crashed in North Carolina during a routine training mission killing all four crewmembers onboard. The aircraft was conducting night vision-aided flight and planned radar approaches into Marine Corps Air Station New River when it experienced a hydraulic line failure and a flight-control system software anomaly. These were the primary causal factors determined from the Judge Advocate General (JAG) investigation report.

3.1.1 Basic Information

The first step in CAST is to compile basic information about the accident. The system involved includes the aircraft, the aircrew, the Marine Medium Tilt Rotor Training Squadron 204, the aircraft manufacturers, the aircraft maintainers, the aircraft regulatory certifiers, Air Traffic Control (ATC), and the airport facility. The losses include the aircraft crashing into the ground during a routine training flight and the death of all aircrew members. The hazards that led to the losses and the resulting safety constraints for system design are the following:

System Hazard 1: Aircraft can no longer be controlled
Safety Constraints:
1. Aircraft must be physically capable of making a safe takeoff, cruise flight, and landing.
2. Aircrew must be trained and evaluated on safely operating the aircraft in accordance with limitations.
3. Physical constructs of the airfield must account for aircraft emergency landings and must minimize potential public damage.

System Hazard 2: Minimum aircraft separation standards are violated (terrain, miscellaneous objects)
Safety Constraints:
1. Aircraft must maintain adequate separation from outside objects.
2. Aircraft must identify and rectify separation standard violations.

System Hazard 3: Structural Integrity of the aircraft is violated
Safety Constraints:
1. Maintenance standards must be enforced to ensure aircraft structural integrity throughout all phases of flight.

Table II lists the proximal event leading up to the loss of the MV-22B, Crossbow 08, and follow on questions raised.

Table II: New River Accident Timeline of Events

ID	Event	Questions
1	On 11 December 2000 at 15:30, MV-22B Osprey Aircraft "Crossbow 08" failed a preflight inspection due to a missing fastener on the wing. The aircrew was redirected to another Osprey that also had a malfunction, which deemed it "down." After a required maintenance inspection, Crossbow 08 was then cleared to fly.	• How long had Crossbow 08 had a missing fastener on the wing? • Does the unit conduct post-flight inspections to account for maintenance problems before the next day's scheduled flights?
2	16:41 The Pilot in Command (PC) and Pilot #1 take off in Crossbow 08 for day familiarization flight. This was one hour and 11 minutes later than the planned take off time for the first Pilot in the training rotation.	• Did the crew re-brief or change the plan based on the delayed takeoff time? • Was the entire crew aware of any changes for the plan? • Is there a procedure in the unit that must be followed for last minute flight changes?
3	17:39 Pilot #1 switches with Pilot #2 and Crossbow 08 takes off for night flight training under night-vision-goggles (NVG).	• Was the PC training faster than planned due to the delay? • What restrictions are in place for EENT (end evening nautical twilight) flight under NVGs?
4	19:18 PC transitions Crossbow 08's nacelles forward to airplane mode, accelerates airspeed to 160 knots, climbs in altitude to 1,400 feet, and takes direction from ATC for a planned radar approach.	• Did the PC or the automation tilt the nacelles? • How does the nacelle automation interact with the flight director (FD) automation for altitude and airspeed?

5	19:23 Crossbow 08 turns to 230 degrees and the automatic flight control system begins raising the nacelles to convert to helicopter mode.	• Did pilots typically let the automation adjust the nacelle angles or did they do it manually? • What were the regulations or guidance in training or for unit operation for how to transition between auto and manual modes?
6	19:23:40 A main hydraulic line ruptured that feeds the aircraft's left swash plate actuators.	• How long had the hydraulic line been damaged before the rupture point? • What are the scheduled and unscheduled maintenance procedures for the hydraulic systems? • Was there pre-knowledge of hydraulic line chaffing on this aircraft or other aircraft in the past?
7	19:23:42 HYD 1 FAIL light illuminates on cockpit display.	• What troubleshooting training does the crew have experience with for hydraulic failures? • What emergency procedure (EP) practice and experience do the aircrews have? • Are there simulator EP requirements for aircrews?
8	19:23:45 New River ATC radios Crossbow 08 and gets no response	• How long does ATC allow for no response from aircrews before troubleshooting or declaring emergencies?
9	19:23:46 HYD 3 FAIL, CRITICAL SWPL FAULT, and PFCS (Primary Flight Control System) caution lights illuminate because the fail-safe mechanism in System Three shuts off fluid before it gets to the leak point. This causes the automatic system for tilting the nacelles to disengage with the rotors at 11 degrees still in airplane mode.	• Why did the software illuminate the PFCS reset button? • Why does the automation of the nacelle tilting shut down with hydraulic failures?

		• Was manual control of the nacelles still an option for the pilots?
10	19:23:48 One of the pilots pushes the PFCS reset button. All faults remain illuminated and the computer sets the pitch of the rotor blades flat, reducing the angle the blades impact the air. Crossbow 08's nose pitches up	• Were there simulator or EPs that prepared pilots for outcomes from pushing the PFCS reset button?
11	19:23:49 One of the pilots pushes the control stick and thrust control forward in response to the abrupt aircraft movement, which causes an engine overspeed with the rotor blades at flat pitch.	
12	19:23:50 Overspeed protection signals the swashplate actuators to restore the blades to previous angles, and with only one hydraulic system to control the left nacelle, there is an uneven balance between the two rotor systems.	• Why does the system design not have equal distribution of hydraulic power when one or more of them fails? Does this not negate the redundancy of having multiple hydraulic pumps?
13	19:23:51 Crossbow 08's nose whips left and causes a roll in that direction	• Is there a system design for tiltrotor that could have prevented the tendency to roll with uneven distribution of power between nacelles?
14	19:23:52 PC attempts to center the nose and level off, causing multiple additional warning advisories on the cockpit display to include 1 &2 torque sensor flt, load limit flt, multi swpl fault, r&l fadec b turbine overspeed, r&l eng np overspeed.	
15	19:23:54 One of the pilots pushes the PFCS reset button for the second time, which causes the rotor blades to go to zero-degree pitch and attempt to reset the two nacelles at different speeds. This leads to the aircraft slowing down, speeding up, and yawing left.	• Why was the software designed to reset the pitch angles? Was this known to the pilots? • Could there have been a hazard analysis on this function when engineers were writing the control laws?
16	19:23:55 – 19:24:05 The pilots push the PFCS reset button 9 times	• Why were the pilots trained to continuously press the reset button? • What did they think resetting the button accomplished?

17	19:24:06 PC declares aircraft emergency to ATC	
18	19:24:10 Crossbow 08 crashes in marshy area seven miles north of New River airport in nose-down altitude.	

3.1.2 Control Structures

The following control structures for the Crossbow 08 accident depict the systems analyzed in CAST. There is one higher-level control structure, which includes the regulatory bodies and the Marine Corps Unit involved. There is one aircraft-level control structure, which helps narrow the focus more towards the physical components of the MV-22B and their interactions with the flight crew and the automation.

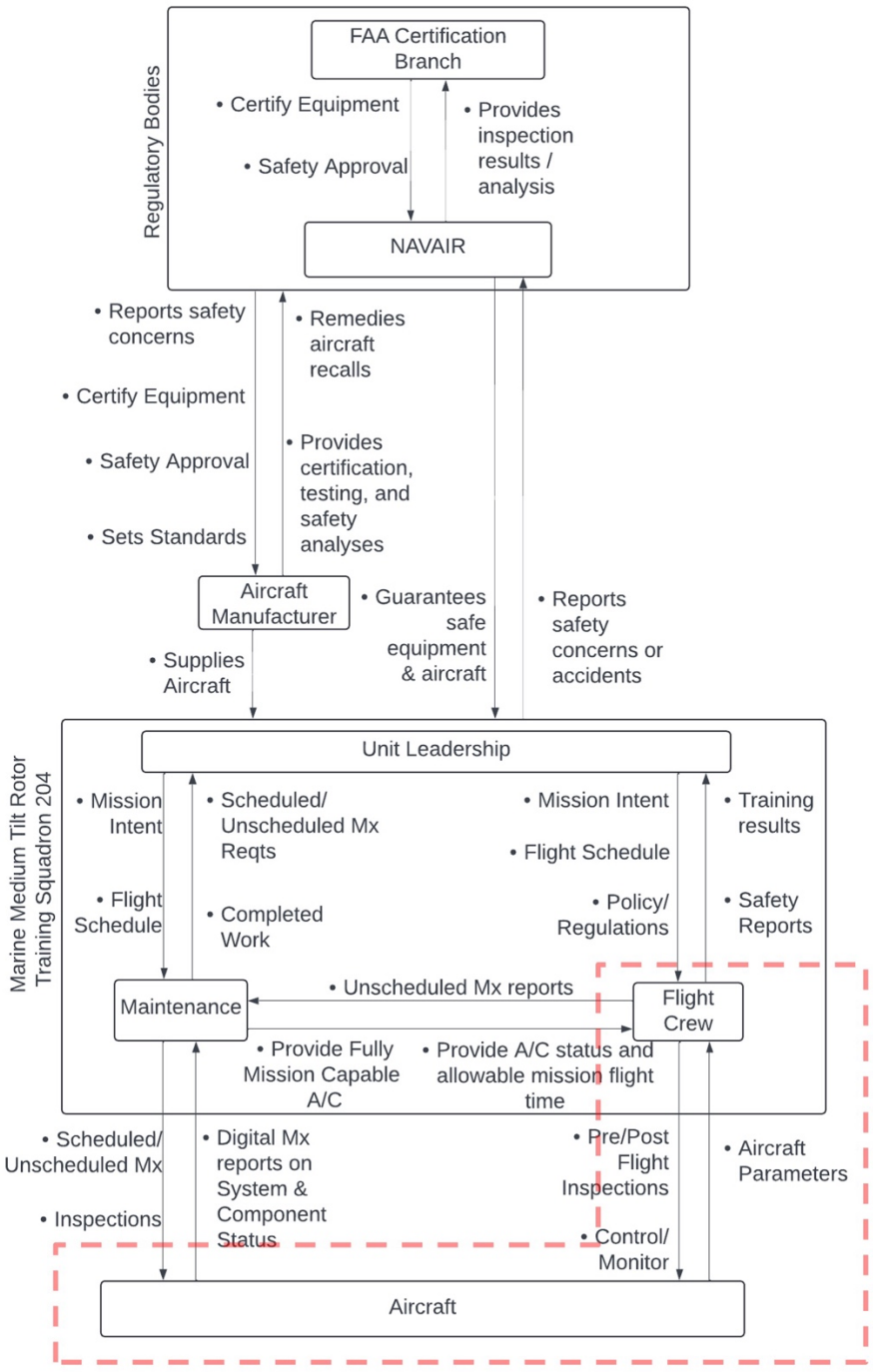

Figure 19: New River MV-22B High-Level Control Structure

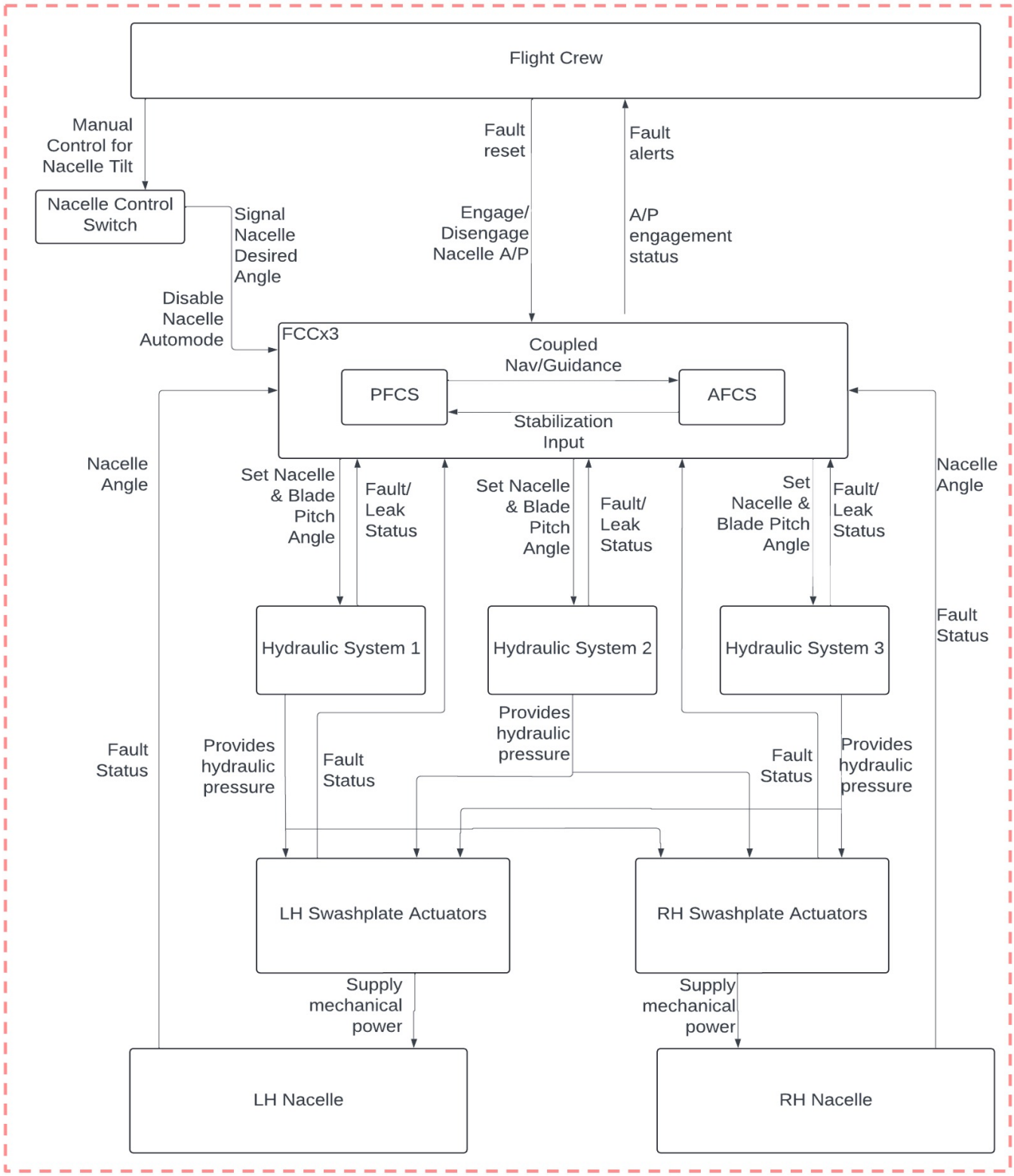

Figure 20: New River MV-22B Aircraft-Level Control Structure

3.1.3 Component Contributary Factors in the Losses

The next step is to examine what role each controller played in the losses and possible explanations for their behaviors. This step helps identify why the current design of the system did not prevent the accident.

3.1.3.1 Role of Physical Components

The primary physical components involved in this MV-22B accident include the three hydraulic pumps, the two actuators, and the two nacelle systems. Together, these constitute the tiltrotor system, which ultimately is the controlled process in this analysis. When analyzing the physical components, the system responsibilities and controls list the required attributes needed for safe operation of this type of aircraft. The next step determines whether the aircraft failed to meet those requirements or if other non-failure interactions led to the loss.

Responsibilities:

The physical components of this system must deliver safe operation and function throughout use. They must provide:

1. Controllability of the aircraft through ground and air maneuvers.
2. Aircraft structural integrity–operation within the limits of material and structural capabilities.
3. Feedback to the human and automatic controllers on operational status.

Safety Controls:

The controls for these physical components include:

1. Sensors
2. Cockpit displays for feedback
3. Alarms (FAIL/LEAK)
4. Redundant components
5. Scheduled and unscheduled maintenance inspections

Missing or inadequate aircraft physical attributes

This accident did experience physical component failure, but additionally it involved unsafe interactions of physical components, missing controls, and design flaws.

1. The hydraulic line 1 experienced continuous chaffing when the nacelle system would tilt. This chafing resulted in a hydraulic leak, which shut down hydraulic pump 1 and isolated hydraulic pump 3, which shared the same line bundle.
    a. The line bundle was located at a portion of the aircraft that was not easily inspectable or visible to maintainers or aircrew–resulting in a missing safety control for inspection criteria.
    b. The hydraulic system isolation caused an uneven balance of power to the two nacelle rotor systems, resulting in uncontrollable operation of flight and ultimately aircraft impact with the ground.

Recommendations:

- Restructure the wire bundle and hydraulic line casing to avoid chaffing.
- Create a window on the airframe near the hydraulic line and wire bundles for easy inspection access.
- Redesign the sensor placement in the hydraulic lines for leak logic and isolation.

3.1.3.2 Role of each Controller in the Losses

Flight Control Computer [FCC]

Responsibilities:

- Translate pilot flight control input into the fly-by-wire system for aircraft operation.
- Provide autopilot (A/P) function for aircraft controllability.
- Provide fault alerts and component status to flight crew.

FCC Control Actions:

- **FCC-UCA-1:** The FCC reset the pitch of the rotor blades to zero and altered the thrust of the two rotor systems when the pilot pressed the PFCS reset button when hydraulic power was uneven to the two rotor systems.
- **FCC-UCA-2:** The FCC stopped the automatic mode of the tiltrotor during a transition state between airplane and helicopter mode.
- **FCC-UCA-3:** The FCC cut off hydraulic pressure from the number three pump to the LH nacelle because of the leak in the number one system, attempting to isolate the leak and not cause a failure in the number three system.

FCC Process Model Flaws:

- **FCC-PMF-1:** The FCC believed that an entire computer system reset was needed when a hydraulic pump failed [FCC -UCA-1].
- **FCC-PMF-2:** The FCC believed that there was not enough power to continue tilting the two nacelle systems because of one hydraulic system failing [FCC-UCA-2].
- **FCC-PMF-3:** The FCC believed that by cutting off the line to the third hydraulic pump, it would isolate the leak and prevent further component failures [FCC-UCA-3].

FCC Contextual Factors:

- **FCC- CF-1:** The uneven distribution of hydraulic power to the nacelles alone would not have caused complete aircraft uncontrollability, but it did when combined with the resetting of the blade pitch angles, thrust power, and tiltrotors in conversion mode [FCC-UCA-1,2,3].

Questions raised:

- Why did the FCC software determine that it needed a full system reset from only one hydraulic pump failure?
- What criteria existed in the logic to stop nacelle tilting?

Recommendations:

- Reassess the algorithm that resets the PFCS when the button is pushed to determine all responses.
- Conduct testing on PFCS resets with other flight control component failures, leaks, or resets.
- Create a criterion in the nacelle tilting logic to determine if the angle should end in helicopter or airplane mode, but not conversion mode during PFCS resets.

Flight Crew [FC]

Responsibilities:

- Maintain personal training and qualification requirements per unit and FAA standards.
- Operate aircraft within physical and structural limits.
- Familiarize oneself with aircraft emergency procedures and respond according to aircraft manuals.
- Conduct pre-flight and post-flight aircraft inspections.
- Ensure aircraft automation is conducting expected tasks.

Flight Crew Control Actions:

- **FC-UCA-1:** Pilot in Command (PC) and Pilot #2 (PI) collectively pressed the PFCS reset button 9 times, each time allowing the PFCS to reset the blade pitch angles and thrust power level.
- **FC-UCA-2:** The aircrew did not take the tiltrotor nacelles out of conversion mode, allowing the aircraft to operate in an unstable state by not producing adequate amounts of lift.
- **FC-UCA-3:** The pilots made both inadvertent and deliberate, abrupt movements in the cyclic and pedals in response to the uncontrollable aircraft movements from the PFCS resets.
- **FC-UCA-4:** Pilot #2 did not maintain night-vision goggle (NVG) currency in accordance with unit standards and flew under NVGs during this flight.
- **FC-UCA-5:** PC and PI #2 did not complete their monthly emergency procedures examination.
- **FC-UCA-6:** Aircrew did not identify the hydraulic line chaffing on preflight inspections.

Flight Crew Process Model Flaws:

- **FC-PMF-1:** The aircrew believed, from training manuals and documented emergency procedures, that if the PFCS reset light was illuminated it must be pressed. There were no limits or consequences to the number of times it can be pressed [FC-UCA-1].
- **FC-PMF-2:** The aircrew believed that by pressing the PFCS reset button, the system would be able to recover from the uncontrollable movements [FC-UCA-1].
- **FC-PMF-3:** The aircrew believed that the unit maintainers provided an aircraft with no maintenance concerns or problems [FC-UCA-6].

Flight Crew Contextual Factors:

- **FC-CF-1:** The abrupt movements of the helicopter, caused by the PFCS reset, caused the pilots to inadvertently move the cyclic and pedals by physical pushing into them [FC-UCA-3].
- **FC-CF-2:** Aircrew did not complete entire emergency procedures for all the illuminated faults [FC-UCA-1,2,5]
- **FC-CF-3:** The hydraulic line chaffing on this aircraft went unnoticed and undocumented by maintainers and aircrew on aircraft inspections and checks [FC-UCA-6].

Questions raised:

- Did the aircrew have experience with these types of emergency procedures in training or the simulator?
- What were the procedures for responding to tiltrotor auto-mode failures?
- What are the priorities for emergencies when an aircrew experiences multiple at one time?

Recommendations:

- Conduct testing on nacelle tilt angle scenarios to determine conversion corridor emergency procedures.
- Reconstruct emergency procedure priority classification for when multiple emergency procedures are experienced.
- Educate flight crews on active safety bulletins for maintenance awareness.

Unit Maintenance [UM]

Responsibilities:

- Conduct scheduled and unscheduled aircraft maintenance tasks.
- Deliver Fully Mission Capable (FMC) aircraft to aircrews for safe operation.
- Provide the allowable aircraft hours and mission tasks for designated aircraft.
- Provide aircrews feedback when maintenance concerns or faults are discovered.
- Track aircraft digital reporting system information before and after each flight.
- Inform unit leadership about fleet maintenance status for mission and training flight scheduling.

UM Control Actions:

- **UM-UCA-1:** Maintainers did not identify hydraulic line chaffing on any inspection or maintenance task for Crossbow 08.
- **UM-UCA-2:** Maintainers did not identify PFCS software anomaly on post-flight digital reports.
- **UM-UCA-3:** Maintainers hastily remedied a missing wing fastener on Crossbow 08 and designated it as the training aircraft, assuming that there were no other maintenance problems.

UM Process Model Flaws:

- **UM-PMF-1:** Maintainers believed that aircrew preflight and postflight inspections would catch potential hydraulic line chaffing or other non-routine inspection areas [UM-UCA-1].
- **UM-PMF-2:** Maintainers believed that PFCS software would report unusual flight control demands or alterations from expected performance [UM-UCA-2]

UM Contextual Factors:

- **UM-CF-1:** Reports of hydraulic line chaffing existed for other MV-22B aircraft across the Marine Corps prior to the Crossbow 08 accident [UM-UCA-1].
- **UM-CF-2:** Post-accident maintenance inspections in the unit found hydraulic line chaffing on all eight MV-22B aircraft [UM-UCA-1].
- **UM-CF-3:** Unit leadership distributed a service bulletin to the maintainers to inspect all MV-22B hydraulic lines [UM-UCA-1].

Questions raised:

- What were unit policies for jumping aircraft for maintenance issues before a training flight?
- Why did preflight and postflight inspections not include the hydraulic lines?
- Did the unit culture encourage proceeding with training missions despite multiple aircraft maintenance setbacks?

Recommendations:

- Improve reporting procedures for setbacks in maintenance requirements–for example, the restriction for viewing and inspecting the hydraulic lines or the troubled digital maintenance system.
- Provide a forum for maintainers to inform leadership with accurate maintenance readiness rates to advise flight schedule and mission planning.
- Create education plan and verification of learning for new maintenance systems.

Aircraft Manufacturer [AM]

Responsibilities:

- Design, manufacture, and certify aircraft in accordance with regulatory body requirements.
- Supply aircraft that have undergone hazard analysis.
- Ensure that aircraft undergo testing that satisfies the customer's mission requirements.
- Respond to and remedy aircraft safety reports or concerns.
- Issue aircraft recall statements to applicable customers.

AM Control Actions:

- **AM-UCA-1:** Engineers designed the MV-22B in a way that allowed for hydraulic line chaffing in the nacelle systems from a wire bundle if given too much slack when the system tilted.
- **AM-UCA-2:** Aircraft manufacturer installed the wire bundle with too much slack on Crossbow 08 allowing for hydraulic line chaffing.

- **AM-UCA-3:** Software engineers coded the PFCS system to reset the blade pitch angles and thrust power to both nacelle systems and did not report that in the operating manual for the Crossbow 08 MV-22B aircraft.
- **AM-UCA-4:** The manufacturing company did not conduct flight testing for multiple hydraulic pump failures or when hydraulic pump leaks combine with PFCS resets.
- **AM-UCA-5:** Engineers designed the aircraft in a way that did not allow routine inspection for the hydraulic lines without removing the outer skin of the aircraft, which makes an aircraft "down" without further in-depth inspections.
- **AM-UCA-6:** Engineers used titanium lines for the hydraulic lines, which are lightweight, brittle, and susceptible to chaffing.
- **AM-UCA-7:** The aircraft manufacturers did not thoroughly test the MV-22B for autorotation capability, which is a helicopter emergency landing technique when power to the engines and rotor systems is insufficient.
- **AM-UCA-8:** AM provided the mishap aircraft to the unit with six noted deficiencies that were corrected prior to the first operational flight.

AM Process Model Flaws:

- **AM-PMF-1:** Engineers assumed that the installers would always position the wire bundles with the correct amount of slack to avoid chaffing [AM-UCA-1,2].
- **AM-PMF-2:** Software engineers believed that if there were any errors in coding, flight testing would identify them [AM-UCA-3].
- **AM-PMF-3:** AM did not believe that hazardous states could arise from uneven balance of hydraulic power to the nacelle systems and, therefore, did not conduct flight testing for this scenario [AM-UCA-4].
- **AM-PMF-4:** Engineers believed the accuracy of the titanium tube certification and quality reports (the tube company was indicted for falsifying these reports) [AM-UCA-6].
- **AM-PMF-5:** AM assumed that tiltrotor aircraft and helicopters would have the same aerodynamic qualities in autorotation states and did not conduct additional flight testing [AM-UCA-7].
- **AM-PMF-6:** Engineers assumed that there was simple access to the hydraulics bay for maintenance [AM-UCA-7].

AM Contextual Factors:

- **AM-CF-1:** The AM did not conduct testing for simultaneous leaks because an actuator in the lab failed [AM-UCA-4].
- **AM-CF-2:** A previous V-22 accident in 1992 sparked a JAG investigation recommending further testing and analysis for hydraulic pump redundancy, hydraulic leak detection logic, and warnings to the flight crew [AM-UCA-4].
- **AM-CF-3:** The AM was comprised of two different contracting companies working as a team. There was historically mismanagement, disorganization of leadership, and lack of accountability in the development of the V-22 [AM-UCA-1,2,3,4,5,6,7].
- **AM-CF-4:** The factory deficiencies were not noted as causal factors in the JAG investigation [AM-UCA-8].

- **AM-CF-5:** AM utilized the U.S. Army pamphlet DA PAM 738-751 (TAMMS A) as primary guidance for determining safety of flight (SOF) conditions and discrepancies for the MV-22B.

Questions raised:
- What human factors analysis occurred in support of traditional hazard analyses completed for the V-22?
- What processes existed to identify and mitigate potential hazardous non-failure scenarios or component interaction scenarios?
- What was the breakdown of authority and responsibility between the two different aircraft manufacturers for the design and certification of the V-22?
- What were the processes for redesign and recertification after mishap recommendations?
- What policies existed for collaboration between engineers and test pilots?
- Was the AM and NAVAIR using the same regulatory guidance for SOF related issues?

Recommendations:
- Reevaluate the methods used in creating test flight requirements to analyze the potential for mode confusion between the human and automated controllers.
- Analyze non-failure scenarios that involve component interactions to improve design.
- Create a system that involves user input and feedback before design approval and implementation.
- Combine probabilistic methods of analyzing safety with scenario-based testing.
- Utilize a non-biased contractor for design safety evaluations.

Unit Leadership (VMMT-204) [UL]
Responsibilities:
- Provide mission intent and training guidance to flight crews and maintainers.
- Adjust and restructure guidance based on aircraft maintenance requirements and feedback.
- Communicate with and report to NAVAIR on aircraft status, safety reports, or information request.
- Implement aircraft recalls or safety bulletins to flight crews and maintainers.
- Report accurate and truthful aircraft maintenance status to higher authorities and regulatory bodies.
- Implement unit safety standards and policies.

UL Control Actions:
- **UL-UCA-1:** UL did not issue specific guidance to maintainers for the hydraulic line inspection criteria for all MV-22B aircraft after receiving the safety bulletin.
- **UL-UCA-2:** UL approved a training flight for the PC and PI #2 when their night currency and emergency procedure testing had lapsed.
- **UL-UCA-3:** UL verbally authorized changes to the flight schedule for the Crossbow 08 mission but did not document in accordance with regulation.
- **UL-UCA-4:** UL told maintainers to falsify readiness rate information for aircraft in the digital system to make the MV-22Bs look more flyable.

- **UL-UCA-5:** UL did not report the inconsistencies and technical errors associated with the new digital maintenance system to NAVAIR.

UL Process Model Flaws:

- **UL-PMF-1:** UL believed that maintainers would know how and where to identify hydraulic line chaffing on the aircraft [UL-UCA-1].
- **UL-PMF-2:** UL believed that senior level pilots would not fly if their currency and testing had lapsed [UL-UCA-2].
- **UL-PMF-3:** UL believed that the digital maintenance system provided the necessary, reliable, and required information for maintainers [UL-UCA-1].
- **UL-PMF-4:** UL believed that maintainers and aircrews would still identify and remedy aircraft maintenance problems even if they reported false readiness rate information to higher authorities [UL-UCA-4].
- **UL-PMF-5:** UL believed that the maintainers could conduct maintenance acceptably despite the difficulties associated with the new digital maintenance system [UL-UCA-5].
- **UL-PMF-6:** UL and NAVAIR believed that once congressional funding was approved for further V-22 manufacturing, then the maintenance and safety problems would have the time and resources to be addressed [UL-UCA-4,5].

UL Contextual Factors:

- **UL-CF-1:** Individual and squadron practices were not in compliance with established regulations and operational risk-management standards [UL-UCA-2,3].
- **UL-CF-2:** UL instilled a culture that supported altering maintenance reports to indicate that their MV-22B aircraft had higher readiness rates than accurate [UL-UCA-4].
- **UL-CF-3:** Further analysis or investigation into hydraulic line chaffing would hinder readiness rates and additional MV-22B funding by congress [UL-UCA-1].
- **UL-CF-4:** Following the Crossbow 08 accident, unit leadership continued to pressure maintainers to lie about aircraft readiness rates to make them look more favorable [UL-UCA-4].
- **UL-CF-5:** Post-accident, a marine secretly recorded the unit commander advising maintenance personnel to falsify maintenance reporting of MV-22B aircraft in order to encourage congress to approve the next funding contract. This recording was sent to NAVAIR, the Secretary of the Navy, and *60 minutes* [UL-UCA-4].

Questions raised:

- What were the safety reporting procedures for unit personnel? Was it discouraged by leadership?
- Was there an instructional process for the transition to the digital maintenance system?
- Was there a negative stigma or culture about discussing behavioral health concerns and stressors?

Recommendations:

- Provide and encourage a reporting system for safety incidents and concerns.
- Ensure that an experienced maintainer and safety officer hold positions and have authority in higher-level decision making.

- Consult unit personnel at all levels for feedback on changes to systems, i.e. the digital maintenance system.

Naval Air Systems Command (NAVAIR)[NA]
Responsibilities:
- Provide integrated air warfare capability to Naval and Marine units.
- Coordinate with aircraft manufacturers for equipment certification, safety approval, and standards verification.
- Provide mission intent for aircraft use to the aircraft manufacturer for design guidance.
- Report safety concerns down to the user for inspection or up to the aircraft manufacturer for redesign.
- Test aircraft capabilities post-production before release for mission use.
- Create technical manuals for training, operation, and maintenance for the user.
- Provide equipment testing and safety analysis to the FAA Military Certification Branch for use approval.

NA Control Actions:
- **NA-UCA-1:** NAVAIR issued a warning bulletin to Marine Corps units for wire chaffing on the Osprey MV-22B without clear instruction or verification guidance.
- **NA-UCA-2:** NAVAIR created a digital maintenance system for the Osprey that would run slowly and consistently provide error codes, making unit maintenance inefficient.
- **NA-UCA-3:** NAVAIR did not communicate with the aircraft manufacturer for safety concerns or redesign despite low readiness rates from the MV-22B unit.
- **NA-UCA-4:** NAVAIR did not identify the software anomaly during initial aircraft testing that caused the reset of the blade pitch angles and thrust power on Crossbow 08.
- **NA-UCA-5:** NAVAIR did not identify the problematic hydraulic line and wire-bundle chaffing on preflight testing of the MV-22B before fielding to the units.
- **NA-UCA-6:** NAVAIR approved a flight manual and emergency procedure manual that instructed pilots to press the PFCS reset button as many times as possible if illuminated.

NA Process Model Flaws:
- **NA-PMF-1:** NAVAIR believed that the aircraft manufacturer's aircraft testing was sufficient and did not provide additional analysis on the hydraulic systems or the PFCS [NA-UCA-4,5].
- **NA-PMF-2:** NAVAIR believed that once congressional funding was approved for further MV-22B manufacturing, then the maintenance and safety problems would have the time and resources to be addressed [NA-UCA-3].
- **NA-PMF-3:** NAVAIR assumed that the unit manufacturers would know how to sufficiently inspect all hydraulic line wire-bundles and did not provide further instruction or guidance [NA-UCA-1].
- **NA-PMF-4:** NAVAIR assumed that the new digital maintenance system was sufficient and if there were any technical errors it would be reported up by the units [NA-UCA-2].

NA Contextual Factors:

- **NA-CF-1:** NAVAIR did not conduct testing that would indicate that pushing the PFCS reset button multiple times could be hazardous [NA-UCA-6].

Questions raised:

- What policy determines the testing and safety analyses NAVAIR completes in addition to what the manufacturer already conducted?
- How often does NAVAIR communicate with the Marine Corps unit leadership on aircraft status? Is there a policy in place for communication methods or meeting requirements?
- Are there required safety protocols that NAVAIR enforces on unit leadership?
- Does NAVAIR have protocol in place for unit acknowledgment and plan forward for safety bulletins?

Recommendations:

- NAVAIR have regular coordination with the end user on new equipment status, system updates, recalls, or safety bulletins.
- NAVAIR reassess safety protocol to include human factors considerations in hazard analyses.
- NAVAIR test scenarios for human and software interaction.

FAA Certification Branch [FCB]

Responsibilities:

- Oversees all safety, certification, and business-related activities with stakeholders.
- Certifies mission equipment, installations, and airworthiness systems.
- Provides guidance and instruction for equipment remedial action based off inspection and analysis results from the stakeholders.
- Investigates and reports aircraft accidents, incidents, and service difficulties.

FCB Control Actions:

- **FCB-UCA-1:** The FAA did not have a specialized branch or personnel trained for certification of military aircraft before the Crossbow 08 accident.
- **FCB-UCA-2:** The FAA did not have a verification policy for acknowledgement of safety bulletins.
- **FCB-UCA-3:** The FAA delegated significant amount of authority to the aircraft manufacturer and NAVAIR for certifying the MV-22B.

FCB Process Model Flaws:

- **FCB-PMF-1:** The FAA assumed that it did not need a specialized branch for sufficient military aircraft certification [FCB-UCA-1,2,3].
- **FCB-PMF-2:** The FAA had over-confidence in the abilities of the aircraft manufacturers and NAVAIR to conduct appropriate testing and supply the necessary flight manuals for users [FCB-UCA-3].

FCB Contextual Factors:

- **FCB-CF-1:** The FAA created a "military" certification branch in 2007 to help narrow the responsibilities for more specialized equipment certification [FCB-UCA-1].
- **FCB-CF-2:** The FAA issued an official Order for "Type Certification Procedures for Military Commercial Derivative Aircraft" in 2007 [FCB-UCA-1].

Questions raised:

- What FAA oversight or authority existed for the coordination between the aircraft manufacturers and NAVAIR?
- Were safety bulletins and safety concerns reported to the FAA from NAVAIR or the aircraft manufacturers?
- What involvement does the FAA play when congress deliberates aircraft continuity or funding?

Recommendations:

- Reevaluate certification procedures for aircraft manufacturers to include an un-biased test pilot and engineer analysis.
- FAA have dedicated personnel trained in military specific equipment and have understanding in mission requirements.

Figure 21 displays four UCAs on the aircraft-level control structure. This gives an abstraction of where the unsafe control influenced the system and led to hazardous states.

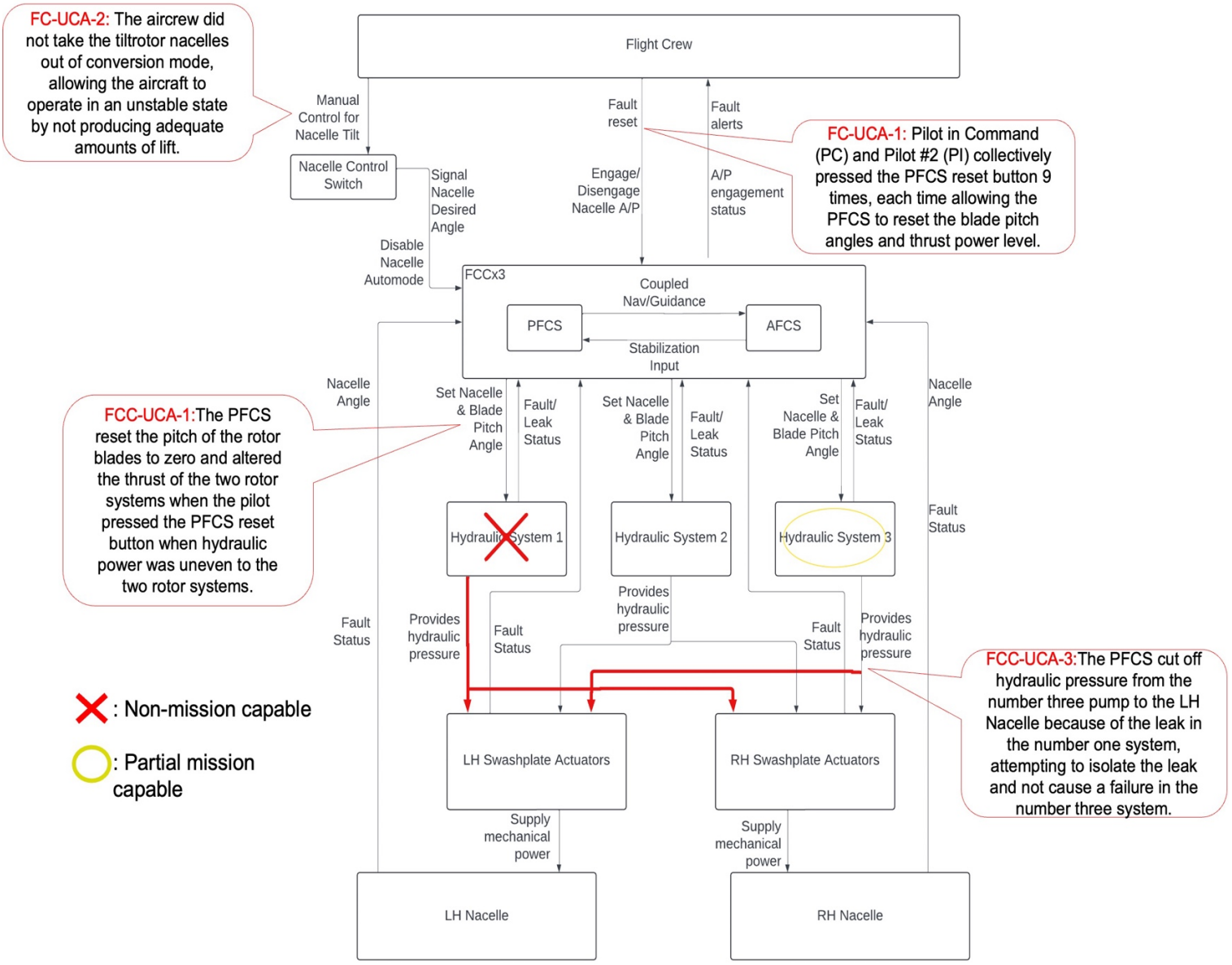

Figure 21: Unsafe Control Actions on the New River Aircraft-Level Control Structure

3.1.4 Control Structure Flaws

This section identifies the systematic factors that contributed to the losses. The focus is the overall perspective of the component interactions and how their controls and constraints did not prevent hazardous states. The systematic factors identify a culture that allowed for components to not fulfill their role in the safety picture.

3.1.4.1 Communication and Coordination

When there is a lack of coordination and communication in an organization, there can be lapses in necessary controls and constraints in the system. In a military organization, multiple layers of leadership and decision-making requires clear and deliberate communication.

When looking at the higher-level control structure for this CAST, the hydraulic line chaffing was a known problem, and a safety bulletin from NAVAIR even existed as a warning for operators. However, because of the lack of verification and specific guidelines for inspection, aircraft faults went unnoticed and unchecked resulting in the Crossbow 08 accident. The feedback loops in the control structure were inadequate and underutilized when implementing the safety bulletin. Had NAVAIR given instruction and acknowledgment requirements and had unit leadership required more thorough verification from maintainers on full and complete inspections, the hydraulic line chaffing may have been remedied.

Another area of interest is the lack of open communication opportunities between the maintainers and unit leadership. A forum for unit personnel to report safety, operational environment, or restrictive practice concerns to leadership would improve the communication lines in the control structure. An understanding between components helps prevent disorganization and malpractice.

In the aircraft-level control structure, there was a misunderstanding of the control authority between the automation, the PFCS, and the aircrew when the reset button illuminated. The coordination between these controllers was misused because of initial design flaws by the manufacturers and regulators. Designers must coordinate with test pilots, systems engineers, and human factors personnel to understand the process models of the various controllers. This initial testing would provide potential redesign considerations before an accident occurs.

3.1.4.2 The Safety Information System (SIS)

An organization's Safety Information System (SIS) provides previous accident information, hazardous trends in like-equipment, effective safety controls and standards, risk assessments, and design improvement based on hazard analysis. The Osprey V-22, as one of the first widely distributed tiltrotor aircraft, did not have the benefit of past engineering technology accident and hazard history other than a handful of V-22 accidents.

All levels of the control structure were operating in unfamiliar territory when it came to the potential hazards associated with this new aircraft design, despite the traditionally used analyses that the aircraft manufacturers and NAVAIR attempted. These analyses did not provide information sufficient for the SIS to have a positive impact on Osprey operation.

Previous V-22 accident investigations, however, reported both causal factors and systemic inadequacies, but recommendations went unchecked and unactioned. An Osprey V-22 accident investigation that occurred in July 1992 reported that NAVAIR's flight manual guiding aircrew

to push the PFCS reset button without a clear understanding of the specific fault was inappropriate. This recommendation was not implemented for change by NAVAIR or other regulatory bodies and the guidance to aircrews remained the same. The SIS was not established or implemented by the safety management system to carry forward the necessary inputs from previous accidents in an impactful manner.

Regulatory bodies such as the FAA and NAVAIR must action and verify accident recommendations for aircraft redesigns so that a SIS can have impactful influence. There was a gap in oversight for actual implemented change to the social system surrounding the Marine Corps Ospreys.

3.1.4.3 Internal and External Economic and Related Factors

The Osprey V-22 has a history of economic and social challenges. The aircraft, while praised for its unique capabilities of both hovering and achieving high airspeeds, has cost the government over $50 billion in research and development, procurement, operational costs, redesign, and accidents.

Around the time of the Crossbow 08 accident, the government was deliberating the approval for "Milestone III," which would put the Osprey at "Full Rate Production." There was intense pressure from Naval higher headquarters to the Marine Medium Tiltrotor Training Squadron 204 (VMMT-204) to improve the aircraft readiness rates so congress would approve spending.

Even after the December 2000 New River accident, unit leadership encouraged maintainers to mask the aircrafts' true maintenance statuses, which were not flyable due to faults and other broken systems. By reporting false readiness rates, leadership could "fix the problems later" after Milestone III was approved. This environment resulted in rushed maintenance practices and an inadequate focus on safety.

Naval leadership failed to recognize the severe design flaws associated with their Osprey maintenance problems and decided that delaying solutions was worth it to save their unit reputations.

3.1.5 Implications of CAST Results and Potential for Mode Confusion

This CAST highlights the potential for mode confusion in tiltrotor aircraft that operate with increasingly complex, mode-rich technology. The aircrew's dependence on resetting the PFCS, combined with a tiltrotor transition angle, displayed a flawed mental model in the system. Although the official accident investigation did not fault the aircrew for pushing the PFCS reset button multiple times because of technical manual guidance, it was still reported as a main causal factor. Osprey engineers wrote a control law that permitted this hazardous system state, which resulted in the loss.

Safety analyses completed in support of this aircraft did not identify hazardous scenarios that could result from a misunderstanding between the human and automation's process models. Traditional hazard analyses focus on component failures alone and do not account for the complex interactions between controllers.

Additionally, the systematic safety environment for the higher-level control structure did not provide the tools necessary for accident avoidance.

3.2 Summary of MV-22B Osprey Tiltrotor Nacelle Angle CAST Results

All information used for this analysis is from public sources (Commanding General, II Marine Expeditionary Force 2012). On 11 April 2012 a MV-22B Osprey tiltrotor aircraft, callsign Elvis 11, crashed in vicinity of Cap Draa, Morocco killing two out of the four crewmembers onboard. The aircraft was conducting an administrative movement of 36 marines during a training mission when it experienced a nacelle transition forward, excessive tail wind, a center of gravity shift, excess nose forward, and impact with the ground. The combination of aerodynamic and environmental considerations was the primary causal factor determined from the Judge Advocate General (JAG) investigation report.

3.2.1 Basic Information

The system involved includes the aircraft, the aircrew, the Marine Medium Tiltrotor Squadron 261, the ground force Marines (Company B, Battalion Landing Team), the aircraft engineers, the aircraft regulatory certifiers, Air Traffic Control (ATC), the USS Iwo Jima, the airport facility, and the surrounding training area. The losses include the aircraft crashing into the ground during a routine training flight and the death of two aircrew members. The hazards that led to the losses and the resulting safety constraints for system design are the following:

System Hazard 1: Aircraft can no longer be controlled
Safety Constraints:

1. Aircraft must be physically capable of making a safe takeoff, cruise flight, and landing.
2. Aircrew must be trained and evaluated on safely operating the aircraft in accordance with limitations.
3. Physical constructs of the airfield must account for aircraft emergency landings and must minimize potential public damage.

System Hazard 2: Minimum aircraft separation standards are violated (terrain, miscellaneous objects)
Safety Constraints:

1. Aircraft must maintain adequate separation from outside objects.
2. Aircraft must be able to detect and recover from separation standard violations.

Table III lists the proximal events leading up to the loss of the MV-22B, Elvis 11, and follow-on questions raised.

Table III: Morocco Accident Timeline of Events

ID	Event	Questions
1	11 April 2012 at 08:30 (zulu) the aircrew showed for their mission brief in the Ready Room on the USS Iwo Jima. The brief included the ship's weather, emergency procedures, and the flight mission plan. The aircraft was partially mission capable (PMC) with no downing discrepancies. The	• Did the aircrew discuss how winds and turbulence were known to affect the landing zone (LZ) for their mission?

	original mission plan was to fly from the USS Iwo Jima to transfer 36 marines from Plage Blanche Airfield to LZ North in two turns.	• What detail was discussed for LZ landing direction, potential hazards, or Go-Around procedures? • Had this aircrew flown together previously? • Had this aircrew flown to this LZ previously?
2	14:55 the aircrew took off approximately five minutes earlier than the original takeoff time (15:00) from the USS Iwo Jima. The aircrew had a late adjustment to their mission plan due to weight and fuel requirements by adding one more turn between Plage Blanche Airfield and LZ North.	• Were all the necessary planning and preflight considerations conducted before takeoff? • Why was this extra leg added later? • Did all members of the aircrew have a thorough understanding of the new plan? • What were unit guidelines for last minute mission adjustments, especially on deployment? • Was the ground force notified of this extra flight leg? • Was the aircraft topped off on fuel or only fueled for the mission requirements? How did that fuel level affect weight and balance?
3	Elvis 11 lands at Plage Blanche Airfield with nose into the wind at 330 degrees to pick up 12 marines for LZ North	• How often were the pilots updating weather and evaluating the wind speeds/directions with each landing and takeoff?
4	Elvis 11 lands at LZ North with nose into the wind at 330 degrees and drops off 12 marines. The pilots notice significant numbers of personnel, tents, and vehicles around the LZ and in particular at the one o'clock and ten o'clock positions of the current landing heading.	• What prelanding checks does the aircrew perform, as dictated by unit regulation? Do those checks include wind verifications? • Was the aircrew unaware of the personnel on the ground prior to their arrival? Was this not included in their LZ

		analysis for hazard identification? • Does the unit have a LZ diagram requirement for mission briefs? • Was there a ground controller for the marines at LZ North, or another form of ATC direction?
5	To avoid overflight of personnel and equipment, the PC lifts the aircraft off the ground, performs a 180-degree pedal turn to the right, transitions nacelles forward, and departs LZ North. Neither pilot noted any concerns with the takeoff procedure.	• Did the PC announce this takeoff plan to the entire aircrew, the ground controller, or ATC? • Was there a windsock at the LZ or other environmental cues for wind? • Did the PC conduct a before takeoff check to include power considerations? • Did the pilot utilize any automation or augmentation for his takeoff?
6	PC passes the controls to the PI during the return trip back to Plage Blanche Airfield	• Did the aircrew check the weather report at Plage Blanche Airfield on the return trip?
7	Elvis 11 lands at Plage Blanche Airfield, picks up 12 more marines, and departs for LZ North on the same 330-degree heading.	• Did ATC report any changes in the wind speeds at the airfield or in vicinity of LZ North?
8	15:50 Elvis 11 lands at LZ North on a 330-degree heading and offloads 12 marines. The winds at the time were measured at 300 degrees at 15 kts	
9	PI notifies PC that he will perform the same takeoff maneuver that the PC did on the previous LZ North departure, and PC approves the maneuver. Aircraft data shows that the winds were 25 kts from the 330-degree direction.	• Did the aircrew do any “before takeoff” checks to include wind verification and power requirements? • What was the culture like in the unit when it came to checklists? • Were there any recurring or additional hazards in the LZ from the last landing?

10	15:53 PI lifts aircraft off the ground to 20 feet, pedal turns nose right to 132 degrees magnetic with the nose slightly downward 5 degrees, transitions the nacelles forward from 87 degrees to 71 degrees, and the aircraft noses down significantly resulting in loss of aircraft control and impact with the ground.	• Did the MV-22B design have any protection for nacelle transition to prevent tilting outside of allowable airspeed limitations? • What wind cueing was available to the pilots in the MV-22B display? • Was there a design consideration for wind speed and nacelle transition protection? • Was there any engaged automation acting during the time of the crash? • Was it customary, expected, or frowned upon for Osprey pilots to pedal turn and immediately begin nacelle transition and takeoff without pausing in a hover?

3.2.2 Control Structures

The following control structures for the Elvis 11 accident depict the systems analyzed in this CAST. While these two control structures (higher-level and aircraft-level) are similar to the CAST conducted in 3.1, there are minor differences for this specific accident, which are highlighted in yellow.

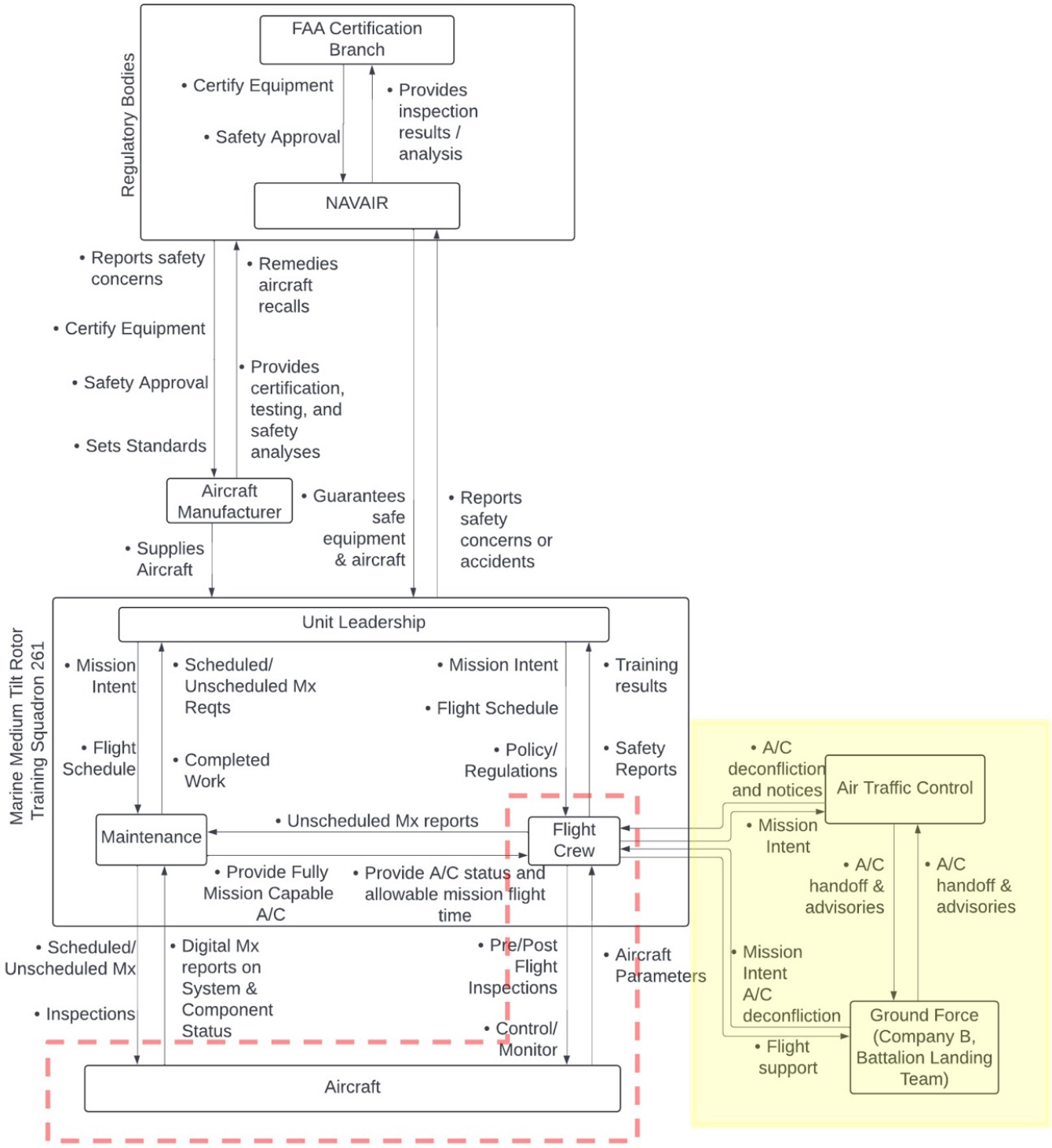

Figure 22: Morocco MV-22B High-Level Control Structure

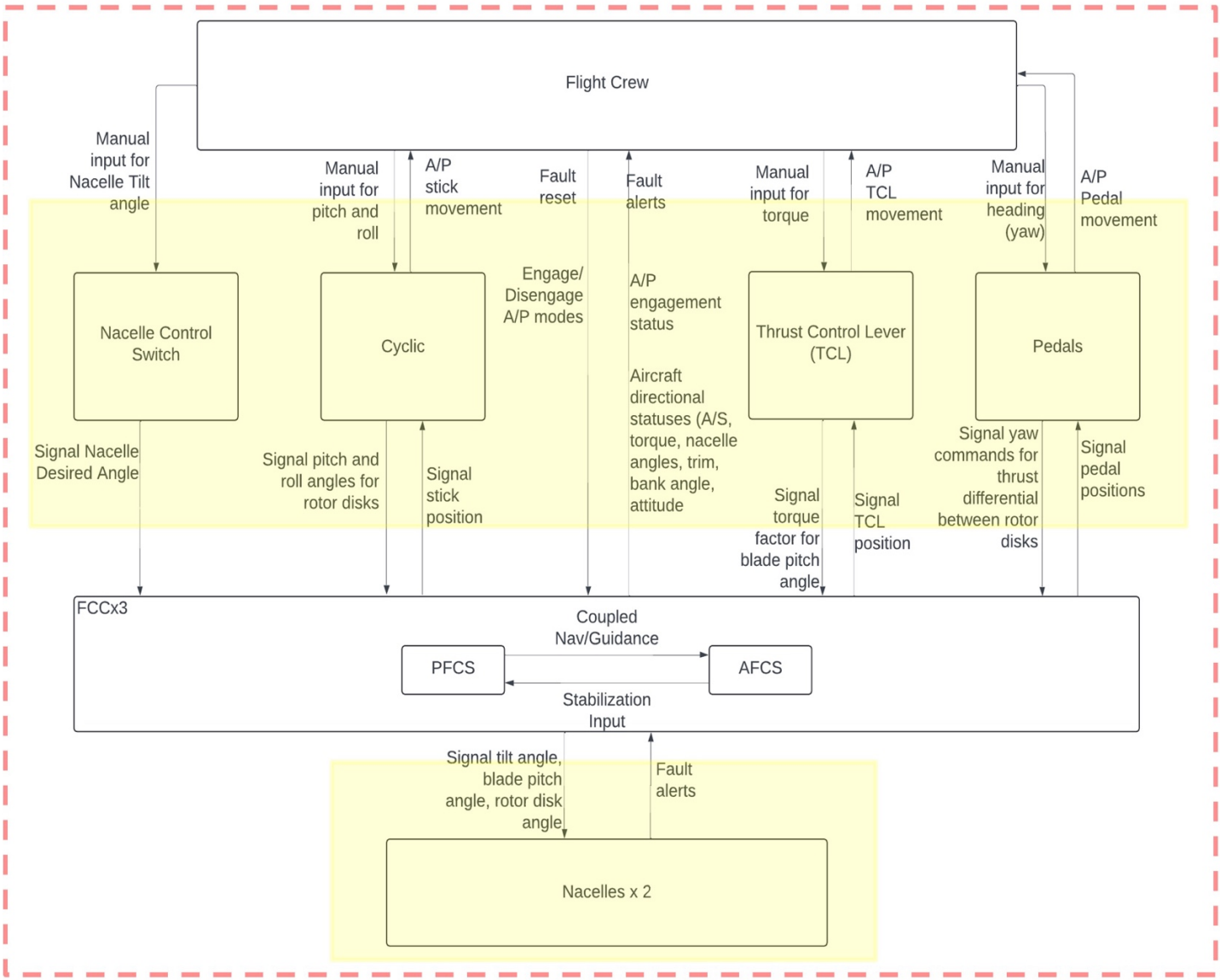

Figure 23: Morocco MV-22B Aircraft-Level Control Structure

3.2.3 Component Contributary Factors in the Losses

3.2.3.1 Role of Physical Components

The primary physical components involved in this MV-22B accident are the nacelle rotor system, the nacelle control switch, the cyclic, thrust control lever (TCL), and the pedals. These physical components connect the primary two controllers in the aircraft-level control structure: the flight crew and the flight control computers (FCC). The system responsibilities and controls are the same as the CAST in 3.1.

Missing or inadequate aircraft physical attributes

This accident did not experience physical component failure, but rather involved unsafe interaction of physical components, missing controls, and design flaws.

1. The combination of a 25-knot tailwind with the nacelle transition forward at low airspeed initiated a change in center of gravity and thrust vector position.
    a. When the nacelles are rotated forward, the aircraft center of gravity shifts forward and down causing a change in the thrust vector. This results in a pitch down moment. If this nacelle transition is performed during low airspeeds, the large pitch down moment may not be recoverable with aft stick. This phenomenon is what Elvis 11 experienced as result of the aircrew's intended flight maneuver. While the manual, at the time, advised caution to this condition, there was no explicit prohibition on flying in that particular flight envelope.
    b. The aircraft's airspeed is measured using a pitot-static system, which calculates airspeed based on the pressure of the air intake and converts it into knots. Before Elvis 11 executed a right yaw, the system indicated an airspeed of 25 knots despite the aircraft being in a hover. This suggests a 25-knot headwind from the 330-degree direction. The system performance display indicated a wind speed and direction to the pilots during the maneuver period.

Recommendations:

- Clearly display wind speed reading for pilot visibility–if winds are approaching a more limiting speed for maneuverability have that displayed differently than a lower, less severe wind speed.
- Design a different source for windspeed information for the computer and pilots so that there is not confusion between windspeed and aircraft airspeed.
- Investigate aerodynamic options in aircraft design to avoid an extensive shift of the center of gravity with nacelle transition.

3.2.3.2 Role of each Controller in the Losses

The responsibilities of controllers are omitted if they are the same as the CAST completed in section 3.1.3.2.

Flight Control Computer [FCC]

FCC Control Actions:

- **FCC-UCA-1:** The FCC signaled the nacelles to transition forward when airspeed was low and a significant tail wind was present.
- **FCC-UCA-2:** The FCC did not signal the nacelles to convert up when the nose pitched down past aircraft operating limits.
- **FCC-UCA-3:** The FCC did not provide auditory or visual warning for nacelle transition during high windspeed and nose down configuration.
- **FCC-UCA-4**: Within the FCC, the AFCS did not provide stabilization input for the PFCS for aircraft control.
- **FCC-UCA-5:** The FCC did not respond to or implement the pilot's aft cyclic command during the nacelle transition and nose down descent.

FCC Process Model Flaws:

- **FCC-PMF-1:** The FCC interpreted and translated the pilots' initial flight control commands in the maneuver as if the aircraft was operating within structural limitations [FCC-UCA-1].
- **FCC-PMF-2:** The FCC was in nacelle angle manual mode, and did not have a control law present to interpret the pilot's aft cyclic command to convert the nacelles up [FCC-UCA-5].

FCC Contextual Factors:

- **FCC-CF-1:** The FCC control laws did not include a nacelle conversion corridor protection for conversion up or transition down based on cyclic position [FCC-UCA-1,2,3,4,5].
- **FCC-CF-2:** The nacelle angle auto-mode was not engaged at the time of the maneuver and accident [FCC-UCA-4].

Questions raised:

- How many nacelle angle modes were available to the pilots during take-off procedures, if any? (Go-Around, constant angle/airspeed, wings-level)
- Did the nacelle angle mode logic process feedback from windspeed sensors?

Recommendations:

- Nacelle protection for transition or conversion outside of the conversion corridor–a physical backstop or visual or auditory warning for pilots to adjust behavior.
- Provide a one-button option on the cyclic or TCL for a "wings-level" type operation, where the computer logic "stashes" the nacelles to an ideal hover position and slows the aircraft's airspeed to zero.
- Ensure that nacelle auto mode logic uses an airspeed source other than pitot static tubes, which could mistake windspeed at a hover for aircraft airspeed.
- Design the FCC logic to analyze and interpret multiple factors for conversion corridor protection to include cyclic position, TCL position, pedal position, windspeed, airspeed, and gross weight.

Flight Crew [FC]

Flight Crew Control Actions:

- **FC-UCA-1:** The junior pilot (PI) did not establish a stable hover *into the wind* before transitioning the nacelles forward in accordance with the MV-22B checklist.
- **FC-UCA-2:** The PI conducted a 180-degree pedal turn and, without a pause in the hover position, transitioned the nacelles forward with a 25-knot tailwind, low airspeed, and a nose down attitude.
- **FC-UCA-3:** The junior pilot did not arrest the significant nose down attitude with converting the nacelles up.
- **FC-UCA-4:** Neither the PC or PI evaluated the effect of windspeed and direction before performing the take-off procedure.
- **FC-UCA-5:** The PI stopped providing control input to the aircraft when aft cyclic did not arrest the nose down attitude.

- **FC-UCA-6:** The flight crew did not brief the executed takeoff maneuver during the pre-mission brief.

Flight Crew Process Model Flaws:

- **FC-PMF-1:** The flight crew believed that the aircraft was physically capable of performing the desired maneuver [FC-UCA-1,2,4].
- **FC-PMF-2:** The flight crew believed that the fly-by-wire technology would prevent the aircraft from performing maneuvers outside of its physical capability [FC-UCA-2].
- **FC-PMF-3:** The flight crew claimed to not know that converting the nacelles up was a technique to prevent nose down attitude [FC-UCA-3].
- **FC-PMF-4:** The PI believed that he lost complete control of the aircraft when he pulled full aft cyclic and it did not prevent the nose downward force [FC-UCA-3].

Flight Crew Contextual Factors:

- **FC-CF-1:** The flight crew, while the PC was on the controls, conducted the same maneuver on a previous take off at the same LZ with presumably lower windspeeds and potentially lower windshear from a nearby cliff face [FC-UCA-1].
- **FC-CF-2:** The accident LZ was geographically positioned near a cliff face that often experienced turbulent wind effects. This information was available to flight crews of this unit but not specifically briefed by ATC [FC-UCA-1,2,3].
- **FC-CF-3:** There were ground force marines, equipment, and vehicles surrounding the LZ in the direction of the wind, prompting the flight crew to conduct the pedal turn and take off to avoid overflight of said hazards [FC-UCA-1,3].
- **FC-CF-4:** The version of the NATOPS flight manual for the MV-22B, at the time of the accident, stated that a normal hover altitude and position should be reached before transitioning the nacelles forward [FC-UCA-1].
- **FC-CF-5:** Fly-by-wire technology will not demand more power than is available causing over torque of the engines, but it will allow for roll and pitch attitudes outside of limits [FC-UCA-1].
- **FC-CF-6:** Vegetation on the LZ was sparse and did not provide visual windspeed cues for pilots during takeoffs and landings [FC-UCA-1,2,4].
- **FC-CF-7:** The PC noted that he had performed this exact maneuver with a tailwind multiple times before this accident [FC-UCA-2].

Questions raised:

- What nacelle conversion and transition maneuvers were MV-22B pilots trained and tested on annually?
- How many FCC modes were available to MV-22B pilots and for what types of missions would they typically utilize them? (I.e. IFR or VFR) Was there a tendency or stigma in the unit for using automation during tactical flight missions?
- Was there quick access for auto-modes of the FCC available to pilots on the cyclic, TCL, or displays?
- Were these pilots trained or have significant flight time on other Marine Corps aircraft before the Osprey, and did that influence their handling qualities of tiltrotor aircraft?

Recommendations:

- Ensure that pilots have the correct process model understanding of all auto-modes available to them for aircraft functionality through flight testing and iterative training.
- Create a design of aircraft controls (cyclic, TCL, displays) that allows pilots to quickly utilize auto-modes in times of emergency.
- Create training scenarios for pilots utilizing different modes of automation and augmentation as well as transition between modes.
- Ensure that pilots understand the unique, hazardous aerodynamic qualities of tiltrotor aircraft effects such as center of gravity and thrust shifts.
- Unit policy should require that flight crews brief an LZ analysis that includes the takeoff and landing directions, hazards on the LZ, windspeeds, go-around procedures, and troop off/onload directions.

Aircraft Manufacturer [AM]

AM Control Actions:

- **AM-UCA-1:** AM did not design the FCC to have conversion corridor protection when pilots would manually adjust nacelle angle outside of structural limitations.
- **AM-UCA-2:** AM did not design the pilot controls (cyclic, TCL, displays) to have quick access to auto-mode functionality (i.e. wings-level, nacelle stash, or decel-to-hover).
- **AM-UCA-3:** AM did not design the nacelles to transition or convert in accordance with cyclic position.
- **AM-UCA-4:** AM did not design the aircraft to visually or audibly warn the flight crew that they were operating within an "avoid" zone for tailwinds.
- **AM-UCA-5:** AM did not design the horizontal stabilizer to interact with and adjust to windspeed readings.

AM Process Model Flaws:

- **AM-PMF-1:** AM believed that their test flights or traditional hazard analyses would solely identify design flaws [AM-UCA-1,2,3,4,5].
- **AM-PMF-2:** AM believed that hazards to flight only involved system or component failures [AM-UCA-1,2,3,4,5].
- **AM-PMF-3:** AM believed that additional design considerations not covered by their team would be identified by NAVAIR [AM-UCA-1,2,3,4,5].
- **AM-PMF-4:** AM believed that pilots would not violate tailwind restrictions associated with nacelle conversion or transition [AM-UCA-1,2,3,4,5].

AM Contextual Factors:

- **AM-CF-1:** The aircraft pitched nose down partially because the tailwind pushed the horizontal stabilizer at the aircraft's tail up and forward [AM-UCA-5].

Questions raised:

- Did nacelle transition and conversion test flight and wind tunnel testing include wind effects from all angles? If so, did those results contribute towards redesign considerations?

- How often would the AM update software and control laws with additional or refined modes?
- Did the AM consider the effects of fixed-wing or rotary-wing pilot flight handling when designing the nacelle conversion/transition for takeoff maneuvers?

Recommendations:
- AM minimizes center of gravity changes on tiltrotor aircraft with other aerodynamic designs–potentially adjust the aircraft's fixed-wing angle.
- AM provides visual or auditory cueing for nacelle transition with tailwind or crosswinds.
- AM conducts flight testing for automation modes intended for takeoff procedures under various environmental conditions.

Naval Air Systems Command (NAVAIR)[NA]

NA Control Actions:
- **NA-UCA-1:** NAVAIR did not include strict restriction for adjusting the nacelle angle with tailwinds or crosswinds in the MV-22B manual, although there is a brief warning.
- **NA-UCA-2:** NAVAIR instructs pilots to apply "aft stick movement to maintain pitch attitude due to thrust and cg effects" but does not connect the warning that this action is ineffective with tailwinds (https://breakingdefense.com/2012/07/marines-peg-bad-flying-as-cause-of-april-v-22-crash-in-morocco/).

NA Process Model Flaws:
- **NA-PMF-1:** NAVAIR believed that a brief advisory about the potential of hazards with tailwinds and nacelle transition would prevent pilots from operating the aircraft under these conditions [NA-UCA-1].

NA Contextual Factors:
- **NA-CF-1:** NAVAIR was under economic and governmental pressure for Osprey reputation and success leading up to this accident because of an upcoming deployment of two Osprey squadrons to Marine Corps Air Station Futenma to replace the CH-46 and CH-53 aircraft with the MV-22B.

Questions raised:
- Did NAVAIR flight testing focus on automation features for takeoff/landing scenarios?
- Did NAVAIR have a Safety Management System that coordinated with the aircraft manufacturer on design updates, concerns, or user input from the line units?

Recommendations:
- NAVAIR creates separate training programs for pilots who have significant time flying fixed-wing or rotary-wing aircraft that specifically highlights the operational differences and potential hazards of tiltrotor aircraft.
- NAVAIR requests automation control laws from the AM that can assist in and protect the aircraft during takeoff and landing maneuvers.

Air Traffic Control [ATC]

Responsibilities:

- Ensure aircraft deconfliction for both visual flight rules (VFR) and instrument flight rules (IFR) modes of flight.
- Ensure that the Automatic Terminal Information Service (ATIS) is operational and updated for aircrew.
- Provide notices for weather alerts, aircraft service changes, or physical hazards.
- Provide aircraft clearances for takeoffs, landings, and route changes.
- Manage airport ramp, taxiway, and runway traffic deconfliction.
- Provide emergency assistance for aircrews under duress.

ATC Control Actions:

- **ATC-UCA-1:** ATC did not provide a weather advisory for winds or turbulence for LZ North.

ATC Process Model Flaws:

- **ATC-PMF-1:** ATC, while not required to report weather advisories for all points in a training area, believed that the flight crew would have awareness of the hazardous weather trends near LZ North [ATC-UCA-1].

Questions raised:

- Did ATC coordinate with the ground force Air Support Element (ASE) on the status of LZ North weather and hazards?

Recommendations:

- ATC coordinates with ASEs on training area specifications for aircraft advisories.

Ground Force Marine Unit [GF]

Responsibilities:

- Provide air traffic deconfliction measures between aircraft, artillery, mortars, or other indirect fire assets.
- Provide management, coordination, and deconfliction for LZ operations.
- Provide mission planning goals, timelines, and integration methods with aviation units prior to mission execution.
- Coordinate with ATC for aircraft control.

GF Control Actions:

- **GF-UCA-1:** The GF did not provide hazard information for LZ North to the flight crew before or during the mission.
- **GF-UCA-2:** The GF ASE did not provide weather information to the flight crew upon landings and takeoffs.

GF Process Model Flaws:

- **GF-PMF-1:** The GF believed that the flight crew would be able to land in a confined LZ despite personnel and vehicles located around its peripheral [GF-UCA-1].

GF Contextual Factors:

- **GF-CF-1:** The GF Air Support Element (ASE) did not have radar capability on the day of this accident and was only providing procedural control of the aircraft. They did not know exactly when the aircraft would land for weather notification and hazard deconfliction [GF-UCA-1,2].

Questions raised:

- What pre-mission planning was conducted between the ground force and the MV-22B flight crew?
- Did the II Marine Expeditionary Force (MEF) have mission planning requirements in their Standard Operating Procedures (SOP) for ground and air coordination?

Recommendations:

- GF units provide aircraft with weather and other hazardous information like personnel and equipment in the area specifically for landings and takeoffs.
- GF reports weather and hazards to ATC for relay to aircraft.

Figure 24 displays four UCAs on the aircraft-level control structure. This gives an abstraction of where the unsafe control influenced the system and led to hazardous states.

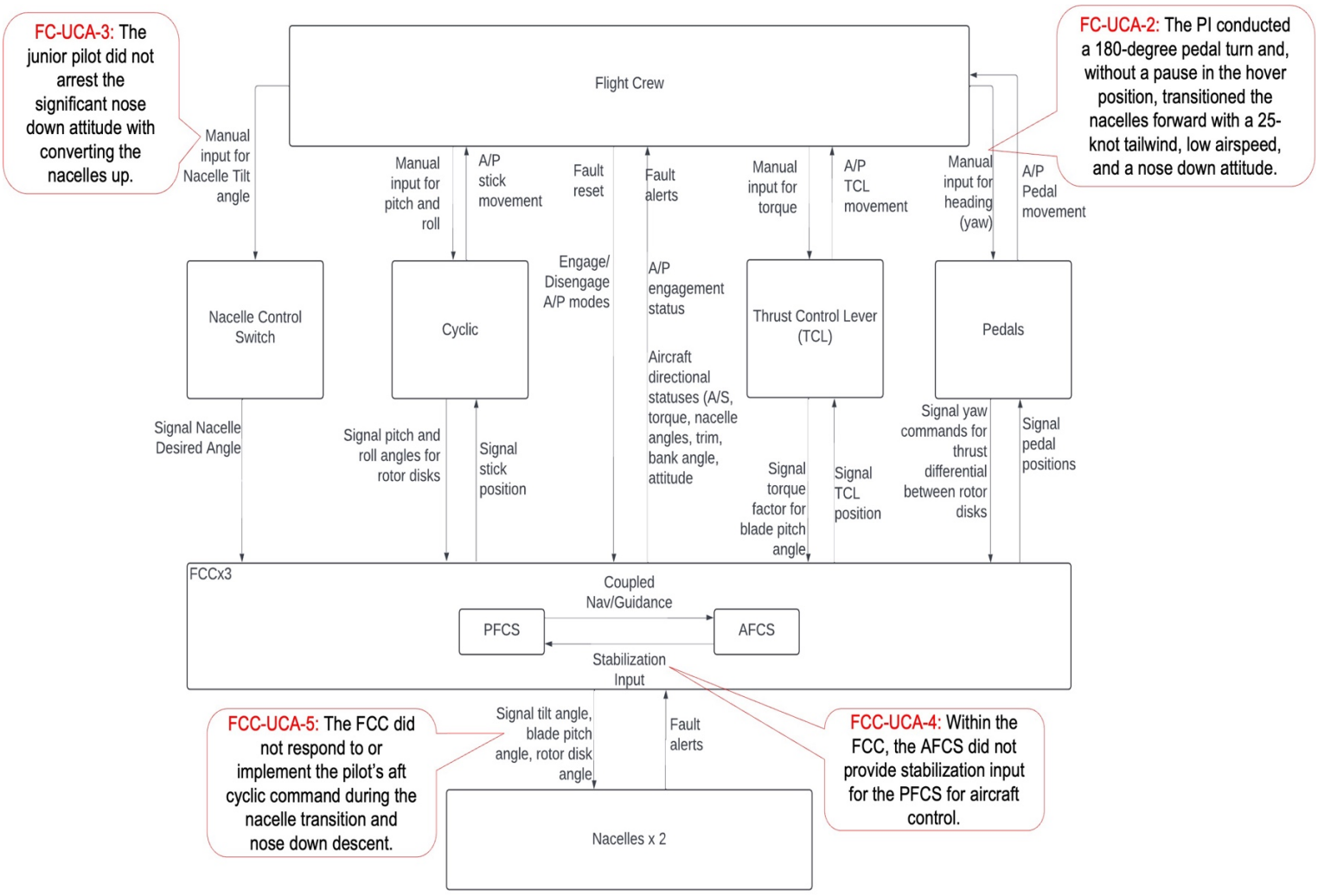

Figure 24: Unsafe Control Actions on the Morocco Aircraft-level Control Structure

3.2.4 Control Structure Flaws

3.2.4.1 Communication and Coordination

Referencing the higher-level control structure in this analysis, the lack of coordination between the flight crew and the ground force led to unplanned and unnecessarily hasty flight maneuvering.

This flight was an administrative movement during a training mission, and they were not operating in a dangerous combat environment. Despite not conducting the appropriate coordination before the mission, the flight crew also had flexibility in their timeline to adjust their flight procedures during the mission through communication with the ground force at the LZ.

When the ground force, or ATC, did not notify the flight crew of the weather advisories or physical hazards on the LZ, the flight crew adjusted their takeoff direction to avoid overflight of personnel and equipment, resulting in a dangerous maneuver with a tailwind. This lack of communication could also be a result of lacking regulatory SOPs at a higher echelon–when units

do not require pre-mission briefings between entities, hazards and accidents are more likely to occur. These briefings serve as controls for verification and understanding between controllers.

In the aircraft-level control structure, there was a lack of understanding and coordination between the flight crew and the computer when the pilot's cyclic commands did not translate into aircraft maneuverability. The control laws did not include guidance for the computer to convert cyclic commands to nacelle tilt operation during low airspeed operations.

As a result of this accident, that particular control law was introduced and implemented in a redesign of the MV-22B.

3.2.4.2 The Safety Information System (SIS)

Although the Osprey had been in full rate production since 2005, considerable redesign considerations from safety issues were only developed after accidents already happened. It is unknown whether NAVAIR and the aircraft manufacturers conducted additional hazard analyses, unprompted by accidents, to identify design flaws.

More importantly, human factors and human integration into these analyses were still not focal points for designers. Without an established and well-regulated SIS, design improvements based on hazard analysis would not be prioritized or even scheduled.

The priority for the organization was to maintain or improve the Osprey's reputation through positive maintenance statuses and continued pilot training, neither of which improve system design.

3.2.4.3 Internal and External Economic and Related Factors

Economic and social pressures continued to afflict the Osprey community at the time of this accident, more than a decade after the New River accident. The MV-22B was scheduled to replace the Marine Corps' CH-53D and CH-46E aircraft stationed in Okinawa, where previous accident occurrences alarmed local officials of endangering civilians and infrastructure.

Also, NAVAIR and the aircraft manufacturer were in the process of making initial foreign sales of the V-22, which would lower the aircraft's unit cost. These sales depended upon a safe reputation of the V-22, which already had a history of accidents related to design flaws and human error.

These concerns resulted in command pressure from congress, through NAVAIR, and to the flight line units to maintain positive results of Osprey maintenance and flying records. This type of pressure can affect the accuracy of maintenance and training statuses as the lowest units may face consequences to their careers when they do not produce the results that higher echelons seek.

3.2.5 Implications of CAST Results and Potential for Mode Confusion

Flawed aircraft design contributed to the pilots' mode confusion when they did not utilize the nacelle control switch to arrest their nose down descent nor did the FCC control laws include cyclic position to influence nacelle angle. Although the pilots had performed this type of takeoff maneuver multiple times in their flying careers, when combined with a particular context of environmental and aerodynamic factors it resulted in a misunderstanding between the pilots' intent and the aircraft's response. This analysis shows that controller actions may be considered

safe in some scenarios but hazardous in others. Although this maneuver was highlighted in the MV-22B manual through a warning statement, engineers did not make any design changes until after the accident occurred. Critical interactions between components of this system, at the higher-level and aircraft-level control structure, were overlooked when analyzing the safety of this aircraft both pre-design and post-design, which contributed to this accident.

Chapter 4 STPA Application for Tiltrotor Aircraft

This chapter presents the results from Systems Theoretic Process Analysis (STPA), which demonstrate the possibility for unsafe control that could lead to hazardous scenarios involving mode confusion in tiltrotor aircraft. These scenarios are linked to the complex handling qualities associated with the transition between helicopter and airplane modes, as well as other novel augmentation features for aircraft design.

This analysis highlights the importance of human-system integration during early design stages of tiltrotor aircraft and can contribute to the overall hazard analysis approach. The analysis may apply to different forms of VTOL design but focuses on a two-rotor, fixed-wing design similar to the V-22.

Figure 25 depicts a computer aided design (CAD) of a V-22 for reference of a two-tiltrotor design. The figure shows the aircraft in VTOL mode and airplane mode.

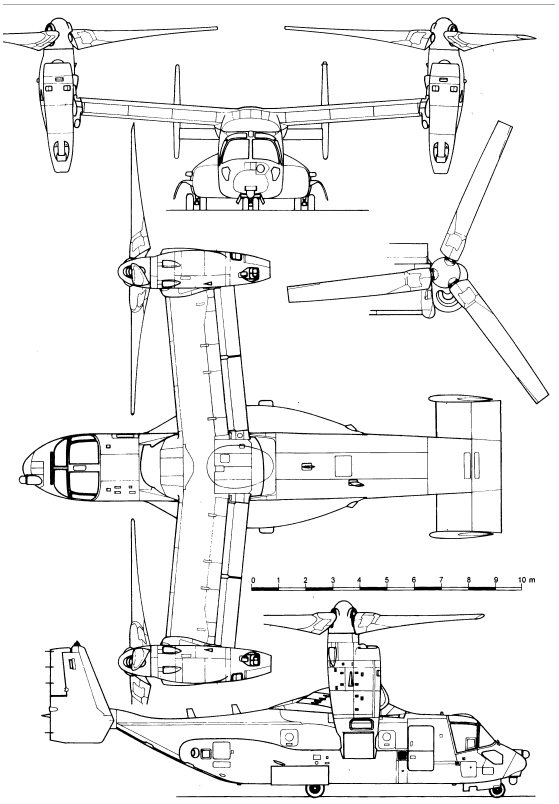

Figure 25: Two-Tiltrotor design for STPA ("Bell Boeing V-22 Osprey," n.d.)

4.1 Define the Purpose of the Analysis

The first step of STPA is to define the purpose of the analysis. Part of this critical step is to define the system boundary and decide where the analysis will focus. For this analysis, the system includes the aircraft and its operators (manned or unmanned). The STPA will focus on design aspects of the aircraft that make it unique as a tiltrotor, including the fly-by-wire flight control computers, the rotating pylons, and pilot controls.

4.1.1 System Losses

Table IV lists the system losses for this STPA. Government regulations, management, or customers may define stakeholder interests. For tiltrotor aircraft in U.S. Department of Defense (DoD) organizations, stakeholders may include military chains of command, a government organization, or a defense contractor, as a few examples.

Table IV: System Losses

Loss ID	Loss Description
L-1	Loss of life or serious injury
L-2	Loss of or damage to aircraft
L-3	Loss of mission
L-4	Loss of reputation

4.1.2 System Hazards

Table V lists the system hazards for this analysis. The hazards are system states that could result in losses from Table IV. By identifying hazards at the system-level, as opposed to just component level failures, this STPA can include more causes of accidents to consider in the design process. Section 2.4.1 provides background information on tiltrotor-specific aerodynamics and system states that are encompassed by these hazards.

Table V: System Hazards

Hazard ID	Hazard Description	Loss Trace
H-1	Aircraft is uncontrollable	L-1, L-2, L-3, L-4
H-2	Aircraft is unable to remain airborne	L-1, L-2, L-3, L-4
H-2.1	Aircraft experiences center of gravity imbalance	L-1, L-2, L-3, L-4
H-2.2	Aircraft loses sufficient lift	L-1, L-2, L-3, L-4
H-3	Structural integrity of the aircraft is violated	L-1, L-2, L-3, L-4
H-4	Minimum aircraft separation standards are violated (other aircraft, terrain, miscellaneous objects)	L-1, L-2, L-3, L-4
H-5	Aircraft is unable to conduct mission tasks	L-3, L-4

4.1.3 System Constraints

The system-level constraints, listed in Table VI, define requirements that a tiltrotor aircraft must satisfy to avoid the system hazards and losses.

Table VI: System Constraints

Safety Constraint ID	Safety Constraint Description	Hazard Trace
SC-1	Aircraft must remain controllable during all manned and unmanned operations	H-1
SC-2	Aircraft must maintain its capability to remain airborne during all modes of operation	H-2
SC-2.1	Aircraft must remain airborne during center of gravity shifts	H-2.1
SC-2.2	Aircraft must produce lift during all VTOL, conversion, or airplane modes while airborne	H-2.1, H-2.2
SC-3	Aircraft must remain within structural limitations during all modes on ground and airborne	H-3
SC-3.1	Pilot or remote controller must operate aircraft within structural limitations	H-3
SC-4	Aircraft must maintain separation from outside objects	H-4
SC-5	Aircraft must have physical capability to perform required mission set	H-5

4.2 Generate a Control Structure

The second step in STPA is to generate a hierarchical control structure that models the control loops and feedback between the controllers of a system. Control structures enforce the safety constraints.

This analysis includes two control structures at different levels of abstraction: one at a higher-level of the aircraft (Figure 26) and one with more system details (Figure 27). Figure 26 shows that the pilot controls the FCC by providing commands to it while the FCC in turn controls the flight control surfaces and dynamics. These control structures are abstractions of a potentially complex aircraft and include subsystems necessary for this specific analysis. It does not include every individual subsystem required in a tiltrotor aircraft but rather what makes a tiltrotor unique and potentially hazardous.

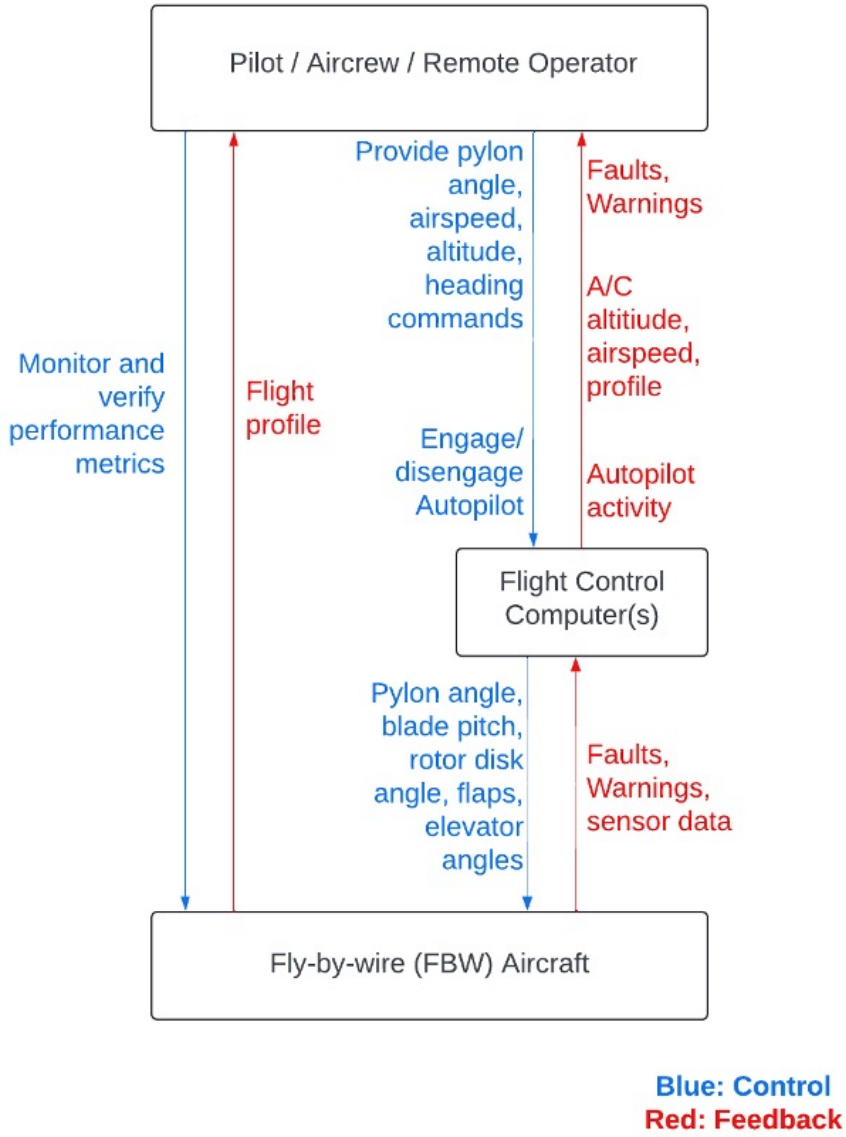

Figure 26: Tiltrotor High-Level Aircraft Control Structure

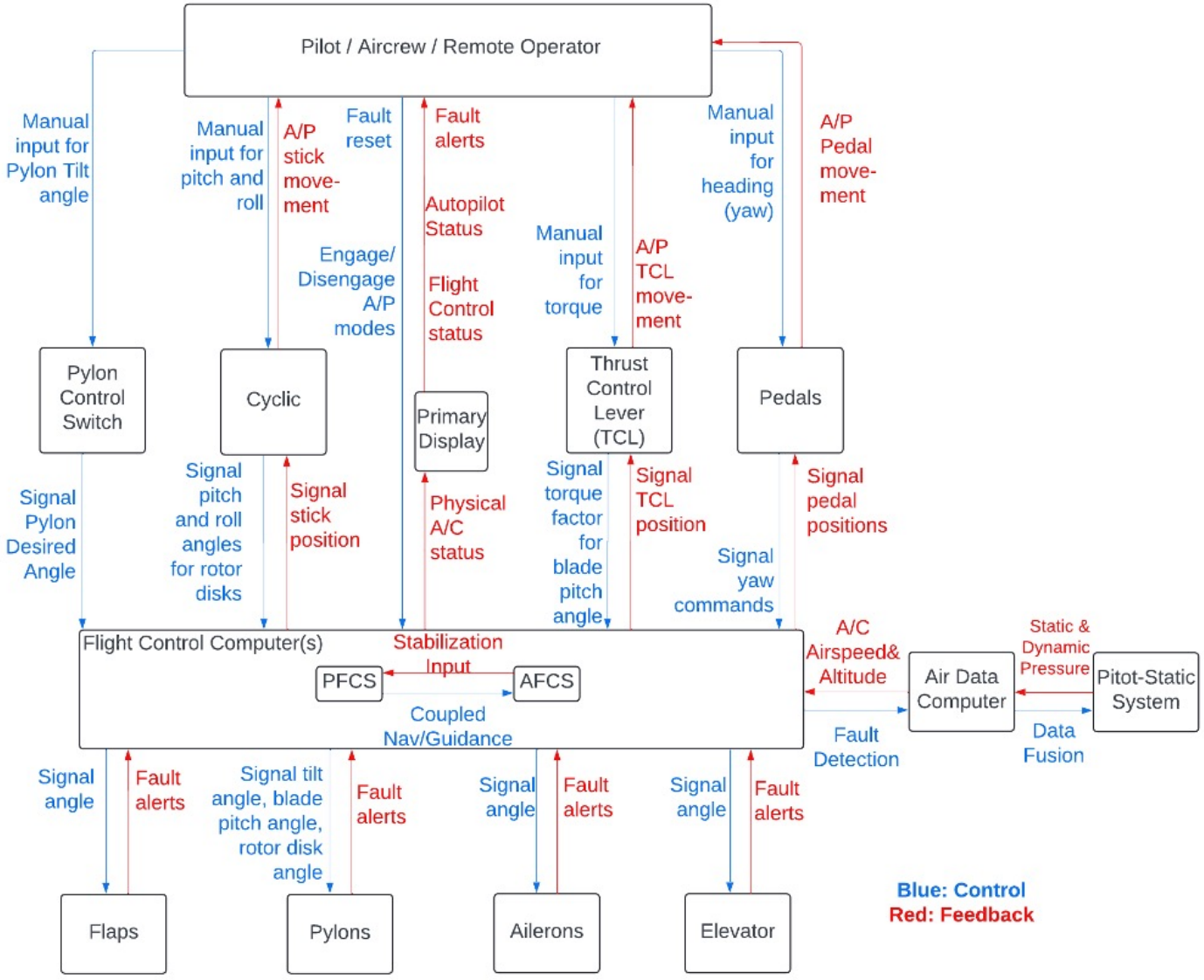

Figure 27: Tiltrotor Specific Aircraft-Level Control Structure

4.3 Identify Unsafe Control Actions

The next step in STPA is to identify unsafe control actions, which are control actions that, in a particular context and worst-case environment, will lead to a hazard. The UCAs identified by STPA can be leveraged to derive functional safety requirements and design decisions. Tables VII and VIII provide more detailed information on the primary control actions of the pilot and the flight control computer with their associated process model beliefs about how other controllers and the aircraft will perform. This relationship helps identify how mode confusion resulting from incorrect process models can lead to the unsafe control actions in Tables IX-XVI.

Table VII: Pilot, Aircrew, or Remote Operator Control Action details

Pilot Control Actions	Process Model Belief
Pilot engages / disengages autopylon	- The FCC will utilize various parameters to adjust pylon angle. Examples are airspeed, windspeed, flight control inputs from cyclic, TCL, or pedals, or GPS location. - The autopylon is or is not available for engagement at any airspeed (lower or upper limit)
Pilot provides an increase / decrease in rotor RPM commands	- Airplane mode: lower RPM results in more efficient handling qualities - Helicopter mode: higher RPM is required to produce lift - Conversion: the transition period for RPM changes
Pilot provides an increase / decrease in thrust commands	- Airplane mode: thrust controls airspeed - Helicopter: thrust controls altitude - Conversion: thrust adjusts both airspeed and altitude
Pilot provides neutral cyclic, TCL, or pedal commands	- Lower augmentation levels: neutral control commands are necessary to center/level the aircraft or stop movement - Higher augmentation levels: neutral control commands are not necessary to stop aircraft movement

Table VIII: FCC Control Action details

FCC Control Actions	Process Model Belief
FCC signals autopylon commands	Uses airspeed, windspeed, and pilot inputs to signal desired pylon angle for aircraft performance. - An increase in airspeed indicates the demand to transition pylons forward - A decrease in airspeed indicates the demand to convert the pylons up - Weight on wheels, zero forward airspeed, or pilot command may turn on/ off autopylon depending on designer control law designation
FCC increases / decreases thrust	- Manual or autopylon changes require different levels of thrust - Different control law modes may or may not have thrust power limits applied (over-torque prevention)

Table IX: Pilot Unsafe Control Actions–Autopylon Engagement

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
Pilot engages autopylon	**PI-UCA-1:** Pilot does not engage autopylon when aircraft landing is deemed unachievable [H-2.2, H-4]	**PI-UCA-2:** Pilot engages autopylon when airspeed is already too low (does not trigger pylon rotation) [H-1, H-2, H-2.2, H-4]	**PI-UCA-4:** Pilot does not engage autopylon before slowing aircraft to an irrecoverable stall airspeed [H-1, H-2, H-2.2, H-4]	**PI-UCA-5:** Pilot engages autopylon mode too long (e.g., does not deactivate autopylon mode) after the mission or flightpath plan has changed [H-4, H-5]
		PI-UCA-3: Pilot engages autopylon when engine energy production is insufficient to generate adequate lift in helicopter mode [H-1, H-2, H-2.2, H-4]		**PI-UCA-6:** Pilot stops engaging autopylon mode (deactivates it) too soon before executing the planned transition [H-1, H-2, H-4, H-5]

Table X: Pilot Unsafe Control Actions–Thrust Control

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
Pilot increases / decrease thrust	**PI-UCA-7:**	**PI-UCA-8:**	**PI-UCA-10**	**PI-UCA-11**
	Pilot does not increase thrust when autopylon transitions forward [H-2, H-2.2, H-4]	Pilot provides excessive torque command (over-torque) when FCC is in alternate control law mode (loses over-torque protections) [H-1, H-2, H-3, H-4]	Pilot provides an increase in thrust before converting pylons up [H-4, H-5]	Pilot stops increasing thrust after pylons have converted full up [H-2.2, H-4, H-5]
		PI-UCA-9		
		Pilot increases / decreases thrust for airspeed while in helicopter mode [H-4, H-5]		

Table XI: Pilot Unsafe Control Actions–Flight Control Commands

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
Pilot provides control command (cyclic, TCL, pylon, or pedals)	**PI-UCA-12:**	**PI-UCA-13:**	**PI-UCA-14:**	**PI-UCA-15:**
	Pilot does not provide neutral control command when maintaining a hover - (RCAH vs ACAH for cyclic) - (TRQ hold vs height hold modes for TCL) - (heading hold vs. turn hold for pedals) [H-2.1, H-4]	Pilot provides neutral stick command when initiating an aircraft movement [H-4]	Pilot provides neutral stick command after increasing augmentation mode [H-4]	Pilot stops providing control commands after reaching designated airspeed for mode change [H-1, H-2.2, H-4, H-5]
				PI-UCA-16:
				Pilot stops providing pylon commands after autopylon disengages or stops movement [H-4]

Table XII: Pilot Unsafe Control Actions–CLAW Mode Change

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
Pilot changes augmentation control law (CLAW) mode	N/A	N/A	**PI-UCA-17:** Pilot does not change CLAW mode before making cyclic, TCL, pylon, or pedal adjustments [H-1, H-2, H-3, H-4]	N/A

Table XIII: Pilot Unsafe Control Action–Landing Approach

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
Pilot conducts landing approach	N/A	**PI-UCA-18:** Pilot approaches to land when the aircraft is in conversion mode [H-1, H-2.1, H-4]		N/A

Table XIV: FCC Unsafe Control Actions–Autopylon

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
FCC signals autopylon commands	**FCC-UCA-1:**	**FCC-UCA-2:**	**FCC-UCA-3:**	**FCC-UCA-4:**
	FCC does not signal autopylon commands when aircraft reaches designated engagement airspeed [H-1, H-2, H-2.2, H-4, H-5]	FCC signals autopylon transition forward when aircraft is in a hover (incorrect airspeed reading due to winds and pitot static readings) [H-1, H-2, H-2.2, H-4]	FCC disengages autopylon during an approach to land before aircraft has confirmed landing [H-1 H-2.1, H-2.2, H-4]	FCC stops signaling autopylon command before pylons are in helicopter or airplane mode (FCC reset or incorrect airspeed readings) [H-1, H-2.1, H-2.2, H-4]

Table XV: FCC Unsafe Control Actions–Thrust Control

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
FCC increases/ decreases thrust	N/A	**FCC-UCA-5:**	**FCC-UCA-7:**	**FCC-UCA-9:**
		FCC provides increase thrust command when pylon cannot begin transition up [H-3, H-4]	FCC does not provide decrease thrust command before pylon begins transition to helicopter mode [H-1, H-2, H-2.1, H-3, H-4]	FCC increases thrust for too long after pylons are transitioned to airplane mode [H-4]
		FCC-UCA-6:	**FCC-UCA-8:**	
		FCC provides excessive torque command (over-torque) beyond structural limits of the configuration [H-1, H-2, H-3, H-4]	FCC does not provide increase thrust command after pylon begins transition to helicopter mode [H-1, H-2, H-2.2, H-4]	

Table XVI: FCC Unsafe Control Actions–Control Commands

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too early / too late / out of order	Stopped too soon / Applied too long
FCC provides control commands (pylons, flaps, flaperons, rudders, elevator, etc)	**FCC-UCA-10:**	**FCC-UCA-11**	N/A	N/A
	FCC does not signal neutral control command when maintaining a hover [H-2.1, H-4]	FCC provides control commands when maintaining a hover [H-2.1, H-4]		

4.4 Generate Causal Scenarios

The fourth step in STPA is to identify scenarios that may lead to unsafe control actions and hazards. Each scenario will have a scenario type shown in Figure 28 and a mode confusion type involving either supervisory modes, display modes, controller operating modes, or operating modes of the controlled process. Some scenarios include multiple UCAs that result from previous, initial UCAs. These scenarios can be used in design considerations when synthesizing human-automation relations for tiltrotor aircraft.

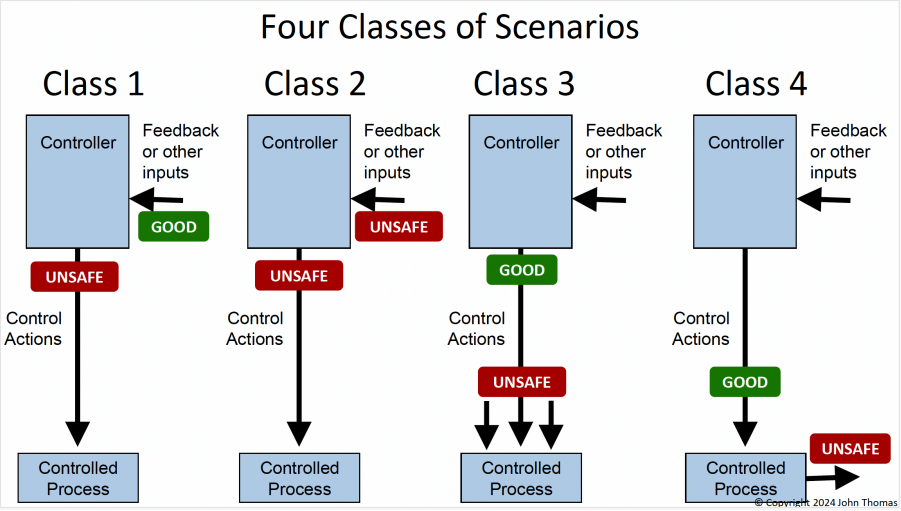

Figure 28: Classes of Scenarios (Thomas 2024)

4.4.1 Pilot Scenarios

4.4.1.1 Supervisory Mode Scenario

Primary UCA:

PI-UCA-1: Pilot does not engage autopylon when aircraft landing is determined unachievable [H-2.2, H-4]

Contributing or Resulting UCAs:

FCC-UCA-3: FCC disengages autopylon during an approach to land before aircraft has confirmed landing [H-1 H-2.1, H-2.2, H-4]

PI-UCA-9: Pilot increases / decreases thrust for airspeed while in helicopter mode [H-4, H-5]

PI-UCA-16: Pilot stops providing pylon commands after autopylon disengages or stops movement [H-4]

Assumptions:

The autopylon in this aircraft design disengages at a hover or zero forward airspeed. The autopylon engagement status is indicated to the pilot.

SC-PI-1: A tiltrotor aircrew is conducting a Visual Flight Rules (VFR) approach to land to the ground. The autopylon is engaged and converts the pylons up towards 90 degrees (or ideal hover angle deemed by vehicle engineers) when the pilot slows down the airspeed. Upon establishment

of zero degrees forward airspeed OR hover, autopylon disengages [FCC-UCA-3] and pilot initiates manual or automatic (via button) go around. The pilot does not engage autopylon [PI-UCA-1] because they believe the autopylon never disengaged from the initial landing [PI-PMB-1]. The pilot does not manually adjust the pylon for the remainder of the go-around procedure [PI-UCA-16] and utilizes the TCL as if the pylon is converting to airplane mode because they believe the autopylon is engaged. If the TCL is used with this process model belief, the pilot would believe they are using the TCL to adjust airspeed, but it would be adjusting altitude [PI-UCA-9]. This could cause the aircraft to lose sufficient lift [H-2.2] or violate minimum aircraft separation standards [H-4]. This scenario is depicted in Figure 29.

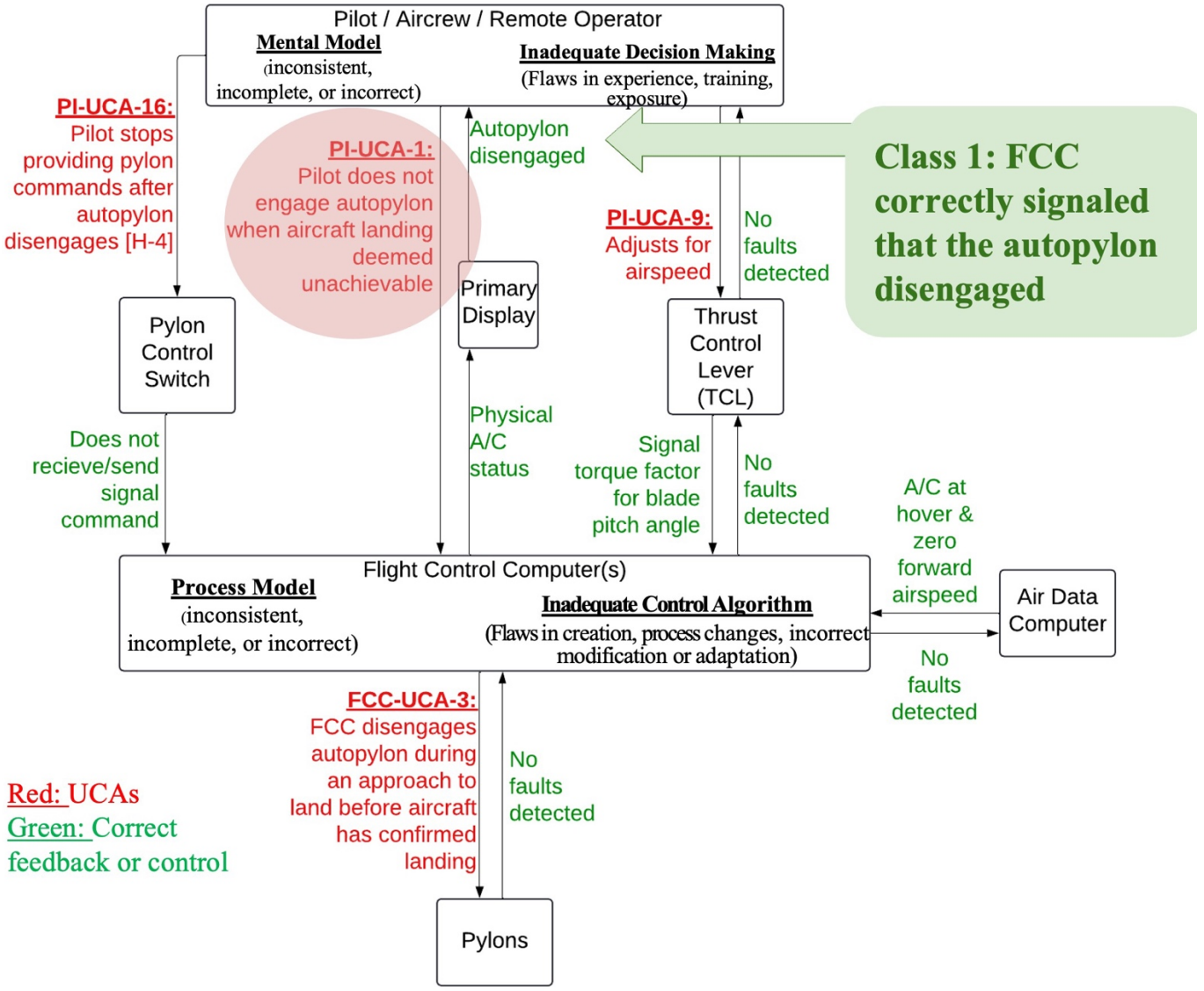

Figure 29: SC-PI-1

Insight: This scenario does not involve system or component failure but still identifies the possibility of hazardous outcomes. This scenario is a classification type one: it involves correct information and feedback from the computer to the pilot but a resulting unsafe control action.

The pilot's process model led to the belief that the autopylon remained engaged when, in reality, the FCC had reached its designated autopylon disengagement criteria. The pilot experienced supervisory mode confusion when they believed the FCC remained in control of the pylon. The pilot did not subsequently re-engage the autopylon or provide manual pylon control. Additionally, they utilized the TCL for airspeed while in altitude mode. A different design of the aircraft and its control laws can prevent the chances of mode confusion between the autopylon control authority and the pilot's process model of beliefs about those functions.

Solutions: The aircraft autopylon design should have clear engage/disengage criteria and be displayed to the aircrew [AP-R01]. For all options, the autopylon ENGAGE versus ARMED should be clear to the aircrew. If there is a computer malfunction that leads to an inoperability of the autopylon, this should be conveyed to the aircrew through visual or auditory warning [AP-R02]. The assumption in this scenario was that the autopylon disengages at zero forward airspeed or a hover, which has the potential to create chances of confusion for the pilot during moments of task saturation or sudden mission changes. Clearer and more definite options are listed below for autopylon design.

1) Option 1: Once the autopylon is turned on by the pilot, it never disengages unless the pilot initiates that demand [AP-R03].
2) Option 2: Autopylon disengages upon weight-on-wheels (WOW) when an aircraft lands. The pilot knows that it will not disengage at any point during the landing sequence until the WOW is signaled [AP-R03].

4.4.1.2 Display Mode Scenario

Primary UCA:
PI-UCA-12: Pilot does not provide neutral control command when maintaining a hover [H-2.1, H-4]

Contributing or Resulting UCAs:
PI-UCA-17: Pilot does not change CLAW mode before making cyclic, TCL, pylon, or pedal adjustments [H-1, H-2, H-3, H-4]
FCC-UCA-10: FCC does not signal neutral control command when maintaining a hover [H-2.1, H-4]

Assumptions:
1) In unique-trim aircraft, the cyclic center position is always in the same physical position for the aircrew. This differs from a displacement-trim aircraft where the center position for the cyclic changes. This scenario example operates with following unique-trim control law (CLAW) modes:
    a. CLAWs 0-1: For all airspeeds CLAWs 0-1 provide Rate Command / Attitude Hold (RCAH) based on cyclic stick position in the roll and pitch directions. When the cyclic is moved from the center position it will initiate a rate change, and when the cyclic is returned to center it will stop the rate change and maintain a new attitude. To return the attitude back to the original value, a counter (or opposing) cyclic movement is required.

b. CLAW 2: For airspeeds 0-TBD knots, this CLAW provides Attitude Command / Attitude Hold (ACAH) and from TBD knots and greater provides RCAH based on cyclic stick position in the roll and pitch directions. In ACAH, when the cyclic is moved from the center position it will initiate an attitude change, and when the cyclic is returned to center it will return the attitude to the trim value (corresponding the stick neutral/detent position). This mode does not require a counter stick movement to return to an original hover attitude.

2) In fly-by-wire aircraft, the flight control system within the FCC has 100% control authority over the aircraft's control surfaces and flight dynamics because there are no mechanical linkages from the pilot controls. Pilot input is sent through electrical signals to the computer, which implements the pilot's commands into actual flight control input.
3) For this scenario, the assumption is that the feedback to the pilot for a CLAW change is inadequate for recognition or confirmation.

SC-PI-2: A pilot is flying a tiltrotor aircraft and maintaining a hover profile in a confined landing zone (LZ). To adjust the aircraft's position, the pilot provides a roll or pitch command in the cyclic but does not provide a neutral command [PI-UCA-12] because they believe that returning the stick to the center position is sufficient to stop the aircraft's movement to reestablish a hover [PI-PMB-2]. They believe that this action is sufficient because their mental model is incorrect and tells them that they are operating in CLAW 2, but they are either not engaged in CLAW 2 or they are not below the designated airspeed before CLAW 2 switches from ACAH to RCAH.

The FCC would not signal a neutral aircraft control command [FCC-UCA-10] because it does not have an algorithm to understand the pilot's desired maneuver. The pilot may then provide additional control inputs to attempt to counter the aircraft movement without adjusting the CLAW mode [PI-UCA-17]. The aircraft movement vector would continue in the direction initially inputted from the pilot's cyclic movement. This movement could cause the aircraft to violate minimum aircraft separation standards [H-4] especially in areas that are confined. This scenario is depicted in Figure 30.

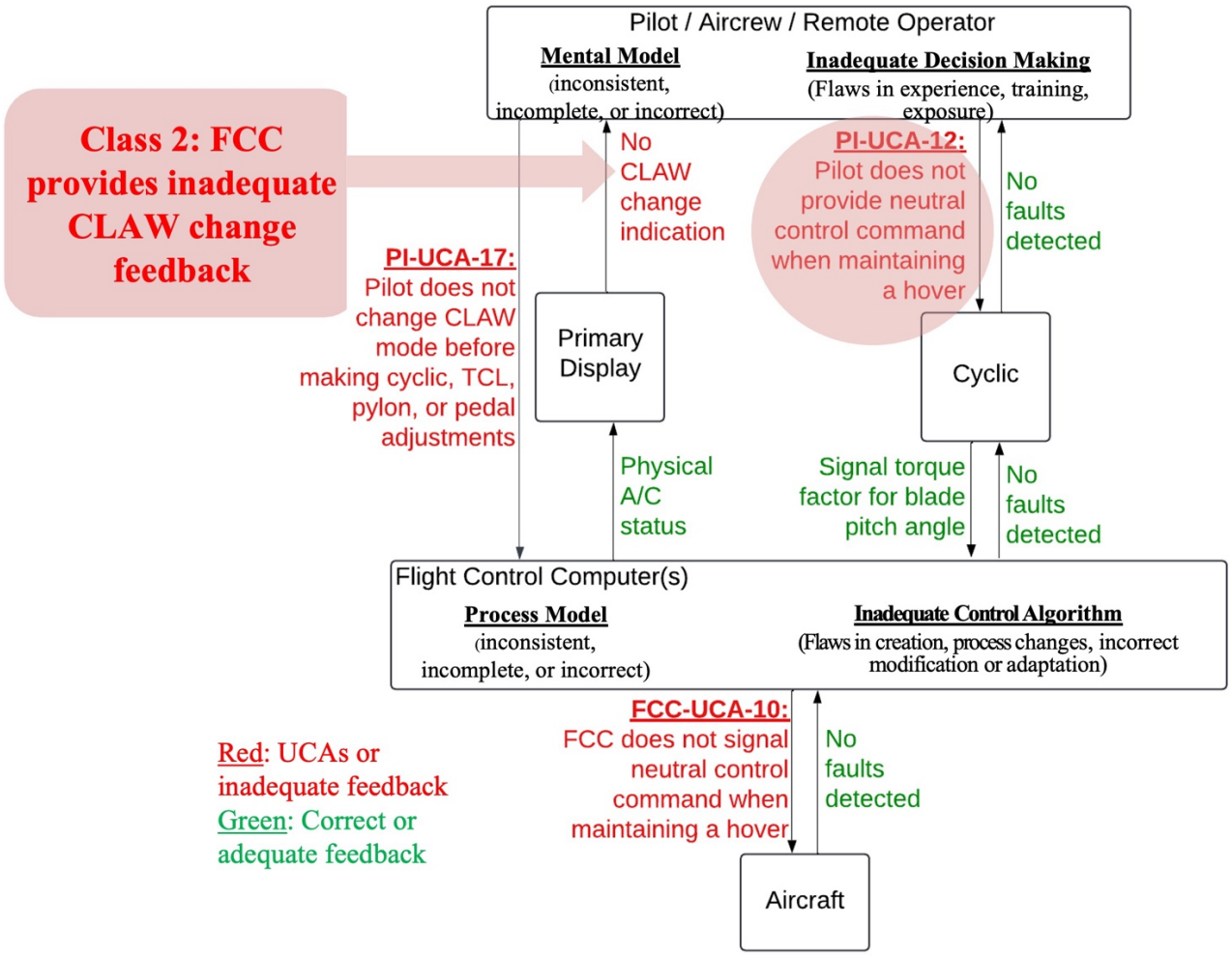

Figure 30: SC-PI-2

Insight: This scenario did not involve any system failure or malfunction and is a classification two: the pilot received inadequate feedback about a CLAW mode change and, therefore, carried out an unsafe control action. The aircraft had multiple operating modes of augmentation assistance (CLAWs 0-2). In this case, the lack of feedback through the different display modes resulted in pilot confusion. The pilot did not provide a counter action to maintain a hover. While upgrades in aircraft augmentation modes are meant to assist pilot and aircraft performance, they provide the opportunity for mismanagement and mode confusion between controllers if the design is inadequate for operator understanding and control.

Solutions: There must be clear distinction between modes, when those modes change, and confirmed understanding from the pilot on operation of those modes. When the mode changes due to an airspeed increase, there should be a clear indication to the pilot. Additional design solutions include:

1) The aircraft's velocity vector and aircraft center position are clearly shown on the pilot's attitude display. There is an example aircraft center position display in Figure 31 and indicated by the orange arrow. When the aircraft experiences a shift in roll or pitch, the

center point would move towards the outside of the circle with an associated vector [FCL-R01].
2) There is a hover page that looks different between CLAW modes or between RCAH versus ACAH modes within a CLAW mode [FCL-R02].
3) There is a clear cue of which CLAW mode is engaged AND active versus armed [FCL-R03].

Figure 31: Example Cyclic / Aircraft center position for Pilot Flight Display ("UH-72A Aircrew Training Manual" 2020)

4.4.1.3 Controller Operating Mode Scenario

Primary UCA:

PI-UCA-8: Pilot provides excessive torque command (over-torque) when FCC is in alternate control law mode (loses over-torque protections) [H-1, H-2, H-3, H-4]

Contributary or Resulting UCAs:

PI-UCA-17: Pilot does not change CLAW mode before making cyclic, TCL, pylon, or pedal adjustments [H-1, H-2, H-3, H-4]

FCC-UCA-6: FCC provides excessive torque command (over-torque) beyond structural limits of the configuration [H-1, H-2, H-3, H-4]

Assumptions:

1) Fly-by-wire aircraft can control the power demand from pilots to avoid potentially "over-torquing" the engine. In mechanically linked aircraft, pilots must control the rate at which they demand power in the collective to avoid this phenomenon because the computer would not solely provide that protection. However, there are instances when temporarily exceeding power demands may be necessary, such as to avoid an obstacle. There may be a specific mode in the fly-by-wire computer that pilots could utilize in these situations.
2) The tiltrotor aircraft in this scenario has two engines for redundancy.
3) In multi-ship formation flying, aircraft that are in positions two or greater may require quick control inputs to maintain spacing with other aircraft surrounding them. This could involve rapid power-demands for altitude or airspeed adjustments.

SC-PI-3: A tiltrotor aircraft is flying third in a multi-ship formation of four aircraft. The four aircraft are in a landing zone picking up troops of soldiers, which increases the overall gross weight of each aircraft. The aircraft pylons are in helicopter mode at 90° up. Upon takeoff, the four aircraft begin a constant angle, steep takeoff out of the confined LZ, which requires high torque. Aircraft three experiences a single engine failure, and the FCC enters an emergency power mode, allowing the operating engine to exceed its limits to temporarily provide more thrust or lift.

The pilot is unaware of the mode change due to inadequate feedback, incorrect mental model of the single-engine failure emergency procedures, or task saturation [PI-PMB-3]. The pilot does not change or adjust the CLAW mode [PI-UCA-17] before providing excessive torque command (over-torque) [PI-UCA-8] to continue the takeoff maneuver in the formation flight, which the FCC allows because of its current mode [FCC-UCA-6]. This excessive torque command may cause the aircraft to lose sufficient lift [H-2], lack the power to remain airborne [H-2], violate its structural integrity [H-3], violate minimum separation standards with other aircraft, trees, or the ground [H-4], and fail to continue its mission tasks [H-5] if the pilot is unaware of the mode change. This scenario is depicted in Figure 32.

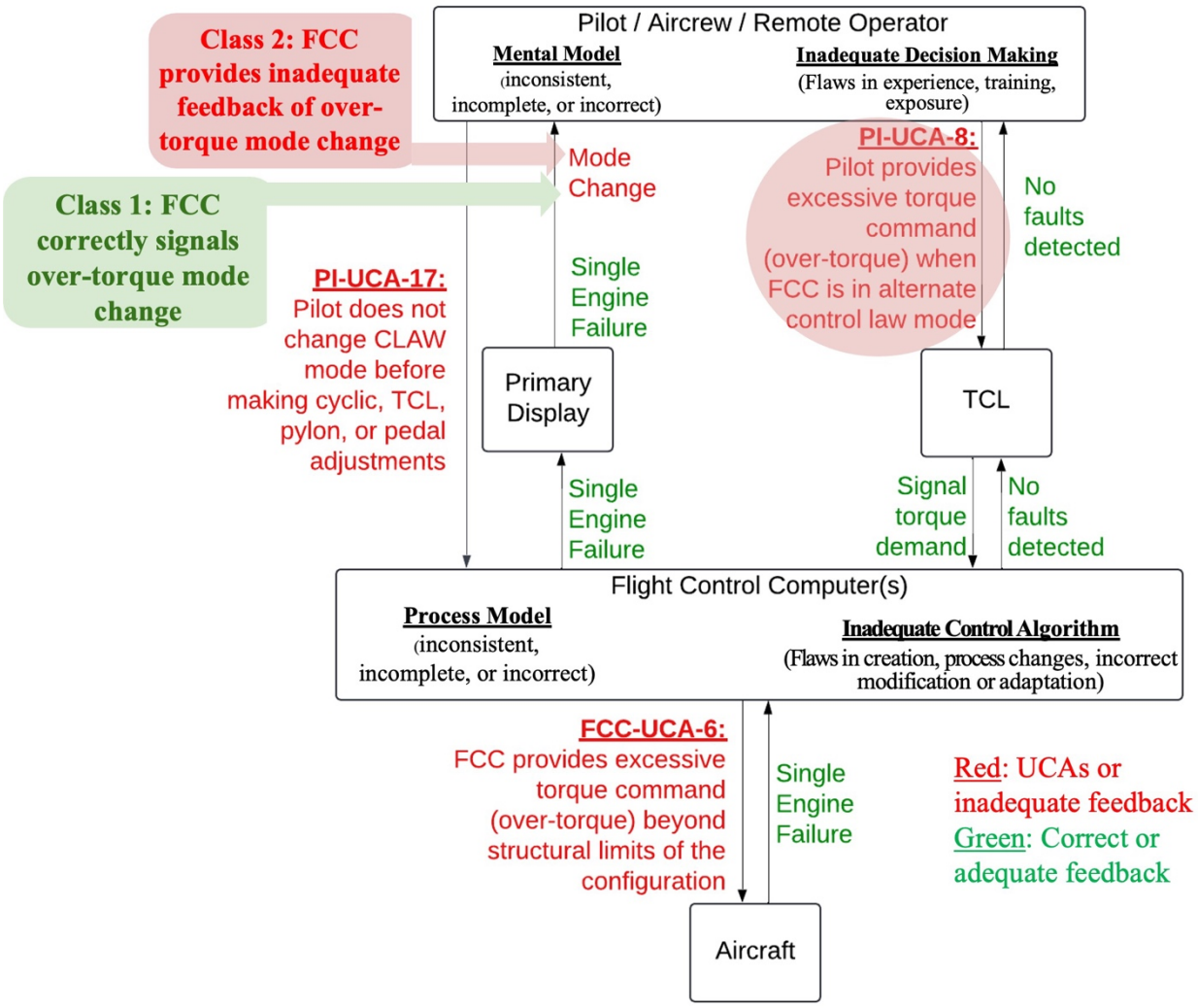

Figure 32: SC-PI-3

Insight: This scenario did involve a system failure of one engine, but the hazards occurred because of multiple UCAs from the pilot and the computer. This can be a classification one or two scenario:

1) The controller (FCC) provides adequate feedback to the pilot that the CLAW mode changed to an emergency mode, but the pilot continues to carry out an unsafe control action because of inadequate decision making or an incorrect mental model of when or how this emergency mode operates.
2) The controller (FCC) provides inadequate or no feedback that the computer is in an emergency mode, resulting in the pilot carrying out unsafe control actions. The computer in this case may have a flawed design in the control algorithm for CLAW mode change indication.

Solutions: While emergency modes are sometimes vital for aircraft survivability, each controller must have a sufficient and complete process model of these modes to prevent misuse that could lead to accidents. Activation of emergency modes could be designed in the following manners:

1) A pilot or remote operator must manually activate an emergency mode to utilize its features. This requirement would decrease chances for mode confusion as the pilot would know that the mode is activated and how that mode will perform [FCL-R04.1].
2) The emergency modes activate automatically given a certain set of parameters; in the case of this scenario, a single engine failure activates a power emergency mode. However, the activation mode is appropriately cued to the pilot through visual and/or auditory means and is explained in designated emergency procedures for single engine failures [FCL-R04.2].

4.4.2 FCC Scenarios

4.4.2.1 Operating Mode of the Controlled Process Scenario

Primary UCA:

FCC-UCA-2: FCC signals autopylon transition forward when aircraft is in a hover (incorrect airspeed reading due to winds and pitot static readings) [H-1, H-2, H-2.2, H-4]

Contributing or Resulting UCAs:

PI-UCA-12: Pilot does not provide neutral control command when maintaining a hover [H-2.1, H-4]

FCC-UCA-11: FCC provides control commands when maintaining a hover [H-2.1, H-4]

Assumptions:

1) Airspeed readings originate from pitot-static systems that convert dynamic pressure into airspeed measured in knots. Pitot tubes measure airspeed as the speed of the aircraft relative to the air, so in the case of an aircraft in a hover with a headwind, the airspeed reading would show the wind speed and not the aircraft's ground speed.
2) Autopylon control laws use airspeed from pitot-static system and pilot control inputs from cyclic, TCL, and pedals to determine appropriate pylon angle.

SC-FCC-1: A tiltrotor aircraft is hovering with autopylon engaged. There is a headwind of TBD knots, which is also the minimum airspeed reading that the FCC interprets as guidance to begin pylon transition forward [FCC-PMB-1]. The FCC signals autopylon transition forward when the aircraft is in a hover from the misunderstood airspeed reading due to winds and pitot static readings [FCC-UCA-2]. The pilot believes that the aircraft pylons are not transitioning because they have not made any forward input on the cyclic to indicate forward airspeed [PI-PMB-4]. The pilot does not provide counter control inputs to the transitioning pylons to maintain a hover [PI-UCA-12]. The FCC would also make erroneous control inputs to the flaperons, elevators, or rudders in addition to the pylons for transitioning the aircraft forward [FCC-UCA-11]. These flight control inputs could result in the aircraft experiencing an unexpected center of gravity shift [H-2.1] or violating minimum aircraft separation standards [H-4]. This scenario is depicted in Figure 33.

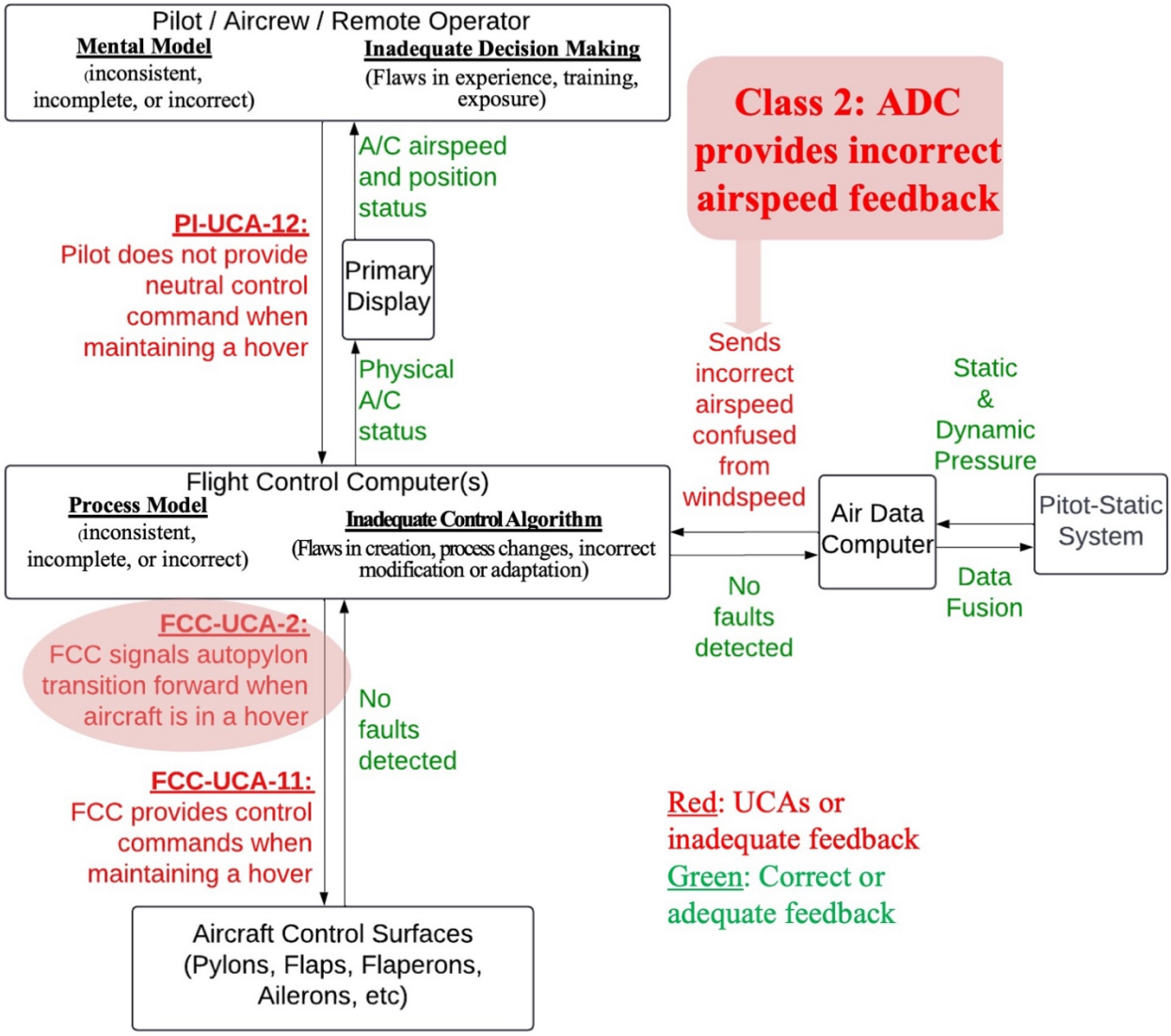

Figure 33: SC-FCC-1

Insight: This scenario did not involve any system failure or malfunction and is a classification two: the controller (FCC) received and interpreted unsafe feedback (windspeed interpreted as aircraft airspeed) and carried out an unsafe control action (transitioning pylons forward). The incorrect feedback from the ADC is not a system failure if it interprets data in a way that was deliberately designed. The FCC experienced mode confusion about the state of the controlled process when it believed the aircraft was initiating movement forward and moved the pylons when the pilot required a stationary hover.

Solutions: This scenario highlights the importance of early design considerations for pylon control laws that interpret multiple inputs for angle adjustments.

1) Autopylon control laws use an additional windspeed reading to supplement the pitot-static tubes to prevent the FCC from having an incorrect process model or inadequate control algorithm of the aircraft's movement [AP-R04].
2) Autopylon initial transitions provide a unique cue to the pilot on the display rather than just indicating the change in angle. An example of a pylon angle indicator is shown in Figure 34 from a V-22 pilot function display (PFD). The green color indicates the safe pylon angle range for the aircraft's given airspeed, and the red would indicate an unsafe angle that could result in a stall. The recommendation is that when the pylon initiates a change from full forward (around 0°) to full up (90°), or vice versa, the display provides a caution or indicator to the pilot/operator that a movement has been initiated [AP-R05].

Figure 34: Pylon angle (1°) on Pilot Function Display ("The V-22," n.d.)

4.4.2.2 Controller Operating Mode Scenarios

Primary UCA:
FCC-UCA-4: FCC stops signaling autopylon command before pylons are in helicopter or airplane mode (FCC reset or incorrect airspeed readings) [H-1, H-2.1, H-2.2, H-4]

Contributing or Resulting UCAs:
PI-UCA-16: Pilot stops providing pylon commands after autopylon disengages or stops movement [H-4]
PI-UCA-4: Pilot does not engage autopylon before slowing aircraft to an irrecoverable stall airspeed [H-1, H-2, H-2.2, H-4]
PI-UCA-18: Pilot approaches to land when the aircraft is in conversion mode [H-1, H-2.1, H-4]

Assumptions: The tiltrotor's airspeed is calculated using information from the pitot-static system, air data computer (ADC), and/or GPS.

SC-FCC-2.1: A tiltrotor aircraft is flying in airplane mode with the autopylon engaged. The aircraft begins to slow down to enter a traffic pattern and landing approach at an airfield. The autopylon function of the FCC begins to convert the pylons up in accordance with the airspeed reduction. The FCC experiences a reset due to either a malfunction or separate system failure and disengages the autopylon while halfway between airplane and helicopter mode (conversion angle mode) [FCC-UCA-4]. The pilot does not reengage autopylon [PI-UCA-4] or manually convert the pylons full up [PI-UCA-16] when the aircraft is in conversion mode because they are either task saturated or do not know that the autopylon disengaged [PI-PMB-5]. The pilot continues the approach to land [PI-UCA-18] while in conversion mode and may lose sufficient lift [H-2.2],

become uncontrollable [H-1], or violate separation standards by crashing into the ground [H-4]. This scenario is depicted in Figure 35.

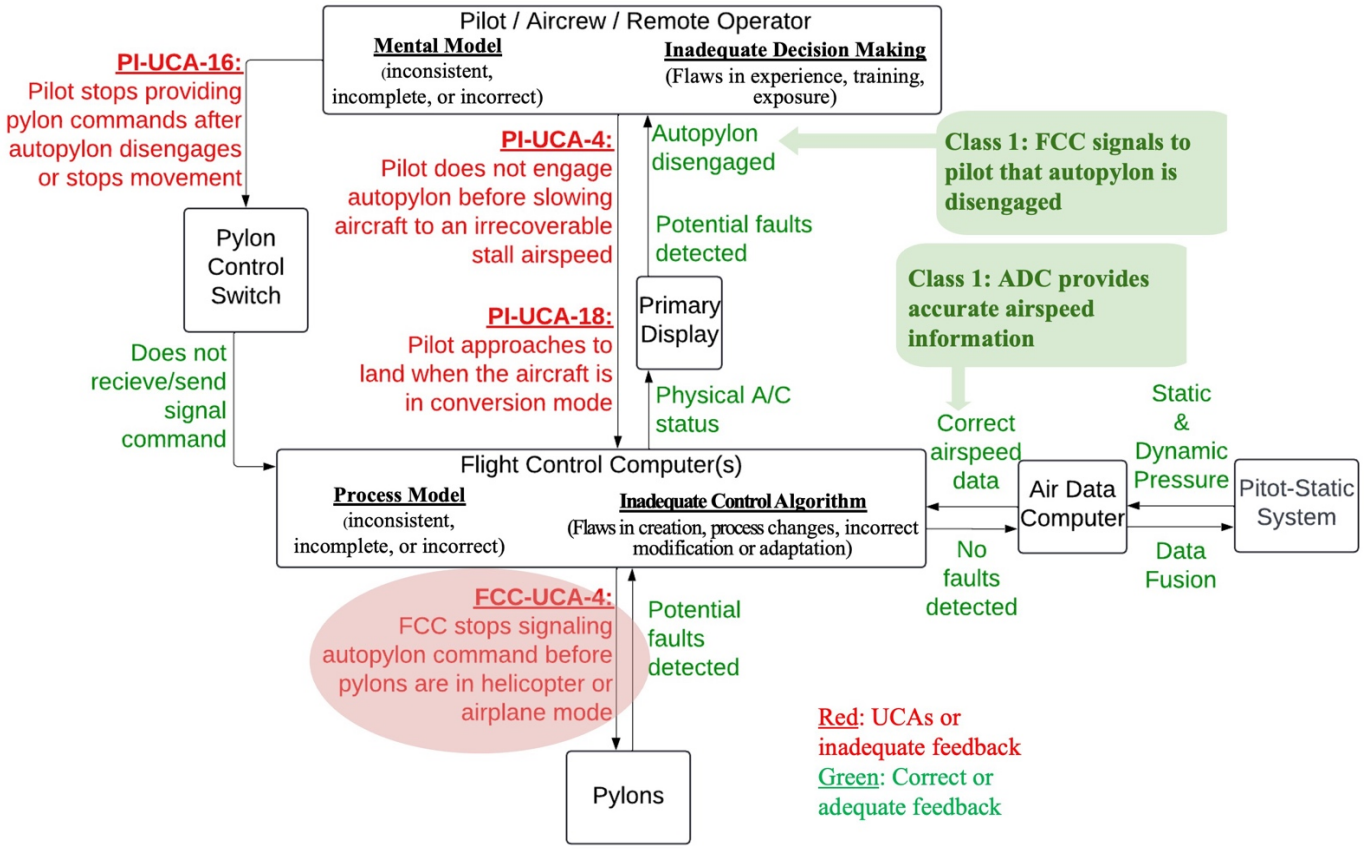

Figure 35: SC-FCC-2.1

Insight: This scenario does involve potential system failure or malfunction and is a classification one: the controller (FCC) received and interpreted correct feedback but disengaged the autopylon in a critical angle during a task saturated moment. The pilot received correct feedback that the autopylon disengaged. The FCC adjusted its operating mode according to control laws for system failures, and the pilot carried out multiple, resulting unsafe control actions due to task saturation or potential mode confusion with the FCC.

SC-FCC-2.2: A tiltrotor aircraft is flying in airplane mode with the autopylon engaged. The aircraft begins to slow down to enter a traffic pattern and landing approach at an airfield. The autopylon function of the FCC begins to convert the pylons up in accordance with the airspeed reduction. The FCC stops signaling autopylon movement because of erroneous airspeed information from the ADC or GPS when the pylon is in conversion mode [FCC-UCA-4]. The autopylon is still engaged so the pilot believes that the autopylon is functioning in accordance with accurate airspeed indicators [PI-PMB-6] so they do not manually convert the pylons full up when the aircraft is in conversion mode [PI-UCA-16]. The pilot continues the approach to land while in conversion mode [PI-UCA-18] and may lose sufficient lift [H-2.2], become uncontrollable [H-1], or violate separation standards by crashing into the ground [H-4]. This scenario is depicted in Figure 36.

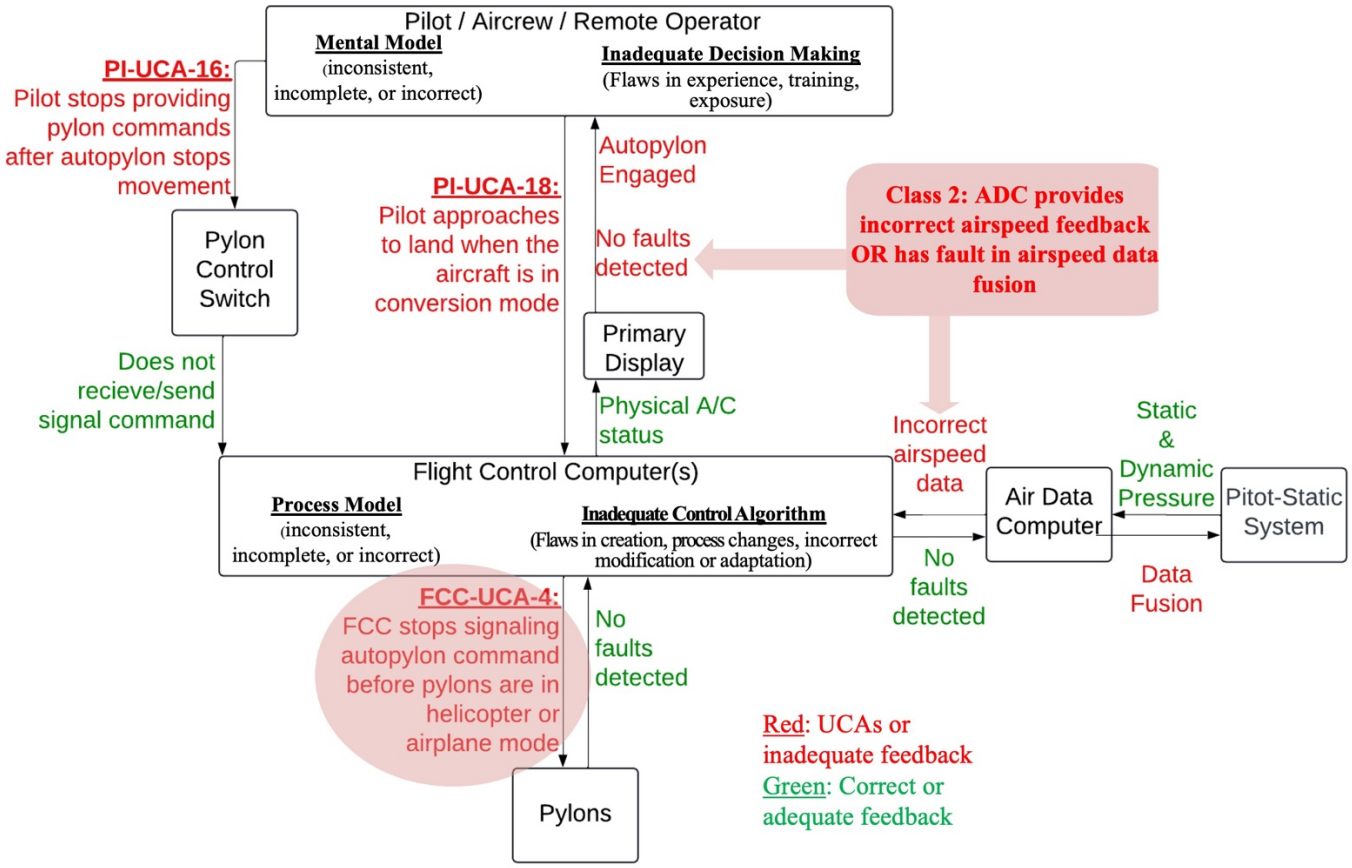

Figure 36: SC-FCC-2.2

Insight: This scenario may involve a system fault if the data fusion function of the FCC or ADC is malfunctioning. If the ADC interpreted airspeed in a programmed or intended way, this scenario would not have occurred from a system failure. Regardless, the control laws for airspeed interpretation by the FCC are crucial for autopylon functionality; the FCC adjusted its operating mode based on incorrect feedback or faulty data fusion, and the pilot was unaware of the mode change due to potential inadequate feedback, incorrect mental model, or lack of exposure with this type of situation. This scenario is a classification two as it provides incorrect airspeed information and results in multiple unsafe control actions from multiple controllers.

Solutions: A tiltrotor aircraft is at its most vulnerable while in conversion mode–it neither benefits fully from the aerodynamic components of helicopter or airplane modes. Lift is generated uniquely with the combination of VTOL and airplane flight controls, and it requires specific handling qualities from the pilot. Options for design to prevent this type of scenario and resulting accident are:

1) If the FCC disengages autopylon mode due to a separate system malfunction, it defaults to either helicopter or airplane mode based on the conversion corridor airspeed. If it is "lower" on the conversion corridor, it defaults to helicopter mode. If it is 'higher" on the conversion corridor, it defaults to airplane mode. The pilot or operator is trained and experienced with either airspeed default [AP-R06.1].

2) If the FCC disengages autopylon due to a separate system malfunction, the pylon is held at whatever angle the disengagement occurred at and sends an appropriate cue to the pilot visually or auditorily for acknowledgement, so they know to manually adjust the pylon or attempt to reengage the autopylon [AP-R06.2].

4.4.2.3 Supervisory Mode Scenario

Primary UCA:

FCC-UCA-1: FCC does not signal autopylon commands when aircraft reaches designated engagement airspeed [H-1, H-2, H-2.2, H-4, H-5]

Resulting UCA:

PI-UCA-15: Pilot stops providing control commands after reaching designated airspeed for mode change [H-1, H-2.2, H-4, H-5].

Assumptions:

1) For this scenario, the autopylon mode is operational only within a designated airspeed range. For example, 30 knots would be the minimum airspeed for the autopylon to engage up to 200 knots.
2) For a two-pilot tiltrotor aircraft, there is a flight director (FD) for each pilot. Only one FD is active and sending signals to the FCC for control authority at one time, but both may be armed at the same time.

SC-FCC-3: A tiltrotor aircraft is hovering with zero knots forward airspeed at 50 feet above ground level (AGL) with zero knots windspeed. Pilot #1 arms but does not engage the autopylon, which they believe will activate the autopylon functions once the aircraft reaches 30 knots of forward airspeed. Pilot #1 initiates forward movement to generate airspeed, but the FCC does not change modes from armed to engaged and thus does not signal autopylon commands when the aircraft reaches 30 knots [FCC-UCA-1]. The pilots' mode confusion could occur because the pilot #2 has their FD engaged while pilot #1 could be in standby mode or just armed on their flight director. Pilot #1 believes that the FCC is controlling the autopylon because they armed the autopylon on their FD but did not take control authority from pilot #2's FD [PI-PMB-7]. The FCC believes that it should not engage autopylon because it does not receive the appropriate signal from either pilots' FD [FCC-PMB-2]. Neither pilot issues pylon commands when reaching the designated airspeed for mode change due to their PMB [PI-UCA-15]. The pilots' and computer's lack of control input could result in the aircraft becoming uncontrollable [H-1], losing lift if the aircraft increases airspeed without pylon transition [H-2.2], violating minimum separation standards [H-4], and being unable to fulfill its mission [H-5]. This scenario is depicted in Figure 37.

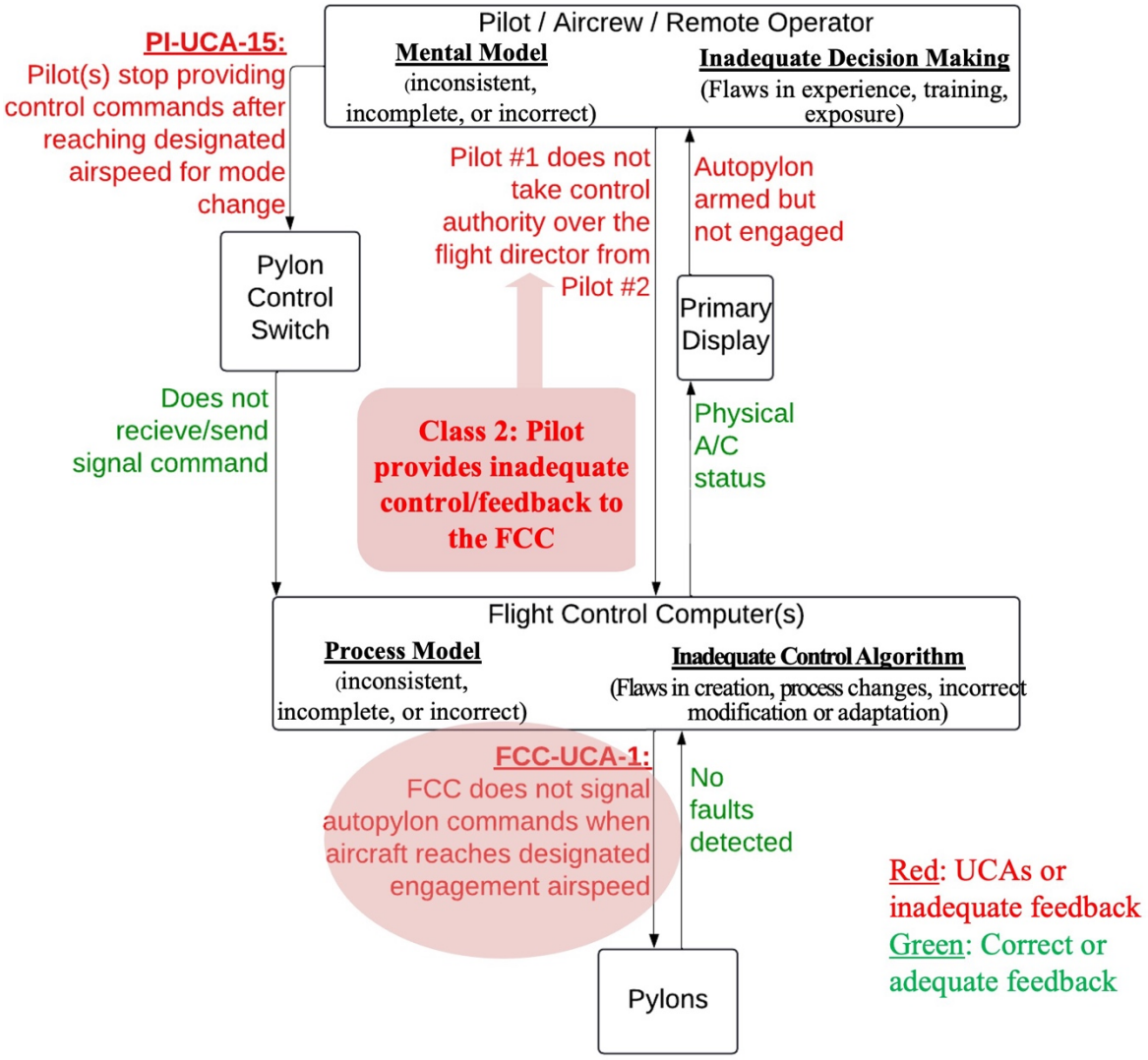

Figure 37: SC-FCC-3

Insight: This scenario does not involve a system failure or malfunction and is a classification two: the FCC received inadequate control from the pilots based on their intention to engage the autopylon resulting in multiple unsafe control actions. This misunderstanding between the pilots and the FCC through the flight director (FD) is common in operational military helicopters today.

Figure 38 depicts an example of a flight director that shows an illuminated green light under FMS, ALTP, IAS, VS, and CPLD. The important distinction is that the CPLD light is green, indicating that this flight director is ENGAGED and actively sending commands to the FCC. If the light under CPLD was yellow, it would only be ARMED and not providing commands to the FCC. While having an "armed" function of the FD versus engaged, a co-pilot may provide back-up to the pilot on the controls with their FD ready to engage in the case of a needed control handover. However, pilots may miss a step in engaging their FD due to inadequate FD architecture, task saturation, or a lack of exposure or experience. Due to mode confusion, the

pilots believed that the FCC had supervisory control over the autopylon mode, and they did not provide the input needed for pylon control throughout their mission.

Figure 38: Flight Director Example ("UH-60 Flight Tutorial | Aerofly FS," n.d.)

Solutions: If an aircraft architecture includes an armed versus engaged feature for autopylon, it must be visible and clear to the pilots to avoid potential mode confusion [AP-R01]. If the autopylon is engaged or disengaged, the pylon should still have "conversion corridor protection" that would adjust the pylon angle if the aircraft reached a threshold airspeed requiring pylon adjustment forward to airplane mode or up to VTOL mode. Corridor protection activation is then cued to the pilot through visual and/or auditory means [AP-R07].

4.5 Summary of Recommendations for Design and Operations

The STPA analysis provides potential options for the software and hardware design of tiltrotor aircraft, including human behavior considerations focused on mode confusion. The outputs can be used for system architecture development, system and subsystem requirements, design recommendations, mitigations, safeguards, or existing design gaps.

This STPA provides unique information not highlighted in traditional hazard analyses. A comparison to traditional hazard analysis methods in Section 4.6 shows the necessity of using STPA to account for the complex relationships between controllers for design considerations. Table XVII summarizes the design recommendations developed from the STPA scenarios to aid in preventing mode confusion in tiltrotor aircraft operations.

Table XVII: Tiltrotor Design Recommendations

Function	Recommendations
Autopylon (AP)	*AP-R01:* Autopylon ARM / ENGAGE / DISENGAGE is cued to the pilots or operators **[SC-PI-1]**
	AP-R02: Autopylon malfunction is cued visually and / or auditorily to the pilots or operators **[SC-PI-1]**
	AP-R03: Autopylon engage / disengagement criteria is determined by either 1) weight-on-wheels or 2) pilot demand **[SC-PI-1]**
	AP-R04: FCC utilizes multiple sources for windspeed data fusion to feed autopylon commands **[SC-FCC-1]**

	AP-R05: Autopylon initial transitions or conversions provide a unique cue to the pilot or operator after TBD minutes of no change **[SC-FCC-1]**
	AP-R06.1: Autopylon disengagement due to failure or malfunction defaults the angle to helicopter or airplane mode based on an airspeed corridor **[SC-FCC-2]**
	AP-R06.2: Autopylon disengagement due to failure or malfunction holds pylon angle but requires pilot or operator acknowledgment for manual control **[SC-FCC-2]**
	AP-R07: Corridor Protection is always active regardless of autopylon engagement to prevent the aircraft from flying in airspeeds outside of airplane or helicopter mode capability **[SC-FCC-3]**
Flight Control Laws (FCL)	*FCL-R01:* Pilot display shows aircraft velocity vector and aircraft center position **[SC-PI-2]**
	FCL-R02: Different control law modes have different hover mode pages presented to the pilots or operators **[SC-PI-2]**
	FCL-R03: ARMED / ENGAGED have clearly different display features **[SC-PI-2]**
	FCL-R04.1: Emergency modes are activated only through pilot or operator command **[SC-PI-3]**
	FCL-R04.2: Emergency mode activation can be automatically initiated but is clearly cued to pilot or operator through visual and/or auditory means **[SC-PI-3]**

4.6 Limitations of Traditional Hazard Analyses for Tilt Aircraft Technology

This section identifies the limitations of traditional hazard analysis techniques in identifying chances of mode confusion for tilt-aircraft and compares them to STAMP methodology. A NASA study conducted on various configurations of VTOL aircraft found that traditional hazard techniques rely heavily on component reliability (Darmstadt and et al., n.d.). These analyses fall short in providing early-stage architecture guidelines focused on mode confusion prevention as they focus solely on component failures.

This study conducted an FHA, FMECA, and FTA for a tilt-wing aircraft, which are included in the Appendix. These analyses specifically focus on the tilt-wing powertrain configuration providing rotary motion to the rotor system. This configuration includes the generators, motors, gearboxes, and interconnecting shafts. The design of the tilt-wing aircraft is depicted in Figure 39. It includes four rotors attached to a tilting wing and utilizes a turboelectric powertrain.

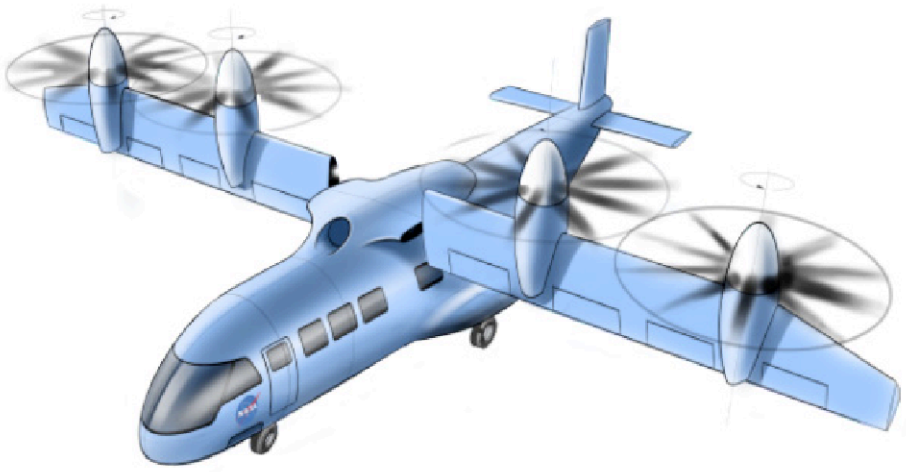

Figure 39: Four-rotor Tilt-wing Aircraft for NASA Study

4.6.1 Functional Hazard Analysis (FHA)

The FHA Function Description “Transmit Adequate Power to Rotors” identified seven failure conditions:

1. Any loss of single propulsor fail
2. Any combination of dual propulsor fail
3. Complete Propulsion loss
4. Dual esc fail
5. Single esc fail
6. Single gearbox fail
7. Dual gearbox fail

These failure conditions include follow-on scenarios with resulting aircraft physical states and pilot/operator required actions for potential survivability. Theoretically, these results provide design considerations to help mitigate and control the possible failures through a Derived Safety Requirements (DSR) list. An example of a failure condition effect from the FHA is listed below:

> Any combination of Dual propulsor Fail *during all phases of operation*: Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Reduced power available. Insufficient power to maintain level fight. Gliding approach to airplane mode or Run-On Landing (ROL). If adequate room exists for flare and roll-out, no damage or loss of occupants. Worst case feasible outcome is loss of air-vehicle/occupant.

While this scenario provides suggestions for how the aircrew can maintain adequate lift of the aircraft, it does not consider the control and feedback loops between the aircrew, aircraft, and computers associated with system failures. It assumes that the human operator will react perfectly, or else failure is imminent. Because of this assumption, most accident investigations deem human error as the main causal factor. Reaction time, mental/process models of the system design, experience, or exposure can all contribute to distinctive scenario results that can then be analyzed to influence design changes.

Applying this FHA to the two-tiltrotor aircraft analyzed in Chapter 4 does not provide the necessary information to analyze the effect of partial or full power loss that could lead to mode confusion like that in scenario SC-PI-3. To revisit that accident scenario, the pilot demands excessive torque command, resulting in propulsion power failure for sufficient thrust and lift. The scenario provided by the FHA here recommends that the pilots conduct a gliding approach or run-on landing depending on the configuration of the pylon angle during propulsion loss, but it does not provide a solution or redesign mitigation considerations for pylons potentially stuck in conversion mode.

STPA provides a different way forward by identifying control interactions and feedback loops between system controllers. These relationships are then used to uncover system design solutions to prevent unsafe control actions associated with mode confusion. STPA identified the following UCAs and follow-on redesign considerations involving a unique case of propulsion loss resulting from excessive torque command:

UCAs

1) **PI-UCA-8:** Pilot provides excessive torque command (over-torque) when FCC is in alternate control law mode (loses over-torque protections) [H-1, H-2, H-3, H-4]
2) **PI-UCA-17:** Pilot does not change CLAW mode before making cyclic, TCL, pylon, or pedal adjustments [H-1, H-2, H-3, H-4]
3) **FCC-UCA-6:** FCC provides excessive torque command (over-torque) beyond structural limits of the configuration [H-1, H-2, H-3, H-4]

Recommendations

While emergency modes are sometimes vital for aircraft survivability, each controller must have a sufficient and complete process model of these modes to prevent misuse that could lead to accidents. Activation of emergency modes could be designed in the following manners:

1) A pilot or remote operator must manually activate an emergency mode to utilize its features. This requirement would decrease chances for mode confusion as the pilot would know that the mode is activated if they understand when and how that mode will perform [FCL-R04.1].

2) The emergency modes activate automatically given a certain set of parameters; in the case of this scenario, a single engine failure activates a power emergency mode. However, the activation mode is appropriately cued to the pilot through visual and/or auditory means and is explained in designated emergency procedures for single engine failures [FCL-R04.2].

These results highlight UCAs from multiple controllers of the system stemming from inadequate control algorithms and incorrect process models. Traditional hazard analyses do not consider process models or the interactions between various controllers when determining the effects of failures for design considerations.

Another example from the FHA describes an event regarding a gearbox failure:

> Dual gearbox failure *on opposite wings:* Failures detected and annunciated to aircrew (chip light, temp/ pressure indications). Loss of ability to spin rotor associated with any two gearboxes will result in loss of sufficient power for airplane mode level flight. Pilot compensation possible via directional control. Safe flight to ROL possible but will require adequate aircrew workload impact. Possible loss of air vehicle and occupants.

This scenario includes the guideline "will require adequate aircrew workload impact," which highlights that additional analysis is needed for human-factors considerations. However, the FHA format does not provide follow-on steps for recommendations of the prevention of hazards through design changes. Additionally, there are multiple assumptions made in this scenario, and an outcome for survivability could vary depending on the inclusion or dismissal of any combination of these assumptions.

The scenario only considers the aircraft state in airplane mode, not VTOL or conversion modes. This analysis could expand upon different outcomes with possible pilot reactions, including the possibility of mode confusion. This scenario does not provide the analysis needed to improve aircraft design and prevent tiltrotor accident scenarios examined from STPA.

The identified failure conditions from this FHA were fed into the FMECA and FTA analyses.

4.6.2 Failure Modes and Effects Criticality Analysis (FMECA)

The FMECA used failure causes from the FHA and historical component failure rates from an industry search. The resulting failure mode criticality numbers indicated further research was needed to improve the analysis in order to meet aircraft certification standards. The following example highlights a scenario developed for prop-rotor functionality:

> Function No. 4: Provide torque to prop-rotors.
> *Failure Cause:* Prop-rotor gearboxes, clutches, shafts
> *End Effect:* 25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in One Motor Inoperable (OMI) avoid region.

While this scenario discusses the possibility that the tilt-wing aircraft could become uncontrollable due to propulsion loss, it does not clarify the end effects associated with VTOL, conversion, or airplane modes of operation. However, this example does provide information for redesign considerations for tilt-wing aircraft, particularly in the event of a torque loss similar to the accident scenario SC-PI-3 in Section 4.4.1.3.

This FMECA scenario does not provide any insight into design considerations associated with non-failure or mode confusion scenarios, like those in the STPA scenarios in Chapter 4.

4.6.3 Fault Tree Analysis (FTA)

The FTA was performed using hazards identified from the FHA specific to the propulsion system. These failures provided the top-level events that were broken down into potential causal events. The probabilities of these events were calculated using the following "AND" and "OR" gates in Figure 40 and equations (1) and (2).

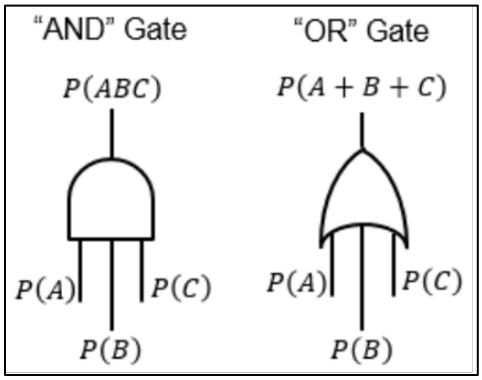

Figure 40: "AND" and "OR" Gate Symbols

$$P(ABC) = P(A) * P(B) * P(C) \quad (1)$$

$$P(A + B + C) = P(A) + P(B) + P(C) - P(A) * P(B) - P(A) * P(C) - P(B) * P(C) + P(A) * P(C) \quad (2)$$

The FTA of note includes the top-level event "Loss of Power Transmission" with an OR gate of "Loss of Propulsion." It includes the mid-level events:

1) Dual electric motor fail
2) Dual gearbox fail
3) One Engine Inoperative (OEI) Propulsion Loss
4) Complete Propulsion Loss
5) Dual ESC Fail

This analysis found consistent probabilities in line with the FMECA results, further implying that the architecture selected for this tilt-wing design does not provide high enough probability and, therefore, reliability statistics for aircraft certification. The FTA does not provide further details for potential scenarios associated with these probabilistic events. This FTA also required a specific aircraft architecture and design for its modeling, making redesign recommendations potentially more consequential or expensive. The FTA does not include human-factors or mode

confusion considerations. It would not have provided design considerations as STPA did earlier in this chapter.

4.6.4 Organizational Analysis

The traditional hazard analysis techniques from the NASA study do not account for organizational factors as CAST's results do in Chapter 3. Systematic factors in an organization can contribute to flawed system design and follow-on accidents, and it is vital to include them early in hazard analysis. Although the STPA from Chapter 4 was performed only on the technical components of the system, the analysis could have included organizational and managerial factors by extending the control structure and the analysis. The step-by-step processes of CAST and STPA are not available in traditional techniques for considering the organization.

Chapter 5 Conclusion

The primary objective of this thesis is to demonstrate how to enhance the safety of tiltrotor aircraft by identifying mode confusion potential using STPA. Tiltrotor and VTOL aircraft offer significant value by combining the aerodynamic efficiencies of fixed-wing and rotary-wing aircraft, such as high airspeeds, hover capability, and increased maneuverability. However, these qualities, combined with increased automation, have the potential to lead to higher chances of mode confusion between aircrews and the flight control computers. It is important to be able to analyze human-machine interaction in aviation safety, specifically in tiltrotor aircraft with complex modes of operation.

The two CAST results identified systematic factors for the V-22 Osprey tiltrotor at the aircraft and higher organizational levels that led to unsafe control actions. These factors involved inappropriate computer control algorithms and controller process model flaws, resulting in mode confusion between the pilots and the automation. Through identifying UCAs and inadequate feedback between controllers, these CASTs provided recommendations for design improvements that may prevent accidents involving mode confusion in future tiltrotor aircraft operations.

STPA provides a unique way forward for identifying hazards for tiltrotor aircraft before an accident occurs. The top-level analysis began with system losses, hazards, and safety constraints and identifies potential loss scenarios. The flexible structure of STPA does not require detailed design information, which reduces any necessary and costly redesign at the end of the system design process.

The various levels of abstraction of the control structures provide different models to help identify hazards that can arise from the interaction of subsystems at various levels of the overall system. The UCAs developed from the control structures involved only the unique features of tiltrotor aircraft, including an autopylon program, unique-trim control laws, and the Thrust Control Lever (TCL). The resulting scenarios include specific instances of potential mode confusion associated with the autopylon control modes, the transition between vertical and horizontal flight, and the utilization of varying levels of flight control augmentation. These scenarios provide the information necessary to develop potential design recommendations and requirements for avoidance of hazards early in the system engineering process. STPA could also be used for other hazards not related only to the unique tiltrotor design.

Traditional hazard analyses do not provide detailed information on the different controllers' mental models or the critical control and feedback loops in tiltrotor control structures. They rarely analyze details of the human operators in their scenarios, as seen in section 4.6. The provided FHA, FMECA, and FTA examples for a four-rotor tilt-wing aircraft focused, as do almost all such analyses, on propulsion failure and the associated responses from the operators that could warrant accident avoidance. When providing human response options, they do not consider critical human-factors data like reaction time, mental models, or mode confusion. In contrast, STAMP methodology, including CAST and STPA, identifies complex interactions between system controllers, including human operators, that could lead to mode confusion, and they do so early in the system engineering process when they can be most useful.

To conclude, this thesis demonstrates the advantage of using STPA to identify mode confusion and provide design recommendations, which traditional hazard analyses do not offer. Optimized control law algorithms and an improved cockpit interface allow tiltrotor aircraft to operate more safely in the aviation environment. Tiltrotor aircraft have been criticized for their complex aerodynamic handling qualities and historically fatal accidents. However, if appropriate

safety analyses are applied to guide design improvements, tiltrotor aircraft have the potential for broader applications and mission diversity over traditional aircraft designs.

5.1 Limitations and Future Work

This thesis is not meant to be exhaustive. The STPA analysis focuses on certain subsystems while neglecting other critical components and other possible contexts. It also limits the understanding of other safety risks unrelated to mode confusion, such as every possible mechanical or structural failure. There is also an operational variability involved in this STPA as different environmental conditions and pilot experience levels still need to be fully accounted for. The analysis does not carefully study cognitive and psychological factors like pilot workload, stress, or fatigue. It does not consider the unique cognitive differences between pilots in the aircraft as opposed to remote operators. Finally, identifying hazards and UCAs depends on the judgment and expertise of the analyst, as is true for every type of hazard analysis. STPA does, however, provide a structured step-by-step process that other techniques do not, and STPA can address these limitations effectively.

There is room for future work when applying STPA to identify mode confusion, as this thesis does not cover many variations of tiltrotor and VTOL aircraft. STPA can be used when integrating manned and unmanned tiltrotor aircraft in multi-ship formations or when investigating the implications of multi-controller systems in air traffic control involving tiltrotor aircraft. A recent dissertation by Kopeikin covers many of these topics, such as coordination among multiple system components and controllers (Kopeikin 2024).

In summary, aircraft engineers, designers, and safety experts can benefit from using and applying STPA when creating and optimizing future tiltrotor aircraft. The results of this thesis prove the usefulness and benefits of using STPA for hazard analysis of tiltrotor aircraft and other advanced aircraft designs.

References

Appleton, Wesley. 2020. “Aeromechanics Modelling of Tiltrotor Aircraft.” Ph.D., England: The University of Manchester (United Kingdom). https://www.proquest.com/docview/2513118333/abstract/F3037051F6C4480BPQ/1.

“Bell Boeing V-22 Osprey.” n.d. Accessed October 23, 2024. https://drawingdatabase.com/bell-boeing-v-22-osprey/.

Bishop, Brittany E., Polly M. Harrington, Rodrigo L. Rose, and Nancy G. Leveson. 2023. “System Theoretic Process Analysis for Identification of Sources of Mode Confusion.” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 67 (1): 2397–2403. https://doi.org/10.1177/21695067231192457.

Commanding General, II Marine Expeditionary Force. 2012. “COMMAND INVESTIGATION INTO THE FACTS AND CIRCUMSTANCES SURROUNDING THE CLASS ‘A’ MISHAP INVOLVING THE MV-22B CRASH THAT OCCURRED NEAR CAP DRA’A MOROCCO ON 11 APRIL 2012.” Manual of the Judge Advocate General. Camp Lejeune, NC: United States Marine Corps.

Darmstadt, Patrick, and et al. n.d. “Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems.” https://ntrs.nasa.gov/citations/20190026443.

Department of Defense. 2023. “MIL-STD-882E w/CHANGE 1: Department of Defense Standard Practice System Safety.” Department of Defense (DoD). http://assist.dla.mil.

Dumitru, Iulia Mădălina, and Mircea Boşcoianu. 2015. “Human Factors Contribution to Aviation Safety.” *International Scientific Committee* 49. https://www.researchgate.net/profile/Gheorghe-Savoiu/publication/347984143_SEARCHING_FOR_SHREADS_OF_ORDER_THE_STRUCTURE_OF_TODAY'S_INTERNATIONAL_SYSTEM/links/5feb57a245851553a004d0a0/SEARCHING-FOR-SHREADS-OF-ORDER-THE-STRUCTURE-OF-TODAYS-INTERNATIONAL-SYSTEM.pdf#page=51.

Ericson, Clifton A. 2005. *Hazard Analysis Techniques for System Safety*. 1st ed. Wiley. https://doi.org/10.1002/0471739421.

“Fundamentals of Flight.” 2022. Washington, D.C.: Headquarters, Department of the Army.

General John R. Dailey, Norman R. Augustine, General James B. Davis, and Dr. Eugene E. Covert. 2001. “V-22 Program Review Report.” Washington, D.C.: Department of Defense.

Haley Davoren. 2024. “Joby Prototype Lost Prop Blade, Exceeded Operating Conditions before 2022 Crash.” Globalair.Com. February 8, 2024. https://www.globalair.com/articles/joby-prototype-lost-prop-blade-exceeded-operating-conditions-before-2022-crash?id=6951.

Kopeikin, Andrew N. 2024. “System-Theoretic Safety Analysis for Teams of Collaborative Controllers.” PhD Thesis, Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/153787.

Leveson, Nancy. 2023. *An Introduction to System Safety Engineering*. Cambridge, Massachusetts: The MIT Press.

Leveson, Nancy G. 2012. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge (Mass.): MIT press.

McQuaid, Joel, Amir Kolaei, Götz Bramesfeld, and Paul Walsh. 2020. "Early Onset Prediction for Rotors in Vortex Ring State." *Journal of Aerospace Engineering* 33 (6): 04020081. https://doi.org/10.1061/(ASCE)AS.1943-5525.0001194.

N. G. Leveson. 2019. *CAST Handbook: How to Learn More from Incidents and Accidents*.

N. G. Leveson and J. Thomas. Mar2018. *STPA Handbook*.

National Transportation Safety Board (NTSB). 2014. "Descent Below Visual Glidepath and Impact With Seawall, Asiana Airlines Flight 214." NTSB/AAR-14/01. Washington, D.C.: National Transportation Safety Board. https://www.ntsb.gov/investigations/accidentreports/reports/aar1401.pdf.

"Osprey Aircraft Crash." 2000. Washington, D.C.: C-SPAN. https://www.c-span.org/video/?163595-1/osprey-aircraft-crash.

Reisweber and King. 2018. "AFS 400 Human Factors Engineering: Human Factors Workshop." Federal Aviation Administration, March 1.

Richard Whittle. 2010. *The Dream Machine: The Untold History of the Notorious V-22 Osprey*. Simon & Schuster.

SAE International. 2023. "ARP4761A: Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment." Warrendale, PA: SAE International. www.sae.org/standards/content/ARP4761A/.

Sarter, Nadine B., and David D. Woods. 1995. "How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37 (1): 5–19. https://doi.org/10.1518/001872095779049516.

"The V-22." n.d. Accessed October 23, 2024. https://forums.flightsimulator.com/t/the-v-22.

Thomas, John. 2024. "STPA Walkthrough: A Formal Scenario Approach." https://psas.scripts.mit.edu/home/wp-content/uploads/2024/STPA-Scenarios-New-Approach.pdf.

"UH-60 Flight Tutorial | Aerofly FS." n.d. Accessed October 23, 2024. https://www.aerofly.com/aircraft-tutorials/uh-60-startup-from-cold-and-dark/.

"UH-72A Aircrew Training Manual." 2020. Fort Rucker, Alabama: Department of Defense (DoD).

Appendix A NASA Traditional Hazard Analysis Techniques

A.1 Tilt-Wing FHA

Table A- 1: Tilt-Wing FHA

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Any loss of single propulsor fail	Away from OEI region	Aircrew detects failure and compensates with remaining thrust to continue flight	Minor
		In OEI region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
	Any combination of Dual propulsor Fail	All	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Reduced power available. Insufficient power to maintain level fight. Gliding approach to airplane mode or Run-On Landing (ROL). If adequate room exists for flare and roll-out, no damage or loss of occupants. Worst case feasible outcome is loss of air-vehicle/occupant	Catastrophic
	Complete Propulsion loss	Within 2 minutes of suitable landing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are adequate to provide power for a normal hover or (ROL).	Severe
		More than 2 minutes from a suitable landing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are NOT adequate to provide power for a normal hover or (ROL). Gliding approach without suitable landing area. Loss of air vehicle and occupants	Catastrophic
Transmit Adequate Power to Rotors	Dual esc fail	Dual ESC failed high: all phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots will need to reduce engine power to land. If hover power can be managed than land normally. If adequate room exists for flare and roll-out as required, no damage or loss of occupants. Worst case feasible outcome is air-vehicle damage and occupant injury	Severe

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of air-craft/crew	Classification of Failure Condition
		Dual ESC Failed Low: All phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Reduced power available. Insufficient power to maintain level fight. Gliding approach to airplane mode or Run-On Landing (ROL). If adequate room exists for flare and roll-out, no damage or loss of occupants. Worst case feasible outcome is loss of air-vehicle/occupant. Hazard classification is the same whether OEI or out of OEI avoid region.	Catastrophic
	Single esc fail	Esc failed hi: all phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots will need to manually modulate engine power Gliding approach to airplane mode or Run-On Landing (ROL).If adequate room exists for flare and roll-out as required, no damage or loss of occupants. Hover landings should still be possible with careful modulation of thrust via aircrew action	Major
		ESC Failed Low: Not OEI Avoid region	Effective loss of torque output from one motor. Pilot detects failure and compensates. ROL required.	Minor
		ESC Failed Low: OEI Avoid region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
Transmit Adequate Power to Rotors	Single gearbox fail	All	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications). Loss of ability to spin rotor associated with that gearbox. Pilot compensation possible via directional control. Safe flight to ROL possible. Air-crew workload impact. Must be within range of suitable landing area.	Major

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
	Dual gearbox fail	Opposite wings	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications. Loss of ability to spin rotor associated with any two gearbox will result in loss of sufficient power for airplane mode level flight. Pilot compensation possible via directional control. Safe flight to ROL possible, but will require adequate Aircrew workload impact. Possible loss of air vehicle and occupants.	Catastrophic
		Same Wings	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications. Loss of ability to spin rotor associated with two gearbox on the same wing will result in loss of sufficient power for airplane mode level flight. If is also assumed to result in loss of flight path control due to excessive yaw. Pilot compensation not possible via directional control. Loss of air vehicle and occupants.	Catastrophic

A.2 Tilt-Wing FMECA

Table 4: Tilt-Wing FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide HVDC power to propulsion system and batteries	Engine, gearbox, AC Generator, AC/DC Converter	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	I	3.33×10^{-4}	1.98×10^{-4}
2	Provide battery storage of electrical energy	Battery Failure	Aircraft fire damages critical systems, causing loss of aircraft	I	1.00×10^{-6}	1.00×10^{-9}
3	Convert HVDC Electrical energy to shaft torque	Electronic Speed Controllers, Electric Motors,	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	I	1.45×10^{-3}	2.90×10^{-4}
4	Provide torque to prop-rotors	Prop--rotor gearboxes, clutches, and shafts	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	I	2.00×10^{-5}	4.00×10^{-6}
5	Provide system cooling for batteries	Battery cooling system	Aircraft fire, loss of controlled flight	I	5.22×10^{-4}	1.72×10^{-7}
				Severity Code I Summary:		**4.92×10^{-4}**

A.3 Tilt-Wing FTA