Limitations of Commercial Aviation Safety Assessment Standards Uncovered in the Wake of the Boeing 737 MAX Accidents

by

Rodrigo Lopes Rose

B.S. Aerospace Engineering
Georgia Institute of Technology, 2022

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN AERONAUTICS AND ASTRONAUTICS

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2024

©2024 Rodrigo Lopes Rose. All rights reserved.

The author hereby grants to MIT a nonexclusive, worldwide, irrevocable, royalty-free license to exercise any and all rights under copyright, including to reproduce, preserve, distribute and publicly display copies of the thesis, or release the thesis under an open-access license.

Authored by: Rodrigo Lopes Rose
Department of Aeronautics and Astronautics
May 8, 2024

Certified by: Nancy G. Leveson
Department of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Jonathan P. How
Department of Aeronautics and Astronautics
Chair, Graduate Program Committee

Limitations of Commercial Aviation Safety Assessment Standards Uncovered in the Wake of the Boeing 737 MAX Accidents

by

Rodrigo Lopes Rose

Submitted to the Department of Aeronautics and Astronautics
on May 8, 2024 in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Aeronautics and Astronautics

ABSTRACT

Commercial aviation accidents, though exceedingly rare, come at a large human, economic, and social cost. Therefore, different stakeholders in industry and government have collaborated to develop standard processes for developing aircraft and assessing their safety, the most popular being the Society of Automotive Engineers' (SAE) Aerospace Recommended Practices (ARPs) 4754 and 4761. However, most of the engineering techniques used for aircraft development and safety assessment were developed in the mid-20th century and formalized into these standards in the 1990s. Modern aircraft often involve complex interactions between hardware, software, and humans, and the engineering techniques used to analyze these systems have not kept up with the pace of technological development.

This thesis studies two recent accidents involving the Boeing 737 MAX (Lion Air flight JT610 and Ethiopian Airlines flight ET302) to identify the limitations that still exist in aviation safety assessment guidance that have contributed to these accidents. A new accident analysis methodology called Causal Analysis based on Systems Theory (CAST) was applied to the 737 MAX accidents to understand why the complex interactions leading to the accidents were not identified during the safety assessment process. The analysis uncovered four main limitations in safety assessment guidance that contributed to the accidents: (a) limited integration of human factors and safety, (b) limited guidance for identifying assumptions, (c) limited ability to capture non-failure based causal scenarios, and (d) limited ability to understand complex nonlinear causal relationships.

A new hazard analysis tool called System-Theoretic Process Analysis (STPA) was then applied to the same systems involved in the 737 MAX accidents to evaluate whether STPA can be used to address the identified limitations. STPA's scenario-based framework that incorporates humans and software into the hazard analysis was found to support validation of human response assumptions, identification of new assumptions, assessing safety of intended behavior, and understanding circular causality or otherwise non-linear causal factors.

Thesis supervisor: Nancy G. Leveson
Title: Professor of Aeronautics and Astronautics

"To think is to *forget* the differences, to generalize, to abstract."

– Jorge Luis Borges
Funes the Memorious, 1942

Acknowledgments

All that I have accomplished in the two years I have spent at MIT is thanks to the support of the wonderful people around me. Here, I would like to express my gratitude to them.

First and foremost, I have to thank my advisor, Professor Nancy Leveson, for all the guidance and support she has given me over the past two years. Nancy, I am sure you hear this from everyone, but your way of looking at the world is fascinating, and has changed how I think, problem solve, and communicate. I am incredibly grateful to have had the opportunity to learn it directly from you.

I also have to thank Dr. John Thomas, whose ability to see the big picture (while not missing the delicate subtleties) in the most complex and gnarly problems inspires me. John, thank you for the hours you have spent reviewing my work and mentoring me. Your pertinent and pragmatic advice has made me a better thinker and communicator.

To my friends Polly Harrington and Brittany Bishop, who joined the group at the same time I did, thank you for the many conversations, brainstorming meetings, writing sessions, and fun shenanigans that got me through this degree.

To the rest of the folks in our research group, thank you for letting me learn about the great work you are all doing, and for taking some time to learn about my work as well. Special thanks go to Andrew Kopeikin, Justin Poh, and Alex Hillman, who helped review this thesis, but also to Michael Schmid, John Barstow, Noam Eisen, Natalie Basnight, and Elizabeth Baker for the great conversations we have had. I also have to thank the rest of the team at the Engineering Systems Laboratory, as well as all my friends from other labs, who have each contributed in their own way to my time here.

There are also a few people I need to thank for their vital support in completing this thesis. The first is Isabel de Luis, who spent a summer with us at MIT and made valuable contributions to this work after only a few days of exposure to our tools and methods. The other is Dr. Laurence Mutuel, who gave her time to reviewing this work and providing feedback.

Next, I would like to thank those that made my studies at MIT possible. Thank you to the team at the U.S. Food and Drug Administration who funded me through my graduate degree, and who gave me the opportunity to explore a field I had I little experience in. To the team from Synensys, Dr. Steve Powell and Alana Keller, working with you has been a delight and I hope we get to collaborate again in the future.

Finally, I am eternally grateful to all those who supported me from afar in this journey. To my parents, Luiz Augusto and Christiane; my grandmother, Marília; my girlfriend, Erin; and all the aunts, uncles, cousins, and friends who were cheering me on from around the world, thank you. My love and gratitude for all of you is immeasurable.

Table of Contents

ABSTRACT *2*

Acknowledgments *4*

List of Figures *6*

List of Tables *7*

Glossary of Acronyms *7*

Chapter 1 Introduction *9*

1.1. Motivation **9**

1.2. Thesis Objective and Approach **9**

Chapter 2 Background *11*

2.1. Airworthiness Requirements **11**

2.1.1. Regulations on Equipment, Systems, and Installations (14 CFR § 25.1309) 11

2.1.2. Regulations on Equipment for Use by the Flight Crew (14 CFR § 25.1302) 12

2.2. Safety Assessment and Development Assurance Standards **12**

2.2.1. ARP4754 12

2.2.2. ARP4761 14

2.2.3. DO-178C 18

2.3. The Systems Theoretic Approach to Safety **19**

2.3.1. Overview of Systems Theory 19

2.3.2. The STAMP Accident Model 21

2.3.3. CAST – Causal Analysis Based on Systems Theory 23

2.3.4. STPA – System Theoretic Process Analysis 24

2.4. The Boeing 737 MAX and MCAS **25**

2.4.1. Functional Overview of MCAS 26

***2.5.* Literature Review on Safety Assessment Standards** **28**

2.5.1. In the Government and Regulatory Community 28

2.5.2. In the Academic Community 30

2.5.3. In the Standards Development Community 31

Chapter 3 Limitations in Current Safety Assessment Standards *32*

3.1. Summary of CAST Results **32**

3.1.1. Basic Information 32

3.1.2. Examination of the Contributions of each Controller in the Loss 34

3.2. Limitations in Safety Assessment Standards **40**

3.2.1. Limited integration of human considerations in the safety assessment process 41

3.2.2. Absence of a systematic methodology that supports the identification of unrecognized assumptions 45

3.2.3. A failure-centric safety assessment process with limited guidance for uncovering and managing non-failure based causal scenarios leading to losses 50

3.2.4. A limited framework for understanding nonlinear causal relationships between functional failure conditions and operational events/conditions 57

Chapter 4 Addressing the Limitations through a System-Theoretic Approach *62*

4.1. Overview of STPA Results **62**

4.1.1. Purpose of the Analysis – System Boundary, Losses, Hazards, and Safety Constraints 62

4.1.2. Control Structures 63
4.1.3. Overview of UCAs and Scenarios 65
4.2. Integration of Human Considerations 68
4.2.1. Inadequate Mental Model Updates 69
4.2.2. Flawed Mental Models of Automation 71
4.2.3. Flawed Human Decision-Making Algorithm 72
4.2.4. Human Error beyond Response to Failures 73
4.3. Support in Identifying Unrecognized Assumptions 74
4.4. Uncovering Non-failure Based Scenarios 77
4.4.1. Causal Scenarios from Non-Developmental Factors 78
4.4.2. Causal Scenarios from Component Interactions 80
4.4.3. Causal Scenarios from Combinations of Failures and Intended Behavior 81
4.5. Identification of Complex Nonlinear Causal Pathways 83
Chapter 5 Conclusion 86
5.1. Summary of Contributions 86
5.2. Limitations and Future Work 87
References 88
Appendix A – 737 MAX Accidents CAST 93
Appendix B – MCAS STPA 120

List of Figures

Figure 1. ARP4754 Aircraft / System Development Process
Figure 2. ARP4761 safety assessment process and its interactions with ARP4754
Figure 3. Different types of systems
Figure 4. Basic feedback control loop
Figure 5. Example hierarchical control structure
Figure 6. Five steps of CAST
Figure 7. Four steps of STPA
Figure 8. Normal MCAS behavior without flight crew input
Figure 9. MCAS behavior with flight crew input
Figure 10. First page of the runaway stabilizer procedure from the 737 MAX QRH in use at the time of the JT610 accident
Figure 11. First two pages of the airspeed unreliable procedure from the 737 MAX Quick Reference Handbook in use at the time of the JT610 accident
Figure 12. Partial 737 MAX fault tree for "Autoflight malfunction at low altitude which results in an unsafe flight path in an autopilot OFF, single channel or fail passive configuration"
Figure 13. Partial 737 MAX fault tree for "Misleading Air Data from the Left and Right ADIRU – Airspeed / Altitude"
Figure 14. Simplified representation of different flight envelopes according to AC 25-7C.

Figure 15. Venn diagram representation of erroneous MCAS activation in different flight envelopes
Figure 16. High level MCAS control structure
Figure 17. Detailed MCAS control structure
Figure 18. Visualization of FC-Scen-1.1
Figure 19. Visualization of FC-Scen-1.2
Figure 20. Visualization of FC-Scen-1.3
Figure 21. Visualization of FC-Scen-6.3
Figure 22. Visualization of MCAS-Scen-2.4
Figure 23. Visualization of MCAS-Scen-4.3
Figure 24. Visualization of MCAS-Scen-9.2
Figure 25. Visualization of MCAS-Scen-3.3

List of Tables

Table I. Excerpt from an AFHA Table
Table II. Condensed Sequence of Events for JT610 and ET302
Table III. Flight Crew Contributions from JT610 CAST
Table IV. Flight Crew Contributions from ET302 CAST
Table V. Aircraft Manufacturer Contributions from JT610 CAST
Table VI. Aircraft Manufacturer Contributions from ET302 CAST
Table VII. Functional Hazard Assessment for MCAS
Table VIII. Probabilities of Occurrence for each Flight Envelope According to FAA AC 25-7C
Table IX. Unsafe Control Actions for MCAS
Table X. Unsafe Control Actions for Flight Crew

Glossary of Acronyms

AAIB	Ethiopian Aircraft Accident Investigation Bureau
AC	Advisory Circular
ADIRU	Air Data Inertial Reference Unit
AFHA	Aircraft Functional Hazard Assessment
AIR	Aerospace Information Report
AOA	Angle of Attack
ARP	Aerospace Recommended Practice
ASA	Aircraft Safety Assessment
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
CAST	Causal Analysis based on Systems Theory
CEA	Cascading Effects Analysis

CFR	Code of Federal Regulations
CMA	Common Mode Analysis
DAL	Development Assurance Level
DO	Document
FAA	Federal Aviation Administration
FCC	Flight Control Computer
FCOM	Flight Crew Operating Manual
FCTM	Flight Crew Training Manual
FHA	Functional Hazard Assessment
FO	First Officer
FTA	Fault Tree Analysis
FDAL	Functional Development Assurance Level
FMEA	Failure Modes and Effects Analysis
IAS	Indicated Air Speed
IDAL	Item Development Assurance Level
JATR	Joint Authorities Technical Review
KNKT	Indonesian National Transportation Safety Committee
MCAS	Maneuvering Characteristics Augmentation System
MF&MS	Multi-function & Multi-system Analysis
ND	Nose Down
NTSB	National Transportation Safety Board
NU	Nose Up
ODA	Organization Designation Authorization
OEM	Original Equipment Manufacturer
PASA	Preliminary Aircraft Safety Assessment
PFD	Primary Flight Display
PSSA	Preliminary System Safety Assessment
QRH	Quick Reference Handbook
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SD	System Dynamics
SFHA	System Functional Hazard Assessment
SSA	System Safety Assessment
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
STS	Speed Trim System
UCA	Unsafe Control Action

Chapter 1

Introduction

1.1. Motivation

The success of the commercial aviation industry is intrinsically linked with its ability to remain safe and be perceived as such by the general population. Commercial aviation accidents, though exceedingly rare, come at a large human, economic, and social cost, and an accident involving one aircraft or airline can have ripple effects that hurt the entire industry. As a result, ensuring all potential sources of accidents are identified and mitigated before commercial aircraft are allowed to enter operation is a priority for aircraft manufacturers, operators, and regulators.

In an effort to improve the safety of commercial aviation, different stakeholders in industry and government have collaborated to develop standard processes for developing aircraft and assessing their safety. These standards, the Society of Automotive Engineers' (SAE) Aerospace Recommended Practices (ARPs) 4754 and 4761, have largely been successful, as shown by the dramatic reduction in hull loss accidents since the early 1990s [1].

However, a majority of the engineering techniques used for aircraft development and safety assessment were developed in the mid-20th century and formalized into standards in the 1990s. New engineering techniques have been created and certification standards are occasionally revised and expanded. However, operating modern aircraft often involves complex interactions between hardware, software, and humans, and the pace of technological change can exceed the rate at which the engineering techniques and standards can adapt.

The few accidents that do occur involving large passenger aircraft reveal what parts of the aviation safety management system are still in need of improvement. The October 2018 loss of Lion Air flight JT610 [2], and the March 2019 loss of Ethiopian Airlines flight ET302 [3], both involving the new Boeing 737 MAX, have highlighted that commercial aircraft are not immune to severe design flaws. Government agencies, academics and the standards community were generally aware of weaknesses in the processes used to assess aircraft safety before the accidents occurred. However, the sudden and severe nature of the crashes, have heightened the impetus for the industry to address these deficiencies before another major accident. Knowing what needs to be changed and what approaches are effective to prevent future aircraft from being certified with significant design flaws requires a systematic evaluation of the limitations of aviation safety assessment standards.

1.2. Thesis Objective and Approach

The objectives of this thesis are twofold. The first objective is to study the Boeing 737 MAX accidents[1] to identify what limitations exist in current aviation safety assessment guidance (ARP4754 and ARP4761) that may have contributed to the accidents. The second objective of this

[1] The expression "737 MAX accidents" is used in this thesis to collectively refer to the crashes of JT610 and ET302.

thesis is to examine if safety assessment methodologies that are based on systems theory can be leveraged to address the identified limitations.

The approach to achieve these objectives begins with a detailed analysis of the 737 MAX accidents using a relatively new accident investigation approach, Causal Analysis based on Systems Theory (CAST). The goal of the CAST is to understand the unsafe decisions made by all stakeholders involved in the accidents, including aircraft operators, maintenance engineers, airline management, aircraft designers, and regulatory authorities, among others. Instead of stopping when the unsafe actions are identified, the CAST identifies the mental model flaws and contextual factors that made each decision-maker's actions appear reasonable to them, even if they were unsafe in hindsight. The limitations in current assurance and certification guidance are identified by examining the mental models of the aircraft designers and safety analysts. This allows for a deeper understanding of why the complex interactions leading to the accidents were not identified during assurance and certification activities.

After identifying the limitations, this study evaluates a new hazard analysis tool based on systems theory, System Theoretic Process Analysis (STPA), and its applicability to the aircraft systems involved in the 737 MAX accidents. The goal here is not to provide a full new framework for assessing the safety of and certifying commercial aircraft. Updating existing guidance and developing new guidance is an effort that should happen in the standards development committees with appropriate representation from industry practitioners and regulators. The goal is instead to identify if there are potential benefits from incorporating the principles of systems theory and its associated tools into the development and safety assessment framework used for aircraft certification. The output of this thesis is thus a set of identified limitations, and an evaluation of how systems theory may help address them[2].

The remainder of this thesis is structured as follows: Chapter 2 provides background information, as well as a literature review of prior work on this subject. Chapter 3 provides an overview of the 737 MAX CAST, and discusses the identified limitations in safety assessment standards. Chapter 4 provides an overview of the STPA conducted, and discusses how the results help address the these limitations. Finally, chapter 5 describes final conclusions and discusses future work.

[2] All of the information used in the CAST and STPA is publicly available and has been sourced from official reports, media publications, and peer-reviewed academic publications.

Chapter 2

Background

This chapter provides the background information necessary to understand the limitations in current commercial aircraft safety assessment standards. Section 2.1 presents an overview of airworthiness regulations applicable to transport category aircraft, and section 2.2 discusses some standards accepted by the FAA as a means of compliance with those regulations. Section 2.3 introduces the System Theoretic Accident Model and Processes (STAMP) causality model and its associated tools for accident analysis and safety assessment. Section 2.4 provides a brief overview of the 737 MAX aircraft systems that were involved in its two major accidents. Finally, section 2.5 presents a review of the literature on safety assessment standards, including previous efforts from the academic, government, and standards development communities to identify and address their limitations.

2.1. Airworthiness Requirements

Title 14 of the Code of Federal Regulations (14 CFR) includes all rules prescribed by the FAA to control aviation activities in the United States. According to 14 CFR, an aircraft receives airworthiness approval if it "conforms to its approved design and is in a condition for safe operation" [14 CFR 21.1(b)(1)], but different categories of aircraft have to adhere to different airworthiness standards. These standards are outlined in different parts of 14 CFR, such as part 23 for general aviation aircraft and part 25 for large commercial "transport category" aircraft. Most other countries use 14 CFR as a basis for their own aviation regulations [4].

2.1.1. Regulations on Equipment, Systems, and Installations (14 CFR § 25.1309)

The regulations meant to control safety of commercial aircraft from a design standpoint fall under 14 CFR § 25.1309, which officially governs an aircraft's equipment, systems, and installations. Complying with § 25.1309 requires demonstrating, among other factors, that an aircraft's systems perform their intended functions under foreseeable operating conditions, that any failure condition that would prevent continued safe flight and landing of the aircraft is extremely improbable, that warning information is provided to alert the flight crew of unsafe operating conditions, and that systems are designed to minimize crew error [14 CFR 25.1309(a)-(c)].

The FAA does not require specific practices to comply with § 25.1309. The only requirement is that compliance be shown "by analysis" or by "ground, flight, or simulator tests." The analysis must consider the possible modes of failure for aircraft systems, the probability of those failures, the resulting effects of those failures, and the capability to detect those failures [14 CFR 25.1309(d)]. However, as guidance for aircraft manufacturers, the FAA does provide advisory circulars (ACs) that outline acceptable means for showing compliance with particular regulatory criteria.

One approved means of compliance for § 25.1309 is AC 25.1309-1, whose last official revision [5] was released in 1988, but whose 2002 ARSENAL draft [6] is considered relatively mature [7].

AC 25.1309-1 provides general guidance for safe aircraft design and recommends particular analytical methods, but does not provide a systematic methodology for aircraft development and safety assessment [8]. Instead, the ARSENAL draft of AC 25.1309-1 references several industry standards that do provide structured processes, such as Aerospace Recommended Practices (ARPs) 4754 and 4761 published by the Society of Automotive Engineers (SAE). These standards are widely used in industry and widely accepted by regulators when evaluating compliance with § 25.1309. These standards are explained in more detail in section 2.2 of this thesis.

2.1.2. Regulations on Equipment for Use by the Flight Crew (14 CFR § 25.1302)

In parallel to § 25.1309, which deals with preventing failures of physical systems, 14 CFR § 25.1302 establishes rules for the design of equipment that the flight crew interacts with. § 25.1302 aims to ensure that the aircraft's systems will not prevent the crew from safely performing all of their necessary tasks. Among other factors, complying with § 25.1302 requires demonstrating that the flight crew will be able to perform all of their tasks using the flight deck controls available, that any information the flight crew needs to use is available and unambiguous, that aircraft systems behave in a predictable manner, and that the systems enable the crew to manage any errors they make [14 CFR 25.1302(a)-(d)].

An approved means of compliance for § 25.1302 is AC 25.1302-1, first released in 2013 [9]. AC 25.1302-1 also serves as a means of compliance for several other certification requirements involving equipment that is used by the flight crew, including § 25.1309 (c), which requires that systems be designed to minimize crew error [14 CFR 25.1309(c)][3]. Though certain sections of AC 25.1302-1 reference requirements from § 25.1309, the processes for system design and prevention of flight crew error in AC 25.1302-1 are not explicitly integrated or linked with the processes for safety assessment in AC 25.1309-1 or any of its referenced standards. This omission limits the power of the certification procedures to prevent accidents involving human interactions, as will be discussed later in this thesis.

2.2. Safety Assessment and Development Assurance Standards

The ARSENAL draft of AC 25.1309-1 references several industry standards that provide structured processes for complying with certification regulation. They are briefly outlined in this subsection.

2.2.1. ARP4754

ARP4754, titled "Guidelines for Development of Civil Aircraft and Systems" [10], provides best practices for developing aircraft that are comprised of multiple subsystems with many dependencies and interactions. Figure 1, taken directly from ARP4754B, provides a general overview of the standard's aircraft and system development process.

---

[3] AC 25.1302-1 primarily deals with ensuring that human error is mitigated through system design, as design is typically seen as the most effective solution to preventing human error, but the AC also recognizes that other aspects outside of § 25.1302, (e.g., licensing and qualification of flight crews, or aircraft operational procedures) may also help mitigate errors. One goal of AC 25.1302-1 is to effectively harmonize the aircraft and system design requirements needed for § 25.1302 compliance with flight crew training, licensing, and procedures.

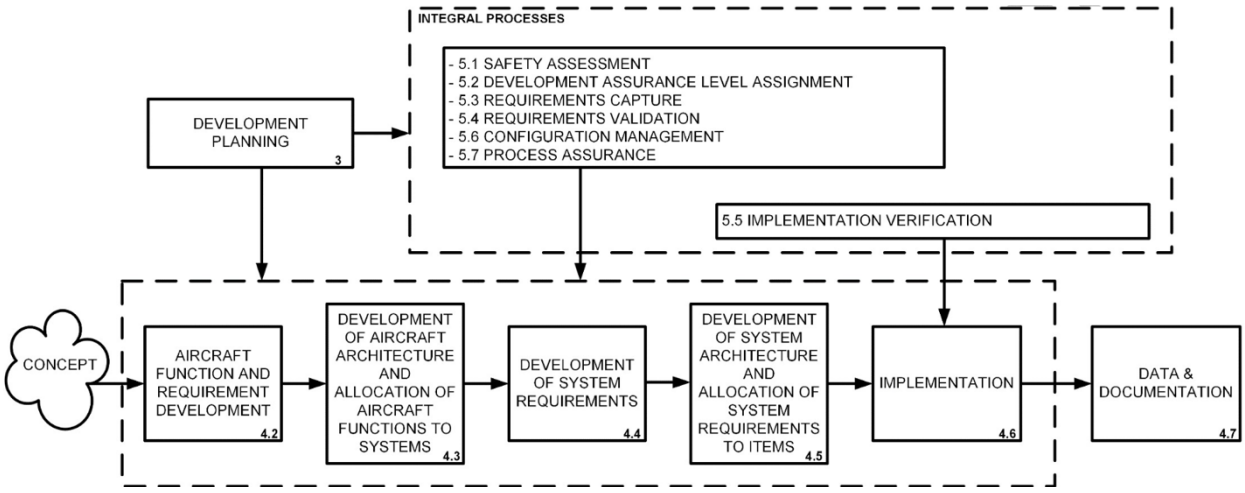


Figure 1. ARP4754 Aircraft / System Development Process (taken directly from [10])

2.2.1.1. Development Planning

ARP4754 begins with the development planning process (labeled 3 in Figure 1). Development planning involves defining the means through which an original equipment manufacturer (OEM) will develop their aircraft or system to ensure that all requirements are met and the necessary level of confidence is achieved to receive certification. This process includes, among other steps, establishing the design process itself, establishing the scope of safety activities, and establishing processes for requirements capture, validation, and verification.

2.2.1.2. Development Process

ARP4754 then provides a generic approach for developing aircraft and aircraft systems, starting at the conceptual stage and ending at certification activities (labeled 4.2 – 4.7 in Figure 1). The first step involves defining the aircraft's high-level functions (e.g., decelerate on ground) and their associated requirements (e.g., "The airplane shall have a means to decelerate on ground"). The next step involves establishing a physical aircraft architecture, grouping aircraft-level functions, and allocating these functions to systems. For example, the "decelerate on ground" function can be allocated to wheel brakes, thrust reversers, spoilers, etc.

The process is then repeated at the aircraft system level, where system functions are defined (e.g., the wheel brake system's function is defined as decelerating the wheels on the ground) and system requirements are generated (e.g., "The wheel brake system shall have a means to decelerate the wheels on the ground"). The system architecture is then defined and system functions are allocated to individual items (components).

Once a system architecture has been developed, with requirements allocated to items, the implementation step involves designing and building items, integrating these items into subsystems, and integrating subsystems into the entire aircraft. ARP4754 allocates requirements to hardware and software items, but does not provide detailed guidance for designing items. ARP4754 instead references additional standards, such as the Radio Technical Commission for Aeronautics' (RTCA) Document 178C (DO-178C) for airborne software [11], and Document 254 (DO-254) for airborne electronic hardware [12].

2.2.1.3. Integral Processes

Additionally, there are a number of "integral processes" (labeled 5.1 – 5.7 in Figure 1) that closely interact with the development process. Detailed guidance on these integral processes is either included directly in ARP4754 or provided in other referenced standards. One such process, the safety assessment process, is briefly described in ARP4754, and expanded upon in ARP4761, which is discussed next. The safety assessment process interacts with every step of the system development process described above.

Another integral process to ARP4754 is the assignment of development assurance levels (DALs). ARP4754 acknowledges that because modern aircraft are highly complex and integrated, errors in the aircraft's requirements, design, or implementation may arise and have catastrophic consequences. ARP4754 defines these kinds of errors as "development errors". The approach to preventing requirements, design, or implementation errors is based on establishing confidence that aircraft and system development was accomplished in a sufficiently disciplined or rigorous manner.

In ARP4754, DALs are divided into functional development assurance levels (FDALs) and item development assurance levels (IDALs). FDALs and IDALs range from A (high rigor) to E (low rigor). Assigning a higher FDAL or IDAL to a function or item indicates that more rigor was applied to the development process for that function or item. The development process objectives that must be met for each FDAL are outlined in ARP4754. For example, a function assigned FDAL A, B, or C needs to have traceability of its requirements to specific rationales, while that is negotiable for FDAL D and not required for FDAL E. The process objectives for IDALs are outlined in DO-178C for software items and DO-254 for hardware items. An assumption is made that software/systems developed with a higher DAL are less likely to have design errors.

Additional integral processes that ARP4754 also covers include requirements capture, requirements verification and validation (V&V), documentation and validation of assumptions, configuration management, and modification analysis.

2.2.2. ARP4761

The safety assessment process briefly described in ARP4754 is explained more thoroughly in a different standard, ARP4761, titled "Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment" [13]. The ARP4761 safety assessment process is composed of multiple steps, each of which feed directly into the ARP4754 development process. Figure 2, taken directly from ARP4761A, depicts the steps of the safety assessment process and its interaction with ARP4754.

ARP4761 uses the words "aircraft-level", "system-level", and "item-level" to refer to different levels of granularity in the safety assessment. The aircraft represents the entire vehicle being developed, while a system is "any combination of subsystems, equipment, or items that perform one or more specific functions" [13]. The aircraft is composed of multiple systems. An item is a set of one or more hardware or software elements treated as a single entity for analytical purposes. Systems are composed of multiple items. For ease of understanding, this section will use terminology consistent with ARP4761.

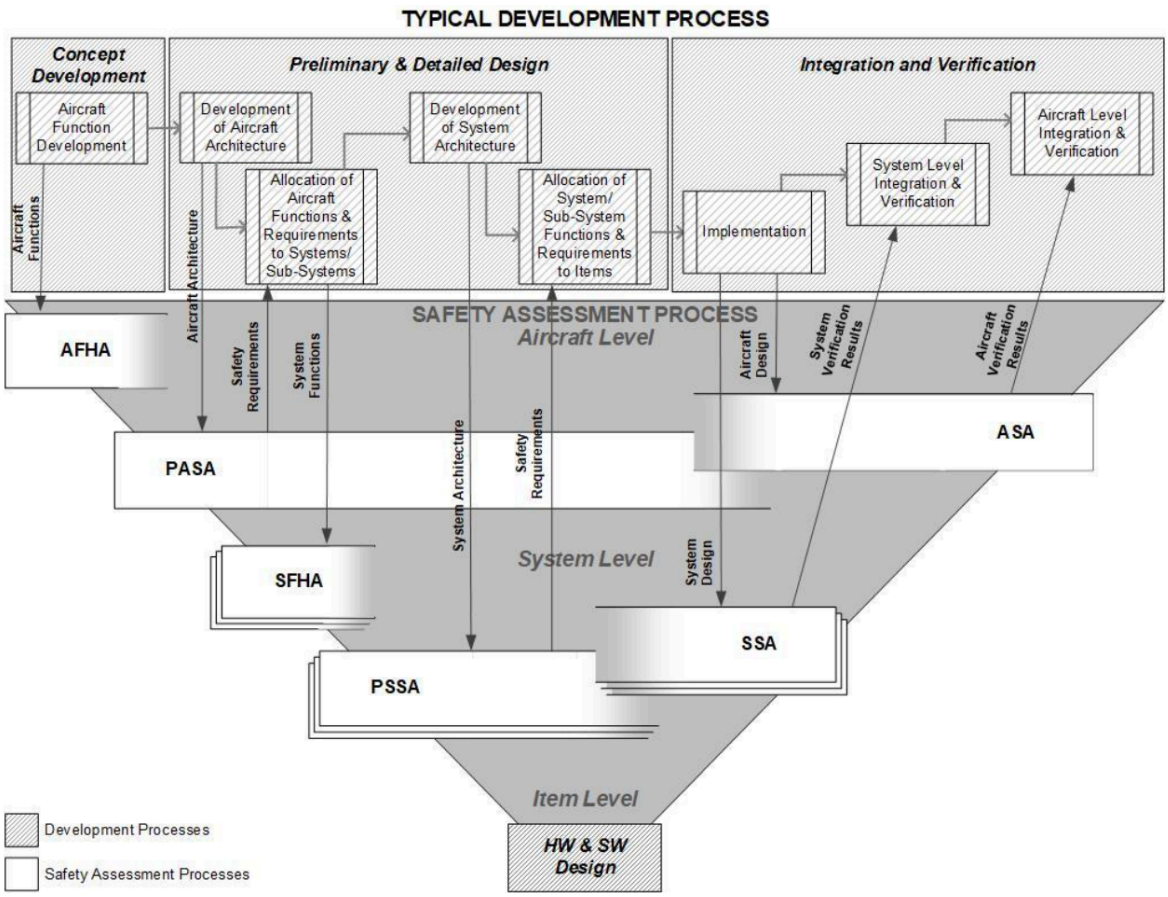


Figure 2. ARP4761 safety assessment process and its interactions with ARP4754 (taken directly from [13])

2.2.2.1. Aircraft Functional Hazard Assessment (AFHA)

The first step in the safety assessment process is the AFHA. The AFHA identifies and classifies the failure conditions associated with the aircraft level functions documented by the ARP4754 process. ARP4761 defines a failure as an "occurrence which affects the operation of an aircraft, system, equipment, item, or piece-part such that it can no longer function as intended" [13], and a failure condition as a "condition having an effect on the aircraft and/or its occupants … caused or contributed to by one or more failures or errors" [13]. ARP4761 defines three types of failure conditions: the total loss of a function, the partial loss of a function, and a malfunction. For the "decelerate on ground" function, the loss of that function means being unable to decelerate on the ground, while a potential malfunction could be an uncommanded deceleration on the ground.

The AFHA considers both single failures and combinations of failures. It also considers failures occurring at different phases of flight, in different operational conditions, or with different levels of awareness by the flight crew. By considering the effects of the failure condition on the aircraft and its occupants, the AFHA analyst then assigns a severity classification to the failure condition, which ranges from "no safety effect" to "minor", "major", "hazardous", and "catastrophic". The severity of the failure condition determines the safety requirement that the aircraft must meet, and the FDAL associated with that aircraft-level function. For example, a

failure condition deemed catastrophic results in the assignment of FDAL A to its associated function. A catastrophic failure condition also comes with the requirement that the probability of that failure condition be on the order of 10^{-9} per flight hour[4], according to AC 25.1309 [6].

Each row of an AFHA table represents a different failure condition, with the columns indicating the function being analyzed, the failure condition itself, the phase of flight in which the failure condition occurs, the effects of the failure condition on the aircraft and its occupants, the severity classification of the failure condition, and any assumptions or observations about the failure condition. Table I below provides an excerpt from an example AFHA table in ARP4761:

Table I. Excerpt from an AFHA Table (adapted from [13])

Function	**Failure Condition**	**Flight Phase**	**Effects**	**Classification**	**References/ Notes**
Decelerate on ground	Loss of ability to decelerate with crew aware	Landing	**Aircraft:** Severe reduction in deceleration capability. Unable to decelerate airplane using airplane manual guidelines within the destination runway. Runway overrun above "XYZ" knots. Potential hull loss. **Flight crew:** Though aware of the condition, crew will already be committed to the landing. Excessive crew workload to attempt to avoid obstacle collision during the high speed overrun. …	Catastrophic	**Assumption:** Overrunning the runway length above "XYZ" knots is considered a high speed overrun. …
…	…	…	…	…	…

2.2.2.2. Preliminary Aircraft Safety Assessment (PASA)

The next step of the safety assessment process is the PASA, which is a systematic evaluation of the aircraft architecture generated by the development process. The PASA takes as inputs the list of aircraft-level functions and their failure conditions from the AFHA, any requirements identified during the development process, any operational considerations like training procedures, and the proposed aircraft architecture. The PASA uses these artifacts to identify specific safety

[4] The probability requirements for other severity classes are: 10^{-7} for a hazardous failure condition, 10^{-5} for a major failure condition, and 10^{-3} for a minor failure condition

requirements for the development of each system (e.g., architectural design constraints, interface requirements, etc.)

The PASA includes an interdependence analysis where each AFHA failure condition is examined to determine what system functions can contribute to that failure condition. The PASA also includes a Multifunction and Multisystem (MF&MS) analysis that considers how failures of individual systems combine to cause an aircraft level failure condition. The PASA is also where FDALs are assigned to different functions based on the severity classifications of AFHA failure conditions.

Finally, PASA also includes a number of analyses that support the MF&MS analysis and FDAL assignment. These supporting analyses include the Combined Functional Failure Effects Analysis that considers the effects of multiple failures at the same time, the Common Cause Analyses that consider independence between functions, and the Cascading Effects Analysis that considers indirect effects resulting from failure conditions.

2.2.2.3. System Functional Hazard Assessment (SFHA)

The next step in ARP4761, the SFHA, is analogous to the AFHA but occurs at the system level, rather than at the aircraft level. After aircraft functions are allocated to systems during the development process, each system is examined in the SFHA to identify failure conditions, their effects, and their severity. The SFHA also considers both single failures and combinations of failures. If failures at the system level can affect aircraft-level functions, the SFHA can be used to update the AFHA as well. The SFHA table looks similar to the AFHA table, and its outputs are used to inform the Preliminary System Safety Assessment (PSSA) in the same way that AFHA outputs inform the PASA.

2.2.2.4. Preliminary System Safety Assessment (PSSA)

The PSSA is a systematic evaluation of a proposed system architecture to determine how one or more failures can lead to the failure conditions identified by the SFHA. The PSSA is analogous to the PASA but occurs at the system level. One of the goals of the PSSA is to determine if the proposed architecture can reasonably be expected to meet the safety objectives identified in previous steps of the safety assessment process like the SFHA and PASA.

In the PSSA, system-level functions and items are assigned FDALs and IDALs respectively based on the severity of their associated failure conditions. The design of the system is then evaluated against the safety requirements to show how physical failures in the system can contribute to the system-level failure conditions. This evaluation typically consists of the construction of a failure model through a number of methods, including dependence diagrams, Markov analysis, model based safety analysis, and fault tree analysis (FTA), which is the most commonly used approach [13].

In FTA, the analyst begins with an undesired top-level event (typically an aircraft or system-level failure condition from the AFHA/SFHA) and systematically determines how any single failure or combination of failures can cause this event. Once the events that can directly cause the top-level event are identified, the fault tree gets progressively more granular to identify the causes of each of those lower-level events. Within the larger ARP4761 process, FTA is most commonly used to evaluate the ability of a system to meet its safety objectives and requirements. These requirements are typically probabilistic and stem from the AFHA/SFHA severity classification

(e.g., "the probability of loss of the ability to decelerate on ground shall not exceed 10^{-9} per flight"), so FTA uses logical operators to combine failure probabilities and determine whether each requirement is met. For more details on FTA, see Appendix G of ARP4761A [13].

The outputs of the PSSA are new proposed safety requirements and assumptions, as well as the evaluation results that provide a rationale for why the chosen architecture meets all safety requirements. The PSSA is an iterative process meant to occur at multiple stages of the development cycle.

2.2.2.5. System Safety Assessment (SSA)

The SSA is a comprehensive and systematic evaluation of implemented aircraft systems to show that the safety requirements generated in previous steps have truly been satisfied by each system. While the PSSA evaluates the proposed architecture for a system and derives new safety requirements, the SSA evaluates the actual implemented system to verify that it meets the safety objectives.

The SSA confirms that the safety requirements derived in the PSSA have been met by verifying independence requirements through Common Mode Analysis and by verifying quantitative requirements through FTA. The SSA also confirms that the probabilistic safety objectives for each failure condition have been satisfied by considering the implementation of functions associated with that failure condition, the design features that mitigate the condition, the features to alert the crew of the condition, and any crew or maintenance actions needed to prevent the condition.

2.2.2.6. Aircraft Safety Assessment (ASA)

The final step of the safety assessment process is the ASA, which comprehensively evaluates the aircraft implementation to show that the AFHA failure conditions and their associated requirements have been addressed. The ASA uses the results from the PASA and each system's SSA to understand whether the aircraft-level failure conditions have truly been mitigated by the implementation. The ASA also places particular focus on ensuring that the interdependencies between aircraft systems and functions in the actual implementation match the analyst's understanding of them.

Another important element of the ASA is ensuring that each step of the safety assessment process has been completed appropriately. The ASA is meant to confirm that all safety assumptions are validated, all prior analyses processes are complete, and all verification activities are complete, among others.

2.2.3. DO-178C

DO-178C, titled "Software Considerations in Airborne Systems and Equipment Certification" [11] is the most commonly used standard for certifying commercial aviation software. DO-178C is recognized by the FAA's AC 20-115D [14] as an acceptable means of complying with airworthiness regulations. The philosophy of DO-178C is that the chance of software errors occurring can be minimized by enhancing the quality or rigor of the software development process [15].

DO-178C begins by discussing how the software development process is integrated with the system development and system safety assessment processes. The standard discusses the allocation

of system-level requirements to software components, and the assignment of DALs to software components. Similar to FDALs and IDALs in ARP4754, assigning a higher DO-178C software DAL indicates that that component can contribute to a higher severity event, and therefore more rigor should be applied to the development process for that component. Annex A of DO-178C provides the objectives that need to be met for each software DAL.

DO-178C then provides guidance on the software life cycle, which includes defining and executing a software development plan. The software development process includes planning and development of software requirements, transformation of the software requirements into code, and and deployment and maintenance of the software [11,15].

Finally, the standard provides guidance on several integral processes that support the software development life cycle, like software verification, configuration management, and quality assurance. The software verification stage, aimed at showing the correctness of the software, requires the analyst to ensure that the software requirements are correct, complete, consistent, and the architecture actually meets the requirements.

2.3. The Systems Theoretic Approach to Safety

Engineers use models to explain why accidents occur and what can be done to prevent them. ARP4754 and ARP4761 do not reference specific accident models. However, the methods they employ are founded on a traditional approach that assumes accidents result from component failures and can be prevented by decomposing systems into component parts or functions and examining them separately. Systems theory provides a different theoretical underpinning for safety, and a number of new safety analysis and design approaches are based on it.

2.3.1. Overview of Systems Theory

Systems theory has its origins in the early to mid-20th century, with the increased need to manage the complexity of technical systems being built at the time. The traditional approach of decomposing systems into component parts, termed *analytic reduction*, was found to be insufficient in explaining the behavior of complex natural and engineered systems [16].

Analytic reduction assumes that each component of a system operates independently, and that their behavior on their own is the same as their behavior as part of a collective system. Analytic reduction also assumes that the interactions between components are simple enough that they can be analyzed pairwise, and separately from the general behavior of each component. There are systems that fit these characteristics, and they have been described by system theorists as having "organized simplicity" [17].

Some other systems are not suitable for analytic reduction because they lack the underlying organization to be decomposed. Systems like weather, that are highly complex but display a degree of regularity and randomness, can be analyzed using statistical methods. Systems theorists describe these systems as having "unorganized complexity" [17].

A third category is systems that are complex enough that they cannot be fully decomposed without losing information about their behavior, but have enough structure that this behavior is not fully random. These systems exhibit "organized complexity" [17]. Examples of systems with organized complexity include biological systems and software-intensive engineered systems like modern commercial aircraft. Systems theory was designed to facilitate analysis of these types of systems. Figure 3 notionally depicts the three types of systems.

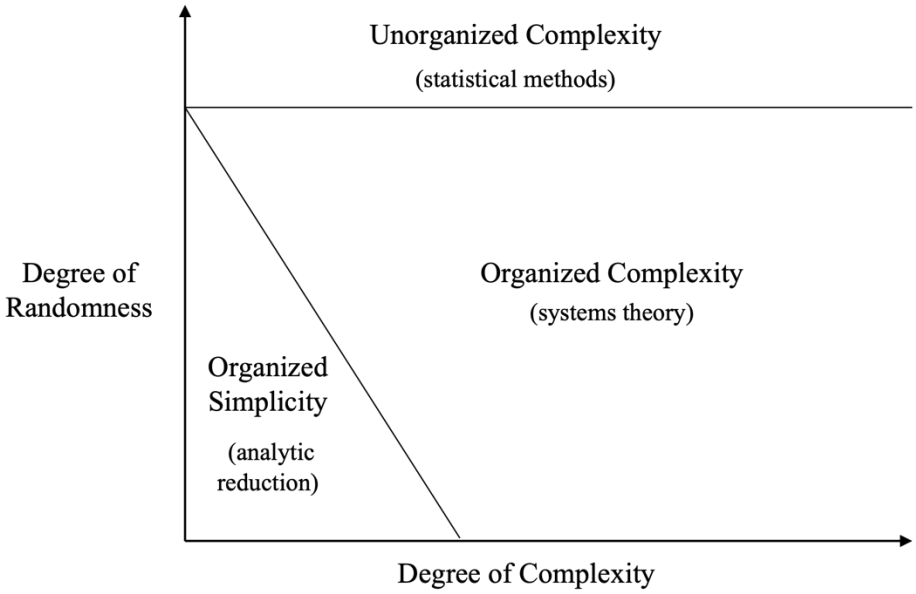


Figure 3. Different types of systems (adapted from [16], originally from [17])

According to systems theory, a key feature of complex systems is *emergence*. Certain properties of a system exist as a result of interactions between its components (and with the environment), meaning they only exist when the system is observed as a whole. For example, it does not make sense to speak of traffic congestion at the level of an individual car, as that property only emerges from the interactions between many cars and their surrounding environment.

Another key tenet of systems theory is *hierarchy*. Managing properties that emerge from interactions between system components requires the ability to enforce constraints on those components' behavior. In the traffic example, the emergent property of congestion can be managed by imposing constraints on cars, such as limiting how many cars can drive in certain areas or during specified times. The higher level in the hierarchy (e.g., city management) can be seen as a *controller* that enforces controls over a *controlled process* at the lower level (e.g., cars).

Controlling the behavior of a system requires several conditions. First, the controller must have a goal it is trying to achieve, like maintaining the altitude of an aircraft. It must also have controls available that can affect the state of the system, like being able to pitch the aircraft up and down. In order to decide when and how to enforce a control, the controller must also have a model of the system, and that model must be informed by *feedback* about the current state of the system.

In engineering, this concept of a controller enforcing controls on a process while being informed by feedback is commonly represented as a *feedback-control loop*, as shown in Figure 4. The feedback control loop is the main systems-theoretic model used for engineering activities.

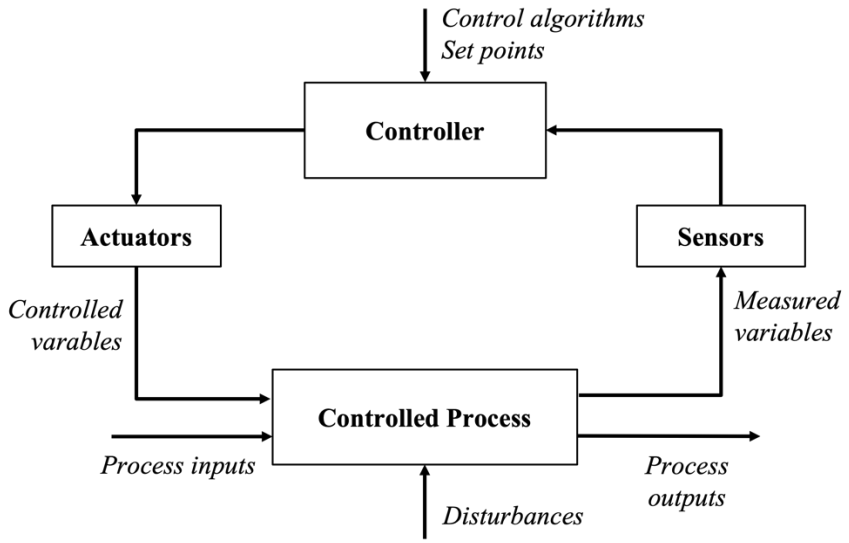


Figure 4. Basic feedback control loop (taken directly from [16])

2.3.2. The STAMP Accident Model

The System Theoretic Accident Model and Processes (STAMP) is a model of accident causality based on systems theory. STAMP was developed to address limitations in traditional accident models, which struggle to fully capture the causes of accidents involving complex systems with interactions between physical components, software, and humans.

Traditional models view accidents as linear chains of events, where an initiating event triggers the next event, which in turn triggers the next, and so on until the accident occurs. Traditional models also often treat accidents as the result of component failure, where a component not performing as designed creates a hazardous system state.

STAMP, on the other hand, views safety as an emergent property of complex systems. In STAMP, it does not make sense to discuss the safety of a single hardware component like a nut or bolt, nor does it make sense to discuss the safety of a single software module. Safety (or lack of safety) emerges from the interactions between the hardware, software, and human components of a system.

Thus, STAMP treats safety as a control problem. Accidents are viewed as loss events resulting from controllers not enforcing appropriate constraints on system behavior, including both individual component behavior and component interactions. Safety constraints can include physical controls like closing a valve, but they can also include organizational constraints like procedures and training. Knowing when and how to enforce these constraints requires appropriate feedback, as indicated in the control loop from Figure 4.

A single control loop is typically not sufficient to provide a detailed understanding of all the interactions in a complex system. Instead, STAMP combines control loops with the concept of hierarchy and models systems as *hierarchical control structures*. A control structure is a set of multiple interconnected control loops, where controllers above typically have control over those below. Like any model, a control structure is an abstraction that only represents the information that is necessary and useful for the safety analysis being done. If necessary, multiple control structures for the same system can be built at different levels of abstraction, to analyze different

system characteristics. Figure 5 shows an example hierarchical control structure in commercial aviation.

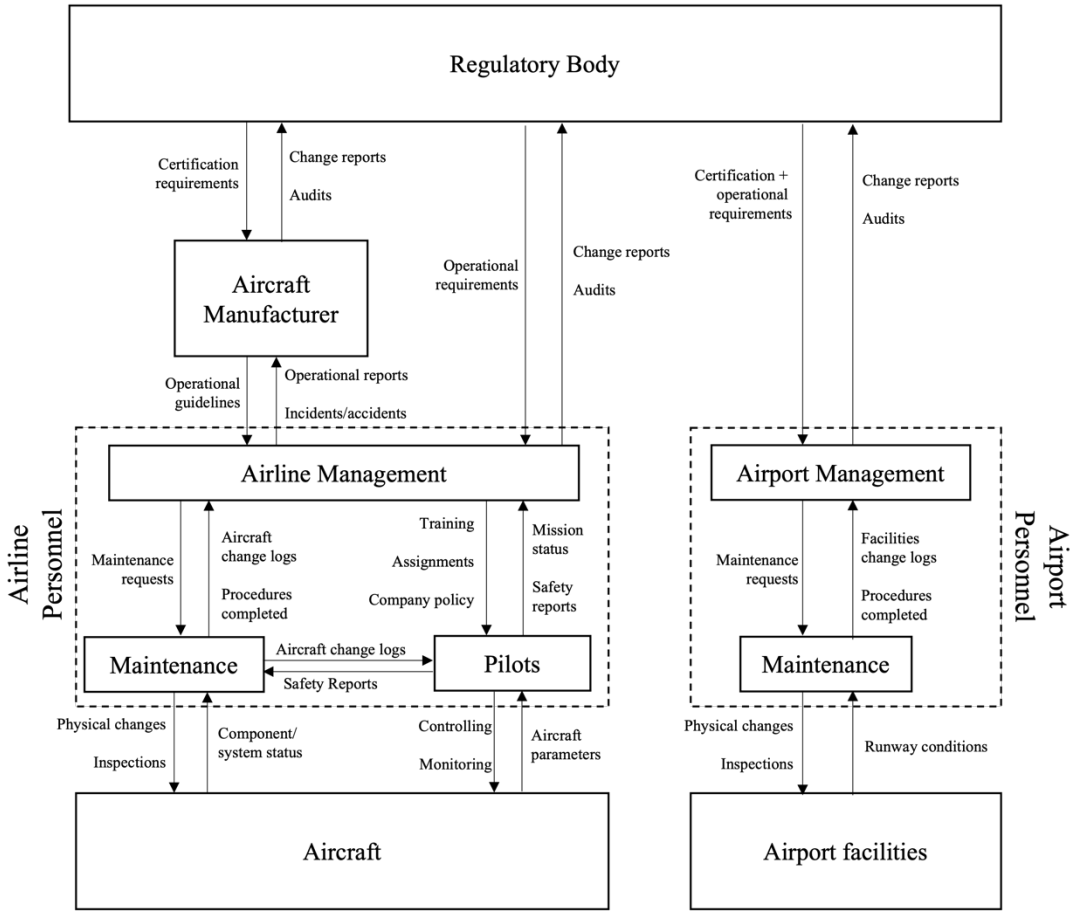


Figure 5. Example hierarchical control structure

Another important concept in STAMP is the *process model*. A process model is a controller's understanding of the system they are managing, of other controllers, and of the environment around them. For human controllers, process models are often called *mental models*. For automated controllers, a process model may be the set of variables the software uses to monitor the state of the system. Every controller uses their process model to make decisions about what actions they should take.

STAMP recognizes that inaccurate, outdated, or conflicting process models are often contributing factors in accidents. For example, if a pilot's mental model is that their aircraft is in a certain autopilot mode when the autopilot has actually disengaged, the pilot may not perform the necessary tasks to maintain control of the aircraft. Process models change over time as software is updated, procedures change, and operators become more familiar with systems. As a result, the process model of a system's designers may be different from that of its operators, a common cause of unexpected behavior.

By combining the concepts of feedback control loops, hierarchy, and process models, STAMP provides an avenue for capturing a wider range of accident causes. STAMP particularly lends itself to identifying situations where every component functioned exactly as designed, but they

interacted in a way that was ultimately unsafe. The STAMP framework is also useful for understanding causal pathways that are nonlinear, like unsafe behavior that reinforces itself or balances out other safe behavior. A number of tools based on STAMP have been developed to support safety activities.

2.3.3. CAST – Causal Analysis Based on Systems Theory

Causal Analysis based on Systems Theory (CAST) is an accident analysis technique based on the STAMP framework. A detailed overview of CAST is found in the CAST Handbook [18]. The goal of CAST is to provide a structured approach that guides experts to think in more depth about the causes of an accident and generate better recommendations to prevent similar accidents in the future.

CAST differs from traditional accident analysis techniques as it does not seek to identify a single "root cause" for the accident. Instead, CAST models the system involved in the accident as a control structure and examines each individual controller to understand their contributions to the accident. Rather than stop at each contribution, though, CAST goes on to identify why it appeared reasonable for each controller to make the decisions they made, even if those decisions were unsafe in hindsight. CAST also does not assign blame for an accident to any component, individual, or organization within the system. Instead, it focuses on understanding why the safety constraints were not enforced appropriately and generating recommendations to ensure they are enforced in the future.

Figure 6 shows the five steps of CAST:

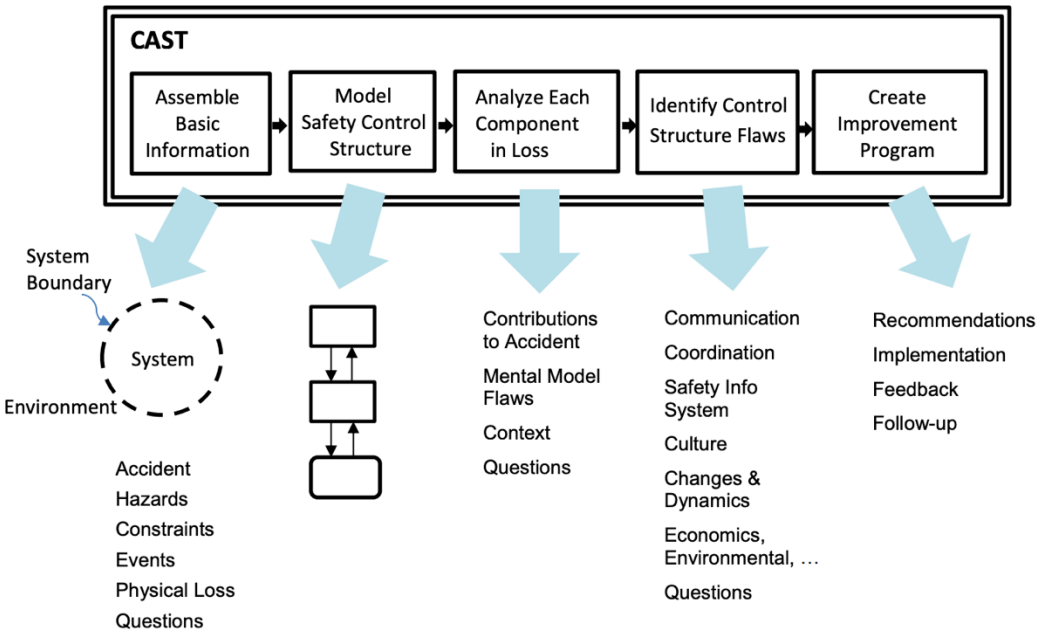


Figure 6. Five steps of CAST (taken directly from [18])

CAST begins by assembling the basic information about the accident. This includes identifying the boundaries of the system involved in the accident, the *losses* and *hazards* that have occurred, the timeline of events leading up to these losses, and any initial questions the analyst has. The

STAMP framework defines losses as anything of value to the stakeholders in a system, including loss of life, loss of property, and loss of reputation, among others. Hazards are defined as system states or sets of conditions that, in a worst-case environment, could lead to a loss.

Once the appropriate information about the accident has been collected, step 2 of CAST is to model the system as a hierarchical control structure. Once the analyst understands the control and feedback relationships that existed (or did not exist) prior to the accident, they can begin analyzing each controller for their contributions to the loss (step 3). Each controller's unsafe decisions are analyzed by considering the process model flaws and contextual factors that made the decision appear reasonable. It is typically easier to begin by analyzing the contributions of controllers at the bottom of the control structure (e.g., automation and operators), as this analysis will generate the appropriate questions to ask when analyzing the controllers higher up (e.g., management and regulators).

Once the contributions of each controller are identified and explained, step 4 of CAST involves analyzing the control structure as a whole to identify the systemic factors that affect the behavior of all controllers. These systemic factors can include communication and coordination problems, safety culture, economic factors, environmental factors, and several others. The outputs of steps 3 and 4 of CAST are then used in step 5 to create an improvement plan to prevent future accidents.

2.3.4. STPA – System Theoretic Process Analysis

System Theoretic Process Analysis (STPA) is a hazard analysis technique based on the STAMP framework. More information about STPA can be found in the STPA Handbook [19]. Though STPA does consider how component failures can lead to accidents, STPA also assumes that accidents can occur when components working as designed interact in unsafe ways.

Figure 7 shows the four steps of STPA:

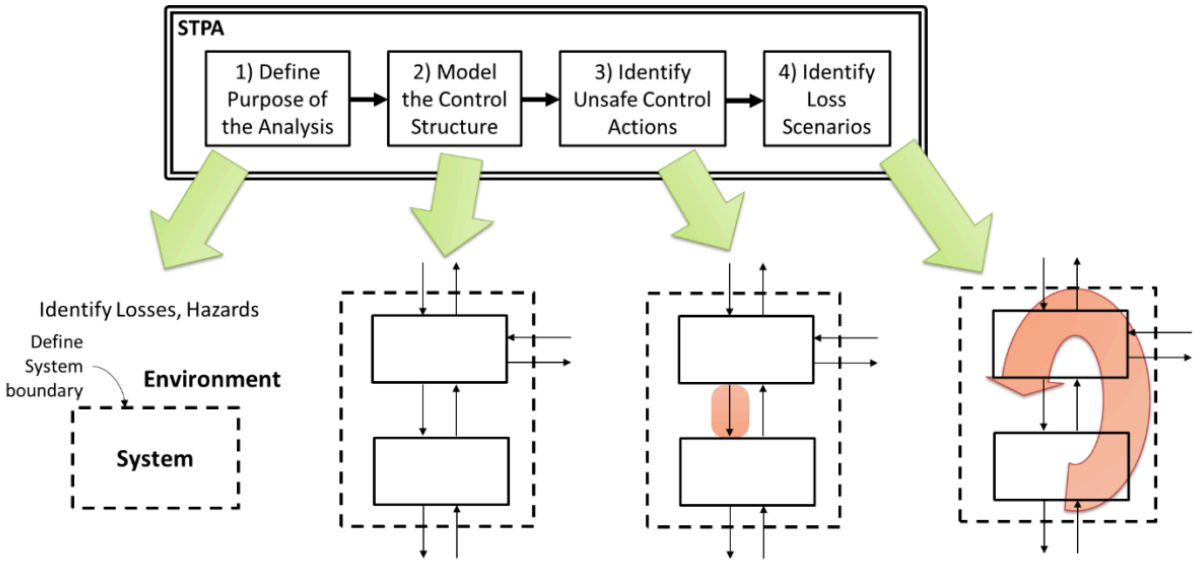


Figure 7. Four steps of STPA (taken directly from [19])

STPA begins by defining the purpose of the analysis, which involves identifying the system being analyzed and establishing its boundaries with the environment. This step also involves

identifying the losses of interest to the stakeholders in the system. Though STPA was originally developed for safety assessment, it can be applied to analyze other emergent system properties like efficiency and maintainability. Anything that is valuable to system stakeholders can be considered a loss in STPA, and typical safety-related losses include loss of life or injury and damage to property. Each STPA loss is also associated with one or more system-level hazards, which are also defined in STPA as system states or sets of conditions that, in a worst-case environment, could lead to a loss.

Step 2 of STPA involves modeling the system as a hierarchical control structure that captures the control and feedback relationships between system elements. The control structure typically begins at a high level of abstraction and is iteratively refined as the analysis progresses and more decisions are made about the system's design. STPA control structures always include software and human operators, and they are analyzed for their potential contribution to losses and hazards just like hardware components are.

In step 3 of STPA, each of the control actions available to each controller in the control structure is analyzed to identify how they may become unsafe. A control action is considered an *unsafe control action* (UCA) if it is made in a context that leads to a hazard. For example, providing manual braking commands may be safe during a normal aircraft landing roll, but may cause a hazard if provided during a takeoff roll. Each UCA contains four parts: the controller taking the action, the control action itself, the UCA type, and the context that makes the action unsafe. More details on UCA types can be found in the STPA Handbook [19].

Finally, step 4 of STPA involves identifying why it may appear reasonable for a controller to make a UCA. STPA identifies UCA causes by generating *causal scenarios*. Causal scenarios typically involve controllers issuing unsafe commands because of flawed process models, which are often the result of inadequate feedback. Other types of scenarios may involve control actions that are commanded appropriately but never actually take place, or result in behavior that was not intended by the controller. The STPA scenarios can then be used to generate recommendations that mitigate the causal factors leading to hazards and losses.

STPA differs from traditional safety assessment techniques as it does not assign severities to UCAs or scenarios, and does not generate probabilistic safety requirements. Instead, STPA identifies behavioral or functional requirements for hardware, software, and human components in order to prevent the system from entering an unsafe state.

2.4. The Boeing 737 MAX and MCAS

The Boeing 737 MAX is the most recent upgrade to the Boeing 737 line of twin-engine, narrow body jets. While the 737 was introduced in the late 1960s, the 737 MAX family was first announced in August 2011 and first entered commercial service in May 2017 [20]. The 737 MAX 8, the shortest in the family, is a derivative of the Boeing 737-800, which belonged to the earlier 737 Next Generation (NG) family.

The new CFM LEAP-1B engines incorporated into the 737 MAX design have a larger fan diameter and differently shaped nacelle from the 737 NG. Boeing discovered that these changes resulted in the aircraft experiencing a nose-up pitching moment at high angles of attack, which affected the aircraft's "stick force per g" characteristics and could place it outside compliance with certain elements of 14 CFR Part 25 [3]. To address this problem, Boeing made aerodynamic changes to the aircraft and introduced a new software-based stability augmentation system called the Maneuvering Characteristics Augmentation System (MCAS). To eliminate the need for

simulator training when transitioning from the 737NG to the 737 MAX, Boeing omitted all mention of MCAS from its flight crew training and operations manuals.

2.4.1. Functional Overview of MCAS

MCAS is a function within the 737's Speed Trim System (STS). The STS is a set of control laws in the 737's Flight Control Computer (FCC), and it exists to improve flight characteristics when the aircraft is operating at low gross weight, aft center of gravity, high thrust, and with the autopilot disengaged. When the flight crew sets a desired speed for the aircraft in manual flight, the STS issues commands to the horizontal stabilizer to ensure the aircraft remains at that speed. For example, if the aircraft loses too much speed, the STS will issue an aircraft nose down (ND) stabilizer command to increase speed, whereas if the aircraft gains too much speed, the STS will issue an aircraft nose up (NU) command to reduce speed [2].

While the STS provides speed stability augmentation, MCAS provides pitch stability augmentation. Figure 8 visualizes MCAS' normal behavior without inputs from the flight crew.

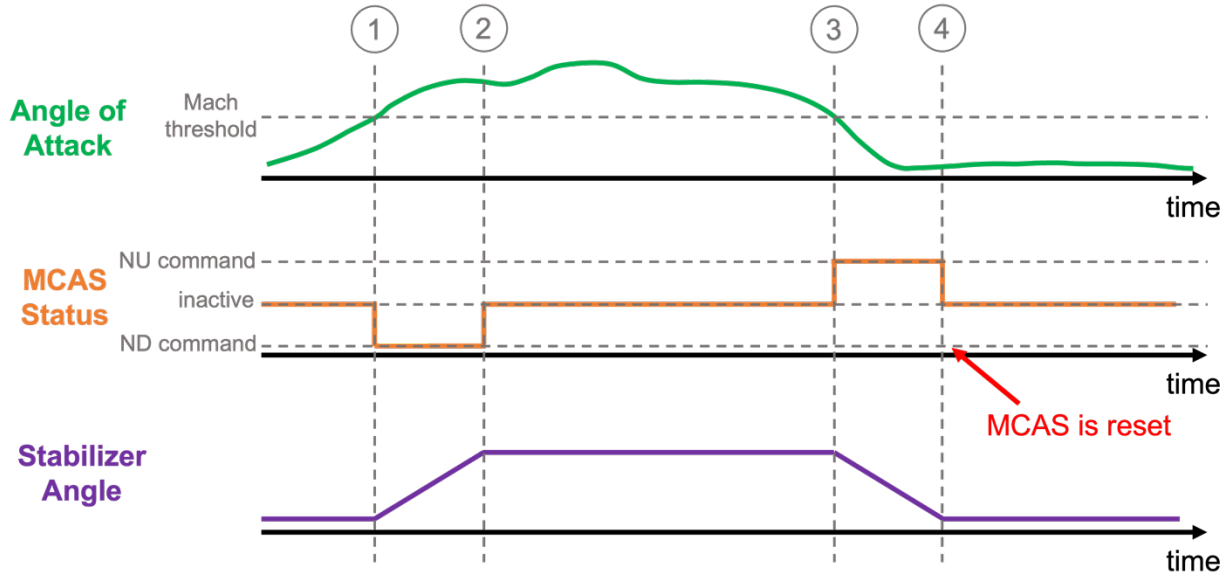


Figure 8. Normal MCAS behavior without flight crew input

By design, MCAS activates when the aircraft is operating in a flaps-up, autopilot off configuration, and the aircraft's angle of attack exceeds a threshold determined by the current Mach number. When it activates, MCAS issues a stabilizer ND command at a rate of 0.27° of stabilizer movement per second, with a magnitude proportional to how much the angle of attack exceeds the Mach number threshold (① to ② in Figure 8). MCAS originally had a maximum authority of 0.6° of stabilizer movement per command, but a change introduced in 2016 allowed MCAS to issue commands up to 2.5° of stabilizer movement [2,21]. The maximum duration of an MCAS command is therefore approximately 9.26 seconds. The stabilizer ND command is not directly meant to pitch the aircraft down; it is instead meant to increase the stick force the pilots feel on the control column and reduce the aircraft's pitch up tendency.

Once the angle of attack goes below the Mach number threshold (③ in Figure 8), MCAS issues a corresponding stabilizer NU command of the same magnitude as the prior ND command,

to bring the stabilizer back to its original position. Upon completion of the NU command (④ in Figure 8), MCAS' cycle is complete, and its control logic is reset.

MCAS behaves slightly differently when the flight crew provides trim commands. Figure 9 depicts MCAS' behavior with flight crew inputs.

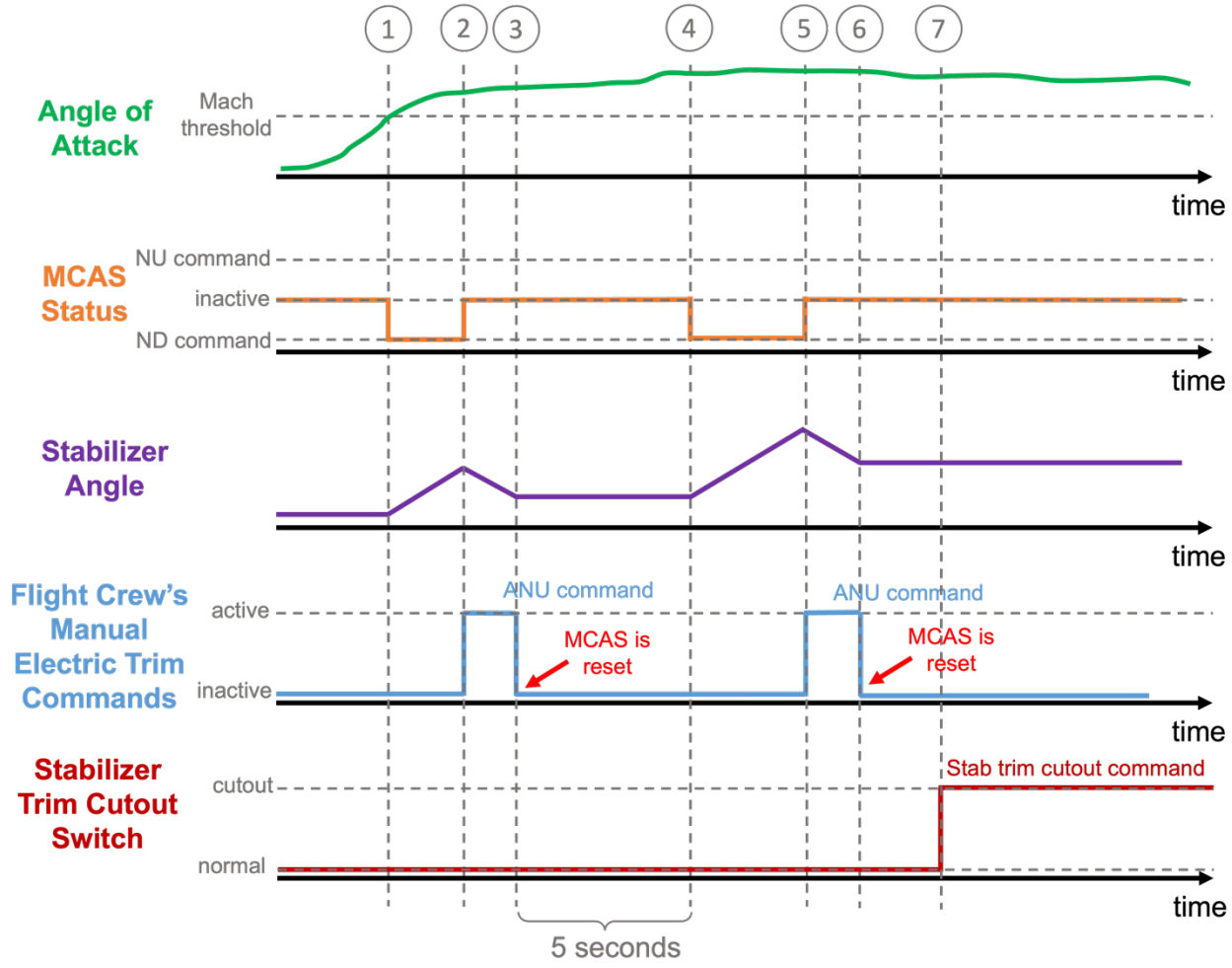


Figure 9. MCAS behavior with flight crew input

MCAS activates when the angle of attack goes above the threshold (① in Figure 9). The flight crew have the ability to interrupt an MCAS command at any point in the process using the manual electric stabilizer trim switches, which are mounted on the control column. Any manual electric stabilizer trim inputs from the flight crew will automatically stop an MCAS command (② in Figure 9), and once the manual command is complete (③ in Figure 9) the system's logic is reset. If MCAS still detects an angle of attack above the Mach threshold five seconds after a reset, it will activate again and initiate a new stabilizer ND command (④ in Figure 9) [2]. This cycle can then repeat itself (⑤ and ⑥ in Figure 9).

To prevent MCAS from activating entirely, the crew also has access to the stabilizer trim cutout switches, located in between the pilots, just below the thrust levers. Moving these switches to the "CUTOUT" position (⑦ in Figure 9) cuts all electric power to the stabilizer trim motor, meaning MCAS cannot activate, but the crew also cannot use electric trim to move the stabilizer. The crew

instead have to rely on physically rotating the stabilizer trim wheels to move the jackscrew that changes stabilizer angle.

Additionally, on all Boeing 737 aircraft, any automatic movement of the horizontal stabilizer can be interrupted by movement of the control column in the opposite direction. For example, if the STS issues a stabilizer ND command, the flight crew may pull back on the control column (which pitches the aircraft up), and the automatic stabilizer ND command will halt. This function is referred to as "control column cutout". However, MCAS activates at high angle of attack maneuvers, so MCAS requires the stabilizer to provide ND commands while the crew is already most likely pulling back on the control column. Therefore, MCAS inhibits the control column cutout function, meaning that pulling back on the control column will have no effect on MCAS' stabilizer ND command.

Like the STS, MCAS is a flight control law within the 737's FCC, but MCAS is only active in the master FCC for any given flight. When the aircraft is powered up, the master FCC defaults to the left FCC, and alternates between left and right for each subsequent flight. Each FCC (left or right) receives angle of attack and Mach information from its associated Air Data Inertial Reference Unit (ADIRU), which in turn receives this information from its associated sensors (left or right angle of attack vanes and pitot-static systems). Thus, when the left FCC is the master FCC, MCAS receives information from the left ADIRU, which collects that information from only the left angle of attack vane.

MCAS was involved in the two major Boeing 737 MAX accidents in October 2018 and March 2019. A summary of these accidents is provided with the overview of the CAST results in Chapter 3. The full CAST results can be found in Appendix A.

2.5. Literature Review on Safety Assessment Standards

Literature on the limitations of the safety assessment processes for commercial aircraft has come primarily from three sources: government or regulatory agencies, the standards development community, and the academic community. Each of these bodies of work are discussed in this section.

2.5.1. In the Government and Regulatory Community

The need for reevaluation of the safety assessment guidance for commercial aircraft has been identified by regulatory authorities and government agencies for at least the last two decades. In a comprehensive report from 2002 [22], the FAA recognized the need for improvement in the safety assurance process, particularly in the approaches to validate and document assumptions regarding human response to failures. Key findings of that report include that "there is no reliable process to ensure that assumptions made in the safety assessments are valid with respect to operations and maintenance activities" and that "a process that challenges the assumptions made in the safety analysis of flight critical functions is necessary" [22]. The report acknowledges that there is little guidance provided in AC 25-1309-1 and in ARP4761/ARP4754 to ensure human performance is adequately considered during airplane design.

Building on the FAA work, a 2006 National Transportation Safety Board (NTSB) report [23] evaluated concerns about the FAA's type certification procedure that were raised by prior accident investigations. That report concluded that "consideration of … human/airplane system interaction failure conditions are not required in the certification-related assessments of safety-critical

systems, and these exclusions limit the scope of the failure conditions considered during the safety assessment process." [23] They then recommended amending the advisory materials for complying with § 25.1309 regulations to include consideration of human/airplane system interaction.

A few accident/incident reports from investigative agencies have identified areas for improvement in safety assessment processes. On several occasions [24–26], the NTSB has reiterated its recommendation from [23] that the advisory materials for safety assessment be amended, particularly surrounding human-aircraft interactions. In the report on a 2010 runway overrun in Columbia, South Carolina, the NTSB specifically called for the revision of guidance such as AC 25.1309-1, to understand why particular design flaws were not caught during the safety assessment process [26]. The Australian Transportation Safety Board also included a discussion of the limitations of traditional safety assessment methods like Failure Modes and Effects Analysis (FMEA) and FTA in its report on an in-flight upset involving an Airbus A330 in 2008, and recognized the existence of new safety assessment methodologies like STPA [27].

In the aftermath of the 737 MAX accidents, investigative bodies and regulatory agencies worldwide acknowledged existing limitations in safety assessment guidance. In the JT610 final report [2], the Indonesian National Transportation Safety Committee (KNKT), conducted a thorough examination of how Boeing applied the ARP processes, including how they performed FHAs and FTAs for MCAS. Though the report identified key deficiencies in the safety assessment of MCAS and the 737 MAX, it did not attempt to trace any such deficiencies to limitations in the methods or guidance. However, in their safety recommendations to the FAA, the KNKT did recognize the potential for a safety gap to exist if the requirements from § 25.1309 and § 25.1302 are considered separately during design. The ET302 final report [3] does not place focus on any such gaps.

In a report specifically centered on assumptions in the certification of the 737 MAX [28], the NTSB concluded that a standardized methodology for evaluating and validating pilot response assumptions is still missing from existing guidance. The Joint Authorities Technical Review (JATR) report on the 737 MAX flight control system also concluded that "existing human factors guidance material (e.g., AC 25.1302-1) may be insufficient to emphasize the importance of human factors and human system integration throughout the certification process" [29].

Additionally, the Official Report of the Special Committee to review the FAA's Aircraft Certification Process [30] recognized that traditional safety assessment methods may be insufficient to address more complex accident causes, like conflicting actions taken by flight crews and automated systems. They recommend the development of new standards to integrate human performance assessments into existing processes for design assurance and validation. The U.S. Congress also recognized these limitations and, in December 2020, approved Public Law 116–260 that includes directives for the FAA to examine tools and methods for integrating human factors considerations into aircraft design and certification processes [31].

Finally, some studies have also identified limitations in the guidance for integrating safety with the larger systems engineering process. In a 2016 report [32], the FAA identified shortcomings with the processes for requirements definition, validation, and verification in ARP4754 that have implications for aircraft safety. They argue that critical gaps exist for validating functional requirements for systems that are highly integrated, and for identifying missing requirements.

In work on verification and validation of aircraft automation for the National Aeronautics and Space Administration, Whitlow et al. [33] found that human factors engineering is not given sufficient attention in ARP4754 and ARP4761 because issues like crew situational awareness are

not formally considered in the process for certifying aircraft systems. Additionally, Alves et al. [34] identify several shortfalls of traditional safety assurance approaches when examining systems with increasing autonomy, including limitations in FHA and SSA when examining the safety of transferring control from automation to humans.

2.5.2. In the Academic Community

In the academic community, systematic evaluations of the limitations in current safety assessment guidance are limited. The majority of the existing literature proposes small extensions to facilitate individual steps of the ARP processes, rather than a comprehensive examination of the methodologies and their theoretical underpinnings in the context of the increasing complexity of modern systems. For example, Delange and Feiler [35] point out that the safety engineering practices proposed in ARP4754 and ARP4761 are highly labor intensive, typically performed by system or safety engineering teams, and not frequently iterated upon after initial development. They recognize that this creates the potential for gaps between system-level requirements and software requirements and propose a framework for automating particular steps of the process.

However, a few studies do go beyond extending individual components of the ARP processes in favor of reflecting on the methods' underlying principles. A majority of these studies identify limitations in the ARP processes by comparing them with other methodologies, such as STPA.

Leveson et al. [36] comprehensively assess the limitations in the ARP processes by conducting an STPA on the wheel brake system example in ARP4761 and comparing the methods at a philosophical level. The study found that the approaches in ARP4761 are well suited for identifying pathways to accidents stemming from component failures, but are less effective at predicting accidents where no components fail, but their intended behavior interacts unsafely. They also found that treating humans separately from system design limits the analyst's ability to consider human-system interaction and examine how humans may be misled by the design of software or hardware. They ultimately conclude that the ARP4761 processes omit important causes of aircraft accidents, and that software and human factors must be integrated directly into safety assessment processes [36]. In other work, Leveson [37] also evaluates the general strengths and weaknesses of FHA, FTA, and FMEA outside the context of ARP4761.

Mutuel [38] provides a detailed examination of the hazard identification process in ARP4761 that evaluates the methodology for five key attributes: coherence, structure, comprehensiveness, integration, and a basis on requirements. They argue that the quality of the hazard identification process through FHA is strongly related to the functional model of the aircraft or system being analyzed, and is thus vulnerable to limitations in the accuracy and completeness of the model used. The primary weaknesses identified in FHA and common cause analysis are in capturing interactions between the system being analyzed and other systems, as well as between the system and its users. To address this, they propose a melded hazard identification methodology that relies on the complementarities of a number of different approaches, including the ARP processes and STPA, among others.

In a different study, Voros [39] discusses challenges for applying the ARP4754 and ARP4761 processes to future air and space vehicles, and proposes recommendations to broaden the scope of analysis in these standards. The article highlights how it may be challenging to understand whether/when to apply each step of the safety assessment process for new types of aircraft, and there is a lack of guidance for performing function definition and identifying specific failure conditions. The standards also make fundamental assumptions about the nature of the system being

evaluated (e.g., that it will be a crewed aircraft), and are overly constrained by the regulatory framework they were originally designed to satisfy. The paper concludes that the core limitation of the ARP processes is that they rely too heavily on specialized knowledge and experience to be properly executed.

Beland [40] also outlined some gaps in the ARP processes, such as capturing complex human-automation interactions, in a presentation on the potential role of STPA in aircraft safety assessment standards. They highlight the potential for incorporating STPA into the PASA and PSSA steps of ARP4761 and call for further studies into the practical considerations of blending the methodologies.

2.5.3. In the Standards Development Community

The community that develops standards for development assurance and safety assessment of commercial aircraft has also recognized gaps in current standards and have made steps towards addressing them.

In its response to [30], the FAA indicated they will work with the committees that develop system safety and human factors standards to explore improved methodologies and tools, especially surrounding human-machine interactions [41]. To achieve that goal, the SAE's S-18 committee officially established subcommittee S-18H, whose objective is to "clarify the relationships and resolve the gaps involving the human considerations in the function development, safety assessments, and human factors processes" [42]. The committee's scope is to examine each step of the ARP4761 process, to identify opportunities for integrating human considerations into them. Though the work of S-18H is not yet complete, they have initialized work on Aerospace Information Report (AIR) 7127 that discusses human considerations for the AFHA and SFHA steps.

In parallel, the S-18 committee has also developed additional AIRs to address gaps in existing standards. AIR7121, which is still a work in progress, discusses the applicability of ARP4754 and ARP4761 to unmanned aircraft systems (UAS), highlighting the shortcomings in these standards regarding the specific technical aspects of UAS. AIR6913, also a work in progress, provides guidelines for incorporating STPA into the development and safety assessment of civil aircraft to address potential limitations. There may be additional efforts from S-18 or other standards development committees in progress to address limitations in existing guidance that are not yet publicly available.

Chapter 3

Limitations in Current Safety Assessment Standards

This chapter provides a summary of the CAST analysis results on the two B737 MAX accidents, and then examines the gaps and limitations that exist in the standards used to assess the safety and certify commercial aircraft[5]. Along with each of the identified limitations is a discussion of how a flaw related to that limitation in the certification procedures manifested itself during the development and safety assessment of Boeing 737 MAX, and contributed to the two accidents involving that aircraft.

3.1. Summary of CAST Results

3.1.1. Basic Information

The first step of CAST is assembling the basic information about the accident. All of the information for this CAST analysis came from publicly available sources [2,3,20,21,28–30,41,43–47]. The losses in both accidents are clear: the destruction of both aircraft and the death of their occupants. The system in each case is defined as the aircraft and its occupants (including the flight crew), the airline, the airport and air traffic control facilities, the aircraft and subsystem manufacturers, and the regulatory authorities that oversaw each step of the aircraft's certification and operation. Elements such as adverse weather or bird strikes are treated as environmental conditions because engineers have no control over them, but measures to mitigate their effects are considered as part of the system, because engineers design them with a purpose.

The system level hazards and safety constraints for both accidents are similar, so they are consolidated in this section:

System Hazard 1: Aircraft does not maintain adequate separation from outside objects
Safety Constraints:

- Aircraft must maintain adequate separation from outside objects
- Aircraft must be able to detect and recover from a violation of adequate separation

System Hazard 2: Aircraft is unable to be controlled
Safety Constraints:

- Aircraft must remain under positive control
- Aircraft must be able to safely recover from a loss of control

System Hazard 3: Aircraft loses ability to remain airborne

[5] At the time of publication of this thesis, the most up-to-date versions of ARP4761 and ARP4754 are ARP4761A and ARP4754B respectively. Ongoing programs may still operate under prior versions of ARP4754 and ARP4761, and may not transition to the most updated guidance unless prompted by regulatory authorities. However, the analysis presented here still examines the most updated versions of the standards.

Safety Constraints:

- Aircraft must be at a speed and attitude which preserves its ability to remain airborne
- Aircraft must be able to detect and recover from a speed or attitude in which it cannot remain airborne

A full timeline of events for each accident can be found in Appendix A. Table II below provides a condensed overview of the sequence of events for each accident:

Table II. Condensed Sequence of Events for JT610 and ET302

Accident	Condensed Sequence of Events
Lion Air Flight JT610	On October 29th, 2018, at 6:20AM local time, Lion Air flight JT610 took off from Soekarno Hatta International Airport in Jakarta, bound for Pangkal Pinang. The aircraft, a Boeing 737 MAX 8, was carrying 189 people on board. Within seconds of leaving the ground, the left control column stick shaker activated, and an indicated airspeed (IAS) disagree message appeared in the cockpit displays. The crew attempted to perform the checklist for unreliable airspeed, but were unable to complete the procedure. When the flaps reached the fully retracted position, the stabilizer began moving in the ND direction, which was countered by the captain with a manual electric NU command. The stabilizer ND motion was commanded by MCAS, which believed the aircraft's AOA to be above the Mach threshold. Over the next few minutes, MCAS issued ND commands 26 times, most of which were partially countered by the flight crew with NU commands. When control of the aircraft was transferred from the captain to the first officer (FO), the FO did not realize the need to retrim the aircraft after each activation, and successive MCAS activations were not sufficiently countered. The aircraft became progressively mistrimmed until it was no longer under positive control. It subsequently crashed into the Java Sea, killing all 189 on board. The KNKT ultimately determined that a miscalibrated AOA vane introduced a 21° bias to the AOA values used by MCAS, leading the system to believe it had exceeded the Mach threshold.
Ethiopian Airlines Flight ET302	On March 10th, 2019, Ethiopian Airlines flight ET302, a Boeing 737 MAX 8 with 157 people on board, took off from Addis Ababa Bole International Airport at 8:38AM, bound for Nairobi, Kenya. Shortly after liftoff, the stick shaker activated along with an IAS disagree message, and a master caution anti-ice warning. After multiple unsuccessful attempts to engage the autopilot, the flight crew retracted the flaps and MCAS issued an automatic stabilizer ND command. The crew countered this with a short manual electric stabilizer NU command, and five seconds later MCAS issued another ND command. After fully countering this command with an NU command, the crew moved the stabilizer trim switches to the "CUTOUT" position, preventing MCAS from activating again. However, noticing they could not manually retrim the aircraft using the trim wheel, the crew returned the trim switches to the normal position, which allowed MCAS to activate again. The aircraft became uncontrollable and crashed a few seconds later, killing all those on board [3]. The Ethiopian Aircraft Accident Investigation Bureau (AAIB) concluded a

	malfunction in the AOA sensor was responsible for the erroneous data MCAS received [3], while the NTSB determined that the sensor was most likely separated from the aircraft through impact with a foreign object [43].

3.1.2. Examination of the Contributions of each Controller in the Loss

The next steps of CAST require the analyst to build a safety control structure for the accident and examine the how each controller in that control structure contributed to the loss. Each controller's unsafe decisions are explained by considering what process model flaws and contextual factors made the unsafe decision appear reasonable.

The full CAST results include an analysis of the unsafe contributions of the aircrafts' physical components, its on-board software, the flight crew, air traffic control, maintenance engineers, airline management, airport management, the aircraft manufacturer, and regulatory authorities, among others.

While the complete results for each controller are in Appendix A, this section includes the results for the flight crews of JT610 and ET302 in Tables III and IV respectively, as well as the results for the aircraft manufacturer in Tables V and VI. The tables describe the contributions of each accident's flight crews to the loss, and include the process model flaws and contextual factors that made their decisions appear reasonable.

Table III. Flight Crew Contributions from JT610 CAST

JT610 Flight Crew Unsafe Control Actions:

- **610FC-UCA-1:** Captain did not diagnose that left-hand airspeed readings were unreliable
- **610FC-UCA-2:** Captain did not call for or perform runaway stabilizer procedure
- **610FC-UCA-3:** Captain did not communicate the need to repeatedly retrim aircraft to FO upon transferring control
- **610FC-UCA-4:** FO did not immediately perform airspeed unreliable memory items when prompted by captain
- **610FC-UCA-5:** FO did not complete airspeed unreliable checklist [610FC-UCA-1]
- **610FC-UCA-6:** FO did not declare emergency or urgency to ATC beyond communicating "flight control problems"
- **610FC-UCA-7:** FO did not retrim aircraft sufficiently after repeated MCAS ND commands upon receiving control
- **610FC-UCA-8:** Crew did not discuss the aircraft problems previously recorded in the Aircraft Flight Maintenance Log (AFML)

JT610 Flight Crew Process Model Flaws:

- **610FC-PMF-1:** Captain's potentially flawed understanding of the aircraft's speed and attitude due to conflicting stick shaker activation and additional cockpit instrumentation indicating level pitch and relatively high speed [610FC-UCA-1, 2]
- **610FC-PMF-2:** Captain's potentially flawed model of the FO's understanding of the aircraft's state [610FC-UCA-3]
- **610FC-PMF-3:** Captain was potentially unaware of the extent he was retrimming the aircraft after each MCAS activation [610FC-UCA-3]
- **610FC-PMF-4:** FO potentially unaware that they would be unable to perform the memory items, if that had not been trained in a long time [610FC-UCA-4]
- **610FC-PMF-5:** FO potentially unaware of the extent to which the aircraft needed to be retrimmed after each MCAS activation, as was preoccupied with airspeed unreliable checklist while captain was doing this [610FC-UCA-7]

- **610FC-PMF-6:** Flight crew most likely did not believe stabilizer runaway was occurring, as the observed stabilizer behavior was not consistent with a runaway (intermittent instead of continuous) [610FC-UCA-2]

JT610 Flight Crew Contextual Factors:

- **610FC-CF-1:** FO was unable to complete airspeed unreliable checklist [610FC-UCA-1, 2]
- **610FC-CF-2:** Stick shaker active from rotation until the end of the flight, with brief pause when flaps were at position 1 [610FC-UCA-1]
- **610FC-CF-3:** Enhanced Ground Proximity Warning System sounded "AIR SPEED LOW – AIR SPEED LOW" when ATC informed that ground speed was 322 knots [610FC-UCA-1]
- **610FC-CF-4:** AOA Disagree message not displayed on B737 MAX 8 not fitted with optional AOA indicator [610FC-UCA-1]
- **610FC-CF-5:** Flight crew did not discuss problems observed on JT043 [610FC-UCA-1, 2, 3]
- **610FC-CF-6:** MCAS never mentioned in flight crew manuals or training [610FC-UCA-2, 3]
- **610FC-CF-7:** Captain was focused on flying the aircraft and retrimming prior to handing control to FO and did not communicate need to retrim [610FC-UCA-1, 2]
- **610FC-CF-8:** Misidentifying non-normal checklists had appeared on the FO's training records [610FC-UCA-4, 5]
- **610FC-CF-9:** FO was cleared to fly, reinforcing belief that he was qualified to perform all necessary duties [610FC-UCA-4, 5]
- **610FC-CF-10:** Step 8 of airspeed unreliable checklist requires aircraft to be trimmed and stabilized condition, a state which was not reached [610FC-UCA-5]
- **610FC-CF-11:** ATC provided eight heading instructions after the flight crew reported that the aircraft was experiencing a flight control problem [610FC-UCA-5]
- **610FC-CF-12:** Airspeed only considered unreliable if indication differs from reference table by over 20KTS or 0.03 Mach; captain's and FO's displays differed by 15KTS [610FC-UCA-5, 6]
- **610FC-CF-13:** Electric trim inputs required to re-trim after MCAS activations were significantly longer than trim inputs pilots are accustomed to making [610FC-UCA-7]
- **610F-CF-14:** Aircraft is typically quite sensitive to trim inputs, so pilots are trained to trim in small bursts as opposed to sustained segments of time [610FC-UCA-7]
- **610FC-CF-15:** Flight crew did not discuss problems observed on JT043 [610FC-UCA-4, 5, 6, 7]
- **610FC-CF-16:** Flight crew may not have been aware of aircraft problems that might reappear during their flight because in the past it was not necessary to read the AFML [610FC-UCA-8]

Questions Raised:

- What are the requirements to consider a situation an emergency/urgency?
- What actions were taken to help the FO remember the memory items during training? Was this a common checklist to be performed? How often was it trained? Did the airline have any way of knowing this pilot did not have the procedure memorized? Where was the non-normal checklist located? Was it easy to access/locate?
- What was the guidance on information that needed to be shared when transferring control from captain to FO?

Table IV. Flight Crew Contributions from ET302 CAST

ET302 Flight Crew Unsafe Control Actions:

- **302FC-UCA-1:** Flight crew did not execute unreliable airspeed memory items and non-normal checklist from quick reference handbook (QRH)
- **302FC-UCA-2:** Captain engaged autopilot A, which was being fed erroneous AOA data
- **302FC-UCA-3:** Flight crew retracted flaps, allowing MCAS to begin activating
- **302FC-UCA-4:** Flight crew only trimmed nose up for 2 seconds (stabilizer moved from 2.1 to 2.3 units) after first MCAS activation
- **302FC-UCA-5:**Flight crew moved stab trim cutout switches to CUTOUT position without first re-trimming the aircraft using manual electric trim
- **302FC-UCA-6:** Flight crew did not monitor airspeed before reaching overspeed condition
- **302FC-UCA-7:** Flight crew was unable to manually re-trim aircraft

- **302FC-UCA-8:** Flight crew returned the stab trim cutout switches to the normal position

ET302 Flight Crew Process Model Flaws:

- **302FC-PMF-1:** Flight crew may have been unaware of IAS Disagree warning (only visual feedback, not aural), as they did not acknowledge it [302FC-UCA-1]
- **302FC-PMF-2:** Flight crew may have believed they were actually stalling, due to stick shaker activation [302FC-UCA-1]
- **302FC-PMF-3:** Flight crew may have not been aware of the erroneous AOA data [302FC-UCA-1, 2]
- **302FC-PMF-4:** If flight crew were aware of AOA issue, they may have believed engaging autopilot would fix the issue due to an interpretation of the wording on the Flight Crew Operating Manual (FCOM) bulletin following JT610 [302FC-UCA-1, 2]
- **302FC-PMF-5:** Flight crew may have been unaware that retracting flaps would have satisfied the conditions for MCAS to activate [302FC-UCA-3]
- **302FC-PMF-6:** Flight crew may have believed they were capable of re-trimming the aircraft manually after moving switches to CUTOUT position, as there is no mention in the FCOM bulletin of the potential for excessive airloads on the stabilizer that prevent manual trim [302FC-UCA-5]
- **302FC-PMF-7:** Flight crew may not have been aware that the aircraft was approaching an overspeed condition, as they had a stick shaker going off the entire flight [302FC-UCA-6]
- **302FC-PMF-8:** Flight crew may have considered that aerodynamically unloading the horizontal stabilizer through the "roller coaster" approach might have placed the aircraft too close to the ground [302FC-UCA-7]
- **302FC-PMF-9:** Flight crew may have believed electric trim was the only way to retrim the aircraft as they were unable to manually trim it [302FC-UCA-8]

ET302 Flight Crew Contextual Factors:

- **302FC-CF-1:** High density altitude at airfield [302FC-PMF-2]
- **302FC-CF-2:** Unreliable airspeed memory items required reducing N1 to 80%, and aircraft was still at low radio altitude (around 50ft) [302FC-UCA-1]
- **302FC-CF-3:** IAS Disagree warning takes 5 seconds to activate, so master caution would have activated before that and drawn crew's attention [302FC-PMF-1, 302FC-UCA-1]
- **302FC-CF-4:** It is difficult to detect that only one stick shaker activated (which could have informed the pilots that it wasn't a real stall, but an AoA issue) [302FC-UCA-1, 302FC-PMF-2]
- **302FC-CF-5:** The difference in IAS from one display to another was just around 20 kts, which is the limit for determining whether to perform the unreliable airspeed NNC [302FC-UCA-1]
- **302FC-CF-6:** Besides stick shaker, first indication of AoA fault was "MASTER CAUTION" and "ANTI-ICE" lights illuminating, which has no memory items and QRH has only one instruction: "Avoid icing conditions" [302FC-UCA-1, 2]
- **302FC-CF-7:** Training to rely on automation. 737 Flight Crew Training Manual (FCTM) states "It is mandatory that the Pilot Flying (PF) fly the airplane while the Pilot Monitoring (PM) accomplishes the NNC. Maximum use of the autoflight system is recommended to reduce crew workload." [302FC-UCA-2]
- **302FC-CF-8:** Wording of the FCOM bulletin: "Boeing would like to call attention to an AOA failure condition that can occur during manual flight only" [302FC-UCA-2, 302FC-PMF-4]
- **302FC-CF-9:** Company policy called for engaging autopilot at 500ft above ground level [302FC-UCA-1]
- **302FC-CF-10:** Wording of the FCOM bulletin and FAA airworthiness directive did not mention "flaps up" as a condition for MCAS activation [302FC-UCA-3, 302FC-PMF-5]
- **302FC-CF-11:** Standard procedure for takeoff would have been to retract flaps at this stage [302FC-UCA-3]
- **302FC-CF-12:** Electric trim inputs required to re-trim after MCAS activations were significantly longer than trim inputs pilots are accustomed to making [302FC-UCA-4]
- **302FC-CF-13:** Aircraft is typically quite sensitive to trim inputs, so pilots are trained to trim in small bursts as opposed to sustained segments of time [302FC-UCA-4]
- **302FC-CF-14:** Guidance from FCOM bulletin for dealing with "uncommanded nose down stabilizer trim" was to "do the Runaway Stabilizer NNC ensuring that STAB TRIM CUTOUT switches are set to CUTOUT". Use of manual electric trim is only mentioned in a note after the primary instructions. [302FC-UCA-5]
- **302FC-CF-15:** Crew was communicating with ATC in the direct moments before overspeed warning sounded [302FC-UCA-6]

- **302FC-CF-15:** The only indication of the aircraft not having transitioned to climb thrust was the A/T indication of ARM instead of N1 [302FC-UCA-6]
- **302FC-CF-16:** Airspeed was at approximately 360-375kts, meaning the aerodynamic forces on the stabilizer were too large for one person to be able to move trim wheel [302FC-UCA-7]
- **302FC-CF-17:** Flight crew needed to continuously pull back on the control column to prevent the aircraft from diving due to the mistrim. Releasing the control column to attempt to trim led to a pitch down, which further increased airspeed and made trim more difficult. [302FC-UCA-7]
- **302FC-CF-18:** 40 turns of the trim wheel were required to fully retrim the aircraft [302FC-UCA-7]
- **302FC-CF-19:** FCOM bulletin has no guidance for re-trimming the aircraft if manual trim is not available and states "manual trim can be used before or after the STAB TRIM CUTOUT switches are moved to CUTOUT." [302FC-UCA-8]

Questions raised:

- How had the crew been trained to diagnose an airspeed unreliable situation? How was the prioritization scheme for dealing with the alerts in the cockpit (i.e. were they supposed to deal with stick shaker first, then IAS disagree?)?
- Why did the FCOM bulletin and airworthiness directives not mention the flaps as a condition for MCAS activation?
- How had the crew been trained to deal with mistrim? How often is this scenario trained?
- Were the crew aware of the need to electrically trim before moving stab trim cutout switches? What kind of training had they received following the JT610 accident?
- Why was there no mention in the FCOM of the potential for excessive airloads to prevent manual trim? Was it determined that, if it was noted in the FCTM, that was sufficient?
- Why was there no more explicit indication to the flight crew that the A/T was no longer controlling engine thrust?
- How often was the flight crew trained to aerodynamically reduce loads before retrimming?
- Did Boeing or the FAA foresee the overspeed condition preventing manual retrim? Why was this not included in the bulletin/directive?

Table V. Aircraft Manufacturer Contributions from JT610 CAST

JT610 Aircraft Manufacturer Control Actions:

- **610OEM-UCA-1:** Engineers did not appropriately validate assumptions that flight crew would respond correctly to erroneous MCAS activations
- **610OEM-UCA-2:** Engineers determined no redesign was necessary when considering the potential for repeated MCAS activations
- **610OEM-UCA-3:** Engineers determined that MCAS-related failure conditions had severity category of "Major", as opposed to hazardous or catastrophic
- **610OEM-UCA-4:** Engineers did not identify the implicit assumption that erroneous MCAS activation was equivalent to a runaway stabilizer (which turned out to be flawed, as MCAS is intermittent while stab runaway is continuous)
- **610OEM-UCA-5:** Engineers assigned MCAS failure conditions a severity of “major”
- **610OEM-UCA-6:** Engineers designed MCAS such that it only received information from one data source
- **610OEM-UCA-7:** Engineers designed AOA Disagree alert such that it only activated if aircraft was fitted with AOA display, and determined that this alert “was not necessary for the safe operation of the airplane”
- **610OEM-UCA-8:** Engineers did not directly inform certification authorities when MCAS’s range of motion was increased
- **610OEM-UCA-9:** Engineers removed mention of MCAS from the 737 MAX FCOM
- **610OEM-UCA-10:** Engineers did not identify the implicit assumption that the airspeed unreliable procedure was unaffected by the presence of MCAS (which turned out to be flawed, as repeated MCAS activations prevent the crew from stabilizing the aircraft to detect an unreliable airspeed)

JT610 Aircraft Manufacturer Process Model Flaws:

- **610OEM-PMF-1:** Engineers believed simulator test to verify that one MCAS activation was able to be countered was sufficient [610OEM-UCA-1, 3]
- **610OEM-PMF-2:** Engineers operated under the assumption that each MCAS activation would be recognized and immediately trimmed out by the flight crew [610OEM-UCA-2, 3, 10]
- **610OEM-PMF-3:** Engineers operated under the assumption that an MCAS activation would look like a stabilizer trim runaway [610OEM-UCA-4, 10]
- **610OEM-PMF-4:** Engineers believed that MCAS did not need an additional layer of redundancy in its source data as MCAS-related failure conditions had a severity category of "Major" [610OEM-UCA-6]
- **610OEM-PMF-5:** Engineers believed that probability of AOA failure was sufficiently low to meet safety requirements based on reliability data traceable to the sensor OEM [610OEM-UCA-6]
- **610OEM-PMF-6:** Engineers did not believe AOA disagree alert was necessary for safe operation of the airplane, as there were no required procedures for pilots to follow if that alert was observed [610OEM-UCA-7]
- **610OEM-PMF-7:** Engineers believed that "crews were not expected to encounter MCAS in normal operation" and that in most cases "the MCAS function is automatic and operates in the background, without any control input from the flight crew" [610OEM-UCA-9, 10]

JT610 Aircraft Manufacturer Contextual Factors:

- **610OEM-CF-1:** Specific failure modes that could lead to undesired MCAS activation were not simulated as part of the MCAS FHA [610OEM-UCA-1, 3, 10]
- **610OEM-CF-2:** FHA is a process for identifying "failure conditions" and classifying their severity that does not consider the source of the failure condition (though the source of the failure condition might affect what the flight crew experiences as the condition occurs) [610OEM-UCA-1, 3, 10]
- **610OEM-CF-3:** ARP4761 guidance assumes that flight crews, cabin crews, maintenance crews, and other individuals participating in the operation of the aircraft follow documented procedures [610OEM-UCA-1, 5, 10]
- **610OEM-CF-4:** Regulatory guidance in AC 25-7C states that a pilot will take immediate action to trim out reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions [610OEM-PMF-2, 610OEM-UCA-2, 3]
- **610OEM-CF-5:** Engineers originally assigned undesired MCAS activation a hazardous rating, but only if it occurred in the "operating flight envelope" as opposed to the "normal flight envelope", and used an exposure argument to assume they could discount 10^{-3} in "acceptable probability" because the chance of being in that envelope in the first place is very low [610OEM-UCA-3, 5]
- **610OEM-CF-6:** At a severity of “major”, the safety objective is on the order of 10^{-5} per flight hour and depending on the reliability information from the sensor manufacturer and the assumed exposure, it may be possible to meet the objective with a single sensor [610OEM-UCA-6, 7]
- **610OEM-CF-7:** ARP4761 does not provide guidance for identifying whether failures are independent from operational events/conditions [610OEM-UCA-3]
- **610OEM-CF-8:** ARP4761 does not provide guidance for identifying undocumented assumptions [610OEM-UCA-4, 10]
- **610OEM-CF-9:** Boeing has a standard set of assumptions used across all Boeing models for FHAs of flight control systems that are consistent with the requirements contained in 14 CFR 25.671 & 25.672 and FAA AC 25-7C for compliance evaluation of 14 CFR 25.143 [610OEM-UCA-1, 2, 3, 4]
- **610OEM-CF-10:** Failures with a severity class of “major” did not require a dedicated FTA, which may have generated a "no single point of failure" requirement [610OEM-UCA-6]
- **610OEM-CF-11:** ARP4761 does not provide guidance for identifying accident causes that do not stem from failures [610OEM-UCA-6]
- **610OEM-CF-12:** Only 25 activations of stick shaker due to AOA failures occurred in 737 aircraft for the past 17 years before JT610, during more than 240 million flight hours [610OEM-UCA-6, 7, 10]
- **610OEM-CF-13:** Revision documents are not required certification deliverables, especially as Boeing operated under the system of Organization Designation Authorization (ODA). [610OEM-UCA-8]
- **610OEM-CF-14:** Engineers received validation from the FAA that the decision to remove MCAS from FCOM was safe, as FAA agreed with the decision after discussion [610OEM-UCA-9]

- **610OEM-CF-15:** Airspeed unreliable procedure was appropriate for other versions of the Boeing 737 [610OEM-UCA-10]

Questions raised:

- What guidance existed in terms of simulating specific accident scenarios during the SSA, when causes of failure conditions have been identified?
- What additional human factors analysis was performed to validate FHA assumptions?
- What analysis was in place to establish the effectiveness of procedural mitigations to hazardous situations?
- What internal guidance/policy existed at Boeing for identifying unrecognized assumptions?
- What internal guidance/policy existed at Boeing for identifying causes of accidents that do not stem from failures (e.g., maintenance procedures, unsafe interactions, etc.)? How did Boeing deal with the fact that failure probabilities cannot account for external events that might damage the AOA sensor?
- What is the rationale behind the determination of what documents are certification deliverables?
- What are the procedures for determining what elements of "non-normal" operating procedure should go in the FCOM?

Table VI. Aircraft Manufacturer Contributions from ET302 CAST[6]

ET302 Aircraft Manufacturer Control Actions:

- **302OEM-UCA-1:** Boeing engineers provided to airlines only a roughly 6-hour non-simulator Logipad training on the differences between 737 MAX and 737 NG following JT610
- **302OEM-UCA-2:** FCOM bulletin provided by Boeing engineers used the following language: "Boeing would like to call attention to an AOA failure condition that can occur during manual flight only." This implies that the AOA malfunction could only occur during manual flight, when in reality it was MCAS activation that could only occur in manual flight
- **302OEM-UCA-3:** FCOM bulletin provided by aircraft manufacturer did not mention the possibility that crews are unable to manually trim the aircraft after moving the stab trim cutout switches to CUTOUT (or that it may require a two-pilot effort, or require elevator load alleviation)
- **302OEM-UCA-4:** Boeing engineers did not respond to a question from the airline regarding how pilots are expected to correct their aircraft's trim while also diagnosing and applying the Airspeed Unreliable checklist

ET302 Aircraft Manufacturer Process Model Flaws:

- **302OEM-PMF-1:** Boeing engineers were operating under the same assumptions with which they had designed MCAS, that pilots would follow posted instructions in an emergency and that if pilots performed the Runaway Stabilizer NNC they would re-trim electrically and not ever require manual trim [302OEM-UCA-1, 3]
- **302OEM-PMF-2:** Boeing engineers may have intended for their FCOM statement to be interpreted as "an aircraft failure condition that can occur during manual flight only, stemming from an AOA failure" [302OEM-UCA-2]
- **302OEM-PMF-3:** Airline management believed simulators were not designed to replicate the erroneous behavior observed in JT610 (and later ET302) [302AM-UCA-2]

ET302 Aircraft Manufacturer Contextual Factors:

- **302OEM-CF-1:** Additional training requirements would have required acknowledging and explaining the MCAS feature to all 737 MAX crews, which would have led to further delays for operators [302OEM-UCA-1]
- **302OEM-CF-2:** Many airlines did not possess 737 MAX simulators in which to perform additional training, and the logistics of processing crews at Boeing's Renton center would have added delays and also costs. [302OEM-UCA-1]
- **302OEM-CF-3:** JT610 investigation was still ongoing as the training was released [302OEM-UCA-1]

[6] Many of the aircraft manufacturer's contributions are shared between JT610 and ET302. Table VI lists only the contributions that were unique to ET302; it does not repeat the contributions that are already listed in Table V.

- **302OEM-CF-4:** As of when the FCOM bulletin was released, the manufacturer had not informed 737 MAX operators of the existence of MCAS [302OEM-UCA-2]
- **302OEM-CF-5:** Information about being unable to manually retrim was already noted in the FCTM, as such: "Excessive airloads on the stabilizer may require effort by both pilots to correct the mis-trim. In extreme cases it may be necessary to aerodynamically relieve the airloads to allow manual trimming. Accelerate or decelerate towards the in-trim speed while attempting to trim manually." However, there is no clarification on what it means to aerodynamically relieve airloads beyond accelerating or decelerating [302OEM-UCA-3]
- **302OEM-CF-6:** Boeing was providing Annex 13 technical support to the on-going Lion Air accident investigation, and deemed Ethiopian Airlines' question too closely related to this event to answer it [302OEM-UCA-4]

Questions raised:

- Did Boeing reevaluate its initial assumptions about pilots' reactions to MCAS activation, and their ability to follow procedure?
- What response did Boeing receive from airlines and pilots regarding the training that was provided? Was there significant misunderstanding and were there many clarification questions submitted?
- How was the language in the FCOM bulletin drafted and evaluated? What incentives did Boeing have to not mention MCAS directly?
- What evaluation went into the decision not to answer the question from the airline? How was it determined that this question related too closely to the accident scenario?

The CAST results reveal a misalignment between the mental models of the aircraft's operators and its designers. The following sections discuss some of the implications of these findings in terms of improving the guidance for aircraft safety assessment.

3.2. Limitations in Safety Assessment Standards

As was shown in the literature review, the aviation safety community has recognized that there are gaps in the civil aviation regulatory environment that allowed for MCAS' unsafe design to be certified and deployed. A majority of the studies published on this topic recognize that Boeing and the FAA made incorrect assumptions about the flight crew's ability to manage the kinds of situations that unfolded on JT610 and ET302. However, no studies systematically trace the causal factors from the 737 MAX accidents to limitations in the safety assessment standards and examine how the standards may not have supported designers as much as intended in evaluating the safety of the aircraft.

The analysis presented here identifies four key limitations in the safety assessment process. They are:

1. Limited integration of human considerations in the safety assessment process
2. Absence of a systematic methodology that supports the identification of unrecognized assumptions
3. A failure-centric safety assessment process with limited guidance for uncovering and managing non-failure based causal scenarios leading to losses
4. A limited framework for understanding nonlinear causal relationships between functional failure conditions and operational events/conditions

The following subsections explore each of these limitations in detail and tie them directly to contributing factors in the Boeing 737 MAX accidents identified through the CAST analysis.

Additional limitations exist in the safety assessment processes that were not as clearly observed in the 737 MAX accidents. When relevant, these limitations are introduced as well and briefly discussed. There may also be additional gaps not identified here, which provide an opportunity for future work.

Additionally, the discussion presented here relates to limitations in the standards as they are written, not necessarily as they are utilized in practice. It is important to recognize that aircraft manufacturers may devote additional resources to perform a more thorough safety assessment going beyond the guidelines in the ARPs. However, the ARPs serve as a baseline and provide the formal guidance utilized by manufacturers, making them a reasonable starting point for understanding the deficiencies in civil aircraft safety assessment and certification.

3.2.1. Limited integration of human considerations in the safety assessment process

The first gap involves the limited integration of human considerations in the safety assessment process. ARP4761 defines a safety assessment process to be used to meet the safety requirements of § 25.1309. Because § 25.1309 deals with systems and equipment, human-related contributions to accidents are intentionally excluded from the scope of the ARP processes. Human factors is typically considered during the design process for each subsystem, following different guidance for complying with § 25.1302. Though intentional, this separation of safety assessment and human factors limits the analyst's ability to capture several types of hazards related to human-system integration[7].

3.2.1.1. Human Factors in ARP4761

Although most human factors considerations are largely excluded from the current ARP processes, they do consider the effects of functional failures on the flight crew, and they allow human response to serve as a mitigation for the severity of the failure conditions identified. The AFHA and SFHA reports that list failure conditions also list the effects of the failure condition on the aircraft, its crew, and its occupants. These effects are used to determine the severity classification of the failure condition.

ARP4761 then specifically calls upon the analyst to "identify assumptions associated with aircraft and crew mitigations to limit the severity classification" [13] and have human factors specialists evaluate and confirm them[8]. However, because the ARP processes commonly assume that flight crews will follow documented procedures, this is not meant to be a comprehensive hazard analysis that identifies how human actions can contribute to hazards. The only requirement of this step is to confirm that the specific crew response being assumed is reasonably executable. However, there is not a clear definition, nor are there clear criteria, for what constitutes a reasonably executable response.

---

[7] SAE6906A, titled "Standard Practice for Human Systems Integration"[48] is an existing standard that covers human-system integration throughout system design, development, testing, production, use, and disposal. However, this standard is not formally integrated with the safety assessment process and there is no clear definition of what is required from a human factors perspective to satisfy safety regulations.

[8] Assumption validation is also called out in ARP4754, whose "Management of Assumptions" section calls for design assumptions associated with crew interaction and performance to be confirmed. The main approach proposed for doing so is reviewing assumptions against "existing industry experience and practice." [10]

Therefore, the scope and depth of the human factors assessment *for safety* is limited. When the human factors assessment is driven primarily by the objective of validating FHA assumptions and assigning severity classifications, the assessment will likely only consider the elements directly relevant to the question, "Will this human response assumption hold, based on the current design?"

However, to truly ensure that the human response to a failure condition will be safe and effective, a number of additional questions would also need to be answered. First, there is the question of what environments or scenarios could lead to this human response assumption *not* holding. Also, what *unintended* responses by the flight crew would be unsafe, and what design decisions need to be made to protect against these *unintended* responses by the flight crew?

In the SFHA example in ARP4761, one of the assumptions listed is "The flight crew will not initiate [a rejected takeoff] due to an annunciated failure of the deceleration function after V1" [13]. In this case, it is not enough to simply document the appropriate procedure (i.e. not initiating a rejected takeoff) and testing whether flight crews know not to do that when the deceleration function fails. Truly ensuring safety requires considering what other scenarios stemming from interactions between the flight crew and the aircraft, might lead them to reasonably initiate the rejected takeoff even if that goes against procedure.

Understanding unexpected behavior is less straightforward than understanding expected behavior. It requires considering all of the factors that may affect a flight crew's decision-making beyond the immediate observable trigger from the failure condition. It is also important to consider how the expected response may itself become unsafe. Are there situations when violating the assumption is actually a safer choice? Though these questions are not explicitly excluded from being considered, the limited goal of the human factors assessment can affect whether and how deeply they are investigated.

3.2.1.2. The 737 MAX Human Factors Assessment

Examining the MCAS FHA and its associated assumptions provides a valuable example for understanding the consequences of not integrating a human factors hazard analysis with the safety assessment process.

The final SFHA for the 737 MAX Stabilizer Trim Control System identified six failure conditions related to MCAS. They are shown along with their associated severity class in Table VII, adapted from [44]. Also shown are the phase of flight and flight envelope that contextualize each event.

Table VII. Functional Hazard Assessment for MCAS

Event	Severity Class	Phase of Flight
Uncommanded MCAS function	Hazardous	All (operational flight envelope)
Loss of MCAS function	Major	All (operational flight envelope)
Uncommanded MCAS operation to maximum authority	Major	All (normal flight envelope)
Uncommanded MCAS operation equivalent to 3 second stabilizer trim runaway	Major	All (normal flight envelope)
Loss of MCAS function	Minor	All (normal flight envelope)
Stabilizer trim runaway with MCAS operation	Minor	Cruise

Three key assumptions were documented by Boeing for use in their FHA evaluation of MCAS and stabilizer trim [2,45]:

- "Unintended stabilizer trim inputs are readily recognized by movement of the stab trim wheel, flight path change or increased column forces" [2].
- "Aircraft can be returned to steady level flight using available column (elevator) alone or stabilizer trim" [2].
- "Continuous unintended nose down stabilizer trim inputs would be recognized as a Stab Trim or Stab Runaway failure and procedure for Stab Runaway would be followed" [2].

These assumptions were derived from a set of fundamental assumptions used in all flight control FHAs across all Boeing models. They are available in the "MCAS Development and Certification Overview" slides presented in [45]. The determination that an uncommanded operation of MCAS up to its maximum authority would have a severity class of "Major" in the normal flight envelope was made by validating these three assumptions through pilot assessments.

According to [45], these assessments involved inserting single unintended MCAS activations into the stabilizer trim system in a simulator, while assessing handling qualities and associated flight crew actions. The results from this simulation led analysts to conclude that MCAS-related "failures" could reasonably be countered using only the aircraft's elevators, but also that stabilizer trim (and its associated cutout switches) were available to address the erroneous MCAS activation if necessary. Such findings were deemed sufficient to justify a severity classification of "Major" for unintended MCAS activation in normal operating conditions.

The flight crews onboard JT610 and ET302, on the other hand, did not respond in the manner predicted or prescribed in the safety assessment. The CAST results shown earlier in tables III and IV identified the reasons the crews may have acted the way they did. The results in tables V and VI explain why Boeing engineers may have acted the way they did. The unexpected responses by the flight crews reveal a disconnect between the mental models of the aircraft's designers and its operators.

The flight crew's decision-making in each case was not informed only by the immediate trigger observed from the failure condition, but by a plethora of additional factors as well. The pilots of both aircraft were operating in the context of multiple alerts and indications going off at the same time, some of which were contradictory and took precedence over others. The alerts required the flight crews to diagnose multiple problems, including a potential impending stall, potential unreliable airspeed indications, and undesired stabilizer trim inputs.

Additionally, the pilots' decision-making strategies may have been influenced by their training and prior experience. Commercial pilots are typically trained to trim aircraft in small bursts as opposed to the sustained time segments needed to overcome MCAS commands. It is impossible to affirm conclusively if these factors were considered during the validation process, but they were not documented in the safety assessment artifacts.

Also, from the description of the human factors assessment, it is unclear whether the pilots performing the simulations were made aware of the MCAS activation prior to the fact or were required to diagnose it themselves. The description states that "the [MCAS] function was allowed to perform to its authority and beyond before pilot action was taken to recover," [45] which appears to indicate that the test pilots were aware of MCAS's maximum authority and may thus have been anticipating the kind of response that would be needed to address the unintended activation.

In papers on Safety III [49] and the limitations of safety cases [50], Leveson describes how safety approaches that focus solely on identifying what must occur in order for a system to function *appropriately* could mislead an analyst and result in missed requirements for safe behavior. The report on the loss of a Royal Air Force Hawker Siddeley Nimrod in Afghanistan in 2006 [51] emphasizes this point by arguing that justifying that a system is safe rather than examining what hazards might render the system unsafe often results in a self-fulfilling prophecy.

The same thinking applies to human factors assessments of flight crew response. As was seen in the 737 MAX case, potentially catastrophic hazards may be missed if tests that are used to validate whether flight crews will appropriately and reliably respond to mitigate the severity of a failure condition do not consider and test the specific conditions that are most likely to lead flight crews *not* to respond in the appropriate manner. Worst-case analysis, which does not limit itself to considering what is expected and addresses the potential for unlikely events, is already present in other processes within ARP4761.

The separation of human factors and safety assessment, however, leads to unlikely events not being emphasized when examining flight crew response. The absence of a worst-case analysis approach is a common source of criticism of the safety case framework [52]. Testing flight crew response in worst-case conditions requires identifying what those conditions are, and that requires an additional hazard analysis of human-related hazards that is absent from ARP4761.

3.2.1.3. Existing Human Hazard Assessments

As described in the background section, considerations of flight crew response and prevention of flight crew error are covered under § 25.1302 and its associated means of compliance. However, certification requirements do not explicitly call for a human hazard analysis. The available guidance also does not support analysts in tracing decisions about human factors to unsafe situations at the aircraft level.

Instead, AC 25.1302-1 relies on the same approach of identifying the expected flight crew actions and whether they have been appropriately documented[9]. The expected flight crew response to MCAS activations *was* documented. What was not considered are all of the other *unexpected* responses (that actually occurred on the accident flights).

In 2023, in an attempt to bridge the gap between safety and human factors certification, EASA released a memorandum [53] that provides an updated framework for consideration of human response to failure in safety assessments. The process proposed by the memorandum is based around task analysis, and requires the analyst to ask several questions about how the flight crew is expected to respond to a failure[10]. Though more thorough than the guidance in the ARPs and in AC 25.1302-1, the process in the memorandum is still focused on documenting *expected* behavior. It does not provide a structured methodology for identifying situations in which the flight crew would not behave as expected.

---

[9] Section 5-3 of AC 25.1302-1 (about novel aircraft features and functions) requires the analyst to consider: "(1) Does each feature and function have a stated intent? (2) Are flightcrew tasks associated with the function described? (3) What assessments, decisions, and actions are flightcrew members expected to make based on information provided by the system?" [9]

[10] These questions require the analyst to consider the event itself, the crew's perception of the event, the crew's information processing, the crew's response, and the implications of the event after it has been managed. Additionally, the questions differ based on whether the particular event being analyzed is explicitly and unambiguously alerted to the crew or whether the crew must deduce the event from multiple indications or effects observed.

Additionally, expected behavior is not binary (i.e, the crew either behaves as expected or does not behave as expected). There may be situations in which the crew's initial response is expected, but they then deviate from that behavior over time. They may also oscillate between expected and unexpected responses at different decision points, for a variety of reasons. Limited guidance exists for identifying the sources of these types of responses.

For example, one of the questions in the memorandum's procedures requires the analyst to consider what logical pathway the crew is assumed to follow in order to diagnose what event has occurred. However, no question asks what other pathways may appear reasonable to a flight crew observing the same inputs, or why the crew may diverge from the expected pathway after initiating the diagnosis[11].

Other questions require the analyst to document what memory items are assumed to be used, what procedures/checklists are assumed to be followed, and how much time is to be spent detecting and responding to the event. Though important, answering such questions is not a systematic methodology for understanding why a flight crew might not carry out each of these tasks.

In one particular case, the memorandum makes an assumption of its own by not asking any questions at all. When considering the case where the flight crew is explicitly alerted to a failure, an analysis of the flight crew's information processing is deemed "not applicable since the crew is expected to directly go from the alert to the procedure/memory item" [53]. Any scenarios by which the crew may misinterpret an explicit alert, or make the conscious decision to follow a different procedure than prescribed, are thus not considered in the analysis.

In the ET302 case, the IAS Disagree light unambiguously pointed to the unreliable airspeed procedure. A multitude of other flight deck effects and procedures that needed to be followed at the same time led the flight crew to not even attempt to complete that procedure.

3.2.1.4. Summary

In summary, the separation of human factors and safety assessment limits analysts' ability to thoroughly examine and mitigate accident causes that stem from human interactions. To better predict causal pathways involving human action (or inaction), it will be necessary to incorporate human factors analysis into the safety assessment process beyond just confirming expected pilot behavior.

3.2.2. Absence of a systematic methodology that supports the identification of unrecognized assumptions

The next limitation involves the absence of a systematic methodology that supports the identification of unrecognized assumptions made during the safety assessment. As described in the previous section, ARP4761 calls for the documentation of all assumptions made throughout the safety assessment process. However, documentation of assumptions is a fundamentally different process than identification of assumptions, and little guidance is provided to ensure that engineers can identify the assumptions they unconsciously make during design or safety assessment.

---

[11] The counterfactual reasoning present in questions like "why did the crew not perform this action when they should have?" is common in accident investigations but, as noted by Dekker [54], stressing what was not done contributes little to understanding what was actually done, or why. Counterfactual reasoning is most helpful during hazard analysis, to understand and predict unexpected behavior before it happens.

3.2.2.1. Documentation vs. Identification of Assumptions

The definition of an assumption naturally implies some level of doubt about the validity of the assertion being made. A statement known to be factual may be still listed as a comment, observation, or reference material in a safety assessment process such as an FHA. Such statements may also be left undocumented, as they are widely understood to be true by those performing the assessment.

However, the distinction between a factual statement and an assumption is often unclear in early stages of development, which may pose challenges for maintaining appropriate documentation. In his work on assumption-based planning, Dewar [55] establishes a taxonomy that distinguishes between the assumptions that planners: a) are documenting; b) are not documenting but are consciously aware they are making; or c) are not consciously aware they are making at all. The first category is termed an *explicit* assumption, while the second and third category are termed *implicit* assumptions.

ARP4761 requires that all assumptions be made *explicit*. In the vernacular of the ARP, an assumption is defined as a statement, principle, or premise offered without proof. Documenting assumptions is a necessary step in any safety assessment—the details needed to fully understand a system's specifications, its operators' responsibilities, and its operational context may not be available from the start of the analysis.

ARP4754's "Management of Assumptions" sections even provides an overview of the types of assumptions that should be considered by the analyst, including operational/environmental assumptions, serviceability assumptions, installation assumptions, and design assumptions associated with crew interface, system interface, and reliability [10].

Note, however, that documentation of assumptions is a fundamentally different process than identification of assumptions. Though in an ideal world all safety-critical assumptions during aircraft development would be made explicit, assumptions may remain or become implicit for a variety of reasons. Fundamental assumptions that may have originally been documented could become ingrained in the common practice of a community, industry, or organization and become implicit when applied to new tasks or projects.

Additionally, and of crucial importance to safety assessment, recognition of implicit assumptions may be hindered by prior mental models that analysts have of their system, its operators, or its operational environment. It is these implicit assumptions that most need to be captured in safety assessments, as they represent a potentially unknown misalignment between the mental models of a system's designers or analysts and the real world in which the system will operate.

Ultimately, neither ARP4761 nor ARP4754 provide a robust and systematic procedure to facilitate the identification of implicit assumptions, beyond indicating the types of factors that should be considered when creating documentation. As is noted in [56], it is a common feature of many open standards to require that particular artifacts be generated, while giving the implementer of the standard freedom to utilize their own processes for generating them.

The ARPs rely on the subject matter expertise of analysts to ensure that the list of documented assumptions in the AFHA, SFHA, and other parts of the safety assessment is correct and complete. Though subject matter expertise is invaluable in the safety assessment process, appropriate guidance may help support the process for analysts with or without the resources and technical heritage of large manufacturers.

3.2.2.2. Implicit Assumption about MCAS' Behavior

During the MCAS design process, a number of implicit assumptions were made that affected design decisions. As described earlier, three key assumptions *were* documented by Boeing for use in their MCAS and stabilizer trim FHA. The two that are relevant for this example are the assumption that unintended stabilizer trim inputs are readily recognized, and the assumption that continuous unintended nose down stabilizer trim inputs would be recognized as a stabilizer runaway and the appropriate procedure would be followed [6].

These assumptions can be categorized as user interface assumptions, as they describe users of a system and their behavior [57]. However, these explicit user interface assumptions are actually associated with multiple undocumented system behavior assumptions that were likely made outside the safety assessment process and transmitted implicitly to the safety analysts.

Figure 10 below depicts the first page of the runaway stabilizer procedure from the 737 MAX Quick Reference Handbook (QRH) that was in use at the time of the JT610 accident.

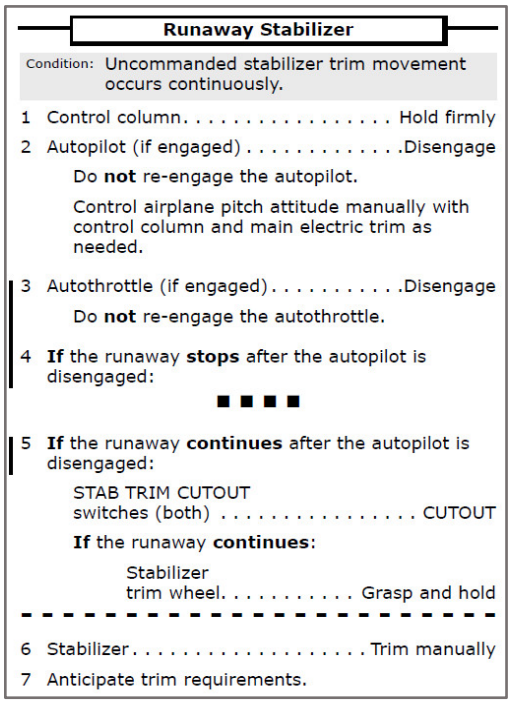


Figure 10. First page of the runaway stabilizer procedure from the 737 MAX QRH in use at the time of the JT610 accident [2]

In the cases of both JT610 and ET302, the flight crew was unable to appropriately diagnose the situation encountered and did not attempt to execute the runaway stabilizer checklist as prescribed, as discussed in the previous section. A detailed analysis of the flight crew's mental models of their situation and the contextual factors influencing their decisions can be found in the CAST results in Appendix A.

Setting aside the multitude of factors discussed previously, like flight deck effects and workload, an element of the system design can also be seen to have contributed to the crew's

response: the feedback observed from the aircraft upon the erroneous activation of MCAS did not align with the feedback that would be expected to trigger a runaway stabilizer procedure.

As stated in the QRH, the condition for performing the runaway procedure is uncommanded stabilizer trim movement occurring "*continuously.*" The reality is that MCAS activation does not result in continuous, but *intermittent* stabilizer trim movement[12]. The four black squares in the QRH indicate that the procedure is complete "if the runaway stops after the autopilot is disengaged," and the procedure only calls for the stabilizer trim cutout switches to be activated if the runaway continues.

Thus, had the flight crews followed the procedure as prescribed, they may have been misled into ending the procedure despite MCAS still being able to activate. Their mental model of the stabilizer runaway may have been updated incorrectly by the intermittent movements. This is compounded if we once again consider the high-workload environment with multiple (and conflicting) cockpit alarms sounding and other non-normal checklists being performed at the same time.

This discrepancy between the condition that would trigger the runaway stabilizer procedure and the actual conditions observed during an erroneous MCAS activation reveals a number of important implicit assumptions made during the design and safety assessment of the system. These include:

- That the stabilizer runaway procedure is the most appropriate response to erroneous MCAS activation
- That erroneous MCAS activation is physically equivalent (or nearly equivalent) to continuous unintended nose down stabilizer motion
- That erroneous MCAS activation is *observable* and *recognizable* as continuous unintended nose down stabilizer motion

None of these assumptions are documented in the FHA or any other Boeing documentation obtained in the aftermath of the accidents, but they follow from the system design and are baked into the procedures called for in the FHA. ARPs 4761 and 4754 would technically require that these assumptions be documented, and the fact that they were not reveals room for more structured guidance on identification of implicit assumptions.

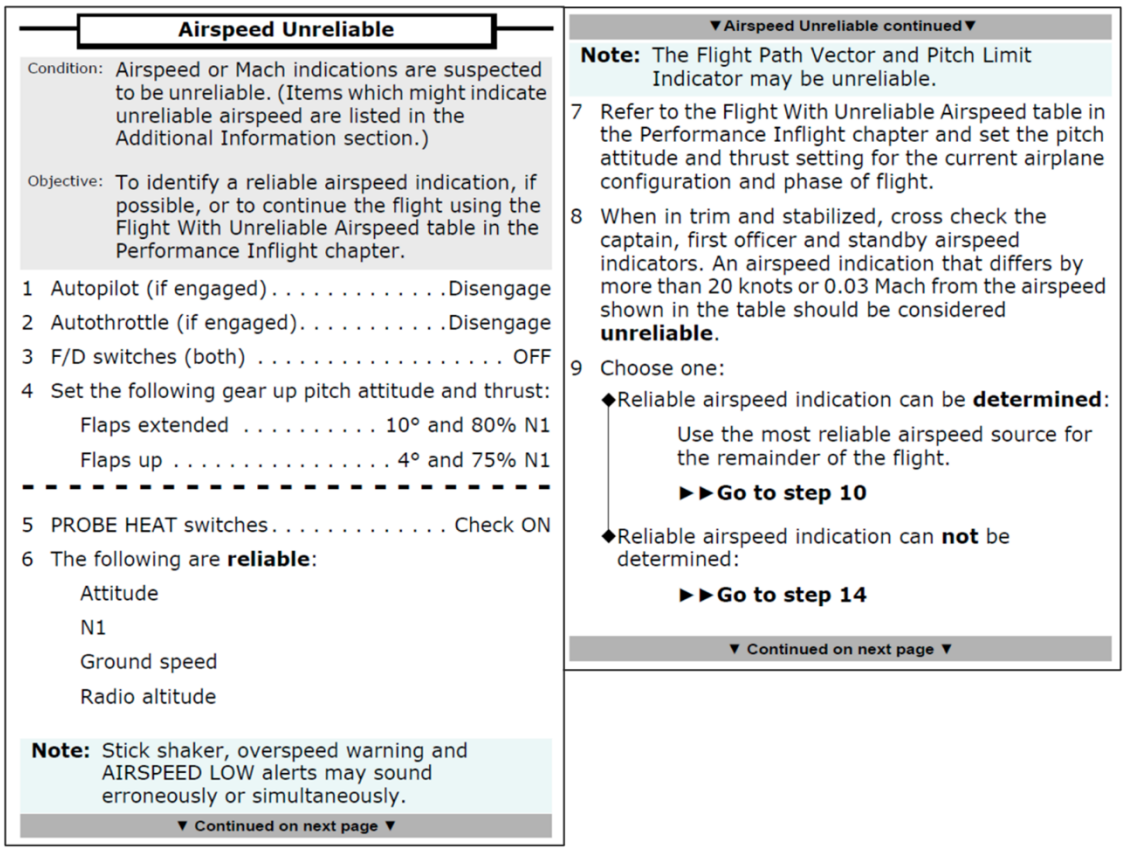
3.2.2.3. Implicit Assumption about Airspeed Unreliable Procedure

An additional implicit assumption is associated with the airspeed unreliable procedure that was meant to be followed upon observation of the IAS Disagree light. The first two pages of this procedure can be seen in Figure 11 below.

The flight crew of JT610 recognized the need for performing the airspeed unreliable procedure, but the procedure was never completed and the erroneous AOA data coming from the captain's sensor was never identified. The first officer's last mention of the airspeed unreliable procedure, as recorded in the cockpit voice recorder, was at step 7, which requires the crew to consult values from a table in the QRH according to their current pitch attitude and thrust setting. Step 8 of the

[12] Each individual MCAS command is bounded by a 2.5º authority and will halt upon receiving any manual electric trim inputs by the flight crew. After halting, MCAS will not activate for 5 seconds, and may then issue another stabilizer trim command that is also bounded by the system's authority.

procedure then requires the aircraft to be "in trim and stabilized" before it becomes possible to diagnose which airspeed indications are unreliable.



Airspeed Unreliable

Condition: Airspeed or Mach indications are suspected to be unreliable. (Items which might indicate unreliable airspeed are listed in the Additional Information section.)

Objective: To identify a reliable airspeed indication, if possible, or to continue the flight using the Flight With Unreliable Airspeed table in the Performance Inflight chapter.

1 Autopilot (if engaged) . . . . . .Disengage
2 Autothrottle (if engaged) . . . . . .Disengage
3 F/D switches (both) . . . . . OFF
4 Set the following gear up pitch attitude and thrust:
Flaps extended . . . . . 10° and 80% N1
Flaps up . . . . . 4° and 75% N1
5 PROBE HEAT switches . . . . . Check ON
6 The following are **reliable**:
Attitude
N1
Ground speed
Radio altitude

Note: Stick shaker, overspeed warning and AIRSPEED LOW alerts may sound erroneously or simultaneously.

▼ Continued on next page ▼

▼Airspeed Unreliable continued▼

Note: The Flight Path Vector and Pitch Limit Indicator may be unreliable.

7 Refer to the Flight With Unreliable Airspeed table in the Performance Inflight chapter and set the pitch attitude and thrust setting for the current airplane configuration and phase of flight.

8 When in trim and stabilized, cross check the captain, first officer and standby airspeed indicators. An airspeed indication that differs by more than 20 knots or 0.03 Mach from the airspeed shown in the table should be considered **unreliable**.

9 Choose one:

◆Reliable airspeed indication can be **determined**:
Use the most reliable airspeed source for the remainder of the flight.
►►**Go to step 10**

◆Reliable airspeed indication can **not** be determined:
►►**Go to step 14**

▼ Continued on next page ▼

Figure 11. First two pages of the airspeed unreliable procedure from the 737 MAX Quick Reference Handbook (QRH) in use at the time of the JT610 accident [2]

The assumption here is that the aircraft will always be able to be maneuvered into stable enough configuration to execute the steps of the checklist. This assumption may have been true for other versions of the Boeing 737, but MCAS introduces a new source of perturbations in trim and pitch attitude in the exact situation that the airspeed unreliable procedure needs to be performed.

Because the details of the FHA for erroneous AOA are not publicly available, it is impossible to say for certain whether this assumption was documented or not. However, the absence of any mention in the flight crew training manual (FCTM) of the possibility of not being able to stabilize or trim the aircraft indicates that this scenario may not have been documented or otherwise identified. This omission once again reveals the need for an improved process of identifying unrecognized assumptions.

3.2.2.4. Counterarguments

A common counterargument to the procedure examples provided above is the fact that flight crew *could* still have diagnosed that the airspeed was unreliable or that uncommanded stabilizer motions were occurring, and performed the appropriate procedures. Despite the misleading

feedback from intermittent MCAS activations, the crews *could* have noticed that mistrim was accumulating, and that *could* have triggered them to follow the runaway procedure.

In fact, the crew in command of flight JT043, which operated the same aircraft involved in the JT610 accident, performed the airspeed unreliable and runaway stabilizer procedures upon observing the IAS Disagree light and three instances of automatic ND trim along with a heavy control column.

However, implicit in this counterargument is yet another unrecognized assumption that often accompanies the explicit human response assumptions documented in FHAs: that flight crews will behave in a uniform, pre-determined manner in response to the failure conditions they encounter.

To understand this point, it is helpful to analyze the response of the crews of JT043, JT610 and ET302 to the erroneous MCAS activations they observed. In all three flights, the Primary Flight Display (PFD) indicated an IAS Disagree warning and the stick shaker activated within seconds of rotation. On JT043, the captain immediately noticed the IAS Disagree warning and performed the airspeed unreliable checklist. After completing the checklist, advising the FO to retrim the aircraft as needed, and declaring an urgency message, the captain recognized repeated stabilizer movement without crew input and subsequently performed the runaway stabilizer procedure as prescribed [2].

The responses on JT610 and ET302 were very different, as shown earlier in the CAST excerpts in Tables III and IV. Neither crew completed the unreliable airspeed procedure, which posed a challenge for them to gain awareness of the condition of their aircraft. The crew of both accident flights did appear to be aware of repeated aircraft-nose-down trim activations. However, each pilot responded very differently to the activations they observed.

The captain of JT610 fully countered a majority of the MCAS activations with manual electric aircraft-nose-up commands, while the first officer of JT610 did not do so, and instead relied on using the control column. The captain of ET302 first relied on engaging the autopilot to prevent MCAS from activating, then partially countered some activations, and finally engaged the stab trim cutout switch.

The CAST results make it clear that the implicit assumption that flight crews will behave in a uniform, pre-determined manner to failure conditions is false. This provides even stronger evidence that the ARPs could benefit from additional guidance when identifying the implicit assumptions being made about system design and human response.

3.2.2.5. Summary

In summary, the ARP4761 process does require that all assumptions be documented but does not provide the necessary guidance to support the analyst in questioning what they believe to be true about their system. More structured methodologies are needed to help designers and analysts identify the assumptions they do not realize they are making.

3.2.3. A failure-centric safety assessment process with limited guidance for uncovering and managing non-failure based causal scenarios leading to losses

The third limitation centers around the failure-driven nature of the safety assessment process. There is currently limited guidance within the standards for identifying the specific scenarios leading to losses that are not caused by component failures. Causal factors like design errors are intentionally outside the scope of ARP4761, and are treated separately in ARP4754, but there is

limited guidance for specifically uncovering the errors (e.g., flawed software requirements) that have the potential for catastrophic consequences. Additionally, though the standards recognize that probabilistic judgment is not suitable for capturing all types of causal factors, the standards could use additional guidance for generating and validating non-probabilistic safety requirements.

3.2.3.1. Design Errors and Missing Requirements

The hazards that are identified in the AFHA and SFHA steps of ARP4761 are categorized as either losses of function or malfunctions[13]. However, the need to frame the hazard analysis within the confines of losses of function and malfunctions limits the safety analyst's ability to consider all types of scenarios that can lead to accidents, especially when a function's behavior as designed is unsafe.

A function performing as intended does not necessarily equate to performing safely [16,36,58]. This distinction is particularly relevant for software-implemented functions like MCAS. The function's intended behavior is derived from the requirements, but those requirements may be incorrect or incomplete.

Deterministic software only executes the commands it is programmed to execute. Therefore, a software function operating differently than desired can only occur if the function's original intent as written in the software requirements is not safe in all operational conditions, or the requirements are implemented incorrectly. Neither of these cases are *failures* as defined and used in ARP4761, so their analysis may be delegated to the ARP4754 processes or the case may be documented and analyzed as if it were a failure.

As an example, consider some of the "failure conditions" identified during the MCAS SFHA in Table VII. Uncommanded MCAS function, uncommanded MCAS operation to maximum authority, and uncommanded MCAS operation equivalent to 3 second stabilizer trim runaway are all in fact instances of the software function behaving as designed, but in a situation where the function was not needed or not safe.

Using the word "uncommanded" to refer to the MCAS activations does not accurately represent the nature of the conditions being analyzed. Barring a hardware failure in the FCC or spurious signal in the avionics wiring, all MCAS activations are *commanded*, regardless of whether the command results from the triggers intended in the requirements specification or from other triggers not considered.

Treating *undesired* or *unsafe* MCAS activations as "uncommanded" leads the analyst to only consider what might cause MCAS to activate without receiving a command (e.g., through a wiring failure), and not to consider the cases where MCAS receives a command to activate that was misguided or unsafe for some reason. Treating "uncommanded action" as a failure or malfunction is not unique to MCAS, but figures extensively in the SFHA guidance within ARP4761, with no mention of these limitations when considering software-implemented functions. To truly ensure a software function is safe, it is necessary to ensure that the safety of that function's behavior is validated even if the behavior is commanded and intended.

It is true that the development assurance process outlined in ARP4754 already provides a means for capturing and eliminating design errors. ARP4754 requires validation of correctness and completeness of requirements. Additionally, ARP4754 requires that functions and items be

[13] A loss of function means a function cannot be performed, either partially or totally. A malfunction is defined as a condition where a function's operation is different than intended.

assigned development assurance levels (FDALs and IDALs)[14]. Development assurance levels are meant to provide confidence that the appropriate level of rigor or discipline was followed when developing a function or item, to lower the chance of design errors existing [10].

However, ARP4754 does not define specific, detailed processes for uncovering design errors. Where ARP4761 includes specific, step-by-step, processes for mitigating failure-based causal scenarios, ARP4754 only defines the *need* for certain processes, (e.g., requirements creation, requirements validation, etc.) and leaves it up to the implementer to determine how to best carry them out.

For instance, the "Requirements Validation" section of ARP4754 indicates that "the format of the validation effort is left to the developer," but that "a structured process should be defined in the validation plan" [10]. The standard then provides generic sets of questions to prevent design errors in the "Correctness Checks" and "Completeness Checks" subsections. These questions are helpful and may guide an analyst with subject matter expertise to identify and document requirement gaps, but are not a step-by-step process to interrogate and challenge what the analyst believes to be true about their system.

As ARP4754 itself states, one of the objectives of validation is to "limit the potential for unintended behavior in the system." [10] Satisfying this objective requires identifying the *specific* scenarios leading the system, as designed and as specified, to not achieve the intended goals. Though the standard does not need to *require* specific analytical tools for requirements validation (and other steps of the process), analysts could benefit from more structured methodologies that support it[15].

In fact, a number of missing requirements for the MCAS function reveal room for improvement in the process for preventing design errors. Based on the severity classification of MCAS' failure conditions, its development assurance level would at least require that the system requirements be correct and complete, including identifying and addressing unintended behaviors. However, on its own the assignment of development assurance levels only ensures that a certain level of rigor is applied when designing the system. It does not ensure that the output of the requirements validation step will be correct and complete. Though the outputs may be affected by the level of rigor at which the analysis is performed, it is the types of analyses performed that will have the larger effect on ensuring correctness and completeness.

Ultimately, several requirements that would have made MCAS a safer function were missed during the development process, like the requirement that MCAS rely on more than one AOA sensor, and the requirement that MCAS could be disengaged without removing access to manual electric trim.

Lastly, one particularly challenging category of design errors to identify are cases where the intended behavior of each individual function is safe, but the interactions between the behavior of multiple functions becomes unsafe. There may be cases where two functions behaving as intended

---

[14] As a reminder, FDALs and IDALs range from A (high rigor) to E (low rigor). Assigning a higher FDAL or IDAL to a function or item indicates that more rigor was applied when designing that function or item. For example, a function assigned FDAL A, B, or C needs to have traceability of its requirements to specific rationales, while that is negotiable for FDAL D and not required for FDAL E.

[15] To achieve the goal of limiting unintended behavior, ARP4754 does propose that operational and maintenance scenarios for normal and abnormal situations be generated to identify missing requirements [10]. However, the methods specified in the standard to be used —state diagrams and timeline diagrams—are ways of documenting scenarios, not step-by-step processes for analyzing the system to identify the scenarios (i.e., misalignments between specification and intent).

at the same time is unsafe, or cases where one function's intended behavior only becomes unsafe when another unrelated function has failed.

The impact of analyzing failures through one process (ARP4761) and design errors through a separate process (ARP4754) is that uncovering cases where combinations of failures and errors have catastrophic consequences becomes challenging. For instance, though the AFHA/SFHA is meant to examine losses of function and malfunctions in particular contexts (e.g., phases of flight and environment), those contexts do not typically include normal, prescribed behavior of other functions. The fact that the safety assessment relies on functional decomposition and the hazards associated with each function are examined in silos, rather than as an integrated system, also makes it difficult to identify unsafe interactions among unrelated functions.

3.2.3.2. Overreliance on Probabilistic Requirements

As described in the ARP4761 overview in Chapter 2, the purpose of classifying failure conditions into severity bins is to associate each condition with a probabilistic safety requirement. These requirements are typically of the form, "The probability of uncommanded operation of function X during surface movement shall be less than Y per flight hour." Although this phrasing is common, it is easily misunderstood. This kind of ARP4761 probabilistic requirement does not (and is not intended to) constrain all causes of uncommanded operation. Such requirements only apply to potential causes that consist entirely of failures, not potential causes involving errors or combinations of errors and failures. Despite the common phrasing above, these requirements do not imply or guarantee that uncommanded operation in general (regardless of the cause) will be within the stated probability or frequency.

The subsequent steps of the ARP4761 process evaluate the proposed architecture to provide a quantitative reasoning that the probabilistic requirement is met, usually through fault tree analysis. However, FTA is a tool rooted in reliability analysis. When applied quantitatively, it supports the analyst in quantifying the probability of component failures. The probability thresholds assigned to each severity class were derived based on reliability statistics of commercial air transport accidents, and the logic behind the procedures for combining probabilities was designed only for reliability items. Aspects relating to operator behavior, operational context, maintenance error, or manufacturing error are not typically considered in these quantitative analyses, because obtaining a meaningful probability for them is infeasible. In addition, it is not possible to identify the probability of software doing something unsafe, as noted directly in ARP4761, so that aspect is covered in ARP4754[16].

FTA does not explicitly assume zero probability for causal factors that are not captured in the fault tree. However, like the example probabilistic requirement above, the results of an FTA can also be easily misunderstood as providing claims or proofs that the general probability for catastrophic conditions is below the required threshold. FTA only claims that the probability of the top-level event being caused by component failures is that low and does not make claims about the probability of other contributions. This interpretation may not be appropriately communicated to management or other stakeholders making decisions about the system.

---

[16] ARP4761 does allow design errors to be expressed in a fault tree alongside failures, but the impact of these errors on the fault tree results is minimal, as the probability of design errors is not quantifiable and there is no process to identify the specific errors to be considered.

Many of the factors that are not easily quantifiable are either introduced as qualitative aspects of the analysis that have limited bearing on meeting the safety requirement, or are excluded from the analysis under the assumption that they will uniformly adhere to a predicated norm (e.g., maintenance will follow procedures, the aircraft will be manufactured according to design, etc.).

The Common Mode Analysis (CMA) in ARP4761 is meant to qualitatively consider how aspects like software error, pilot training, or manufacturing defects can invalidate logic in the FTA (e.g., increase the resulting probability of two events connected by an "and" gate, compared to the simple multiplication of the events' probability). However, CMA typically relies on tailoring generic sets of questions to identify causal factors, like "Could independence be affected by a common failure of software specification?" [13]. CMA does not provide a step-by-step methodology for uncovering how aspects like specific software specification flaws or maintenance errors may arise and affect the safety of the aircraft.

In the Boeing 737 MAX case, no fault tree was constructed for any of the MCAS-related failure conditions identified during the SFHA[17]. The only recorded mention of MCAS within a 737 MAX fault tree is as a bottom-level node in the tree whose top-level event is "Autoflight malfunction at low altitude which results in an unsafe flight path in an autopilot OFF, single channel or fail passive configuration." A partial representation of this fault tree is depicted below in Figure 12, based on information contained in the JT610 final report [2]:

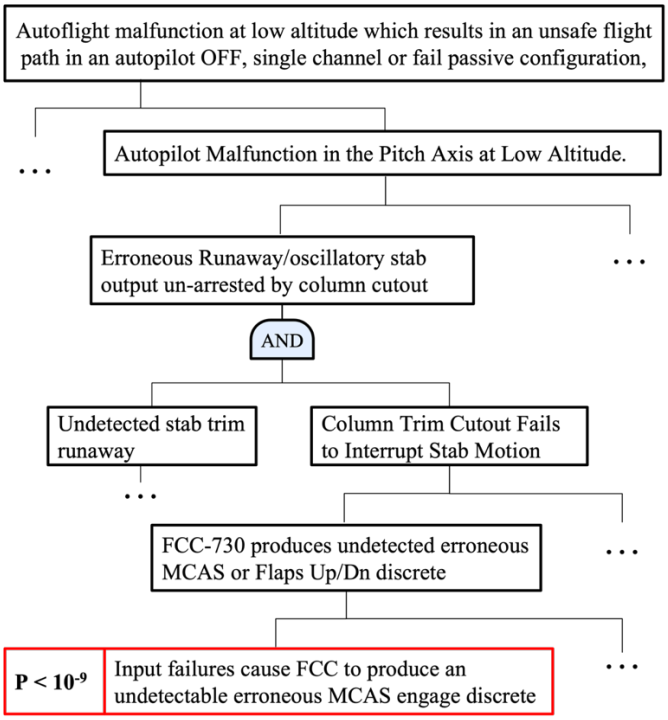


Figure 12. Partial 737 MAX fault tree for "Autoflight malfunction at low altitude which results in an unsafe flight path in an autopilot OFF, single channel or fail passive configuration"

[17] All MCAS failure conditions were assigned a severity of minor or major (barring one case that will be discussed in the next section) and therefore did not require a dedicated FTA

The JT610 report notes that the node "FCC-730 produces undetected erroneous MCAS of Flaps Up/Dn discrete" is what first generated a requirement constraining the probability of an erroneous MCAS activation. The bottom-level event of the fault tree indicated that the probability of "input failures" leading the FCC to produce an erroneous MCAS command was under 10^{-9} [2], so the safety requirement of preventing MCAS activations was deemed satisfied. No justification is provided for the validity of this probabilistic assessment. Additionally, as [46] accurately points out, this bottom node does not protect against the FCC producing an MCAS command because of misleading data. It only protects against failures in the FCC's own hardware producing an erroneous command.

What goes unaddressed in every discussion of the 737 MAX fault trees is the fact that fault trees, as a model, lack a framework to capture the kinds of causal factors that led to the MCAS activations onboard JT610 and ET302. As became clear in the aftermath of the accidents, hardware failures in the FCC are not the only causal factor that can lead MCAS to activate erroneously.

As a software-implemented control law that activates based on angle of attack, Mach number, autopilot status, and flap position, misleading data from any of these sources can cause MCAS to activate. None of these factors were ever associated with MCAS-related events in the 737 MAX fault trees. Even if they were, determining an exact probability for misleading angle of attack data is difficult because so many sources of misleading AOA are not actual reliability failures.

In fact, Boeing did construct a fault tree for "Misleading Air Data from the Left and Right ADIRU – Airspeed / Altitude", which can be seen in Figure 13.

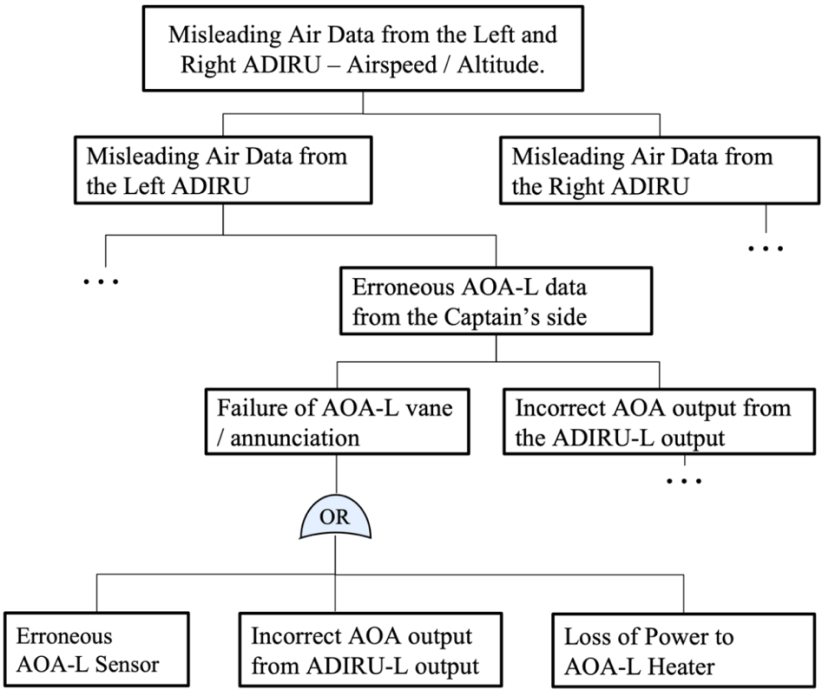


Figure 13. Partial 737 MAX fault tree for "Misleading Air Data from the Left and Right ADIRU – Airspeed / Altitude" [2]

Examining the bottom-level events that can cause the "misleading air data" condition reveals the limited scope of causal factors that fault trees can uncover. Though the probability assigned to "Erroneous AOA-L Sensor" was not documented in the JT610 report, this value likely originated

from the failure rate provided by the sensor supplier. This reliability metric may provide an accurate estimate for the rate of random hardware failures of the AOA sensor, but other non-random factors that lead to erroneous AOA data are not captured in that number.

The JT610 report stated that the AOA sensor installed on the Indonesian aircraft had been mis-calibrated during a repair [2]. The NTSB response to the ET302 accident report concluded that the Ethiopian aircraft's AOA sensor vane had most likely been separated from the aircraft by impact with a foreign object such as a bird [43], a well-documented problem at Addis Ababa Bole Airport [59]. Neither of these cases are random reliability failures.

A search on the Aviation Safety Reporting System (ASRS) database reveals a number of other incidents from the Boeing 737 Classic and Next Generation models in which the stick shaker or IAS Disagree flags activated as a result of misleading AOA sensor data. Reports included AOA vanes cracked by ladders and ladder stands during maintenance [report number 1683964, 1869908], tape residue stuck to an AOA vane [report number 1224941], bird strikes [report number 1897807, 1871513] and bent or broken AOA vanes for undetermined reasons [report number 1337942, 880257].

None of these factors were included in the "misleading data" fault tree because, as nonrandom failures, it is impossible to obtain meaningful probabilities for their occurrence. However, this does not mean that these factors do not directly affect the probability of the top-level condition. Without an appropriate methodology for integrating qualitative results into the quantitative analysis, it can be challenging to identify cases where a combination of non-failure related causal factors invalidate the design with respect to its quantitative safety requirements. Once again, though FTA does not explicitly assume zero probability for causal factors that are not captured in the fault tree, the assumptions that underly the precise number quantifying the likelihood of a catastrophic condition may not be appropriately communicated to management or other stakeholders.

One could argue that it should not fall upon the safety assessment to ensure that maintenance teams, manufacturing teams, or other stakeholders adhere to the norms prescribed to them. This is a valid point, but it does not preclude the safety assessment from considering how non-adherence can impact the hazards identified. By excluding non-failure related causal factors, analysts can miss an opportunity for recommending or requiring additional protections in the system design that may not be difficult to implement. There is a further disincentive towards introducing new safety measures when the number obtained from the reliability analysis provides the analyst with a false sense that safety has been assured, despite the limited types of causal factors considered.

Consider another example from the 737 MAX safety assessment. The "Angle of Attack Failure" section of the system safety assessment only discusses (and protects against) AOA sensor failures related to the AOA resolver circuit. When these failures occur, any parameters computed using AOA data are outputted as "No Computed Data" [2]. However, this analysis only captures failures in the electrical circuitry that processes the AOA signal, not misleading data from the AOA sensor itself.

Misleading data from the sensor could clearly originate from non-failure sources, and the effects can be just as safety critical as misleading data from circuit failure. Excluding these sources from the safety assessment is a missed opportunity for introducing stronger design mitigations. Misleading data from other, potentially undetected causes was assigned the probability of $<10^{-5}$ for a single sensor and $<10^{-9}$ for both sensors based on the fault tree in Figure 4, further reinforcing the belief that safety has been assured, despite the exclusion of important causal factors.

3.2.3.3. Summary

The ARP4761 process supports the analyst in identifying how reliability failures contribute to aircraft-level losses, but could use additional guidance for considering non-failure related scenarios like design errors, missing requirements, and other external factors. The overreliance on probabilistic safety requirements limits analysts' ability to consider all kinds of causal factors that lead to accidents.

3.2.4. A limited framework for understanding nonlinear causal relationships between functional failure conditions and operational events/conditions

The fourth limitation identified involves the ability to capture complex causal relationships that do not fit neatly into a linear cause-and-effect model (i.e., event A causes event B, where B has no real effect on A in return). Without the ability to model and understand different types of causality, it can be challenging to identify whether certain operational events or conditions are truly independent from certain hazards.

3.2.4.1. Operational Events and Conditions in ARP4761

When constructing an FHA table for a function, the same failure condition may appear repeatedly, modified by different factors, which include: flight phase (e.g., taxi, takeoff, cruise), environmental conditions (e.g., airfield temperature, visibility), environmental events (e.g., windshear), and an additional set of factors termed operational conditions and events [13].

Operational conditions are specific aircraft parameters such as weight, speed, and altitude, which may be directly related to the phase of flight being considered. Operational events are "occurrences and flight operations" that happen at a distinct time, have a known statistical probability based on fleet or industry-wide rates of occurrence, and are not expected to be experienced frequently during an aircraft's service life. Example operational events in ARP4761 include rejected takeoffs, in-flight diversions, or baggage compartment fires [13].

The standard indicates that operational conditions "should be considered at their worst-case limits" [13] within the phase of flight being considered, meaning that a failure condition whose severity is affected by a factor like airspeed should be analyzed at the worst possible airspeed and under the worst possible conditions.

Similarly, operational events are added to the relevant failure condition statements and the effects/severity of the failure conditions are analyzed with and without the operational event. The standard notes that operational events must be verified to be independent from the original failure condition. [13] Here lies the gap: a systematic methodology is not provided to help identify the causal relationships that exist between failure conditions and operational events/conditions.

Functions of modern commercial aircraft are typically quite complex, and the causal relationships between system behavior and operational conditions are not always obvious without a method that facilitates uncovering them. For example, it is clear that the severity of the loss of oxygen masks is increased if there is a fire onboard the aircraft. However, it may not be immediately clear whether there is a causal relationship in the opposite direction as well. Could a fire cause the loss of oxygen masks? If it is assumed that every causal relationship is straightforward and linear, then the subsequent assumptions of independence between operational events/conditions and hazards may be incorrect.

There are methods within ARP4761 that are meant to generate independence requirements and ensure that such independence actually exists between functions, systems, and items. However, this assessment occurs during the PASA and PSSA steps, which come *after* the severity classification assignment during the AFHA and SFHA. No methodology is provided to identify, at the time of the hazard analysis, whether the hazard is itself independent from the operational conditions that exacerbate it.

3.2.4.2. Independence of Operational Conditions involving MCAS

Examining the operational events/conditions that modify the failure conditions identified during the MCAS SFHA provides a valuable case study of nonlinear causality that is not emphasized by the current safety assessment process.

For context, FAA AC 25-7C [60] defines three flight envelopes for use in determining acceptable aircraft handling qualities. These envelopes are based on measurements of several flight parameters, including speed, load factor, angle of attack, pitch attitude, roll attitude, side-slip angle, altitude and presence of buffet. A detailed definition of each envelope is found in Appendix 5 of AC 25-7C [60]. In essence, the normal flight envelope encompasses routine or prescribed flight conditions, the operational flight envelope encompasses the first onset of warnings for each of the key parameters mentioned above, and the limit flight envelope encompasses the aircraft's design limits or electronic flight control system protection limits. Figure 14 shows a simplified representation of the thresholds between the different flight envelopes for a few parameters. A full description is available in AC 25-7C [60].

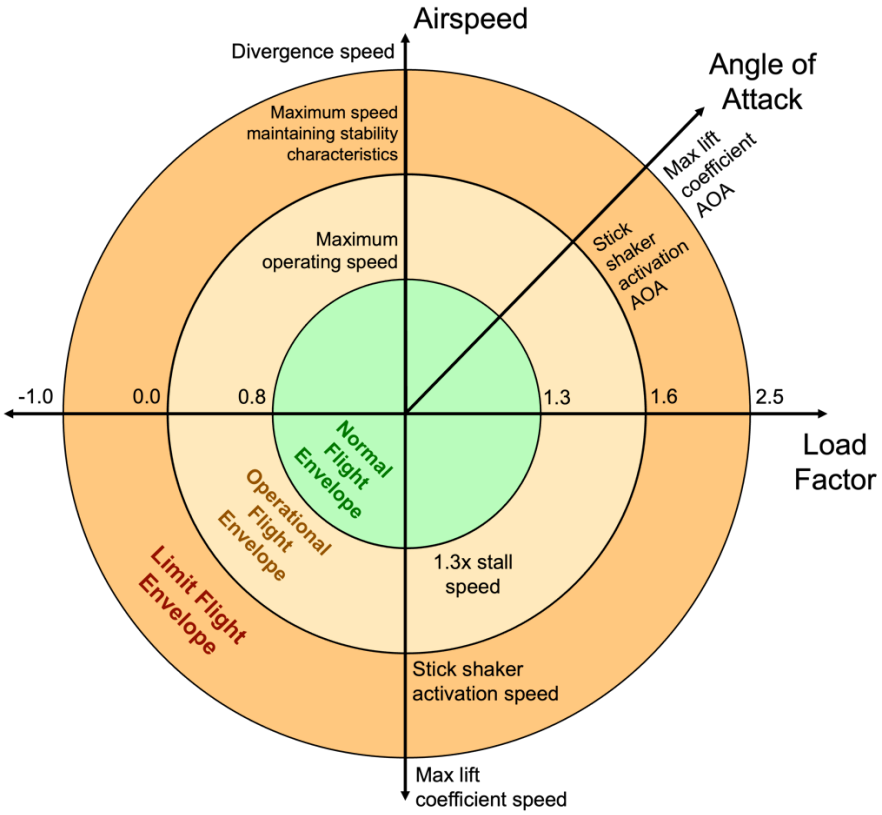


Figure 14. Simplified representation of different flight envelopes according to AC 25-7C.

AC 25-7C's probability of occurrence guidelines indicate the following probabilities for being in each flight envelope during a given flight hour:

Table VIII. Probabilities of Occurrence for each Flight Envelope according to FAA AC 25-7C

Flight Envelope	Probability of Occurrence
Normal	10^{0}
Operational	10^{-3}
Limit	10^{-5}

The failure conditions from the MCAS SFHA (seen in Table VII) utilize the normal and operational flight envelopes as operational events or conditions that modify them. The FHA indicates that uncommanded MCAS activations up to its maximum authority or equivalent to a 3-second stabilizer runaway were both assigned the severity of "Major" in the normal flight envelope. However, in the operational flight envelope, any uncommanded MCAS activation was assigned the higher severity of "Hazardous".

This severity classification assignment would indicate that, in the normal flight envelope, the acceptable probability for an undesired MCAS activation would be 10^{-5}, while in the operational flight envelope, the acceptable probability would be 10^{-7}. The operational flight envelope is typically seen as approaching an unsafe condition in which the aircraft is outside its allowable envelope and less able to be controlled, which may have informed the higher severity classification.

Per guidance in FAA AC 25.1309-1A [5], a "detailed safety analysis" must be conducted for all failures categorized as hazardous or catastrophic. This is meant to ensure the average probability per flight hour for each failure is lower than the acceptable probability for the severity class. The general limitations of failure-based probabilistic assessment were discussed in the prior section, so that will be set aside for this discussion.

Ultimately, a flawed independence relationship allowed Boeing to treat the severity of an MCAS activation in the operational flight envelope as only "Major", avoiding the need to perform a more detailed assessment to identify and protect against the potential causes of the erroneous activation.

To highlight how this probabilistic reasoning was likely conducted and to understand the independence relationship, it is helpful to denote the events of erroneous MCAS activation and the different flight enveloped by mathematical symbols, as follows:

- **Event *A***: Erroneous MCAS activation
- **Event *N***: Aircraft is in normal flight envelope
- **Event *X***: Aircraft is in operational flight envelope

A Venn diagram visualization of these events with their associated probabilities is seen in Figure 15. A similar visualization is presented in [46].

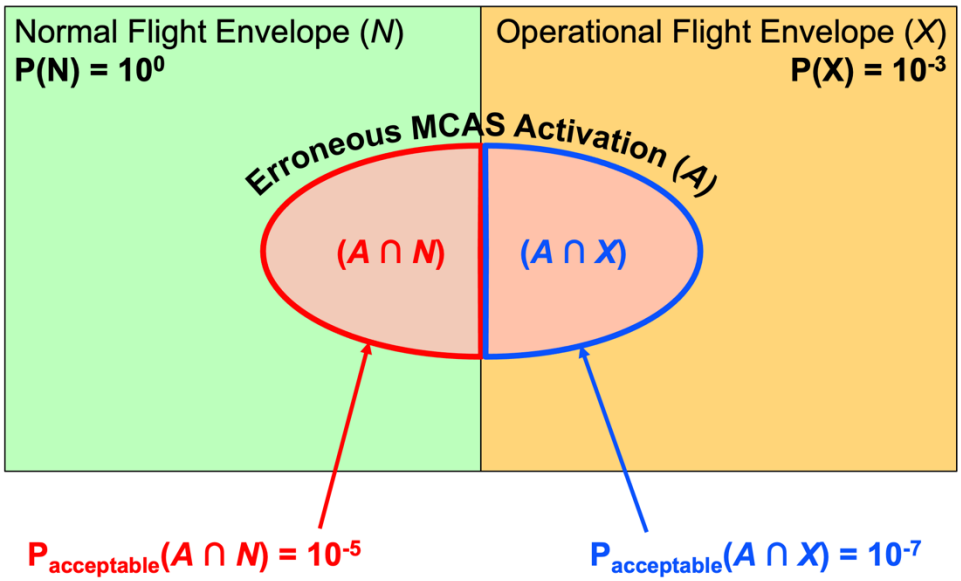


Figure 15. Venn diagram representation of erroneous MCAS activation in different flight envelopes

Knowing that uncommanded MCAS activation (event A) is classified as hazardous when the aircraft is in the operational flight envelope (event X), guidance from AMC 25.1309 dictates that the acceptable probability of uncommanded MCAS activation in that situation must be 10^{-7}, or:

$$P_{acceptable}(A \cap X) = 10^{-7} \tag{1}$$

The subscript *acceptable* is included in this equation to indicate this is a probability target that must be reached, not an actual probability.

Guidance from FAA AC 25-7C Appendix 5 gives the general probability of being in the operational flight envelope (event X) as 10^{-3}, or:

$$P(X) = 10^{-3} \tag{2}$$

The operational flight envelope is a condition whose probability is given in FAA AC 25-7C, so $P(X)$ does not have the *acceptable* subscript. Though the validity of such a value is questionable in itself, the more critical flaw arose when Boeing engineers made the assumption that an erroneous MCAS activation and being in the operational flight envelope are independent. Under that assumption, the following equation holds:

$$P_{acceptable}(A \cap X) = P_{acceptable}(A) * P(X) \tag{3}$$

Rearranging equation (3) and replacing known variables with the values from equations (1) and (2) yields:

$$P_{acceptable}(A) = \frac{P_{acceptable}(A \cap X)}{P(X)} = \frac{10^{-7}}{10^{-3}} = \mathbf{10^{-4}} \tag{4}$$

This reasoning results in the conclusion that the acceptable probability for an erroneous MCAS activation is $\mathbf{10^{-4}}$, which is less restrictive than the probability requirement for events of "major" severity. As a result, Boeing made the decision that a more detailed hazard assessment to identify and protect against the causes of erroneous MCAS activation was not necessary.

The reality is that an erroneous MCAS activation would result in a sudden nose-down pitching moment applied to the aircraft by the stabilizer trim system. This pitch-down directly affects the aircraft's angle of attack and pitch attitude, and, through coupling, may affect the aircraft's airspeed and load factor, among other parameters. Equation (3) does not hold, because the probability of event *X* increases as soon as event *A* occurs, due to the change in aircraft orientation that would ensue from an erroneous MCAS activation. Thus, the operational event associated with the failure condition is not truly independent of the latter.

As Lemme [46] and the JATR report on JT610 [29] appropriately note, the procedure of taking probability credits based on flight envelopes is not recommended in ARP4761, nor is it standard practice for complying with § 25.1309. The probabilities in AC 25-7C are meant to be used in selecting flight test cases to evaluate aircraft handling qualities, not in supporting the quantitative analysis called for in ARP4761.

However, the flawed independence reasoning observed in this example is not a result of the nonstandard procedure. It is only a factor that allowed the nonstandard procedure to be applied as it was. Even if the probability discount had not been applied and erroneous MCAS activations had been treated as "hazardous," the flawed independence relationship would likely still have obscured the true severity of erroneous MCAS activations.

Had the analysts realized that MCAS itself could place the aircraft in the operational condition that makes an erroneous MCAS activation more severe, more attention may have been given to the case of repeated activations. However, uncovering this flawed independence relationship requires identifying the circular and reinforcing causal loop that exists between the MCAS command and the operational condition. Particularly when the non-linear causal relationship occurs across the physical system's boundary (e.g., between system and environment, the system and its operators, etc.), it can be challenging to uncover the relationship without a more wide-ranging analysis that does not exclude external factors.

Without significant guidance from the standard for considering non-linear causal pathways, their identification depends on the experience and insight of qualified engineers. Once again, subject matter expertise is crucial for any safety assessment process, but additional procedural support can stand to benefit analysts or companies without decades of technical heritage.

3.2.4.3. Summary

The hazard analysis methods in ARP4761 are based on chain-of-event models of accident causality that make it challenging to identify causal relationships that are non-linear (e.g., circular causality where an event has an effect, and that effect continuously reinforces the original event). To better understand independence relationships between hazards and operational conditions, the safety assessment process needs methodologies that can capture complex non-linear relationships.

Chapter 4

Addressing the Limitations through a System-Theoretic Approach

This chapter presents a discussion of how a system-theoretic approach to safety assessment can help mitigate the limitations identified in the previous chapter. First, a case study is introduced that applies STPA to MCAS and its associated systems to identify the kinds of additional causal factors that a system-theoretic approach may help uncover. The rest of this chapter mirrors chapter 3, focusing on the four specific limitations identified earlier and exploring how STPA can support an analyst in the facets of safety assessment for which there is limited guidance in the standards.

The goal of this chapter is not to provide a new, comprehensive methodology for assessing the safety of and certifying commercial aircraft. However, opportunities to incorporate STPA and other system-theoretic approaches into the existing safety assessment process are discussed when appropriate.

It is important to recognize that the STPA case study presented here was conducted after the 737 MAX accidents. It is therefore subject to the unavoidable hindsight bias that comes from being aware of the causal factors that led to the accidents. However, the case study still provides valuable insight into the kinds of causal factors emphasized by the STPA framework and how they differ from those captured in a traditional safety assessment. The STPA also uncovered several scenarios that are unique and did not occur during the accidents, but could have occurred. The full STPA results can be found in Appendix B.

4.1. Overview of STPA Results

4.1.1. Purpose of the Analysis – System Boundary, Losses, Hazards, and Safety Constraints

The first step of STPA involves defining the purpose of the analysis, which includes setting the boundary of the system being analyzed. STPA can be performed at multiple stages of development and at multiple levels of abstraction, including above the "aircraft level" outlined in ARP4761. Though this case example focuses on MCAS and conducts STPA at a similar level of abstraction to the SFHA, the "system" that is used to define the system-level losses and hazards is still the entire 737 MAX aircraft. Also included within the boundary of the system are the aircraft's operators, the flight crew.

The system-level losses of importance to the Boeing 737 MAX stakeholders include loss of life, loss of property, loss of mission, and loss of stakeholder satisfaction. Specifically, they are:

- **L-1.** Loss of life or injury to aircraft occupants
- **L-2.** Destruction or damage to aircraft structure
- **L-3.** Inability of aircraft to reach its programmed/desired destination
- **L-4.** Loss of passenger or operator confidence in safety/efficacy of aircraft

The losses that this case study will primarily focus on are L-1 and L-2. The hazards associated with them can include:

- **H-1.** Aircraft does not maintain adequate separation from outside objects [L-1, L-2]
- **H-2.** Aircraft loses ability to remain airborne [L-1, L-2]
    - **H-2-1.** Aircraft cannot generate sufficient lift to remain airborne [L-1, L-2]
    - **H-2-2.** Aircraft has excessively high rate of descent [L-1, L-2]
- **H-3.** Aircraft is unable to be controlled [L-1, L-2]
    - **H-3-1.** Aircraft is out of trim in pitch direction [L-1, L-2]
    - **H-3-2.** Aircraft is longitudinally unstable [L-1, L-2]
- **H-4.** Aircraft moves outside approved/programmed flight zone [L-1, L-2, L-3]
- **H-5.** Aircraft creates a hostile environment to its occupants [L-1, L-4]

The safety constraints associated with these hazards are:

- **R-1.** Aircraft must maintain adequate separation from outside objects [H-1]
- **R-2.** Aircraft must preserve its ability to remain airborne [H-2]
    - **R-2-1.** Aircraft must maintain an attitude/orientation where it is able to generate lift [H-2-1]
    - **R-2-2.** Aircraft rate of descent must not exceed <TBD> [H-2-2]
- **R-3.** Aircraft must be able to be controlled [H-3]
    - **R-3-1.** Aircraft must remain in trim in pitch direction throughout flight [H-3-1]
    - **R-3-2.** Aircraft must remain longitudinally stable throughout flight [H-3-2]
- **R-4.** Aircraft must remain within approved/programmed flight zone [H-4]
- **R-5.** Aircraft must not create a hostile environment to its occupants [H-5]

This study will focus on two of the hazards outlined above: H-2 and H-3. The focus of the STPA will be to determine potential scenarios in which the aircraft could: a) lose the ability to remain airborne; or b) lose controllability or pitch stability.

4.1.2. Control Structures

Figures 16 and 17 depict hierarchical control structures for MCAS at two levels of abstraction. Figure 16 is a highly abstracted version of the control structure, while Figure 17 presents the system in more detail. The information used to build these control structures comes from the MCAS functional descriptions provided in [2] and [45].

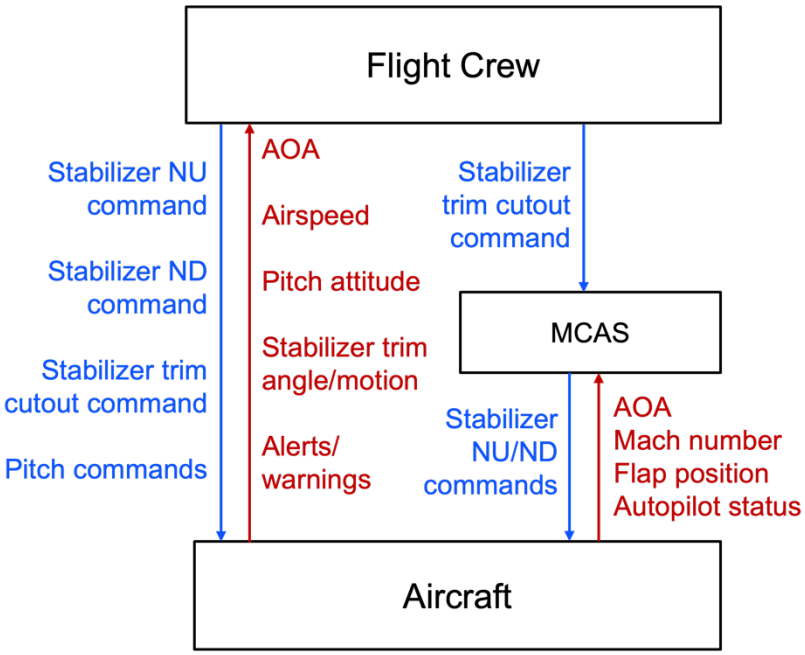


Figure 16. High level MCAS control structure

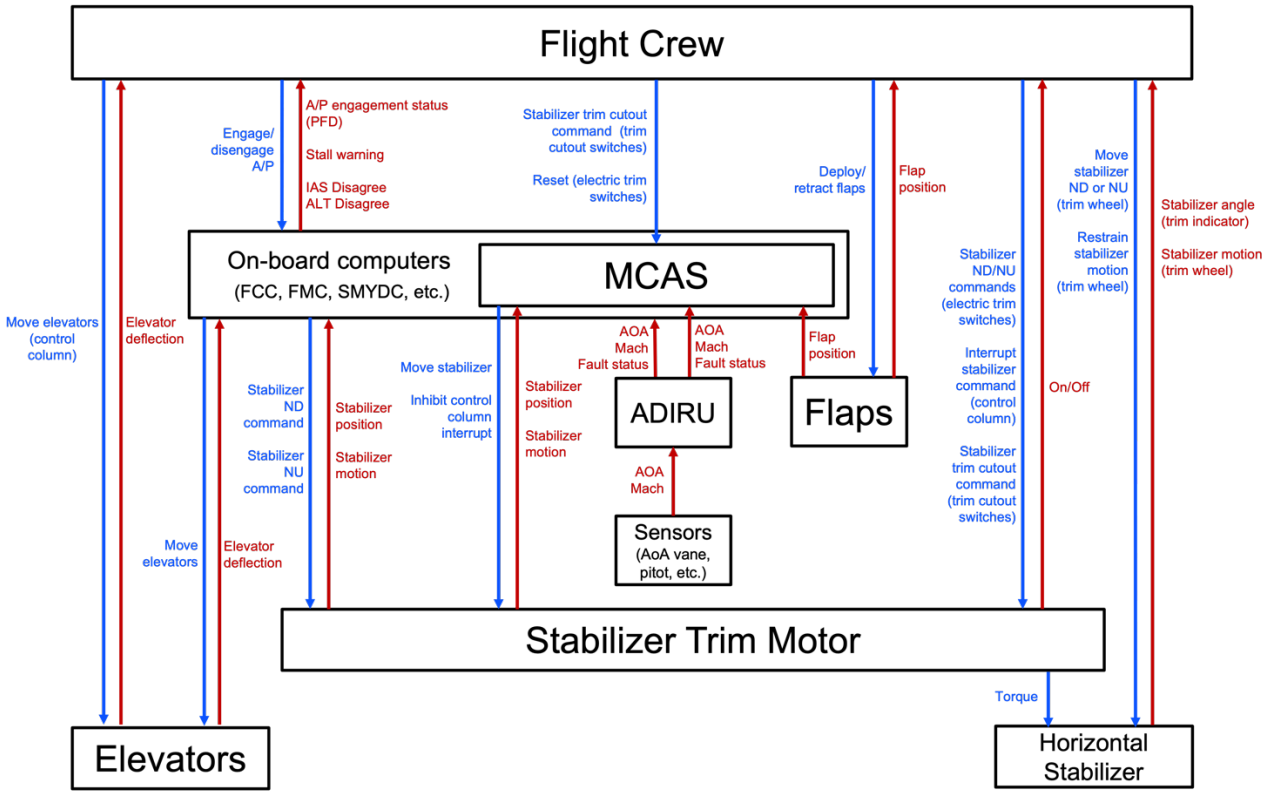


Figure 17. Detailed MCAS control structure

4.1.3. Overview of UCAs and Scenarios

The next step of STPA is to examine each of the control actions identified in the control structure to determine the contexts in which those control actions could be unsafe. This study examined a limited number of control actions for two controllers: the flight crew and MCAS. The twelve UCAs that were documented for MCAS are shown in Table IX, while the twelve UCAs documented for the flight crew are shown in Table X.

Table IX. Unsafe Control Actions for MCAS

Control Action	**Not providing causes hazard**	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
Move stabilizer ND	**MCAS-UCA-1:** MCAS does not provide stabilizer ND command when AOA threshold is exceeded during flaps up, high angle of attack maneuver [H-2]	**MCAS-UCA-2:** MCAS provides stabilizer ND command when aircraft is not in flaps up, high angle of attack maneuver [H-2, H-3] **MCAS-UCA-3:** MCAS provides stabilizer ND command when aircraft is out of trim in ND direction [H-2, H-3] **MCAS-UCA-4:** MCAS provides stabilizer ND command resulting in stabilizer movement of more than the maximum of 2.5^{o} [H-2, H-3] **MCAS-UCA-5:** MCAS provides stabilizer ND command when stabilizer trim is affecting aircraft pitch [H-2, H-3]	**MCAS-UCA-6:** MCAS provides stabilizer ND command too late after aircraft enters flaps up, high angle of attack maneuver [H-2]	**MCAS-UCA-7:** MCAS provides stabilizer ND command for too long compared to the AOA value's exceedance of the threshold at the current Mach number [H-2, H-3]

Move stabilizer NU	**MCAS-UCA-8:** MCAS does not provide stabilizer NU command when AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]	**MCAS-UCA-9:** MCAS provides stabilizer NU command when aircraft is in flaps up, high angle of attack maneuver and MCAS has not previously moved stabilizer ND [H-2, H-3]	**MCAS-UCA-10:** MCAS provides stabilizer NU command too late after AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]	**MCAS-UCA-11:** MCAS provides stabilizer ND command for too long compared to MCAS' previous stabilizer ND command [H-2, H-3] **MCAS-UCA-12:** MCAS stops providing stabilizer NU command too soon before matching duration of MCAS' previous stabilizer ND command [H-2, H-3]

Table X. Unsafe Control Actions for Flight Crew

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Move stabilizer NU	**FC-UCA-1:** Flight crew does not provide stabilizer NU command when unintended ND stabilizer motion by MCAS occurs [H-2, H-3]	**FC-UCA-2:** Flight crew provides stabilizer NU command when intended ND stabilizer motion by MCAS occurs during flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-3:** Flight crew provides stabilizer NU command too late (>4 seconds) after unintended ND stabilizer motion by MCAS occurs [H-2, H-3]	**FC-UCA-4:** Flight crew stops providing stabilizer NU command too early before aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3] **FC-UCA-5:** Flight crew provides

				stabilizer NU command for too long after aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3]
Stabilizer trim cut out command	**FC-UCA-6:** Flight crew does not provide stabilizer trim cutout command when MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-7:** Flight crew provides stabilizer trim cutout command during flaps up, high angle of attack maneuver [H-2, H-3] **FC-UCA-8:** Flight crew provides stabilizer trim cutout command when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	**FC-UCA-9:** Flight crew provides stabilizer trim cutout command too late (>4 seconds) after MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	N/A
Move stabilizer trim cut out switches to normal	**FC-UCA-10:** Flight crew does not move stabilizer trim cut out switches to normal when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	**FC-UCA-11:** Flight crew moves stabilizer trim cutout switches to normal when MCAS provides trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-12:** Flight crew moves stabilizer trim cut out switches to normal too late after aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	N/A

Each of these UCAs were analyzed to identify the causal scenarios that could lead to the UCA. The complete list of scenarios identified can be seen in Appendix B. Though some scenarios revealed causal factors that were already captured in the MCAS SFHA, PSSA and SSA, many other scenarios revealed contributions from human decision-making, component interactions without failures, and complex nonlinear causal pathways. These scenarios serve as examples for how STPA can be used to address some of the limitations in the safety assessment standards identified in chapter 3. The following subsections address each of these limitations individually and highlight the findings from specific MCAS STPA scenarios.

4.2. Integration of Human Considerations

The main limitations discussed in chapter 3 regarding integration of human considerations in the safety assessment process revolved around the absence of a process for assessing hazards related to human action (or inaction). A key aspect of the system-theoretic approach to safety is that the human is considered as much a part of the system as the physical components are, which means human contributions to hazardous states are not excluded from the analysis.

It is true that STPA does not provide a human factors assessment framework specifically designed to validate human response assumptions. However, STPA does provide a framework for thinking about and identifying the scenarios in which a human response assumption may not hold. If a particular behavior is expected of a pilot in response to a "failure," not behaving in the appropriate manner can be treated as a UCA. Similarly, if a particular behavior is known to *not* be appropriate following a "failure," that inappropriate response could also be treated as a UCA.

The scenario generation step of STPA then requires the analyst to examine the human operator's decision-making process to understand why it would appear reasonable for them to make a UCA. The analyst performing STPA is not allowed to assume that the operator will always perceive their surroundings appropriately, form a correct mental model, correctly decide the action to take, and correctly execute that action. The analyst must instead consider why the operator may *not* behave in a safe manner.

The STPA scenarios can uncover cases where the human may not respond as anticipated, and serve as inputs for determining what kind of simulator testing should be done, or what features of the system design should be changed to avoid unintended behaviors. As Malmquist et al. [61] note, the scenario or narrative being tested in a simulator is just as important as the physical realism of the simulator. STPA can provide the guidance to build effective scenarios from a human factors perspective that is missing from traditional safety assessment approaches.

Thomas [62] provides an updated model for a human controller in STPA that facilitates the scenario identification process by requiring the analyst to more deeply consider how the human operator makes decisions, and France [63] provides an application of that model to a complex system. From the perspective of that model, factors that can lead a human to make a UCA include: (a) flaws in the formation or updating of the human's mental models of their situation; (b) flaws in the human's existing model of the automation or environment; or (c) flaws in the human's decision-making process for selecting an appropriate control action.

The subsections below use scenarios from the MCAS STPA to demonstrate how STPA can be used to assess why a human may react differently than expected for the three reasons listed above. The UCA being analyzed is:

FC-UCA-1: Flight crew does not provide stabilizer NU command when stabilizer ND motion by MCAS occurs outside a flaps up, high angle of attack maneuver

This UCA was selected because the original safety assessment assumed that unintended stabilizer trim inputs would be readily recognized, and that the stabilizer runaway procedure would be followed. The runaway procedure involves manually controlling the aircraft using control column inputs and stabilizer NU commands, so not performing this behavior can be considered a UCA and scenarios can be generated to explain why that might occur.

4.2.1. Inadequate Mental Model Updates

From the perspective of mental model formation and updates, STPA can guide the analyst in thinking about the feedback provided to the flight crew and how it may affect their understanding of the current situation in desired or undesired ways. For instance, consider the following scenario for FC-UCA-1, which is visualized in Figure 18[18]:

FC-Scen-1.1: Flight crew are unaware of the stabilizer ND motion, or are aware of the motion but do not diagnose it as unusual or unintended. Flight crew therefore do not provide stabilizer NU command to counter it [FC-UCA-1]. MCAS has a maximum limit of 2.5^{o} for each individual stabilizer ND command, so a short duration command only causes slight movement of the stabilizer trim wheel and trim indicator. Unintended activations of MCAS (see scenarios for MCAS-UCA-2 in Appendix B) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Movement of the stabilizer may go unnoticed by flight crew preoccupied with other more salient stimuli in the cockpit. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch down excessively [H-2] and approach terrain [H-1, H-4].

[18] As a convention, in all scenario visualizations the UCA is colored red, other control actions are colored blue, and feedback paths are colored maroon. Solid lines refer to controls or feedback that are transmitted (even if erroneously), and dotted lines refer to control actions that are not issued or feedback that is missing.

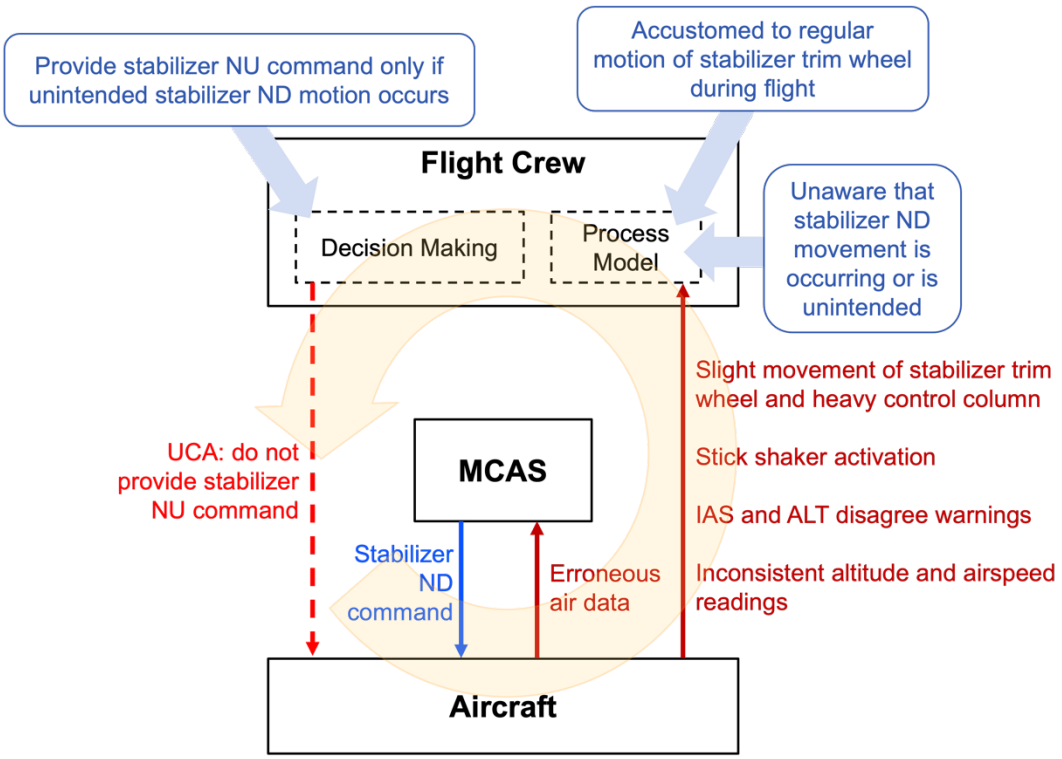


Figure 18. Visualization of FC-Scen-1.1

Providing a stabilizer NU command in response to unintended stabilizer ND motion requires enough information to diagnose that stabilizer motion has occurred and that it was unintended. As is seen in this scenario, if the flight crew does not behave as expected, it may be because they do not receive sufficient feedback to inform their mental model of the situation, or do not perceive that feedback appropriately.

The STPA handbook [19] provides guidance for identifying missing, incorrect, or misinterpreted feedback. Additionally, France [63] expands upon that guidance by drawing from Wickens et al.'s model [64] of perception and proposing several questions for examining mental model updates. These questions can force the analyst to consider how salient a piece of feedback is to the flight crew, how much effort the crew will need to expend to perceive the feedback, how expected or unexpected the feedback will be, and how much relative importance the flight crew will attribute to that feedback.

As an example, consider the salience of the feedback observed during an unintended MCAS activation in FC-Scen-1.1. The expectation is that the flight crew will perceive movement of the stabilizer trim wheel and feel increased control column forces, and will then provide a stabilizer NU command to counter MCAS. However, MCAS has a limit for each individual command, resulting in only short duration movements of the stabilizer trim wheel.

Additionally, the true salience of a particular piece of feedback can only be understood in the context of the other stimuli experienced at the same time. It is therefore necessary to consider what other effects the flight crew would be observing at the same time as an unintended MCAS activation. The scenarios for MCAS-UCA-2 in Appendix B reveal that unintended MCAS activations may also coincide with additional flight deck effects if the source of the activation is erroneous data from AOA or pitot-static probes, such as stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. The loud, violent nature of the

stick shaker is more salient than the trim wheel and column forces, and may be more likely to attract the flight crew's attention. Asking questions about the effectiveness of feedback can help the analyst understand if further design changes are needed to guide the flight crew to make appropriate decisions.

4.2.2. Flawed Mental Models of Automation

STPA can also help guide the analyst to consider the effects of the flight crew having a mental model of the automation that does not fully represent the system's state or behavior. For example, consider the following scenario for FC-UCA-1, visualized in Figure 19:

> **FC-Scen-1.2:** Flight crew notice the stabilizer ND motion and diagnose it as unintended, but believe they can stop and overcome the unintended stabilizer motion using control column inputs alone. Flight crew therefore do not provide stabilizer NU command to counter ND motion [FC-UCA-1]. All automatic stabilizer ND commands (except those issued by MCAS) can be interrupted through a control column input in the opposite direction. During stabilizer trim commands issued by MCAS, the control column cutout feature is inhibited and will not interrupt the stabilizer ND commands. Flight crews are not made aware of the existence of MCAS, nor its ability to inhibit the control column cutout feature. Flight crew may notice aircraft responding to control column inputs and may not realize the stabilizer ND commands were not interrupted. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not sufficiently use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

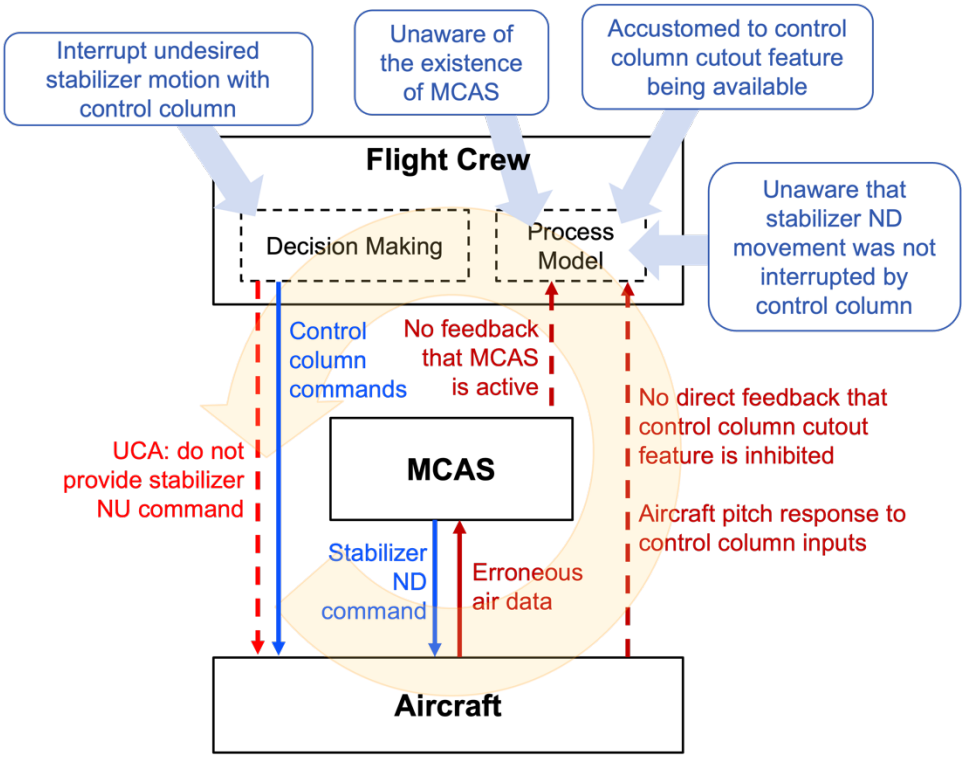


Figure 19. Visualization of FC-Scen-1.2

In this scenario, the flight crew perceive the "failure" in a timely manner and update their mental model of the situation accordingly, but a flaw in their broader overarching model of the system's state and behavior leads them to make an incorrect decision. STPA does not assume the flight crew fully understands the system they are operating; it instead actively seeks out scenarios in which the crew's understanding of the system differs from its true behavior. Identifying these types of scenarios can help the safety analyst identify the additional feedback, training, or procedures that need to be incorporated to ensure crew awareness.

In FC-Scen-1.2, the flight crew are unaware that a control action which is usually available (the control column interrupt feature) is not actually executable in their specific situation. One factor contributing to this flawed mental model is the fact that the flight crew are unaware of the automation mode that is driving the undesired behavior, a phenomenon known as *mode confusion*. No training manuals, operation manuals, or cockpit displays inform them of the existence of MCAS, meaning the flight crew is not aware this mode/function exists in the first place. Though FC-Scen-1.2 did not play out in either of the 737 MAX accidents, it is not difficult to see how a flight crew might reasonably behave in this manner.

In their work on mode confusion, Sarter and Woods [65] emphasize that training and feedback must be designed to enhance the crew's skill at attending to and interpreting signals from automation. Even better would be to design the aircraft to eliminate mode confusion. STPA coupled with the guiding questions in [62] provide a framework for the analyst to explicitly examine what the operator knows or believes about the system. By asking what the system does in its current mode, what actions are available to the operator in the current mode, and what the relationship is between operator inputs and system behavior, STPA can help identify what system design and feedback is necessary to best support the flight crew in responding appropriately. A process specifically designed for identifying sources of mode confusion using STPA in early development can be found in [66].

4.2.3. Flawed Human Decision-Making Algorithm

From a decision-making perspective, STPA can also help identify situations in which the crew forms the appropriate mental model of the situation, but make the conscious choice to execute a different control action than what is expected. As an example, consider scenario FC-Scen-1.4 below, visualized in Figure 20:

> **FC-Scen-1.3:** The flight crew notice the stabilizer ND motion and diagnose it as unintended, but do not issue stabilizer NU commands [FC-UCA-1] because they prioritize resolving other flight deck alerts and indications first. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings that are more salient than the stabilizer ND motion. If at low altitude, flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts, according to how they were trained. As a result, the aircraft is out of trim by a variable number of degrees [H-3-1]. If the flight crew intentionally pitch down to avoid a stall, the aircraft may enter an excessive nose-down attitude [H-2] and approach terrain [H-1, H-4].

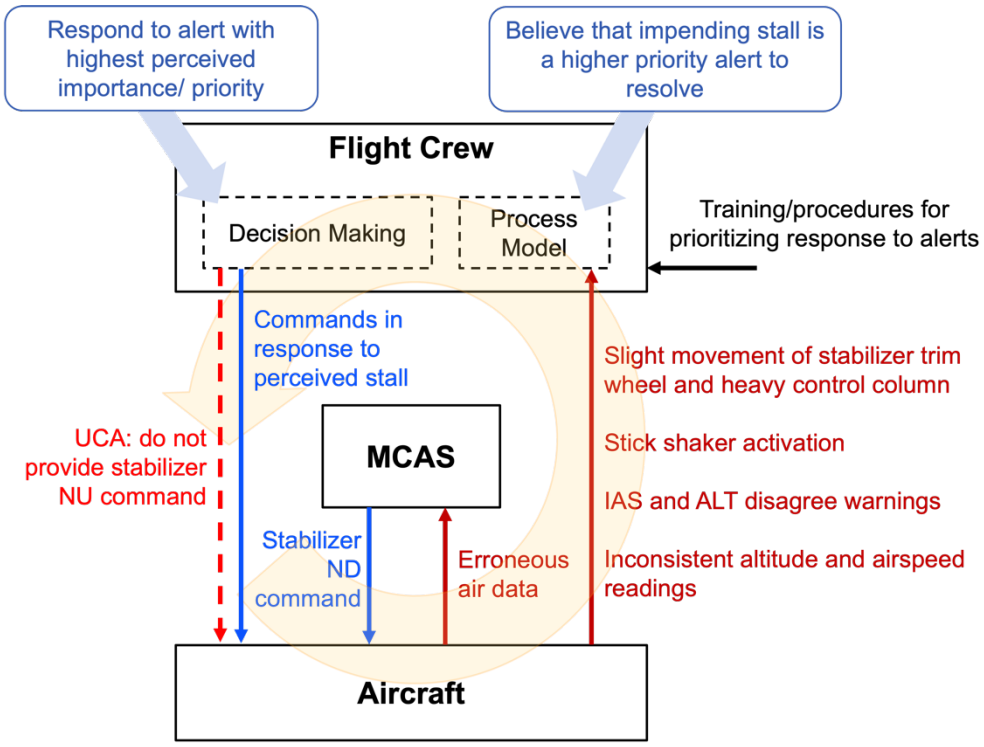


Figure 20. Visualization of FC-Scen-1.3

A human's decision-making is often influenced by their goals and by the alternatives available to them for achieving these goals [63]. If a flight crew perceives multiple alerts at the same time, their response may be prioritized based on whichever alternative most quickly, effortlessly, or effectively achieves their primary goal of keeping the aircraft in the air. In the example of FC-Scen-1.3, the impending stall (indicated by the stick shaker) may be seen as the biggest threat to the safety of the aircraft. The control actions that address the most severe threat (e.g., pitching down to counter the stall) may thus be seen as the most appropriate even if they exacerbate the effects of other "failures" like the erroneous MCAS activation.

Factors that can shape a flight crew's decision-making include training, procedures, and past experience [19]. In the STPA vernacular, these are all controls enforced on the flight crew by controllers above them, such as airline management, an aircraft manufacturer, or a regulatory authority. When examining whether a flight crew will respond as expected, an analyst may ask what external controls affect their decision-making. For instance, what guidelines exist for prioritizing alerts? Are there potential company policies or practices that may lead crews to choose a different response (e.g., relying more or less on automation)? Considering questions like these through the STPA framework can allow the analyst to identify additional elements of procedure, training, or policy that are necessary to prevent undesired behavior.

4.2.4. Human Error beyond Response to Failures

Finally, STPA also provides a framework for an additional hazard analysis that is absent from ARP4761 and not formalized in the means of compliance for 14 CFR 25.1302: identifying unsafe human actions that are *not* in response to any function loss or malfunction. Though a malfunction

did occur in the case of the 737 MAX accidents, a number of other accidents have resulted from unsafe actions taken by flight crews operating otherwise perfectly functional aircraft.

For example, the flight crew of American Airlines flight 965 placed their aircraft on the wrong flight path by selecting "R" from a waypoint list in the flight management system (FMS) instead of the desired "ROZO" [67]. In another instance, when landing with a (intentionally) disabled thrust reverser, the captain of TAM Linhas Aéreas flight 3054 left the aircraft's number 2 engine thrust lever at the "climb" position instead of "idle", preventing the autobrake and spoilers from activating and causing the aircraft to overshoot the runway [68]. In yet another example, a test pilot on a Scaled Composites Model 339 SpaceShipTwo unlocked the spacecraft's feathering system too early, leading the craft to disintegrate in midair [69].

Though these accidents have in the past been attributed primarily to pilot error, it is clear that elements of system design, operational procedure, and airline management all played a role in making the flight crews' actions appear reasonable to them, despite being unsafe in hindsight. Understanding how and why a human may be led to take an unsafe action, as well as understanding the effects of such an action, are crucial elements of safety assurance that could benefit from a structured methodology.

In fact, because the SS2 had an experimental permit, it was subject to the regulations of 14 CFR Part 437, which specifically require the safety analyst to identify and describe hazards, including those resulting from human errors [14 CFR 437.55(a)(1)(iv)]. However, in NTSB interviews following the SpaceShipTwo accident, Scaled Composites engineers specifically noted the lack of an "industry recognized analytical tool for performing this analysis." [70] STPA can serve as a useful tool for performing a human factors hazard analysis.

STPA provides an analytical method for identifying causes and consequences of human error, even beyond human response to "failures". The context portion of a UCA typically describes the system state or environmental conditions in which taking a particular action is unsafe [19]. This context can include a loss of function or malfunction in an associated system (e.g., flight crew does not provide manual braking commands during normal landing when autobrake is unavailable) but can also simply be an operational state (e.g., flight crew does not provide manual braking commands during normal landing). Upon identifying the contexts that make an action unsafe, STPA actively seeks to identify any scenarios which would make that action appear reasonable to the flight crew.

Each STPA scenario traces directly to a UCA, which traces directly to one or more hazards, which themselves trace directly to one or more losses. Thus, the STPA artifacts also provide the traceability between human "errors" and aircraft-level losses which is missing from the current safety assessment process. Understanding exactly how a feature of the system can lead a human to act in a way that ultimately leads to a loss allows for more informed decision-making about the design of the systems the flight crew will interact with.

4.3. Support in Identifying Unrecognized Assumptions

Chapter 3 pointed out how the processes in ARP4761 call for the documentation of assumptions, but do not provide a methodology that can support the identification of unrecognized assumptions. Though STPA is a hazard analysis tool and not an explicit methodology for identifying assumptions, many STPA artifacts such as the hierarchical control structure, unsafe control actions, and causal scenarios can be used to recognize safety-critical assumptions about system design. In her work on risk management through leading safety indicators, Leveson [71]

identifies how safety-critical engineering assumptions can be formed and outlines how the different artifacts of STPA can be used to identify them.

The first set of STPA artifacts generated are the system-level losses and hazards of interest. Preventing or mitigating the losses and hazards is a high-level goal that will drive design decisions. Therefore, the inclusion or exclusion of any particular loss or hazard can represent an implicit assumption if not properly documented. For instance, consider the system-level hazards for an electric vertical takeoff and landing (eVTOL) aircraft. The inclusion of a hazard such as "aircraft moves outside approved flight zone" implicitly assumes a structure in the national airspace system that may or may not exist. Though the losses and hazards for transport category aircraft rarely change and may not reveal deeply ingrained assumptions, analyzing the losses and hazards for aircraft that are drastically different in configuration or mission profile may provide new insight.

Though high-level overarching assumptions are useful to identify, Dewar [55] notes that it is usually at lower levels of detail that implicit assumptions become more challenging to identify and have a more pronounced impact, as they may directly underlie design decisions. Thus it is in the UCA and scenario generation steps (that make use of the hierarchical control structure) that STPA provides the greatest benefit in terms of identifying assumptions.

A key difference between an STPA control structure and other types of system models is that the control structure does not assume obedience or effectiveness [19]. Including any control or feedback in an STPA control structure only indicates that a mechanism will exist to enforce that control, or that a pathway will be created to send that piece of feedback. It is *not* implied that any controls and feedback will be effective, will be utilized at the right time, or will even be available in the first place. It is in fact a goal of STPA to determine, using UCAs and scenarios, the ways in which existing feedback-control loops can be ineffective.

The process for generating UCAs provides a major opportunity for identifying undocumented assumptions. Considering or not considering a control action as a UCA represents an assumption about the safety of that action. As Thomas et al. [72] note, the absence of a UCA or UCA category in a particular context can be an indication of an implicit assumption that that action is safe.

For example, consider an automated controller whose controls include deploying ground spoilers on landing. One potential UCA for this controller could be, "Automated controller does not provide ground spoiler deployment command when landing speed exceeds <X>." At the same time, another potential UCA could be "Automated controller *provides* ground spoiler deployment command when landing speed exceeds <X>." Excluding either of these UCAs may implicitly indicate that in this context, that control action is believed or assumed to be safe. Even if that truly is the case and the control action is safe, identifying and documenting this assumption can help the analyst keep track of what they believe to be true about the system. If changes in system design or operational procedures are introduced in the future, the assumption can then more easily be revisited and revalidated.

Finally, the scenario step of STPA then forces the analyst to question why a controller in a system (working as designed) may issue an unsafe command. This provides the analyst with the opportunity to most thoroughly and systematically question their own beliefs about the system's capabilities and behavior. Before the analysis, an analyst or designer may hold the implicit assumption that a particular UCA cannot possibly occur. However, in STPA the UCA is considered a ground truth (i.e., the UCA has definitely happened), and the goal is to find the conditions that satisfy that truth. Consider, for example, the following flight crew UCA relating to MCAS:

FC-UCA-6: Flight crew does not provide stabilizer trim cut out command when MCAS issues trim commands outside of a flaps up, high angle of attack maneuver

The ground truth in this UCA is that MCAS *is* issuing trim commands outside of a flaps up, high angle of attack maneuver, and the flight crew *is not* providing a stabilizer trim cut out command. The different types of scenarios can then reveal different unrecognized assumptions that make the UCA true.

For example, if there exists a scenario in which the control action is not executed (e.g., the flight crew *do* provide a stabilizer trim cutout command, but the command does not change the state of the system), then there may be an implicit assumption about the effectiveness of that mitigation of the hazard. If there exists a scenario in which the control action is attempted but cannot successfully be performed (e.g., the flight crew cannot access the stabilizer trim switches), then there may be an implicit assumption about the availability of a mitigation to a hazard[19]. If there exists a scenario in which the control action is never attempted (e.g., the flight crew never try to move the stabilizer trim switches), then there may be an implicit assumption about the system behavior and feedback that would trigger that action. One example of this latter category is FC-Scen-6.3 from the MCAS STPA, which is seen below and visualized in Figure 21:

FC-Scen-6.3: The flight crew notice the stabilizer ND motion, but do not believe the motion to be a stabilizer trim runaway that requires a stabilizer trim cutout command. A stabilizer trim runaway is defined as continuous movement of the stabilizer trim wheel, and the stabilizer runaway procedure is concluded if unintended stabilizer motion stops when the autopilot is disengaged. MCAS only operates with autopilot off, and stabilizer ND motion will stop after either 9.2 seconds or any manual electric stabilizer trim commands by the flight crew. The flight crew notice that they can interrupt and overcome the stabilizer motion using stabilizer NU commands alone and diagnose the situation as something other than a stabilizer trim runaway. The flight crew therefore do not provide a stabilizer trim cutout command to counter ND motion [FC-UCA-6]. The flight crew are not aware that countering MCAS-issued stabilizer ND commands with only manual electric stabilizer NU commands allows MCAS to issue repeated commands (see MCAS-Scen-7.4). As a result, the aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use the control column to maintain altitude and attitude, the aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

[19] Though the stabilizer trim switches may appear easily accessible in the 737 cockpit, it is not unheard of for a flight crew to be unable to perform a necessary action because they cannot physically reach a cockpit interface. The captain of Sichuan Airlines flight 8633 was not able to reach his oxygen mask after a windshield blowout because it was located to his left and he needed to keep his left hand on the sidestick to maintain control of the aircraft [73].

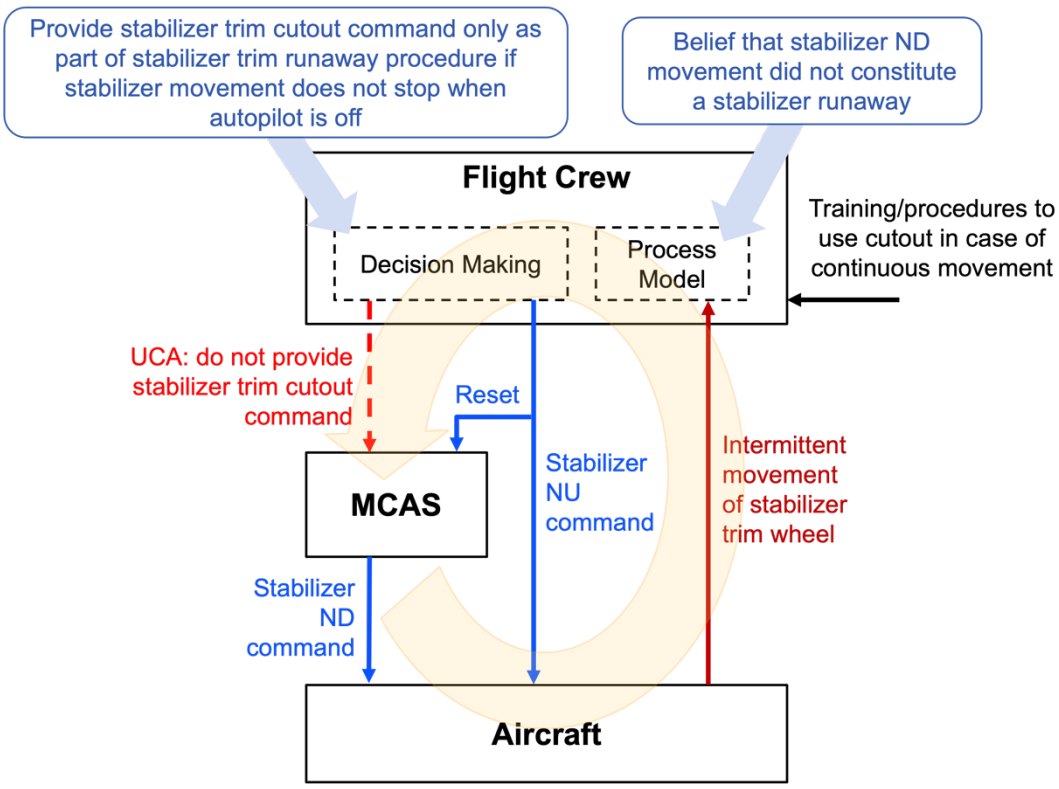


Figure 21. Visualization of FC-Scen-6.3

In this scenario, the reason the flight crew do not provide the control action as expected is because the system behavior that is expected to trigger that control action (continuous movement of the stabilizer) is different from the actual behavior exhibited by the system (intermittent movement of the stabilizer). The belief that erroneous stabilizer commands issued by MCAS would look the same as erroneous stabilizer commands issued by other automated systems or caused by a true stabilizer runaway is a safety-critical implicit assumption whose identification requires questioning what the analyst (and designer) believe to be true about their system. Thus, though assumptions are not an explicit output of STPA, the framework does force the analyst to consider how their system may behave in ways they do not expect.

For a more rigorous approach to identifying unrecognized assumptions using STPA and a framework for continuously evaluating assumptions during operation, the reader can refer to [71]. Upcoming work by Justin Poh, to be completed in 2024, will also provide a more detailed STPA-based approach to identifying implicit assumptions.

4.4. Uncovering Non-failure Based Scenarios

Section 3.3 highlighted how the processes in ARP4761 support the analyst in understanding how component or functional failures can lead to catastrophic losses, but they could use additional guidance for uncovering loss scenarios that stem from non-failure related causal factors. The STAMP framework is built on an accident causality model that does not treat safety as a problem of preventing component failures, but as a problem of ensuring the appropriate controls are enforced to manage system behavior. Tools under the STAMP umbrella, like STPA, are therefore

uniquely positioned to provide analysts with a systematic methodology for uncovering those scenarios where no component has failed but an accident can still occur.

4.4.1. Causal Scenarios from Non-Developmental Factors

An STPA starts by identifying losses and hazards, and proceeds to identify the unsafe control actions that might cause them. Because a goal of STPA is to identify scenarios that can lead UCAs to happen, STPA makes no assumptions about proper aircraft maintenance, manufacturing, or operations, which in ARP4761 are all assumed to follow specified procedure. If a particular maintenance error, manufacturing defect, operational activity, or other external factor can lead a controller to provide a UCA, then it is identified by STPA and included in the results.

When examining why an automated controller might provide a UCA, STPA does consider the possibility that component failures lead to the action. For example, an electrical/wiring failure could cause a spurious signal in a flight control computer and trigger a control action at the wrong time. However, STPA also considers the possibility that the control action is provided intentionally when the automated controller receives the feedback that would trigger that action, even if that feedback is inaccurate or misleading.

For example, if an autobrake controller uses weight-on-wheels to determine when to issue braking commands, then STPA would examine how that data may be incorrect or misleading and cause the controller to issue a command at the wrong time. If, for instance, inappropriate maintenance can cause the weight-on-wheels sensor to provide misleading data, STPA would identify that as part of a causal scenario.

As another example, consider the following UCA and scenario identified in the MCAS STPA, which are visualized in Figure 22:

> **MCAS-UCA-2:** MCAS provides stabilizer ND command when aircraft is not in flaps up, high angle of attack maneuver [H-2, H-3]

> **MCAS-Scen-2.4:** MCAS provides a stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor was bent or otherwise damaged during maintenance procedures, leading it to produce an erroneously high signal that is still within the sensor's defined range. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.

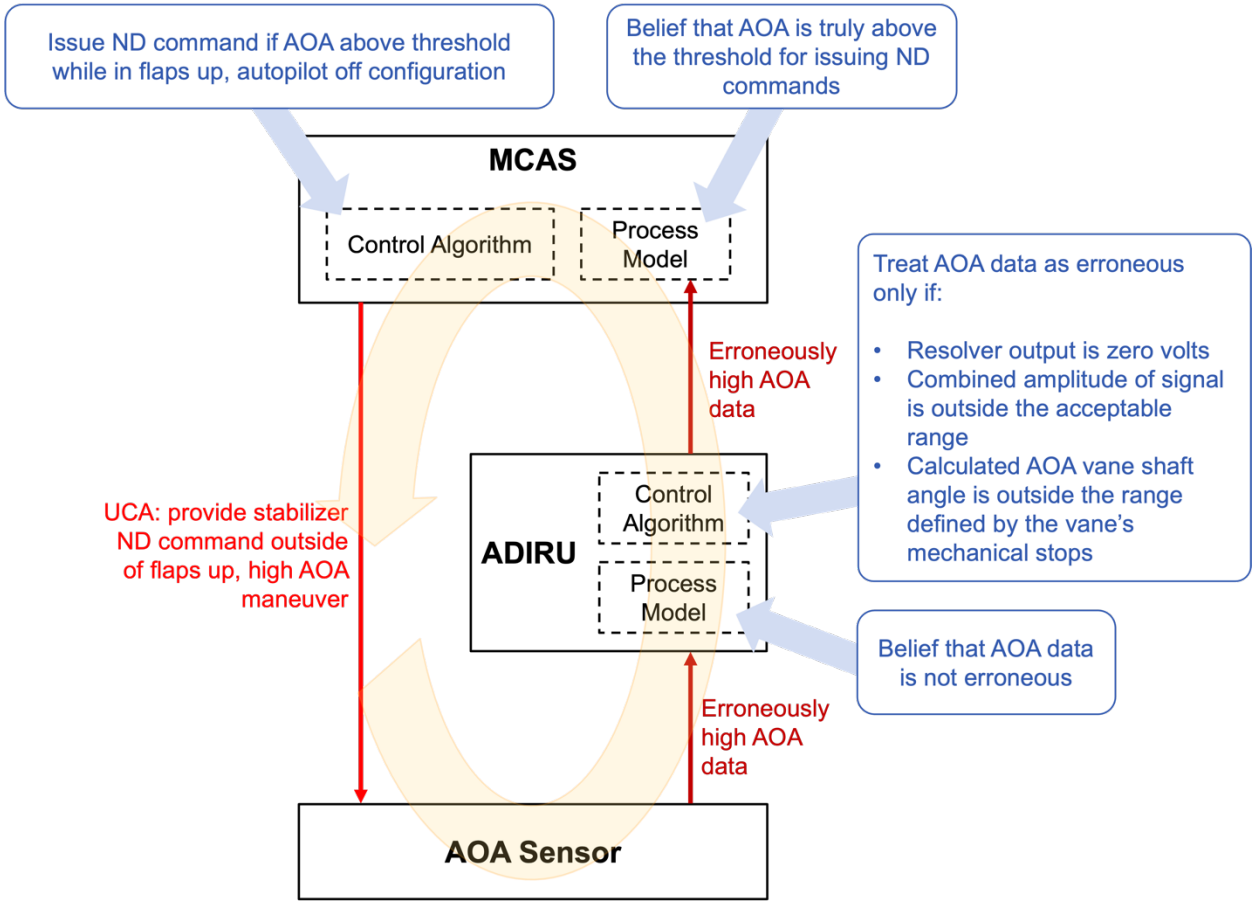


Figure 22. Visualization of MCAS-Scen-2.4

In this scenario, MCAS uses incorrect AOA data as feedback to inform its decision to provide a stabilizer ND control action when it should not have. Though incorrect AOA data could stem from a component failure, this scenario shows it could also stem from improper maintenance of the AOA sensor. The scenario also considers how the system interprets the incorrect data it receives. If the system is meant to reject data it considers incorrect (as the ADIRU was meant to do for certain patterns of AOA data), then the scenario generation process could help identify situations where incorrect feedback can bypass the checks and still be used to make decisions.

Feedback is not the only element of a control loop that can be affected by external factors like improper maintenance. The STPA handbook [19] highlights other kinds of maintenance-related scenarios STPA can help uncover. These include, for example, the case where a piece of automation is shut down for maintenance, and when it restarts it assumes that the system's state is the same as when the automation was shut down.

Ultimately, if it is determined during safety assessment that factors like maintenance can contribute to hazardous situations, as in MCAS-Scen-2.4, STPA can also be used to examine the maintenance and manufacturing processes and identify how these errors could come to be. For instance, performing a more detailed STPA on the procedures for maintaining the AOA sensor could then uncover what specific maintenance practices might lead the sensor to generate incorrect data.

Slominski [74] demonstrated how STPA can be used to assess the serviceability of systems with software and physical components. Some of the scenarios uncovered in that STPA could be

used to inform component design or component integration into larger systems. For example, some scenarios revealed how missing or ambiguous feedback about the fault status of sensors could lead technicians to replace those sensors improperly or unnecessarily. These STPA findings could inform decisions about the appropriate feedback that should be provided to technicians replacing the sensors.

Though the examples above focused on maintenance, STPA can also be used to understand the safety implications other factors outside the design process, like manufacturing or management.

4.4.2. Causal Scenarios from Component Interactions

Once losses and hazards have been identified in an STPA, it does not matter whether hazardous states are entered because of a component failure or because of normal, intended operation of a component or function. When examining why an automated controller might provide a UCA, STPA does still consider the possibility that component failures lead to the action (e.g., an electrical/wiring failure causes a spurious signal in a flight control computer). However, STPA also considers the normal conditions that are expected to trigger that control action. If there exist any normal operational scenarios in which the control action is unsafe, but the conditions to trigger it are still met, STPA would identify them and generate requirements to mitigate them.

There are several types of interactions that STPA can help an analyst uncover. Automated controllers can interact unsafely by providing control actions that conflict with each other, by providing repeated or duplicate control actions, by not providing control actions because they assume other controllers already have, among many other reasons. Leveson [36] provides several examples of interactions uncovered using STPA where no components failed but the aircraft still entered a hazardous state. These examples include an autobrake controller not issuing appropriate commands because an anti-skid system affected feedback about wheel speed, and hydraulic control software intentionally ignoring autobrake commands because it believes manual braking commands have already been provided. Another application of STPA to an aircraft engine thrust control malfunction system was able to identify scenarios in which the system, working as designed, could issue commands that shut down the engine in flight [75,76].

Additionally, the unsafe interactions identified using STPA are not limited to physical components. Interactions between human and automated controllers are also examined. For example, when examining how a rotorcraft blade de-icing function could be prevented from operating, STPA uncovered cases where the auxiliary power unit failed and did not provide power to the system, but also cases where the flight crew did not switch on the auxiliary power unit because they were unaware that the system was needed [77].

The application of STPA to MCAS also uncovered scenarios in which interactions resulted in hazardous situations without components or subsystems failing. As an example, consider the following UCA-Scenario pair, which is also visualized in Figure 23:

> **MCAS-UCA-4:** MCAS provides stabilizer ND command resulting in stabilizer movement of more than the maximum of 2.5^{o} [H-2, H-3]
>
> **MCAS-Scen-4.3:** MCAS initiates a stabilizer ND command while the speed trim system is already providing a stabilizer ND command, causing the stabilizer ND command to proceed at a rate higher than 0.27^{o}/sec [MCAS-UCA-4]. The system may not possess protections against

two simultaneous commands from different automated controllers, and the commanded rate of stabilizer motion from both commands may be added. As a result, the stabilizer moves at a faster rate than expected and the aircraft is out of trim by at least 2.5° [H-3-1].

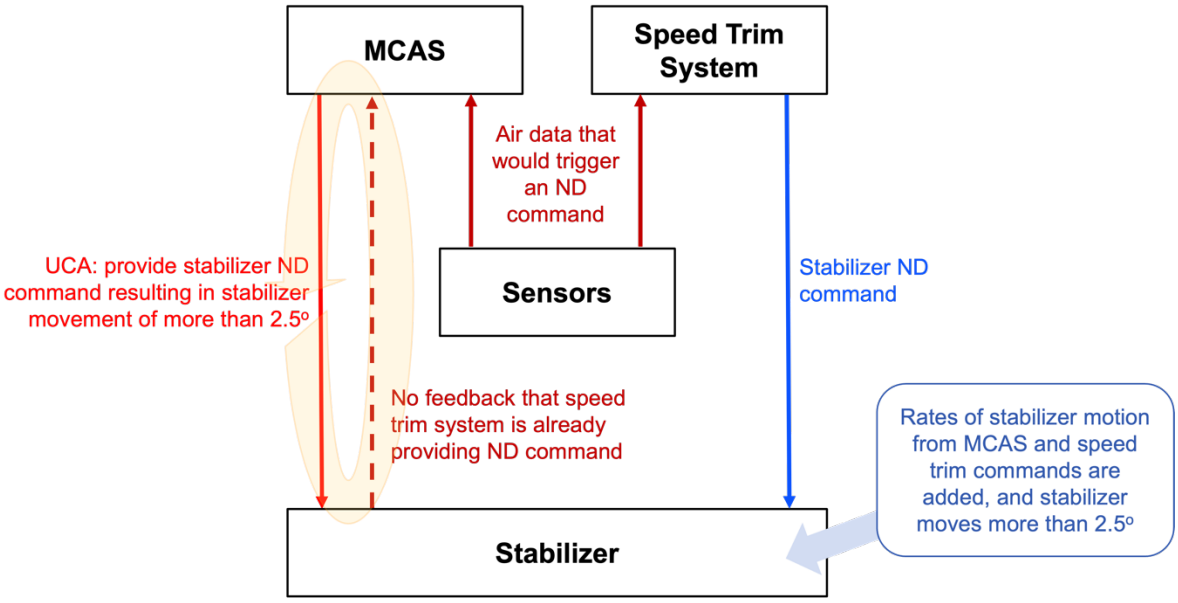


Figure 23. Visualization of MCAS-Scen-4.3

In this scenario, two intended software commands are issued at the same time and interact to place the aircraft in a potentially hazardous state. It is important to note that the inclusion of MCAS-Scen-4.3 here is not meant to imply that the *actual* design of MCAS at the time of the 737 MAX accidents was susceptible to additive commands from the speed trim system. There is not enough publicly available documentation on the MCAS and speed trim system logic to infer how the systems would react to simultaneous commands. It may be that the original design already protects against this scenario through its software logic. However, STPA forces the analyst to question how these two systems interact and ensure that the protection truly exists if the interaction can lead to a hazard.

4.4.3. Causal Scenarios from Combinations of Failures and Intended Behavior

STPA can also identify cases where a single component failure is not safety-critical, but when that failure is combined with the *intended* behavior of a different system, a hazard can result. The cascading effects analysis (CEA) in ARP4761 already considers cases where an initiating condition (usually a failure) has a direct effect on the functionality of one system, and multiple indirect effects on the functionality of other systems. The additional scenarios that STPA can uncover are those where a failure has no direct or indirect effect on the functionality of another system (i.e., that system's behavior is unchanged), but that unchanged functionality now becomes unsafe.

For example, in the thrust control malfunction case discussed earlier [75,76], the traditional safety assessment found that single-point hardware failures in the engine or sensors would appear to be mitigated and have no direct safety effect. The STPA then revealed that a combination of

those same hardware failures and the *intended* behavior of the thrust control malfunction system (which may be unaffected by the failure) can actually have catastrophic consequences.

As another example, consider the following UCA-Scenario pair uncovered in the MCAS STPA, and visualized in Figure 24:

MCAS-UCA-9: MCAS provides stabilizer NU command when aircraft is in flaps up, high angle of attack maneuver and MCAS has not previously moved stabilizer ND [H-2, H-3]

MCAS-Scen-9.2: A failure or malfunction in the stabilizer trim motor hardware or the jackscrew prevents an MCAS stabilizer ND command from actually moving the stabilizer when AOA value goes above the threshold for the current Mach number. MCAS may not register that the stabilizer ND command has not resulted in actual movement of the stabilizer, and may provide a stabilizer NU command anyway [MCAS-UCA-9]. If the hardware failure only prevents jackscrew rotation in one direction, the stabilizer NU command may still go through and result in movement of the stabilizer. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the MCAS stabilizer NU command [H-2, H-3-1].

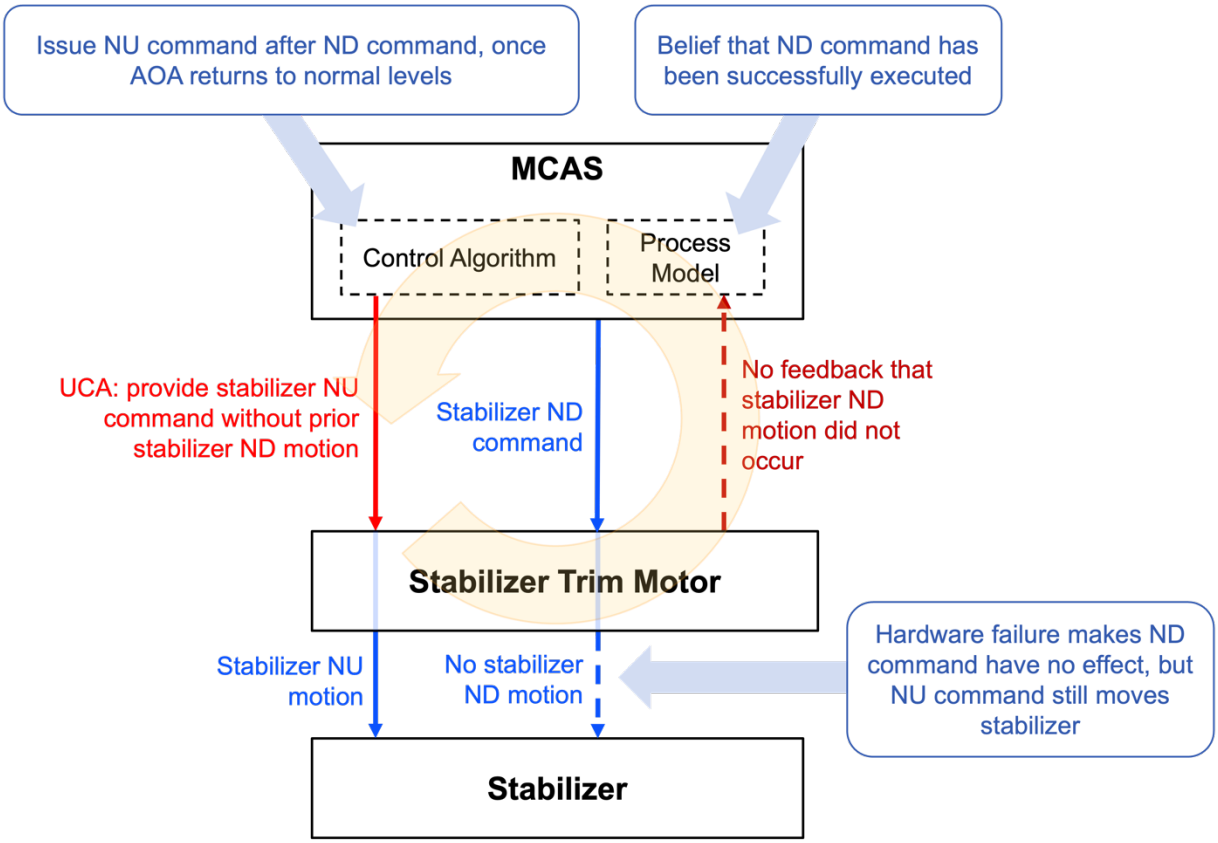


Figure 24. Visualization of MCAS-Scen-9.2

According to its original design, once the angle of attack goes below the Mach number threshold, MCAS would issue a stabilizer NU command to cancel out its earlier stabilizer ND command. In this scenario, a hardware failure prevents the ND command from actually moving the stabilizer but does not prevent an NU command from moving the stabilizer in the opposite

direction. The intended functionality of canceling out the ND command with an NU command then becomes unsafe even if it completely unaffected by the hardware failure. The safety of the intended NU command is dependent on successful execution of the ND command, which does not happen because of the hardware failure.

Similar to MCAS-Scen-4.3 from the previous subsection, it is unknown whether the *actual* design of MCAS at the time of the 737 MAX accidents checked for successful execution of the ND command before issuing an NU command. It is possible that the MCAS designers already protected against this scenario. The SFHA for MCAS did include "Loss of MCAS function" [2], so the effects of not issuing a stabilizer ND command may have been considered, but no step in the ARP4761 process would have explicitly guided the analysts to consider what intended behavior becomes unsafe when that failure occurs. STPA can fill that gap by serving as a framework for questioning the safety implications of a failure *combined* with other normal functionality.

4.5. Identification of Complex Nonlinear Causal Pathways

As described in section 3.4, causal factors in modern commercial aircraft accidents are not always straightforward and linear, which makes them difficult to proactively identify with techniques based on linear accident models. Capturing these complex causal factors requires a different perspective on how accidents develop, which the STAMP causality model provides.

As outlined in chapter 2, STAMP views systems as sets of interrelated components that interact through feedback-control loops. STAMP then views an accident as a series of violations of the safety constraints that are in place to control the behavior of that system [16]. Tools that are based on STAMP, like STPA and CAST, can model and analyze system behavior that does not neatly conform to a linear chain of causal events.

The STPA control structure is naturally a nonlinear representation of the functions and behavior of a system. The controller in a feedback-control loop can affect the behavior of the controlled process, and in turn the state of the controlled process affects the decisions made by the controller. Where an FHA would individually examine each discrete event (e.g., loss of braking function, erroneous activation of braking function, etc.), the scenario-based framework of STPA allows the analyst to consider the event as well as the nonlinear dynamics that ensue from that event (e.g., erroneous activation of braking function, followed by pilot reaction, followed potentially by another erroneous activation, and so on).

The field of system dynamics (SD) [78], which arose in the management circles, studies phenomena whose cause and effect relationships are not linear or obvious. Some causal relationships can be *reinforcing*, for example the case where a person inputs a command into a computer system, there is subsequent a delay in response so they input additional commands, which only increases the delay for the commands to be processed. On the other hand, some causal relationships can be *balancing*. Consider the case where a product goes to market and sees a high accident rate. A regulator may notice that and enact stronger safety controls on that product, which lowers the accident rate. The regulator may then notice the low accident rate and determine that some controls can be loosened, which then increases the accident rate once again.

Though SD is not built into the STPA process and the models each approach uses are not equivalent, the concept of reinforcing and balancing loops can help support the identification of causal scenarios involving nonlinear or cyclic behavior. An analyst might consider, for instance, whether providing a control action once can reinforce a controller's beliefs and lead them to provide the action again. In turn, they might also consider whether providing a control action once

can reinforce or amplify the *effects* of providing that action again later. On the other hand, the analyst can also consider whether providing a necessary control action can trigger another controller to provide an unnecessary action that neutralizes or invalidates the first.

Consider the following UCA and scenario as an example of cyclic and reinforcing behavior leading to a hazard. The scenario is visualized in Figure 25 below, where the numbers 1 through 4 represent the temporal sequence of events.

MCAS-UCA-3: MCAS provides stabilizer ND command when aircraft is out of trim in ND direction [H-2, H-3]

MCAS-Scen-3.3: MCAS provides a stabilizer ND command after already having provided a stabilizer ND command that was not fully countered. After a first MCAS activation (see scenarios for MCAS-UCA-2), MCAS's flight control law is reset without MCAS having provided or completed providing a stabilizer NU command to counter a prior ND command. This occurs because the flight crew provides electric stabilizer trim commands before the AOA value goes below the threshold for the current Mach number, when MCAS would have begun providing the stabilizer NU command. MCAS's control law is reset and MCAS then provides a stabilizer ND command a second time five seconds after the reset [MCAS-UCA-3]. If the flight crew reacts in the same manner to the second MCAS command, the system is reset again and the UCA may repeat itself. As a result, the aircraft is out of trim by an amount dependent on the number of successive MCAS stabilizer ND commands [H-3-1].

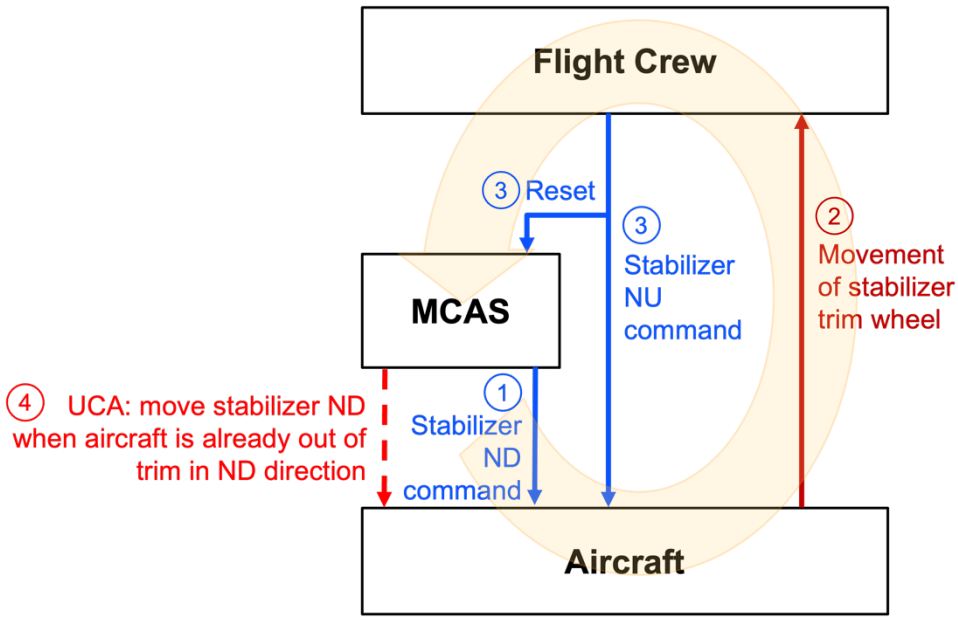


Figure 25. Visualization of MCAS-Scen-3.3

In this scenario, the flight crew's response to an MCAS activation actually leads MCAS to activate again, which in turn can lead the flight crew to respond again. Though the temporal sequence is linear (because time is linear), the causality is circular, and the scenario can repeat itself multiple times as a result. Identifying scenarios that exhibit circular causality like this one can force the analyst to examine the effects of repeated control actions.

The STPA handbook [19] explicitly lists “repeated” control actions as a subcategory of when providing a control action may be unsafe. Traditional failure-based safety assessment processes do not typically include “repeated” failures in their analysis, because physical components tend to fail once and then remain in a failed state. However, intended functions may repeatedly activate in an unsafe context, and STPA can help uncover scenarios for why that might occur.

Examining repeated control actions can also force the analyst to question their assumptions regarding the independence of system behavior and operational states or conditions. If a control action is only unsafe in a particular context, then the analyst needs to verify that the control action itself cannot place the system in that context. The context that makes the command in MCAS-UCA-3 unsafe is the fact that the aircraft is already out of trim in the ND direction. By revealing that the aircraft could be out of trim because of MCAS itself, the scenario helps uncover that the UCA and the context are not independent.

Chapter 5

Conclusion

5.1. Summary of Contributions

This thesis provided an analysis of the current processes used to assess the safety of commercial aircraft, with a focus on uncovering areas for improvement in existing standards. The study's methodology involved first applying Causal Analysis based on Systems Theory to the Boeing 737 MAX accidents. The findings from CAST were then used to identify four key areas where current safety assessment guidance could be improved, to increase the chance of proactively identifying the kinds of causal factors that caused those crashes.

The findings showed that current standards are limited when it comes to integrating human considerations in the safety assessment process, including validating human response assumptions, and identifying how unintended human interactions can create unsafe situations. The standards also do not provide a systematic methodology that supports the identification of unrecognized assumptions, despite emphasizing the need for documenting them. The safety assessment process is also heavily focused on identifying how component and functional failures can have catastrophic consequences, with limited guidance for uncovering unsafe scenarios that stem from external factors or interactions between components working as designed. Finally, the linear chain-of-events based methods recommended for safety assessment are limited in their ability to capture more complex non-linear causal relationships, especially those between functional failures and operational events and conditions. The CAST revealed how each of these limitations played a role in the 737 MAX accidents.

Besides identifying areas for improvement, another contribution of this thesis is exploring how a systems theoretic approach to safety assessment can help address these gaps. System Theoretic Process Analysis was applied to the key systems involved in the 737 MAX accidents to show the kinds of causal factors that STPA can identify. The scenario-based framework that incorporates humans and software into the hazard analysis was found to support validation of human response assumptions, identification of assumptions, assessing safety of intended behavior, and understanding complex non-linear causal relationships.

Finally, an additional contribution of this work is a demonstration of how CAST can be used to understand the factors influencing decisions made during design and safety assessment processes. Thoroughly investigating accidents involving system design errors requires understanding not only how the system's complexity affected a flight crew's actions, but also why that complexity was built into the system in the first place, and why the complex interactions leading to the accident were not identified during assurance and certification activities. The application of CAST to the 737 MAX accidents demonstrates the potential for accident investigators to generate recommendations not only for fixing specific design flaws, but also to improve design practices, safety assessment standards, and regulatory oversight processes.

5.2. Limitations and Future Work

Though the findings of this study provide a baseline for understanding the gaps in current safety assessment guidance, there is still plenty of room for future research into this topic.

First, the STPA in this study was done on a system that has already been involved in two major accidents. Therefore, it is difficult to completely avoid hindsight bias in the analysis results, as certain MCAS design flaws are already well known and have been extensively studied. Thus, there is room for researchers and industry professionals to apply STPA to novel systems that may or may not have already been certified using traditional approaches to identify resource requirements and further compare certification approaches.

Additionally, the goal of this study was to identify certain limitations in safety assessment standards and examine whether STPA as a methodology can help address these gaps. It was not our goal to provide a new STAMP-based framework for developing and assessing the safety of commercial aircraft. It is clear that STPA has benefits when it comes to identifying and mitigating safety concerns, but it is still unclear how exactly the methodology can be incorporated into the safety assessment process and be used as a means for complying with regulation. Understanding STPA's role and developing new guidelines for its use towards certification should be a collaborative effort with appropriate representation from industry, academia, and government. The aviation community (and the safety community more broadly) should be actively working towards ensuring that safety assessment approaches keep up with the complexity of the systems being built.

References

[1] "Statistical Summary of Commercial Jet Airplane Accidents - Worldwide Operations 1959-2022," The Boeing Company, September 2023.

[2] Komite Nasiional Keselamatan Transportasi, "Aircraft Accident Investigation Report: PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP; Tanjung Karawang, West Java; Republic of Indonesia; 29 October 2018," KNKT.18.10.35.04, Jakarta, October 2019.

[3] Aircraft Accident Investigation Bureau, "Investigation Report on Accident to the B737-MAX 8 Reg. ET-AVJ Operated by Ethiopian Airlines," The Federal Democratic Republic of Ethiopia Ministry of Transport and Logistics, December 2022.

[4] Ibrahim, M., and Durak, U., "The Current Regulatory Framework and the Overarching Properties," presented at the 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC), Barcelona, Spain, 2023. https://doi.org/10.1109/DASC58513.2023.10311222

[5] Federal Aviation Administration, "AC 25.1309-1A: System Design and Analysis," Jun 21 1988.

[6] Federal Aviation Administration, "AC 25.1309-1B ARSENAL Draft: System Design and Analysis," Jun 10 2002.

[7] Spitzer, C. R., Ed., "Avionics: Development and Implementation," CRC Press, Boca Raton, 2007.

[8] Atherton, M. J., "System Theoretic Framework for Assuring Safety and Dependability of Highly Integrated Aero Engine Control Systems," Thesis. Massachusetts Institute of Technology, 2005.

[9] Federal Aviation Administration, "AC 25.1302-1: Installed Systems and Equipment for Use by the Flightcrew," May 03 2013.

[10] S-18 Aircraft and Sys Dev and Safety Assessment Committee, "ARP4754B: Guidelines for Development of Civil Aircraft and Systems," SAE International. https://doi.org/10.4271/ARP4754B

[11] Radio Technical Commission for Aeronautics, "DO-178C: Software Considerations in Airborne Systems and Equipment Certification," Jan 05 2012.

[12] Radio Technical Commission for Aeronautics, "DO-254: Design Assurance Guidance for Airborne Electronic Hardware," Apr 19 2000.

[13] S-18 Aircraft and Sys Dev and Safety Assessment Committee, "ARP4761A: Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment," SAE International. https://doi.org/10.4271/ARP4761A

[14] Federal Aviation Administration, "AC 20-115 D: Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )," Jul 21 2017.

[15] Jacklin, S., "Certification of Safety-Critical Software Under DO-178C and DO-278A," presented at the Infotech@Aerospace 2012, Garden Grove, California, 2012. https://doi.org/10.2514/6.2012-2473

[16] Leveson, N. G., "Engineering a Safer World: Systems Thinking Applied to Safety," The MIT Press, Cambridge, Massachusetts, 2017.

[17] Weinberg, G. M., "An Introduction to General Systems Thinking: Gerald M. Weinberg," Dorset House, New York, NY, 2001.

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

[19] Leveson, N. G., and Thomas, J., "STPA Handbook," Mar2018.

[20] Herkert, J., Borenstein, J., and Miller, K., "The Boeing 737 MAX: Lessons for Engineering Ethics," *Science and Engineering Ethics*, Vol. 26, No. 6, 2020, pp. 2957–2974. https://doi.org/10.1007/s11948-020-00252-y
[21] Federal Aviation Administration, "Summary of the FAA's Review of the Boeing 737 MAX," U.S. Department of Transportation, November 2020.
[22] Federal Aviation Administration, "Commercial Airplane Certification Process Study: An Evaluation of Selected Aircraft Certification, Operations and Maintenance Processes," March 2002.
[23] National Transportation Safety Board, "Safety Report on the Treatment of Safety-Critical Systems in Transport Airplanes," NTSB/SR-06/02 PB2006-917003 Notation 7752A, April 2006.
[24] National Transportation Safety Board, "Loss of Control and Crash Marlin Air Cessna Citation 550, N550BP Milwaukee, Wisconsin June 4, 2007," NTSB/AAR-09/06 PB2009-910406, 490 L'Enfant Plaza, S.W. Washington, D.C. 20594, October 2009.
[25] National Transportation Safety Board, "Safety Recommendation," National Transportation Safety Board, Washington, D.C. 20594, August 2009.
[26] National Transportation Safety Board, "Runway Overrun During Rejected Takeoff Global Exec Aviation Bombardier Learjet 60, N999LJ Columbia, South Carolina September 19, 2008," NTSB/AAR-10/02 PB2010-910402, 490 L'Enfant Plaza, S.W. Washington, D.C. 20594, April 2010.
[27] Australian Transportation Safety Bureau, "In-Flight Upset 154 Km West of Learmonth, WA 7 October 2008 VH-QPA Airbus A330-303," AO-2008-070, Australian Government, 62 Northbourne Avenue Canberra, Australian Capital Territory 2601, December 2011.
[28] National Transportation Safety Board, "Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance," Safety Recommendation Report ASR-19-01, Washington, DC 20594, September 2019.
[29] Joint Authorities Technical Review, "Boeing 737 MAX Flight Control System Observations, Findings and Recommendations," October 2019.
[30] Special Committee to Review the Federal Aviation Administration's Aircraft Certification Process, "Official Report of the Special Committee to Review the Federal Aviation Administration's Aircraft Certification Process | US Department of Transportation," January 2020.
[31] 116th United States Congress, "Consolidated Appropriations Act, 2021," Public Law 116–260, 127, 2020.
[32] Federal Aviation Administration, "Safety Issues and Shortcomings with Requirements Definition, Validation, and Verification Processes Final Report.," DOT/FAA/TC-16/39, William J. Hughes Technical Center, Aviation Research Division, Atlantic City International Airport, New Jersey, 08405, December 2016.
[33] Whitlow, S., Wilkinson, C., and Hamblin, C., "Assessing V&V Processes for Automation with Respect to Vulnerabilities to Loss of Airplane State Awareness."
[34] Alves, E., Bhatt, D., Hall, B., Driscoll, K., Murugesan, A., and Rushby, J., "Considerations in Assuring Safety of Increasingly Autonomous Systems," NNL16AA06B, National Aeronautics and Space Administration, May 2018.
[35] Delange, J., and Feiler, P., "Architecture Fault Modeling with the AADL Error-Model Annex," presented at the 2014 40th EUROMICRO Conference on Software Engineering

and Advanced Applications (SEAA), Verona, Italy, 2014. https://doi.org/10.1109/SEAA.2014.20
[36] Leveson, N., Wilkinson, C., Fleming, C., Thomas, J., and Tracy, I., "A Comparison of STPA and the ARP 4761 Safety Assessment Process."
[37] Leveson, N. G., "An Introduction to System Safety Engineering," The MIT Press, 2023.
[38] Mutuel, L. H., "Melding System Safety Methodologies for a Structured and Comprehensive Risk Assessment of Optionally Manned Aircraft," presented at the 2020 IEEE/AIAA 39th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 2020. https://doi.org/10.1109/DASC50938.2020.9256552
[39] Voros, R., "Generalizing Aspects of System Safety to Broaden Applicability," *SAE International Journal of Advances and Current Practices in Mobility*, Vol. 3, No. 3, 2021, pp. 1272–1284. https://doi.org/10.4271/2021-01-0037
[40] Beland, S., "Role of STPA in Aircraft Standards (SAE S-18)," Cambridge, MA, Mar 27 2018.
[41] Federal Aviation Administration, "Response to Official Report of the Special Committee on the Federal Aviation Administration's Aircraft Certification Process," U.S. Department of Transportation, April 2020.
[42] S-18 Aircraft and Sys Dev and Safety Assessment Committee, "Scoping Document: S-18H Human Considerations for Safety Assessment Committee," Society of Automotive Engineers.
[43] National Transportation Safety Board, "Response to Final Aircraft Accident Investigation Report Ethiopian Airlines Flight 302 Boeing 737-8 MAX, ET-AVJ Ejere, Ethiopia March 10, 2019," January 2023, p. 7.
[44] National Transportation Safety Board, "System Safety and Certification Specialist's Report," DCA19RA017, Washington, D.C. 20594, August 2019.
[45] House Committee on Transportation and Infrastructure, "THE BOEING 737 MAX: EXAMINING THE DESIGN, DEVELOPMENT, AND MARKETING OF THE AIRCRAFT," October 2019.
[46] Peter Lemme, "Flawed Assumptions Pave a Path to Disaster," Satcom Guru, Oct 28 2019. Retrieved 20 November 2023. https://www.satcom.guru/2019/10/flawed-assumptions-pave-path-to-disaster.html
[47] Lengyel, D. M., "Examining Risk Management Failures: The Case of the Boeing 737 MAX Program," *Enterprise Risk Management*, Vol. 8, No. 1, 2023, p. 1. https://doi.org/10.5296/erm.v8i1.20916
[48] G-45 Human Systems Integration, "SAE6906A: Standard Practice for Human Systems Integration," SAE International. https://doi.org/10.4271/SAE6906A
[49] Leveson, N., "Safety III: A Systems Approach to Safety and Resilience."
[50] Leveson, N. G., "The Use of Safety Cases in Certification and Regulation," Working Paper, Massachusetts Institute of Technology. Engineering Systems Division, November 2011.
[51] Charles Haddon-Cave, "The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006," October 2009.
[52] Houck, O. A., "Worst Case and the DEEPWATER HORIZON Blowout: There Ought To Be a Law," *Tulane Environmental Law Journal*, Vol. 24, No. 1, 2010, pp. 1–18.

[53] European Union Aviation Safety Agency, “Certification Memorandum: Flight Crew Human Factors Assumptions in Aircraft and System Safety Assessments,” CM–SA-002 Issue 02.
[54] Dekker, S., “The Field Guide to Understanding ‘Human Error,’” CRC Press, Boca Raton, FL London New York, 2014.
[55] Dewar, J. A., “Assumption-Based Planning: A Tool for Reducing Avoidable Surprises,” Cambridge University Press, Cambridge ; New York, 2002.
[56] Osborne, M., Hawkins, R., Nicholson, M., and Alexander, R., “Understanding Safety Engineering Practice: Comparing Safety Engineering Practice as Desired, as Required, and as Observed,” *Safety Science*, Vol. 172, 2024, p. 106424. https://doi.org/10.1016/j.ssci.2024.106424
[57] Rahimi, M., Xiong, W., Cleland-Huang, J., and Lutz, R., “Diagnosing Assumption Problems in Safety-Critical Products,” presented at the 2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE), Urbana, IL, 2017. https://doi.org/10.1109/ASE.2017.8115659
[58] Leveson, N. G., “An Introduction to System Safety Engineering,” The MIT Press, 2023.
[59] Yohannes, E., Bekele, A., and Woldu, Z., “Bird Strike Incidence at Addis Ababa Bole International Airport,” *SINET: Ethiopian Journal of Science*, Vol. 23, No. 2, 2000, pp. 215–229. https://doi.org/10.4314/sinet.v23i2.18167
[60] Federal Aviation Administration, “AC 25-7C: Flight Test Guide For Certification Of Transport Category Airplanes,” Oct 16 2012.
[61] Malmquist, S., Carstens, D. S., and Dahlstrom, N., “Almost Like the Real Thing – The Hidden Limits in Flight Simulation and Training,” *Human Factors in Simulation and Training*, CRC Press, Boca Raton, 2023, pp. 141–158. https://doi.org/10.1201/9781003401360-6
[62] Thomas, J., “Enhancing Human Factors Analysis with STPA,” Cambridge, MA, Mar2021.
[63] France, M. E., “Engineering for Humans: A New Extension to STPA,” Massachusetts Institute of Technology, 2017.
[64] Wickens, C. D., “Noticing Events in the Visual Workplace: The SEEV and NSEEV Models,” *The Cambridge Handbook of Applied Perception Research*, edited by R. R. Hoffman, P. A. Hancock, M. W. Scerbo, R. Parasuraman, and J. L. Szalma, Cambridge University Press, 2015, pp. 749–768. https://doi.org/10.1017/CBO9780511973017.046
[65] Sarter, N. B., and Woods, D. D., “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*, Vol. 37, No. 1, 1995, pp. 5–19. https://doi.org/10.1518/001872095779049516
[66] Bishop, B. E., Harrington, P. M., Rose, R. L., and Leveson, N. G., “System Theoretic Process Analysis for Identification of Sources of Mode Confusion,” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 67, No. 1, 2023, pp. 2397–2403. https://doi.org/10.1177/21695067231192457
[67] Aeronautica Civil of the Republic of Colombia, “Controlled Flight Into Terrain American Airlines Flight 965 Boeing 757-223, N651AA near Cali, Colombia December 20, 1995,” Aeronautica Civil, Santafé de Bogotá, November 1996.
[68] Aeronautical Accident Investigation and Prevention Center (CENIPA), “Final Report A - Nº 67/CENIPA/2009,” 67/CENIPA/2009, Command of Aeronautics, October 2009.

[69] National Transportation Safety Board, “In-Flight Breakup During Test Flight Scaled Composites SpaceShipTwo, N339SS Near Koehn Dry Lake, California October 31, 2014,” NTSB/AAR-15/02 PB2015-105454, 490 L’Enfant Plaza, S.W. Washington, D.C. 20594.
[70] National Transportation Safety Board, “System Safety Group Chairman’s Factual Report,” DCA15MA019, April 2015.
[71] Leveson, N., “A Systems Approach to Risk Management through Leading Safety Indicators,” *Reliability Engineering & System Safety*, Vol. 136, 2015, pp. 17–34. https://doi.org/10.1016/j.ress.2014.10.008
[72] Thomas, J., Sgueglia, J., Suo, D., Leveson, N., Vernacchia, M., and Sundaram, P., “An Integrated Approach to Requirements Development and Hazard Analysis,” presented at the SAE 2015 World Congress & Exhibition, 2015. https://doi.org/10.4271/2015-01-0274
[73] Civil Aviation Administration of China, “Aircraft Severe Incident Investigation Report,” SWCAAC-SIR-2018-1, June 2020.
[74] Slominski, H. M., “Using STPA and CAST to Design for Serviceability and Diagnostics,” Massachusetts Institute of Technology, Cambridge, MA, 2020.
[75] Fletcher, W. S., “Application of System Theoretic Process Analysis to Requirements and Algorithms for a Thrust Control Malfunction Protection System,” Cambridge, MA, Mar2014.
[76] Thomas, J., “Empirical Evaluations of STPA in the Aviation Industry,” Cambridge, MA, Jun2023.
[77] Abrecht, B., Arterburn, D., Horney, D., Schneider, J., Abel, B., and Leveson, N., “A New Approach to Hazard Analysis for Rotorcraft,” presented at the AHS Development, Affordability and Qualification of Complex Systems Specialists’ Meeting, Huntsville, AL, 2016.
[78] Sterman, J. D., “Business Dynamics: Systems Thinking and Modeling for a Complex World,” Irwin/McGraw-Hill, Boston, 2009.

Appendix A – 737 MAX Accidents CAST

A.1. Basic Information

The first step of CAST is assembling the basic information about the accident. All of the information for this CAST analysis came from publicly available sources [2,3,20,21,28–30,41,43–47]. The losses in both accidents are clear: the destruction of both aircraft and the death of their occupants. The system in each case is defined as the aircraft and its occupants (including the flight crew), the airline, the airport and air traffic control facilities, the aircraft and subsystem manufacturers, and the regulatory authorities that oversaw each step of the aircraft's certification and operation. Elements such as weather or bird strikes are treated as environmental conditions since engineers have no control over them, but measures to counteract this are considered as part of the system, as engineers design them with a purpose.

The system level hazards and safety constraints for both accidents are similar, so they are consolidated in this section:

System Hazard 1: Aircraft does not maintain adequate separation from outside objects
Safety Constraints:

- Aircraft must maintain adequate separation from outside objects
- Aircraft must be able to detect and recover from a violation of adequate separation

System Hazard 2: Aircraft is unable to be controlled
Safety Constraints:

- Aircraft must remain under positive control
- Aircraft must be able to safely recover from a loss of control

System Hazard 3: Aircraft loses ability to remain airborne
Safety Constraints:

- Aircraft must be at a speed and attitude which preserves its ability to remain airborne
- Aircraft must be able to detect and recover from a speed or attitude in which it cannot remain airborne

Tables I and II below indicate the proximal events leading up to the losses of JT610 and ET302 respectively:

Table A.I. Proximal Events Leading up to Loss of Flight JT610

ID	Event
1	On 10/28/2018, the left Angle of Attack (AOA) sensor was replaced on the aircraft registered PK-LQP in Denpasar. The AOA sensor was a 21° bias.
2	That same day, Lion Mentari Air flight JT043 flew from Denpasar to Jakarta. During the flight, there were many indications, including Indicated Airspeed Disagree (IAS DISAGREE) and Altitude Disagree (ALT DISAGREE), due to the 21° bias on the AOA sensor. The left control column stick shaker was active during the flight and MCAS was activated many times, however, the flight crew was able to stop the repetitive MCAS activations by switching the stabilizer trim to CUT OUT.

3	After landing in Jakarta, the flight crew reported some malfunctions on the aircraft, but didn't include the activation of the stick shaker and the switching of the stabilizer trim to CUT OUT in the report
4	On 10/29/2018, 23:20:33 UTC, Lion Mentari Air flight JT610 took off normally, however the left control column stick shaker activated, which continued for most of the flight
5	23:20:44, the First Officer (FO) advised the captain of IAS DISAGREE. The left indicated airspeed (IAS) was 164 knots and the right IAS was 173 knots. The IAS DISAGREE message appeared until the end of the recording.
6	23:21:12, the FO advised the captain of ALT DISAGREE and the captain acknowledged. The altimeter on the captain's PFD indicated 340 feet and on the FO's PFD indicated 570 feet
7	23:21:37, the captain instructed the FO to perform memory items for airspeed unreliable. The FO did not respond to this request
8	23:21:45, the FO requested clearance from the Tower East (TE) air traffic controller for a holding point for their condition. The TE controller asked what the aircraft problem was, and the FO responded, "flight control problem". The TE controller did not acknowledge the flight crew request to go to a holding point and only remembered the problem reported by the flight crew
9	23:22:04, the FO suggested whether the captain wanted to reconfigure the flaps setting to flaps 1, and the captain agreed.
10	23:22:32, the aircraft Enhance Ground Proximity Warning System (EGPWS) sounded "BANK ANGLE" three times, and the aircraft roll momentarily reached 35°
11	23:22:33, the flaps reached the fully retracted position and the automatic Aircraft Nose Down (ND) trim was active for 10 seconds, during which the horizontal stabilizer pitch trim decreased from 6.1 to 3.8 units
12	23:22:48, the flaps reached position 1 and the left control column stick shaker stopped briefly
13	23:22:54, the automatic ND trim activated for 8 seconds. 6 seconds later, the aircraft EGPWS sounded "AIR SPEED LOW" twice.
14	23:23:00, the flight crew selected flaps 5 and the flaps began to travel from position 1 to 5. The captain commanded NU trim for 5 seconds and the pitch trim was recorded at 4.8 units. 4 seconds later the left control column stick shaker activated and continued until the end of the recording
15	At 23:24:05, the captain commanded the FO to perform the Airspeed Unreliable Non-Normal checklist (NNC), which was acknowledged by the FO. The FO at first was unable to locate the Airspeed Unreliable checklist. At 23:25:17, the FO located the Airspeed Unreliable checklist and began reading it
16	23:25:27, the automatic ND trim was activated by the Maneuver Characteristic Augmentation System (MCAS) for 2 seconds and was interrupted by the captain who commanded NU trim for 6 seconds
17	From 23:26:00 to 23:26:45, MCAS activated 6 times with the captain countering it using NU trim
18	The TE controller instructed the flight crew to turn right heading 070° to avoid traffic. The FO did not respond to the TE controller's instruction. The controller then called JT610 twice and the FO responded at 23:27:13
19	From 23:27:29 to 23:29:14, MCAS activated 9 times with the captain countering it using NU trim
20	23:30:02, the FO contacted the Arrival (ARR) controller and advised them that they were experiencing a flight control problem. The ARR controller advised the crew to prepare for landing on runway 25L
21	From 23:30:18 to 23:30:38, MCAS activated twice, and the captain countered it using NU trim
22	23:30:48, the captain asked the FO to take control of the aircraft, which he did
23	23:31:15, MCAS activated for about 3 seconds until it was interrupted at 23:31:17 when the FO commanded NU trim for 1 second. The FO's column sensor force recorded 65 pounds of back pressure
24	23:31:27, MCAS activated for 8 seconds, and the FO's control column sensor force recorded 82 pounds
25	23:31:43, MCAS activated for 4 seconds, and the FO's control column sensor recorded 93 pounds

26	23:31:53, MCAS activated until the DFDR stopped recording at 23:31:54 and the Cockpit Voice Recorder (CVR) stopped recording 1 second later

Table A.II. Proximal Events Leading up to Loss of Flight ET302

ID	Event
1	03/10/2019, 05:36:12 UTC, Ethiopian Airlines flight ET302 lined up on runway 07R at Addis Ababa Bole International Airport (ADD) in Addis Ababa, Ethiopia, bound for Jomo Kenyatta International Airport in Nairobi, Kenya
2	Takeoff procedures were executed as normal, at 05:38:34 the FO called “rotate” and the airplane lifted off
3	05:38:44, shortly after liftoff, the left and right recorded AOA values began deviating and left stick shaker activated
4	05:38:48, the “MASTER CAUTION” and “ANTI-ICE” lights on the glare shield Illuminated
5	05:38:56, the captain attempted to engage the autopilot, which did not engage
6	05:39:01, captain attempted to engage autopilot again, which still did not engage
7	05:39:23, crew successfully engaged autopilot
8	05:39:38, 800ft above field elevation was reached and autothrottle (A/T) switched to ARM mode
9	05:39:45, captain initiated retraction of flaps
10	05:39:56, the A/P disconnected automatically
11	05:40:00, flaps completed retraction and MCAS issued automatic nose-down trim command for 9 seconds
12	05:40:14, captain trimmed nose up for about 2 seconds with the main electric trim switches
13	05:40:22, five seconds after the end of captain’s trim inputs, MCAS issued a second automatic nose-down trim
14	05:40:28, crew reacted with manual electric trim for 9 seconds
15	05:40:38, stab trim cutout switches moved to “CUTOUT” position
16	05:40:43, MCAS issued third automatic nose-down trim command, which does nothing as cutout switches were engaged
17	05:40:45, captain repeatedly requested the F/O to pull up with him
18	05:41:21, aircraft speed exceeded 340Kt and the overspeed warning sounded
19	05:41:47, captain asked FO if the trim was functional and recommended manual trim
20	05:41:56, FO was unable to trim manually
21	05:42:47, captain and FO acknowledged “left alpha vane” issue
22	05:43:04, stabilizer trim cutout switches moved back to original position
23	05:43:11, crew attempted to reengage autopilot and issue two short manual electric trim commands
24	05:43:21, MCAS issued fourth automatic nose-down trim command
25	05:43:36, the enhanced ground proximity warning system (EGPWS) sounded: “Terrain, Terrain, Pull Up, Pull up”
26	05:43:44, end of cockpit voice recording

A.2. Safety Control Structures

The control structures which describe the systems being examined are shown in the figures below. The control structures for JT610 and ET302 are similar, but not identical.

A.2.1. JT610 Control Structures

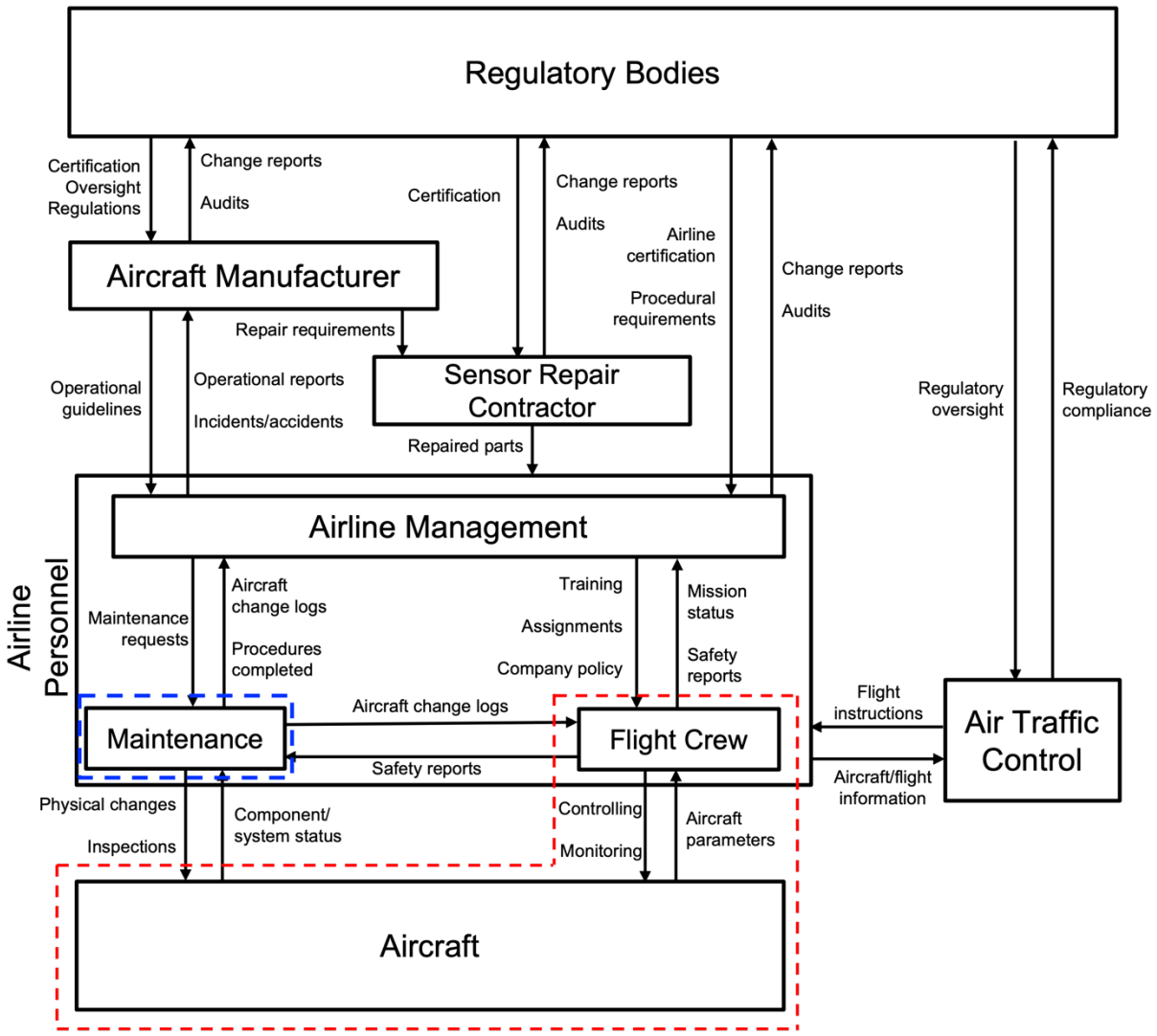


Figure A.1. JT610 higher level control structure

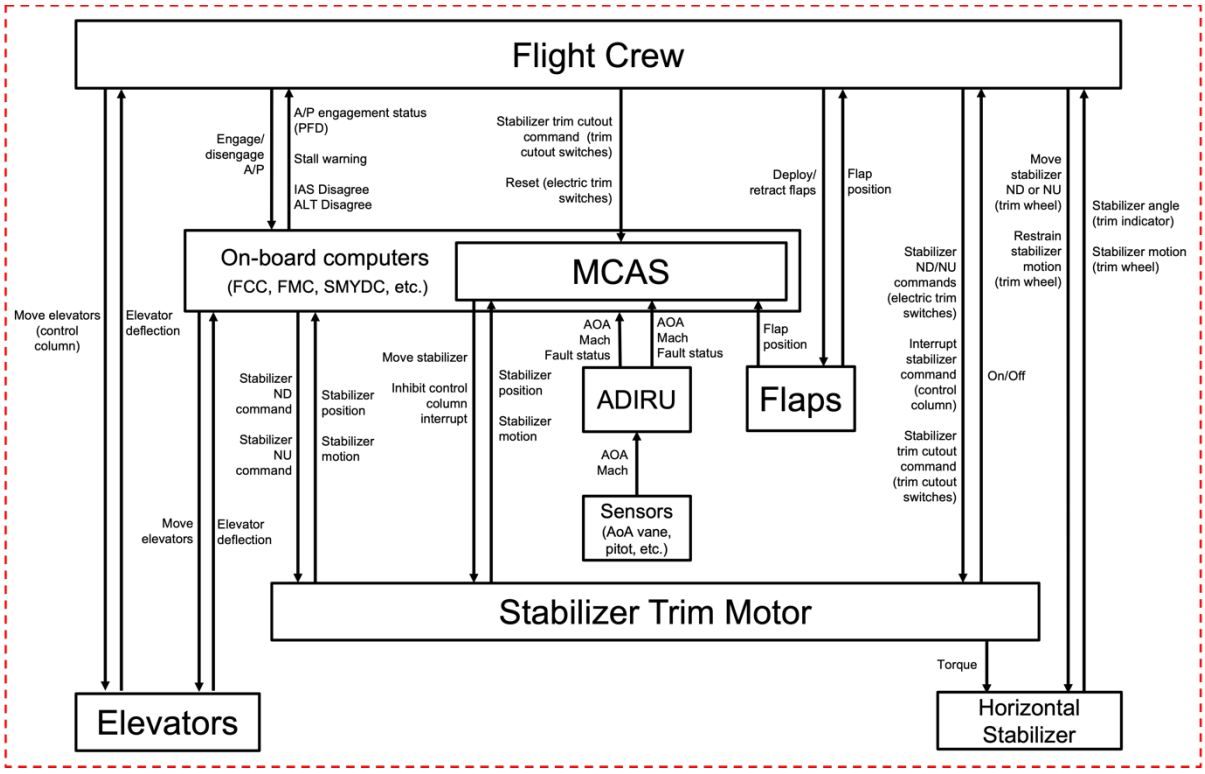


Figure A.2. JT610 aircraft-level control structure

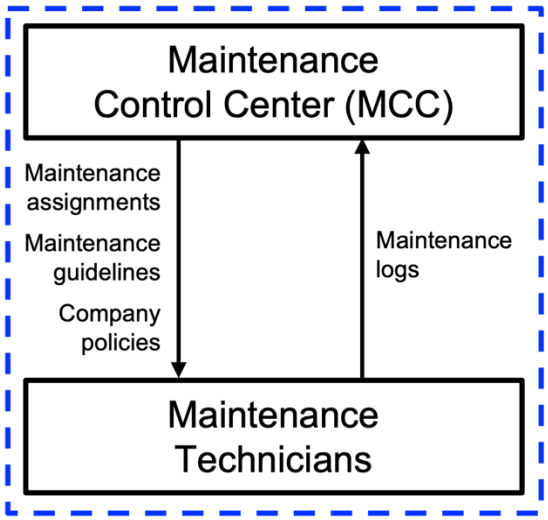


Figure A.3. JT610 maintenance control structure

A.2.2. ET302 Control Structures

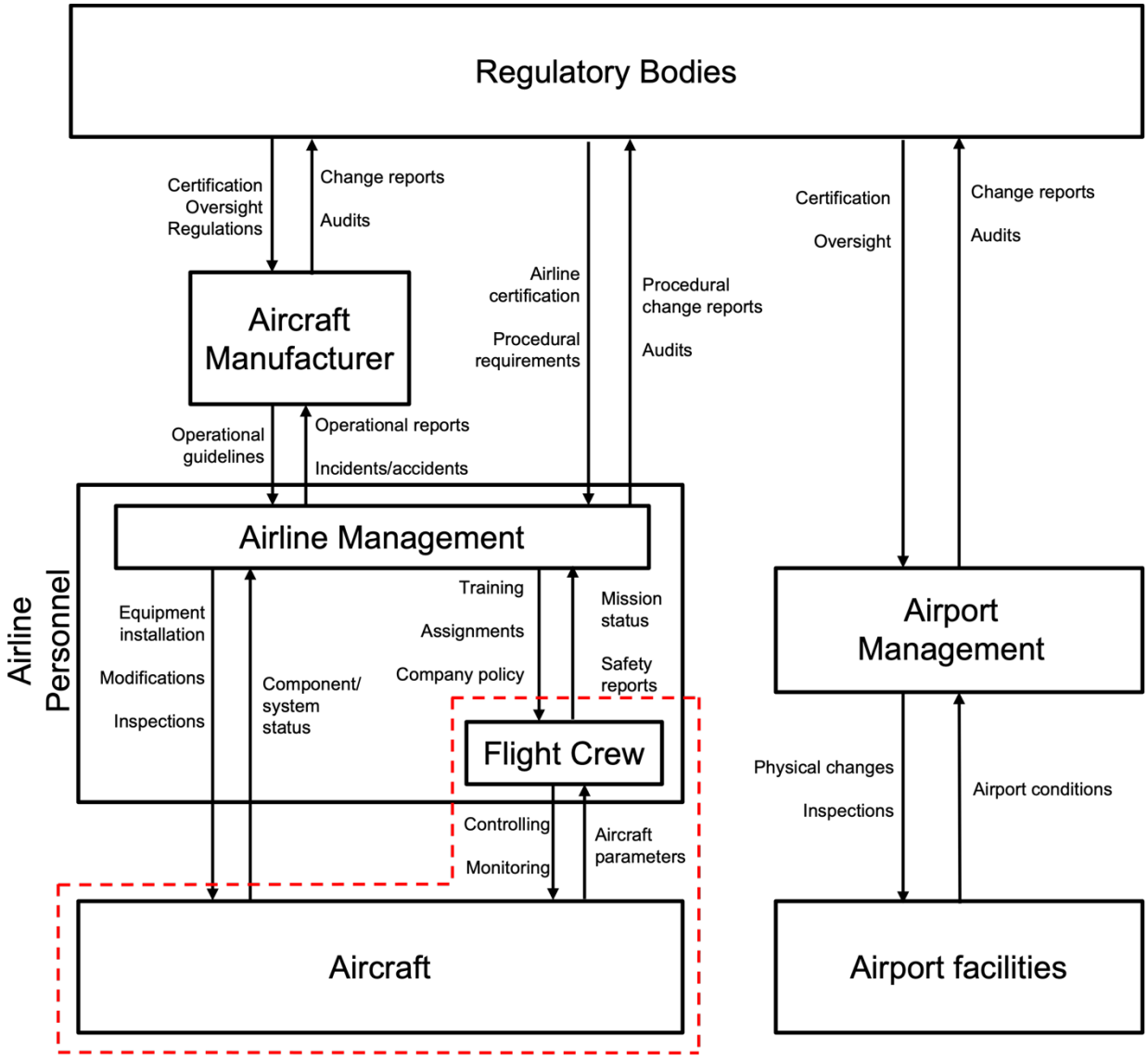


Figure A.4. ET302 higher level control structure

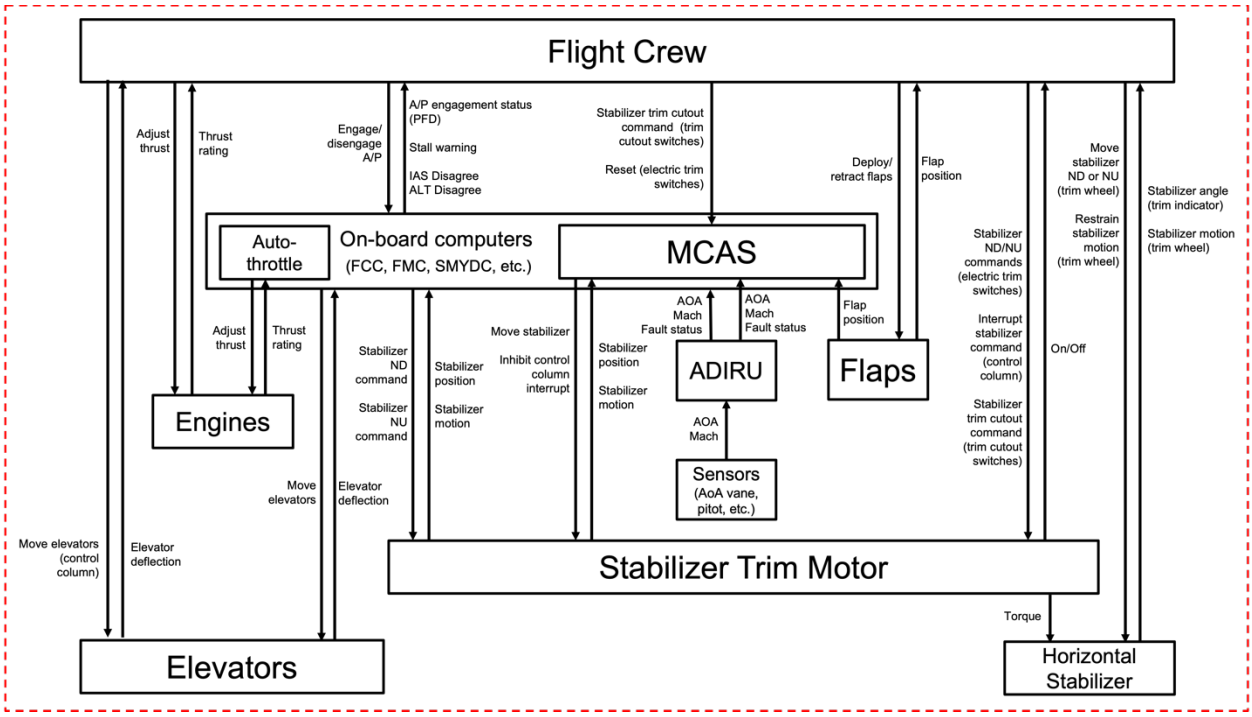


Figure A.5. ET302 aircraft-level control structure

A.3. Contributions of each Controller in the Losses

A.3.1. Role of Physical Components

The main safety requirement for the physical system is to provide physical protection against the system hazards described in section A.1. The requirements and the equipment/controls meant to satisfy these requirements are described below:

Requirements:

- Provide the ability for the aircraft to be controlled
- Provide feedback to the human and automated controllers of the aircraft
- Provide alarms to the flight crew in case the requirements above are not being met

Safety Equipment/Controls:

- Control surfaces
- Sensors
- Cockpit displays and alarms

Next, it is necessary to examine whether failures or unsafe interactions caused these controls to be unable to enforce their respective safety requirements in each of the accidents. Also discussed below are the contextual factors which contributed to these unsafe interactions.

Failures:

- **JT610:** No physical failures occurred during flight JT610 until the moment of impact. However, the left angle of attack (AOA) sensor possessed a bias of 21° which was not visible to the flight crew, and ultimately influenced the commands issued by the aircraft's automated systems. The reasons for this bias will be discussed during the analysis of the role of each controller in the accident.
- **ET302:** A single physical failure likely occurred during flight ET302, before the moment of impact. Ten seconds after rotation, the left AOA sensor value began diverging from the right sensor value. Left AOA went from 11.1° to 35.7° to 74.5° within a span of ¾ seconds. This erroneous AOA value ultimately influenced the commands issued by the aircraft's automated systems. The reasons for the erroneous values are disputed, with the most likely explanation being impact with a foreign object (most likely a bird).

Unsafe Interactions:

- **JT610:** All physical components of the aircraft functioned exactly as they had been designed to function, up to the moment of impact. The only true unsafe interaction occurred between the AOA sensor with the bias and MCAS, as MCAS used erroneous data shared by the AOA sensor
- **ET302:** Besides the faulty left AOA sensor, all other physical components of the aircraft functioned as they had been designed to function, up to the moment of impact. The main unsafe interaction between these components occurred between the aircraft's manual stabilizer trim system and the overall flight conditions encountered near the end of the flight. Due to an overspeed condition (the reasons for which will be examined in a later section), manual stabilizer trim became unavailable to the flight crew as a result of high aerodynamic loading of the horizontal stabilizer.

In summary, besides the faulty left AOA sensor on ET302, no physical components of either system failed or performed in any way that contradicted their functional requirements. The erroneous activation of MCAS on both flights occurred as a result of erroneous AOA data, which the system utilized when determining when whether or not to activate.

A.3.2. Role of each Controller in the Loss of JT610

A.3.2.1. On-board computers (FCC, FMC, SMYDC, etc. but not including MCAS)

Responsibilities:

- Assist flight crew in controlling aircraft
- Inform flight crew of the current state of the aircraft and its automated systems
- Alert pilots of actions needed in order to maintain safe flight

JT610 Computer Control Actions:

- **610Comp-UCA-1:** Stick shaker activated when aircraft was not in a stall
- **610Comp-UCA-2:** The enhanced ground proximity warning system (EGPWS) falsely sounded "AIRSPEED LOW" 2 times

JT610 Computer Process Model Flaws:

- **610Comp-PMF-1:** Stall management/yaw damper computer (SMYDC) believed the aircraft was in a stall when it wasn't due to the 21° bias in the left AOA sensor [610Comp-UCA-1]
- **610Comp-PMF-2:** The EGPWS believed the airspeed was low because of the incorrectly indicated airspeed on the captain's side, computed using the erroneous AOA [610Comp-UCA-2]

JT610 Computer Contextual Factors:

- **610Comp-CF-1:** The left AOA sensor was calibrated incorrectly and had a bias of 21°. Because the captain was the Pilot Flying (PF), the left AOA sensor was used to inform the SMYDC and EGPWS [610Comp-UCA-1, -2]

Questions raised:

- Why did the SMYDC and EGPWS select only one AOA sensor to consider for stall warning? Was it possible to detect that the stick shaker only activated on the left side?

A.3.2.2. MCAS

Responsibilities:

- Provide commands to move the horizontal stabilizer in the direction of "aircraft nose down" (ND) during flaps up, high angle of attack maneuvers
- Provide an increase in stick force gradient and a reduced pitch up tendency in the aforementioned condition

JT610 MCAS Control Actions:

- **610MCAS-UCA-1:** MCAS repeatedly activated and commanded nose-down trim when aircraft was not at a high angle of attack
- **610MCAS-UCA-2:** MCAS inhibited flight crew's ability to override electric trim commands using the control column

JT610 MCAS Process Model Flaws:

- **610MCAS-PMF-1:** MCAS determined aircraft was beyond the AOA threshold for activation due to receiving erroneous AOA values from air data inertial reference system (ADIRS) [610MCAS-UCA-1]

JT610 MCAS Contextual Factors:

- **610MCAS-CF-1:** MCAS belongs to the FCC, each of which only pulls information from its associated ADIRS [610MCAS-UCA-1]
- **610MCAS-CF-2:** The left AOA sensor was calibrated incorrectly and had a bias of 21° [610MCAS-UCA-1]
- **610MCAS-CF-3:** MCAS intentionally inhibits control column cutout because the original situation in which MCAS was designed to act would require it to act in opposition to pilots' control column inputs [610MCAS-UCA-2]

Questions raised:

- Why did the FCC only source its information from one ADIRS?
- Why are there no ways for flight crews to deactivate MCAS without removing their own access to electric trim?
- Was there a way for MCAS to detect how much was retrimmed by the crew and not reactivate to the full extent in response?

A.3.2.3. Flight Crew

Responsibilities:

- Configure aircraft for current phase of flight by arming/disarming and activating/deactivating aircraft systems
- Ensure correct execution of automated tasks through verification
- Continuously monitor aircraft functions and alarms
- Respond to unsafe conditions that develop
- Make decisions about safety-critical procedures to be executed

JT610 Flight Crew Unsafe Control Actions:

- **610FC-UCA-1:** Captain did not diagnose that left-hand airspeed readings were unreliable
- **610FC-UCA-2:** Captain did not call for or perform runaway stabilizer procedure
- **610FC-UCA-3:** Captain did not communicate the need to repeatedly retrim aircraft to FO upon transferring control
- **610FC-UCA-4:** FO did not immediately perform airspeed unreliable memory items when prompted by captain
- **610FC-UCA-5:** FO did not complete airspeed unreliable checklist [610FC-UCA-1]
- **610FC-UCA-6:** FO did not declare emergency or urgency to ATC beyond communicating "flight control problems"
- **610FC-UCA-7:** FO did not retrim aircraft sufficiently after repeated MCAS ND commands upon receiving control
- **610FC-UCA-8:** Crew did not discuss the aircraft problems previously recorded in the Aircraft Flight Maintenance Log (AFML)

JT610 Flight Crew Process Model Flaws:

- **610FC-PMF-1:** Captain's potentially flawed understanding of the aircraft's speed and attitude due to conflicting stick shaker activation and additional cockpit instrumentation indicating level pitch and relatively high speed [610FC-UCA-1, 2]
- **610FC-PMF-2:** Captain's potentially flawed model of the FO's understanding of the aircraft's state [610FC-UCA-3]
- **610FC-PMF-3:** Captain was potentially unaware of the extent he was retrimming the aircraft after each MCAS activation [610FC-UCA-3]
- **610FC-PMF-4:** FO potentially unaware that they would be unable to perform the memory items, if that had not been trained in a long time [610FC-UCA-4]
- **610FC-PMF-5:** FO potentially unaware of the extent to which the aircraft needed to be retrimmed after each MCAS activation, as was preoccupied with airspeed unreliable checklist while captain was doing this [610FC-UCA-7]
- **610FC-PMF-6:** Flight crew most likely did not believe stabilizer runaway was occurring, as the observed stabilizer behavior was not consistent with a runaway (intermittent instead of continuous) [610FC-UCA-2]

JT610 Flight Crew Contextual Factors:

- **610FC-CF-1:** FO was unable to complete airspeed unreliable checklist [610FC-UCA-1, 2]
- **610FC-CF-2:** Stick shaker active from rotation until the end of the flight, with brief pause when flaps were at position 1 [610FC-UCA-1]
- **610FC-CF-3:** Enhanced Ground Proximity Warning System sounded "AIR SPEED LOW – AIR SPEED LOW" when ATC informed that ground speed was 322 knots [610FC-UCA-1]
- **610FC-CF-4:** AOA Disagree message not displayed on B737 MAX 8 not fitted with optional AOA indicator [610FC-UCA-1]
- **610FC-CF-5:** Flight crew did not discuss problems observed on JT043 [610FC-UCA-1, 2, 3]
- **610FC-CF-6:** MCAS never mentioned in flight crew manuals or training [610FC-UCA-2, 3]
- **610FC-CF-7:** Captain was focused on flying the aircraft and retrimming prior to handing control to FO and did not communicate need to retrim [610FC-UCA-1, 2]
- **610FC-CF-8:** Misidentifying non-normal checklists had appeared on the FO's training records [610FC-UCA-4, 5]
- **610FC-CF-9:** FO was cleared to fly, reinforcing belief that he was qualified to perform all necessary duties [610FC-UCA-4, 5]

- **610FC-CF-10:** Step 8 of airspeed unreliable checklist requires aircraft to be trimmed and stabilized condition, a state which was not reached [610FC-UCA-5]
- **610FC-CF-11:** ATC provided eight heading instructions after the flight crew reported that the aircraft was experiencing a flight control problem [610FC-UCA-5]
- **610FC-CF-12:** Airspeed only considered unreliable if indication differs from reference table by over 20KTS or 0.03 Mach; captain's and FO's displays differed by 15KTS [610FC-UCA-5, 6]
- **610FC-CF-13:** Electric trim inputs required to re-trim after MCAS activations were significantly longer than trim inputs pilots are accustomed to making [610FC-UCA-7]
- **610F-CF-14:** Aircraft is typically quite sensitive to trim inputs, so pilots are trained to trim in small bursts as opposed to sustained segments of time [610FC-UCA-7]
- **610FC-CF-15:** Flight crew did not discuss problems observed on JT043 [610FC-UCA-4, 5, 6, 7]
- **610FC-CF-16:** Flight crew may not have been aware of aircraft problems that might reappear during their flight because in the past it was not necessary to read the AFML [610FC-UCA-8]

Questions Raised:

- What are the requirements to consider a situation an emergency/urgency?
- What actions were taken to help the FO remember the memory items during training? Was this a common checklist to be performed? How often was it trained? Did the airline have any way of knowing this pilot did not have the procedure memorized? Where was the non-normal checklist located? Was it easy to access/locate?
- What was the guidance on information that needed to be shared when transferring control from captain to FO?

A.3.2.4. Air Traffic Control (ATC)

Responsibilities:

- Monitor and direct aircraft movement
- Issue navigational instructions to pilots
- Prioritize airspace for aircraft experiencing difficulties or having declared an emergency

JT610 ATC Control Actions:

- **610ATC-UCA-1:** ATC did not acknowledge the captain's request to go to a holding point
- **610ATC-UCA-2:** ATC gave several new heading instructions to the flight crew when the crew had not yet reached the previously instructed heading

JT610 ATC Process Model Flaws:

- **610ATC-PMF-1:** ATC most likely did not consider the situation as severe as it was, since the flight crew did not declare an emergency or urgency [610ATC-UCA-1]
- **610ATC-PMF-2:** ATC may have thought the new heading positions were needed due to external circumstances (nearby aircraft, etc.) [610ATC-UCA-2]

JT610 ATC Contextual Factors:

- **610ATC-CF-1:** Tower controller did not acknowledge the flight crew's request, and when questioned about it, they claimed they did not remember the FO requesting a holding point [610ATC-UCA-1]

Questions raised:

- Could ATC have considered the flight control problem a suspected emergency even before it was declared? When can an ATC declare an emergency even if the captain/FO doesn't?

A.3.2.5. Maintenance Engineers

Responsibilities:

- Follow orders from airline management with regards to modifications that need to be made to aircraft
- Perform inspections on aircraft to determine aircraft state and changes that need to be made
- Inform airline management of changes made to aircraft through reports
- Determine the urgency of corrective control measures based on perceived risk of each aircraft modification

JT610 Maintenance Engineer Control Actions:

- **610ME-UCA-1:** Maintenance engineer in Denpasar installed an AOA sensor with a bias when replacing the left AOA sensor prior to flight JT043
- **610ME-UCA-2:** Maintenance engineer in Denpasar used an alternate installation test rather than the standard installation test for the AOA sensor
- **610ME-UCA-3:** Maintenance engineer in Jakarta released the aircraft into service without rectifying the problem or recording whether they had conducted the IFIM task for "IAS DISAGREE shows on PFD – captain's"

JT610 Maintenance Engineer Process Model Flaws:

- **610ME-PMF-1:** Maintenance personnel believed that the sensor they used for the replacement was not faulty because the tests they conducted during installation did not indicate that the sensor had a bias [610ME-UCA-1]
- **610ME-PMF-2:** The engineer thought that the alternative method would give the same results as the normal test [610ME-UCA-2]
- **610ME-PMF-3:** The engineer may have thought they had enough information to give to the Interactive Fault Isolation Manual (IFIM) to get a correct rectification task, as engineers were prone to entering the problem symptom reported by the flight crew in the IFIM first instead of reviewing the Onboard Maintenance Function (OMF) maintenance message [610ME-UCA-3]

JT610 Maintenance Engineer Contextual Factors:

- **610MT-CF-1:** The test equipment for the standard test (AOA test fixture SPL-1917) was not available in Denpasar [610ME-UCA-2]
- **610MT-CF-2:** IFIM task for "ALT DISAGREE shows on PFD – Captain's" and "IAS DISAGREE shows on PFD – Captain's" only requires performing visual inspection to the AOA sensors, so there was no requirement to perform AOA value test. [610ME-UCA-3]

Questions raised:

- What is the company/organization policy on using the Onboard Maintenance Function (OMF) vs. the IFIM? Are there policies stating they should/must use the OMF first to ensure they have all information possible?

A.3.2.6. Maintenance Control Center

Responsibilities:

- Set policies regarding aircraft maintenance procedures according to instructions from aircraft manufacturer
- Assign maintenance tasks to technicians and monitor performance

JT610 Maintenance Control Center Control Actions:

- **610MCC-UCA-1:** Defined a "repetitive problem" differently between Lion Air Company Maintenance Manual (CMM) and the Batam Aero Technic (BAT) Approved Maintenance Organization Quality System Manual (AMOQSM)

JT610 Maintenance Control Center Process Model Flaws:

- **610MCC-PMF-1:** Lion Air management believed its policy and the policy of BAT were the same because BAT is a subsidiary of Lion Air, but manuals had different policies [610MCC-UCA-1]

JT610 Maintenance Control Center Contextual Factors:

- **610MCC-CF-1:** Lion Air did not monitor repetitive problem policy of BAT as a subcontracted entity [610MCC-UCA-1]

Questions raised:

- Was the Lion Air CMM policy communicated to the BAT workers, and vice versa? If so, how? What did the synchronization efforts look like for company policy?

A.3.2.7. Lion Air Management

Responsibilities:

- Follow documented procedures for operating and maintaining aircraft
- Receive directives from aircraft manufacturer and regulatory bodies on changes to aircraft or procedures and make decisions on the execution of non-mandatory changes
- Communicate with maintenance team and order actions based on pilot reports and regular inspections
- Communicate with pilots regarding the responsibilities of their missions or any changes to aircraft or procedures
- Document, manage and act upon reports of safety-related incidents

JT610 Airline Management Control Actions:

- **610AM-UCA-1:** Airline management maintained inadequate training policy for pilots with difficulty handling the aircraft
- **610AM-UCA-2:** Lion Air management elected not to enable the AOA indicator on the PFDs

JT610 Airline Management Process Model Flaws:

- **610AM-PMF-1:** Airline management believed that additional briefings/ rehearsals alone could improve their pilots' ability to handle aircraft, as had been the case in the past [610AM-UCA-1]

JT610 Airline Management Contextual Factors:

- **610AM-CF-1:** Boeing's own guidance did not consider the AOA indicator mandatory, so the airline may have deferred to Boeing's judgement to save on cost [610AM-UCA-2]

Questions raised:

- What incentives existed for Lion Air to maintain the same training programs if they have seen a recurrence of the same difficulties after the treatment? Had briefings/rehearsals been shown to be the most effective treatment earlier?

A.3.2.8. Sensor Repair Contractor

Responsibilities:

- Repair aircraft sensors according to instructions provided by sensor/aircraft manufacturer
- Communicate with aircraft operators regarding changes to equipment

JT610 Sensor Repair Contractor Control Actions:

- **610SRC-UCA-1:** Sensor repair contractor provided Lion Air with a miscalibrated AOA sensor

JT610 Sensor Repair Contractor Process Model Flaws:

- **610SRC-PMF-1:** Sensor repair contractor staff believed sensor was calibrated, as the miscalibration was undetectable [610SRC-UCA-1]

JT610 Sensor Repair Contractor Contextual Factors:

- **610SRC-CF-1:** During resolver calibration, utilization of the Peak API and selection of REL/ABS switch in the REL position selection may have led to improper calibration because there were no written instructions for the correct utilization of the Peak API in accordance with the Company Maintenance Manual (CMM) requirements. With the REL/ABS switch in the REL position for the return-to-service testing, the improper calibration would not be detected [610SRC-UCA-2]

Questions raised:

- Why were there no written instructions for correct utilization of Peak API?

A.3.2.9. Aircraft Manufacturer

Responsibilities:

- Design and manufacture aircraft according to certification requirements imposed by regulatory bodies
- Communicate with aircraft operators regarding changes to aircraft or procedures
- Document, manage and act upon reports of safety-related incidents

JT610 Aircraft Manufacturer Control Actions:

- **610OEM-UCA-1:** Engineers did not appropriately validate assumptions that flight crew would respond correctly to erroneous MCAS activations
- **610OEM-UCA-2:** Engineers determined no redesign was necessary when considering the potential for repeated MCAS activations
- **610OEM-UCA-3:** Engineers determined that MCAS-related failure conditions had severity category of "Major", as opposed to hazardous or catastrophic
- **610OEM-UCA-4:** Engineers did not identify the implicit assumption that erroneous MCAS activation was equivalent to a runaway stabilizer (which turned out to be flawed, as MCAS is intermittent while stab runaway is continuous)
- **610OEM-UCA-5:** Engineers assigned MCAS failure conditions a severity of “major”
- **610OEM-UCA-6:** Engineers designed MCAS such that it only received information from one data source
- **610OEM-UCA-7:** Engineers designed AOA Disagree alert such that it only activated if aircraft was fitted with AOA display, and determined that this alert “was not necessary for the safe operation of the airplane”
- **610OEM-UCA-8:** Engineers did not directly inform certification authorities when MCAS’s range of motion was increased
- **610OEM-UCA-9:** Engineers removed mention of MCAS from the 737 MAX FCOM
- **610OEM-UCA-10:** Engineers did not identify the implicit assumption that the airspeed unreliable procedure was unaffected by the presence of MCAS (which turned out to be flawed, as repeated MCAS activations prevent the crew from stabilizing the aircraft to detect an unreliable airspeed)

JT610 Aircraft Manufacturer Process Model Flaws:

- **610OEM-PMF-1:** Engineers believed simulator test to verify that one MCAS activation was able to be countered was sufficient [610OEM-UCA-1, 3]
- **610OEM-PMF-2:** Engineers operated under the assumption that each MCAS activation would be recognized and immediately trimmed out by the flight crew [610OEM-UCA-2, 3, 10]

- **610OEM-PMF-3:** Engineers operated under the assumption that an MCAS activation would look like a stabilizer trim runaway [610OEM-UCA-4, 10]
- **610OEM-PMF-4:** Engineers believed that MCAS did not need an additional layer of redundancy in its source data as MCAS-related failure conditions had a severity category of "Major" [610OEM-UCA-6]
- **610OEM-PMF-5:** Engineers believed that probability of AOA failure was sufficiently low to meet safety requirements based on reliability data traceable to the sensor OEM [610OEM-UCA-6]
- **610OEM-PMF-6:** Engineers did not believe AOA disagree alert was necessary for safe operation of the airplane, as there were no required procedures for pilots to follow if that alert was observed [610OEM-UCA-7]
- **610OEM-PMF-7:** Engineers believed that "crews were not expected to encounter MCAS in normal operation" and that in most cases "the MCAS function is automatic and operates in the background, without any control input from the flight crew" [610OEM-UCA-9, 10]

JT610 Aircraft Manufacturer Contextual Factors:

- **610OEM-CF-1:** Specific failure modes that could lead to undesired MCAS activation were not simulated as part of the MCAS FHA [610OEM-UCA-1, 3, 10]
- **610OEM-CF-2:** FHA is a process for identifying "failure conditions" and classifying their severity that does not consider the source of the failure condition (though the source of the failure condition might affect what the flight crew experiences as the condition occurs) [610OEM-UCA-1, 3, 10]
- **610OEM-CF-3:** ARP4761 guidance assumes that flight crews, cabin crews, maintenance crews, and other individuals participating in the operation of the aircraft follow documented procedures [610OEM-UCA-1, 5, 10]
- **610OEM-CF-4:** Regulatory guidance in AC 25-7C states that a pilot will take immediate action to trim out reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions [610OEM-PMF-2, 610OEM-UCA-2, 3]
- **610OEM-CF-5:** Engineers originally assigned undesired MCAS activation a hazardous rating, but only if it occurred in the "operating flight envelope" as opposed to the "normal flight envelope", and used an exposure argument to assume they could discount 10^{-3} in "acceptable probability" because the chance of being in that envelope in the first place is very low [610OEM-UCA-3, 5]
- **610OEM-CF-6:** At a severity of “major”, the safety objective is on the order of 10^{-5} per flight hour and depending on the reliability information from the sensor manufacturer and the assumed exposure, it may be possible to meet the objective with a single sensor [610OEM-UCA-6, 7]
- **610OEM-CF-7:** ARP4761 does not provide guidance for identifying whether failures are independent from operational events/conditions [610OEM-UCA-3]
- **610OEM-CF-8:** ARP4761 does not provide guidance for identifying undocumented assumptions [610OEM-UCA-4, 10]
- **610OEM-CF-9:** Boeing has a standard set of assumptions used across all Boeing models for FHAs of flight control systems that are consistent with the requirements contained in 14 CFR 25.671 & 25.672 and FAA AC 25-7C for compliance evaluation of 14 CFR 25.143 [610OEM-UCA-1, 2, 3, 4]
- **610OEM-CF-10:** Failures with a severity class of “major” did not require a dedicated FTA, which may have generated a "no single point of failure" requirement [610OEM-UCA-6]
- **610OEM-CF-11:** ARP4761 does not provide guidance for identifying accident causes that do not stem from failures [610OEM-UCA-6]
- **610OEM-CF-12:** Only 25 activations of stick shaker due to AOA failures occurred in 737 aircraft for the past 17 years before JT610, during more than 240 million flight hours [610OEM-UCA-6, 7, 10]
- **610OEM-CF-13:** Revision documents are not required certification deliverables, especially as Boeing operated under the system of Organization Designation Authorization (ODA). [610OEM-UCA-8]
- **610OEM-CF-14:** Engineers received validation from the FAA that the decision to remove MCAS from FCOM was safe, as FAA agreed with the decision after discussion [610OEM-UCA-9]
- **610OEM-CF-15:** Airspeed unreliable procedure was appropriate for other versions of the Boeing 737 [610OEM-UCA-10]

Questions raised:

- What guidance existed in terms of simulating specific accident scenarios during the SSA, when causes of failure conditions have been identified?
- What additional human factors analysis was performed to validate FHA assumptions?
- What analysis was in place to establish the effectiveness of procedural mitigations to hazardous situations?
- What internal guidance/policy existed at Boeing for identifying unrecognized assumptions?
- What internal guidance/policy existed at Boeing for identifying causes of accidents that do not stem from failures (e.g., maintenance procedures, unsafe interactions, etc.)? How did Boeing deal with the fact that failure probabilities cannot account for external events that might damage the AOA sensor?
- What is the rationale behind the determination of what documents are certification deliverables?
- What are the procedures for determining what elements of "non-normal" operating procedure should go in the FCOM?

A.3.2.10. Regulatory Authorities

Responsibilities:

- Provide certification requirements by which aircraft manufacturers, airlines and airports need to abide in order to continue operating
- Oversee aircraft manufacturers, airlines and airports and identify safety concerns
- Assess changes made to aircraft, facilities, and procedures
- Issue directives to require aircraft manufacturers, airlines, or airports to comply with new regulations

JT610 Regulatory Authorities Control Actions:

- **610RA-UCA-1:** FAA regulators and certifiers approved Boeing's decision to remove mention of MCAS from 737 MAX FCOM
- **610RA-UCA-2:** FAA's Changed Product Rule allowed 737 MAX to be certified according to older standards than were in place when the certification effort occurred (and not obtain a new type certificate), meaning some features of the aircraft did not change since initial certification in the 1960s
- **610RA-UCA-3:** FAA regulators and certifiers did not prescribe a "special condition" for MCAS, which would have placed it under harder scrutiny for not being covered under existing regulations
- **610RA-UCA-4:** FAA regulators and certifiers delegated a significant amount of the oversight of the 737 MAX certification plans to the Boeing ODA for approval, rather than the FAA's independent analysts

JT610 Regulatory Authorities Process Model Flaws:

- **610RA-PMF-1:** FAA regulators and certifiers agreed with Boeing's belief that "Crews were not expected to encounter MCAS in normal operation." [610RA-UCA-1]
- **610RA-PMF-2:** FAA regulators and certifiers were unaware of the increased range of MCAS (up to 2.5 degrees) and the fact that MCAS could activate at slower speeds as Boeing never submitted "Revision D" for FAA approval [610RA-UCA-1]
- **610RA-PMF-3:** FAA regulators and certifiers did not have adequate information about the potential hazards stemming from loss of AOA function, as the "Single and Multiple Failure" document was not submitted to the FAA, since it was not a required certification deliverable [610RA-UCA-1]
- **610RA-PMF-4:** FAA regulators and certifiers was not aware of any changes from the 737-800 to the 737 MAX that would have required Boeing to apply for a new type certificate, so the FAA did not see the need to require special condition and certification by newer standards [610RA-UCA-2, 3]
- **610RA-PMF-5:** FAA regulators and certifiers had gained confidence in Boeing’s ability to self-analyze over time and were accustomed to delegating oversight responsibilities to ODAs [610RA-UCA-4]

JT610 Regulatory Authorities Contextual Factors:

- **610RA-CF-1:** AFM.FAR 25.1585(b) states that "Information or procedures not directly related to airworthiness or not under the control of the crew must not be included, nor must any procedure that is accepted as basic airmanship." [610RA-UCA-1]
- **610RA-CF-2:** Requiring certification to new standards would have prevented Boeing from maintaining a "common flight deck philosophy" within the 737 fleet and may have called into question the ability to have the same type rating between the 737 MAX and the 737 NG. [610RA-UCA-2]
- **610RA-CF-3:** FAA regulators and certifiers rely on Boeing engineers to identify significant changes in their aircraft, and FAA then reviews and assesses those determinations [610RA-UCA-2, 3]
- **610RA-CF-4:** Boeing engineers argued MCAS had been covered under existing regulations relating to flight control systems (25.671, 25.672, 25.1309, and 25.1329), and was included on the military Boeing 767 refueling tanker (albeit in a different form) [610RA-UCA-2, 3]
- **610RA-CF-5:** FAA's oversight of ODA program does not target oversight on particular systems based on risk [610RA-UCA-4]
- **610RA-CF-6:** ODAs are unable to maintain independence from development and oversight responsibilities (same engineer worked on a design and approved it as an ODA) [610RA-UCA-4]

Questions raised:
- What oversight existed over Boeing's classification of the changes between the 737NG and 737 MAX?
- What oversight existed over Boeing's decision to equate MCAS on the 737 MAX with 767 if they contained key design differences?
- How does the FAA manage conflicts of interest when the ODA is also assigned additional responsibilities at the manufacturer?

A.3.3. Role of each Controller in the Loss of ET302

A.3.3.1. On-board computers (FCC, FMC, SMYDC, etc. but not including MCAS)

ET302 Computer Control Actions:
- **302Comp-UCA-1:** On-board computers provided inappropriate feedback to flight crew regarding their aircraft state (left stick shaker activated when the aircraft was not approaching a stall condition, displayed altitude and airspeed values became lower than the actual altitude and airspeed)
- **302Comp-UCA-2:** Autopilot commanded a pitch down as soon as it engaged
- **302Comp-UCA-3:** Autopilot disconnected after 32 seconds
- **302Comp-UCA-4:** Auto-throttle (A/T) remained in ARM mode and maintained takeoff thrust throughout entire flight, rather than transitioning to climb thrust

ET302 Computer Process Model Flaws:
- **302Comp-PMF-1:** SMYDC calculated the aircraft was approaching a stall condition due to receiving erroneous AOA values from ADIRS [302Comp-UCA-1]
- **302Comp-PMF-2:** Autopilot calculated aircraft was below the minimum operational speed when it was not, as SMYDC computed an erroneous minimum operational speed due to receiving erroneous AOA values from ADIRS [610Comp-UCA-2]
- **302Comp-PMF-3:** Erroneous left-hand (LH) baro-corrected altitude was used to switch A/T from THR HOLD to ARM mode, which happened 16 seconds too late [610Comp-UCA-4]
- **302Comp-PMF-4:** N1 target of 89%, as would be appropriate for climb, was deemed invalid due to discrepancies in left and right-hand true airspeed [610Comp-UCA-4]

ET302 Computer Contextual Factors:
- **302Comp-CF-1:** The left AOA sensor was most likely separated from the aircraft by a bird strike. The left AOA sensor was used to inform the SMYDC and EGPWS [610Comp-PMF-1, 2, 3; 610Comp-UCA-1, 2, 3, 4]

- **302Comp-CF-2:** Autopilot A uses information from left ADIRS, which was transmitting erroneous AOA values [610Comp-UCA-2, -3]
- **302Comp-CF-3:** Autopilot attempted to meet two objectives that required conflicting control actions (pitch down to increase speed and reach minimum operational speed, and pitch up to climb and capture selected altitude), neither objective was met, and the autopilot disengaged after not being able to climb at the necessary rate [610Comp-UCA-3]

Questions raised:
- Why was the erroneous AOA value not able to be detected and disregarded by the SMYDC and autopilot? Would it have been possible to detect that the calculated minimum operational airspeed was higher than the maximum operational airspeed? Is there any real situation where this might happen?
- Would it have been possible to detect the fluctuations in AOA and disregard it based on a physical impossibility?
- How does the autopilot system prioritize which objectives to meet?
- What kind of warning did the flight crew receive about the invalidity of the A/T commands?

A.3.3.2. MCAS

ET302 MCAS Control Actions:
- **302MCAS-UCA-1:** MCAS repeatedly activated and commanded nose-down trim when aircraft was not at a high angle of attack
- **302MCAS-UCA-2:** MCAS inhibited flight crew's ability to override electric trim commands using the control column

ET302 MCAS Process Model Flaws:
- **302MCAS-PMF-1:** MCAS determined aircraft was beyond the AOA threshold for activation due to receiving erroneous AOA values from air data inertial reference system (ADIRS) [302MCAS-UCA-1]

ET302 MCAS Contextual Factors:
- **302MCAS-CF-1:** MCAS belongs to the FCC, each of which only pulls information from its associated ADIRS [302MCAS-UCA-1]
- **302MCAS-CF-2:** The left AOA sensor was most likely separated from the aircraft by a bird strike [302MCAS-UCA-1]
- **610MCAS-CF-3:** MCAS intentionally inhibits control column cutout because the original situation in which MCAS was designed to act would require it to act in opposition to pilots' control column inputs [302MCAS-UCA-2]

Questions raised:
- What is the rationale behind the 5 second time limit for MCAS re-activation? Would it have been possible/feasible to inhibit MCAS re-activation if pilots manually re-trimmed following an earlier MCAS activation?

A.3.3.3. ET302 Flight Crew

ET302 Flight Crew Unsafe Control Actions:
- **302FC-UCA-1:** Flight crew did not execute unreliable airspeed memory items and non-normal checklist from quick reference handbook (QRH)
- **302FC-UCA-2:** Captain engaged autopilot A, which was being fed erroneous AOA data
- **302FC-UCA-3:** Flight crew retracted flaps, allowing MCAS to begin activating
- **302FC-UCA-4:** Flight crew only trimmed nose up for 2 seconds (stabilizer moved from 2.1 to 2.3 units) after first MCAS activation

- **302FC-UCA-5:**Flight crew moved stab trim cutout switches to CUTOUT position without first re-trimming the aircraft using manual electric trim
- **302FC-UCA-6:** Flight crew did not monitor airspeed before reaching overspeed condition
- **302FC-UCA-7:** Flight crew was unable to manually re-trim aircraft
- **302FC-UCA-8:** Flight crew returned the stab trim cutout switches to the normal position

ET302 Flight Crew Process Model Flaws:

- **302FC-PMF-1:** Flight crew may have been unaware of IAS Disagree warning (only visual feedback, not aural), as they did not acknowledge it [302FC-UCA-1]
- **302FC-PMF-2:** Flight crew may have believed they were actually stalling, due to stick shaker activation [302FC-UCA-1]
- **302FC-PMF-3:** Flight crew may have not been aware of the erroneous AOA data [302FC-UCA-1, 2]
- **302FC-PMF-4:** If flight crew were aware of AOA issue, they may have believed engaging autopilot would fix the issue due to an interpretation of the wording on the Flight Crew Operating Manual (FCOM) bulletin following JT610 [302FC-UCA-1, 2]
- **302FC-PMF-5:** Flight crew may have been unaware that retracting flaps would have satisfied the conditions for MCAS to activate [302FC-UCA-3]
- **302FC-PMF-6:** Flight crew may have believed they were capable of re-trimming the aircraft manually after moving switches to CUTOUT position, as there is no mention in the FCOM bulletin of the potential for excessive airloads on the stabilizer that prevent manual trim [302FC-UCA-5]
- **302FC-PMF-7:** Flight crew may not have been aware that the aircraft was approaching an overspeed condition, as they had a stick shaker going off the entire flight [302FC-UCA-6]
- **302FC-PMF-8:** Flight crew may have considered that aerodynamically unloading the horizontal stabilizer through the "roller coaster" approach might have placed the aircraft too close to the ground [302FC-UCA-7]
- **302FC-PMF-9:** Flight crew may have believed electric trim was the only way to retrim the aircraft as they were unable to manually trim it [302FC-UCA-8]

ET302 Flight Crew Contextual Factors:

- **302FC-CF-1:** High density altitude at airfield [302FC-PMF-2]
- **302FC-CF-2:** Unreliable airspeed memory items required reducing N1 to 80%, and aircraft was still at low radio altitude (around 50ft) [302FC-UCA-1]
- **302FC-CF-3:** IAS Disagree warning takes 5 seconds to activate, so master caution would have activated before that and drawn crew's attention [302FC-PMF-1, 302FC-UCA-1]
- **302FC-CF-4:** It is difficult to detect that only one stick shaker activated (which could have informed the pilots that it wasn't a real stall, but an AOA issue) [302FC-UCA-1, 302FC-PMF-2]
- **302FC-CF-5:** The difference in IAS from one display to another was just around 20 kts, which is the limit for determining whether to perform the unreliable airspeed NNC [302FC-UCA-1]
- **302FC-CF-6:** Besides stick shaker, first indication of AOA fault was "MASTER CAUTION" and "ANTI-ICE" lights illuminating, which has no memory items and QRH has only one instruction: "Avoid icing conditions" [302FC-UCA-1, 2]
- **302FC-CF-7:** Training to rely on automation. 737 Flight Crew Training Manual (FCTM) states "It is mandatory that the Pilot Flying (PF) fly the airplane while the Pilot Monitoring (PM) accomplishes the NNC. Maximum use of the autoflight system is recommended to reduce crew workload." [302FC-UCA-2]
- **302FC-CF-8:** Wording of the FCOM bulletin: "Boeing would like to call attention to an AOA failure condition that can occur during manual flight only" [302FC-UCA-2, 302FC-PMF-4]
- **302FC-CF-9:** Company policy called for engaging autopilot at 500ft above ground level [302FC-UCA-1]
- **302FC-CF-10:** Wording of the FCOM bulletin and FAA airworthiness directive did not mention "flaps up" as a condition for MCAS activation [302FC-UCA-3, 302FC-PMF-5]
- **302FC-CF-11:** Standard procedure for takeoff would have been to retract flaps at this stage [302FC-UCA-3]
- **302FC-CF-12:** Electric trim inputs required to re-trim after MCAS activations were significantly longer than trim inputs pilots are accustomed to making [302FC-UCA-4]
- **302FC-CF-13:** Aircraft is typically quite sensitive to trim inputs, so pilots are trained to trim in small bursts as opposed to sustained segments of time [302FC-UCA-4]

- **302FC-CF-14:** Guidance from FCOM bulletin for dealing with "uncommanded nose down stabilizer trim" was to "do the Runaway Stabilizer NNC ensuring that STAB TRIM CUTOUT switches are set to CUTOUT". Use of manual electric trim is only mentioned in a note after the primary instructions. [302FC-UCA-5]
- **302FC-CF-15:** Crew was communicating with ATC in the direct moments before overspeed warning sounded [302FC-UCA-6]
- **302FC-CF-15:** The only indication of the aircraft not having transitioned to climb thrust was the A/T indication of ARM instead of N1 [302FC-UCA-6]
- **302FC-CF-16:** Airspeed was at approximately 360-375kts, meaning the aerodynamic forces on the stabilizer were too large for one person to be able to move trim wheel [302FC-UCA-7]
- **302FC-CF-17:** Flight crew needed to continuously pull back on the control column to prevent the aircraft from diving due to the mistrim. Releasing the control column to attempt to trim led to a pitch down, which further increased airspeed and made trim more difficult. [302FC-UCA-7]
- **302FC-CF-18:** 40 turns of the trim wheel were required to fully retrim the aircraft [302FC-UCA-7]
- **302FC-CF-19:** FCOM bulletin has no guidance for re-trimming the aircraft if manual trim is not available and states "manual trim can be used before or after the STAB TRIM CUTOUT switches are moved to CUTOUT." [302FC-UCA-8]

Questions raised:

- How had the crew been trained to diagnose an airspeed unreliable situation? How was the prioritization scheme for dealing with the alerts in the cockpit (i.e. were they supposed to deal with stick shaker first, then IAS disagree?)?
- Why did the FCOM bulletin and airworthiness directives not mention the flaps as a condition for MCAS activation?
- How had the crew been trained to deal with mistrim? How often is this scenario trained?
- Were the crew aware of the need to electrically trim before moving stab trim cutout switches? What kind of training had they received following the JT610 accident?
- Why was there no mention in the FCOM of the potential for excessive airloads to prevent manual trim? Was it determined that, if it was noted in the FCTM, that was sufficient?
- Why was there no more explicit indication to the flight crew that the A/T was no longer controlling engine thrust?
- How often was the flight crew trained to aerodynamically reduce loads before retrimming?
- Did Boeing or the FAA foresee the overspeed condition preventing manual retrim? Why was this not included in the bulletin/directive?

A.3.3.5. Addis Ababa Airport Management

Responsibilities:

- Follow documented procedures for operating and maintaining airport facilities
- Receive directives from regulatory bodies on changes needed to facilities
- Communicate with maintenance team and order actions
- Document, manage and act upon reports of safety-related incidents

ET302 Airport Management Control Actions:

- **302ADD-UCA-1:** Did not sufficiently control bird strike risk at Bole International Airport in Addis Ababa (ADD)

ET302 Airport Management Process Model Flaws:

- **302ADD-PMF-1:** Airport management may have been unaware of the actual risk posed by bird strikes at ADD, as only one major incident had been reported there (Boeing 767-300, registration ET-AMG on November 26, 2018) and the main report outlining that came out in November 2019, after the ET302 accident [302ADD-UCA-1]

ET302 Airport Management Contextual Factors:

- **302ADD-CF-1:** Last in-depth study into bird strike incidence at Addis Ababa was from the year 2000 (later one in 2020) [302ADD-UCA-1]
- **302ADD-CF-2:** Measures to address bird presence at the airport typically involve imposing restrictions outside airport bounds (garbage disposal systems, open slaughterhouses, etc.), which the airport may not have the authority to do [302ADD-UCA-1]
- **302ADD-CF-3:** Airport had met all regulatory requirements from aviation authorities for bird strike risk assessment and bird control measures, as per Ethiopian Civil Aviation Authority (ECAA) proclamation 616/2009 [302ADD-UCA-1]

Questions raised:

- How were the regulatory requirements around bird control implemented and verified at ADD? What criteria was used to determine compliance and how often was compliance re-evaluated?

A.3.3.6. Ethiopian Airlines Management

ET302 Airline Management Control Actions:

- **302AM-UCA-1:** Airline management only provided a roughly 6 hour non-simulator Logipad training on the differences between 737 MAX and 737 NG following JT610
- **302AM-UCA-2:** Airline management did not verify pilots' understanding of or ability to diagnose and follow FAA AD #: 2018-23-51 and Boeing FCOM bulletin ETH-12
- **302AM-UCA-3:** Potential inadequate safety culture with respect to reporting unsafe occurrences (reported interrogations and intimidation of employees who refused to perform or reported unsafe occurrences)

ET302 Airline Management Process Model Flaws:

- **302AM-PMF-1:** Airline management believed Logipad training was sufficient, as it was the only training required by the aircraft manufacturer and approved by regulators following JT610 [302AM-UCA-1]
- **302AM-PMF-2:** Airline management may have believed the training provided by the manufacturer was sufficient, as it was the only training required by the aircraft manufacturer and approved by regulators following JT610, and did not call for further examinations [302AM-UCA-2]
- **302AM-PMF-3:** Airline management believed simulators were not designed to replicate the erroneous behavior observed in JT610 (and later ET302) [302AM-UCA-2]

ET302 Airline Management Contextual Factors:

- **302AM-CF-1:** The existence/functionality of MCAS was not disclosed in any of the manuals provided by the aircraft manufacturer to the airline management [302AM-UCA-1]
- **302AM-CF-2:** Further examination of flight crew understanding of the directives may have generated delays if crews were unable to demonstrate an ability to diagnose the problem and follow the directives [302AM-UCA-2]
- **302ADD-CF-3:** Economic pressures and close relationship with regulatory authorities due to high market share likely influenced safety culture at airline, as Ethiopian Airlines is owned by the Ethiopian government, who also controls the country's regulatory authorities [302AM-UCA-3]

Questions raised:

- What methods did the airline have to question the necessary training following JT610?
- What were pilots' initial reactions to the information in the directives? Was it well-understood or were there reports of significant misunderstandings/ need for clarifications?
- What kind of international regulatory oversight exists around airline safety culture, and around the relationship between airlines and local regulatory authorities?

A.3.3.7. Aircraft Manufacturer (beyond those contributions noted for JT610)

ET302 Aircraft Manufacturer Control Actions:

- **302OEM-UCA-1:** Boeing engineers provided to airlines only a roughly 6-hour non-simulator Logipad training on the differences between 737 MAX and 737 NG following JT610
- **302OEM-UCA-2:** FCOM bulletin provided by Boeing engineers used the following language: "Boeing would like to call attention to an AOA failure condition that can occur during manual flight only." This implies that the AOA malfunction could only occur during manual flight, when in reality it was MCAS activation that could only occur in manual flight
- **302OEM-UCA-3:** FCOM bulletin provided by aircraft manufacturer did not mention the possibility that crews are unable to manually trim the aircraft after moving the stab trim cutout switches to CUTOUT (or that it may require a two-pilot effort, or require elevator load alleviation)
- **302OEM-UCA-4:** Boeing engineers did not respond to a question from the airline regarding how pilots are expected to correct their aircraft's trim while also diagnosing and applying the Airspeed Unreliable checklist

ET302 Aircraft Manufacturer Process Model Flaws:

- **302OEM-PMF-1:** Boeing engineers were operating under the same assumptions with which they had designed MCAS, that pilots would follow posted instructions in an emergency and that if pilots performed the Runaway Stabilizer NNC they would re-trim electrically and not ever require manual trim [302OEM-UCA-1, 3]
- **302OEM-PMF-2:** Boeing engineers may have intended for their FCOM statement to be interpreted as "an aircraft failure condition that can occur during manual flight only, stemming from an AOA failure" [302OEM-UCA-2]
- **302OEM-PMF-3:** Airline management believed simulators were not designed to replicate the erroneous behavior observed in JT610 (and later ET302) [302AM-UCA-2]

ET302 Aircraft Manufacturer Contextual Factors:

- **302OEM-CF-1:** Additional training requirements would have required acknowledging and explaining the MCAS feature to all 737 MAX crews, which would have led to further delays for operators [302OEM-UCA-1]
- **302OEM-CF-2:** Many airlines did not possess 737 MAX simulators in which to perform additional training, and the logistics of processing crews at Boeing's Renton center would have added delays and also costs. [302OEM-UCA-1]
- **302OEM-CF-3:** JT610 investigation was still ongoing as the training was released [302OEM-UCA-1]
- **302OEM-CF-4:** As of when the FCOM bulletin was released, the manufacturer had not informed 737 MAX operators of the existence of MCAS [302OEM-UCA-2]
- **302OEM-CF-5:** Information about being unable to manually retrim was already noted in the FCTM, as such: "Excessive airloads on the stabilizer may require effort by both pilots to correct the mis-trim. In extreme cases it may be necessary to aerodynamically relieve the airloads to allow manual trimming. Accelerate or decelerate towards the in-trim speed while attempting to trim manually." However, there is no clarification on what it means to aerodynamically relieve airloads beyond accelerating or decelerating [302OEM-UCA-3]
- **302OEM-CF-6:** Boeing was providing Annex 13 technical support to the on-going Lion Air accident investigation, and deemed Ethiopian Airlines' question too closely related to this event to answer it [302OEM-UCA-4]

Questions raised:

- Did Boeing reevaluate its initial assumptions about pilots' reactions to MCAS activation, and their ability to follow procedure?
- What response did Boeing receive from airlines and pilots regarding the training that was provided? Was there significant misunderstanding and were there many clarification questions submitted?
- How was the language in the FCOM bulletin drafted and evaluated? What incentives did Boeing have to not mention MCAS directly?
- What evaluation went into the decision not to answer the question from the airline? How was it determined that this question related too closely to the accident scenario?

A.3.3.8. Regulatory Authorities (beyond those contributions noted for JT610)

ET302 Regulatory Authorities Control Actions:

- **302RA-UCA-1:** Airworthiness directive provided by FAA did not mention the possibility that crews are unable to manually trim the aircraft after moving the stab trim cutout switches to CUTOUT (or that it may require a two pilot effort, or require elevator load alleviation)

ET302 Regulatory Authorities Process Model Flaws:

- **302RA-PMF-1:** FAA engineers were operating under the same assumptions with which they had certified MCAS, that pilots would follow posted instructions in an emergency and that if pilots performed the Runaway Stabilizer NNC they would re-trim electrically and not ever require manual trim [302RA-UCA-1]

ET302 Aircraft Manufacturer Contextual Factors:

- **302RA-CF-1:** Information about being unable to manually retrim was already noted in the FCTM [302RA-UCA-1]

Questions raised:

- How was the language in the airworthiness directive drafted and evaluated? What incentives did the FAA have to not mention the flaps directly?

A.4. Control Structure Flaws

Besides the individual control actions executed or not executed by each component, CAST provides a framework for examining the systemic factors which affect the entire control structure and contribute to the loss. The main factors being considered in this analysis are changes to the system over time and external economic factors.

A.4.1. Changes to System and Environment over Time

As is the case with most accidents, the losses of JT610 and ET302 came after a major change. The aircraft design was updated with new features, while the flight crew procedures to deal with the consequences of the design change were left the same. Management of the design change was a responsibility not just of the aircraft manufacturer, but also of the regulatory authorities that approved of the change. There was an incentive on Boeing's part to make the changes to the 737 MAX's flying appear as small as possible, so that pilots of earlier 737 models could more easily transition to the MAX without needing expensive training. Furthermore, the ability to consider the changes in the 737 MAX as not "novel or unusual" such that the aircraft did not require a new type certificate may have reduced the level of scrutiny towards the design changes.

The inadequate management of the change can also be understood by examining the methods used to evaluate the effects of this change. Without appropriate guidance for validating human factors assumptions in safety assessment, identifying undocumented assumptions, and identifying safety-critical scenarios that do not stem from component failures, it becomes a challenging to properly assess the implications of the design change. The close relationship between the regulator and aircraft manufacturer and their use of the same general methodologies for safety assessment defeated some of the independence in the certification process and likely contributed to the inadequate management of the design change.

A.4.2. Economic Factors

Many of the decisions made by the 737 MAX's designers, regulators, and operators were driven by cost and schedule pressures that ended up negatively affecting safety and quality. Airbus' announcement of the A320neo in 2010 placed significant pressure on Boeing to respond quickly with a new aircraft of their own, and the decision was made to upgrade the existing 737 as opposed to designing a completely new aircraft as it would save both time and financial resources. Reusing tried and tested designs does, in theory, make both the design and certification efforts shorter. However, the introduction of new design features breaks the assumption that the tried and tested design is truly safe, which in reality resulted in significantly higher costs for Boeing (and the aviation industry as a whole) after the accidents occurred.

A.5. Summary of Contribution of each Controller and Recommendations

The table below provides a summary of the contributions of each controller to the losses, as well as the associated recommendations that came from the CAST results. For a full description of the process model flaws and contextual factors that explain these contributions, see the results in sections A.3 and A.4.

Controller	Contributions to Losses	Recommendations
Physical Components	Left AOA sensor provided misleading data to ADIRU on both flights. AOA sensor on JT610 had a 21^{o} bias introduced during calibration, and AOA sensor on ET302 was most likely separated from the aircraft by a bird strike.	• Reassess calibration procedures to improve detection of bias • Redesign algorithm that determines validity of AOA data to consider cases where data is within valid range but not consistent with physical environment
On-board computers (FCC, FMC, SMYDC, etc. but not including MCAS)	On both flights, computers provided inappropriate feedback to flight crews regarding aircraft state (left stick shaker activated when the aircraft was not approaching a stall condition, displayed altitude and airspeed values became lower than the actual altitude and airspeed). On ET302, autothrottle remained in ARM mode and did not reduce thrust from takeoff setting to climb setting.	• Reassess algorithm that activates stall warning systems to consider cases where AOA data from both sensors diverges • Reassess saliency of the feedback to the flight crew about autothrottle state
MCAS	On both flights, MCAS repeatedly activated and commanded nose-down trim when aircraft was not at a high angle of attack, because it was being fed inaccurate AOA data. MCAS also inhibited flight crew's ability to override electric trim commands using the control column.	• Redesign algorithm that activates MCAS to consider cases where AOA data from both sensors diverges • Redesign pilot interface such that MCAS can be deactivated without removing access to manual electric trim

		• Reassess the need for MCAS to inhibit control column cutout
Flight Crew	On both flights, crew did not complete unreliable airspeed procedure and diagnose that AOA sensor was providing inaccurate data. Flight crew also did not complete stabilizer trim runaway procedure as they did not diagnose the intermittent stabilizer movement caused by MCAS as a stabilizer runaway. Crew of JT610 did not ever engage stabilizer trim cutout switch, while crew of ET302 engaged it but returned it to the normal position when they were unable to manually retrim the aircraft. Both crews did not sufficiently counter MCAS' stabilizer trim commands, as MCAS was not a part of their mental model of the aircraft's automation.	• Conduct studies to reevaluate saliency of IAS Disagree warning • Conduct studies to determine the feasibility of informing flight crews if the stick shaker is activating on just one or both sides • Reassess optionality of AOA display • Inform flight crews of the existence and behavior of MCAS • Redesign stabilizer runaway procedures to include intermittent stabilizer movement, or create a new procedure for addressing MCAS activations • Improve flight crew awareness of procedures for aerodynamically relieving stabilizer loads if manual trim is unavailable • Reevaluate airspeed unreliable checklist to ensure it can be performed even if aircraft cannot be stabilized
Air Traffic Control (ATC)	ATC did not acknowledge JT610 crew's request to go to a holding point and gave the crew several new instructions as they dealt with flight control problems, because ATC was not aware of the nature of the emergency.	• Reassess ATC policies surrounding declaration of emergency on behalf of a flight crew
Maintenance Engineers	A maintenance engineer installed an AOA sensor with a bias when replacing the left AOA sensor on the aircraft that would operate JT610. A maintenance engineer used an alternate installation test rather than the standard installation test for the AOA sensor, and a different engineer released the aircraft without rectifying the problem.	• Improve AOA sensor installation tests to ensure they appropriately indicate sensor bias • Identify reasons for usage of alternate installation tests and install controls to ensure appropriate tests are utilized

Maintenance Control Center	Defined a “repetitive problem” differently than their mother airline, so did not report AOA sensor problems observed on prior flights.	• Establish consistency of definitions between airline and subsidiaries
Airline Management	Both Lion Air and Ethiopian Airlines elected not to enable AOA indicator on flight displays, as the indicator was optional. After JT610, Ethiopian Airlines management only provided a roughly 6 hour non-simulator Logipad training on the differences between 737 MAX and 737 NG, as that was all that was provided by Boeing. Ethiopian Airlines management also did not verify pilots' understanding of or ability to diagnose and follow the airworthiness directive on MCAS released after JT610.	• Reassess airline policies around decision-making for optional aircraft systems • Provide appropriate (non-punitive) pathways for flight crews to report doubts or misunderstandings surrounding new or updated aircraft procedures
Airport Management	Addis Ababa airport management did not sufficiently control bird strike risk at airfield.	• Conduct studies to reevaluate bird strike risk at Addis Ababa and enforce stronger controls if possible
Aircraft Manufacturer	Boeing engineers did not appropriately validate assumptions that flight crew would respond correctly to erroneous MCAS activations and did not identify the implicit assumption that erroneous MCAS activation was equivalent to a runaway stabilizer (which turned out to be flawed, as MCAS is intermittent while stab runaway is continuous). This allowed them to remove mention of MCAS from the flight crew operations manual (FCOM). They also determined no redesign was necessary when considering the potential for repeated activations and determined that MCAS-related failure conditions had severity category of "Major", as opposed to hazardous or	• Reevaluate methods used to determine the appropriate simulator tests needed to validate human response assumptions • Consider implementing a scenario-based approach to identifying cases that might invalidate human response assumptions • Reevaluate methods used to identify and document implicit assumptions • Reevaluate methods used to identify potential causes of aircraft-level hazards to include non-failure scenarios like design error and maintenance error • Reevaluate reliance on probabilistic methods of safety assessment when designing

	catastrophic. This severity classification meant that MCAS was designed such that it only received information from one data source.	systems that involve interactions between software and humans • Reevaluate methods used to identify independence relationships between failures and operational events • Reevaluate decision-making process for inclusion or exclusion of information from FCOM
Regulatory Authorities	The FAA's Changed Product Rule allowed 737 MAX to be certified according to older standards than were in place when the certification effort occurred (and not obtain a new type certificate), meaning some features of the aircraft did not change since initial certification in the 1960s. FAA regulators and certifiers approved Boeing's decision to remove mention of MCAS from 737 MAX FCOM, and delegated a significant amount of the oversight of the 737 MAX certification plans to the Boeing ODA for approval, rather than the FAA's independent analysts.	• Reevaluate methods used to assess and certify the human factors analysis conducted by aircraft manufacturers • Reevaluate reliance on probabilistic safety requirements to certify commercial aircraft that involve complex human-software interactions • Reevaluate policies surrounding modified aircraft and reutilization of existing type certificates • Reevaluate the role of ODAs in the safety assessment process and introduce stronger controls to avoid conflicts of interest

Appendix B – MCAS STPA

B.1. Purpose of the Analysis – System Boundary, Losses, Hazards, and Safety Constraints

The first step of STPA involves defining the purpose of the analysis, which includes setting the boundary of the system being analyzed. STPA can be performed at multiple stages of development and at multiple levels of abstraction, including above the "aircraft level" outlined in ARP4761. Though this case example focuses on MCAS and conducts STPA at a similar level of abstraction to the SFHA, the "system" that is used to define the system-level losses and hazards is still the entire 737 MAX aircraft. Also included within the boundary of the system are the aircraft's operators, the flight crew.

The system-level losses of importance to the Boeing 737 MAX stakeholders include loss of life, loss of property, loss of mission, and loss of stakeholder satisfaction. Specifically, they are:

- **L-1.** Loss of life or injury to aircraft occupants
- **L-2.** Destruction or damage to aircraft structure
- **L-3.** Inability of aircraft to reach its programmed/desired destination
- **L-4.** Loss of passenger or operator confidence in safety/efficacy of aircraft

The losses that this case study will primarily focus on are L-1 and L-2. The hazards associated with them can include:

- **H-1.** Aircraft does not maintain adequate separation from outside objects [L-1, L-2]
- **H-2.** Aircraft loses ability to remain airborne [L-1, L-2]
    - **H-2-1.** Aircraft cannot generate sufficient lift to remain airborne [L-1, L-2]
    - **H-2-2.** Aircraft has excessively high rate of descent [L-1, L-2]
- **H-3.** Aircraft is unable to be controlled [L-1, L-2]
    - **H-3-1.** Aircraft is out of trim in pitch direction [L-1, L-2]
    - **H-3-2.** Aircraft is longitudinally unstable [L-1, L-2]
- **H-4.** Aircraft moves outside approved/programmed flight zone [L-1, L-2, L-3]
- **H-5.** Aircraft creates a hostile environment to its occupants [L-1, L-4]

The safety constraints associated with these hazards are:

- **R-1.** Aircraft must maintain adequate separation from outside objects [H-1]
- **R-2.** Aircraft must preserve its ability to remain airborne [H-2]
    - **R-2-1.** Aircraft must maintain an attitude/orientation where it is able to generate lift [H-2-1]
    - **R-2-2.** Aircraft rate of descent must not exceed <TBD> [H-2-2]
- **R-3.** Aircraft must be able to be controlled [H-3]
    - **R-3-1.** Aircraft must remain in trim in pitch direction throughout flight [H-3-1]
    - **R-3-2.** Aircraft must remain longitudinally stable throughout flight [H-3-2]
- **R-4.** Aircraft must remain within approved/programmed flight zone [H-4]
- **R-5.** Aircraft must not create a hostile environment to its occupants [H-5]

This study will focus on two of the hazards outlined above: H-2 and H-3. The focus of the STPA will be to determine potential scenarios in which the aircraft could: a) lose the ability to remain airborne; or b) lose controllability or pitch stability.

B.2. Control Structures

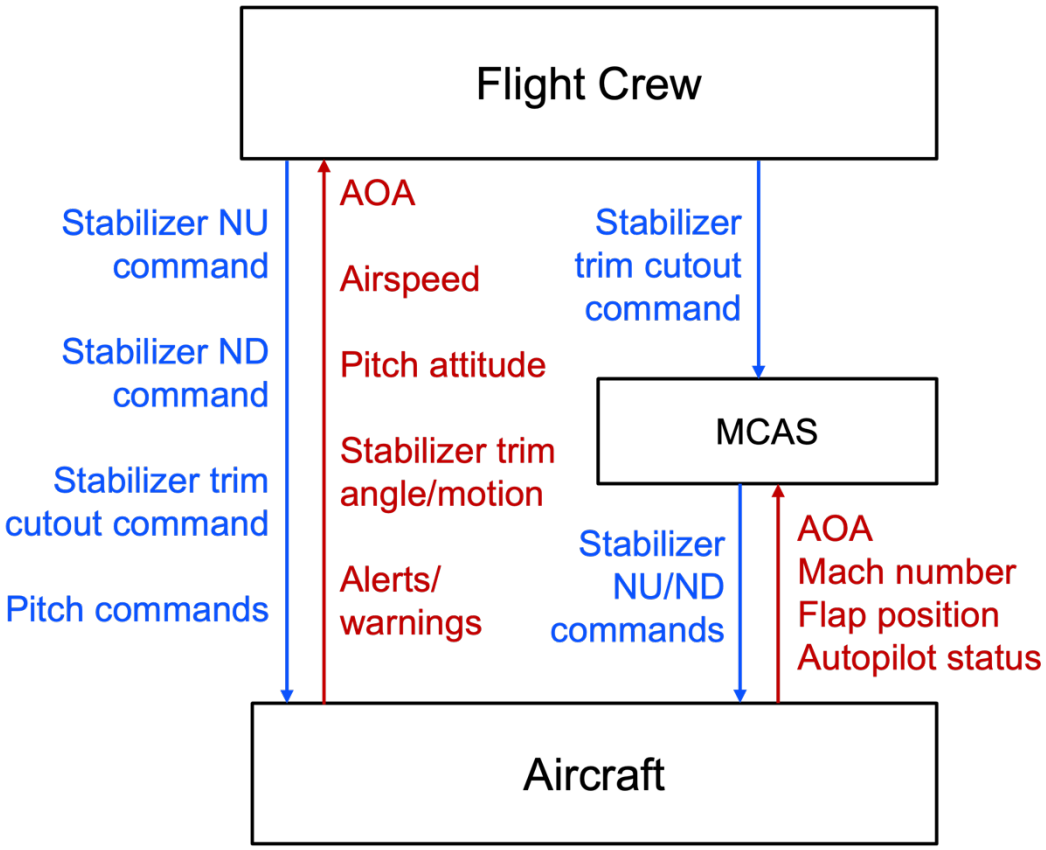


Figure B.1. High level MCAS control structure

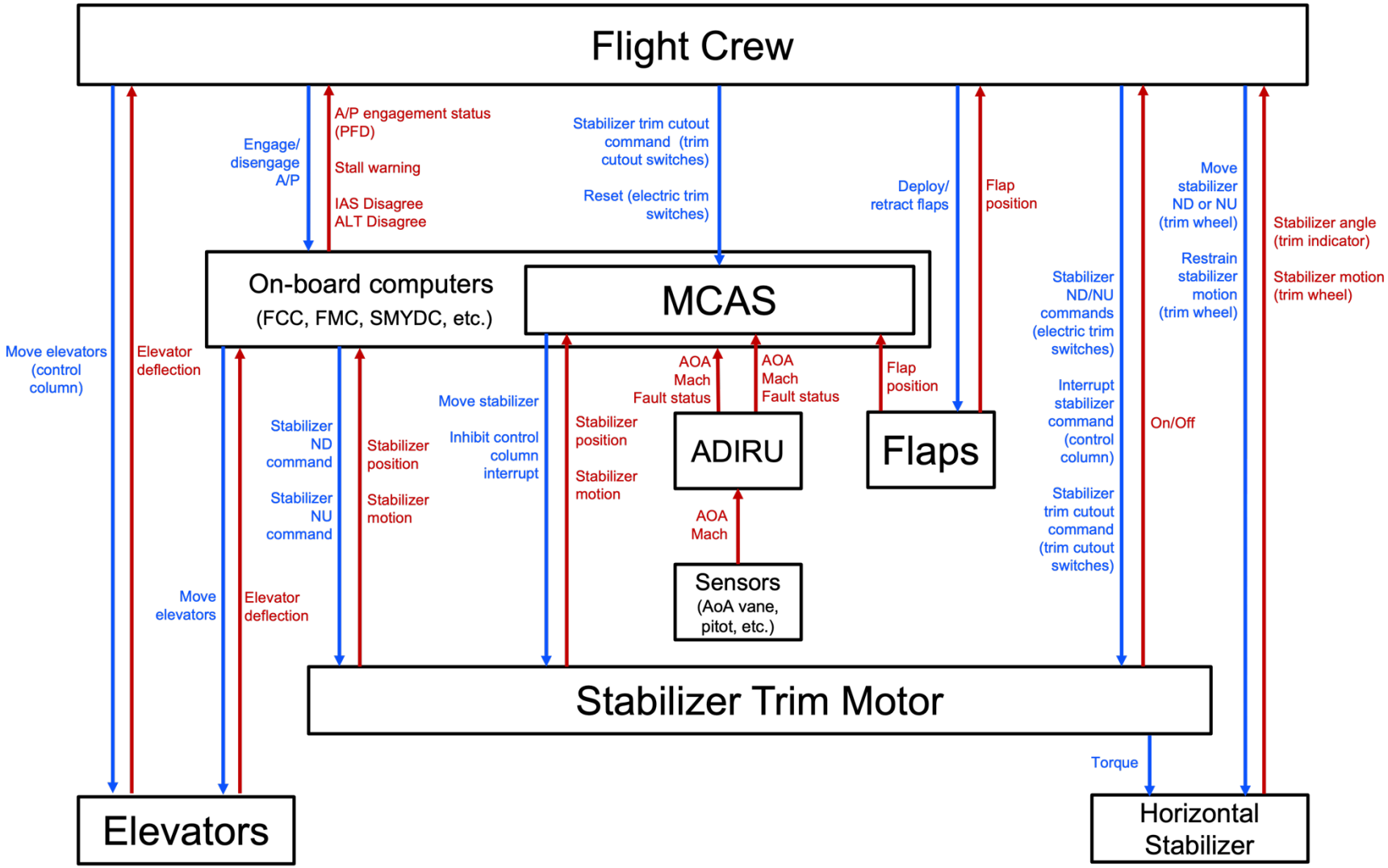


Figure B.2 Detailed MCAS control structure

B.3. Unsafe Control Actions

B.3.1. MCAS UCAs

Table II. Unsafe Control Actions for MCAS

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Move stabilizer ND	**MCAS-UCA-1:** MCAS does not provide stabilizer ND command when AOA threshold is exceeded during flaps up, high angle of attack maneuver [H-2]	**MCAS-UCA-2:** MCAS provides stabilizer ND command when aircraft is not in flaps up, high angle of attack maneuver [H-2, H-3] **MCAS-UCA-3:** MCAS provides stabilizer ND command when aircraft is out of trim in ND direction [H-2, H-3] **MCAS-UCA-4:** MCAS provides stabilizer ND command resulting in stabilizer movement of more than the maximum of 2.5^{o} [H-2, H-3] **MCAS-UCA-5:** MCAS provides stabilizer ND command when stabilizer trim is affecting aircraft pitch [H-2, H-3]	**MCAS-UCA-6:** MCAS provides stabilizer ND command too late after aircraft enters flaps up, high angle of attack maneuver [H-2]	**MCAS-UCA-7:** MCAS provides stabilizer ND command for too long compared to the AOA value's exceedance of the threshold at the current Mach number [H-2, H-3]

Move stabilizer NU	**MCAS-UCA-8:** MCAS does not provide stabilizer NU command when AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]	**MCAS-UCA-9:** MCAS provides stabilizer NU command when aircraft is in flaps up, high angle of attack maneuver and MCAS has not moved stabilizer ND prior [H-2, H-3]	**MCAS-UCA-10:** MCAS provides stabilizer NU command too late after AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]	**MCAS-UCA-11:** MCAS provides stabilizer ND command for too long compared to MCAS' previous stabilizer ND command [H-2, H-3] **MCAS-UCA-12:** MCAS stops providing stabilizer NU command too soon before matching duration of MCAS' previous stabilizer ND command [H-2, H-3]

B.3.1. Flight Crew UCAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Move stabilizer NU	**FC-UCA-1:** Flight crew does not provide stabilizer NU command when unintended ND stabilizer motion by MCAS occurs [H-2, H-3]	**FC-UCA-2:** Flight crew provides stabilizer NU command when intended ND stabilizer motion by MCAS occurs during flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-3:** Flight crew provides stabilizer NU command too late (>4 seconds) after unintended ND stabilizer motion by MCAS occurs [H-2, H-3]	**FC-UCA-4:** Flight crew stops providing stabilizer NU command too early before aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3] **FC-UCA-5:** Flight crew provides stabilizer NU command for too long after aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3]

Stabilizer trim cut out command	**FC-UCA-6:** Flight crew does not provide stabilizer trim cut out command when MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-7:** Flight crew provides stabilizer trim cut out command during flaps up, high angle of attack maneuver [H-2, H-3] **FC-UCA-8:** Flight crew provides stabilizer trim cut out command when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	**FC-UCA-9:** Flight crew provides stabilizer trim cut out command too late (>4 seconds) after MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	N/A
Move stabilizer trim cut out switches to normal	**FC-UCA-10:** Flight crew does not move stabilizer trim cut out switches to normal when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	**FC-UCA-11:** Flight crew moves stabilizer trim cutout switches to normal when MCAS is providing trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]	**FC-UCA-12:** Flight crew moves stabilizer trim cut out switches to normal too late after aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]	N/A

B.4. Scenarios

B.4.1. MCAS Scenarios

MCAS-UCA-1: MCAS does not provide stabilizer ND command when AOA threshold is exceeded during flaps up, high angle of attack maneuver [H-2]
MCAS-Scen-1.1: MCAS does not provide stabilizer ND command due to a failure or malfunction in the FCC hardware or wiring.
MCAS-Scen-1.2: MCAS does not provide stabilizer ND command because MCAS incorrectly believes the AOA threshold has not been exceeded for the current Mach number. MCAS is operating on incorrect Mach number or AOA data, stemming from a failure or malfunction in the ADIRU hardware or wiring.
MCAS-Scen-1.3: MCAS does not provide stabilizer ND command because MCAS incorrectly believes the AOA threshold has not been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively low AOA data, which appears to indicate the aircraft is at an AOA below the Mach number threshold when it is actually above. The AOA sensor was bent or separated from the aircraft by impact with a foreign object, leading it to produce an inaccurate signal.
MCAS-Scen-1.4: MCAS does not provide stabilizer ND command because MCAS incorrectly believes the AOA threshold has not been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively low AOA data, which appears to indicate the aircraft is at an AOA below the Mach number threshold when it is actually above. The AOA sensor was bent or otherwise damaged during maintenance procedures, leading it to produce an erroneously low signal.
MCAS-Scen-1.5: MCAS does not provide stabilizer ND command because MCAS incorrectly believes the AOA threshold has not been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively low AOA data, which appears to indicate the aircraft is at an AOA below the Mach number threshold when it is actually above. A fixed bias was introduced into the AOA sensor during maintenance procedures, leading it to produce an erroneously low signal.

MCAS-UCA-2: MCAS provides stabilizer ND command when aircraft is not in flaps up, high angle of attack maneuver [H-2, H-3]
MCAS-Scen-2.1: MCAS provides stabilizer ND command due to a failure or malfunction in the FCC hardware or wiring.

MCAS-Scen-2.2: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS is operating on incorrect Mach number or AOA data, stemming from a failure or malfunction in the ADIRU hardware or wiring.
MCAS-Scen-2.3: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor was bent or separated from the aircraft by impact with a foreign object, leading it to produce an inaccurate signal that is still within the sensor's defined range. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.
MCAS-Scen-2.4: MCAS provides a stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor was bent or otherwise damaged during maintenance procedures, leading it to produce an erroneously high signal that is still within the sensor's defined range. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.
MCAS-Scen-2.5: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. A fixed bias was introduced into the AOA sensor during maintenance procedures, leading it to produce an inaccurate signal that is still within the sensor's defined range. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.
MCAS-Scen-2.6: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor was obstructed

as a result of maintenance procedures, leading it to produce an inaccurate signal that is still within the sensor's defined range.
MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.

MCAS-Scen-2.7: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor lost heating and froze, making it unable to rotate and leading it to produce an inaccurate signal that is still within the sensor's defined range.
MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.

MCAS-Scen-2.8: MCAS provides stabilizer ND command because MCAS incorrectly believes the AOA threshold has been exceeded for the current Mach number. MCAS receives incorrect feedback in the form of excessively high AOA data, which appears to indicate the aircraft is at an AOA above the Mach number threshold when it is actually not. The AOA sensor was separated from the aircraft as a result of installation errors, leading it to produce an inaccurate signal that is still within the sensor's defined range.
MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could trigger an MCAS activation.

MCAS-UCA-3: MCAS provides stabilizer ND command when aircraft is out of trim in ND direction [H-2, H-3]

MCAS-Scen-3.1: MCAS provides a stabilizer ND command after already having provided a stabilizer ND command that was not fully countered. After a first MCAS activation (see scenarios for MCAS-UCA-2), MCAS's flight control law is reset by the AOA value going below the threshold for the current Mach number, and MCAS provides a stabilizer NU command. MCAS then activates a second time because the AOA value once again goes above the threshold for the current Mach number [MCAS-UCA-3]. This can occur if the AOA value periodically oscillates from being above and below the Mach number threshold. The oscillation may stem from a damaged, obstructed or improperly calibrated AOA sensor or pitot-static probe (see MCAS scenarios 2.3 – 2.9). As a result, the aircraft is out of trim by at most 2.5^{o} [H-3-1].

MCAS-Scen-3.2: MCAS provides a stabilizer ND command after already having provided a stabilizer ND command that was not fully countered. After a first MCAS activation (see scenarios for MCAS-UCA-2), MCAS's flight control law is reset without MCAS having provided or completed providing a stabilizer NU command. This can occur due to a failure or malfunction in the FCC hardware or wiring, triggering a spurious MCAS reset command. MCAS then provides a stabilizer ND a second time five seconds after the reset [MCAS-UCA-3]. As a result, the aircraft is out of trim by an amount dependent on the number of successive MCAS stabilizer ND commands [H-3-1].
MCAS-Scen-3.3: MCAS provides a stabilizer ND command after already having provided a stabilizer ND command that was not fully countered. After a first MCAS activation (see scenarios for MCAS-UCA-2), MCAS's flight control law is reset without MCAS having provided or completed providing a stabilizer NU command to counter a prior ND command. This occurs because the flight crew provides electric stabilizer trim commands before the AOA value goes below the threshold for the current Mach number, when MCAS would have begun providing the stabilizer NU command. MCAS's control law is reset and MCAS then provides a stabilizer ND command a second time five seconds after the reset [MCAS-UCA-3]. If the flight crew reacts in the same manner to the second MCAS command, the system is reset again and the UCA may repeat itself. As a result, the aircraft is out of trim by an amount dependent on the number of successive MCAS stabilizer ND commands [H-3-1].
MCAS-Scen-3.4: MCAS provides a stabilizer ND command after already having provided a stabilizer ND command that was not fully countered. After a first MCAS activation (see scenarios for MCAS-UCA-2), MCAS's flight control law is reset without MCAS having provided or completed providing a stabilizer NU command. This occurs because the flight crew moves the stabilizer trim cutout switches to the CUTOUT position and back to the normal position before the AOA value goes below the threshold for the current Mach number. MCAS's control law is reset and MCAS then provides a stabilizer ND command a second time five seconds after the reset [MCAS-UCA-3]. As a result, the aircraft is out of trim by an amount dependent on the number of successive MCAS stabilizer ND commands [H-3-1].

MCAS-UCA-4: MCAS provides stabilizer ND command resulting in stabilizer movement of more than the maximum of 2.5^{o} [H-2, H-3]
MCAS-Scen-4.1: MCAS initiates a stabilizer ND command and failures in the FCC's internal clock cause MCAS not to halt the stabilizer ND command (of rate 0.27^{o}/sec) after 9.2 seconds [MCAS-UCA-4]. As a result, aircraft is out of trim by at least 2.5^{o} [H-3-1].
MCAS-Scen-4.2: MCAS initiates a stabilizer ND command and failures in the FCC's hardware or wiring cause MCAS to provide a stabilizer ND command of rate higher than 0.27^{o}/sec for at most 9.2 seconds [MCAS-UCA-4]. As a result, aircraft is out of trim by at least 2.5^{o} [H-3-1].
MCAS-Scen-4.3: MCAS initiates a stabilizer ND command while the speed trim system is already providing a stabilizer ND command, causing the stabilizer ND command to proceed at a rate higher than 0.27^{o}/sec [MCAS-UCA-4]. The system may not possess protections against two

simultaneous commands from different automated controllers, and the commanded rate of stabilizer motion from both commands may be added. As a result, the stabilizer moves at a faster rate than expected and the aircraft is out of trim by at least 2.5° [H-3-1].

MCAS-UCA-5: MCAS provides stabilizer ND command when stabilizer trim is affecting aircraft pitch [H-2, H-3]

MCAS-Scen-5.1: MCAS provides repeated stabilizer ND commands (see scenarios for MCAS-UCA-3). As a result, the aircraft is out of trim by an amount dependent on the number of successive MCAS stabilizer ND commands. MCAS does not receive feedback about the change in pitch since the ND was command was issued, so MCAS is unable to detect if the ND commands are affecting aircraft pitch or not. As a result, the aircraft is further driven out of trim [H-3-1].

MCAS-UCA-6: MCAS provides stabilizer ND command too late after aircraft enters flaps up, high angle of attack maneuver [H-2]

MCAS-Scen-6.1: MCAS provides stabilizer ND command too late after aircraft enters flaps up, high angle of attack maneuver [MCAS-UCA-6] because AOA sensor input is delayed due to a failure or malfunction in the FCC or ADIRU hardware or wiring.

MCAS-UCA-7: MCAS provides stabilizer ND command for too long compared to the AOA value's exceedance of the threshold at the current Mach number [H-2, H-3]

MCAS-Scen-7.1: MCAS initiates a stabilizer ND command and failures in the FCC's internal clock cause MCAS not to halt the stabilizer ND command (of rate 0.27°/sec) after the appropriate time based on the AOA threshold [MCAS-UCA-7]. As a result, aircraft is out of trim by a variable amount of degrees [H-3-1].

MCAS-Scen-7.2: MCAS initiates a stabilizer ND command with the AOA at a certain value above the threshold. While MCAS is active, the aircraft's pitch or environment changes and the AOA value decreases, possibly but not necessarily dipping below the threshold. MCAS may have determined the duration of the stabilizer ND command based on the initial AOA value and may not adjust the duration of the command in real-time based on AOA changes [MCAS-UCA-7]. As a result, MCAS issues a stabilizer ND command for longer than necessary and aircraft is out of trim by a variable amount of degrees [H-3-1].

MCAS-Scen-7.3: MCAS initiates a stabilizer ND command with the AOA at a certain value above the threshold. While MCAS is active, the aircraft's airspeed changes and the Mach number threshold is altered, possibly but not necessarily placing the AOA below the threshold. MCAS may have determined the duration of the stabilizer ND command based on the initial AOA value and threshold and may not adjust the duration of the command in real-time based on Mach number

changes [MCAS-UCA-7]. As a result, MCAS issues a stabilizer ND command for longer than necessary and aircraft is out of trim by a variable amount of degrees [H-3-1].

MCAS-UCA-8: MCAS does not provide stabilizer NU command when AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]

MCAS-Scen-8.1: A failure or malfunction in the FCC hardware or wiring prevents MCAS from providing a stabilizer NU command when AOA threshold is no longer exceeded [MCAS-UCA-8]. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1].

MCAS-Scen-8.2: MCAS incorrectly believes the AOA threshold is still exceeded for the current Mach number and does not provide stabilizer NU command [MCAS-UCA-8]. MCAS may be operating on incorrect Mach number or AOA data. The incorrect data may stem from a failure or malfunction in the ADIRU hardware or wiring. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1].

MCAS-Scen-8.3: MCAS incorrectly believes the AOA threshold is still exceeded for the current Mach number and does not provide stabilizer NU command [MCAS-UCA-8]. MCAS may be operating on incorrect Mach number or AOA data. The incorrect data may stem from a damaged, obstructed or improperly calibrated AOA sensor or pitot-static probe. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could lead MCAS to believe the AOA threshold is still exceeded. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1].

MCAS-Scen-8.4: MCAS's flight control law is reset after MCAS provides a stabilizer ND command and before MCAS initiates a stabilizer NU command. This occurs because the flight crew provides electric stabilizer trim commands before the AOA value goes below the threshold for the current Mach number, when MCAS would have begun providing the stabilizer NU command. MCAS's control law is reset and MCAS then does not provide stabilizer NU command [MCAS-UCA-8]. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1].

MCAS-Scen-8.5: MCAS's flight control law is reset after MCAS provides a stabilizer ND command and before MCAS initiates a stabilizer NU command. This occurs because the flight crew moves the stabilizer trim cutout switches to the CUTOUT position and back to the normal position before the AOA value goes below the threshold for the current Mach number. MCAS's control law is reset and MCAS then provides a stabilizer ND command a second time five seconds after the reset [MCAS-UCA-8]. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1].

MCAS-UCA-9: MCAS provides stabilizer NU command when aircraft is in flaps up, high angle of attack maneuver and MCAS has not previously moved stabilizer ND [H-2, H-3]
MCAS-Scen-9.1: A failure or malfunction in the FCC hardware or wiring prevents MCAS from providing a stabilizer ND command when AOA value goes above the threshold for the current Mach number. MCAS may not register that the stabilizer ND command has not gone through and may provide stabilizer NU command anyway [MCAS-UCA-9]. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the MCAS stabilizer NU command [H-2, H-3-1].
MCAS-Scen-9.2: A failure or malfunction in the stabilizer trim motor hardware or the jackscrew prevents an MCAS stabilizer ND command from actually moving the stabilizer when AOA value goes above the threshold for the current Mach number. MCAS may not register that the stabilizer ND command has not resulted in actual movement of the stabilizer, and may provide a stabilizer NU command anyway [MCAS-UCA-9]. If the hardware failure only prevents jackscrew rotation in one direction, the stabilizer NU command may still go through and result in movement of the stabilizer. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the MCAS stabilizer NU command [H-2, H-3-1].

MCAS-UCA-10: MCAS provides stabilizer NU command too late after AOA threshold is no longer exceeded following flaps up, high angle of attack maneuver [H-2, H-3]
MCAS-Scen-10.1: MCAS incorrectly believes the AOA threshold is still exceeded for the current Mach number and takes too long to provide stabilizer NU command [MCAS-UCA-10]. MCAS may be operating on incorrect Mach number or AOA data. The incorrect data may stem from a damaged, obstructed or improperly calibrated AOA sensor or pitot-static probe. MCAS receives data from the ADIRU, which only generates an "AOA signal failed" flag if the resolver output is zero volts, the combined amplitude of the signal is outside the acceptable range, or the calculated AOA vane shaft angle is outside the range defined by the vane's mechanical stops. Erroneous AOA data that does not fall within these categories would be treated as valid by the ADIRU and could lead MCAS to believe the AOA threshold is still exceeded. As a result, the aircraft is out of trim by an amount dependent on the magnitude of the prior MCAS stabilizer ND command [H-3-1], until the NU command is provided.

MCAS-UCA-11: MCAS provides stabilizer ND command for too long compared to MCAS' previous stabilizer ND command [H-2, H-3]
MCAS-Scen-11.1: MCAS initiates a stabilizer NU command and failures in the FCC's internal clock cause MCAS not to halt the stabilizer NU command (of rate 0.27º/sec) after the command duration matches previous stabilizer ND command [MCAS-UCA-11]. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].

MCAS-Scen-11.2: MCAS initiates a stabilizer NU command and failures in the FCC lead MCAS to not store or lose information relating to the duration of the previous stabilizer ND command. MCAS's process model no longer contains information about the necessary duration of the corresponding stabilizer NU command, causing MCAS not to halt the stabilizer NU command after the duration matches previous stabilizer ND command [MCAS-UCA-11]. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].

MCAS-UCA-12: MCAS stops providing stabilizer NU command too soon before matching duration of MCAS' previous stabilizer ND command [H-2, H-3]
MCAS-Scen-12.1: MCAS initiates a stabilizer NU command and failures in the FCC's internal clock cause MCAS to halt the stabilizer NU command (of rate 0.27º/sec) before reaching the duration that matches the previous stabilizer ND command [MCAS-UCA-12]. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].
MCAS-Scen-12.2: MCAS initiates a stabilizer NU command and failures in the FCC lead MCAS to not store or lose information relating to the duration of the previous stabilizer ND command. MCAS's process model no longer contains information about the necessary duration of the corresponding stabilizer NU command, causing MCAS to halt the stabilizer NU command before reaching the duration that matches the previous stabilizer ND command [MCAS-UCA-12]. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].
MCAS-Scen-12.3: MCAS initiates a stabilizer NU command when AOA value goes below the threshold for the current Mach number, but the AOA then oscillates back above the Mach number threshold before MCAS has completed the stabilizer NU command. MCAS then halts the stabilizer NU command before reaching the duration that matches the previous stabilizer ND command [MCAS-UCA-12]. MCAS may then initiate another stabilizer ND command. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].

B.4.2. Flight Crew Scenarios

FC-UCA-1: Flight crew does not provide stabilizer NU command when stabilizer ND motion by MCAS occurs outside a flaps up, high angle of attack maneuver [H-2, H-3]
FC-Scen-1.1: Flight crew are unaware of the stabilizer ND motion, or are aware of the motion but do not diagnose it as unusual or unintended. Flight crew therefore do not provide stabilizer NU command to counter it [FC-UCA-1]. MCAS has a maximum limit of 2.5^{o} for each individual stabilizer ND command, so a short duration command only causes slight movement of the stabilizer trim wheel and trim indicator. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Movement of the stabilizer may go unnoticed by flight crew preoccupied with other more salient stimuli in the cockpit. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch down excessively [H-2] and approach terrain [H-1, H-4].
FC-Scen-1.2: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but believe they can stop and overcome the unintended stabilizer motion using control column inputs alone. Flight crew therefore do not provide stabilizer NU command to counter ND motion [FC-UCA-1]. All automatic stabilizer ND commands (except those issued by MCAS) can be interrupted through a control column input in the opposite direction. During stabilizer trim commands issued by MCAS, the control column cutout feature is inhibited and will not interrupt the stabilizer ND commands. Flight crews are not made aware of the existence of MCAS, nor its ability to inhibit the control column cutout feature. Flight crew may notice aircraft responding to control column inputs and may not realize the stabilizer ND commands were not interrupted. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not sufficiently use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-1.3: The flight crew notice the stabilizer ND motion and diagnose it as unintended, but do not issue stabilizer NU commands [FC-UCA-1] because they prioritize resolving other flight deck alerts and indications first. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings that are more salient than the stabilizer ND motion. If at low altitude, flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts, according to how they were trained. As a result, the aircraft is out of trim by a variable number of degrees [H-3-1]. If the flight crew intentionally pitch down to avoid a stall, the aircraft may enter an excessive nose-down attitude [H-2] and approach terrain [H-1, H-4].

FC-Scen-1.4: Flight crew provides stabilizer NU commands but the commands do not result in NU motion of the stabilizer [FC-UCA-1]. Flight crew may provide electric trim commands and a failure in the hardware or wiring of the stabilizer trim motor results in the commands not being actuated upon. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-Scen-1.5: Flight crew is unable to provide stabilizer NU commands [FC-UCA-1]. Flight crew cannot provide electric stabilizer NU command because stabilizer trim cutout switches have been activated before aircraft is retrimmed following unintended stabilizer ND motion. Flight crew then cannot successfully provide manual NU trim command because aerodynamic forces on the horizontal stabilizer are too high and moving the stabilizer trim wheel requires excessive physical strength. Flight crew may also need two hands for other cockpit tasks such as maintaining the aircraft's altitude and attitude or performing other non-normal procedures. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-2: Flight crew provides stabilizer NU command when intended ND stabilizer motion by MCAS occurs during flaps up, high angle of attack maneuver [H-2, H-3]

FC-Scen-2.1: Flight crew notice stabilizer ND motion they did not command and do not realize that motion is crucial to increasing the stick force gradient and reducing the aircraft's pitch up tendency. They therefore provide stabilizer NU command that counters intended stabilizer ND motion [FC-UCA-2]. Flight crew are not made aware of the existence of MCAS, nor the difference in pitch-up tendencies between the Boeing 737 MAX and 737NG in high angle of attack maneuvers. Though the flight crew may recognize the stabilizer motion as the existing Speed Trim System, MCAS moves the stabilizer at a faster rate and under different circumstances. Flight crew may be intentionally performing flaps up, high angle of attack maneuver to avoid a collision. As a result, the aircraft pitches up according to its natural tendency and may approach a stall [H-2-1].

FC-UCA-3: Flight crew provides stabilizer NU command too late (>4 seconds) after unintended ND stabilizer motion by MCAS occurs [H-2, H-3]

FC-Scen-3.1: Flight crew are not immediately aware of the stabilizer ND motion and therefore provide stabilizer NU command too late to fully counter it [FC-UCA-3]. MCAS has a maximum limit of 2.5º for each individual stabilizer ND command, so a short duration command only causes slight movement of the stabilizer trim wheel and trim indicator. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Movement of the stabilizer may go unnoticed by flight crew preoccupied with other stimuli in the cockpit. Flight crew may only become aware of stabilizer ND motion after feeling high control column forces for an extended

period of time. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-3.2: Flight crew notice the stabilizer ND motion but do not immediately diagnose the motion as unintended and therefore take too long to provide stabilizer NU command to counter ND motion [FC-UCA-3]. They may believe the motion to be intended by the flight control computer to counter a physical phenomenon they cannot perceive or appropriately react to. In autopilot off configuration, flight crew are not notified when automatic trim commands are issued by the speed trim system, nor are they informed what conditions were met to issue that command. Flight crew commonly observe movement of the stabilizer trim wheel during flight, especially during takeoff/landing operations. Flight crew may only become aware that stabilizer ND motion is unintended after feeling high control column forces for an extended period of time. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-3.3: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but initially believe they can stop and overcome the unintended stabilizer motion using control column inputs alone. All automatic stabilizer ND commands (except those issued by MCAS) can be interrupted through a control column input in the opposite direction. During stabilizer trim commands issued by MCAS, the control column cutout feature is inhibited and will not interrupt the stabilizer ND commands. Flight crews are not made aware of the existence of MCAS, nor its ability to inhibit the control column cutout feature. Flight crew only realize that the stabilizer ND commands were not interrupted after control column forces continue for extended periods of time following the stabilizer motion. Only then do the flight crew provide stabilizer NU command to counter ND motion [FC-UCA-3]. If in the meantime the flight crew do not sufficiently use the control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-3.4: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but take too long to provide stabilizer NU commands [FC-UCA-3] because they prioritize resolving other flight deck alerts and indications first. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings that are more salient than the stabilizer ND motion. Flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts. If in the meantime the flight crew do not sufficiently use the control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-3.5: Flight crew is unable to immediately provide stabilizer NU commands [FC-UCA-3]. Flight crew cannot provide electric stabilizer NU command because stabilizer trim cutout switches have been activated before aircraft is retrimmed following unintended stabilizer ND motion. Flight crew then cannot successfully provide manual NU trim command because aerodynamic forces on the horizontal stabilizer are too high and moving the stabilizer trim wheel requires excessive physical strength. Flight crew may also need two hands for other cockpit tasks

such as maintaining the aircraft's altitude and attitude or performing other non-normal procedures. Flight crew takes time to realize that they cannot provide manual NU trim command and need to move stabilizer trim cutout switches back to "normal" position. Only after moving the cutout switches back do the flight crew provide stabilizer NU command to counter ND motion. If in the meantime the flight crew do not sufficiently use the control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-4: Flight crew stops providing stabilizer NU command too early before aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3]

FC-Scen-4.1: Flight crew are unaware of the length of the prior unintended stabilizer ND motion and therefore do not provide sufficient stabilizer NU command to counter it [FC-UCA-4]. In autopilot off configuration, flight crew are not notified when automatic trim commands are issued by the speed trim system, nor are they informed what conditions were met to issue that command. Flight crew commonly observe movement of the stabilizer trim wheel during flight, especially during takeoff/landing operations, and may not notice the unintended motion as soon as it begins. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects that draw the flight crew's attention. As a result, aircraft is out of trim by a variable number of degrees [H-3-1] and MCAS is reset.

FC-Scen-4.2: Flight crew are unaware of the length of their own stabilizer NU command and therefore do not provide sufficient command to counter a prior stabilizer ND command [FC-UCA-4]. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects that draw the flight crew's attention. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts and not pay significant attention to the length of their own stabilizer NU command. As a result, aircraft is out of trim by a variable number of degrees [H-3-1] and MCAS is reset.

FC-Scen-4.3: Changes in the aircraft's speed, attitude, or configuration alter the stabilizer angle that achieves neutral trim, as compared to before the unintended stabilizer ND motion. Flight crew are unaware of the appropriate duration of a stabilizer NU command to counter the prior stabilizer ND command given the aircraft's new condition. They therefore stop providing stabilizer NU too early [FC-UCA-4]. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects and the flight crew may modify the aircraft's configuration as part of a procedure to address other cockpit alerts before initiating a stabilizer NU command. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].

FC-UCA-5: Flight crew provides stabilizer NU command for too long after aircraft reaches neutral trim following unintended stabilizer ND motion by MCAS [H-2, H-3]

FC-Scen-5.1: Flight crew are unaware of the length of the prior unintended stabilizer ND motion and therefore unintentionally provide excessive stabilizer NU command to counter it [FC-UCA-5]. In autopilot off configuration, flight crew are not notified when automatic trim commands are issued by the speed trim system, nor are they informed what conditions were met to issue that command. Flight crew commonly observe movement of the stabilizer trim wheel during flight, especially during takeoff/landing operations, and may not notice the unintended motion as soon as it begins. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects that draw the flight crew's attention. As a result, aircraft is out of trim by a variable number of degrees [H-3-1] and MCAS is reset.

FC-Scen-5.2: Flight crew are unaware of the length of the prior unintended stabilizer ND motion and therefore intentionally provide excessive stabilizer NU command to counter it [FC-UCA-5]. In autopilot off configuration, flight crew are not notified when automatic trim commands are issued by the speed trim system, nor are they informed what conditions were met to issue that command. Additional flight deck effects may draw the flight crew's attention and they may not notice when the prior stabilizer ND motion began. If the aircraft is already in a pitch down orientation, or is at low altitude, the flight crew may overcorrect the aircraft's trim in the NU direction to prevent further pitch down. As a result, aircraft is out of trim by a variable number of degrees [H-3-1] and MCAS is reset.

FC-Scen-5.3: Flight crew are unaware of the length of their own stabilizer NU command and therefore provide excessive command to counter a prior stabilizer ND command [FC-UCA-5]. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects that draw the flight crew's attention. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts and not pay significant attention to the length of their own stabilizer NU command. As a result, aircraft is out of trim by a variable number of degrees [H-3-1] and MCAS is reset.

FC-Scen-5.4: Changes in the aircraft's speed, attitude, or configuration alter the stabilizer angle that achieves neutral trim, as compared to before the unintended stabilizer ND motion. Flight crew are unaware of the appropriate duration of a stabilizer NU command to counter the prior stabilizer ND command given the aircraft's new condition. They therefore provide an excessive stabilizer NU [FC-UCA-5]. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects and the flight crew may modify the aircraft's configuration as part of a procedure to address other cockpit alerts before initiating a stabilizer NU command. As a result, aircraft is out of trim by a variable number of degrees [H-3-1].

FC-UCA-6: Flight crew does not provide stabilizer trim cutout command when MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]

FC-Scen-6.1: Flight crew are unaware of the stabilizer ND motion and therefore do not provide stabilizer trim cutout command to counter it [FC-UCA-6]. MCAS has a maximum limit of 2.5^{o}

for each individual stabilizer ND command, so a short duration command only causes slight movement of the stabilizer trim wheel and trim indicator. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings. Movement of the stabilizer may go unnoticed by flight crew preoccupied with other stimuli in the cockpit. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-Scen-6.2: Flight crew notice the stabilizer ND motion but do not believe the motion to be unintended and therefore do not provide stabilizer trim cutout command to counter it [FC-UCA-6]. They may believe the motion to be intended by the flight control computer to counter a physical phenomenon they cannot perceive or appropriately react to. In autopilot off configuration, flight crew are not notified when automatic trim commands are issued by the speed trim system, nor are they informed what conditions were met to issue that command. Flight crew commonly observe movement of the stabilizer trim wheel during flight, especially during takeoff/landing operations. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-Scen-6.3: The flight crew notice the stabilizer ND motion, but do not believe the motion to be a stabilizer trim runaway that requires a stabilizer trim cutout command. A stabilizer trim runaway is defined as continuous movement of the stabilizer trim wheel, and the stabilizer runaway procedure is concluded if unintended stabilizer motion stops when the autopilot is disengaged. MCAS only operates with autopilot off, and stabilizer ND motion will stop after either 9.2 seconds or any manual electric stabilizer trim commands by the flight crew. The flight crew notice that they can interrupt and overcome the stabilizer motion using stabilizer NU commands alone and diagnose the situation as something other than a stabilizer trim runaway. The flight crew therefore do not provide a stabilizer trim cutout command to counter ND motion [FC-UCA-6]. The flight crew are not aware that countering MCAS-issued stabilizer ND commands with only manual electric stabilizer NU commands allows MCAS to issue repeated commands (see MCAS-Scen-7.4). As a result, the aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use the control column to maintain altitude and attitude, the aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-Scen-6.4: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but do not provide stabilizer trim cutout command [FC-UCA-6] because they prioritize resolving other flight deck alerts and indications first. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings that are more salient than the stabilizer ND motion. Flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If

flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-6.5: Flight crew provides stabilizer trim cutout command but the commands do not stop stabilizer ND motion [FC-UCA-6]. A failure in the hardware or wiring of the cutout switches or stabilizer trim motor results in the cutout command not reaching the motor. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-7: Flight crew provides stabilizer trim cutout command during flaps up, high angle of attack maneuver [H-2, H-3]
FC-Scen-7.1: Flight crew notice stabilizer ND motion they did not command and do not realize that motion is crucial to increasing the stick force gradient and reducing the aircraft's pitch up tendency. After providing stabilizer NU command to counter stabilizer ND motion, MCAS is reset and provides another stabilizer ND command 5 seconds later. Flight crew therefore provides stabilizer trim cut out command to prevent repeated intended stabilizer ND motion [FC-UCA-7]. Flight crew may be intentionally performing flaps up, high angle of attack maneuver to avoid a collision and are not made aware of the existence of MCAS, nor the difference in pitch-up tendencies between the Boeing 737 MAX and 737NG in high angle of attack maneuvers. Though the flight crew may recognize the stabilizer motion as the existing Speed Trim System, MCAS moves the stabilizer at a faster rate and under different circumstances. As a result of the stabilizer trim cutout command, the aircraft pitches up according to its natural tendency and may approach a stall [H-2-1].

FC-UCA-8: Flight crew provides stabilizer trim cutout command when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]
FC-Scen-8.1: Flight crew notice repeated automatic stabilizer ND commands and provide stabilizer trim cutout command [FC-UCA-8] without awareness that they will not be able to manually retrim aircraft using stabilizer trim wheels. Runaway stabilizer procedure requires flight crew to "control airplane pitch attitude manually with control column and main electric trim as needed" but does not specifically require aircraft to be neutrally trimmed before providing stabilizer trim cutout command. Flight crew are not provided feedback on whether or not they will be able to manually trim the aircraft based on the current flight parameters. As a result of the stabilizer trim cutout command, the aircraft remains out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-9: Flight crew provides stabilizer trim cutout command too late (>4 seconds) after MCAS issues trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]
FC-Scen-9.1: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but believe they can stop and overcome the unintended stabilizer motion using stabilizer NU commands alone. Flight crew notice automatic stabilizer ND commands are interrupted and can be fully countered by manual electric stabilizer NU commands. Flight crew are not aware that countering MCAS-issued stabilizer ND commands with only manual electric stabilizer NU commands allows MCAS to issue repeated commands (see scenario 7.4 for MCAS-UCA-7). Flight crew therefore do not provide stabilizer trim cutout command to counter ND motion until they notice multiple repeated MCAS commands [FC-UCA-9]. As a result, aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, or use appropriate manual electric trim commands to bring aircraft to neutral trim, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].
FC-Scen-9.2: Flight crew notice the stabilizer ND motion and diagnose it as unintended, but take too long to provide stabilizer trim cut out command [FC-UCA-9] because they prioritize resolving other flight deck alerts and indications first. Unintended activations of MCAS (see scenarios for MCAS-UCA-2) may also coincide with additional flight deck effects. If the source of the unintended MCAS activation is erroneous data from AOA or pitot-static probes, the flight crew may also experience effects like stick shaker activation, inconsistent airspeed and altitude displays, and IAS or ALT disagree warnings that are more salient than the stabilizer ND motion. Flight crew may prioritize addressing a potential impending stall or performing the necessary procedure to address other cockpit alerts. If in the meantime the flight crew do not use control column to maintain altitude and attitude, or use appropriate manual electric trim commands to bring aircraft to neutral trim, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-10: Flight crew does not move stabilizer trim cut out switches to normal when aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]
FC-Scen-10.1: Flight crew believe that moving stabilizer trim cutout switches to "normal" may reactivate unintended stabilizer ND commands previously observed and therefore decide to not move stabilizer trim cutout switches [FC-UCA-10]. Flight crew had earlier provided stabilizer trim cutout command according to stabilizer trim runaway procedure to address unintended stabilizer ND commands. Runaway procedure only includes guidance to "trim manually" and does not provide a recommended response if the aircraft cannot be manually retrimmed. 737 flight crew training manual (FCTM) indicates the crew may need to "aerodynamically relieve the airloads to allow manual trimming" by "[accelerating] or [decelerating] towards the in-trim speed" but does not provide specific procedures for doing so. Flight crew may believe that attempting to manually trim is safer than restoring use of manual electric trim while at the same time reactivating a potential stabilizer runaway. As a result, aircraft remains out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-11: Flight crew moves stabilizer trim cutout switches to normal when MCAS provides trim commands outside of a flaps up, high angle of attack maneuver [H-2, H-3]
FC-Scen-11.1: After flight crew provide stabilizer trim cutout command according to stabilizer trim runaway procedure, flight crew becomes aware that they cannot manually retrim the aircraft because aerodynamic forces on the horizontal stabilizer are too high and moving the stabilizer trim wheel requires excessive physical strength. Flight crew may also need two hands for other cockpit tasks such as maintaining the aircraft's altitude and attitude or performing other non-normal procedures. Flight crew cannot aerodynamically relieve loads on the stabilizer due to proximity to the ground. Flight crew decides to move stabilizer trim cutout switches to normal [FC-UCA-11] in order to reactivate manual electric stabilizer trim. As a result, MCAS is reset and may issue unintended stabilizer ND commands (see scenarios for MCAS-UCA-2 and MCAS-UCA-3), and aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].

FC-UCA-12: Flight crew moves stabilizer trim cut out switches to normal too late after aircraft is out of trim and cannot be manually retrimmed [H-2, H-3]
FC-Scen-12.1: Flight crew believe that moving stabilizer trim cutout switches to "normal" may reactivate unintended stabilizer ND commands previously observed and therefore decide to not move stabilizer trim cutout switches, until they realize they cannot retrim the aircraft using manual trim wheels. Flight crew had earlier provided stabilizer trim cutout command according to stabilizer trim runaway procedure to address unintended stabilizer ND commands. Runaway procedure only includes guidance to "trim manually" and does not provide a recommended response if the aircraft cannot be manually retrimmed. 737 flight crew training manual (FCTM) indicates the crew may need to "aerodynamically relieve the airloads to allow manual trimming" by "[accelerating] or [decelerating] towards the in-trim speed" but does not provide specific procedures for doing so. Flight crew may take time to determine that they cannot manually retrim the aircraft, and may make an attempt to aerodynamically relieve airloads on the stabilizer depending on their altitude. Only after being unsuccessful in manually retrimming the aircraft does the flight crew move stabilizer trim cutout switches back to "normal" [FC-UCA-12]. As a result, MCAS is reset and may issue unintended stabilizer ND commands (see scenarios for MCAS-UCA-2 and MCAS-UCA-3), and aircraft is out of trim by a variable number of degrees [H-3-1]. If flight crew do not use control column to maintain altitude and attitude, aircraft may pitch excessively down [H-2] and approach terrain [H-1, H-4].