Master Thesis

A System Safety Assessment of an Unmanned, Solar-Powered Stratospheric Aircraft Using the STPA Methodology

Luca Stoll

Timeframe:	November 05, 2019 – June 08, 2020
Supervisor:	M. Sc. Florian Nikodem (DLR)
	M. Sc. Johannes Kuhnert Roca (ILS)

Institute of Aircraft Systems (ILS)
University of Stuttgart
Professor Dr.-Ing. Reinhard Reichel

Nr. M-63

Aufgabenstellung

Masterarbeit

Durchführung eines System Safety Assessments nach der STAMP-Methodik am Beispiel eines unbemannten, solarbetriebenen Stratosphärenflugzeugs

INSTITUT FÜR LUFTFAHRTSYSTEME
Ansprechpartner:
M.Sc. Johannes Kuhnert Roca
Universität Stuttgart
Institut für Luftfahrtsysteme
Pfaffenwaldring 27
70569 Stuttgart
+49 (0)711 685 69537
johannes.kuhnert-roca@ils.uni-stuttgart.de

Kontext

Moderne Luftfahrzeuge werden zunehmend komplexer, das heißt ihr Gesamtverhalten lässt sich trotz vollständiger Informationen über ihre Einzelkomponenten und deren Wechselwirkungen nicht eindeutig beschreiben. Im Zuge dessen sind nicht nur die Sicherheitsbetrachtungen einzelner Komponenten des Luftfahrzeugs relevant, sondern vor allem auch Sicherheitsbetrachtungen über die Interaktion dieser Komponenten untereinander. So können zwei Komponenten im System Luftfahrzeug durchaus ihren Spezifikationen gerecht funktionieren, im Zusammenspiel der beiden Komponenten können sich aber sicherheitskritische Folgen ergeben. Von besonderem Interesse ist dabei die Interaktion mit dem Menschen, zum Beispiel in Form eines Piloten oder der Bediener eines unbemannten Luftfahrzeugs. In der Interaktion von Mensch und komplexem System können sich schnell gefährliche Fehlerzustände entwickeln.

Aufgabe

Am Beispiel einer unbemannten solarbetriebenen Stratosphärenflugzeugs, welches zurzeit im DLR entwickelt wird, soll ein System Safety Assessment nach der Systems-Theoretic Accident Model and Processes (STAMP) Methodik durchgeführt werden. Dazu erfolgt zunächst die Einarbeitung in das Projekt Hochfliegende Unbemannte Plattform (HAP) und die speziellen sicherheitsrelevanten Eigenschaften und Voraussetzungen von unbemannten, solarbetriebenen Stratosphärenflugzeugen. Anschließend ist das allgemeine Vorgehen bei System Safety Assessments in der zivilen Luftfahrt sowie der STAMP-Methodik zu analysieren. Die wesentlichen Unterschiede der STAMP-Methodik zu den beschriebenen Vorgehensweisen in der SAE ARP 4754A sind dabei herauszustellen. Hauptteil der Arbeit ist die Anwendung der STAMP-Methodik in Form eines System Safety Assessments an einem repräsentativen Beispiel innerhalb des HAP Projekts, in dem der Mensch, z.B. in Form des Operators, interagiert.

Die Arbeitsschritte im Einzelnen:

1. Einarbeiten in das DLR Projekt HAP bzw. in die spezifischen Eigenheiten von unbemannten, solarbetriebenen Stratosphärenflugzeugen
2. Literaturrecherche und einarbeiten in das Vorgehen bei System Safety Assessments, im speziellen in die STAMP-Methodik
3. Herausstellen der wesentlichen Unterschiede der STAMP-Methodik zu den in der Luftfahrt üblichen System Safety Assessment Methoden, die in ARP 4754A beschrieben sind
    a) Darstellung der wesentlichen Grundlagen der in der bemannten Luftfahrt verwendeten Preliminary System Safety Methoden
    b) Darstellung der wesentlichen Grundlagen der STAMP-Methodik
    c) Analyse und Darstellung der Unterschiede der Methoden aus a. und b.
4. Anwenden der STAMP-Methodik auf Beispiele im DLR Projekt HAP in denen der Mensch Relevanz hat

   a) Auswahl eines geeigneten Beispiel innerhalb des Projekts HAP
   b) Durchführung eines qualitativen System Safety Assessments mittels STAMP-Methodik
   c) Zusammenfassung der Ergebnisse des Assessments
   d) Erarbeiten von Verbesserungsvorschlägen für das gewählte Beispiel, falls diese nach den Ergebnissen des SSA mittels STAMP-Methodik als notwendig erachtet werden

5. Dokumentation entsprechend der Vorgaben zur Anfertigung von Masterarbeiten der Fakultät für Luft- und Raumfahrttechnik und Geodäsie der Universität Stuttgart

Die Ergebnisse der Arbeit sind in einem Vortrag zu präsentieren.

Beginn:	05.11.2019
Abgabe:	04.05.2020
Betreuer ILS:	M.Sc. Johannes Kuhnert Roca
Betreuer DLR:	M.Sc. Florian Nikodem
Prüfer:	Dipl.-Ing. Matthias Lehmann

Datum, Unterschrift Betreuer: ______

Datum, Unterschrift Student: 05.11.2019 ______

Rechtliche Bestimmungen: Der Bearbeiter ist grundsätzlich nicht berechtigt, irgendwelche Arbeits- und Forschungsergebnisse, von denen er bei der Bearbeitung Kenntnis erhält, ohne Genehmigung des Betreuers dritten Personen zugänglich zu machen. Bezüglich erreichter Forschungsleistungen gilt das Gesetz über Urheberrecht und verwendete Schutzrecht (Bundesgesetzblatt I/S. 1273, Urheberschutzgesetz vom 09.09.1965). Der Bearbeiter hat das Recht, seine Erkenntnisse zu veröffentlichen, soweit keine Erkenntnisse und Leistungen der betreuenden Institute und Unternehmen eingeflossen sind. Die von der Studienrichtung erlassenen Richtlinien zur Anfertigung der Masterarbeit sowie die Prüfungsordnung sind zu beachten.

Statement of Authorship

I hereby assert that I wrote this master thesis independently with help of the supervisors and did not use any sources and tools other than the ones stated. The thesis or relevant content thereof has not already been used at any other educational institution to obtain graduation.

I further declare that the thesis complies with copy right protection regulations according to the rules of good scientific practice. [1] Insofar as the thesis includes content of third parties (e.g. pictures, drawings, text passages etc.) I have marked the content as such (quotation, indication of source etc.) and I have obtained any necessary permissions to use this content from the owners. I am aware that in case of a non-accidental violation of these regulations I will have to bear the consequences.

L. Stoll

Stuttgart, 08.06.2020

Luca Stoll

[1] As described in the DFG-regulations regarding "'Sicherung guter wissenschaftlicher Praxis"' or in the statute of the University of Stuttgart regarding "'Sicherung der Integrität wissenschaftlicher Praxis und zum Umgang mit Fehlerverhalten in der Wissenschaft"'

Declaration of Right of Use

I hereby agree that my master thesis with the topic:

A System Safety Assessment of an Unmanned, Solar-Powered Stratospheric Aircraft Using the STPA Methodology

will be stored in the library of the Institute of Aircraft Systems (ILS), accessible to the public effective immediately and that the thesis will be mentioned on the website of the Institute as well as in the online-catalog of the library of the University of Stuttgart. The latter means permanent worldwide accessibility of the biographical data of the thesis (title, author, publishing year, etc.).

For this purpose I will provide a second printed copy, besides the examination copy, and a digital version to my supervisor.

I declare the University of Stuttgart the owner of the additional printed copy and of the digital version. I declare a simple unlimited right of use of the thesis and the results of my work within the context of creating this thesis for research and education purposes. If the Institute for Aircraft Systems has agreements about the rights of use of this thesis, these agreements also apply to work results within the context of creating this thesis.

L. Stoll

Stuttgart, 08.06.2020

Luca Stoll

Abstract

A System Safety Assessment of an Unmanned, Solar-Powered Stratospheric Aircraft Using the STPA Methodology

Developed for electromechanical systems, traditional safety analysis methods can not provide sufficient guidance to handle the complexity of modern, software intensive systems. New ways of modeling complex systems and human operators in their sociotechnical environment and performing holistic, guided safety analysis based on these models have been developed by Nancy Leveson, Professor of Aeronautics and Astronautics and Professor of Engineering Systems at the Massachusetts Institute of Technology (MIT). This assignment compares the basic principles of the approach on how to achieve safety of a system proposed by the SAE ARP4754A and the approach proposed by Nancy Leveson's Systems-Theoretic Accident Model and Processes (STAMP) causality theory, including the thereon based Systems-Theoretic Process Analysis (STPA) hazard analysis method. General definitions and assumptions, boundaries, potential weaknesses and advantages of the approaches are estimated, compared and summarized. STPA, including an extension based on works by M. France and J. P. Thomas on how to model and analyze human operators effectively, is further applied on exemplary parts of the High Altitude Platform (HAP) unmanned, solar-powered stratospheric aircraft of the German Aerospace Center (DLR). Applicability is shown, safety issues and causal loss scenarios in the system are identified, and design, operation and operator training recommendations are given. Identified advantages, difficulties and recommendations of practical application of STAMP/STPA are discussed. A proposal on how to include STAMP/STPA in future versions of the SAE ARP4754A is given.

Kurzzusammenfassung der Abschlussarbeit

Durchführung eines System Safety Assessments nach der STPA-Methodik am Beispiel eines unbemannten, solarbetriebenen Stratosphärenflugzeugs

Traditionelle, für elektromechanische Systeme entwickelte, sicherheitsanalytische Methoden bieten keine ausreichende Hilfestellung, um der Komplexität moderner, software-intensiver Systeme beizukommen. Neue Ansätze zur Modellierung von komplexen Systemen und den menschlichen Bedienern in ihrer soziotechnischen Umgebung und zur Ausführung ganzheitlicher, geführter Sicherheitsanalysen basierend auf diesen Modellen sind von Nancy Leveson, Professorin für Aeronautics und Astronautics und für Engineering Systems am Massachusetts Institute of Technology (MIT), entwickelt worden. Die vorliegende Arbeit vergleicht die grundlegenden Prinzipien zum Erlangen von Sicherheit in einem System des Ansatzes nach SAE ARP4754A und des Ansatzes nach Nancy Leveson's Systems-Theoretic Accident Model and Processes (STAMP) Kausalitätstheorie inklusive der darauf basierenden Systems-Theoretic Process Analysis (STPA) Analysemethode. Generelle Definitionen und Annahmen, Grenzen, potentielle Schwächen und Vorteile der Ansätze werden abgeschätzt, verglichen und zusammengefasst. STPA, inklusive einer Erweiterung zur effektiveren Modellierung von menschlichen Bedienern basierend auf Arbeiten von M. France und J. P. Thomas, wird auf exemplarische Teile des unbemannten, solarbetriebenen High Altitude Platform (HAP) Stratosphärenflugzeugs des Deutschen Zentrums für Luft- und Raumfahrttechnik (DLR) angewandt. Die Anwendbarkeit von STPA und der Erweiterung auf ein solches System wird demonstriert, Sicherheitsprobleme und kausale Verlustszenarien im System werden identifiziert und Design-, Betriebs- und Bediener-Training-Empfehlungen werden erstellt. Dabei beobachtete Vorteile und Schwierigkeiten sowie Empfehlungen zur praktischen Anwendung von STAMP/STPA werden besprochen. Ein Vorschlag zur Integration von STAMP/STPA in zukünftige Versionen der SAE ARP4754A wird unterbreitet.

"Human error is no longer a property of the human;
it's a property of the system we put them in."

John P. Thomas, MIT

Contents

List of Figures

List of Tables

List of Abbreviations

AMC	**A**cceptable **M**eans of **C**ompliance
ARP	**A**erospace **R**ecommended **P**ractice
ARP4754A	SAE International **A**erospace **R**ecommended **P**ractice 4754 Revision A
ARP4761	SAE International **A**erospace **R**ecommended **P**ractice 4761
ASA	**A**ircraft **S**afety **A**ssessment
CCA	**C**ommon **C**ause **A**nalysis
CMA	**C**ommon **M**ode **A**nalysis
CS	**C**ertification **S**pecifications
DD	**D**ependence **D**iagram
DLR	**D**eutsches **Z**entrum für **L**uft- und **R**aumfahrt e.V. (German Aerospace Center)
EASA	**E**ropean Union **A**viation **S**afety **A**gency
EU	**E**uropean **U**nion
FHA	**F**unctional **H**azard **A**ssessment
FMEA	**F**ailure **M**odes and **E**ffects **A**nalysis
FMES	**F**ailure **M**odes and **E**ffects **S**ummary
FTA	**F**ault **T**ree **A**nalysis
HAP	**H**igh **A**ltitude **P**latform
IR	**I**mplemented **R**ules
MA	**M**arkov **A**nalysis
PASA	**P**reliminary **A**ircraft **S**afety **A**ssessment
PSSA	**P**reliminary **S**ystem **S**afety **A**ssessment
rpm	**r**evolutions **p**er **m**inute
SSA	**S**ystem **S**afety **A**ssessment
STAMP	**S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocesses
STPA	**S**ystems-**T**heoretic **P**rocess **A**nalysis
SysML	**S**ystems **M**odeling **L**anguage
tbd	**t**o **b**e **d**iscussed
UCA	**U**nsafe **C**ontrol **A**ction
ZSA	**Z**onal **S**afety **A**nalysis

1 Introduction

The digital technical revolution changed aerospace technology. Modern aerospace systems are analog-digital symbioses with functions implemented in software, which had previously been electro-mechanical or human operator tasks or entirely impossible to realize. The digitalization of aerospace systems thus enables adding functionality without adding relevant weight. The added functionality and implementation in software and computer hardware increased the number of processes having influence on the aircraft and their interactions, which means the complexity of the system increased. The change in responsibility shifted the human operators role from a direct operator of a system to a manager of the automated, complex system.

Traditional safety engineering techniques were developed for less complex, electromechanical systems. The safety analysis methods therein are based on the assumption that accidents are solely the result of a combination of independent random failures in a system and the chain of failures resulting from these failures eventually ending in an accident. For this assumption to be true, the design must provide independence of the causes of these random independent failures and not provide any hazards when all components work the way they are intended to, without failures.

Nancy Leveson's, Professor of Aeronautics and Astronautics and Professor of Engineering Systems at the Massachusetts Institute of technology (MIT), accident causality research resulted in a criticism of the use of these traditional accident models and the corresponding hazard analysis methods on modern systems, as they were not sufficient to prevent the investigated accidents. Relying on engineering skills to design and analyze systems and the interactions therein, they could not deal with the level of complexity in modern systems leading to accidents without component failures, but with unsafe interactions between "functioning as intended" components or erroneous control actions by humans operators.

To address the technological changes that lead to these complex modern day systems and thus the new upcoming type of accidents, Leveson developed **S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocesses (STAMP) as a new accident causality theory, based on systems thinking and systems theory instead of reliability engineering. STAMP treats safety as a control problem, rather than a failure problem. Accidents are the result of inadequate enforcement of constraints on system behavior. With the reasons for the inadequate enforcement ranging from component failures, system and software design errors and erroneous human decision making to even socio-technical aspects such as company culture or societal influences.

Systems-**T**heoretic **P**rocess **A**nalysis (STPA) is a hazard analysis method based on STAMP. It is intended to identify potential causes of accidents (scenarios that can lead to losses) and so gain safety relevant knowledge about a system which can be used to create measures to control or mitigate hazards in the system design. Studies found that STPA can potentially identify more causes of hazards than traditional methods, including causes involving component failures, component interaction failures and human errors. [1] [2]

In this assignment the theoretic principles of traditional safety engineering and safety engineering techniques will be compared to the principles proposed by STAMP and engineering techniques based on STAMP. Further the STAMP technique will be applied on a real system to investigate applicability and potential boundaries, strengths and difficulties in the practical application.

For this purpose for the traditional principles and techniques the processes and methods as described in the SAE International **A**erospace **R**ecommended **P**ractice 4754 Revision A (ARP4754A) have been chosen, because of the widespread use of these processes and methods in aerospace industry. The therein proposed ways to achieve safety in a system and the underlying assumptions are discussed in chapter 2.

The STAMP causality theory and the STPA hazard analysis method are introduced in chapter 3 and an introduction to an extension to STPA by M. France and J. P. Thomas on how to model and analyze human operators more effectively is given.

The safety engineering principles and techniques of STAMP/STPA and ARP4754A are then compared in chapter 4.

In chapter 5, STPA, including the introduced extension, is applied to exemplary parts of the **D**eutsches **Z**entrum für **L**uft- und **R**aumfahrt e.V. (German Aerospace Center) (DLR) **H**igh **A**ltitude **P**latform (HAP) unmanned, solar-powered stratospheric aircraft.

Results and conclusions of the assignment are summarized in chapter 6.

2 The SAE ARP4754A approach to achieve safety

In chapter 2 the approach to achieve safety as described in the SAE ARP4754A and related documents are discussed.

Legal relations are herein explained for the legal sphere of the **E**uropean **U**nion (EU), the SAE International **A**erospace **R**ecommended **P**ractice (ARP) apply in similar manner for the United States of America and other legal spheres.

SAE International ARPs are not needed to be followed to gain a lawful aircraft certification under EU law. They are supposed to help to show compliance with the **E**ropean Union **A**viation **S**afety **A**gency (EASA) **C**ertification **S**pecifications (CS) and the EASA **A**cceptable **M**eans of **C**ompliance (AMC) and so with the EU Regulations to make it easier to gain such certification from the EASA. Neither CSs nor AMCs need to be followed to gain a lawful certification under EU law either:

"Certification Specifications (CS) are non-binding technical standards adopted by EASA to meet the essential requirements of the Basic Regulation. CSs are used to establish the certification basis (CB) as described below. Should an aerodrome operator not meet the recommendation of the CS, they may propose an Equivalent Level of Safety (ELOS) that demonstrates how they meet the intent of the CS. [...] Acceptable Means of Compliance (AMC) are non-binding. The AMC serves as a means by which the requirements contained in the Basic Regulation and the IRs can be met." [3]

Only the EU Regulations and **I**mplemented **R**ules (IR) have to be met for certification. The relations for the EU certification are shown in figure 2.1.

"The [SAE ARP4754A] guidelines [...] were developed in the context of Title 14 Code of Federal Regulations (14CFR) Part 25 and European Union Aviation Safety Agency (EASA) Certification Specification (CS) CS-25. [...] The current trend in system design is an increasing level of integration between aircraft functions and the systems that implement them. While there can be considerable value gained when integrating systems with other systems, the increased complexity yields increased possibilities for errors, particularly with functions that are performed jointly across multiple systems. [...] the use of the ARP4754/ED-79 in aircraft certification has become increasingly widespread." [4]

Through the increasingly widespread use of the ARP4754/ED-79 and the revised version ARP4754A, they and the related documents are the ideal documents to compare the therein described processes and methods on how to achieve safety to the processes and methods enabled through STAMP.

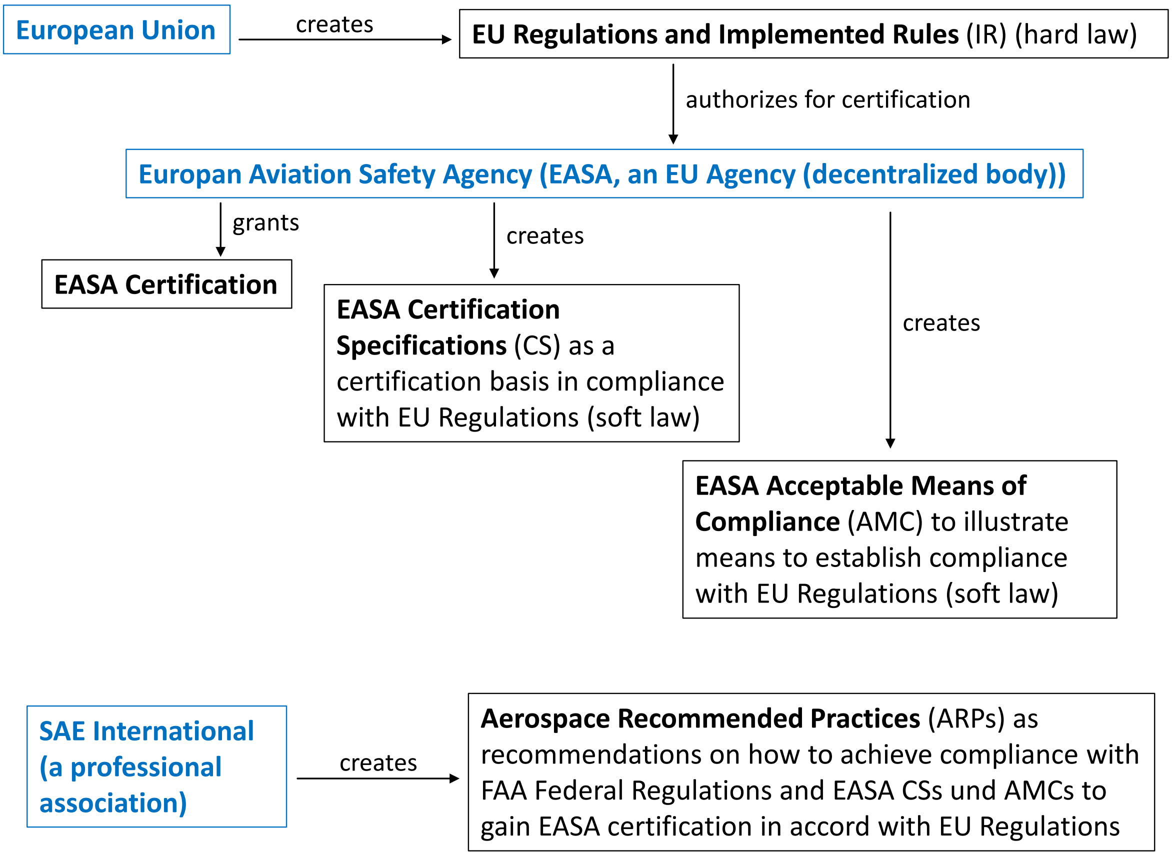

European Union
creates
EU Regulations and Implemented Rules (IR) (hard law)
authorizes for certification
Europan Aviation Safety Agency (EASA, an EU Agency (decentralized body))
grants
EASA Certification
creates
EASA Certification Specifications (CS) as a certification basis in compliance with EU Regulations (soft law)
creates
EASA Acceptable Means of Compliance (AMC) to illustrate means to establish compliance with EU Regulations (soft law)
SAE International (a professional association)
creates
Aerospace Recommended Practices (ARPs) as recommendations on how to achieve compliance with FAA Federal Regulations and EASA CSs und AMCs to gain EASA certification in accord with EU Regulations

Figure 2.1: ARP relations

For the purpose of this comparison important definitions from the ARP4754A are:

"ASSESSMENT: An evaluation based upon engineering judgment."

"COMMON CAUSE: Event or failure which bypasses or invalidates redundancy or independence."

"COMMON MODE FAILURE: An event which affects a number of elements otherwise considered to be independent."

"ERROR: An omitted or incorrect action by a crewmember or maintenance person, or a mistake in requirements, design, or implementation (derived from AMC 25.1309)"

"FAILURE: An occurrence which affects the operation of a component, part or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: errors may cause Failures, but are not considered to be Failures. (AMC 25.1309)"

"FAILURE CONDITION: A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events (AMC 25.1309)"

"FAILURE EFFECT: A description of the operation of a system or item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of a system or an item"

"FAILURE MODE: The way in which the failure of a system or item occurs"

"FUNCTIONAL HAZARD ASSESSMENT [FHA]: A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity."

"ITEM: A hardware or software element having bounded and well-defined interfaces."

"PARTICULAR RISKS: Particular risks are defined as those events or influences which are external to the aircraft or within the aircraft but external to the system(s) and item(s) being analyzed, but which may violate failure independence claims."

"PRELIMINARY SYSTEM SAFETY ASSESSMENT [PSSA]: A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items"

"REQUIREMENT: An identifiable element of a function specification that can be validated and against which an implementation can be verified"

"RISK: The combination of the frequency (probability) of an occurrence and its associated level of severity"

"SAFETY: The state in which risk is acceptable"

"SYSTEM: A combination of inter-related items arranged to perform a specific function(s)"

"SYSTEM SAFETY ASSESSMENT: A systematic, comprehensive evaluation of the implemented system to show that the relevant safety requirements are met"

"VALIDATION: The determination that the requirements for a product are correct and complete. [Are we building the right aircraft/ system/ function/ item?]"

"VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met. [Did we build the aircraft/ system/ function/ item right?]"

"ZONAL SAFETY Analysis: The safety analysis standard with respect to installation, interference between systems, and potential maintenance errors that can affect system safety."

ARP4754A describes the complete aircraft development process, methods and processes in this complete process are in detail explained in related documents as shown in figure 2.2.

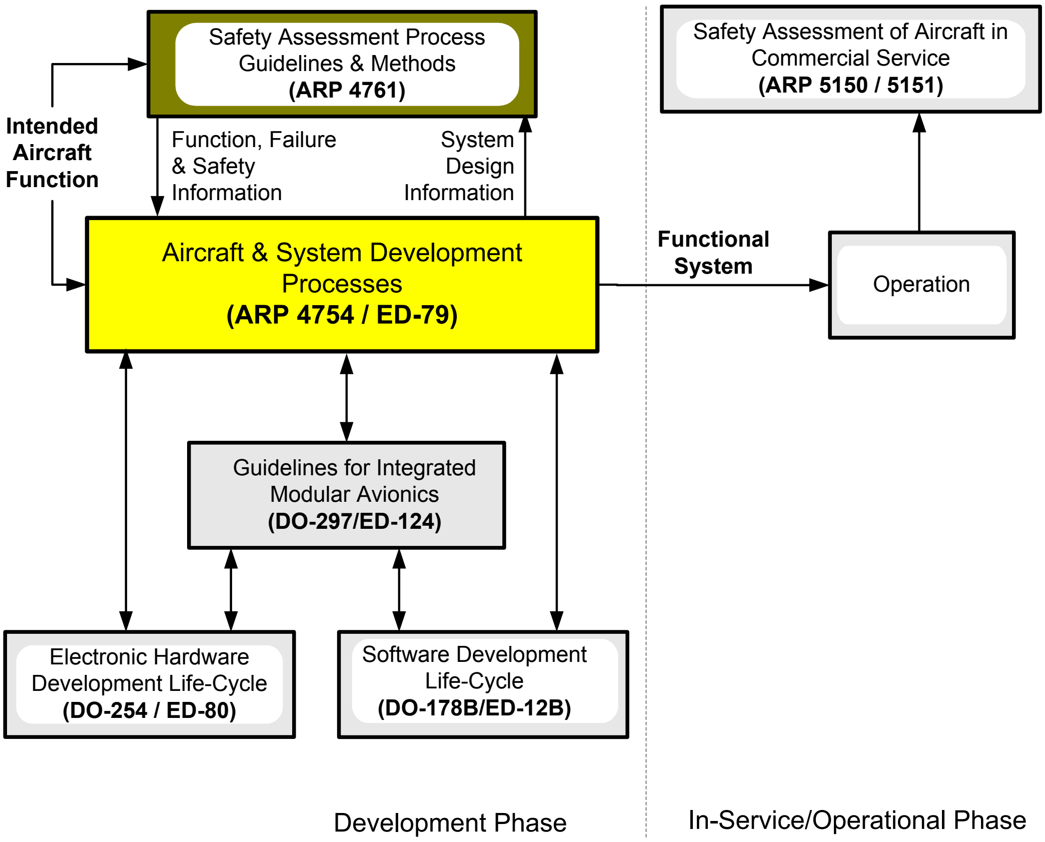

Safety Assessment Process Guidelines & Methods (ARP 4761)
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
Aircraft & System Development Processes (ARP 4754 / ED-79)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Functional System
Operation
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Electronic Hardware Development Life-Cycle (DO-254 / ED-80)
Software Development Life-Cycle (DO-178B/ED-12B)
Development Phase
In-Service/Operational Phase

Figure 2.2: ARP4754A and related documents [4]

Safety in the ARP4754A is defined as events with a defined severity, which means a certain type of loss, only happen with a defined probability. The general idea in the ARP4754A on how to achieve this safety is to use the defined probability for a certain type of loss as a budget, which is divided between all the functions, which, when not provided, could lead to that certain type of loss, such that the aircraft does not exceed the probability for that certain loss. To make sure a component provides a certain function with the defined probability, requirements are generated for the components. The requirements-based safety approach starts the system design and safety requirements generation in a top down manner at the whole aircraft as highest level, going down to single items as the lowest level. The requirements of a lower level are to fulfill and are traceable to the requirements of a higher level. Derived requirements can exist, which are not traceable to a requirement of a higher level, but which are needed to fulfill, support or enable a function. The integration and verification process then starts from this item level again all the way up to aircraft level.

There is little guidance provided on analyzing if the set of requirements actually implements safety, which would mean the requirements are complete such that the probability of providing a function is actually met by the intended design:

"The completeness of a set of requirements by its nature may be difficult to prove. As a basis for performing a completeness check of requirements, it is possible to use the list of possible types of requirements (see 5.3.1). Individuals with a generally stated need for the system may have unstated or unanticipated specific needs and expectations. Completeness is viewed as a probable outcome of following a validation process that may include a combination of templates and checklists, as well as the involvement of actual customers, users, maintainers, certification authorities and developers." [4]

The correctness of the failure probability that is allowed for a certain component depends on the outcome of the failure of this component and the number and interaction of how other components are adding failure probabilities to the corresponding probability budget of the outcome. This correctness is tried to be analyzed by **F**ault **T**ree **A**nalysis (FTA) or similar methods such as **D**ependence **D**iagram (DD) or **M**arkov **A**nalysis (MA) as a top down approach, starting from the unwanted event, and **F**ailure **M**odes and **E**ffects **A**nalysis (FMEA) and **F**ailure **M**odes and **E**ffects **S**ummary (FMES) as a bottom up approach, starting at the item failure:

"After identifying the failure conditions in the FHA, the FTA/DD/MA can be applied as part of the PSSA to determine what single failures or combinations of failures can exist (if any) at the lower levels that might cause each failure condition. When an FMEA/FMES is performed, a comparison should be accomplished to ensure all significant effects identified are in the FTA/DD/MA as Basic Events. The FTA/DD/MA Basic Events get their failure rates from the FMEAs and/or FMESs." [5]

Further, to assign the probability budget correctly, system states where several functions are not being provided through a common cause or through interactions of the functioning as intended components on a lower level, will either have to not exist in the system design or must be assigned with a probability from the overall probability budget. Doing so includes the assumption that all such interactions are known and a probability can be assigned to them. This analysis is called **C**ommon **C**ause **A**nalysis (CCA).

The general system safety assessment of the aircraft as defined above is divided into several parts in the ARP4754A to fit to different development stages. The parts consist of the **F**unctional **H**azard **A**ssessment (FHA), the **P**reliminary **A**ircraft **S**afety **A**ssessment (PASA), the **P**reliminary **S**ystem **S**afety **A**ssessment (PSSA), the **S**ystem **S**afety **A**ssessment (SSA), the **A**ircraft **S**afety **A**ssessment (ASA) and the CCA as shown in figure 2.3. The parts will be described in the following. It can be misleading that the term "System Safety Assessment" is used for one part of the overall system safety assessment of the aircraft.

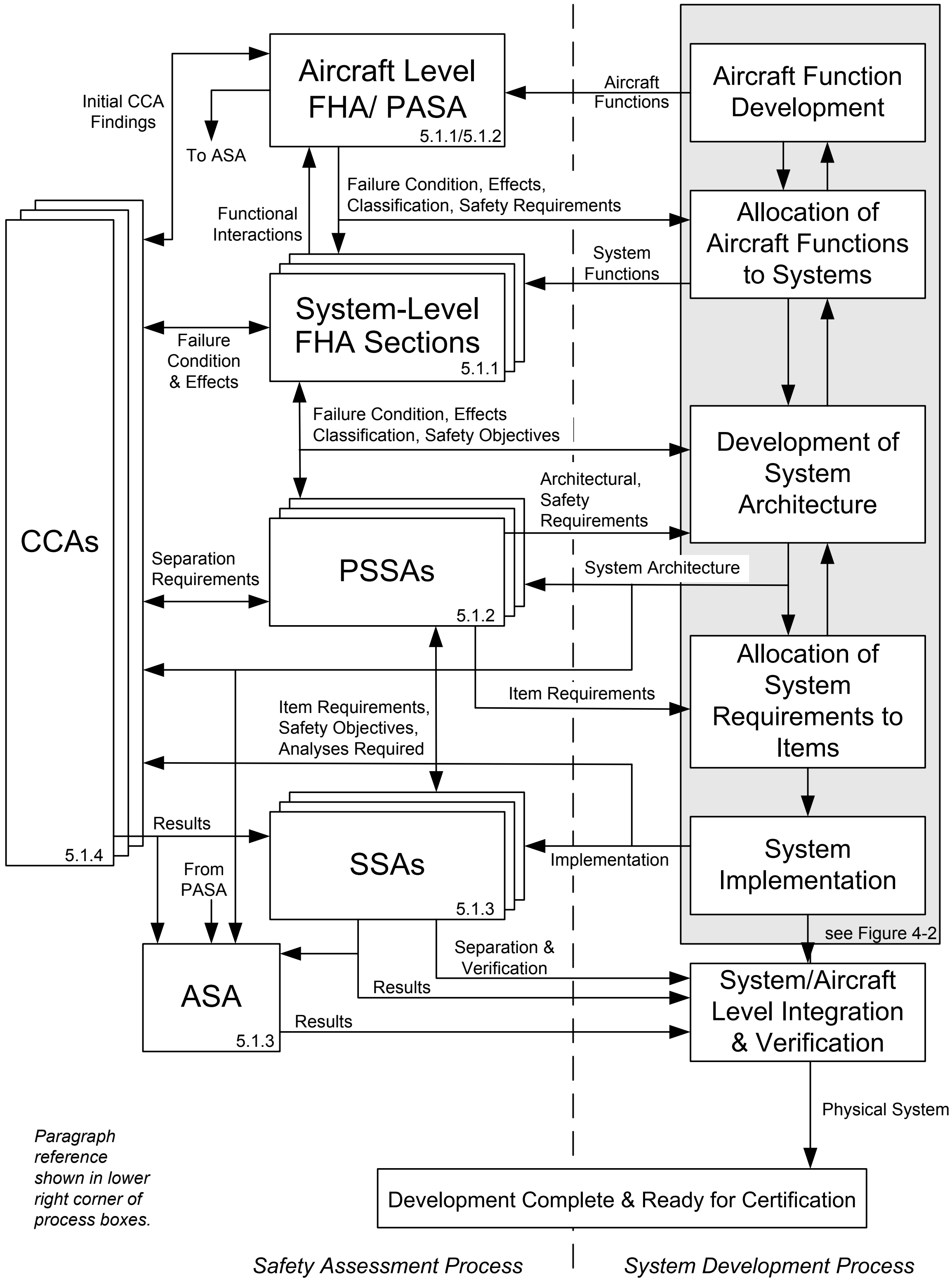


Figure 2.3: ARP4754A safety assessment process [4]

This safety assessment process can be embedded into the aircraft development V-cycle as shown in figure 2.4.

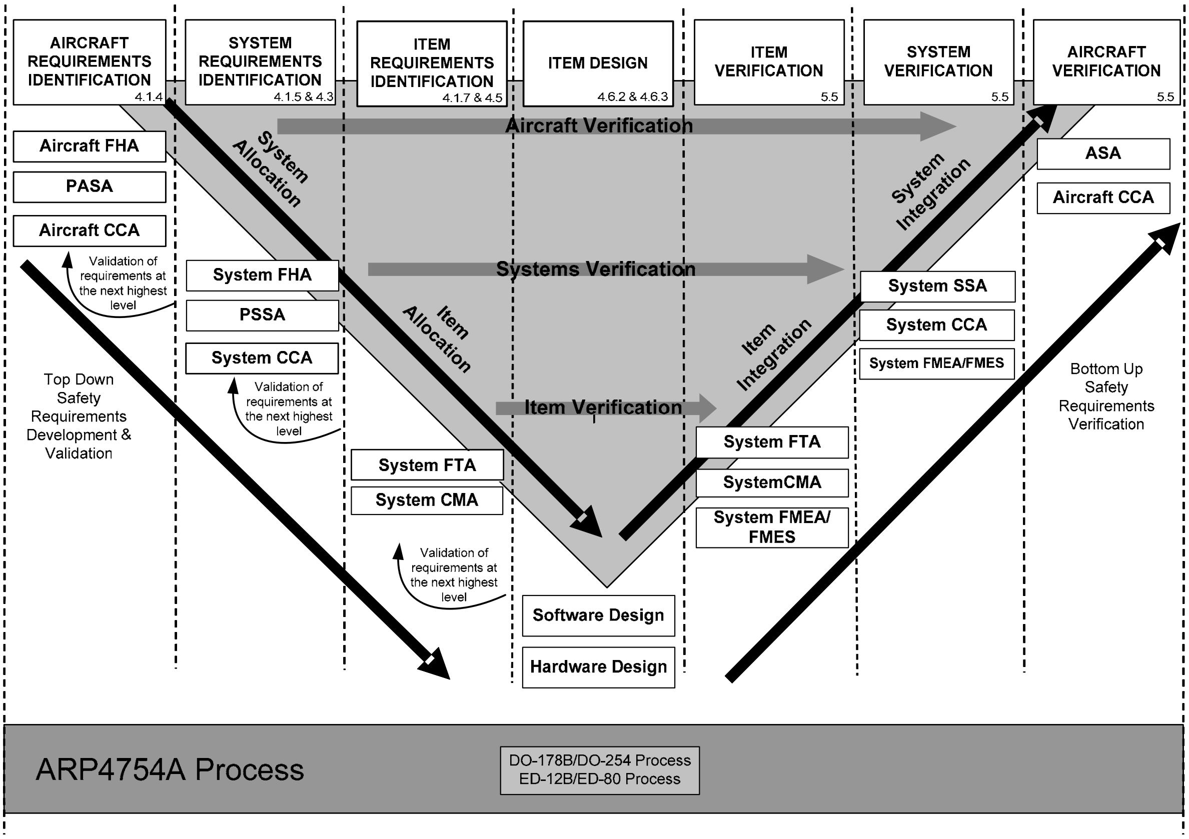


Figure 2.4: Safety assessment process embedded in the development V-cycle [4]

Functional Hazard Assessment (FHA)

The first step in the Arp4754A approach to achieve safety is to collect all aircraft or system functions and analyze what outcome the event of losing this function partly or completely could have. Note that the assumptions here are that all aircraft functions, which are needed to provide safe aircraft operations are known, which here means there are no other functions than the ones mentioned in the FHA, whose loss could lead to any kind of aircraft event and there are no other functions needed to prevent losses. Further it is assumed that the functions are so well designed that no losses can occur when the functions are provided as intended. This assumption is reasonable as long as the functions are easy to analyze on completeness, which means it is reasonable on high abstraction levels, like for example aircraft level. For lower abstraction levels, where more complexity is added, analysis methods like FTA, FMEA, etc. as mentioned above are proposed to use to analyze the completeness of functions and the completeness of knowledge about the outcome if these functions are lost.

The safety Assessments (PASA, PSSA, SSA and ASA)

The definitions of these 4 parts of the overall aircraft safety assessment are:

"Preliminary Aircraft Safety Assessment / Preliminary System Safety Assessment (PASA/PSSA): Establish the aircraft or specific system or item safety requirements and provide a preliminary indication that the anticipated aircraft or system architectures can meet those safety requirements. The PASA and PSSA are updated throughout the system development process ultimately resulting in the Aircraft Safety Assessment and System Safety Assessments." [5]

"Aircraft Safety Assessment / System Safety Assessment (ASA/SSA): Collects, analyzes, and documents verification that the aircraft and systems, as implemented, meet the safety requirements established by the PASA and the PSSA." [5]

The methods used in these assessments are shown in figure 2.5 and are described thereafter.

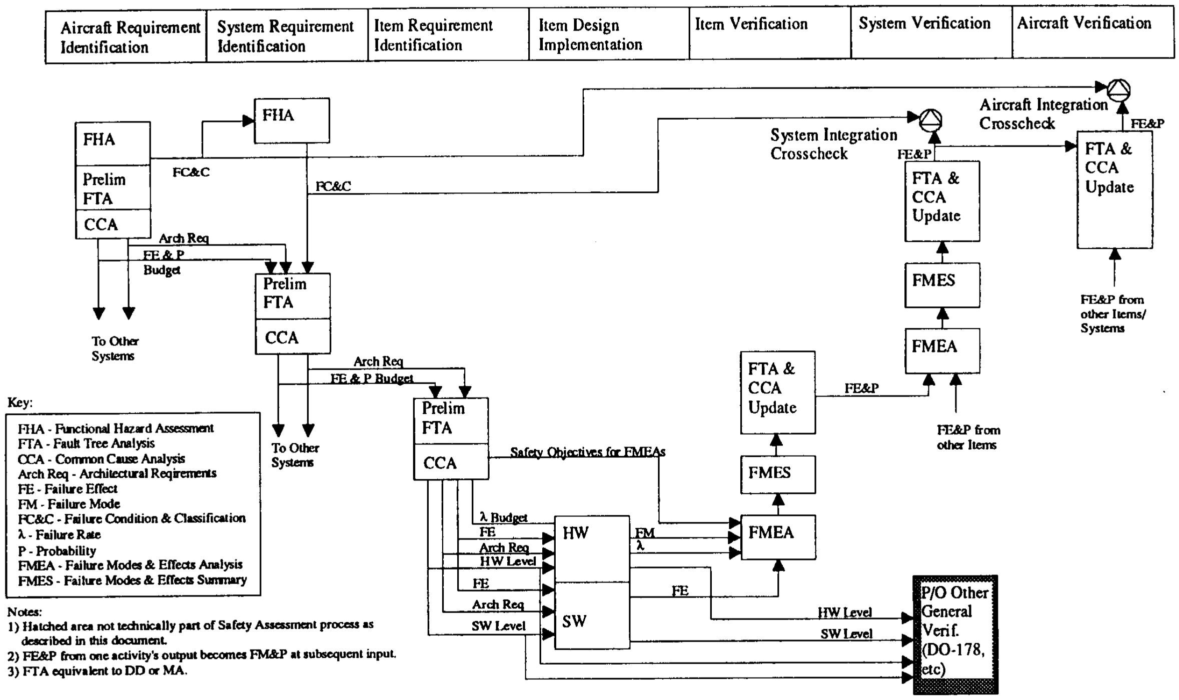

Aircraft Requirement Identification
System Requirement Identification
Item Requirement Identification
Item Design Implementation
Item Verification
System Verification
Aircraft Verification
FHA
Prelim FTA
CCA
FC&C
FHA
FC&C
Arch Req
FE & P Budget
To Other Systems
Prelim FTA
CCA
Arch Req
FE & P Budget
To Other Systems
Prelim FTA
CCA
Safety Objectives for FMEAs
λ Budget
FE
Arch Req
HW Level
FE
Arch Req
SW Level
HW
SW
FM
λ
FE
FMEA
FMES
FTA & CCA Update
FE&P
FMEA
FE&P from other Items
FMES
FTA & CCA Update
FE&P
System Integration Crosscheck
Aircraft Integration Crosscheck
FE&P
FTA & CCA Update
FE&P from other Items/ Systems
HW Level
SW Level
P/O Other General Verif. (DO-178, etc)
Key:
FHA - Functional Hazard Assessment
FTA - Fault Tree Analysis
CCA - Common Cause Analysis
Arch Req - Architectural Reqirements
FE - Failure Effect
FM - Failure Mode
FC&C - Failure Condition & Classification
λ - Failure Rate
P - Probability
FMEA - Failure Modes & Effects Analysis
FMES - Failure Modes & Effects Summary
Notes:
1) Hatched area not technically part of Safety Assessment process as described in this document.
2) FE&P from one activity's output becomes FM&P at subsequent input.
3) FTA equivalent to DD or MA.

Figure 2.5: ARP4761 safety assessment process [5]

Fault Tree Analysis (FTA)

FTA, DD and MA are methods to analyze what failures in a system could lead to an unwanted event. The three methods have similar underlying principles, so for the comparison of all three methods to STPA it is sufficient to only describe FTA here. "Note that wherever FTA is shown it can be replaced by an equivalent analysis method such as DD or MA." [5]

FTA is a top down failure analysis method, which uses Boolean logic to determine what failures or combination of failures could lead to an unwanted top event. The fault tree model uses chain causality to describe the causes of events as a chain of failures. To model this chain causality for the top event no extra model of the system is created to provide guidance for detecting failures or combinations of failures, which could lead to a certain event. FTA can be used as a qualitative or, if the failures are assigned with a probability, a quantitative approach. The quantitative result only actually represents the probability of the event happening, if the failures are random events and don't have common causes, which are left out of the calculation. To reduce this uncertainty a CCA is proposed to be performed as described below. Further, only failures are analyzed which could lead to a top event, not if functions or the interactions of functions are being insufficient of preventing a top level event, which would mean the requirements are insufficient.

The 4 proposed FTA steps are:

"1. State the undesired top level event (and its probability of failure objective or failure rate objective if applicable) in a clear, concise statement.

2. Develop the upper and intermediate tiers of the fault tree, determine the intermediate failures and combinations which are minimum, immediate, necessary, and sufficient to cause the top level event to occur and interconnect them by the appropriate fault tree logic symbols. Extend each fault event to the next lower level.

3. Develop each fault event down through successively more detailed levels of the system design until the root causes are established or until further development is deemed unnecessary.

4. Establish probability of failure budgets or failure rate budgets, evaluate the ability of the system to comply with the safety objectives, and redesign the system if deemed necessary (PSSA process)." [5]

Figure 2.6 shows the meaning of the symbols used to create the fault tree and so model the failure chain leading to an unwanted event.

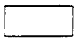
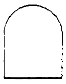
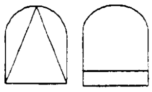
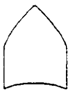
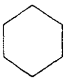
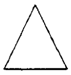
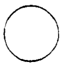
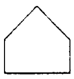
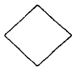
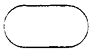
Symbol	Name	Definition
	Description Box	Description of an output of a logic symbol or of an event
	AND-Gate	Boolean Logic gate - event can occur when all the next lower conditions are true
	Priority AND-Gate	Boolean Logic gate - event can occur when all the next lower conditions occur in a specific sequence (sequence is usually represented by a conditional event)
	OR-Gate	Boolean Logic gate - event can occur if any one or more of the next lower conditions are true
	Inhibit	Output fault occurs if the (single) input fault occurs in the presence of an enabling conditional event.
	Transfer	Indicates transfer of information
	Basic Event	Event which is internal to the system under analysis, requires no further development
	House	Event which is external to the system under analysis, it will or will not happen (Pf=1 or Pf=0)
	Undeveloped Event	Event which is not developed further because it has little impact on the top level event or because the details necessary for further event development are not readily available
	Conditional Event	A condition which is necessary for a failure mode to occur

Figure 2.6: FTA symbols [5]

An example of such a fault tree is shown in figure 2.7.

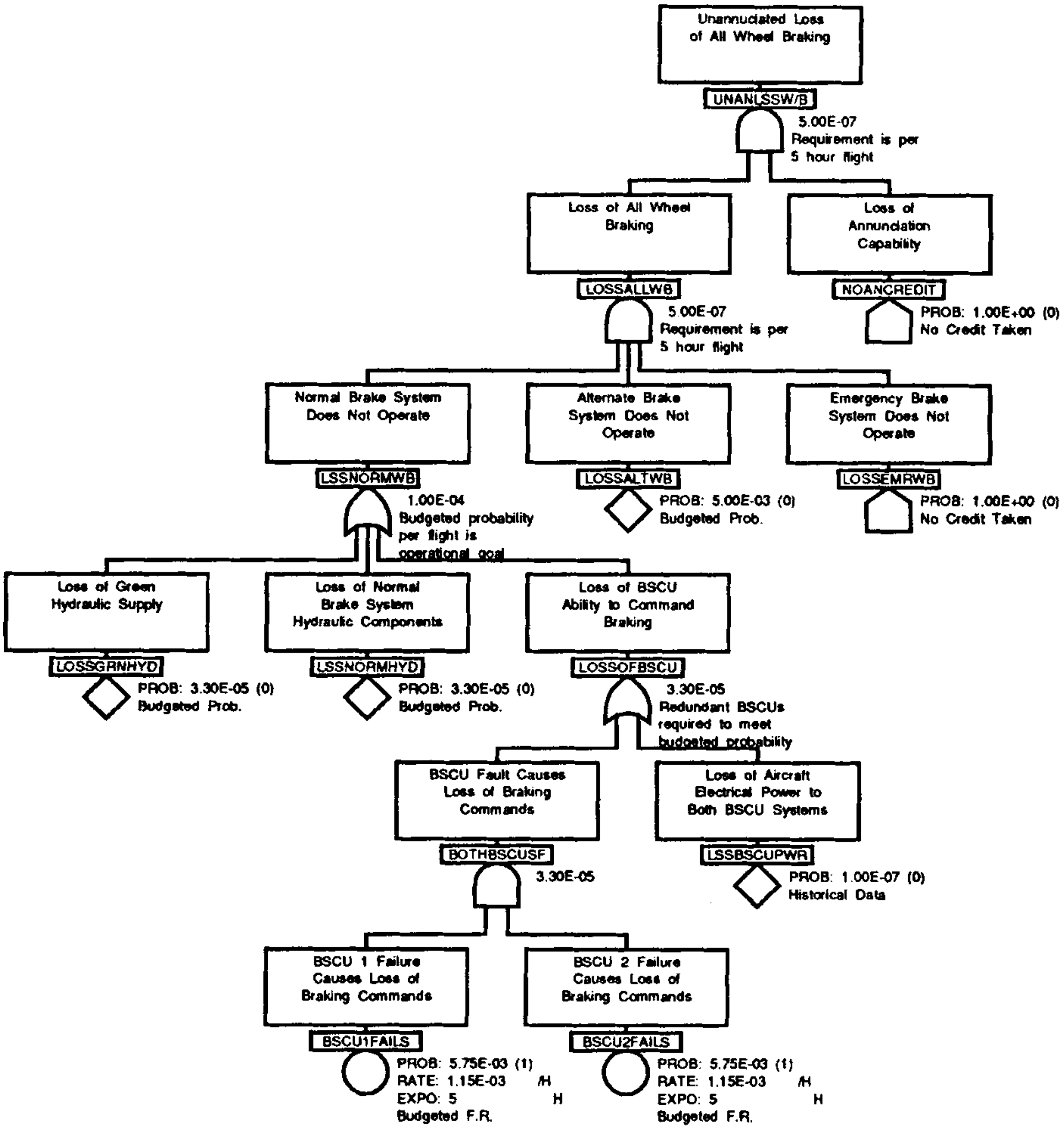
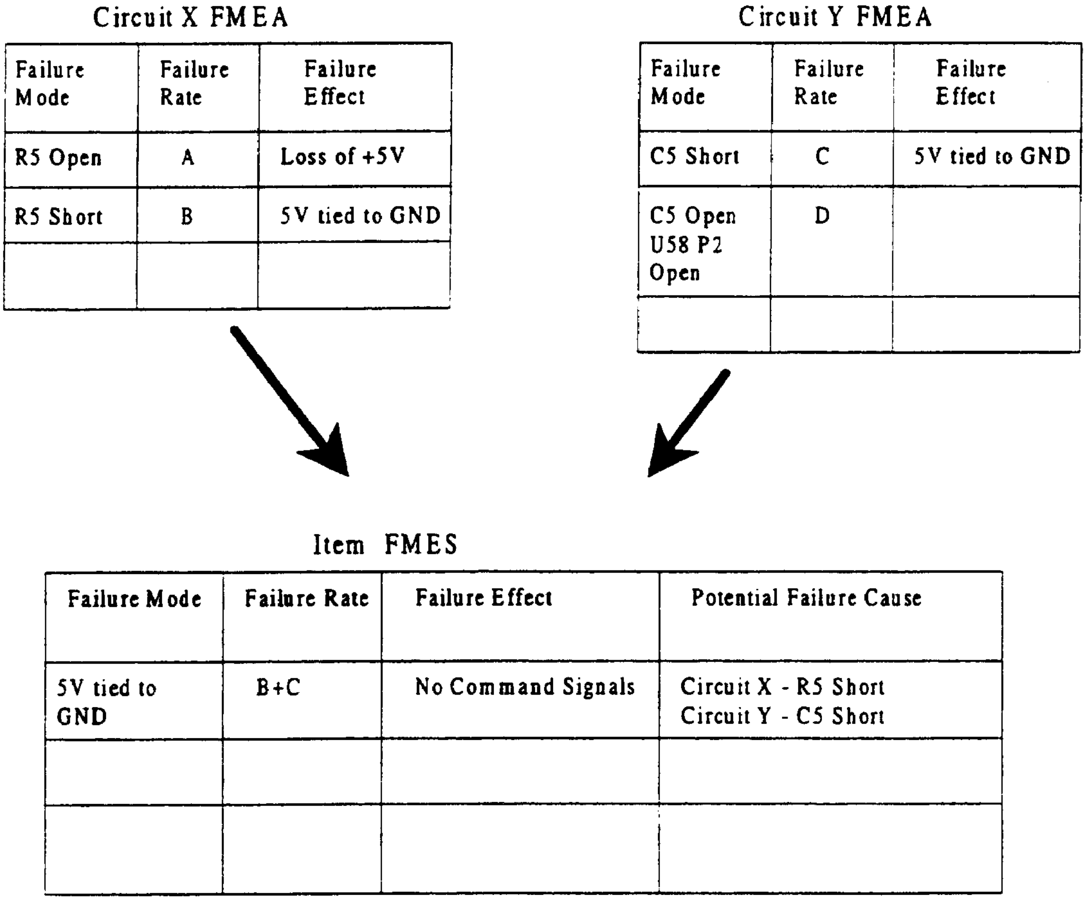

Unannuciated Loss of All Wheel Braking
UNANLSSW/B
5.00E-07 Requirement is per 5 hour flight
Loss of All Wheel Braking
Loss of Annunciation Capability
LOSSALLWB
5.00E-07 Requirement is per 5 hour flight
NOANCREDIT
PROB: 1.00E+00 (0) No Credit Taken
Normal Brake System Does Not Operate
Alternate Brake System Does Not Operate
Emergency Brake System Does Not Operate
LSSNORMWB
1.00E-04 Budgeted probability per flight is operational goal
LOSSALTWB
PROB: 5.00E-03 (0) Budgeted Prob.
LOSSEMRWB
PROB: 1.00E+00 (0) No Credit Taken
Loss of Green Hydraulic Supply
Loss of Normal Brake System Hydraulic Components
Loss of BSCU Ability to Command Braking
LOSSGRNHYD
PROB: 3.30E-05 (0) Budgeted Prob.
LSSNORMHYD
PROB: 3.30E-05 (0) Budgeted Prob.
LOSSOFBSCU
3.30E-05 Redundant BSCUs required to meet budgeted probability
BSCU Fault Causes Loss of Braking Commands
Loss of Aircraft Electrical Power to Both BSCU Systems
BOTHBSCUSF
3.30E-05
LSSBSCUPWR
PROB: 1.00E-07 (0) Historical Data
BSCU 1 Failure Causes Loss of Braking Commands
BSCU 2 Failure Causes Loss of Braking Commands
BSCU1FAILS
PROB: 5.75E-03 (1) RATE: 1.15E-03 /H EXPO: 5 H Budgeted F.R.
BSCU2FAILS
PROB: 5.75E-03 (1) RATE: 1.15E-03 /H EXPO: 5 H Budgeted F.R.

Figure 2.7: A fault tree example [5]

Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Summary (FMES)

FMEA is a bottom-up method to analyze what outcome a failure of an item, component etc. on a certain level, can have on the next higher level. FMEA is usually used on the existing design to verify a proposed architecture and to support the top down analysis methods. FMES is then used to verify the architectures failure probability for a certain event by grouping all similar effects from the FMEA results and so adding all the failure probabilities for that event as shown in figure 2.8



Circuit X FMEA

Failure Mode	Failure Rate	Failure Effect
R5 Open	A	Loss of +5V
R5 Short	B	5V tied to GND

Circuit Y FMEA

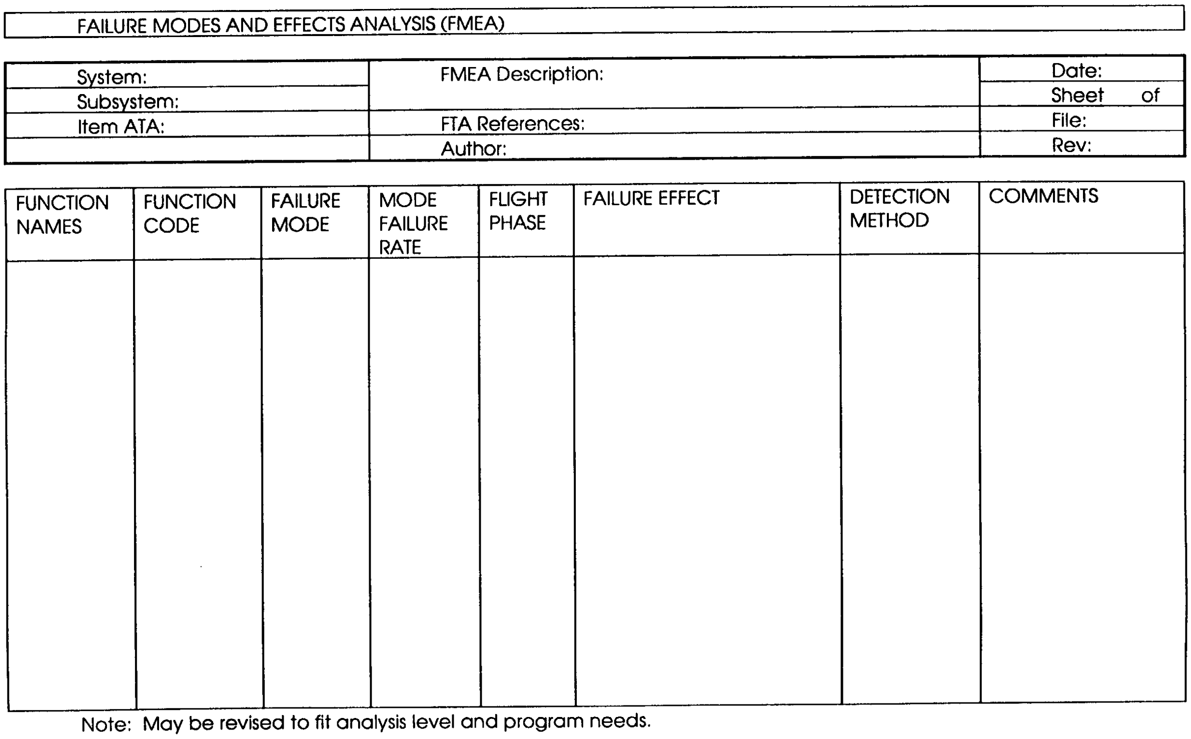
Failure Mode	Failure Rate	Failure Effect
C5 Short	C	5V tied to GND
C5 Open U58 P2 Open	D	

Item FMES

Failure Mode	Failure Rate	Failure Effect	Potential Failure Cause
5V tied to GND	B+C	No Command Signals	Circuit X - R5 Short Circuit Y - C5 Short

Figure 2.8: Relation between FMEA and FMES [5]

Similar to FTA, FMEA uses chain causality to connect the failures and its effects from the lowest item level to aircraft level as a chain of failures and effects. No extra model of the functionality of the aircraft system is created to provide guidance for the safety engineer. The safety engineer has to rely on their understanding of the system and the design documents provided. Templates as shown in figure 2.9 are used to document the FMEA and FMES results. It is only analyzed what happens if the requirements are not fulfilled, which means a function is not provided or not provided as described by the requirements due to a certain failure. It is not analyzed if the requirements are correct and complete, which means the functions, when provided as described in the requirements, are sufficient to prevent top level events and there are no interactions of functioning as intended components, which could lead to a top level event. To create certainty about the independence of the failures, and so the correctness of the quantitative FMES results, a CCA has to be performed additionally.



FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

System:	FMEA Description:	Date:
Subsystem:		Sheet of
Item ATA:	FTA References:	File:
	Author:	Rev:

FUNCTION NAMES	FUNCTION CODE	FAILURE MODE	MODE FAILURE RATE	FLIGHT PHASE	FAILURE EFFECT	DETECTION METHOD	COMMENTS

Note: May be revised to fit analysis level and program needs.

Figure 2.9: FMEA template [5]

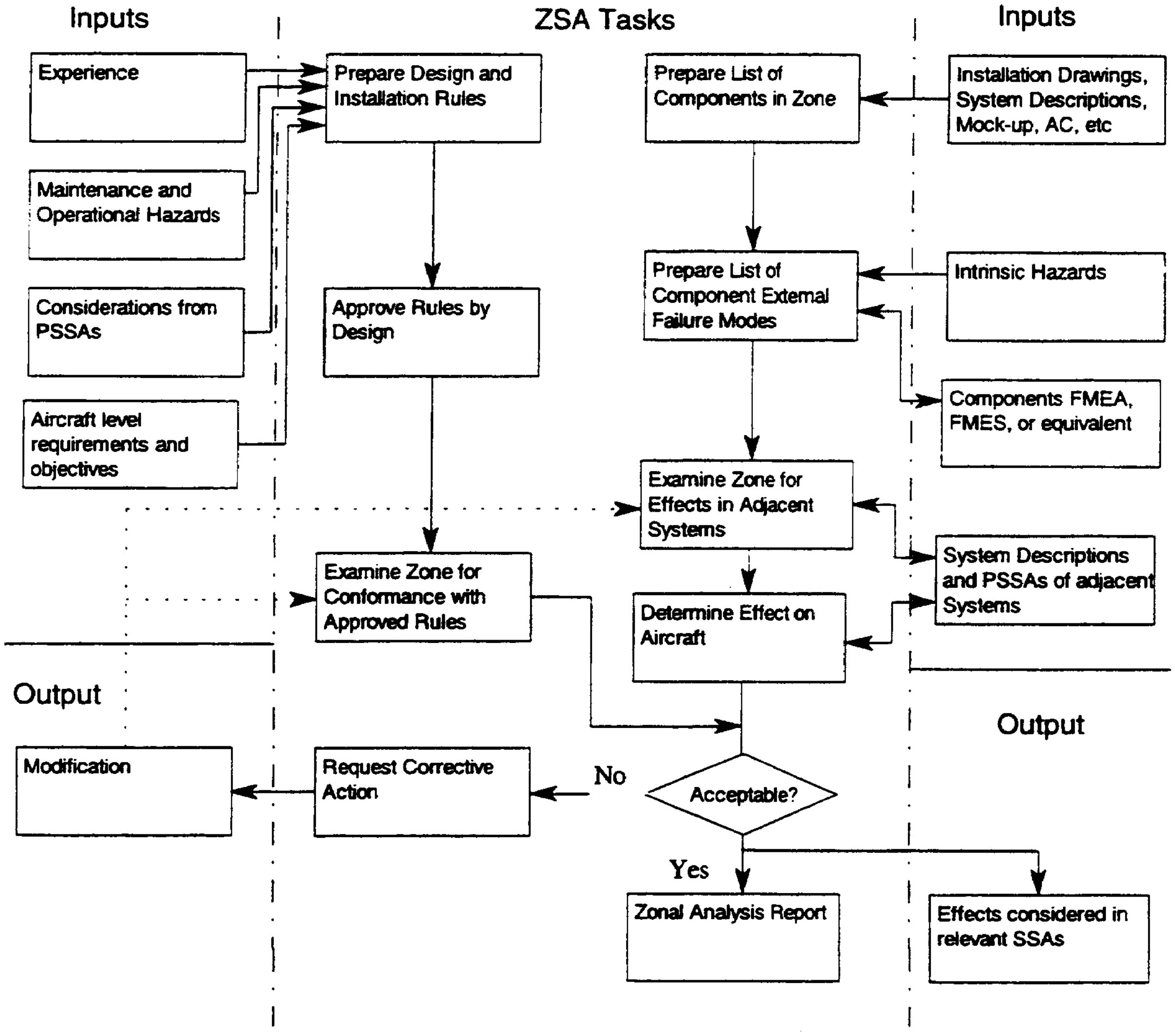
Common Cause Analysis (CCA)

CCA is the method of analyzing the independence of failures, which is required for the correctness of the assumptions of the top-down and bottom-up safety analysis methods as described above. Further it is supposed to analyze the "goodness" of the design, which means if the requirements and the implementation of these requirements in the design and the actual hardware are sufficient to provide the intended aircraft functions. CCA consists of three parts: **Z**onal **S**afety **A**nalysis (ZSA), **P**articular **R**isks **A**nalysis (CCA) and **C**ommon **M**ode **A**nalysis (CMA).

Zonal Safety Analysis (ZSA)

ZSA is qualitative analysis method to detect common failures through location of physical implementation. Possible failures through installation, physical local interference and maintenance errors shall be detected. The aircraft is partitioned into zones, the zones are then analyzed as shown in figure 2.10. No additional model other than the aircraft zones is created to provide guidance for the safety engineer.

Note that ZSA uses inputs from FMEA and so has the same weaknesses as FMEA as mentioned above. It only analyzes possible failures, which could occur through the 3 causes: installation, interference and maintenance. It does not analyze how local physical implementation could install needs for requirement change. This means a component could provide a function in way that still meets the requirements, so no failure exists, but through the local physical implementation the function is modified in a way that is insufficient for functions on a higher level, so through the physical local implementation the requirement is no longer correct.



Inputs
ZSA Tasks
Inputs
Experience
Maintenance and Operational Hazards
Considerations from PSSAs
Aircraft level requirements and objectives
Prepare Design and Installation Rules
Approve Rules by Design
Examine Zone for Conformance with Approved Rules
Prepare List of Components in Zone
Prepare List of Component External Failure Modes
Examine Zone for Effects in Adjacent Systems
Determine Effect on Aircraft
Installation Drawings, System Descriptions, Mock-up, AC, etc
Intrinsic Hazards
Components FMEA, FMES, or equivalent
System Descriptions and PSSAs of adjacent Systems
Output
Output
Modification
Request Corrective Action
No
Acceptable?
Yes
Zonal Analysis Report
Effects considered in relevant SSAs

Figure 2.10: ZSA overview [5]

Particular Risks Analysis (PRA)

PRA is a qualitative analysis method for particular events, which can be or lead to common causes for failures extending single aircraft zones. Examples of such events are fire, leaking fluids, lightning and so on. Only failures caused by such events are investigated, not sufficiency of requirements apart from failures as described above. The SAE International **A**erospace **R**ecommended **P**ractice 4761 (ARP4761) proposes the following steps for PRA:

"a. Define the details of the particular risk to be analyzed. (e.g., tire/wheel burst)

b. Define the failure model to be used for the analysis. (e.g., tire burst model and wheel burst model)

c. List the requirements to be fulfilled. (e.g., FAR/JAR 729(f))

d. Define the affected zones/areas. (e.g., landing gear bays)

e. Define the affected systems/items. (cross-check with ZSA)

f. Define the design and installation precautions taken. (cross-check with design and installation guidelines used in the ZSA)

g. Review the consequences of the particular risk on the affected items. (cross-check with FMEA/PSSAs)

h. Review the effect of the particular risk on the aircraft due to failure modes of items or their combinations. (cross-check with SSAs)" [5]

The failure model outlined in step b. is not an additional model of the architecture, but consists of a collection of possible outcomes by engineering judgements and similar prior occurences, so it is more of a lessons learned document than significant additional guidance to analyse the design: "In order to have a standardized set of conditions for the evaluation of the consequences of tire failures a failure model has been derived from a study of occurrence reports and previous practice adopted for certification of previous aircraft." [4]

Common Mode Analysis (CMA)

ARP4761 states CMA as the analysis of the "goodness" of the design in a "logical way" using "design experience". CMA seeks qualitative evaluation that technical implementation (design, manufacturing, maintenance) provides independence of failures. No additional model of the functionality of the aircraft system or subsystems are created, the analysis is based on design experience and design documents, checklists of things to look at are proposed as guidance. "Project specific CMA checklists should be derived based on the example data and previous experience (common knowledge or experience in similar aircraft). The level of detail of these checklists depends upon the degree of complexity or novelty of the technology or system under study." [5] To provide guidance to create such checklists, general checklists are provided as shown in figure 2.12. The CMA steps are shown in figure 2.11.

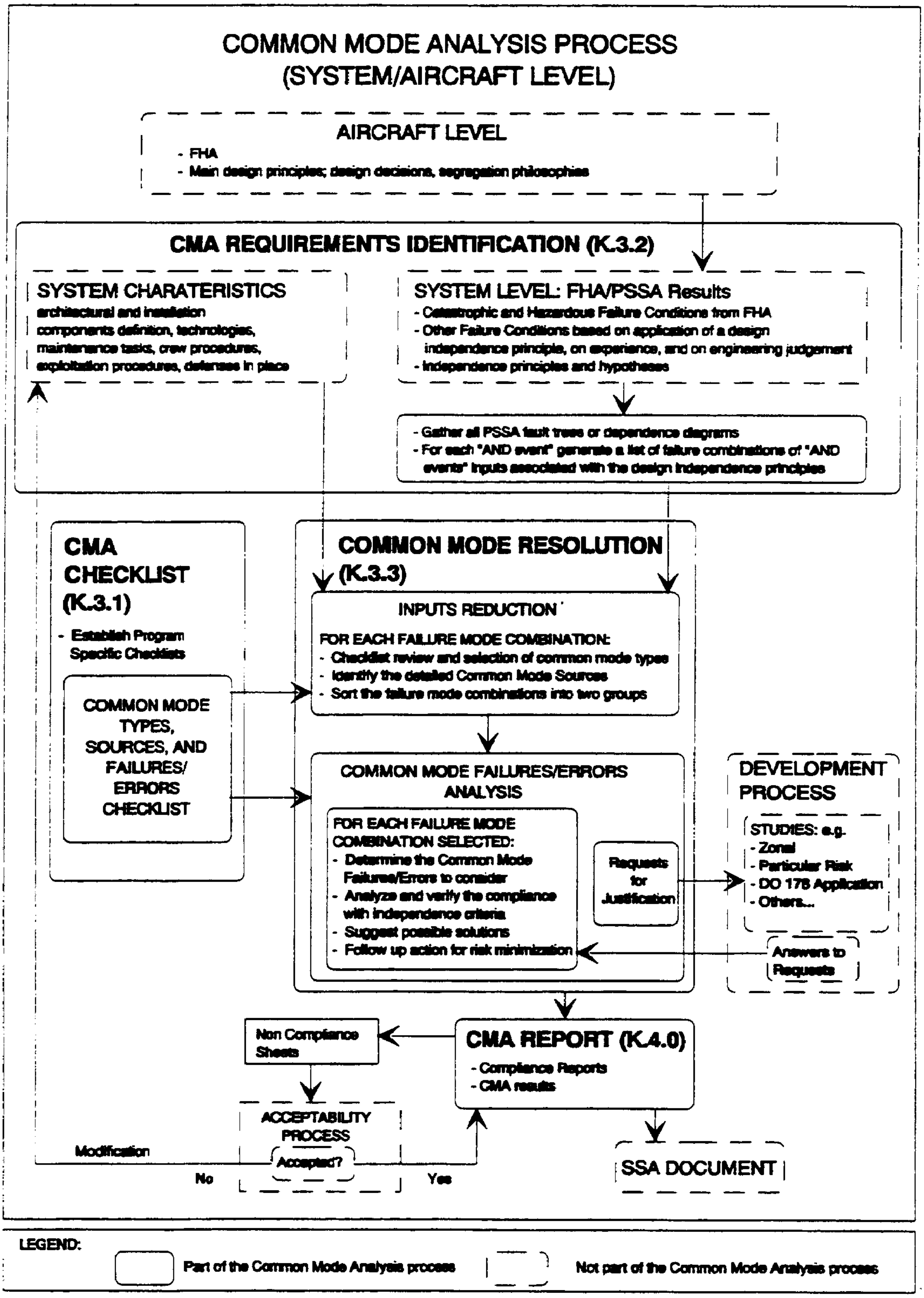
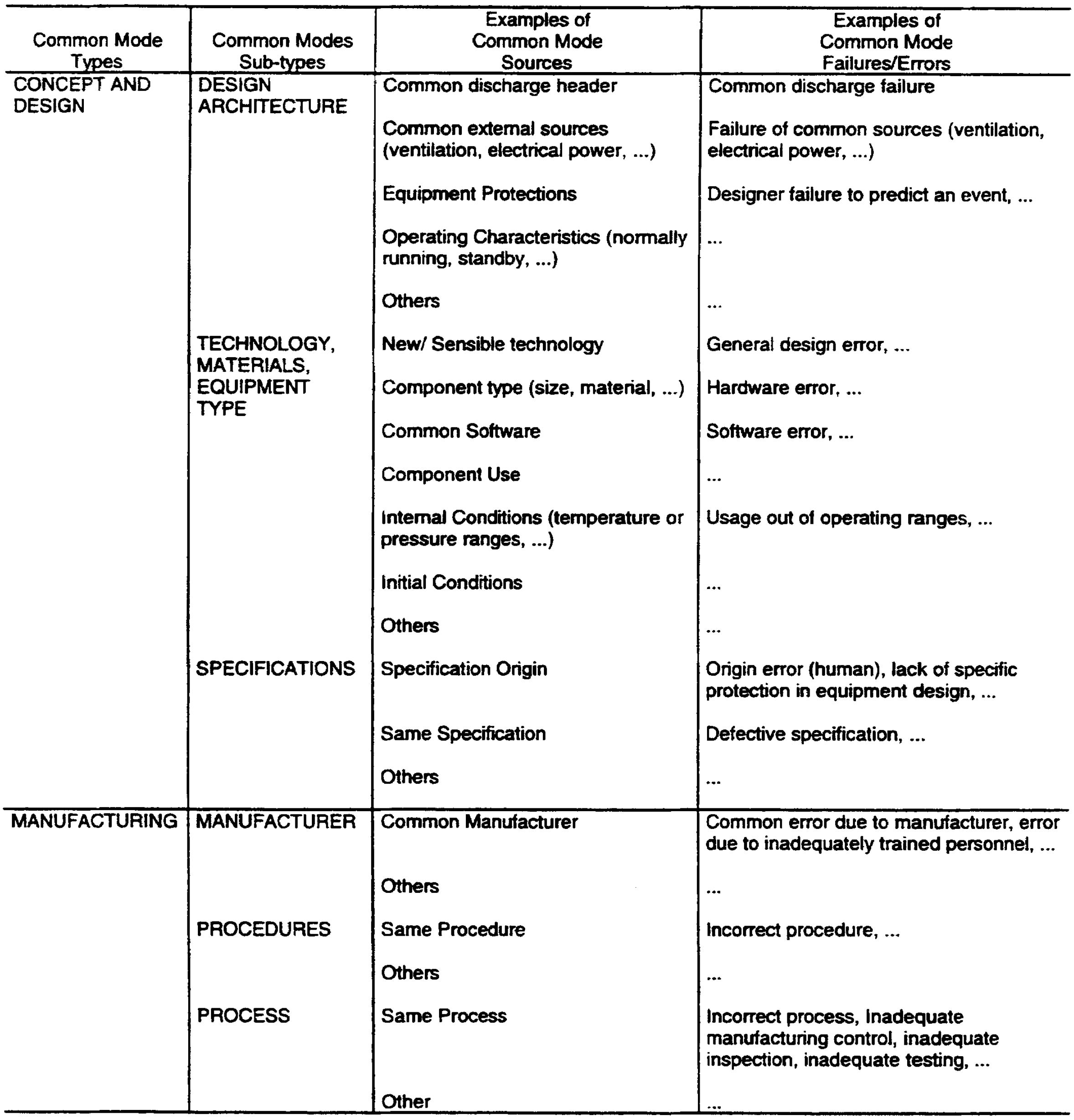

COMMON MODE ANALYSIS PROCESS
(SYSTEM/AIRCRAFT LEVEL)
AIRCRAFT LEVEL
- FHA
- Main design principles; design decisions, segregation philosophies
CMA REQUIREMENTS IDENTIFICATION (K.3.2)
SYSTEM CHARATERISTICS
architectural and installation
components definition, technologies,
maintenance tasks, crew procedures,
exploitation procedures, defenses in place
SYSTEM LEVEL: FHA/PSSA Results
- Catastrophic and Hazardous Failure Conditions from FHA
- Other Failure Conditions based on application of a design independence principle, on experience, and on engineering judgement
- Independence principles and hypotheses
- Gather all PSSA fault trees or dependence diagrams
- For each "AND event" generate a list of failure combinations of "AND events" inputs associated with the design independence principles
CMA CHECKLIST (K.3.1)
- Establish Program Specific Checklists
COMMON MODE TYPES, SOURCES, AND FAILURES/ ERRORS CHECKLIST
COMMON MODE RESOLUTION (K.3.3)
INPUTS REDUCTION
FOR EACH FAILURE MODE COMBINATION:
- Checklist review and selection of common mode types
- Identify the detailed Common Mode Sources
- Sort the failure mode combinations into two groups
COMMON MODE FAILURES/ERRORS ANALYSIS
FOR EACH FAILURE MODE COMBINATION SELECTED:
- Determine the Common Mode Failures/Errors to consider
- Analyze and verify the compliance with independence criteria
- Suggest possible solutions
- Follow up action for risk minimization
Requests for Justification
DEVELOPMENT PROCESS
STUDIES: e.g.
- Zonal
- Particular Risk
- DO 178 Application
- Others...
Answers to Requests
CMA REPORT (K.4.0)
- Compliance Reports
- CMA results
Non Compliance Sheets
ACCEPTABILITY PROCESS
Accepted?
Modification
No
Yes
SSA DOCUMENT
LEGEND:
Part of the Common Mode Analysis process
Not part of the Common Mode Analysis process

Figure 2.11: CMA overview [5]



Common Mode Types	Common Modes Sub-types	Examples of Common Mode Sources	Examples of Common Mode Failures/Errors
CONCEPT AND DESIGN	DESIGN ARCHITECTURE	Common discharge header	Common discharge failure
		Common external sources (ventilation, electrical power, ...)	Failure of common sources (ventilation, electrical power, ...)
		Equipment Protections	Designer failure to predict an event, ...
		Operating Characteristics (normally running, standby, ...)	...
		Others	...
	TECHNOLOGY, MATERIALS, EQUIPMENT TYPE	New/ Sensible technology	General design error, ...
		Component type (size, material, ...)	Hardware error, ...
		Common Software	Software error, ...
		Component Use	...
		Internal Conditions (temperature or pressure ranges, ...)	Usage out of operating ranges, ...
		Initial Conditions	...
		Others	...
	SPECIFICATIONS	Specification Origin	Origin error (human), lack of specific protection in equipment design, ...
		Same Specification	Defective specification, ...
		Others	...
MANUFACTURING	MANUFACTURER	Common Manufacturer	Common error due to manufacturer, error due to inadequately trained personnel, ...
		Others	...
	PROCEDURES	Same Procedure	Incorrect procedure, ...
		Others	...
	PROCESS	Same Process	Incorrect process, Inadequate manufacturing control, inadequate inspection, inadequate testing, ...
		Other	...

Figure 2.12: Example of a general CMA checklist [5]

3 Introduction to the Systems-Theoretic Accident Model and Processes (STAMP) Causality Theory

In chapter 3 an introduction to STAMP is given, STPA will be explained in chapter 3.1 and an STPA extension for modeling human controllers more effectively will described in chapter 3.2.

STAMP is an accident causality theory developed by Nancy Leveson, Professor of Aeronautics and Astronautics and Professor of Engineering Systems at the Massachusetts Institute of Technology (MIT), as a result of her perception of the technical revolution from analog to analog/digital systems not being followed by an adequate revolution of safety engineering techniques. Leveson's accident causality research resulted in a criticism of the sole use of traditional accident models and the corresponding analysis methods (like FTA, FMEA and so on) on modern systems, as they were not sufficient to prevent the investigated modern accidents. Leveson's findings support that modern accidents majorly do not result from component failures, but from unanticipated unsafe interactions between functioning as intended components herein called component interaction failures. The unanticipated unsafe interactions between components lead to system design errors displayed in flawed requirements and "human errors", which are then solely a result of improper system design for human operators. The reason for this shift in accident causality is an increased system complexity as a result of the increasing number of functions and interactions in the system enabled through the implementation of functions in software, instead of in electromechanical hardware. This increased system complexity leads to a mental unmanageability of the system interactions for engineers. Traditional analysis methods were developed for electromechanical systems and don't support the mental manageability of interactions well (see chapter 4). They are based on chain causality models, which is weak in showing component interactions. Leveson finds that complex systems are modeled most favorable for safety engineering by using systems theory and control theory.

In the main STAMP work "Engineering a safer world" [6], Leveson explains with 9 arguments why new and different safety engineering approaches are needed. The 9 arguments are:

Reduced ability to learn from experience: The immensely reduced time to market (from 30 to 2-3 years for basic technical discoveries) reduces the ability of testing systems adequately.

Changing nature of accidents: Modern accidents majorly result from component interaction failures rather than from component failures.

Fast pace of technological change: Technology changes faster than traditional engineering techniques can respond to the unknowns of the new technology.

New types of hazards: New types of man-made hazards like chemicals in food, antibiotic resistant bacteria, pharmaceutical products and so on are emerging.

Increasing complexity and coupling: Modern systems are beyond mental manageability for humans.

Decreasing tolerance for single accidents: Losses from single accidents are increasing, a single aircraft accident can financially ruin companies, financial system meltdowns can affect the world's economy, a fly fix fly approach is no longer possible.

Difficulty in selecting priorities and making trade offs: Companies are operating in aggressive financial environments, asking for less accident tolerance, while simultaneously asking for more performance leads to tighter cost/schedule/safety trade-offs.

More complex relationships between humans and automation: More system functions and increased system automation lifts humans up into higher levels of decision making. While the automation carries decisions out, the human is more of a system manager, which creates new types of error: mode confusion, new inadequate human machine interactions and so on.

Changing regulatory and public views of safety: With increasing usage and interrelations of technology, individuals can't control their own risks, which is shifting the responsibility to government bodies, which must trade of tight regulations against companies' financial pressures.

The old and new assumptions of safety engineering Leveson identifies in "Engineering a safer world" [6] are:

"Assumption 1: Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur."

"New Assumption 1: High reliability is neither necessary nor sufficient for safety."

"Assumption 2: Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chain of events leading to the loss."

"New Assumption 2: Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately."

"Assumption 3: Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information."

"New Assumption 3: Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis."

"Assumption 4: Most accidents are caused by operator error. Rewarding safe behavior and punishing unsafe behavior will eliminate or reduce accidents significantly."

"New Assumption 4: Operator behavior is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works."

"Assumption 5: Highly reliable software is safe."

"New Assumption 5: Highly reliable software is not necessarily safe. Increasing software reliability or reducing implementation errors will have little impact on safety."

"Assumption 6: Major accidents occur from the chance simultaneous occurrence of random events."

"New Assumption 6: Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk."

"Assumption 7: Assigning blame is necessary to learn from and prevent accidents or incidents."

"New Assumption 7: Blame is the enemy of safety. Focus should be on understanding how the system behavior as a whole contributed to the loss and not on who or what to blame for it."

The three therefrom emerging new pillars for safety engineering and of STAMP are:

1. The most basic concept in safety engineering is a constraint, not an event. Events, and so accidents, then only occur when safety constraints have not been enforced successfully.

2. Hierarchical control structures as known from system theory are used to model systems. Processes on higher levels control processes on lower levels using feedback from the controlled processes as shown in figure 3.1.

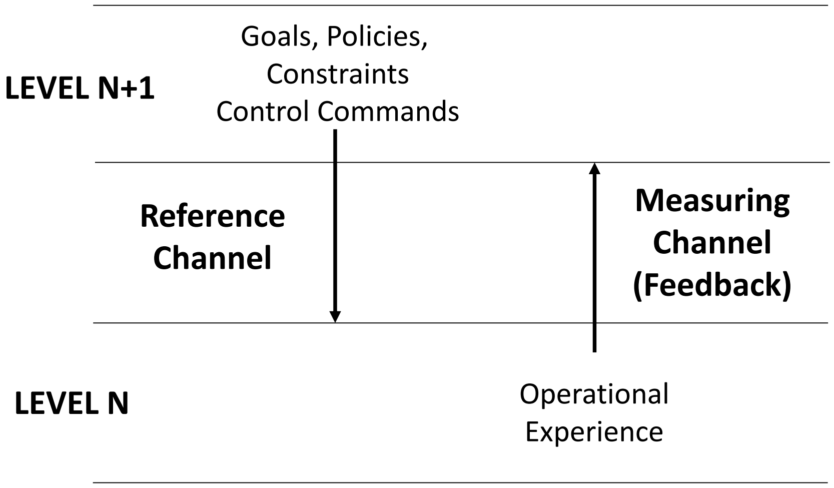


Figure 3.1: Control levels and communication channels [6]

3. Process models, of the human controller, which are the human controller's beliefs about the process, or embedded in software or electromechanical structures of automated controllers, are defining the enforced constraints.

STAMP as a new accident causality theory based on these three pillars has now a foundation of systems thinking and systems theory instead of reliability engineering and treats safety as an emerging system property and a control problem, rather than a failure problem. Systems herein are interrelated dynamic processes in a state of dynamic equilibrium. Safety, as the freedom of losses, is then achieved by continuously and successfully enforcing constraints on the system state through designing and maintaining a functioning safety control structure including the corresponding process models. Accidents herein are complex, dynamic processes, which involve the complete sociotechnical system, which was not able to create appropriate control action enforcement. With the reasons for the inadequate enforcement ranging from component failures, system and software design errors and erroneous human decision making to company culture and societal or political influences. Based on the STAMP causality theory several engineering methods have been derived as shown in figure 3.2.

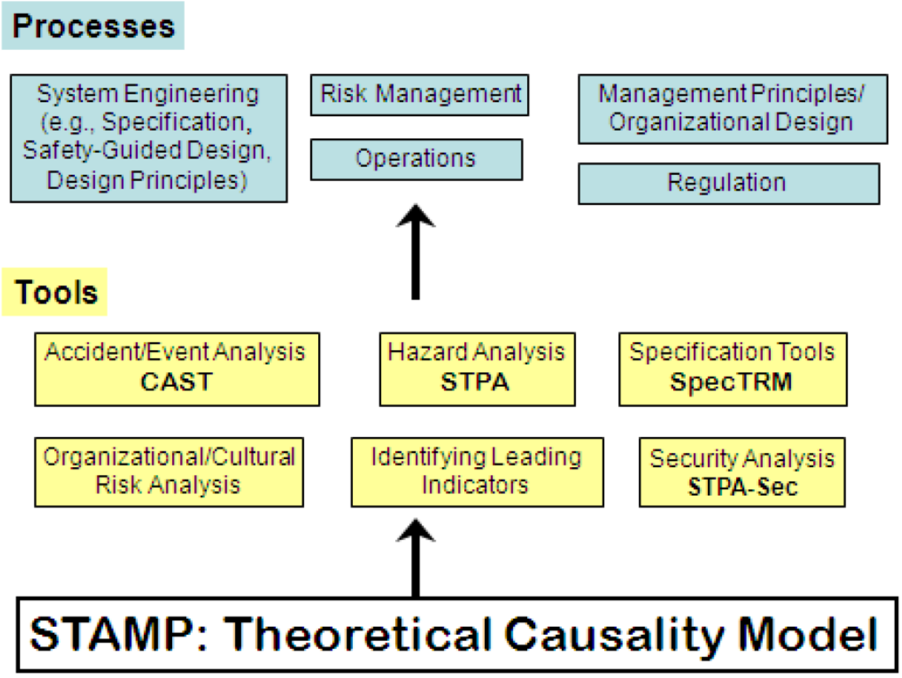

Processes
System Engineering (e.g., Specification, Safety-Guided Design, Design Principles)
Risk Management
Operations
Management Principles/ Organizational Design
Regulation
Tools
Accident/Event Analysis CAST
Hazard Analysis STPA
Specification Tools SpecTRM
Organizational/Cultural Risk Analysis
Identifying Leading Indicators
Security Analysis STPA-Sec
STAMP: Theoretical Causality Model

Figure 3.2: An overview of the derived STAMP methods [7]

STPA will be used for this assignment and will therefore be further described in chapter 3.1

3.1 The Systems-Theoretic Process Analysis (STPA) method

STPA is a holistic, qualitative, top down hazard analysis method based on the STAMP causality theory described in chapter 3. The basic idea is to model systems using control feedback loops, rather than using chain causality, with the goal of increasing the safety engineers and designers mental comprehensiveness of the complex system and its internal and external interactions, without losing information. Modeling the system using control theory automatically sorts the system components by interaction, which makes it easier to identify component interaction failures (software, hardware and human errors), rather than just component failures (see definitions in chapter 3). Guidance is provided on how to model the system in the new way and how to analyze the system based on the new kind of model to anticipate all possible accidents existing through the system design, its environment and its operation including the human operators. It further enables analysis of the impact of company culture and societal and political structures on safety of a project or system.

A critical advantage of STPA is that it can be applied at any part of the standard systems engineering V-model life cycle, enabling early system design for safety, which reduces project costs. The possible usage of applying STPA at the different steps is shown in figure 3.3.

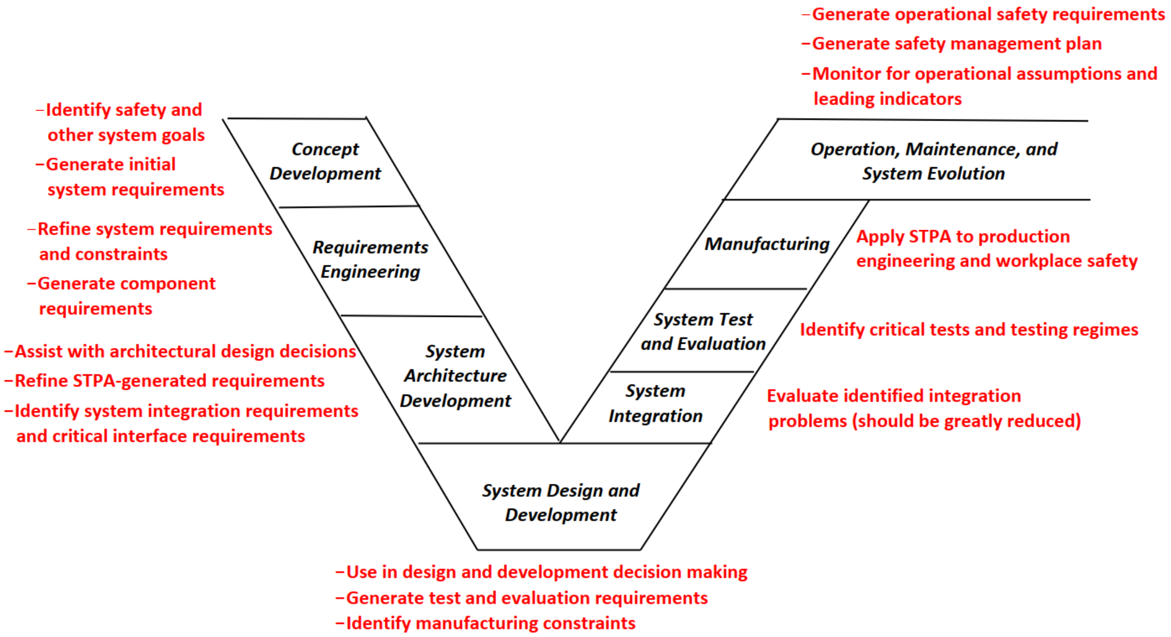

–Generate operational safety requirements
–Generate safety management plan
–Monitor for operational assumptions and leading indicators
–Identify safety and other system goals
–Generate initial system requirements
Concept Development
Operation, Maintenance, and System Evolution
–Refine system requirements and constraints
–Generate component requirements
Requirements Engineering
Manufacturing
Apply STPA to production engineering and workplace safety
–Assist with architectural design decisions
–Refine STPA-generated requirements
–Identify system integration requirements and critical interface requirements
System Architecture Development
System Test and Evaluation
Identify critical tests and testing regimes
System Integration
Evaluate identified integration problems (should be greatly reduced)
System Design and Development
–Use in design and development decision making
–Generate test and evaluation requirements
–Identify manufacturing constraints

Figure 3.3: STPA in the V-model life cycle [8]

The STPA method can be divided in 4 main steps as shown in figure 3.4:

1. Define purpose of the analysis: Identify losses (stakeholder interests), system-level hazards and system-level constraints
2. Model the control structure: Model your system using control theory
3. Identify unsafe control actions: Analyze your control actions
4. Identify loss scenarios: Identify causal scenarios leading to losses

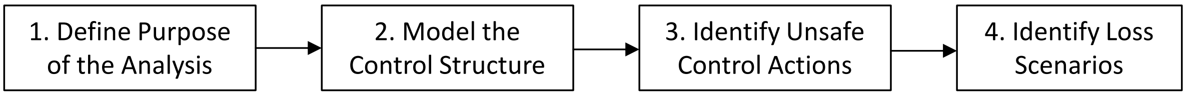

1. Define Purpose of the Analysis
2. Model the Control Structure
3. Identify Unsafe Control Actions
4. Identify Loss Scenarios

Figure 3.4: The 4 STPA steps [8]

The following explanation of the STPA steps is based on the STPA Handbook, all examples are taken from this Handbook [8].

Step 1: Define purpose of the Analysis

Step 1 is to define the purpose of the analysis, it consists of 4 parts. An overview of this step is shown in figure 3.5, the parts will be described in the following.

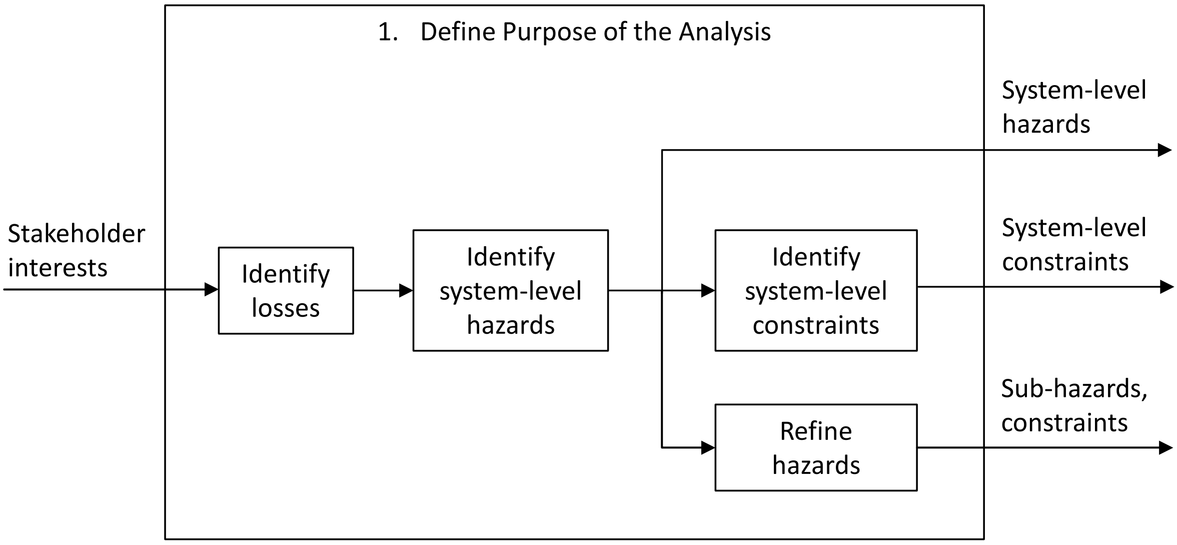


Figure 3.5: STPA step 1 [8]

Step 1.1. Identifying losses

"Definition: A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders." [8]

The losses are identified by considering the stakeholders interests. Every STPA result will be traceable to one or more losses. The losses will be numbered and any special considerations or assumptions made will be documented.

Examples of typical losses are:

L-1: Loss of life or injury to people
L-2: Loss of or damage to vehicle
L-3: Loss of or damage to objects outside the vehicle
L-4: Loss of mission
L-5: Loss of customer satisfaction
L-6: Loss of sensitive information
L-7: Environmental loss
L-8: Loss of power generation
L-9: Loss of reputation

Step 1.2. Identify system-level hazards

"Definition: A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss." [8]

"Definition: A system is a set of components that act together as a whole to achieve some common goal, objective, or end. A system may contain subsystems and may also be part of a larger system." [8]

To identify system-level hazards the system definition, thus the system boundaries, must be clear. A useful way to set the system boundaries is to include the parts in the system which the system designers can influence. The system-level hazards will then be identified by identifying system states or conditions that will lead to a loss in worst-case environmental conditions. There are no methods to help identifying these hazards, but the level of abstraction makes this step relatively easy. A usual set of system-level hazards consists of no more than 7 to 10 hazards. The system-level hazards will be numbered and mapped to the identified losses. Examples of typical system-level hazards are:

H-1: Aircraft violate minimum separation standards in flight [L-1, L-2, L-4, L-5]
H-2: Aircraft airframe integrity is lost [L-1, L-2, L-4, L-5]
H-3: Aircraft leaves designated taxiway, runway, or apron on ground [L-1, L-2, L-5]
H-4: Aircraft comes too close to other objects on the ground [L-1, L-2, L-5]
H-5: Satellite is unable to collect scientific data [L-4]
H-6: Vehicle does not maintain safe distance from terrain and other obstacles [L-1, L-2, L-3, L-4]
H-7: UAV does not complete surveillance mission [L-4]
H-8: Nuclear power plant releases dangerous materials [L-1, L-4, L-7, L-8]

Step 1.3. Identify system level constraints

„Definition: A system-level constraint specifies system conditions or behaviors that need to be satisfied to prevent hazards (and ultimately prevent losses)." [8]

System-level constraints are identified by inverting the system-level hazards. The system-level constraints will be numbered and mapped to the related system-level hazard. Examples of inverting system-level hazards to system-level constraints are:

H-1: Aircraft violate minimum separation standards [L-1, L-2, L-4, L-5]
SC-1: Aircraft must satisfy minimum separation standards from other aircraft and objects [H-1]
H-2: Aircraft airframe integrity is lost [L-1, L-2, L-4, L-5]
SC-2: Aircraft airframe integrity must be maintained under worst-case conditions [H-2]

Step 1.4. Refine system-level hazards (optional)

For complex applications it can be useful to refine the system-level hazards into sub-hazards for comprehensibility reasons. This is not an indispensable step. The sub-hazards will have to be inverted into constraints again.

Step 2: Model the Control Structure

Step 2 is to model a hierarchical control structure. The control structure is the system model STPA works with, it provides guidance for the analysis and understanding of the safety relevant parts of the system.

"Definition: A hierarchical control structure is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system." [8]

Basic feedback control loops, as shown in figure 3.6, consist of a controller providing control actions to a controlled process. The controller obtains feedback from the controlled process which can update its process model of the controlled process or parts of it. The control algorithm represents the controller's decision-making process. The controller's process model might be embedded in the control algorithm. Problems can occur at any point of this control loop.

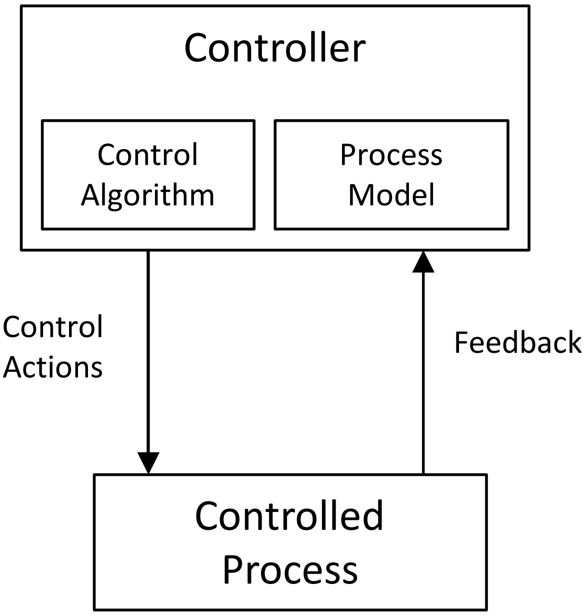


Figure 3.6: Basic control loop[8]

Such control loops can be used to identify complex software and human interactions that can lead to losses. For a human controller the process model is called a mental model and the control algorithm may be called operating procedures or decision-making rules.

Real systems will have several overlapping and interacting control loops; they can be modeled in a hierarchical control structure which contains at least five types of elements: controllers, control actions, feedback, other inputs to and from components and controlled processes. A simple example for a hierarchical control structure in aviation is shown in figure 3.7. Downward arrows represent control actions (commands), upward arrows represent feedback. A control structure is neither a physical nor an executable (simulation) model. It simply indicates that a mechanism will be created to send the control actions and feedback information, while not implying anything about how the system will actually behave in practice. Detail (including sensors and actuators) to the abstract control structure will be added iteratively. At this point the types of commands and feedback that might be provided matters, not the specific implementation. It is good practice to document any clarifying information about the control structure.

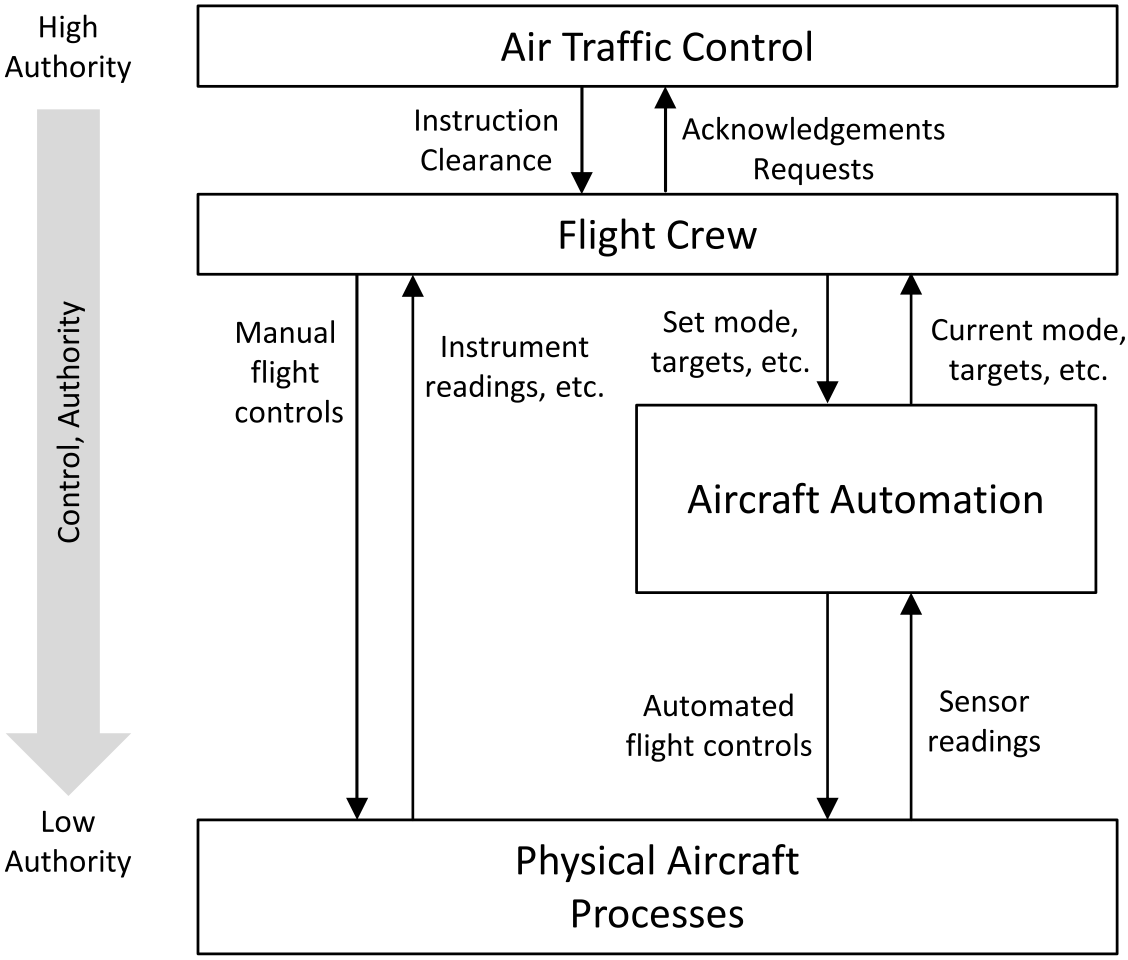


Figure 3.7: Simple aviation hierarchical control structure

A more generic control structure including sociotechnical aspects is shown in figure 3.8.

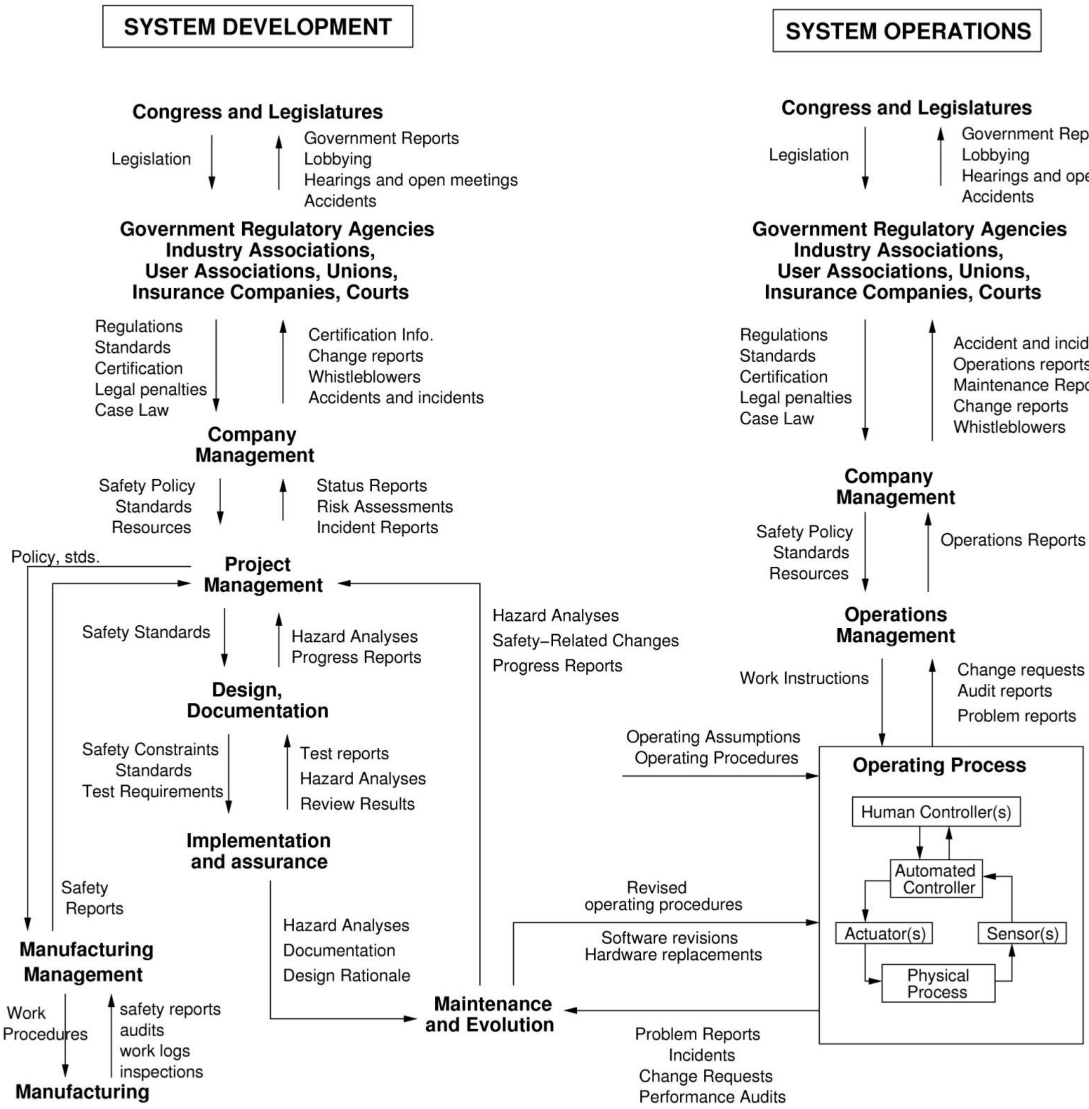


Figure 3.8: A sociotechnical control structure [9]

To refine control structures, subsystems needed to enforce the constraints identified in the STPA step 1, need to be identified. In the following the wheel braking sub-system example from [8] is used to demonstrate how to further refine control structures and how to work with the control structure in the following steps. Figure 3.9 shows a simple subsystem breakdown of an aircraft. To control hazards like H-3: Aircraft leaves designated taxiway, runway, or apron on ground [L-1, L-2, L-5] or H-4: Aircraft comes too close to other objects on the ground [L-1, L-2, L-5] a wheel braking subsystem is needed. Identifying how this subsystem is controlled further refines the control structure, as shown in figure 3.10.

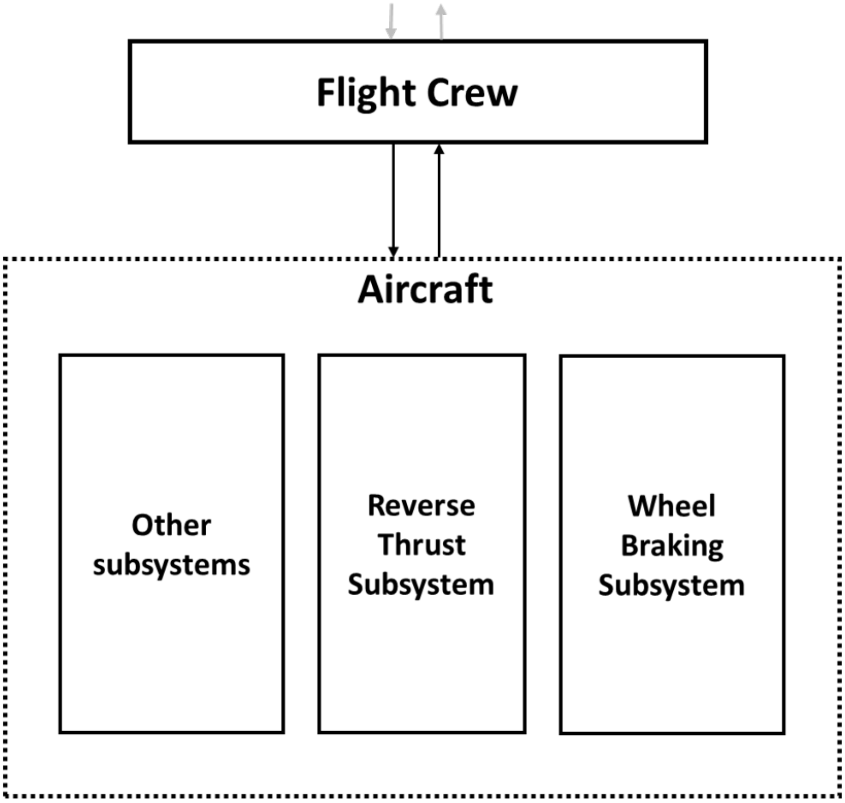


Figure 3.9: Aircraft sub-systems [8]

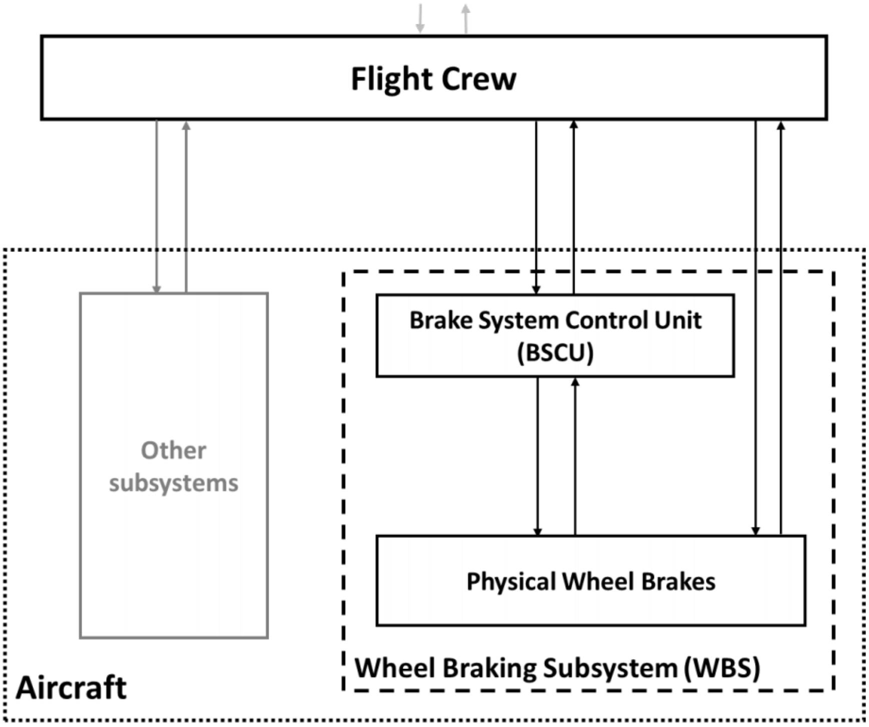

Flight Crew
Brake System Control Unit (BSCU)
Other subsystems
Physical Wheel Brakes
Wheel Braking Subsystem (WBS)
Aircraft

Figure 3.10: Refined wheel-braking sub-system [8]

The controllers will then be assigned with responsibilities that together are to enforce the system-level constraints. Examples of such responsibilities are:

Physical Wheel Brakes
R-1: Decelerate wheels when commanded by BSCU or Flight Crew [SC-6.1]
BSCU
R-2: Actuate brakes when requested by flight crew [SC-6.1]
R-3: Pulse brakes in case of a skid (Anti-skid) [SC-6.2]
R-4: Automatically engage brakes on landing or rejected takeoff (Autobrake) [SC-6.1]
Flight crew
R-5: Decide when braking is needed [SC-6.1, SC-6.3]
R-6: Decide how braking will be done: Autobrake, normal braking, or manual braking [SC-6.1]
R-7: Configure BSCU and Autobrake to prepare for braking [SC-6.1]
R-8: Monitor braking and disable BSCU, manually brake in case of malfunction [SC-6.1, SC-6.2]

Based on these responsibilities it is simple to define control actions for each controller as shown in figure 3.11.

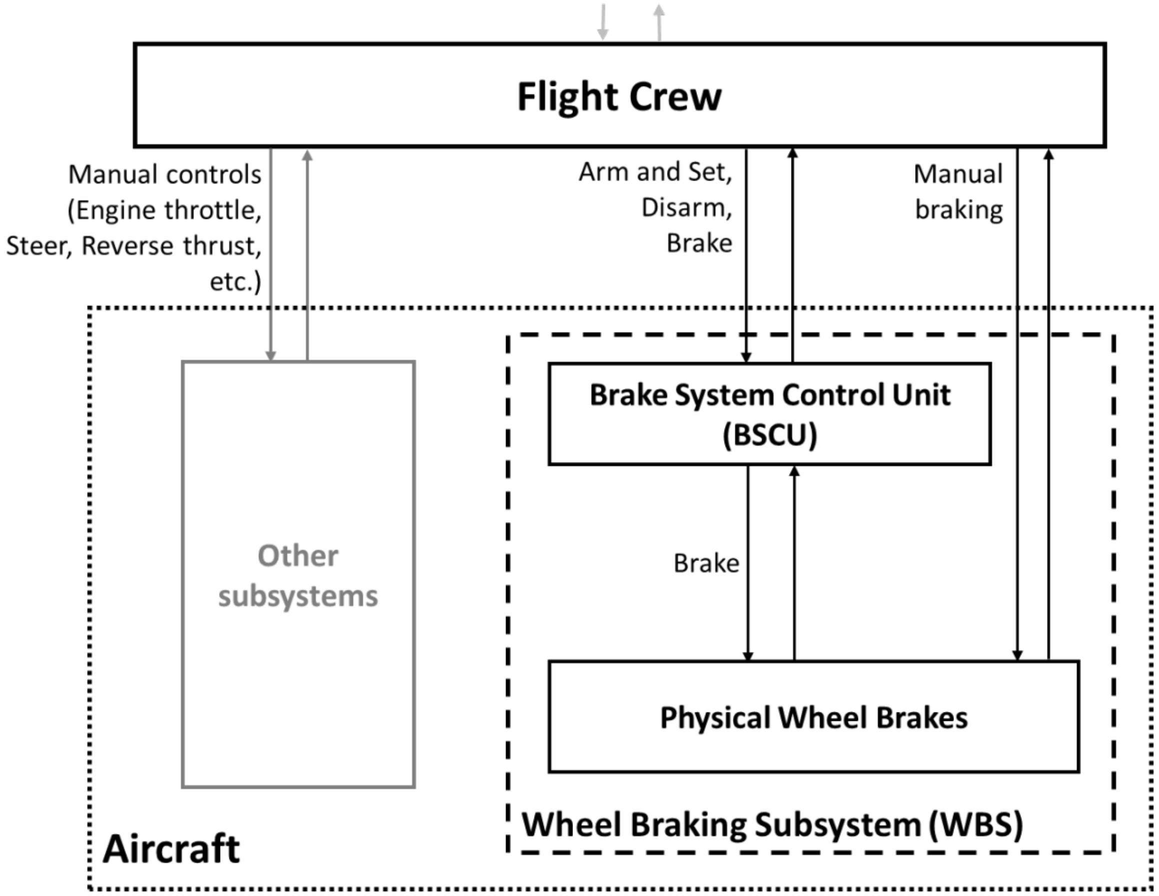

Flight Crew
Manual controls (Engine throttle, Steer, Reverse thrust, etc.)
Arm and Set, Disarm, Brake
Manual braking
Brake System Control Unit (BSCU)
Brake
Other subsystems
Physical Wheel Brakes
Wheel Braking Subsystem (WBS)
Aircraft

Figure 3.11: Refined wheel-braking sub-system with control actions [8]

To define needed feedback, the process models needed by the controllers to make decisions, are to identify. For this purpose the responsibilities once again provide guidance. Examples of identified process models and so needed feedback are:

BSCU Responsibility	Process Model	Feedback
Actuate brakes when requested by flight crew [SC-6.1]	Braking is requested by flight crew	Brake pedal applied
Pulse brakes in case of a skid (Anti-skid) [SC-6.2]	Aircraft is skidding	Wheel speeds Inertial reference unit
Automatically engage brakes on landing or RTO (Autobrake) [SC-6.1]	Aircraft landed Takeoff is rejected	Weight on wheels Throttle lever angle

Table 3.1: Identifying needed feedback to being able to fulfill responsibilities[8]

The process of using the responsibilities to further refine the control structure and identify underlying controllers can be repeated until any desired level of detail is reached. Figure 3.12 shows the further refined wheel braking subsystem with the needed feedback.

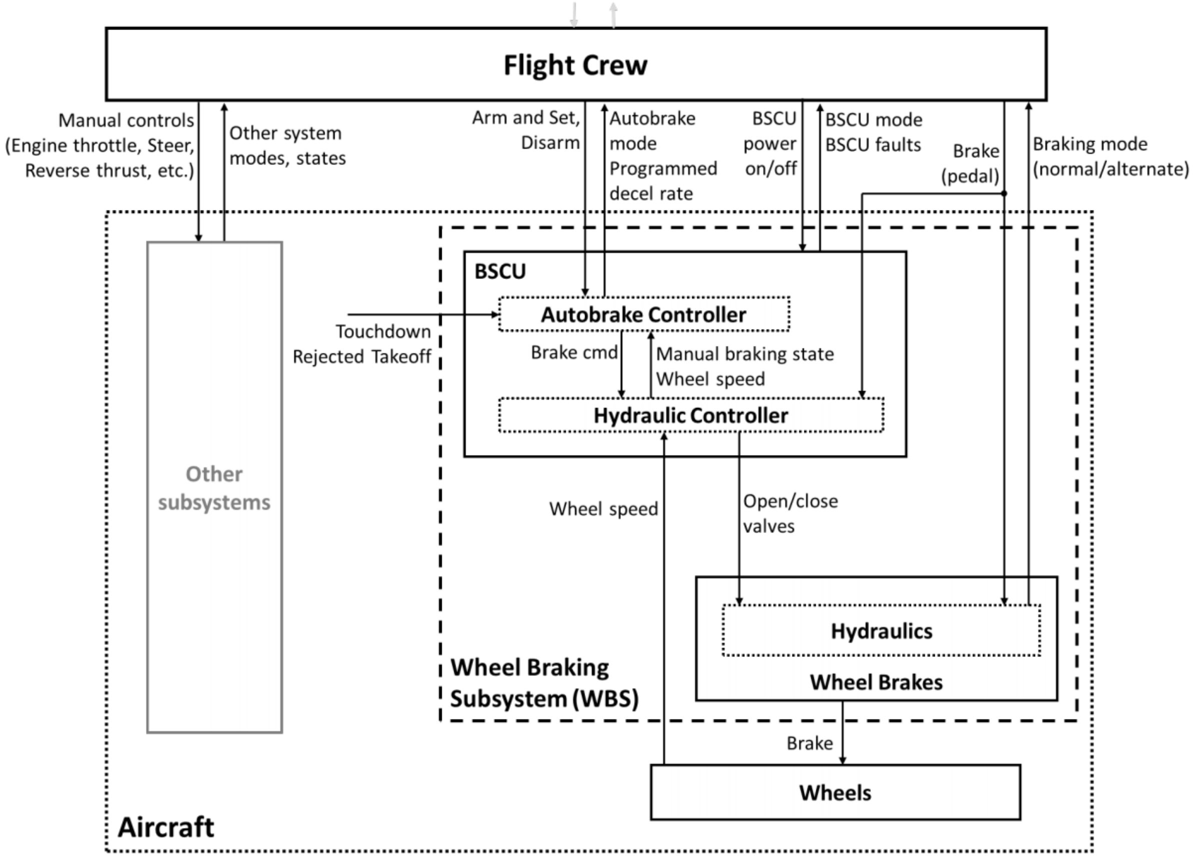

Flight Crew
Manual controls (Engine throttle, Steer, Reverse thrust, etc.)
Other system modes, states
Arm and Set, Disarm
Autobrake mode Programmed decel rate
BSCU power on/off
BSCU mode BSCU faults
Brake (pedal)
Braking mode (normal/alternate)
Other subsystems
BSCU
Autobrake Controller
Touchdown Rejected Takeoff
Brake cmd
Manual braking state Wheel speed
Hydraulic Controller
Wheel speed
Open/close valves
Hydraulics
Wheel Brakes
Wheel Braking Subsystem (WBS)
Brake
Wheels
Aircraft

Figure 3.12: Further refined wheel-braking sub-system with control actions and feedback [8]

Step 3: Identify Unsafe Control Actions

Step 3 is to identify unsafe control actions with the goal to identify behaviors that should be prevented. An overview of this step is shown in figure 3.13, the parts will be described in the following.

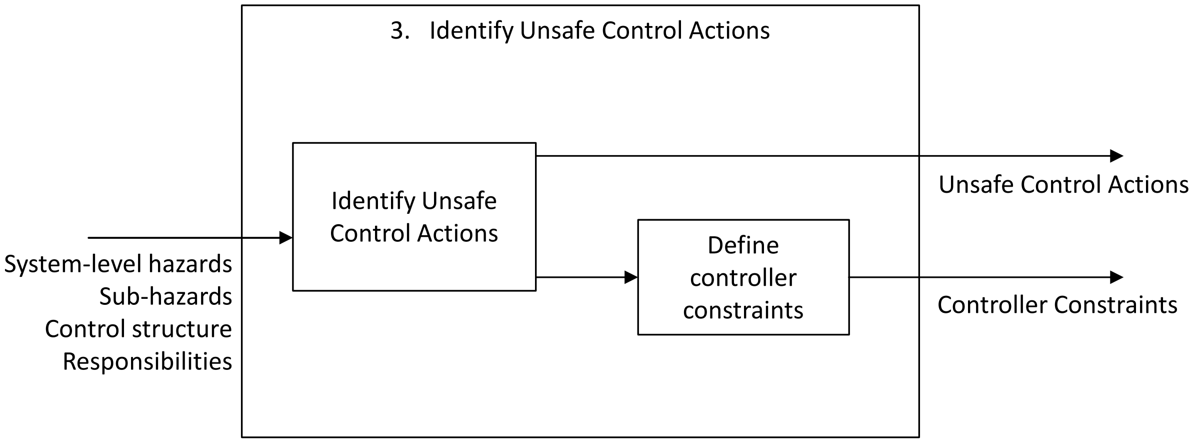


Figure 3.13: STPA step 3 [8]

3.1 Identifying Unsafe Control Actions

"Definition: An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard." [8]

A control action can be unsafe in four ways:

1. Not providing the control action leads to a hazard.
2. Providing the control action leads to a hazard.
3. Providing a potentially safe control action but too early, too late, or in the wrong order
4. The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones).

Note that not providing here means the controller does not provide the control action, it is not related to any execution problems such as signal is corrupted or signal gets lost on the way. Every control action in the control structure has to be analyzed considering these four ways. The context in which the unsafe control action occurs is hereby critical and has to be considered. Every **U**nsafe **C**ontrol **A**ction (UCA) must be traceable to one or more system-level hazard. Thus UCAs should contain the following five parts: Source, Type, Control Action, Context, Link to Hazards. Any special reasoning behind UCAs should be documented, especially when working with complex systems. Examples of UCAs for the wheel braking system are:

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Brake	UCA-1: BSCU Autobrake does not provide the Brake control action during landing roll when the BSCU is armed [H-4.1]	UCA-2: BSCU Autobrake provides Brake control action during a normal takeoff [H-4.3, H-4.6] UCA-5: BSCU Autobrake provides Brake control action with an insufficient level of braking during landing roll [H-4.1] UCA-6: BSCU Autobrake provides Brake control action with directional or asymmetrical braking during landing roll [H-4.1, H-4.2]	UCA-3: BSCU Autobrake provides the Brake control action too late (>TBD seconds) after touchdown [H-4.1]	UCA-4: BSCU Autobrake stops providing the Brake control action too early (before TBD taxi speed attained) when aircraft lands [H-4.1]

Table 3.2: Identifying unsafe control actions [8]

For human control actions the same approach is used. Examples are:

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Power Off BSCU	UCA-1: Crew does not provide BSCU Power Off when abnormal WBS behavior occurs [H-4.1, H-4.4, H-7]	UCA-2: Crew provides BSCU Power Off when Anti-Skid functionality is needed and WBS is functioning normally [H-4.1, H-7]	Crew powers off BSCU too early before Autobrake or Anti-Skid behavior is completed when it is needed [H-4.1, H-7]	N/A

Table 3.3: Identifying unsafe control actions for human controllers [8]

3.2 Defining Controller Constraints

„Definition: A controller constraint specifies the controller behaviors that need to be satisfied to prevent UCAs" [8]

Controller constraints are defined by inverting the UCAs. For example:

Unsafe Control Actions	Controller Constraints
UCA-1: BSCU Autobrake does not provide the Brake control action during landing roll when the BSCU is armed [H-4.1]	C-1: BSCU Autobrake must provide the Brake control action during landing roll when the BSCU is armed [UCA-1]
UCA-2: BSCU Autobrake provides Brake control action during a normal takeoff [H-4.3, H-4.5]	C-2: BSCU Autobrake must not provide Brake control action during a normal takeoff [UCA-2]
UCA-3: BSCU Autobrake provides the Brake control action too late (>TBD seconds) after touchdown [H-4.1]	C-3: BSCU Autobrake must provide the Brake control action within TBD seconds after touchdown [UCA-3]
UCA-4: BSCU Autobrake stops providing the Brake control action too early (before TBD taxi speed attained) during landing roll [H-4.1]	C-4: BSCU Autobrake must not stop providing the Brake control action before TBD taxi speed is attained during landing roll [UCA-4]
UCA-5: BSCU Autobrake provides Brake control action with an insufficient level of braking during landing roll [H-4.1]	C-5: BSCU Autobrake must not provide less than TBD level of braking during landing roll [UCA-5]

Table 3.4: Identifying controller constraints [8]

Step 4: Identify Loss Scenarios

Step 4 is identifying the loss scenarios. An overview of this step is shown in figure 3.14, the parts will be described in the following.

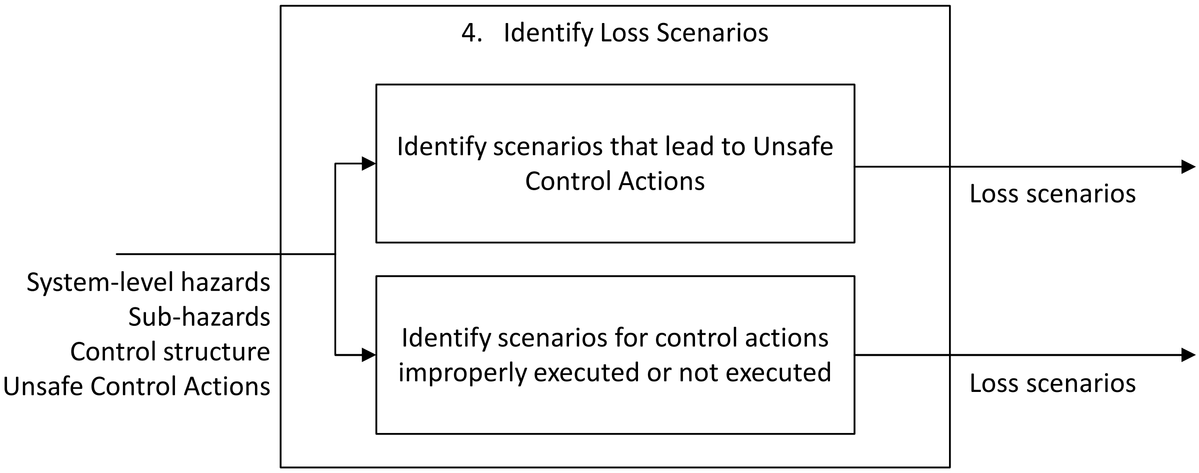

4. Identify Loss Scenarios
Identify scenarios that lead to Unsafe Control Actions
Identify scenarios for control actions improperly executed or not executed
System-level hazards
Sub-hazards
Control structure
Unsafe Control Actions
Loss scenarios
Loss scenarios

Figure 3.14: STPA step 4 [8]

"Definition: A loss scenario describes the causal factors that can lead to the Unsafe Control Actions and to hazards." [8]

At this step it can be useful to refine the safety control structure in a way that ads actuators and sensors as shown in the generic control structure in figure 3.15.

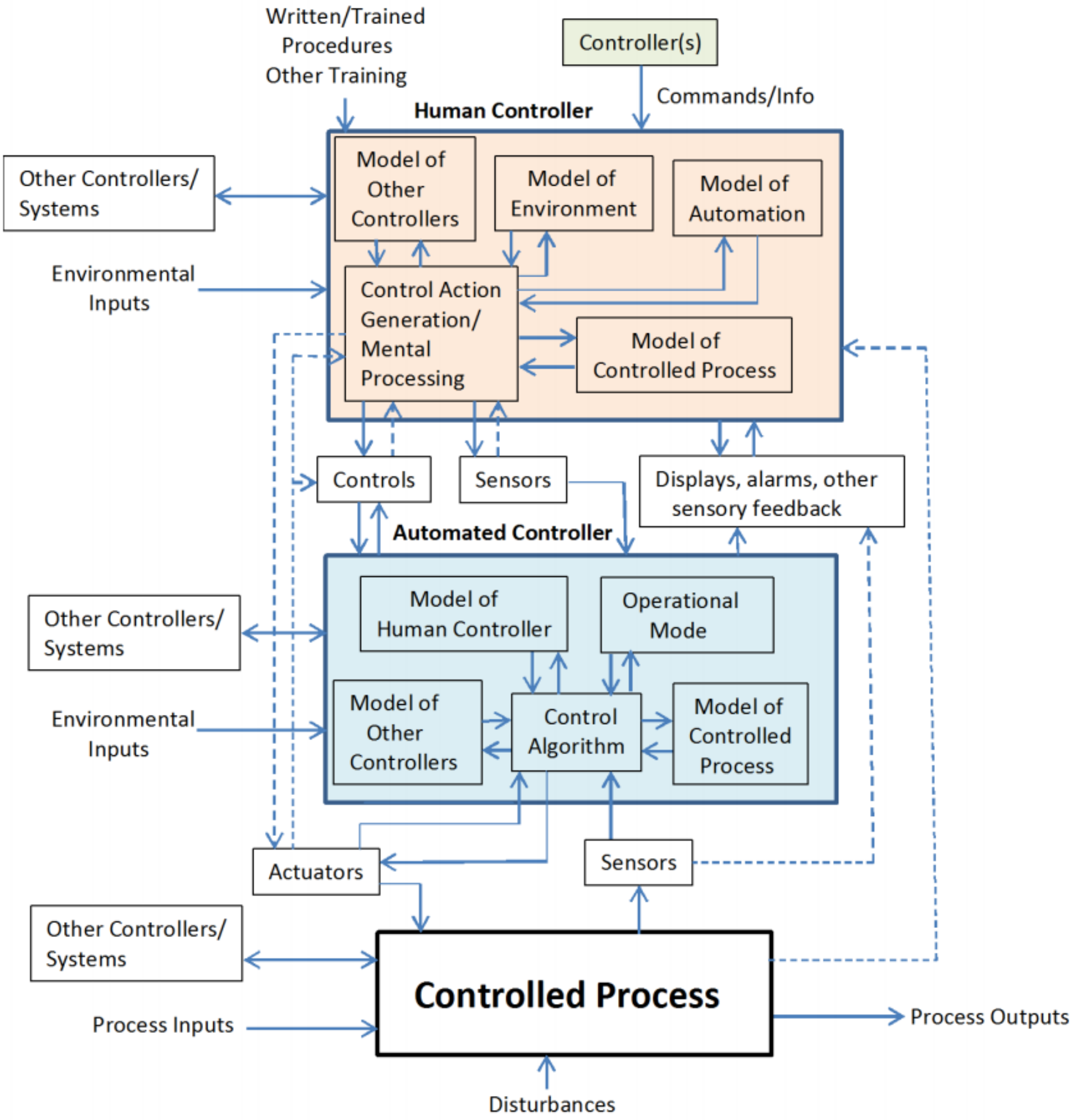

Written/Trained Procedures Other Training
Controller(s)
Commands/Info
Human Controller
Other Controllers/ Systems
Model of Other Controllers
Model of Environment
Model of Automation
Environmental Inputs
Control Action Generation/ Mental Processing
Model of Controlled Process
Controls
Sensors
Displays, alarms, other sensory feedback
Automated Controller
Other Controllers/ Systems
Model of Human Controller
Operational Mode
Environmental Inputs
Model of Other Controllers
Control Algorithm
Model of Controlled Process
Actuators
Sensors
Other Controllers/ Systems
Controlled Process
Process Inputs
Process Outputs
Disturbances

Figure 3.15: Generic safety control structure with sensors and actuators [6]

There are two types of loss scenarios:

a) An UCA occurs
b) A control action is not executed or executed improperly

Note the difference between "not provided" (by the controller) and "not executed" (does not happen after being provided by the controller). These two types of loss scenarios emerge from two different parts in the control structure as shown in figure 3.16.

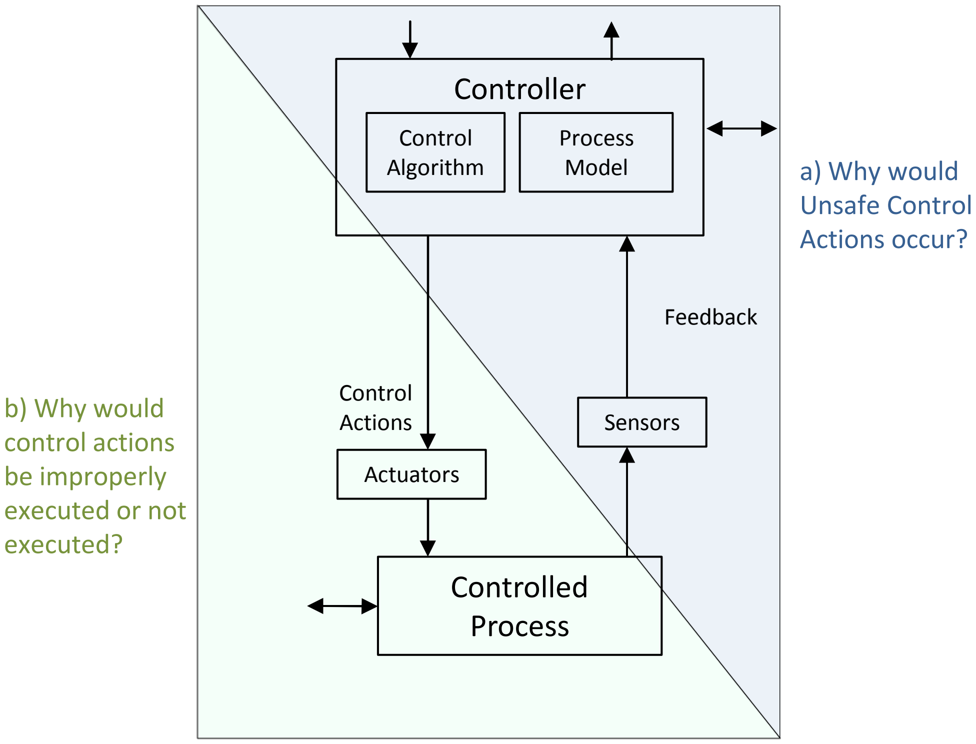

Controller
Control Algorithm
Process Model
a) Why would Unsafe Control Actions occur?
Feedback
Control Actions
Actuators
Sensors
b) Why would control actions be improperly executed or not executed?
Controlled Process

Figure 3.16: The safety control structure divided by the two types of possible loss scenarios[8]

In general there are four types of scenarios resulting:

Type a.1) unsafe controller behavior
Type a.2) inadequate feedback and information
Type b.3) scenarios involving the control path
Type b.4) scenarios related to the controlled process

a.1) Unsafe controller behavior can have four general reasons:

a.1.1) Failures involving the controller (for physical controllers)

Example:

UCA-1: BSCU Autobrake does not provide the Brake control action during landing roll when the BSCU is armed. [H-4.1]

Scenario 1 for UCA-1: The BSCU Autobrake physical controller fails during landing roll when BSCU is armed, causing the Brake control action to not be provided [UCA-1]. As a result, insufficient deceleration may be provided upon landing [H-4.1]

a.1.2) Inadequate control algorithm

- Flawed implementation of the specified control algorithm
- The specified control algorithm is flawed
- The specified control algorithm becomes inadequate over time due to changes or degradation

Example:

UCA-3: BSCU Autobrake provides the Brake control action too late (>TBD seconds) after touchdown. [H-4.1]

Scenario 1 for UCA-3: The aircraft lands, but processing delays within the BSCU result in the Brake control action being provided too late [UCA-3]. As a result, insufficient deceleration may be provided upon landing. [H-4.1]

a.1.3) Unsafe control input (from another controller)

- UCA of another controller, identified by analyzing the other controller for UCAs.

a.1.4) Inadequate process model

- Controller receives incorrect feedback/information
- Controller receives correct feedback/information but interprets it incorrectly or ignores it
- Controller does not receive feedback/information when needed (delayed or never received)
- Necessary controller feedback/information does not exist

Example:

Controller process model (belief) that could cause the UCA: Aircraft is in flight.

Controller does not receive information when needed: Touchdown indication is not received.

Scenario 2 for UCA-2: The BSCU is armed and the aircraft begins landing roll. The BSCU does not provide the Brake control action [UCA-2] because the BSCU incorrectly believes the aircraft is in the air and has not touched down. This flawed process model will occur if the touchdown indication is not received upon touchdown. Scenario will be finished below!

a.2) Inadequate feedback and information can result from:

a.2.1) Feedback or information not received

- Feedback/info sent by sensor(s) but not received by controller
- Feedback/info is not sent by sensor(s) but is received or applied to sensor(s)
- Feedback/info is not received or applied to sensor(s)
- Feedback/info does not exist in control structure or sensor(s) do not exist

a.2.2) Inadequate feedback is received

- Sensor(s) respond adequately but controller receives inadequate feedback/info
- Sensor(s) respond inadequately to feedback/info that is received or applied to sensor(s)
- Sensor(s) are not capable or not designed to provide necessary feedback/info

Example:

Finishing Scenario 2 for UCA-2 above: True state from UCA context: Aircraft is in landing roll (see Scenario 2 above).

Information received: Touchdown indication is not received upon touchdown (see Scenario 2 above).

How this could happen given the true state: Reported wheel speed is insufficient, reported weight on wheels is insufficient, wheel speed or weight on wheels indications are delayed, etc.

Scenario 2 for UCA-2: The BSCU is armed and the aircraft begins landing roll. The BSCU does not provide the Brake control action [UCA-2] because the BSCU incorrectly believes the aircraft is in the air and has not touched down. This flawed process model will occur if the touchdown indication is not received upon touchdown. The touchdown indication may not be received when needed if any of the following occur:

- Wheels hydroplane due to a wet runway (insufficient wheel speed)
- Wheel speed feedback is delayed due to filtering used
- Conflicting air/ground indications due to crosswind landing
- Failure of wheel speed sensors
- Failure of air/ground switches
- Etc.

As a result, insufficient deceleration may be provided upon landing. [H-4.1]

b.3) Scenarios involving the control path can occur due to:

b.3.1) Control action not executed

- Control action is sent by controller but not received by actuator(s)
- Control action is received by actuator(s) but actuator(s) do not respond
- Actuator(s) responds but the control action is not applied to or received by the controlled process

b.3.2) Control action improperly executed

- Control action is sent by controller but received improperly by actuator(s)
- Control action is received correctly by actuator(s) but actuator(s) respond inadequately
- Actuator(s) respond adequately, but the control action is applied or received improperly at the controlled process
- Control action is not sent by controller, but actuators or other elements respond as if it had been sent

Example:

Control action: BSCU sends Brake command

Improper execution: Insufficient braking applied

Scenario 2: The BSCU sends the Brake command upon landing, but insufficient braking is applied due to slow actuator response. As a result, insufficient deceleration may be provided upon landing. [H-4.1]

b.4) Scenarios related to the controlled process can occur due to:

b.4.1) Control action not executed

- Control action is applied or received by the controlled process but the controlled process does not respond

b.4.2) Control action improperly executed

- Control action is applied or received by the controlled process but the controlled process responds improperly
- Control action is not applied or received by the controlled process but the process responds as if the control action had been applied or received

Example:

Control action: BSCU sends Brake command

Scenario 6: The BSCU sends Brake command, but the brakes are not applied because the wheel braking system was previously commanded into alternate braking mode (bypassing the BSCU). As a result, insufficient deceleration may be provided upon landing. [H-4.1]

All UCAs identified in step 3 will so be analyzed using all the type a scenarios to create the loss scenarios. All control actions in the safety control structure will be analyzed using the type b scenarios to create the loss scenarios. The loss scenarios will be mapped to the system-level hazards. It is crucial to create complete scenarios with context instead of just causal factors to prevent overlooking combinations or interaction of several factors, non-trivial factors and non-obvious factors which can all lead to UCAs and so losses.

The outputs of STPA shown in figure 3.17 might be used to:

"- Drive the system architecture
- Create requirements
- Identify design recommendations
- Identify mitigations and safeguards needed
- Define test cases and create test plans
- Drive new design decisions (if STPA is used during development)
- Evaluate existing design decisions and identify gaps and changes needed
- Develop leading indicators of risk
- Design more effective safety management systems"[8]

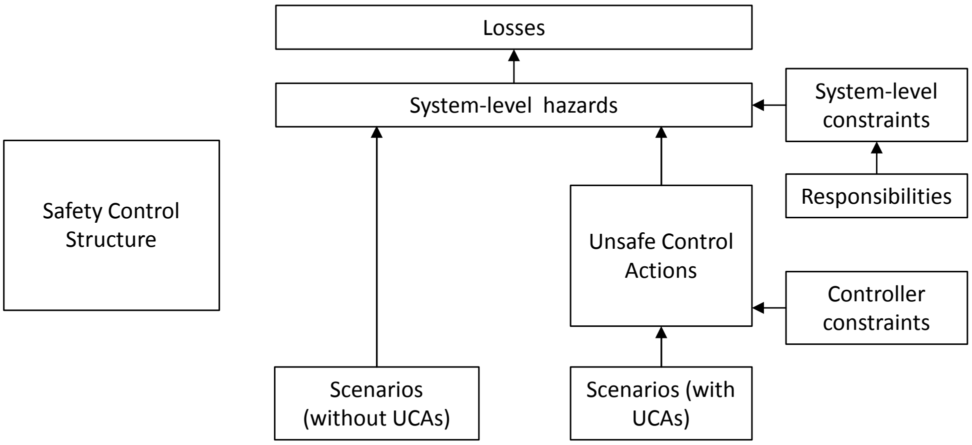


Figure 3.17: STPA outputs[8]

3.2 Engineering for Humans a New Extension to STPA

John P. Thomas, Co-Author of the STPA Handbook, suggested an extension to STPA to provide more guidance than provided in the STPA Handbook for modeling and analyzing the human controller and predicting the human controller behavior in the system environment. This extension was then developed by Megan E. France [10], resulting in the generic frame on how to model a human controller shown in figure 3.18. This model is based on experience with common accidents where human controllers were blamed to be the "root cause". Modeling the human controller in this way helps analyzing why loss scenarios involving a human error occurred and being able to change the design or operations in a way to pretend such errors, rather than just stating it as a human error and trying to assign a probability to the occurrence of such error. Further this model can be used as a dialogue basis for discussions between safety, system and human factors engineers.

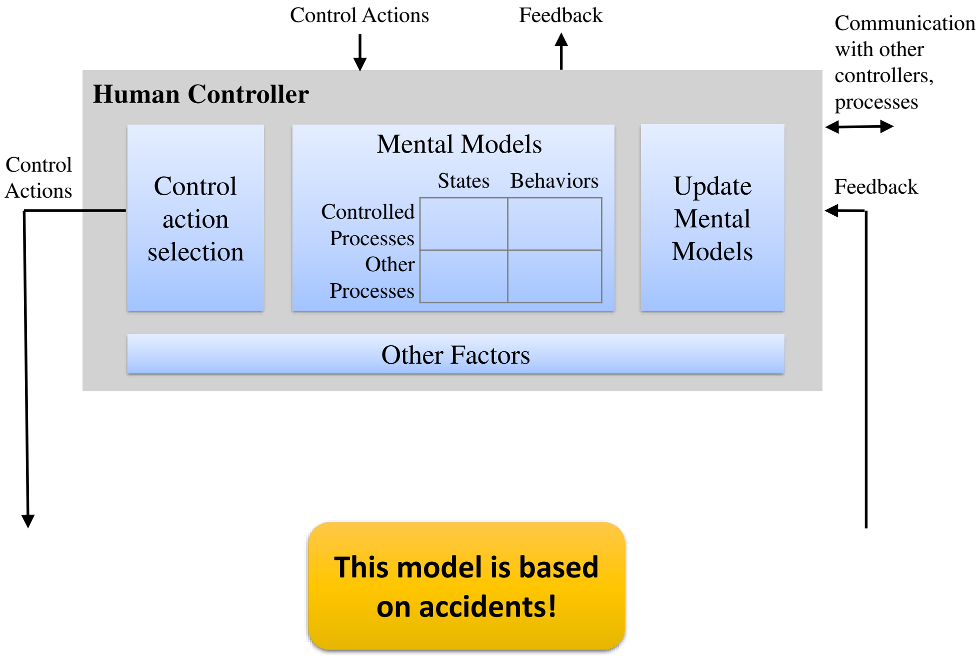


Figure 3.18: Generic model frame for a human controller [11]

The mental models table of the human controller represents the human controller's beliefs about the system states and behaviors and its environment. It is helpful to create the mental model table for a human controller generically first, including all of the Safety Pilot's mental models of the system, using the safety control structure, and the possible state and behavior beliefs thereof. For every unsafe control action identified in step 3, this template is then used in step 4 to identify mental model flaws which could lead the human controller to provide this unsafe control action. Loss scenarios can then be identified by analyzing the 3 main parts of the new model: "How did the operator choose which control action to perform? [Flawed control action selection through skills, goals, time pressure and so on] What does the operator know or believe about the system? [Mental model flaws, initial false beliefs, false beliefs through false updates] And how did the operator come to have their current knowledge or beliefs? [Flawed mental model updates through feedback, training, experience and so on]" [10]

4 Comparison of the SAE ARP4754A and the STAMP/STPA approaches to achieve safety

The SAE ARP4754A approach to safety has been described in chapter 2. Why there is a need for new safety engineering techniques and the new proposed approach in STAMP and STPA has been described in chapter 3. In chapter 4 now a summarizing comparison of the two approaches, assumptions and abilities of the methods to achieve safety is given. A discussion of the identified struggles and limitations of STPA during application as identified in chapter 5 is then given in chapter 6.

The two different definitions of safety (the freedom of losses in STAMP vs. the state where risk is acceptable in ARP4754A) can make it seem as if the two different approaches on how to achieve safety have two different goals then. But they work towards the same direction, which is freedom of losses, ARP4754A just allows to stop on the way at a point where losses are held to a certain level. This is coming from the traditional assumption, that freedom of losses cannot be achieved in reasonable cost and service constraints and the following idea to, for certification, use the level of losses, which seems to be societal acceptable.

It is unclear if this assumption is still holding up at all or if the numbers associated with it are still holding up, as it seems like as modern technology exceeds the for certification necessary failure probabilities of components and parts and so on. But new causes of accidents are rising which stem from the complexity of the system and so overseen interactions of components or human errors, as discussed in chapter 3. If these findings are correct, there would be a need of reevaluating the reliability numbers asked for in the regulations and the methods used for safety engineering in the regulations. This also means a reevaluation of the societal acceptance of traditional risks, as this traditional risk is probably preventable in reasonable cost and service constraints with changing the certification criteria by adding new methods like STPA and lowering allowed loss probabilities. This goes without an analysis of actual accident numbers trends and so loss trends, as the question is not "are the numbers going down or up or staying the same?", but "are the accidents preventable in reasonable cost and service constraints?". So, is the loss associated with the probability of that loss, the risk, acceptable or not.

STPA does not seek to replace quantitative analysis methods, which aim to verify reliability. It aims to analyze which combination of which functions are safe (completeness of requirements), if they are provided reliably and it aims to give reliability analysis methods complete sets of scenarios, which can lead to losses (independence of failures), such that the reliability analysis includes all possible accident causes.

ARP4754A starts with analyzing what losses would be caused by missing or malfunctioning high-level aircraft functions. The losses to prevent in ARP4754A are already defined through the certification regulations. STPA starts with defining losses which are to be prevented and then defines constraints, which must be enforced to prevent those losses. High-level controllers are assigned with control actions, which together shall enforce the defined constraints.

The assumptions in the ARP4754A approach are:

a) No other aircraft functions exist, whose loss can cause any relevant aircraft event

b) No function, which is needed to prevent a relevant aircraft event, is missing initially

c) The functions are so well defined that a combination of their functionality can not lead to a loss

The STPA assumptions are:

a) No other constraints must be enforced to prevent the defined losses

b) No control action, which is needed to enforce a constraint, is missing initially

Both sets of assumptions are reasonable on aircraft level, as it is easy to have a complete understanding of the high-level functions and their interactions and the high-level control actions.

The approach proposed in the ARP4754A is to now identify functions and their requirements on the next lower level, that need to be provided such that the functions on the higher level will be provided with their assigned probability. The levels here refer to the breakdown of the aircraft as highest level into sub-systems all the way down to items, as described in chapter 3. These functions are described by requirements and are assigned with a failure rate (failure probability per time).

The assumptions here are:

1. The physical implementation of the components can meet or exceed the assigned failure rate.

2. The assigned failure rates are independent, which means failures will not have common causes, which are overlooked, such that the assigned failure rate would have to be higher than calculated.

3. Functions on a lower level, if they are provided as defined per the requirements, will together in their interaction provide a function on a higher level. So, there are no states where functions being provided the way they are described in the requirements, but do not together provide the function on a higher level that they are supposed to (component interaction failures), which means requirements would be incorrect or incomplete.

4. Human operators are providing functions which can be assigned with a failure rate.

As, when assumptions 2., 3 and 4. are true, accidents are the result of a chain of failures, these three assumptions about the aircraft system then allow to use a chain causality analysis of the system functions to find all the failures or combinations of failures which could lead to a certain event on aircraft level. The chain causality analysis can so be used to validate and verify that the system provides the high-level aircraft functions reliably and no single point failures exist which can lead to a certain event.

These chain causality analysis methods are FTA/DD/MA and FMEA/FMES.

The weakness of the ARP4754A approach results from the weakness of these analysis methods to find all failures and combination of failures which lead to an aircraft level function not being provided and from the weaknesses of the approach on how to justify the four assumptions. To justify assumption 1. is not a goal of STPA and is therefore not analyzed in this assessment. The other three assumptions are discussed in the following.

Assumption 2:

To justify assumption 2 the CCA shall be performed. All three herein used methods heavily rely on the safety engineers understanding of the analyzed system. The guidance provided to develop this understanding are design documents, lessons learned documents, personal experience, checklists, defining physical local zones (ZSA) or defining particular events (PRA). No additional model of dependencies in the system is used to provide guidance for the safety engineer. The model of the dependencies is then only a mental model, existing only in the safety engineer's head, which the safety engineer uses to find all dependencies. The more complex a system is, the more unlikely it is for the safety engineer to being able to develop a complete mental model of the system dependencies and so find all common causes for failures existing in a system.

Assumption 3:

To justify assumption 3 the requirements must be analyzed on correctness and completeness. As the requirements per definition together describe the functions, the functionality of the system must be analyzed. Is a complete set of functions defined and implemented such that together they are reliably providing the aircraft level functions and are the interactions of the functions in the way they are defined and implemented having states where they are interacting, such that the providing of an aircraft level function could be missing? The analysis of the functionality of the system is, just as the CCA, mostly a weakly guided skill of the designers and safety engineers, as only the mental model is used again with the weaknesses described above. An example of such weak guidance is: "Allocation of System Requirements to Items: In practice, system architecture development and the allocation of requirements are tightly-coupled, iterative processes. With each iteration cycle, the identification and understanding of the requirements increases and the allocation of the system-level requirements to hardware or software items becomes clearer. Outputs of this allocation effort are requirements allocated to hardware and software, inclusive of safety objectives, development assurance levels and function/performance requirements." [4] If there is no model of the system functionality, there can also be no structured and guided approach on how to analyze this model.

Assumption 4:

Assumption 4 has two main problems: It is difficult to assign a failure rate to a human task in general because of the incomplete understanding of the "technical" behavior of the average human (average would be ok as only a certain failure rate has to be justified) and the failure rate of the human task relies on the environment the human operates in, the workload and the complexity of the task itself. Thus, additional models of the human operator and their belief about the system (the human operator mental models) need to be used as guidance for developing human operator environments and human operator tasks. Such guidance is not provided by the ARP4754A.

Even when all the assumptions, which are needed to be true to being able to use chain causality analysis methods, are justified by proper analysis results, the analysis methods (FTA/DD/MA and FMEA/FMES) must still find all failures and combinations of failures which lead to an aircraft level function not being provided. As in the methods, as described in chapter 2, no model of the system functionality is used for guidance, the analyzes methods have the same problems dealing with complex system architectures as CCA mentioned above.

STPA is based on the 3 pillars of STAMP: The most basic concept in safety engineering is a constraint, not an event, hierarchical control and feedback structures as known from system theory are used to model systems, process models of the human controller (the human controller's beliefs about the process) or embedded in software or electromechanical structures of automated controllers are defining the enforced constraints; and can so directly help on the identified weaknesses of the ARP4754A approach on safety:

STPA does not rely on a mental model of the functionality and dependencies of the system, but creates this model, the safety control structure, using control and feedback loops. It can seem like this is an additional source of error, that the model does not actually represent the system, but this source of error exists for the mental model just as well and so this source of error can not be eliminated by any analysis approach. It is rather that this can be described as one of the main advantages of STPA that this source of error can be controlled much more effective, as the model is now taken out of the safety engineer's head and graphically accessible and so it can be discussed with the engineering experts of the relevant system part, component and so on. Further, this model is now not volatile. The model does not only graphically represent the functionality of the system, it also is able to make the system more mentally manageable by sorting the system by functionality and interaction, without losing information. The physical architecture is completely embedded in the structure of the model.

Modeling the system using control theory now enables a structured approach on analyzing the functionality of the system, step 3 and 4 of the STPA approach. This analyzing of the system in the ARP7454A is depending on the way the safety engineer approaches it personally and is only guided by checklists and similar. In STPA this analysis is a guided step by step approach on how to analyze the safety control structure and so the system design based on the model.

Human operators can now be modeled in their environment, highlighting their inputs, tasks and general interactions with the system. The models of the system used by the human operators (their believes about the system) and the models embedded in software or electromechanical hardware used by automated controllers are now part of the system model, such that the needs of these controllers to update their models adequately to provide their functions, become clear.

Abstraction levels can be used to model the system from the very beginning of the design process with not much information of the actual physical implementation known. This enables an early designing for safety, which is favorable for the project success as late changes are cost intensive.

A proposal on how to implement STPA in the ARP4754A approach on achieving safety is given in chapter 6.

5 STPA applied to the DLR High Altitude Platform (HAP) Project

Two different approaches on how to achieve safety have been described and summarized in chapters 2, 3 and 4. In chapter 5 the STAMP approach is now applied to the HAP project using the STPA methodology. In chapter 5.1 an introduction and description of the HAP project is given, chapter 5.2 contains the 4 steps of the STPA.

Being an ongoing project underlying project and design changes there is no possible current, exact and complete description of the HAP project. The state of the art model based system engineering approach for the project uses the **S**ystems **M**odeling **L**anguage (SysML) to model the HAP system, the resulting documents are good source for the current intended design. Further information about the project used in this thesis stems from the continuously updated documents "HAP Project Plan" [12], "HAP Configuration" [13] and "HAP Concept of Operations" [14] and from personal meetings and discussions with HAP system engineers, of which the latter will not be cited as sources. The purpose of chapter 5.1 is to give a project overview to the reader, the information herein is not relevant for the hazard analysis using STPA in chapter 5.2. In chapter 5.2 it is discussed how the assumptions made about the project during the STPA need to be verified to use the results of the STPA for the actual project.

5.1 DLR HAP Project Description

In chapter 5.1 the DLR HAP project will be introduced. Chapter 5.1.1 states the motivation to develop a solar-powered high altitude platform at the German Aerospace Center (DLR), in chapter 5.1.2 a technical overview about the system design and the concept of operations is given.

5.1.1 DLR HAP Project Motivation

Unmanned, solar powered high-altitude platforms are able to operate stationary above any desired location and so combine the flexibility of high-altitude aircraft and the autonomy of satellites. The resulting applications range from the conventional applications of manned aircraft, such as earth observation and in-situ measurements in the stratosphere, to satellite-like applications, such as providing communication hubs or surveillance of crisis areas.

A research platform of such kind being available at the DLR will enable the testing of new technologies of the platform itself as well as the testing of new payloads and operational scenarios. Similar to geostationary satellites the platform shall be able to continuously cover a certain area without orbit caused waiting times. The start and landing possibility shall enable maintenance or changes of platform and payload. The platform is supposed to fly in altitudes between 15-20 km above low population areas, but not limited to closed airspace. An EASA CS-23 certification is not part of the project. The payload capacity is supposed to be up to 5 kg, a flight duration of at least 90 days shall be possible and a position accuracy of less than 50m during payload operation shall be reached. To demonstrate the possibility to use inexpensive components, especially for the solar generator and batteries and gaining a high flexibility and band-with in the operation possibilities are special goals for the project to enable the German Aerospace Center and so the Federal Republic of Germany to play a major role in the future development of high altitude platforms for a wide range of applications.

5.1.2 DLR HAP Project Technical Overview

The HAP aircraft as shown in figure 5.2 provides three main services: position, attitude and electrical power, if needed, for a payload.

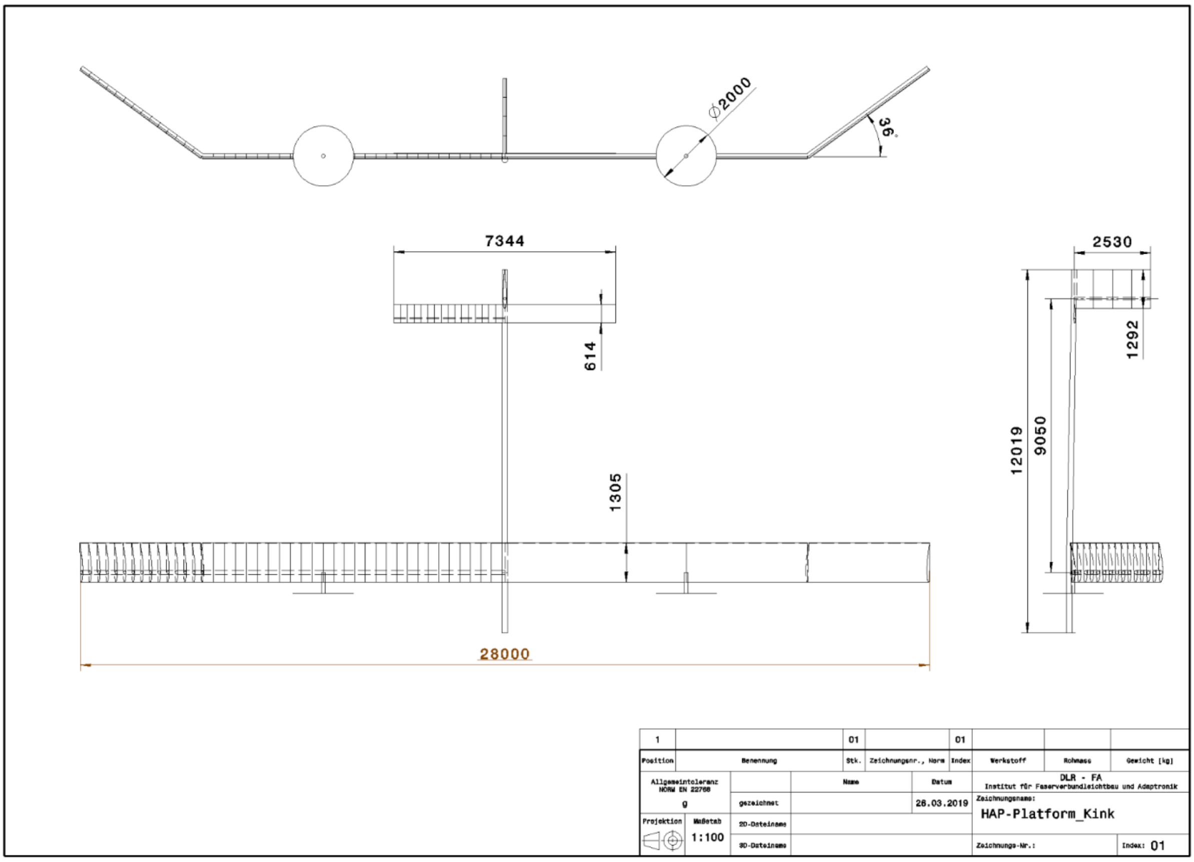


Figure 5.1: HAP three-sided view [14]

To provide these services there is a need for controlled start/landing, acceleration control, attitude control, electrical power provision and structural integration of the payload.

The components used to meet these needs are:

The *aircraft structure* to shape aerodynamic and dynamic properties of the aircraft, for structural integration of the payload and for controlled landing, as the aircraft will land without landing gear, using only friction between the aircraft structure and the ground to decelerate.

Two foldable *rotors* to provide controllable thrust and controlled landing. The rotos need to be foldable as the rotors need to be folded for controlled landing, otherwise they will touch the ground.

Movable *control surfaces* to change aerodynamic and dynamic properties of the aircraft structure.

A *power connection* to the payload.

A *start vehicle* for controlled start. The aircraft will start on top of a start vehicle using only friction between the aircraft structure and the start vehicle structure to be accelerated through the start vehicle.

To be able to abort the flight independently from the functionality of all other components a *termination device* will be added. The mechanism to provide this function is not finally decided upon yet, all discussed concepts would change the aerodynamics of the aircraft in a way that the new glide ratio forces the aircraft towards ground, even when all other components are out of control. The new glide ratio will still allow the aircraft to make distance while losing attitude, this must be considered for the decision making about when and if to use the termination component.

A ground crew is intended to operate the aircraft and the payload.

An overview of the intended technology to realize the functionality and controllability of these components is given in figure 5.2, which shows the the HAP system architecture modeled using SysML. To model the HAP system architecture four different levels of abstraction are used, level 0 to level 3. The model has a clear order, the complete HAP System is level 0. Level 1 shows the HAP-Sub Systems, which the HAP System consists of. Level 2 shows the Sub-Sub-Systems, which the Sub-Systems consist of. Level 3 shows the components, which the sub-sub-systems consist of.

This kind of modeling groups the components of which the HAP system consists of into "logical" groups by the type of function they are supposed to provide, which makes them mentally more manageable and lets them being designed somewhat independently. It does not provide a model of functionality, the functionality solely lies in the understanding of the components' functions and interactions of the person studying this model.

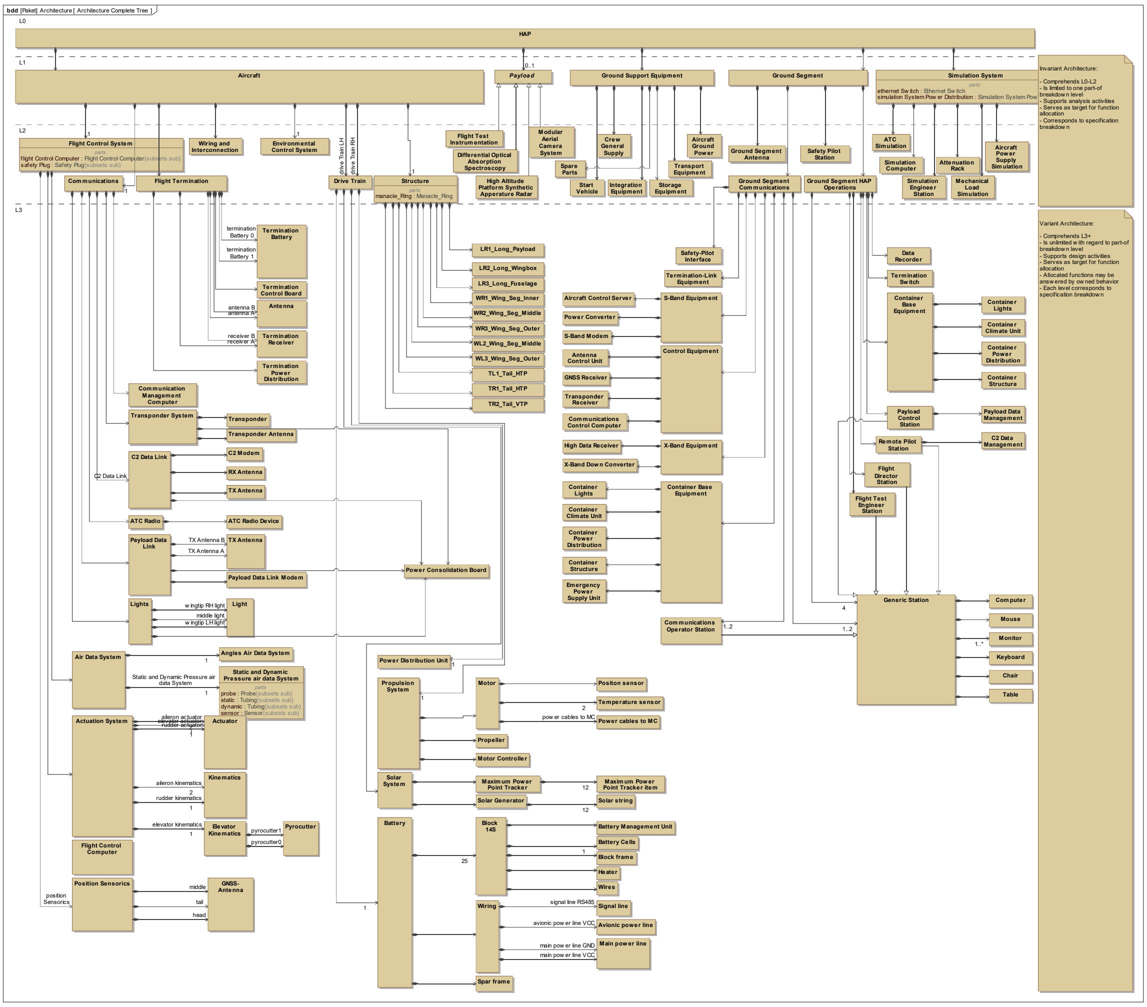


Figure 5.2: HAP System architecture modeled using SysML

The operations of the aircraft are divided in phases and sub-phases as shown in table C.3.

The aircraft is intended to be operated in three different main modes:

A mode in which the control surfaces' position and the rotors' **r**evolutions **p**er **m**inute (rpm) is controlled from a human operator on ground via remote control and line of sight feedback. This mode is used for the start and landing phase. Herein further called *Safety Mode*.

A mode in which a human operator on ground sends flight parameters, for example attitude angles, velocity and flight direction etc., to the aircraft's flight computer and the flight computer controls the control surfaces' position and the rotors' rpm, such that the aircraft fulfills these flight parameters. Herein further called *Remote Mode*.

A mode in which a human operator on ground sends waypoints to the aircraft's flight computer and the flight computer controls the control surfaces' position and the rotors' rpm, such that the aircraft follows these waypoints in its flight path. Herein further called *Waypoints Mode*.

The ground crew consists of:

Phase	Sub-Phase
Planning	Flight Planning
	Ground Operations/Flight Preparations
Ascent	Start
	Ascending Flight
Operating Altitude	Mission Flight
	Transfer Flight
	Energy Management Maneuver
	Emergency Maneuver
Descent	Descending Flight
	Landing Approach and Landing
Post-processing	Ground Operations/Post-processing

Table 5.1: HAP operational phases

The *Flight Director* has the mission and ground operations supervision, the obligation to start the flight part of a mission, the start sub-phase, and to terminate the flight.

The *Safety Pilot* controls the aircraft on sight in Safety Mode via remote control during the start and landing sub-phases. The Safety Pilot communicates with the Start Vehicle Driver to together operate the aircraft during the start sub-phase.

The *Remote Pilot* sets the aircraft mode, commands flight parameters during Remote Mode or waypoints during Waypoints Mode to the flight computer or gives the Safety Pilot the obligation to control the aircraft during Safety Mode. The Remote Pilot is the only human operator who directly speaks with the Testrange Control to request runway and airspace clearance. The Remote Pilot reports to the Flight Director the status of Test Range Control.

The *Start Vehicle Driver* drives the start vehicle during Safety Mode and communicates with the Safety Pilot to together operate the aircraft during the start sub-phase.

Testrange Control has the supervision of the testrange and airspace and gives testrange and airspace clearance and warnings to the Remote Pilot.

The *Flight Test Engineer* monitors critical flight parameters and ground operations parameters and gives warnings to the Flight Director and the Remote Pilot.

The goal of a STPA of this HAP system is to detect all potential accident scenarios existing through the combination and interaction of: the proposed design of the components, including the human operators in the system, the proposed operational procedures and the system environment.

5.2 DLR HAP STPA Application

Chapter 5.2 contains the application of STPA on the chosen parts of the HAP system described hereafter.

As proposed in the assignment of this thesis the STPA will be applied to a part of the HAP system, which is representative to investigate the applicability, benefits and completeness of STPA as a hazard analysis method for a HAP like complex system with its human operators.

For the 4 STPA steps the chosen representative parts are:

Step 1 in chapter 5.2.1: System-level losses, hazards and constraints refined to a high level system overview with focus on the start and landing sub-phases. The term *high level* in this thesis describes the level of analytical refinement represented in figure 5.4).

Step 2 in chapter 5.2.2: High level system overview.

Step 3 in chapter 5.2.3: High level system overview for the start sub-phase.

Step 4 in chapter 5.2.4: High level system overview for the start sub-phase for the Safety Pilot human operator for the attitude control action.

Additional documentation such as assumptions, comments and clarifications are added where considered necessary or helpful.

5.2.1 STPA Step 1: Losses, hazards and constraints

In a project the losses have to be identified by and agreed upon with the stakeholders. For the purpose of this master thesis the losses were chosen without consolidation of all the stakeholders, but with feedback of HAP system engineers. The potential error in step 1 is to overlook hazards, as the system-level hazards have to be complete, such that they are covering all potential hazards in the whole system, and there is no method to provide guidance to define these hazards, as explained in 3.1. For that reason it is to recommend to rather start defining the system-level hazards broad than too precise to allow later steps, 3 and 4, to detect more refined hazards.

The *HAP System* in this assessment is defined as the aircraft, start vehicle and the ground crew with its equipment, see system boundary in figure 5.4. The hazard assessment only analyzes scenarios which could lead the aircraft and the start vehicle to directly cause, direct physical cause, any of the defined losses, this includes the operations of the ground crew, the ground crew environment and the design and interaction of their equipment, for example ground crew equipment causes a fire which leads to ground crew not being able to provide their control actions, causing the aircraft to leave the intended airspace. It does not include the scenarios which could lead the ground crew, the ground crew environment or their equipment to directly cause any of the defined losses, for example ground crew equipment causes a fire in the ground crew building and there is no emergency evacuation plan for the ground crew, which leads to the death of the Flight Director. As a result the defined system-level hazards are hazards of the *aircraft/start vehicle sub-system* of the HAP System, which herein is defined as the aircraft and the start vehicle. In the following the identified losses, system-level hazards and system-level constraints will be given and discussed, when considered necessary, thereafter. The red highlighted parts are open decisions, which yet have to be made by the responsible engineers.

Losses

L-1: Loss of life or injury to people

L-2: Loss of or damage to the aircraft

L-3: Loss of or damage to the start vehicle

L-4: Loss of or damage to objects outside the aircraft/start vehicle

L-5: Loss of mission

L-6: Loss of sensitive information

System-level hazards

H-1: Aircraft in flight gets too close to other objects [L-1, L-2, L-3, L-4, L-5, L-6]

H-2: Controlled flight of aircraft into terrain [L-1, L-2, L-3, L-4, L-5, L-6]

H-3: Loss of aircraft/start vehicle control ability [L-1, L-2, L-3, L-4, L-5, L-6]

H-4: Aircraft/start vehicle structural integrity is lost [L-1, L-2, L-3, L-4, L-5, L-6]

H-5: Aircraft/start vehicle on ground gets too close to other objects [L-1, L-2, L-3, L-4, L-5]

H-6: Aircraft/start vehicle leaves designated runway [L-1, L-2, L-3, L-4, L-5]

H-7: System is unable to fulfill mission [L-5]

H-8: Aircraft leaves designated airspace [L-1, L-2, L-3, L-4, L-5, L-6]

System-level constraints

SC-1: Aircraft in flight must keep **to be d**iscussed (tbd) distance to other objects [H-1]

SC-2: Aircraft must not fly controlled into terrain [H-2]

SC-3: Aircraft/start vehicle control must be maintained [H-3]

SC-4: Aircraft/start vehicle structural integrity must be maintained [H-4]

SC-5: Aircraft/Start vehicle on ground must keep tbd distance to other objects [H-5]

SC-6: Aircraft/Start vehicle must stay in designated runway [H-6]

SC-7: System must be able to fulfill mission [H-7]

SC-8: Aircraft must not leave designated airspace [H-8]

Loss of sensitive information (L-6) in this assessment means the loss of flight hardware to a third party, for example parts of the aircraft landing on sites of third parties. *Third party* here means other than the DLR or the Test Range. The loss of other information is not considered in this assessment.

The mission loss (L-7) extends the hazard analysis to being able to detect hazards that are a threat to the functionality of the system. This might speak against the intuitive conception of safety, but note, that a safe system in STPA is defined as the system being free of the defined losses 3.1, which leaves it to the stakeholders to decide what safety for this project means. Without this loss, for example, it would not be necessarily considered a hazard if the aircraft would be unable to take off.

H-2, H-3 and H-8 could also be described as refined hazards of H-1 as they also describe situations where the aircraft gets too close to an object, but they are also refined hazards of H-7 and H-3 is also a refined hazard of H-4. This does not apply to H-6, as the start vehicle driving outside the runway can lead to the assigned losses without getting too close to an object, through the undefined ground the start vehicle is driving on. To avoid unnecessary repetition of the same hazards in the later refinement, H-2, H-3 and H-8 can also be described as system-level hazards as no information is lost and it gives a better overview. Note that the hazard refinement is not linked to any probability, STPA is a qualitative hazard assessment, with the goal of completeness of the identified causal scenarios.

H-7 is necessary as there can be no other hazards occurring, but the system is still unable to fulfill the mission (L-5).

The system-level hazard considerations of this assessment exclude all operational phases prior to start sub-phase and after the landing sub-phase. Such excluded hazards could be occurring to the system for example during transportation to the test range site, maintenance, taxiing to the runway and so on.

The start sub-phase in this assessment is defined as from the moment the aircraft/start vehicle system is standing still on the runway after taxiing has ended, note that this is before any start command has been given by any of the human operators on ground, until a not yet defined procedure declares the end of the start sub-phase, for example after the aircraft reaches a certain altitude or the start abortion is complete, the end of the start phase will be declared through human operator commands.

The landing sub-phase in this assessment is defined as from the moment a not yet defined procedure declares the beginning of the landing phase until the aircraft is standing still on the runway and a not yet defined procedure declares the ending of the landing sub-phase.

The term *in flight* in this assessment means the aircraft is separated from the start vehicle and not touching the ground with intention. The term *on ground* in this assessment means the aircraft is either attached to the start vehicle or touching the ground with intention during landing. The term *objects* in this assessment includes people, for example the Safety Pilot, and the ground.

The term *runway* in this assessment describes the surface on which the start vehicle is supposed to drive un during the start sub-phase and on which the aircraft is supposed to land on during the landing sub-phase.

The term *ground-space* in this assessment describes the space the aircraft/start vehicle is supposed to operate in while being on ground, this space can be wider and longer than the runway surface as parts of the aircraft start vehicle system, which are not intended to touch the ground, e.g the aircraft's wings, could reach into such wider/longer space. This definition is necessary to identify objects as hazards even if they are outside the runway, but reach into the ground-space.

The term *airspace* in this assessment describes the space the aircraft is supposed to operate in while being in flight.

The system-level hazards are refined with respect to flight phases and the HAP system design and then transformed into refined system-level constraints. As explained in chapter 3.1 this step is not necessary for all STPA applications, but for complex systems like HAP it helps comprehending the system complexity for modeling the safety control structure in step 2. The set of refined hazards will still have to be complete, which means it has to cover all potential hazards in the whole system, such that a refinement is only recommended where confidence about keeping completeness can be created. As the controllers have responsibilities, which will become control actions, and these responsibilities will be mapped to the safety constraints, refining the hazards and so the constraints will automatically lead to a more refined controller responsibility study and so to a more refined safety control structure.

The refined hazards can be found in appendix A.

5.2.2 STPA Step 2: Safety Control Structure

Chapter 5.2.2 contains the listing of the identified controller responsibilities, a gap analysis to the refined hazards and the modeling and discussion of the safety control structure.

Controller Responsibilities

The safety constraints for the start and landing sub-phases will be mapped to responsibilities of the different controllers existing through the HAP System design, a safety constraint can be provided by the combination of responsibilities of several controllers. The responsibilities were identified using the information described in the introduction of chapter 5. Even though it is not refined in the safety control structure, see figure 5.4, it is assumed for these responsibilities that the Safety Pilot uses a remote control to provide the control actions to the aircraft. Through the mapping it will become clear if there are safety constraints which are not represented in a controller responsibility yet in the existing design, which means this safety issue is unresolved in the existing design. This gap analysis result is the first analysis result of this assessment. If there would be no existing design yet, the safety control structure and so the design could be modeled such, that every safety constraint is represented in a controller responsibility. Everything in red color is an unresolved safety issue, either a definition is missing, or a safety constraint could not be assigned to one or several controller responsibilities. The definitions will have to implement the refined constraints, which they originate from. If a controller has no responsibilities during a certain phase, for example the automated controller during start/landing, this especially means that they are not allowed to provide any control action during this phase, which has to be provided by the technical and operational design.

The potential error at this step is overlooking to map a constraint in general or overlooking to map a constraint because it was not considered applicable to the analyzed phase. To resolve this issue it is to recommend to use some kind of STPA software tool, which automatically creates warnings, if constraints are not assigned to a responsibility yet. For this purpose it would be necessary to give the refined hazards a phase attribute, such that the software tool can check if the hazard is applicable for the analyzed phase. The software tool would have to be certified in some way or at least would have to provide access to the source code of the tool for the safety engineer to being able to check if the mapping and warnings are implemented correctly.

How feasible the responsibilities and their technical/operational implementations are to provide sufficient control fort he identified safety constraints will be analyzed in steps 3 and 4.

In this step it becomes clear why refining the hazards to the used level was useful, being able to map more detailed hazards to the identified responsibilities of the different controllers gives the ability to overview how well the current design already covers the existing hazards to a deeper level of the design. It must be noted, that the actual controller tasks will differ from this level of refinement, see for example the Safety Pilot's control actions in figure 5.4: the attitude control action will actually be moving levers on a remote control in a certain way. The final level of refinement in a safety assessment chosen for the safety control structure depends on the confidence the safety engineers have about their system understanding. This is a potential weakness of STPA, it is unclear if STPA is still practical, see for example the number of loss scenarios in chapter 5.2.4, if the safety control structure is refined all the way down to part level. But it is imaginable with the help of adequate STPA software as mentioned above. The level of refinement chosen, needs to be a level where the safety engineers can be sure the components on this level, in this case a component is everything that has a box in the safety control structure, can be treated as black boxes, meaning there is no interaction with other components other than the ones already identified for the component during the STPA, which means there is not only no additional physical interaction, but also there needs to be no additional knowledge about the current state of other components, out of system inputs or the system environment. The danger here is, just as in general with complex systems, the hidden interactions are not easy to anticipate as shown in chapter 3.

Note, that this potential weakness of STPA is less a weakness of the method, than rather the new boundary to which STPA extends the possible methodical analysis of complex systems including interaction failures. It can seem like other methods, see chapter 4, analyze complex systems all the way down to part level or all the way up from part level, but this is a creation of false confidence about system safety, as this analysis is only for failures of components, as in something does not work the way it is intended to, not for component interactions. The responsibilities for the Safety Pilot are shown in the following as an example, the complete responsibilities can be found in appendix B.

Safety Pilot

Start

R-1: Safety Pilot gives start command to Start Vehicle Driver after receiving start command from Remote Pilot [SC-1.1.2.1, SC-5.1.2.2, SC-5.3.2.1, SC-5.3.2.1]

R-2: Safety Pilot starts remote start together with Start Vehicle Driver after giving start command to Start Vehicle Driver [SC-1.1.2.1, SC-5.1.2.2]

R-3: Safety Pilot controls aircraft acceleration while attached to the Start Vehicle via remote control such that tbd acceleration constraints are not violated [SC-5.1.1.1.1]

R-4: Safety Pilot controls aircraft attitude (pitch, yaw, roll) while attached to the Start Vehicle via remote control such that it is not tilted towards Start Vehicle/ground during start [SC-5.1.1.1.3]

R-5: Safety Pilot controls aircraft attitude (pitch, yaw, roll) in flight via remote control such that it is not tilted towards Start Vehicle/ground during start [SC-1.1.1.1.1, SC-1.1.1.4.1]

R-6: Safety Pilot controls aircraft altitude change in flight via remote control such that it is not moved towards Start Vehicle/ground and does not violate tbd safety margin [SC-1.1.1.1.2, SC-1.1.1.4.2, SC-2.1, SC-8.1.1]

R-7: Safety Pilot controls aircraft planar flight direction and speed in flight via remote control such that, together with R-20, it is not moved towards Start Vehicle during start and such that it does not leave the designated airspace [SC-1.1.1.1.3, SC-8.1.1]

R-8: Safety Pilot monitors via sight that tbd aircraft safety margin of aircraft altitude minus altitude ground/objects on ground is not violated [SC-2.3]

SC-8.1.2: Who is responsible and what is the needed feedback, as only the Flight Director can terminate?

SC-3.1.1, SC-3.2.1: Who is responsible?

SC-4.1.2.1: How is made sure that the Safety Pilot does not violate structural maneuver constraints?

R-9: After receiving collision avoidance maneuver command from the Remote Pilot, the Safety Pilot evaluates in tbd way if he commands start abort to Start Vehicle Driver, collision avoidance maneuver to Start Vehicle Driver or/and he performs collision avoidance maneuver in flight in tbd way [SC-1.1.2.3, SC-5.1.2.3, SC-5.3.2.2]

Landing

R-10: Safety Pilot starts remote landing after receiving landing command from the Remote Pilot [SC-1.1.2.1, SC-5.2.2.1]

R-11: Safety Pilot controls aircraft attitude (pitch, yaw, roll) in flight and on ground via remote control such that it is not tilted towards ground during landing [SC-1.1.1.5.1, H-5.2.1.3.1]

R-12: Safety Pilot folds up aircraft rotors in flight via remote control when aircraft descents to tbd altitude during landing and keeps them folded up [SC-1.1.1.5.2, SC-5.2.1.3.2]

SC-4.1.2.1: How is made sure that the Safety Pilot does not violate structural maneuver constraints?

R-13: After receiving collision avoidance maneuver command from the Remote Pilot, the Safety Pilot performs collision avoidance maneuver in flight in tbd way [SC-1.1.2.3]

SC-5.2.2.3: Who is responsible and how is it intended to be implemented?

R-14: Safety Pilot lands aircraft via remote control in tbd way such that sufficient and symmetric enough deceleration is provided through friction of aircraft with ground that aircraft does not leave designated runway (SC-6.2.1, SC-6.2.2, SC-6.2.3)

R-15: Safety Pilot controls aircraft acceleration (xyz) via remote control such that it stays in tbd airspace (SC-8.1.1)

SC-8.1.2: Who is responsible and what is the needed feedback, as only the Flight Director can terminate?

Start and Landing

R-16: Safety Pilot stays out of designated runway and airspace during start/landing [SC-1.1.1.3.1, SC-5.1.1.2.1, SC-5.2.1.2.1, 5.3.1.1.1]

The responsibilities are transferred into control actions in the safety control structure. The potential error here is to forget a responsibility, a possible counter measure is to use a STPA software tool as described above. The control actions do not always represent the full responsibility, only the part that has to do with interaction with other components, internal tasks, like evaluation of certain situations for example, will influence the control action selection of the controllers in step 4. Control actions, which exist through the already existing intended design, not through safety considerations of the first step of the STPA, must be added during step 2 to be analyzed in steps 3 and 4 on how they can potentially be unsafe.

Safety Control Structure

It is critical that the safety control structure represents the actual intended design, such that the actual intended design is analyzed. For this thesis the information described in the introduction of chapter 5 was used to model the HAP design in the most actual way. As HAP is an ongoing project in the design phase, design changes are made and the safety control structure has to be verified to model the actual intended design, if it is supposed to be used for the project. The simulation system was not considered part of this assignment, for a complete STPA it must be added. Control actions for phases other than the start/landing sub phases were not transferred from refined hazards and so responsibilities, but assumed using the cited sources, as this assessment focuses on the start/landing sub phases. To analyze any other phases, these control actions must be transferred from refined hazards as well to be complete. As mentioned above these possible additional control actions influence the STPA results for the start/landing sub-phases in the way that they have to be checked to not being provided during the start/landing sub phases, in step 3, and scenarios need to be identified how they could be provided nevertheless, in step 4.

In general the hierarchy and notations as explained in chapter 3.1 are used in the safety control structure models, but for comprehensibility and as controllers can change their hierarchy towards each other depending on the phase of the mission, it is useful to additionally to the upwards and downwards arrows notation use different colors or other markers for the arrows, where controllers control each other reciprocally, such that both controllers can provide feedback and control actions to each other and there is a clear differentiation between those two categories. Coloring the arrows is not changing the characteristic of the safety control structure. An alternative is to put all controllers which control each other reciprocally on the same hierarchy level, but this results in a less comprehensible safety control structure. The notation used for this assessment is: The black downwards arrows and the red arrows represent control actions, the black upwards arrows and the blue arrows represent feedback or other information.

Figure 5.3 shows the top-level HAP system safety control structure, figure 5.4 shows the HAP system at the level of refinement used for this STPA. In figure 5.3 the main controllers, general control and feedback loops and the controlled process are shown. The HAP System is divided into two parts, the ground operations and the aircraft. The Ground Operations Crew controls the Physical Aircraft Processes either directly or through the Automated Controller on board of the aircraft. For the start a Start Vehicle is used which is also controlled by the Ground Operations Crew. The Ground Operations Crew is enabled and limited by commands by the out of the system boundary Test Range Control. All controllers can have out of system inputs from the system environment, the training they received and etc.

In figure 5.4 the safety control structure is further refined. The control and feedback loops, as existing in the intended design, are added. The different roles in the Ground Operations Crew and their interactions are shown. It becomes now obvious what control actions each controller has to fulfill, what feedback they are intended to receive, what feedback they are intended to give and so what parts of the system they influence and what parts of the system they are influenced by. It further becomes obvious who has what kind of influence on the aircraft. Take the Safety Pilot as an example: The Safety Pilot has to control their own position, to not get into the ground-space. The Safety Pilot receives start/landing/collision avoidance or abort commands from the Remote Pilot and has to control the aircraft's attitude, acceleration and the position of the foldable rotors accordingly and has to give the according commands to the Start Vehicle Driver. The Safety Pilot gives feedback to the Remote Pilot about the commands received and receives feedback from Start Vehicle Driver about the commands received. The Safety Pilot further receives feedback from the Start Vehicle Driver about the current speed of the Start Vehicle and so the aircraft. The Safety Pilot receives only line of sight feedback from the aircraft and the Start Vehicle. During all times the Automated Controller and the Flight Director also have the ability to influence the aircraft, but are not intended to do so during the Safety Pilot's regular operations. When the Safety Pilot has fulfilled their part of the operations, the Safety Pilot gives back the control to the Remote Pilot, who then controls the aircraft through the Automated Controller. The Safety Pilot receives feedback from the Remote Pilot when the Remote Pilot has taken over control of the aircraft.

The functionality of the technical implementations to carry out these interactions are then subject to further refinements of the safety control structure.

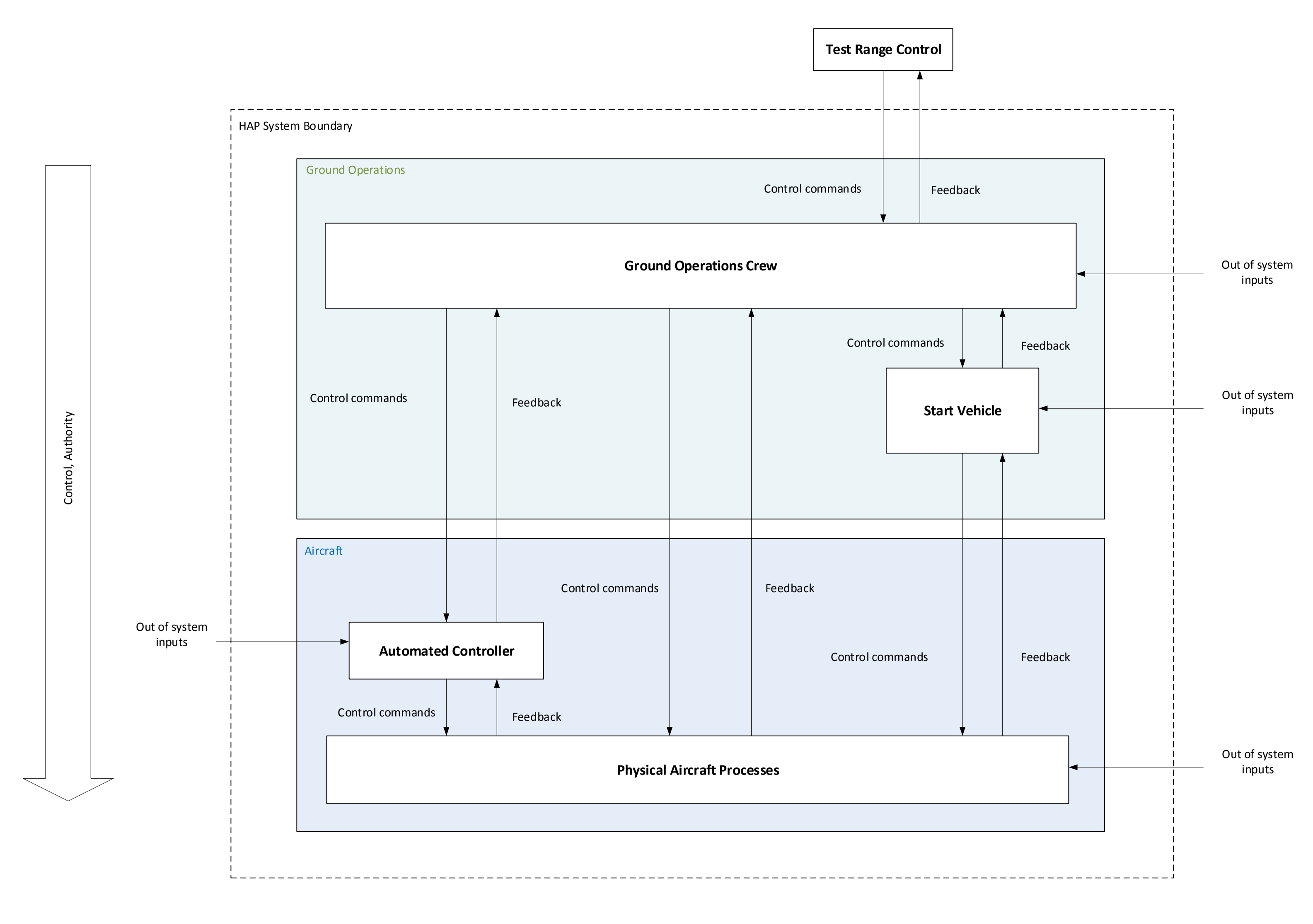


Figure 5.3: HAP safety control structure

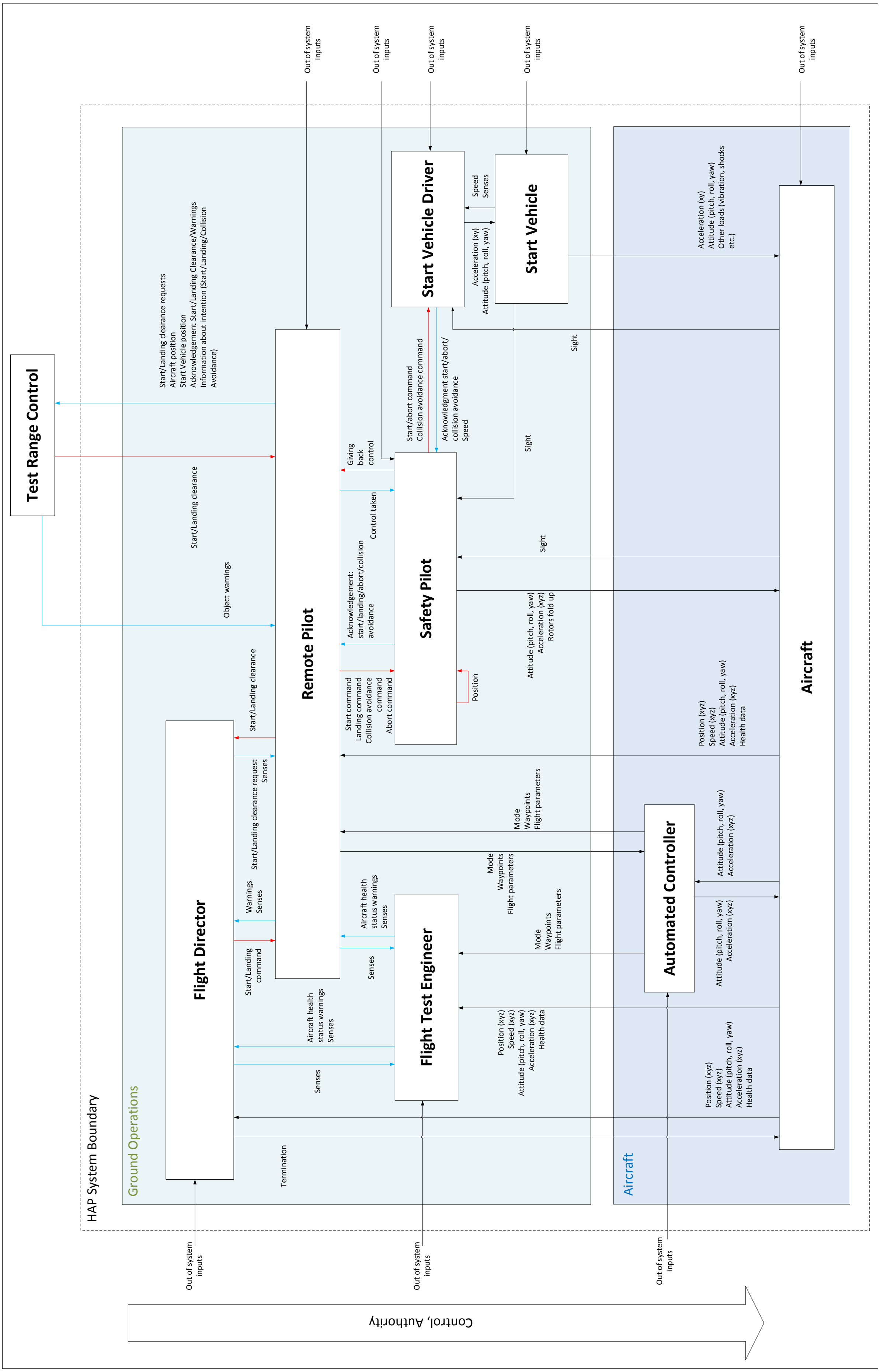


Figure 5.4: HAP safety control structure refined

The Flight Director, the Remote Pilot and the Flight Test Engineer are intended to be in the same room during operations, which means they can see and hear each other, this is represented in the feedback „senses" among them in the safety control structure.

Test Range Control is not part of the HAP system, which means it is analyzed during the STPA as it was assigned with responsibilities to prevent the identified hazards, but there is little influence on the design for the HAP system engineers. The mutual assumptions and the HAP operational concept must be clear for all parties. The exact necessities to clarify would be identified in STPA in step 3 and 4, which is not a part of this thesis as mentioned before.

The difference between feedback or other information and control actions is the decision making: Feedback is information or data, "This is a measurement result" or "This is a status", but no decision about what to do or not to do. Control actions include the decision to do or not to do something or the decision that something is safe or not safe to do as in the enabling control actions, for example the start clearance.

Sensors providing feedback can be smart in a way that they create information from data, like the Flight Test Engineer, who can use aircraft data to create information about the health status of the aircraft. The Flight Test Engineer does not decide if this information, the health status, enables the aircraft to start, this decision is made by the Flight Director. Test Range Control, on the contrary, does not only provide the information that the runway and the airspace are clear, it uses this information for the decision, that the aircraft is now allowed to start and gives start clearance. So, with not providing this control action, it directly influences the aircraft to not getting to close to other objects. The Flight Test Engineer withholding the information about the health status does not disable the Flight Director to command start, by operational rule, not by function. This operational design decision makes the aircraft health status from the Flight Test Engineer feedback and the start clearance from Test Range Control a control action.

Mistakes of this matter do not have a significant impact on the safety assessment: „It can also be helpful to realize that mistakes about who controls whom in the control structure usually do not have a significant impact on the results of the analysis. For example, suppose control action X is mischaracterized as feedback X. Because it is characterized as feedback, the step that identifies unsafe control actions will not consider how a missing or delayed control action X might lead to a hazard. However, the next step examines potential feedback problems and will identify the same scenarios when considering how missing or delayed feedback X might lead to a hazard." [8]

5.2.3 STPA Step 3: Unsafe Control Actions

Every control action identified in the safety control structure is now analyzed on how it can be unsafe during the start sub-phase and then mapped to the regarding refined hazards as described in chapter 3.1. Everything in red color is an unresolved safety issue. Examples of the unsafe control actions for the start sub-phase before takeoff are shown in table 5.2, the complete unsafe control actions can be found in appendix C.

The unsafe control actions are transferred into controller constraints, which are mapped to the unsafe control actions and can directly be transferred into controller requirements. Examples of the controller constraints for the start sub-phase before takeoff are shown in table 5.3, the complete controller constraints can be found in appendix D.

The four categories, the safety control structure and the safety constraints, which are mapped to the responsibilities, which were transferred into the control actions, give guidance to identify unsafe control actions. If control actions are added to the safety control structure, for example through the refinement of the safety control structure, the step of identifying unsafe control actions has to be done for the added control actions. An example is the remote control needed for the control path of the Safety Pilot. Refining the safety control structure adding the remote control, creates the control action of turning the remote control on. If control actions are added, which have been identified through the refinement of hazards of other operational phases for example and are so not needed for the start sub-phase, these control actions still have to undergo step 3 for the start sub-phase, to identify how these control actions can be unsafe in a way that they are provided during the start sub-phase.

An unsafe control action that is not identifiable in step 3 is a control action, which is not intended in the design, but added by a human controller, for example the Safety Pilot tells the Start Vehicle driver to accelerate at a higher rate. This kind of hazard will be identified in step 4.

It is assumed in this assessment that at the beginning of the start sub-phase the aircraft and start vehicle are ready for start with the correct health status at the designated runway start position, the rotors are folded down and all the human controllers and ground systems are ready for start and in position. To make sure this status exists at the beginning of the start sub-phase this must either be checked in the previous phase as an enabler of the start-sub phase or it must be added to the start sub-phase and its regarding hazard analysis. To be able to check if the HAP System is ready to start, the needed start status of all system components must be analyzed. The results of a STPA of the complete operational phases of the HAP System, for example the loss scenarios, can be used to identify these needs.

The chosen notation for the unsafe control actions and the controller constraints in the following section does not mention the operational phase for every unsafe control action/controller constraint as they are already sorted by the two operational sections: start sub-phase before takeoff and start sub-phase after takeoff. Those sections were differenced for this assessment as they represent the two sections with the most different operational and system status properties during the here analyzed start-sub phase. The whole start sub-phase could also be analyzed at once, with the regarding effects on comprehensibility for the safety engineer.

Takeoff herein means the aircraft is in flight as defined above and has no physical contact to the start vehicle.

The velocity *v1* is herein defined as the velocity of the start vehicle at which the start vehicle needs to start decelerating such that the deceleration rate does not cause unwanted movements of the aircraft on top of the start vehicle and the start vehicle has enough runway length left to not leave the runway. Depending on the start position and the acceleration rate of the start vehicle, this velocity can vary. This velocity is the operational point during the start-sub phase until which an abort of the start through the start vehicle driver is possible without further risks such as leaving the runway or decelerating out of the deceleration constraints.

H-7, is not being further considered in this assessment, as for comprehensiveness the focus is on the losses other than purely not being able to carry out a mission.

In this step human error will potentially lead to missing unsafe control actions and to missing mapping of hazards, especially when more refined levels of the safety control structure are used.

This is a potential weakness of the STPA method, but only against complete analytical safety rather than against other methods, which do not provide the guidance of the categories and the safety control structure as discussed in chapter 4. An independent review or an independent execution is to recommend for this step to catch potential human errors.

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	UCA-1: The Safety Pilot does not control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]	UCA-2: The Safety Pilot controls the aircraft attitude tbd insufficiently/exceeding [H-5.1.1.1.9, H-4.1.2.1] UCA-3: The safety Pilot controls the aircraft attitude such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-4: The Safety Pilot controls the aircraft attitude tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.9, H-4.1.2.1] UCA-5: The safety Pilot controls the aircraft attitude tbd time after external forces act on the aircraft [H-5.1.1.1.9, H-4.1.2.1]	UCA-6: The Safety Pilot stops controlling the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]
Safety Pilot	Acceleration (xyz)	UCA-7: The Safety Pilot does not control the aircraft acceleration [H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	UCA-8: The Safety Pilot controls the aircraft acceleration insufficiently (out of tbd acceleration constraints) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] UCA-9: The safety Pilot controls the aircraft acceleration such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-10: The Safety Pilot controls the aircraft acceleration tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] UCA-11: The safety Pilot controls the aircraft acceleration tbd time after external forces act on the aircraft [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]	UCA-12: The Safety Pilot stops controlling the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]
Safety Pilot	Rotors fold up	N/A	UCA-13: The Safety Pilot folds the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	UCA-14: The Safety Pilot gives start command to the Start Vehicle Driver before he got a start command from the Remote Pilot during start before takeoff [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-	UCA-16: The Safety Pilot gives start command to the Start Vehicle Driver tbd time after receiving start command from the Remote Pilot [H-	N/A

Table 5.2: Unsafe control actions start before takeoff

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	C-1: The Safety Pilot must control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]	C-2: The Safety Pilot must control the aircraft attitude tbd sufficiently/not exceeding [H-5.1.1.1.9, H-4.1.2.1] C-3: The safety Pilot must control the aircraft attitude such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-4: The Safety Pilot must control the aircraft attitude no later than tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.9, H-4.1.2.1] C-5: The safety Pilot must control the aircraft attitude no later than tbd time after external forces act on the aircraft [H-5.1.1.1.9, H-4.1.2.1]	C-6: The Safety Pilot must not stop controlling the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]
Safety Pilot	Acceleration (xyz)	C-7: The Safety Pilot must control the aircraft acceleration [H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	C-8: The Safety Pilot must control the aircraft acceleration sufficiently (in tbd acceleration constraints) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] C-9: The safety Pilot must control the aircraft acceleration such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-10: The Safety Pilot must control the aircraft acceleration no later than tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] C-11: The Safety Pilot must control the aircraft acceleration no later than tbd time after external forces act on the aircraft [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]	C-12: The Safety Pilot must not stop controlling the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]
Safety Pilot	Rotors fold up	N/A	C-13: The Safety Pilot must not fold the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	C-14: The Safety Pilot must not give start command to the Start	C-16: The Safety Pilot must give start command to the	N/A

Table 5.3: Controller constraints start before takeoff

5.2.4 STPA Step 4: Loss Scenarios

In chapter 5.2.4 the example loss scenarios for the Safety Pilot are identified.

As described in chapter 3.1, it is useful for this step to refine the safety control structure in a way that adds the sensor and actuator paths and the mental models and decision making of the human controllers. For the mental models and decision making of the human controllers, the approach described in 3.2 is used.

To analyze the loss scenarios involving the safety pilot, a cut out of the safety control structure is refined including all the interactions, which have potential influence on the Safety Pilot. This cut out is only possible without losing confidence about missing interactions with other components, as the safety control structure in figure 5.4 represents a HAP system model, which is already sorted by interactions. It is possible that a further refinement of the safety control structure in figure 5.4 visualizes hidden interactions, which would be missed in the way the safety control structure is cut here. The problem of missing such interactions is a problem of the level of refinement of the uncut safety control structure as discussed in chapter 5.2.2, but it becomes obvious why at this step 4 of the STPA; Identifying loss scenarios without exactly knowing the complete tasks of the controller makes the interaction assumption somewhat broad. An example: The level of refinement used in this assessment shows that the Safety Pilot has a radio voice link to communicate with the Start Vehicle Driver and it is assumed that the Safety Pilot uses a remote control to control the aircraft. It is not known if the Safety Pilot needs to use both hands to control the aircraft with the remote control, but also needs to use a hand to operate the device to communicate with the start vehicle driver, which both would not be possible at the same time.

When identifying loss scenarios related to response times, it useful is to keep in mind that the response time of the control system to a certain event consists of the time the sensors need to deliver data about the event to the controller, the time the controller needs for the decision making and to provide a control action and the time the actuator path needs to carry out a control action.

The refined and cut safety control structure is shown in figure 5.5. The mental model table is intentionally left blank for clarity reasons, the complete mental model table is described thereafter.

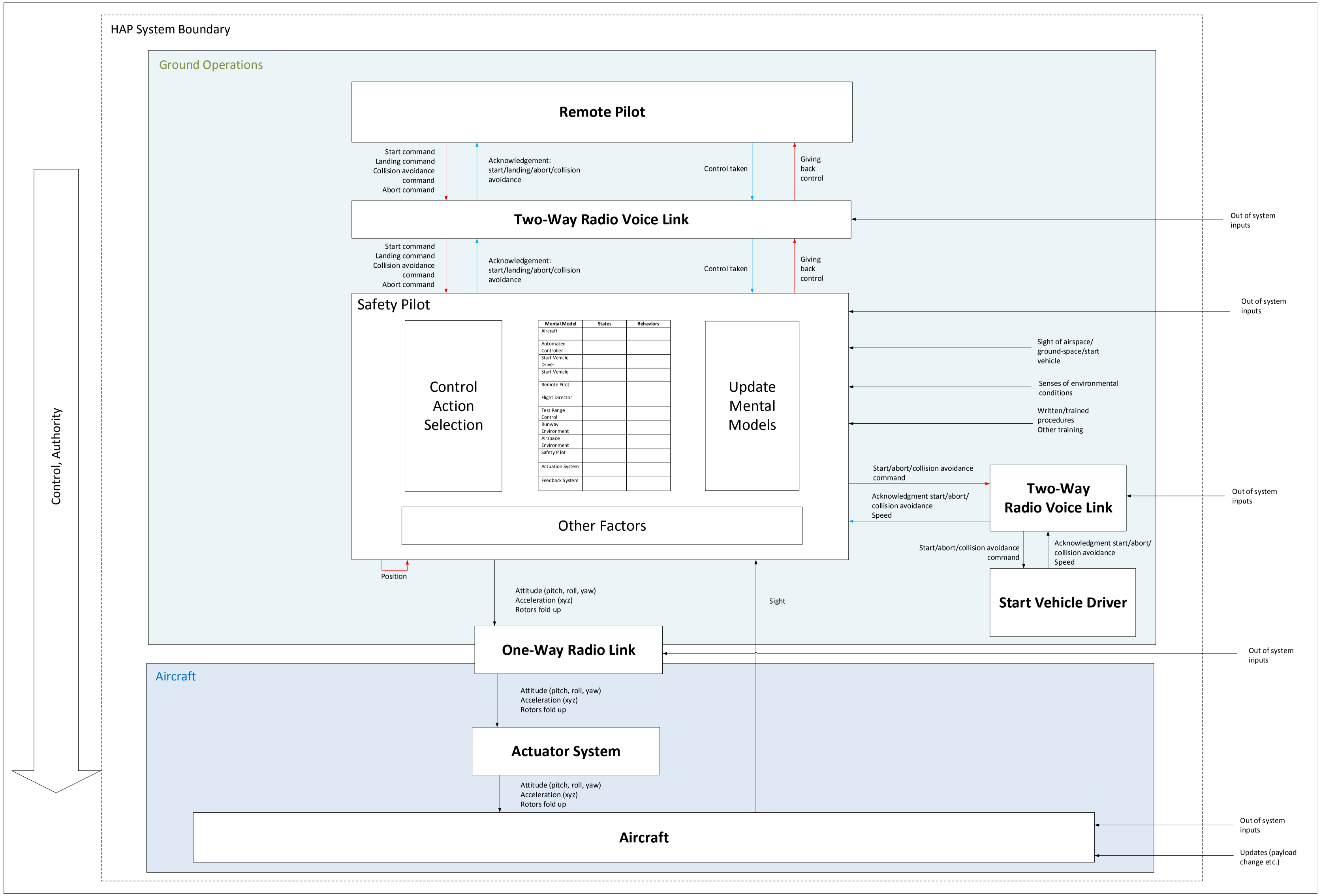


Figure 5.5: Safety Pilot refined safety control structure

Mental Models	States	Behaviors
Aircraft	Attached/in Flight Position (xyz) Attitude (pitch, roll, yaw) Acceleration (xyz) Rotors rpm Control surfaces position Configuration (including payload updates)	Reaction to remote control stick movements (change of state) including response time
Automated Controller	Modes	Behavior of each Mode: Controlling/Not controlling aircraft processes
Start Vehicle Driver	No Action Start Abort Collision Avoidance	Controlling start vehicle acceleration (xy) Controlling start vehicle attitude (pitch, roll, yaw) Response time
Start Vehicle	Position (xy) Acceleration (xy)	Reaction to start vehicle driver control actions
Remote Pilot	Modes No Action Start Abort Collision Avoidance	Changing/Not changing Mode Changing/Not changing states Response time
Flight Director	No Action Start Termination	Terminating/Not terminating
Test Range Control	Clearance given/No clearance given	Warning/Not warning if objects come in
Ground Space Environment	Clearance Wind Rain/Snow/Hail Humidity	Change of states

Continued on next page

Table 5.4: Safety Pilot mental models variables

Table 5.4 – continued from previous page

Mental Models	States	Behaviors
	Temperature Lightning Friction runway ground (ice, snow, water, dry, temperature) Particles Animals	
Airspace Environment	Clearance Wind Rain/Snow/Hail Humidity Temperature Radiation Lightning Particles Animals	Change of States
Safety Pilot	Position No Action Start Abort Collision Avoidance	Changing/Stayin in Position Need and way to control/Not control the aircraft depending on the automated controller mode and the action Reaction speed
Feedback System		Response time Correctness of response

Table 5.5: Safety Pilot mental models variables

The Safety Pilot's possible beliefs about the HAP System and it's environment, the Safety Pilot's mental models and the possible variables thereof, are identified using the safety control structure in figure 5.4. This table table 5.4 shown above is used to create the mental model flaws of the Safety Pilot for each unsafe control action. The Safety Pilot's possible believes about the actuator system response time are adressed in the Safety Pilot's possible believes about the response time of the aircraft to the Safety Pilot's remote control stick movements.

As explained in chapter 3.1 there are two types of loss scenarios, scenarios which lead to unsafe control actions and scenarios involving the control path. To provide guidance while creating the loss scenarios, the following template was created, combining the guidance given in the STPA Handbook [8] and the guidance given in the extension to STPA for human controllers [10].

Template to create unsafe control actions

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers.

2) Inadequate process model

Extension 1: Identify Mental Model variables

Extension 2: Identify Mental Model Flaws, identify all possible flaws, identify scenarios with flaws initially existing in the mental model

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers." [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

2) Inadequate feedback is received

b1) Scenarios involving the control path

1) Control action not executed

2) Control action improperly executed

b2) Scenarios related to the controlled process

1) Control action not executed

2) Control action improperly executed

All unsafe control actions have to be analyzed using the template for the type a scenarios, all control actions have to be analyzed using the template for the type b scenarios.

UCA-1 to UCA-6 were analyzed as an example for type a loss scenarios. The Safety Pilot's attitude control action was analyzed as an example for type b scenarios. The type a scenarios for UCA-1 and the type b scenarios for the attitude control action are shown in the following, the complete type a scenarios can be found in appendix E.

Somewhat hidden loss scenarios are such involving human controllers communicating things, which would de facto be a control action, but this control action is not intended in the system design. An example is the Safety Pilot telling the Start vehicle driver to accelerate at a higher rate. These scenarios have to be identified when analyzing the controller receiving the unintended control action, as it is only a loss scenario if it leads to an unsafe control action of the receiving controller. For example: The Start Vehicle Driver receives the command to accelerate at a higher rate, which leads the Start Vehicle Driver to accelerate out of acceleration constraints. Both controllers have to be trained to neither provide unintended control actions nor react to unintended control actions. Further, human operators having too many tasks at once can always lead to flawed control action selection or flawed mental model updates, as the feedback can be received but not being realized, for example the Safety Pilot sees an attitude change, but does not consciously receive it as the Safety Pilot is too busy with other tasks.

Ideas for possible actions to prevent the described loss scenarios are provided, but for these, as for all design changes, a reanalysis using STPA has to be done to analyze if they are not adding additional hazards to the system. For example wearing shaded glasses to protect the Safety Pilot from the sun rays potentially lowers the Safety Pilot's eyesight.

Type a scenarios for UCA-1: The Safety Pilot does not control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-1: The safety pilot has a medical condition during start before takeoff, including having to use a toilet or conditions caused by the Safety Pilot's environment for example particles in eye, insect bites, wind in eyes, struck by lightning etc., causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical checks right before start, protective gear: sunglasses/shaded airtight safety glasses, insects protection, being well hydrated, providing the possibility to use a toilet or similar, no start during lightning conditions.

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-1 are shown in E.1.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Safety Pilot		X	The Safety Pilot believes the Safety Pilot does not need to control the aircraft attitude during Start Phase when the current action is no action (start vehicle not moving before or after one of the other actions), regular start, abort or collision avoidance.
MM-2	Automated Controller	X		The Safety Pilot believes the Automated Controller is not in Safety Mode and so controls the aircraft attitude, when the Automated Controller is in Safety Mode and does not control the aircraft attitude.
MM-3	Automated Controller		X	The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude and so the Safety Pilot in Safety Mode does not need to control the aircraft attitude.
MM-4	Flight Director	X		The Safety Pilot believes the Flight Director Terminated the flight and so the Safety Pilot does not need to control the aircraft attitude, when the Flight Director did not terminate the flight.

Table 5.6: Safety Pilot mental model flaws for UCA-1

Scenario 2 for UCA-1: The Safety Pilot believes the Safety Pilot does not need to control the aircraft attitude during start before takeoff, when the current action is: no action, regular start, abort or collision avoidance [MM-1], causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot about the need to control the aircraft attitude when the current action is no action, regular start, abort or collision avoidance [MM-1] during start before takeoff, even when the start vehicle is not moving before the start or after abort or collision avoidance.

Scenario 3 for UCA-1: The Safety Pilot believes the Automated Controller is not in Safety Mode and so controls the aircraft attitude, when the Automated Controller is in Safety Mode and does not control the aircraft attitude [MM-2] during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot that the Automated Controller is in Safety Mode during start before takeoff.

Scenario 4 for UCA-1: The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude and so the Safety Pilot in Safety Mode does not need to control the aircraft attitude [MM-3] during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot that the Automated Controller in Safety Mode does not control the aircraft attitude.

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 5 for UCA-1: The Safety Pilot gets the impression from the aircraft behavior that there is no need for the Safety Pilot to control the aircraft attitude during the start before takeoff when the current action is no action, regular start, abort or collision avoidance. [MM-3] This causes the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Train the Safety Pilot about the need to always control the aircraft attitude during start before takeoff, no matter the Safety Pilot's impressions of the aircraft dynamics during simulator training. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 6 for UCA-1: The Safety Pilot gets the command from the Remote Pilot that there is no need for the Safety Pilot to control the aircraft attitude during the start before takeoff when the current action is no action, regular start, abort or collision avoidance. [MM-3] This causes the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Train the Safety Pilot about the control hierarchy and control actions, such that he is aware to ignore invalid commands from other controllers.

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

Scenario 7 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but he decides, due to personal experience with similar aircraft, lack of training with this aircraft, training with this aircraft that indicated to him he does not need to control the attitude etc., that it is safe not to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator training that shows the Safety Pilot that it is needed. Telling the Safety Pilot about this causal scenario and making him understand it.

If simulators are used, they provide new hazards, such as differences in model and reality, simulator software flashed on flight hardware etc., which have to be analyzed in another STPA.

Scenario 8 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but he decides the sight attitude feedback received makes it unclear if controlling the attitude actually causes more harm than to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot about how to judge the received feedback, simulator practice with similar to reality attitude sight feedback.

Scenario 9 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but the Safety Pilot has too much to do or the Safety Pilot did not get enough training,for example just read a manual once, that the Safety Pilot forgets or decides not to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with evaluation if the Safety Pilot provided all control actions.

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers." [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

N/A, if the sight is disturbed this only leads to UCA-2, for sensor problems see Scenario 1

2) Inadequate feedback is received

N/A, stopping to control the aircraft attitude is UCA-6

Type b scenarios for the Safety Pilot's attitude (pitch, roll, yaw) control action

It might be useful to give all control actions a number, just as the unsafe control actions, to make it easier to track if all control actions where analyzed regarding loss scenarios of type

b. Also some type of software that raises awareness of some kind if there are no type b loss scenarios for a control action yet, is to recommend to avoid human errors.

There needs to be a too late/to early, stopped too soon/applied too long, too fast/too slow, for example angle change rate control surfaces, category for type b scenarios. Even if there is no controller, so no decision making, involved, these are needs the intended design will have to fulfill.

For the case b scenarios no possible actions are given to mitigate the risks, as the actual design was not analyzed here, rather the needs an intended design will have to fulfill.

b1) Scenarios involving the control path

1) Control action not executed

Scenario 1: The Safety Pilot changes the sticks on the remote control to provide the attitude control action, but there is no attitude control signal sent from the remote control, for example because it is turned off, it has no power, it is broken, there is a design error etc., which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 2: The attitude control signal is sent from the remote control, but not received from the actuator system, because the signal is too weak, disturbances on the way to the receiver, inadequate receiver, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 3: The attitude control actuator system received the signal but does but not react to it due to inadequate design or malfunction, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

2) Control action improperly executed, executed when it should not have been, too late, too soon, too long, to short, wrong rates: too fast, too slow etc

Scenario 4: The Safety Pilot changes the sticks on the remote control to provide the attitude control action, but there is an inadequate attitude control signal sent from the remote control as in signal sent too late, control action represented by signal is too long, to short, wrong change rates , for example because the remote control has no power, it is broken, there is a design error etc., causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 5: The Safety Pilot does not change the sticks on the remote control, but there is an attitude control signal sent from the remote control causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 6: The attitude control signal is sent from the remote control, but inadequately received from the actuator system as in signal received too late, control action represented by signal is too long, to short, wrong change rates etc., for example because the signal is too weak, disturbance on the way to the receiver, receiver inadequate etc., causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 7: The signal is not sent from the remote control, but the actuator system receives a signal, which it interprets as valid attitude control signal, for example random signal wrongly interpreted as attitude control signal or attitude control signal from a different transmitter, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 8: The attitude control actuator system received the signal but reacts inadequately as in reaction too late, applied too long, to short, wrong change rates etc. because of inadequate design or a malfunction, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 9: The actuator system did not receive an attitude control signal but acts as if an attitude control signal would have been received because of a malfunction or a design error, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

b2) Scenarios related to the controlled process

1) Control action not executed

Scenario 10: The actuator system does apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does not react because there is not enough power of the control action, environmental disturbances to the control action, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 11: The actuator system does apply the attitude control action, the process, here the control surfaces and probably rotor rpm if used for attitude control, does react to the control action, but the aircraft attitude does not change because of a control surfaces design error or environmental disturbances, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

2) Control action improperly executed, executed when it should not have been, too late, too soon, too long, to short, wrong rates: too fast, too slow etc.

Scenario 12: The actuator system does apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does not react adequately as in too long, to short, wrong change rates etc. to the control action because there is not enough power of the control action or because of environmental disturbances, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 13: The actuator system does apply the attitude control action, the process, here the control surfaces and probably rotor rpm if used for attitude control, does react to the control action, but the aircraft attitude change improperly because of a control surfaces design error or environmental disturbances, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 14: The actuator system does not apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does react as if the control action would have been applied due to environmental disturbances, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

6 Summary and Conclusion

Two different approaches on achieving safety in a system have been described and discussed, the approach proposed by the ARP4754A in chapter 2 and the STAMP approach with the STPA hazard analysis method and the STPA extension for modeling and analyzing human operators in chapter 3.

In chapter 4, a comparison of the two approaches led to weaknesses being identified in the ARP4754A approach on how to analyze complex systems and so achieve complete and correct sets of safety requirements and their verification. The main point of critique is, that ARP4754A almost entirely relies on the engineers' understanding, the engineers' mental models, of a systems functionality and interactions. It has been discussed how STPA with providing a model of the functionality and interaction of the system and a structured approach on how to analyze the system based on this model can help on these weaknesses, such that better design decisions can be made, a more complete set of and more correct requirements can be found and a more complete verification of these requirements can be achieved to make the system safer.

The STPA method has then been applied on exemplary parts of the DLR HAP Project in chapter 5. Therein it has been found that STPA is applicable and beneficial to the afety assessment process in complex systems like HAP. An overview of the system functionality and interactions therein could be created quickly, several open safety issues have been identified. The safety control structure was found to be extremely helpful as a basis of discussion between experts of different parts of the project (design, operations, management) and for a better understanding of the functionality and the interactions of the complex system. The potential of STPA on more detailed levels of the design has been discussed. A model of a human operator has been embedded in the safety control structure, which enabled detailed and guided analysis of potential safety issues including the human operator, their tasks and environment. Causal scenarios, which can potentially lead to losses have been identified. Recommendations regarding the system and operations design and training procedures have been given on how to avoid these scenarios. General recommendations for the practical application of each certain STPA step have been identified and described including the use of STPA software and recommendations for attributes of such software.

Performing STPA on a complex system is not trivial, but the guidance to a more complete understanding of the system is exceptionally strong in comparison to the methods in proposed in ARP4754A. The confidence about the completeness of the found safety issues, and so the safety of the system, is in the end still the confidence of the safety engineer, but STPA gives a sound basis to justify this confidence.

Based on the results of chapters 4 and 5, this thesis finds that the risk in systems being certified using the ARP4754A approach on achieving safety is no longer acceptable, as the STAMP/STPA approach on achieving safety in a system can reduce this risk without unreasonable effort. This thesis therefore proposes to adapt STPA to the ARP4754A approach on how to achieve safety. One way of integrating STPA into this safety process can be:

Use STPA on the left side of the development V-cycle as shown in figure 2.5 instead of FHA, PRA and CMA. Use STPA results as a basis of the ZSA. For quantification perform FTA/DD/MA alongside STPA on each abstraction level using the STPA results of this level as a basis. Use STPA on the right side of the development V-cycle for a basis of FMEA/FMES and to develop testing and operator training.

This thesis further recommends to install a committee to push the development, or the certification of an already existing, STPA software package and use this STPA software package to assist in the processes mentioned above.

Bibliography

[1] T. Ishimatsu, N. Leveson, J. Thomas, and C. Fleming, *Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis.* Journal of Spacecraft and Rockets Vol. 51, No. 2, 2014.

[2] J. Chen, Y. Lu, S. Zhang, and P. Tang, *STPA-based Hazard Analysis of a Complex UAV System in Take-off.* 3rd International Conference on Transportation Information and Safety, Wuhan, P. R. China, 2015.

[3] EASA, *What is the status of 'Implementing Rules', 'Acceptable Means of Compliance' (AMC), 'Certification Specifications' (CS), Alternative Means of Compliance (AltMOC), 'Guidance Material' (GM), 'Special Conditions' and 'Frequently Asked Questions'(FAQ)?* 2019. [Online]. Available: `https://www.easa.europa.eu/faq/19117` (visited on 05/01/2020).

[4] SAE, *ARP 4754 REV. A.* 2010.

[5] SAE, *ARP 4761.* 1996.

[6] N. Leveson, *Engineering a Safer World - Systems Thinking Applied to Safety.* MIT Press, 2011, ISBN: 9780262016629.

[7] N. Leveson, *An STPA Primer Version 1.* 2013. [Online]. Available: `http://www.santoslab.org/pub/high-assurance/module-risk-management/reading/STPA-Primer-v0.pdf` (visited on 04/27/2020).

[8] N. Leveson and J. Thomas, *STPA Handbook.* 2018. [Online]. Available: `https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf` (visited on 04/21/2020).

[9] J. Thomas, *Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis.* 2013. [Online]. Available: `http://sunnyday.mit.edu/JThomas-Thesis.pdf` (visited on 04/25/2020).

[10] M. France, *Engineering for Humans: A New Extension to STPA.* 2017. [Online]. Available: `http://sunnyday.mit.edu/megan-thesis.pdf` (visited on 04/20/2020).

[11] J. Thomas, *System-Theoretic Process Analysis (STPA):Engineering for Humans.* 2019. [Online]. Available: `http://psas.scripts.mit.edu/home/wp-content/uploads/2019/04/STPA-Engineering-for-Humans.pdf` (visited on 04/27/2020).

[12] A. Bierig, F. Nikodem, and H. Schumann, *Hochfliegende unbemannte Plattform (HAP) Projektplan*, Version 1.0. 2019.

[13] S. Niemann, M. Rahm, and F. Nikodem, *Hochfliegende unbemannte Plattform (HAP) P2.1: Beschreibung Konfiguration*, Version 1.0. 2019.

[14] S. Kaltenhäuser, T. Mühlhausen, and I. Jessen, *Hochfliegende unbemannte Plattform (HAP) B1: Betriebskonzept (ConOps)*, Version 0.14. 2019.

A Refined System-level Hazards and Refined System-level Constraints

A.1 Refined H-1 and SC-1

H-1: Aircraft in flight gets too close to other objects [L-1, L-2, L-3, L-4, L-5, L-6]

H-1.1: Aircraft in flight gets too close to other objects during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1: Aircraft in flight gets too close to designated objects in airspace during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.1: Aircraft in flight gets too close to start vehicle during start [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.1.1: Aircraft attitude (pitch, yaw, roll) tilts aircraft towards start vehicle [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.1.2: Aircraft altitude change moves aircraft towards start vehicle [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.1.3: Aircraft planar flight direction moves aircraft towards start vehicle [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.2: Aircraft in flight gets too close to start vehicle during landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.2.1: Start vehicle gets into designated airspace during landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.3: Aircraft in flight gets too close to Safety Pilot during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.3.1: Safety Pilot gets into designated airspace during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.4: Aircraft in flight gets too close to ground during start [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.4.1: Aircraft attitude (pitch, yaw, roll) tilts aircraft towards ground [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.4.2: Aircraft altitude change moves aircraft towards ground [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.5: Aircraft in flight gets too close to ground during landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.5.1: Aircraft attitude (pitch, yaw, roll) tilts aircraft towards ground [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.5.1: Aircraft rotors are not folded up during landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.1.6: Aircraft in flight gets too close to other designated objects in airspace during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.2: Aircraft in flight gets too close to not-designated objects in airspace during start/landing [L-1, L-2, L-3, L-4, L-5]

H-1.1.2.1: Start/landing phase is started with an object being in the airspace [L-1, L-2, L-3, L-4, L-5]

H-1.1.2.2: An object enters the airspace after start/landing is started [L-1, L-2, L-3, L-4, L-5]

H-1.2: Aircraft in flight gets too close to other objects during all other flight phases [L-1, L-2, L-3, L-4, L-5, L-6]

SC-1: Aircraft in flight must keep tbd distance to other objects [H-1]

SC-1.1: Aircraft in flight must keep tbd distance to other objects during start/landing [H-1.1]

SC-1.1.1: Aircraft in flight must keep tbd distance to designated objects in airspace during start/landing [H-1.1.1]

SC-1.1.1.1: Aircraft in flight must keep tbd distance to start vehicle during start [H-1.1.1.1]

SC-1.1.1.1.1: Aircraft attitude (pitch, yaw, roll) must not tilt aircraft towards start vehicle [H-1.1.1.1.1]

SC-1.1.1.1.2: Aircraft altitude change must not move aircraft towards start vehicle [H-1.1.1.1.2]

SC-1.1.1.1.3: Aircraft planar flight direction and speed must not move aircraft towards start vehicle [H-1.1.1.1.3]

SC-1.1.1.2: Aircraft in flight must keep tbd distance to start vehicle during landing [H-1.1.1.2]

SC-1.1.1.2.1: Start vehicle must stay out of designated airspace during landing [H-1.1.1.2.1]

SC-1.1.1.3: Aircraft in flight must keep tbd distance to Safety Pilot during start/landing [H-1.1.1.3]

SC-1.1.1.3.1: Safety Pilot must stay out of designated airspace during start/landing [H-1.1.1.3.1]

SC-1.1.1.4: Aircraft in flight must keep tbd distance to ground during start [H-1.1.1.4]

SC-1.1.1.4.1: Aircraft attitude (pitch, yaw, roll) must not tilt aircraft towards ground [H-1.1.1.4.1]

SC-1.1.1.4.2: Aircraft altitude change must not move aircraft towards ground [H-1.1.1.4.2]

SC-1.1.1.5: Aircraft in flight must keep tbd distance to ground during landing [H-1.1.1.5]

SC-1.1.1.5.1: Aircraft attitude (pitch, yaw, roll) must not tilt aircraft towards ground [H-1.1.1.5.1]

SC-1.1.1.5.2: Aircraft rotors must be folded up when aircraft descents to tbd altitude together with go from health status if runway will be reached and must stay folded up [H-1.1.1.5.1]

SC-1.1.1.6: Aircraft in flight must keep tbd distance to other designated objects in airspace during start/landing [H-1.1.1.6]

SC-1.1.2: Aircraft in flight must keep tbd distance to not-designated objects in airspace during start/landing [H-1.1.2]

SC-1.1.2.1: Start/landing phase must not be started with an object being in the airspace [H-1.1.2.1]

SC-1.1.2.2: No other objects enter the airspace after start/landing is started [H-1.1.2.2]

SC-1.1.2.3: Other objects entering the airspace after start/landing must be detected, risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold [H-1.1.2.2]

SC-1.2: Aircraft in flight must keep tbd distance to other objects during all other flight phases [H-1.3]

SC-1.2.1: No other objects enter the airspace [H-1.2.2]

SC-1.2.2: Other objects entering the airspace must be detected, risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold [H-1.1.2]

A.2 Refined H-2 and SC-2

H-2: Controlled flight of aircraft into terrain [L-1, L-2, L-3, L-4, L-5, L-6]

H-2.1: Aircraft violates tbd safety margin of aircraft altitude minus altitude ground/objects on ground during start/landing [L-1, L-2, L-3, L-4, L-5, L-6]

H-2.2: Aircraft violates tbd safety margin of aircraft altitude minus altitude ground/objects on ground during all other flight phases [L-1, L-2, L-3, L-4, L-5, L-6]

SC-2: Aircraft must not flight controlled into terrain [H-2]

SC-2.1: Aircraft must not violate tbd safety margin of aircraft altitude minus altitude ground/objects on ground during start/landing [H-2.1]

SC-2.2: Aircraft must not violate tbd safety margin of aircraft altitude minus altitude ground/objects on ground during all other flight phases [H-2.2]

SC-2.3: If tbd aircraft safety margin of aircraft altitude minus altitude ground/objects on ground is violated risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold during start/landing [H-2.1]

SC-2.4: If tbd aircraft safety margin of aircraft altitude minus altitude ground/objects on ground is violated risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold during all other flight phases [H-2.2]

A.3 Refined H-3 and SC-3

H-3: Loss of aircraft/start vehicle control ability [L-1, L-2, L-3, L-4, L-5, L-6]

H-3.1: Loss of ability to control aircraft acceleration (xyz) [L-1, L-2, L-3, L-4, L-5, L-6]

H-3.2: Loss of ability to control aircraft attitude (pitch, roll, yaw) [L-1, L-2, L-3, L-4, L-5]

H-3.3: Loss of ability to control start vehicle acceleration (xy) [L-1, L-2, L-3, L-4, L-5]

H-3.4: Loss of ability to control start vehicle attitude (pitch, roll, yaw) [L-1, L-2, L-3, L-4, L-5]

SC-3: Aircraft/start vehicle control ability must be maintained [H-3]

SC-3.1: Ability to control aircraft acceleration (xyz) must be maintained [H-3.1]

SC-3.1.1: Ability to control aircraft acceleration (xyz) must be monitored and risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold [H-3.1]

SC-3.2: Ability to control aircraft attitude (pitch, roll, yaw) must be maintained [H-3.2]

SC-3.2.1: Ability to control aircraft attitude (pitch, roll, yaw) must be monitored and risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold [H-3.2]

SC-3.3: Ability to control start vehicle acceleration (xy) must be maintained [H-3.3]

SC-3.3.1: Ability to control start vehicle acceleration (xy) must be monitored and risk of not being able to provide services must be evaluated in tbd way, start vehicle must abort mission if risk passes tbd threshold is [H-3.3]

SC-3.4: Ability to control start vehicle attitude (pitch, roll, yaw) must be maintained [H-3.4]

SC-3.4.1: Ability to control start vehicle attitude (pitch, roll, yaw) must be monitored and risk of not being able to provide services must be evaluated in tbd way, start vehicle must abort mission if tbd risk threshold is reached [H-3.3]

A.4 Refined H-4 and SC-4

H-4: Aircraft/start vehicle structural integrity is lost [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.1: Aircraft structural integrity is lost [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.1.1: Aircraft structure does not withstand designated loads [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.1.2: Aircraft structure is exposed to not designated loads [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.1.2.1: Aircraft violates maneuver constraints [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.1.2.2: Aircraft operates in exceeding environmental conditions [L-1, L-2, L-3, L-4, L-5, L-6]

H-4.2: Start vehicle structural integrity is lost [L-1, L-2, L-3, L-4, L-5]

H-4.2.1: Start vehicle structure does not withstand designated loads [L-1, L-2, L-3, L-4, L-5]

H-4.2.2: Start vehicle structure is exposed to not designated loads [L-1, L-2, L-3, L-4, L-5]

H-4.2.2.1: Start vehicle violates maneuver constraints [L-1, L-2, L-3, L-4, L-5]

H-4.2.2.2: Start vehicle operates in exceeding environmental conditions [L-1, L-2, L-3, L-4, L-5, L-6]

SC-4: Aircraft/start vehicle structural integrity must be maintained [H-4]

SC-4.1: Aircraft structural integrity must be maintained [H-4.1]

SC-4.1.1: Aircraft structure must withstand designated loads [H-4.1.1]

SC-4.1.2: Aircraft structure must not be exposed to not designated loads [H-4.1.2]

SC-4.1.2.1: Aircraft must not violate maneuver constraints [H-4.1.2.1]

SC-4.1.2.2: Aircraft must not operate in exceeding environmental conditions [H-4.2.2.2]

SC-4.1.2.3: Environmental conditions and predictions must be evaluated before start and risk of exceeding environmental conditions must be evaluated in tbd way, if risk passes tbd threshold start must be postponed [H-4.2.2.2]

SC-4.1.2.4: Environmental conditions and predictions must be monitored and evaluated during operation and risk of exceeding environmental conditions must be evaluated in tbd way, if risk passes tbd threshold start must be postponed [H-4.2.2.2]

SC-4.2: Start vehicle structural integrity must be maintained [H-4.2]

SC-4.2.1: Start vehicle structure must withstand designated loads [H-4.2.1]

SC-4.2.2: Start vehicle structure must not be exposed to not designated loads [H-4.2.2]

SC-4.2.2.1: Start vehicle must not violate maneuver constraints [H-4.2.2.1]

SC-4.2.2.2: Start vehicle must not operate in exceeding environmental conditions [H-4.2.2.2]

A.5 Refined H-5 and SC-5

H-5: Aircraft/Start vehicle on ground gets too close to other objects [L-1, L-2, L-3, L-4, L-5]

H-5.1: Aircraft-start vehicle system (attached) gets too close to other objects [L-1, L-2, L-3, L-4, L-5]

H-5.1.1: Aircraft-start vehicle system (attached) gets too close to designated objects [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1: Aircraft attached to start vehicle gets too close to the start vehicle/ground [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.1: Excessive acceleration aircraft through rotors [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.2: Asymmetric acceleration aircraft through rotors [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.3: Excessive acceleration aircraft through control surfaces [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.4: Asymmetric acceleration aircraft through control surfaces [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.5: Excessive acceleration start vehicle [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.6: Asymmetric acceleration start vehicle [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.7: Excessive deceleration start vehicle [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.8: Asymmetric deceleration start vehicle [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.1.9: Aircraft attitude (pitch, yaw, roll) tilts aircraft towards start vehicle/ground [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.2: Aircraft-start vehicle system (attached) gets too close to the Safety Pilot [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.2.1: Safety Pilot gets into designated ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.1.1.3: Aircraft-start vehicle system (attached) gets too close to other designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.1.2: Aircraft-start vehicle system (attached) gets too close to not-designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.1.2.1: Start phase is started with an object being in the ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.1.2.2: An object enters the ground-space after start phase is started [L-1, L-2, L-3, L-4, L-5]

H-5.2: Aircraft on ground gets too close to other objects while being separated from the start vehicle (after landing) [L-1, L-2, L-3, L-4, L-5]

H-5.2.1: Aircraft on ground gets too close to designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.1: Aircraft on ground gets too close to start vehicle [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.1.1: Start vehicle gets into designated ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.2: Aircraft on ground gets too close to Safety Pilot [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.2.1: Safety Pilot gets into designated ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.3: Aircraft on ground gets too close to ground [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.3.1: Aircraft attitude (pitch, yaw, roll) tilts aircraft towards ground [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.3.2: Rotors are being unfolded [L-1, L-2, L-3, L-4, L-5]

H-5.2.1.4: Aircraft on ground gets too close to other designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.2.2: Aircraft on ground gets too close to not-designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.2.2.1: Landing phase is started with an object being in the airspace [L-1, L-2, L-3, L-4, L-5]

H-5.2.2.2: An object enters the ground-space after landing phase is started [L-1, L-2, L-3, L-4, L-5]

H-5.3: Start vehicle gets too close to other objects while being separated from the aircraft [L-1, L-2, L-3, L-4, L-5]

H-5.3.1: Start vehicle gets too close to designated objects in ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.3.1.1: Start vehicle gets too close to the Safety Pilot [L-1, L-2, L-3, L-4, L-5]

H-5.3.1.1.1: Safety Pilot gets into designated ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.3.1.2: Start vehicle gets too close to the aircraft [L-1, L-2, L-3, L-4, L-5]

H-5.3.1.3: Start vehicle gets too close to other designated objects in ground-space [L- 1, L-2, L-3, L-4, L-5]

H-5.3.2: Start vehicle gets too close to not-designated objects in the ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.3.2.1: Start phase is started with an object being in the ground-space [L-1, L-2, L-3, L-4, L-5]

H-5.3.2.2: An object enters the ground-space after start phase is started [L-1, L-2, L-3, L-4, L-5]

SC-5: Aircraft/Start vehicle on ground must keep tbd distance to other objects [H-5]

SC-5.1: Aircraft-start vehicle system (attached) must keep tbd distance to other objects [H-5.1]

SC-5.1.1: Aircraft-start vehicle system (attached) must keep tbd distance to other designated objects [H-5.1.1]

SC-5.1.1.1: Aircraft attached to start vehicle must keep tbd distance to the start vehicle/ground [H-5.1.1.1]

SC-5.1.1.1.1: Aircraft must not violate tbd acceleration constraints [H-5.1.1.1.1, 5.1.1.1.2, H-5.1.1.1.3, 5.1.1.1.4]

SC-5.1.1.1.2: Start vehicle must not violate tbd acceleration/deceleration constraints [H-5.1.1.1.5, 5.1.1.1.6, H-5.1.1.1.7, 5.1.1.1.8]

SC-5.1.1.1.3: Aircraft attitude (pitch, yaw, roll) must not tilt aircraft towards start vehicle/ground [5.1.1.1.9]

SC-5.1.1.2: Aircraft-start vehicle system (attached) must not get too close to the Safety Pilot [H-5.1.1.2]

SC-5.1.1.2.1: Safety pilot must stay out of designated runway [H-5.1.1.2.1]

SC-5.1.1.3: Aircraft-start vehicle system (attached) must not get too close to other designated objects in ground-space [H-5.1.1.3]

SC-5.1.2: Aircraft-start vehicle system (attached) must not get too close to not-designated objects in ground-space [H-5.1.2]

SC-5.1.2.1: Start phase must not be started with an object being on the runway [H-5.1.2.1]

SC-5.1.2.2: No other objects enter the runway after start phase is started [H-5.1.2.2]

SC-5.1.2.3: Other objects entering the runway after start must be detected, risk of collision must be evaluated in tbd way and aircraft must either start collision avoidance maneuver or be terminated if risk passes tbd threshold [H-5.1.2.2]

SC-5.2: Aircraft on ground must keep tbd distance to other objects while being separated from the start vehicle (after landing) [H-5.2]

SC-5.2.1: Aircraft on ground must keep tbd distance to designated objects on runway [H-5.2.1]

SC-5.2.1.1: Aircraft on ground must keep tbd distance to start vehicle [H-5.2.1.1]

SC-5.2.1.1.1: Start vehicle must stay out of designated ground-space [H-5.2.1.1.1]

SC-5.2.1.2: Aircraft on ground must keep tbd distance to Safety Pilot [H-5.2.1.2]

SC-5.2.1.2.1: Safety Pilot must stay out of designated ground-space [H-5.2.1.2.1]

SC-5.2.1.3: Aircraft on ground must keep tbd distance to ground [H-5.2.1.3]

SC-5.2.1.3.1: Aircraft attitude (pitch, yaw, roll) must not tilt aircraft towards ground [H-5.2.1.3.1]

SC-5.2.1.3.2: Rotors must stay folded up after landing [SC-5.2.1.3.2]

SC-5.2.1.4: Aircraft on ground must keep tbd distance to other designated objects on runway [H-5.2.1.4]

SC-5.2.2: Aircraft on ground must keep tbd distance to not-designated objects on runway[H-5.2.2]

SC-5.2.2.1: Landing phase must not be started with an object being in the runway [H-5.2.2.1]

SC-5.2.2.2: No other objects enter the runway after landing phase is started [H-5.2.2.2]

SC-5.2.2.3: Other objects entering the runway after landing must be detected, risk of collision must be evaluated in tbd way and aircraft must start collision avoidance maneuver in tbd way [H-5.1.2.2]

SC-5.3: Start vehicle must keep tbd distance to other objects while being separated from the aircraft [H-3]

SC-5.3.1: Start vehicle must keep tbd distance to designated objects on runway [SC-5.3.1]

SC-5.3.1.1: Start vehicle must keep tbd distance to the Safety Pilot [H-5.3.1.1]

SC-5.3.1.1.1: Safety Pilot must stay out of the runway [H-5.3.1.1.1]

SC-5.3.1.2: Start vehicle must keep tbd distance to the aircraft [H-5.3.1.2]

SC-5.3.1.3: Start vehicle must keep tbd distance to other designated objects on the runway [H-5.3.1.2]

SC-5.3.2: Start vehicle must keep tbd distance to not-designated objects on the runway [H-5.3.2]

SC-5.3.2.1: Start phase must not be started with an object being in the runway [H-5.3.2.1]

SC-5.3.2.2: No other objects enter the runway after landing phase is started [H-5.3.2.2]

SC-5.3.2.3: Other objects entering the runway during start phase must be detected, risk of collision must be evaluated in tbd way and start vehicle must start collision avoidance maneuver in tbd way [H-5.3.2.2]

A.6 Refined H-6 and SC-6

H-6: Aircraft/Start vehicle leaves designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.1: Start vehicle with Aircraft attached leaves designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.1.1: Deceleration is insufficient upon rejected takeoff or during collision avoidance maneuver [L-1, L-2, L-3, L-4, L-5]

H-6.1.2: Asymmetric deceleration maneuvers system off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.1.3: Asymmetric acceleration maneuvers system off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.2: Aircraft on ground leaves designated runway while being separated from the start vehicle (after landing) [L-1, L-2, L-3, L-4, L-5]

H-6.2.1: Deceleration is insufficient after landing [L-1, L-2, L-3, L-4, L-5]

H-6.2.2: Asymmetric deceleration maneuvers aircraft off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.2.3: Acceleration maneuvers aircraft off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.3: Start vehicle leaves designated runway while being separated from the aircraft [L-1, L-2, L-3, L-4, L-5]

H-6.3.1: Deceleration is insufficient after takeoff [L-1, L-2, L-3, L-4, L-5]

H-6.3.2: Asymmetric deceleration maneuvers start vehicle off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.3.3: Excessive acceleration is provided after takeoff [L-1, L-2, L-3, L-4, L-5]

H-6.3.4: Asymmetric acceleration maneuvers start vehicle off designated runway [L-1, L-2, L-3, L-4, L-5]

H-6.3.5: Steering maneuvers the start vehicle off the runway [L-1, L-2, L-3, L-4, L-5]

SC-6: Aircraft/Start vehicle must stay in designated runway [H-6]

SC-6.1: Start vehicle with Aircraft attached must stay in designated runway [L-1, L-2, L-3, L-4, L-5]

SC-6.1.1: Sufficient deceleration must be provided upon rejected takeoff or during collision avoidance maneuver [H-6.1.1]

SC-6.1.2: Asymmetric deceleration must not maneuver system off designated runway [H-6.1.2]

SC-6.1.3: Asymmetric acceleration must not maneuver system off designated runway [H-6.1.3]

SC-6.2: Aircraft on ground must not leave designated runway while being separated from the start vehicle (after landing) [H-6.2]

SC-6.2.1: Sufficient deceleration must be provided after landing [H-6.2.1]

SC-6.2.2: Asymmetric deceleration must not maneuver aircraft off designated runway [H-6.2.2]

SC-6.2.3: Acceleration must not maneuver aircraft off designated runway [H-6.2.3]

SC-6.3: Start vehicle must not leave designated runway while being separated from the aircraft [H-6.3]

SC-6.3.1: Sufficient deceleration must be provided after takeoff [H-6.3.1]

SC-6.3.2: Asymmetric deceleration must not maneuver start vehicle off designated runway [H-6.3.1]

SC-6.3.3: Excessive acceleration must not be provided after takeoff [H-6.3.3]

SC-6.3.4: Asymmetric acceleration must not maneuver aircraft off designated runway [H-6.3.4]

SC-6.3.5: Steering must not maneuver the start vehicle off the runway [H-6.3.6]

A.7 Refined H-7 and SC-7

H-7: System is unable to fulfill mission [L-5]

H-7.1: Aircraft is unable to fulfill mission [L-5]

H-7.2: Ground control is unable to fulfill mission [L-5]

H-7.2.1: Ground control cannot provide necessary services to keep aircraft in designated position at the designated time [L-5]

H-7.3: Payload is unable to fulfill mission [L-5]

H-7.3.1: Payload does not operate adequately when in right position at right time [L-5]

H-7.4: Payload Ground control is unable to fulfill mission [L-5]

H-7.4.1: Payload ground control cannot provide necessary services to keep payload operating adequately when in right position at right time [L-5]

SC-7: System must be able to fulfill mission [H-7]

SC-7.1: Aircraft must be able to fulfill mission [H-7.1]

SC-7.1.1: Aircraft must be able to be in designated position at the designated time [H-7.1.1]

SC-7.2: Ground control must be able to fulfill mission [H-7.2]

SC-7.2.1: Ground control must be able to provide necessary services to keep aircraft in designated position at the designated time [H-7.2.1]

SC-7.3: Payload must be able to fulfill mission [H-7.3]

SC-7.3.1: Payload must be able to operate adequately when in right position at right time [H-7.3.1]

SC-7.4: Payload Ground control must be able to fulfill mission [H-7.4]

SC-7.4.1: Payload ground control cannot provide necessary services to keep payload operating adequately when in right position at right time [H-7.4.1]

A.8 Refined H-8 and SC-8

H-8: Aircraft leaves designated airspace [L-1, L-2, L-3, L-4, L-5, L-6]

H-8.1: Aircraft leaves designated airspace during Start/Landing [L-1, L-2, L-3, L-4, L-5]

H-8.2: Aircraft leaves designated airspace during all other flight phases [L-1, L-2, L-3, L-4, L-5, L-6]

SC-8: Aircraft must not leave designated airspace [H-8]

SC-8.1: Aircraft must not leave designated airspace during Start/Landing [H-8.1]

SC-8.1.1: Sufficient acceleration (xyz) must be provided [H-8.1]

SC-8.1.2: Sufficiency of aircraft acceleration (xyz) must be monitored and risk of collision/leaving the airspace must be evaluated in tbd way and aircraft must either start avoidance maneuver or be terminated if risk passes tbd threshold [H-8.1]

SC-8.2: Aircraft leaves designated airspace during all other flight phases [H-8.2]

SC-8.2.1: Sufficient acceleration (xyz) must be provided [H-8.2]

SC-8.2.2: Suffiency of aircraft acceleration (xyz) must be monitored and risk of collision/leaving the airspace must be evaluated in tbd way and aircraft must either start avoidance maneuver or be terminated if risk passes tbd threshold [H-8.2]

B Controller Responsibilities

Safety Pilot

Start

R-1: Safety Pilot gives start command to Start Vehicle Driver after receiving start command from Remote Pilot [SC-1.1.2.1, SC-5.1.2.2, SC-5.3.2.1, SC-5.3.2.1]

R-2: Safety Pilot starts remote start together with Start Vehicle Driver after giving start command to Start Vehicle Driver [SC-1.1.2.1, SC-5.1.2.2]

R-3: Safety Pilot controls aircraft acceleration while attached to the Start Vehicle via remote control such that tbd acceleration constraints are not violated [SC-5.1.1.1.1]

R-4: Safety Pilot controls aircraft attitude (pitch, yaw, roll) while attached to the Start Vehicle via remote control such that it is not tilted towards Start Vehicle/ground during start [SC-5.1.1.1.3]

R-5: Safety Pilot controls aircraft attitude (pitch, yaw, roll) in flight via remote control such that it is not tilted towards Start Vehicle/ground during start [SC-1.1.1.1.1, SC-1.1.1.4.1]

R-6: Safety Pilot controls aircraft altitude change in flight via remote control such that it is not moved towards Start Vehicle/ground and does not violate tbd safety margin [SC-1.1.1.1.2, SC-1.1.1.4.2, SC-2.1, SC-8.1.1]

R-7: Safety Pilot controls aircraft planar flight direction and speed in flight via remote control such that (together with R-20) it is not moved towards Start Vehicle during start and such that it does not leave the designated airspace [SC-1.1.1.1.3, SC-8.1.1]

R-8: Safety Pilot monitors via sight that tbd aircraft safety margin of aircraft altitude minus altitude ground/objects on ground is not violated [SC-2.3]

SC-8.1.2: Who is responsible and what is the needed feedback (only the Flight Director can terminate)?

SC-3.1.1, SC-3.2.1: Who is responsible?

SC-4.1.2.1: How can the Safety Pilot fulfill structural maneuver constraints?

R-9: After receiving collision avoidance maneuver command from the Remote Pilot, the Safety Pilot evaluates in tbd way if he commands start abort to Start Vehicle Driver, collision avoidance maneuver to Start Vehicle Driver or/and he performs collision avoidance maneuver in flight in tbd way [SC-1.1.2.3, SC-5.1.2.3, SC-5.3.2.2]

Landing

R-10: Safety Pilot starts remote landing after receiving landing command from the Remote Pilot [SC-1.1.2.1, SC-5.2.2.1]

R-11: Safety Pilot controls aircraft attitude (pitch, yaw, roll) in flight and on ground via remote control such that it is not tilted towards ground during landing [SC-1.1.1.5.1, H-5.2.1.3.1]

R-12: Safety Pilot folds up aircraft rotors in flight via remote control when aircraft descents to tbd altitude (only during landing) and keeps them folded up [SC-1.1.1.5.2, SC-5.2.1.3.2]

SC-4.1.2.1: How can the Safety Pilot fulfill structural maneuver constraints?

R-13: After receiving collision avoidance maneuver command from the Remote Pilot, the Safety Pilot performs collision avoidance maneuver in flight in tbd way [SC-1.1.2.3]

SC-5.2.2.3: Who is responsible and how is it intended to be implemented?

R-14: Safety Pilot lands aircraft via remote control in tbd way such that sufficient and symmetric enough deceleration is provided through friction of aircraft with ground that aircraft does not leave designated runway (SC-6.2.1, SC-6.2.2, SC-6.2.3)

R-15: Safety Pilot controls aircraft acceleration (xyz) via remote control such that it stays in tbd airspace (SC-8.1.1)

SC-8.1.2: Who is responsible and what is the needed feedback (only the Flight Director can terminate)?

Start and Landing

R-16: Safety Pilot stays out of designated runway and airspace during start/landing [SC-1.1.1.3.1, SC-5.1.1.2.1, SC-5.2.1.2.1, 5.3.1.1.1]

Start Vehicle Driver

Start

R-17: Start Vehicle Driver controls Start Vehicle acceleration/deceleration while aircraft is attached via pedals and steering wheel such that tbd acceleration/deceleration constraints are not violated [SC-5.1.1.1.2]

R-18: Start Vehicle Driver controls Start Vehicle attitude (pitch, yaw, roll) via pedals and steering such that the aircraft is not tilted towards ground [SC-1.1.1.1.1, SC-1.1.1.4.1]

R-19: Start Vehicle Driver starts start phase together with Safety Pilot after receiving start command from Safety Pilot and not seeing unwanted objects in runway or airspace [SC-1.1.2.1, SC-5.1.2.2, SC-5.3.2.1]

R-20: Start Vehicle Driver controls Start Vehicle acceleration (xy) via pedals and steering wheel such that (together with R-7) it is not moved towards aircraft in flight during start and such that it is not maneuvered off designated runway (asymmetric acceleration/deceleration, deceleration after takeoff must be sufficient) [SC-1.1.1.1.3, SC-5.3.1.2, SC-6.1.3, SC-6.3.1, SC-6.3.2, H-6.3.3, H-6.3.4, H-6.3.6]

R-21: Start Vehicle Driver accelerates Start Vehicle such that tbd velocity at tbd point of runway is reached [SC-2.1]

R-22: Start Vehicle Driver monitors ability to accelerate Start Vehicle (xy) [SC-3.2.1]

SC-3.3.1, SC-3.4.1: Who is responsible?

SC-4.1.2.1, SC-4.2.2.1: How can the Start Vehicle Driver fulfill structural maneuver constraints?

R-23: After receiving start abort command or collision avoidance command the Start Vehicle Driver evaluates in tbd way the way to abort start/avoid collision and then aborts start/avoids collision in tbd way [SC-1.1.2.3, SC-5.1.2.3, SC-5.3.2.2, SC-6.1.1, SC-6.1.2]

Landing R-24: Start Vehicle Driver keeps Start Vehicle out of designated airspace and runway during landing [SC-1.1.1.2.1, SC-5.2.1.1.1]

Flight Director

Start and Landing

R-25: Flight Director requests start/landing clearance from the Remote Pilot [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

R-26: Flight Director gives start/landing command to the Remote Pilot only after receiving start/landing clearance from the Remote Pilot [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

SC-4.2.2.2, SC-6.2.3: Who is responsible?

R-27: After receiving termination recommendation from the Remote Pilot, the Flight Director terminates the aircraft [SC-1.1.2.3, SC-5.1.2.3]

Remote Pilot

Start and Landing

R-28: Remote Pilot reports aircraft position to the Test Range Control and requests start/landing clearance from Test Range Control after receiving start/landing clearance request from the Flight Director [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

R-29: Remote Pilot reports start/landing clearance to the Flight Director after receiving start/landing clearance from Test Range Control [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

R-30: Remote Pilot gives start/landing command to the Safety Pilot after receiving start/landing command from the Flight Director [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

R-31: After receiving a warning from RTC that other objects are in risk to enter runway/airspace during start/landing the Remote Pilot evaluates risk of collision in tbd way and either commands collision avoidance maneuver to Safety Pilot or recommends termination to Flight Director if risk passes tbd threshold [SC-1.1.2.3, SC-5.1.2.3, SC-5.3.2.1, SC-5.3.2.2]

Test Range Control

Start and Landing

R-32: After receiving start/landing clearance request from the Remote Pilot, Test Range Control makes sure no objects are and will not be in the runway/airspace during the time the aircraft and the Start Vehicle will be there and then gives start/landing clearance [SC-1.1.2.1, SC-5.1.2.2, SC-5.2.2.1, SC-5.3.2.1]

R-33: After giving start/landing clearance, Test Range Control does not give clearance to other objects to enter the runway/airspace until aircraft and Start Vehicle leave runway/airspace. Test Range Control warns other objects if there is a risk that they enter runway/airspace during that time [SC-1.1.2.2, SC-5.1.2.2, SC-5.2.2.2, SC-5.3.2.2]

R-34: Test Range Control gives a warning to the Remote Pilot if other objects are in risk to enter runway/airspace during start/landing [SC-1.1.2.3, SC-5.1.2.3, SC-5.3.2.2]

C Unsafe Control Actions

C.1 Unsafe Control Actions start sub-phase before takeoff

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	UCA-1: The Safety Pilot does not control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]	UCA-2: The Safety Pilot controls the aircraft attitude tbd insufficiently/exceeding [H-5.1.1.1.9, H-4.1.2.1] UCA-3: The safety Pilot controls the aircraft attitude such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-4: The Safety Pilot controls the aircraft attitude tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.9, H-4.1.2.1] UCA-5: The safety Pilot controls the aircraft attitude tbd time after external forces act on the aircraft [H-5.1.1.1.9, H-4.1.2.1]	UCA-6: The Safety Pilot stops controlling the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]
Safety Pilot	Acceleration (xyz)	UCA-7: The Safety Pilot does not control the aircraft acceleration [H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	UCA-8: The Safety Pilot controls the aircraft acceleration insufficiently (out of tbd acceleration constraints) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] UCA-9: The safety Pilot controls the aircraft acceleration such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-10: The Safety Pilot controls the aircraft acceleration tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] UCA-11: The safety Pilot controls the aircraft acceleration tbd time after external forces act on the aircraft [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]	UCA-12: The Safety Pilot stops controlling the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]
Safety Pilot	Rotors fold up	N/A	UCA-13: The Safety Pilot folds the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	UCA-14: The Safety Pilot gives start command to the Start Vehicle Driver before he got a start command from the Remote Pilot during start before takeoff [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-	UCA-16: The Safety Pilot gives start command to the Start Vehicle Driver tbd time after receiving start command from the Remote Pilot [H-	N/A

Continued on next page

Table C.1: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
			5.1.2.2 H-5.3.2.1, H-5.3.2.2] UCA-15: The Safety Pilot gives start command to the Start Vehicle Driver a second time [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	
Safety Pilot	Abort command tbd	UCA-17: The Safety Pilot does not give abort command to the Start Vehicle Driver after receiving abort command from the remote Pilot and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2] H-5.3.2.1, H-5.3.2.2]	UCA-18: The Safety Pilot gives abort command to the Start Vehicle Driver when abort is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-19: The Safety Pilot gives abort command to the Start Vehicle Driver tbd time after receiving abort command from the remote Pilot and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] UCA-20: The Safety Pilot gives abort command to the Start Vehicle Driver after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Safety Pilot	Collision avoidance command tbd	UCA-21: The Safety Pilot does not give Collision avoidance command to the Start Vehicle Driver after receiving collision avoidance command from the remote Pilot and collision avoidance is	UCA-22: The Safety Pilot gives collision avoidance command to the Start Vehicle Driver when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-23: The Safety Pilot gives collision avoidance command to the Start Vehicle Driver tbd time after receiving collision avoidance command from the remote Pilot and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A

Continued on next page

Table C.2: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]		UCA-24: The Safety Pilot gives collision avoidance command to the Start Vehicle Driver after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	
Safety Pilot	Position	UCA-25: The Safety Pilot is not in his tbd dedicated position [H-5.1.1.2.1]	N/A	N/A	UCA-26.1: The Safety Pilot leaves tbd dedicated position [H-5.1.1.2.1]
Safety Pilot	Giving back control	UCA-26: The Safety Pilot gives back control to the Remote Pilot [H-5.1.1.1.9, H-4.1.2.1 H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	N/A	N/A	N/A
Start Vehicle Driver	Acceleration (xy)	UCA-27: The Start vehicle driver does not control start vehicle acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-6.1] UCA-28: The Start vehicle driver does not control start vehicle acceleration after receiving abort/collision avoidance command [H-	UCA-29: The Start Vehicle Driver controls the start vehicle acceleration insufficiently (out of tbd acceleration constraints) [H-5.1.1.1.5, H-5.1.1.1.6, H-5.1.1.1.7, H-5.1.1.1.8, H-6.1.1, H-6.1.2, H-6.1.3, H-4.1.2.1, H-4.2.2.1] UCA-30: The Start Vehicle Driver controls the start vehicle acceleration such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-31: The Start vehicle driver controls start vehicle acceleration tbd time after the Safety Pilot starts accelerating the aircraft [H-5.1.1.1.1, H-5.1.1.1.2, H-4.1.2.1, H-4.2.2.1] UCA-32: The Start vehicle driver controls start vehicle acceleration tbd time after receiving abort/collision avoidance maneuver	UCA-33: The Start vehicle driver stops controlling start vehicle acceleration [H-5.1.1.1.7, H-5.1.1.1.8, H-6.1.1, H-6.1.2, H-4.1.2.1, H-4.2.2.1]

Continued on next page

Table C.3: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		1.1.2, H-4.1.2.1, H-4.2.2.1]		command from the Safety Pilot [H-1.1.2, H-4.1.2.1, H-4.2.2.1]	
Start Vehicle Driver	Attitude (pitch, yaw, roll)	UCA-34: The Start vehicle driver does not control start vehicle attitude [H-5.1.1.1.9, H-4.1.2.1]	UCA-35: The Start vehicle driver controls the start vehicle attitude tbd insufficiently [H-5.1.1.1.9, H-4.1.2.1] UCA-36: The Start vehicle driver controls the start vehicle attitude such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-37: The Start vehicle driver controls the start vehicle attitude tbd time after the start vehicle starts accelerating [H-5.1.1.1.9, H-4.1.2.1] UCA-38: The Start vehicle driver controls the start vehicle attitude tbd time after external forces act on the start vehicle [H-5.1.1.1.9, H-4.1.2.1]	UCA-39: The Start vehicle driver stops controlling the start vehicle attitude [H-5.1.1.1.9, H-4.1.2.1]
Start Vehicle (treated as actuator, not controller (no process model, no decision making, at least not one that we will look at during the design), therefore analysis in step 4). A risk consciously taken (in this safety assesment)!	N/A	N/A	N/A	N/A	N/A
Remote Pilot	Mode	UCA-40: The Remote Pilot has not set the Mode	UCA-41: The Remote Pilot sets the Mode “Waypoints” [H-4.1.2, H-	N/A	N/A

Continued on next page

Table C.4: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		"Safety" before start phase is started [H-4.1.2, H-5.1.2]	5.1.2] UCA-42: The Remote Pilot sets the Mode		
			"Remote" [H-4.1.2, H-5.1.2] UCA-43: The Remote Pilot sets the Mode "Safety" [H-4.1.2, H-5.1.2]		
Remote Pilot	Waypoints	N/A	N/A	N/A	N/A
Remote Pilot	Flight Parameters	N/A	N/A	N/A	N/A
Remote Pilot	Start command	N/A	UCA-44: The Remote Pilot gives start command to the Safety Pilot before he got start command from the Flight Director [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] UCA-45: The Remote Pilot gives start command to the Safety Pilot a second time [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-46: The Remote Pilot gives start command to the Safety Pilot tbd time after receiving start command from the Flight Director [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Landing command	N/A	UCA-47: The Remote Pilot gives landing command to the Safety Pilot [tbd]	N/A	N/A
Remote Pilot	Collision Avoidance command	UCA-48: The Remote Pilot does not give Collision avoidance command to the Safety Pilot after receiving a warning from Test Range Control and collision avoidance is	UCA-49: The Remote Pilot gives collision avoidance command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-50: The Remote Pilot gives collision avoidance command to the Safety Pilot tbd time after receiving a warning from Test Range Control and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A

Continued on next page

Table C.5: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Remote Pilot		appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2, H-5.3.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]		UCA-51: The Remote Pilot gives collision avoidance command to the Safety Pilot after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	
Remote Pilot	Abort command	UCA-52: The Remote Pilot does not give abort command to the Safety Pilot after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2] H-5.3.2.1, H-5.3.2.2]	UCA-53: The Remote Pilot gives abort command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-54: The Remote Pilot gives abort command to the Safety Pilot tbd time after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] UCA-55: The Remote Pilot gives abort command to the Safety Pilot after tbd v1 [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Start clearance	N/A	UCA-56: The Remote Pilot gives start clearance to the flight director without having received start clearance from test range control [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-57: The Remote Pilot gives start clearance to the flight director tbd time after receiving start clearance from test range control [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Landing clearance	N/A	N/A	N/A	N/A
Automated Controller	Attitude	N/A	UCA-58: The automated controller controls the aircraft attitude [H-5.1.1.9]	N/A	N/A

Continued on next page

Table C.6: Unsafe control actions start before takeoff

Table C.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Automated Controller	Acceleration	N/A	UCA-59: The automated controller controls the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4]	N/A	N/A
Flight Test Engineer (treated as a sensor, does not send any control actions, only feedback)	N/A	N/A	N/A	N/A	N/A
Flight Director	Start command	N/A	UCA-60: The Flight Director gives start command to the Remote Pilot before getting start clearance from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	UCA-61: The Flight Director gives start command to the Remote Pilot tbd time after receiving start clearance from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Flight Director	Landing command	N/A	UCA-62: The Remote Pilot gives landing command to the Remote Pilot [tbd]	N/A	N/A
Flight Director	Termination	UCA-63: The Flight Director does not terminate the flight when termination is tbd appropriate [tbd]	UCA-64: The Flight Director does terminate the flight when termination is tbd not appropriate [tbd]	UCA-65: The Flight Director does terminate the flight tbd time after termination is tbd appropriate [tbd]	N/A
Test Range Control	Landing clearance	N/A	N/A	N/A	N/A
Test Range Control	Start clearance	N/A	UCA-66: Test Range Control gives start clearance with an object being in or threatening to enter designated runway or airspace [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A	N/A

Table C.7: Unsafe control actions start before takeoff

C.2 Unsafe Control Actions start sub-phase after takeoff

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	UCA-67: The Safety Pilot does not control the aircraft attitude [H-1.1.1.1.1, H-1.1.1.4.1]	UCA-68: The Safety Pilot controls the aircraft attitude tbd insufficiently/exceeding [H-1.1.1.1.1, H-1.1.1.4.1] UCA-69: The safety Pilot controls the aircraft attitude such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-70: The Safety Pilot controls the aircraft attitude tbd time after takeoff [H-1.1.1.1.1, H-1.1.1.4.1] UCA-71: The safety Pilot controls the aircraft attitude tbd time after external forces act on the aircraft [H-1.1.1.1.1, H-1.1.1.4.1]	UCA-72: The Safety Pilot stops controlling the aircraft attitude before the remote pilot has taken over control [H-1.1.1.1.1, H-1.1.1.4.1]
Safety Pilot	Acceleration (xyz)	UCA-73: The Safety Pilot does not control the aircraft acceleration [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]	UCA-74: The Safety Pilot controls the aircraft acceleration insufficiently (out of tbd acceleration constraints) [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1] UCA-75: The safety Pilot controls the aircraft acceleration such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	UCA-76: The Safety Pilot controls the aircraft acceleration tbd time after takeoff [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1] UCA-77: The safety Pilot controls the aircraft acceleration tbd time after external forces act on the aircraft [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]	UCA-78: The Safety Pilot stops controlling the aircraft acceleration before the remote pilot has taken over control [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]
Safety Pilot	Rotors fold up	N/A	UCA-79: The Safety Pilot folds the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	UCA-80: The Safety Pilot gives start command to the Start Vehicle Driver [tbd]	N/A	N/A
Safety Pilot	Abort command tbd	UCA-81: The Safety Pilot does not give abort command to the Start Vehicle Driver after receiving abort	UCA-82: The Safety Pilot gives abort command to the Start Vehicle Driver when abort is inappropriate in tbd way [H-5.3.1.2]	UCA-83: The Safety Pilot gives abort command to the Start Vehicle Driver tbd time after receiving abort command from the	N/A

Continued on next page

Table C.8: Unsafe control actions start after takeoff

Table C.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		command from the remote Pilot and abort is appropriate [H-5.3.2]		remote Pilot and abort is appropriate [H-5.3.2]	
Safety Pilot	Collision avoidance command tbd	UCA-84: The Safety Pilot does not give Collision avoidance command to the Start Vehicle Driver after receiving collision avoidance command from the remote Pilot and collision avoidance is appropriate [H-5.3.2]	UCA-85: The Safety Pilot gives collision avoidance command to the Start Vehicle Driver when collision avoidance is inappropriate in tbd way [H-5.3.1.2]	UCA-86: The Safety Pilot gives collision avoidance command to the Start Vehicle Driver tbd time after receiving collision avoidance command from the remote Pilot and collision avoidance is appropriate [H-5.3.2]	N/A
Safety Pilot	Position	UCA-87: The Safety Pilot is not in his tbd dedicated position [H-1.1.1.3.1, H-5.3.1.1.1]	N/A	N/A	UCA-88: The Safety Pilot leaves tbd dedicated position before the next phase is started [H-1.1.1.3.1, H-5.3.1.1.1]
Safety Pilot	Giving back control	UCA-89: The Safety Pilot does not give back control to the Remote Pilot at the tbd end of the start phase [H-1.1.1, H-2.1, H-4.1.2, H-8]	N/A	UCA-90: The Safety Pilot gives back control to the Remote Pilot before tbd end of the start phase is reached [tbd]	N/A
Start Vehicle Driver	Acceleration (xy)	UCA-91: The Start vehicle driver does not control start vehicle acceleration [H-	UCA-93: The Start Vehicle Driver controls the start vehicle acceleration insufficiently (out of tbd acceleration constraints) [H-4.2.2.1,	UCA-94: The Start vehicle driver controls start vehicle acceleration tbd time after takeoff [H-4.2.2.1,	UCA-95: The Start vehicle driver stops controlling start vehicle acceleration

Continued on next page

Table C.9: Unsafe control actions start after takeoff

Table C.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		4.2.2.1, H-5.3.1.2, H-6.3] UCA-92: The Start vehicle driver does not control start vehicle acceleration after receiving abort/collision avoidance command [H-5.3.1.2, H-5.3.2]	H-5.3.1.2, H-6.3]	H-5.3.1.2, H-6.3]	before the next phase is started [H-6.3]
Start Vehicle Driver	Attitude (pitch, yaw, roll)	UCA-96: The Start vehicle driver does not control start vehicle attitude [H-4.2.2.1, H-5.3.1.2]	UCA-97: The Start vehicle driver controls the start vehicle attitude tbd insufficiently [H-4.2.2.1, H-5.3.1.2]	UCA-98: The Start vehicle driver controls the start vehicle attitude tbd time after takeoff [H-4.2.2.1, H-5.3.1.2] UCA-99: The Start vehicle driver controls the start vehicle attitude tbd time after external forces act on the start vehicle [H-4.2.2.1, H-5.3.1.2]	UCA-100: The Start vehicle driver stops controlling the start vehicle attitude before the next phase is started [H-5.3.1.2]
Start Vehicle (treated as actuator, not controller (no process model, no decision making, at least not one that we will look at during the design), therefore analysis in	N/A	N/A	N/A	N/A	N/A

Continued on next page

Table C.10: Unsafe control actions start after takeoff

Table C.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
step 4). A risk consciously taken (in this safety assesment)!					
Remote Pilot	Mode	UCA-101: The Remote Pilot does not set the Mode “Waypoints” or “Remote” after getting the “giving back control” command [H-1.1.1, H-4.1.2]	UCA-102: The Remote Pilot sets the Mode “Waypoints” before getting the “giving back control” command [H-1.1.1, H-4.1.2] UCA-102.1: The Remote Pilot sets the Mode “Remote” before getting the “giving back control” command [H-1.1.1, H-4.1.2] UCA-103: The Remote Pilot sets the Mode “Safety” [H-1.1.1, H-4.1.2]	UCA-104: The Remote Pilot sets the Mode “Waypoints” or “Remote” tbd time after getting the “giving back control” command [H-1.1.1, H-4.1.2]	N/A
Remote Pilot	Waypoints	N/A	N/A	N/A	N/A
Remote Pilot	Flight Parameters	N/A	N/A	N/A	N/A
Remote Pilot	Start command	N/A	UCA-105: The Remote Pilot gives start command to the Safety Pilot [tbd]	N/A	N/A
Remote Pilot	Landing command	N/A	UCA-106: The Remote Pilot gives landing command to the Safety Pilot [tbd]	N/A	N/A
Remote Pilot	Collision Avoidance command	UCA-107: The Remote Pilot does not give Collision avoidance command to the Safety Pilot after receiving a warning from Test Range Control and collision	UCA-108: The Remote Pilot gives collision avoidance command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.1, H-2.1, H-4.1.2.1, H-4.2.2.1, H-5.3.1, H-6.3, H-8.1]	UCA-109: The Remote Pilot gives collision avoidance command to the Safety Pilot tbd time after receiving a warning from Test Range Control and collision avoidance is appropriate [H-1.1.2 H-5.3.2]	N/A

Continued on next page

Table C.11: Unsafe control actions start after takeoff

Table C.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		avoidance is appropriate [H-1.1.2 H-5.3.2]			
Remote Pilot	Abort command	UCA-110: The Remote Pilot does not give abort command to the Safety Pilot after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2 H-5.3.2]	UCA-111: The Remote Pilot gives abort command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.1, H-2.1, H-4.1.2.1, H-4.2.2.1, H-5.3.1, H-6.3, H-8.1]	UCA-112: The Remote Pilot gives abort command to the Safety Pilot tbd time after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2 H-5.3.2]	N/A
Remote Pilot	Start clearance	N/A	N/A	N/A	N/A
Remote Pilot	Landing clearance	N/A	N/A	N/A	N/A
Automated Controller	Attitude	N/A	UCA-113: The automated controller controls the aircraft attitude [H-1.1.1, H-4.1.2]	N/A	N/A
Automated Controller	Acceleration	N/A	UCA-114: The automated controller controls the aircraft acceleration [H-1.1.1, H-4.1.2, H-8.1]	N/A	N/A
Flight Test Engineer (treated as a sensor, does not send any control actions, only feedback)	N/A	N/A	N/A	N/A	N/A
Flight Director	Start command	N/A	UCA-115: The Flight Director gives start command to the Remote Pilot [tbd]	N/A	N/A
Flight Director	Landing command	N/A	UCA-116: The Remote Pilot gives landing command to the Remote Pilot [tbd]	N/A	N/A

Continued on next page

Table C.12: Unsafe control actions start after takeoff

Table C.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Flight Director	Termination	UCA-117: The Flight Director does not terminate the flight when termination is tbd appropriate [tbd]	UCA-118: The Flight Director does terminate the flight when termination is tbd not appropriate [tbd]	UCA-119: The Flight Director does terminate the flight tbd time after termination is tbd appropriate [tbd]	N/A
Test Range Control	Landing clearance	N/A	N/A	N/A	N/A
Test Range Control	Start clearance	N/A	N/A	N/A	N/A

Table C.13: Unsafe control actions start after takeoff

D Controller Constraints

D.1 Controller Constraints start sub-phase before takeoff

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	C-1: The Safety Pilot must control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]	C-2: The Safety Pilot must control the aircraft attitude tbd sufficiently/not exceeding [H-5.1.1.1.9, H-4.1.2.1] C-3: The safety Pilot must control the aircraft attitude such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-4: The Safety Pilot must control the aircraft attitude no later than tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.9, H-4.1.2.1] C-5: The safety Pilot must control the aircraft attitude no later than tbd time after external forces act on the aircraft [H-5.1.1.1.9, H-4.1.2.1]	C-6: The Safety Pilot must not stop controlling the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]
Safety Pilot	Acceleration (xyz)	C-7: The Safety Pilot must control the aircraft acceleration [H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	C-8: The Safety Pilot must control the aircraft acceleration sufficiently (in tbd acceleration constraints) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] C-9: The safety Pilot must control the aircraft acceleration such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-10: The Safety Pilot must control the aircraft acceleration no later than tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1] C-11: The Safety Pilot must control the aircraft acceleration no later than tbd time after external forces act on the aircraft [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]	C-12: The Safety Pilot must not stop controlling the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4, H-4.1.2.1]
Safety Pilot	Rotors fold up	N/A	C-13: The Safety Pilot must not fold the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	C-14: The Safety Pilot must not give start command to the Start	C-16: The Safety Pilot must give start command to the	N/A

Continued on next page

Table D.1: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
			Vehicle Driver before he got a start command from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-15: The Safety Pilot must not give start command to the Start Vehicle Driver a second time [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	Start Vehicle Driver no later than tbd time after receiving start command from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	
Safety Pilot	Abort command tbd	C-17: The Safety Pilot must give abort command to the Start Vehicle Driver after receiving abort command from the remote Pilot and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2] H-5.3.2.1, H-5.3.2.2]	C-18: The Safety Pilot must not give abort command to the Start Vehicle Driver when abort is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-19: The Safety Pilot must not give abort command to the Start Vehicle Driver later than tbd time after receiving abort command from the remote Pilot and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-20: The Safety Pilot must not give abort command to the Start Vehicle Driver after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Safety Pilot	Collision avoidance command tbd	C-21: The Safety Pilot must give Collision avoidance command to the Start Vehicle Driver after receiving collision	C-22: The Safety Pilot must not give collision avoidance command to the Start Vehicle Driver when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-23: The Safety Pilot must give collision avoidance command to the Start Vehicle Driver no later than tbd time after receiving collision avoidance command from the	N/A

Continued on next page

Table D.2: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		avoidance command from the remote Pilot and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]		remote Pilot and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-24: The Safety Pilot must not give collision avoidance command to the Start Vehicle Driver after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	
Safety Pilot	Position	C-25: The Safety Pilot must be in his tbd dedicated position [H-5.1.1.2.1]	N/A	N/A	C-26: The Safety Pilot must not leave tbd dedicated position [H-5.1.1.2.1]
Safety Pilot	Giving back control	C-26: The Safety Pilot must not give back control to the Remote Pilot [H-5.1.1.1.9, H-4.1.2.1 H-5.1.1.1.3, H-5.1.1.1.4, H-5.1.1.1.5, H-5.1.1.1.6, H-4.1.2.1]	N/A	N/A	N/A
Start Vehicle Driver	Acceleration (xy)	C-27: The Start vehicle driver must control start vehicle acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-6.1] C-28: The Start vehicle driver	C-29: The Start Vehicle Driver must control the start vehicle acceleration sufficiently (in tbd acceleration constraints) [H-5.1.1.1.5, H-5.1.1.1.6, H-5.1.1.1.7, H-5.1.1.1.8, H-6.1.1, H-6.1.2, H-6.1.3, H-4.1.2.1, H-4.2.2.1]	C-31: The Start vehicle driver must control start vehicle acceleration no later than tbd time after the Safety Pilot starts accelerating the aircraft [H-5.1.1.1.1, H-	C-33: The Start vehicle driver must not stop controlling start vehicle acceleration [H-5.1.1.1.7, H-5.1.1.1.8,

Continued on next page

Table D.3: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		must control start vehicle acceleration after receiving abort/collision avoidance command [H-1.1.2, H-4.1.2.1, H-4.2.2.1]	C-30: The Start Vehicle Driver must control the start vehicle acceleration such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	5.1.1.1.2, H-4.1.2.1, H-4.2.2.1] C-32: The Start vehicle driver must control start vehicle acceleration no later than tbd time after receiving abort/collision avoidance maneuver command from the Safety Pilot [H-1.1.2, H-4.1.2.1, H-4.2.2.1]	H-6.1.1, H-6.1.2, H-4.1.2.1, H-4.2.2.1]
Start Vehicle Driver	Attitude (pitch, yaw, roll)	C-34: The Start vehicle driver must control start vehicle attitude [H-5.1.1.1.9, H-4.1.2.1]	C-35: The Start vehicle driver must control the start vehicle attitude tbd sufficiently [H-5.1.1.1.9, H-4.1.2.1] C-36: The Start vehicle driver must control the start vehicle attitude such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-37: The Start vehicle driver must control the start vehicle attitude no later than tbd time after the start vehicle starts accelerating [H-5.1.1.1.9, H-4.1.2.1] C-38: The Start vehicle driver must control the start vehicle attitude no later than tbd time after external forces act on the start vehicle [H-5.1.1.1.9, H-4.1.2.1]	C-39: The Start vehicle driver must not stop controlling the start vehicle attitude [H-5.1.1.1.9, H-4.1.2.1]
Start Vehicle (treated as actuator, not controller (no process model, no decision making, at least not one that we will	N/A	N/A	N/A	N/A	N/A

Continued on next page

Table D.4: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
look at during the design), therefore analysis in step 4). A risk consciously taken (in this safety assessment)!					
Remote Pilot	Mode	C-40: The Remote Pilot must set the Mode “Safety” before start phase is started [H-4.1.2, H-5.1.2]	C-41: The Remote Pilot must not set the Mode “Waypoints” [H-4.1.2, H-5.1.2] C-42: The Remote Pilot must not set the Mode “Remote” [H-4.1.2, H-5.1.2] C-43: The Remote Pilot must not set the Mode “Safety” [H-4.1.2, H-5.1.2]	N/A	N/A
Remote Pilot	Waypoints	N/A	N/A	N/A	N/A
Remote Pilot	Flight Parameters	N/A	N/A	N/A	N/A
Remote Pilot	Start command	N/A	C-44: The Remote Pilot must not give start command to the Safety Pilot before he got start command from the Flight Director [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-45: The Remote Pilot must not give start command to the Safety Pilot a second time [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-46: The Remote Pilot must give start command to the Safety Pilot no later than tbd time after receiving start command from the Flight Director [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Landing command	N/A	C-47: The Remote Pilot must not give landing	N/A	N/A

Continued on next page

Table D.5: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
			command to the Safety Pilot [tbd]		
Remote Pilot	Collision Avoidance command	C-48: The Remote Pilot must give Collision avoidance command to the Safety Pilot after receiving a warning from Test Range Control and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2, H-5.3.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-49: The Remote Pilot must not give collision avoidance command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-50: The Remote Pilot must give collision avoidance command to the Safety Pilot no later than tbd time after receiving a warning from Test Range Control and collision avoidance is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-51: The Remote Pilot must not give collision avoidance command to the Safety Pilot after tbd v1 is reached [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Abort command	C-52: The Remote Pilot must give abort command to the Safety Pilot after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2] H-5.3.2.1, H-5.3.2.2]	C-53: The Remote Pilot must not give abort command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-54: The Remote Pilot must give abort command to the Safety Pilot not later than tbd time after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2] C-55: The Remote Pilot must not give give abort command to the Safety Pilot after tbd v1 [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2	N/A

Continued on next page

Table D.6: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
				H-5.3.2.1, H-5.3.2.2]	
Remote Pilot	Start clearance	N/A	C-56: The Remote Pilot must not give start clearance to the flight director without having received start clearance from test range control [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-57: The Remote Pilot must give start clearance to the flight director no later than tbd time after receiving start clearance from test range control [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Remote Pilot	Landing clearance	N/A	N/A	N/A	N/A
Automated Controller	Attitude	N/A	C-58: The automated controller must not control the aircraft attitude [H-5.1.1.1.9]	N/A	N/A
Automated Controller	Acceleration	N/A	C-59: The automated controller must not control the aircraft acceleration [H-5.1.1.1.1, H-5.1.1.1.2, H-5.1.1.1.3, H-5.1.1.1.4]	N/A	N/A
Flight Test Engineer (treated as a sensor, does not send any control actions, only feedback)	N/A	N/A	N/A	N/A	N/A
Flight Director	Start command	N/A	C-60: The Flight Director must not give start command to the Remote Pilot before getting start clearance from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	C-61: The Flight Director must give start command to the Remote Pilot no later than tbd time after receiving start clearance from the Remote Pilot [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A
Flight Director	Landing command	N/A	C-62: The Remote Pilot must not give landing command to the Remote	N/A	N/A

Continued on next page

Table D.7: Controller constraints start before takeoff

Table D.1 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
			Pilot [tbd]		
Flight Director	Termination	C-63: The Flight Director must terminate the flight when termination is tbd appropriate [tbd]	C-64: The Flight Director must not terminate the flight when termination is tbd not appropriate [tbd]	C-65: The Flight Director must terminate the flight no later than tbd time after termination is tbd appropriate [tbd]	N/A
Test Range Control	Landing clearance	N/A	N/A	N/A	N/A
Test Range Control	Start clearance	N/A	C-66: Test Range Control must not give start clearance with an object being in or threatening to enter designated runway or airspace [H-1.1.2.1, H-1.1.2.2, H-5.1.2.1, H-5.1.2.2 H-5.3.2.1, H-5.3.2.2]	N/A	N/A

Table D.8: Controller constraints start before takeoff

D.2 Controller Constraints start sub-phase after takeoff

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Safety Pilot	Attitude (pitch, yaw, roll)	C-67: The Safety Pilot must control the aircraft attitude [H-1.1.1.1.1, H-1.1.1.4.1]	C-68: The Safety Pilot must control the aircraft attitude tbd sufficiently/not exceeding [H-1.1.1.1.1, H-1.1.1.4.1] C-69: The safety Pilot must control the aircraft attitude such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-70: The Safety Pilot must control the aircraft attitude no later than tbd time after takeoff [H-1.1.1.1.1, H-1.1.1.4.1] C-71: The safety Pilot must control the aircraft attitude no later than tbd time after external forces act on the aircraft [H-1.1.1.1.1, H-1.1.1.4.1]	C-72: The Safety Pilot must not stop controlling the aircraft attitude before the remote pilot has taken over control [H-1.1.1.1.1, H-1.1.1.4.1]
Safety Pilot	Acceleration (xyz)	C-73: The Safety Pilot must control the aircraft acceleration [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]	C-74: The Safety Pilot must control the aircraft acceleration sufficiently (in tbd acceleration constraints) [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1] C-75: The safety Pilot must control the aircraft acceleration such that it is favorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]	C-76: The Safety Pilot must control the aircraft acceleration no later than tbd time after takeoff [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1] C-77: The safety Pilot must control the aircraft acceleration no later than tbd time after external forces act on the aircraft [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]	C-78: The Safety Pilot must not stop controlling the aircraft acceleration before the remote pilot has taken over control [H-1.1.1.1.2, H-1.1.1.1.3, H-1.1.1.4.2, H-2.1, H-4.1.2.1, H-8.1]
Safety Pilot	Rotors fold up	N/A	C-79: The Safety Pilot must not fold the rotors up [tbd]	N/A	N/A
Safety Pilot	Start command	N/A	C-80: The Safety Pilot must not give start command to the Start Vehicle Driver [tbd]	N/A	N/A
Safety Pilot	Abort command tbd	C-81: The Safety Pilot must give abort command	C-82: The Safety Pilot must not give abort command to the Start	C-83: The Safety Pilot must give abort command to	N/A

Continued on next page

Table D.9: Controller constraints start after takeoff

Table D.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		to the Start Vehicle Driver after receiving abort command from the remote Pilot and abort is appropriate [H-5.3.2]	Vehicle Driver when abort is inappropriate in tbd way [H-5.3.1.2]	the Start Vehicle Driver no later than tbd time after receiving abort command from the remote Pilot and abort is appropriate [H-5.3.2]	
Safety Pilot	Collision avoidance command tbd	C-84: The Safety Pilot must give Collision avoidance command to the Start Vehicle Driver after receiving collision avoidance command from the remote Pilot and collision avoidance is appropriate [H-5.3.2]	C-85: The Safety Pilot must not give collision avoidance command to the Start Vehicle Driver when collision avoidance is inappropriate in tbd way [H-5.3.1.2]	C-86: The Safety Pilot must give collision avoidance command to the Start Vehicle Driver no later than tbd time after receiving collision avoidance command from the remote Pilot and collision avoidance is appropriate [H-5.3.2]	N/A
Safety Pilot	Position	C-87: The Safety Pilot must be in his tbd dedicated position [H-1.1.1.3.1, H-5.3.1.1.1]	N/A	N/A	C-88: The Safety Pilot must not leave tbd dedicated position before the next phase is started [H-1.1.1.3.1, H-5.3.1.1.1]
Safety Pilot	Giving back control	C-89: The Safety Pilot must give back control to the Remote Pilot at the tbd end of the start phase [H-1.1.1, H-2.1, H-4.1.2, H-8]	N/A	C-90: The Safety Pilot must give back control to the Remote Pilot before tbd end of the start phase is reached [tbd]	N/A
Start Vehicle Driver	Acceleration (xy)	C-91: The Start vehicle driver must control	C-93: The Start Vehicle Driver must control the start vehicle acceleration	C-94: The Start vehicle driver must control start vehicle	C-95: The Start vehicle driver must

Continued on next page

Table D.10: Controller constraints start after takeoff

Table D.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		start vehicle acceleration [H-4.2.2.1, H-5.3.1.2, H-6.3] C-92: The Start vehicle driver must control start vehicle acceleration after receiving abort/collision avoidance command [H-5.3.1.2, H-5.3.2]	sufficiently (in tbd acceleration constraints) [H-4.2.2.1, H-5.3.1.2, H-6.3]	acceleration no later than tbd time after takeoff [H-4.2.2.1, H-5.3.1.2, H-6.3]	not stop controlling start vehicle acceleration before the next phase is started [H-6.3]
Start Vehicle Driver	Attitude (pitch, yaw, roll)	C-96: The Start vehicle driver must control start vehicle attitude [H-4.2.2.1, H-5.3.1.2]	C-97: The Start vehicle driver must control the start vehicle attitude tbd sufficiently [H-4.2.2.1, H-5.3.1.2]	C-98: The Start vehicle driver must control the start vehicle attitude no later than tbd time after takeoff [H-4.2.2.1, H-5.3.1.2] C-99: The Start vehicle driver must control the start vehicle attitude no later than tbd time after external forces act on the start vehicle [H-4.2.2.1, H-5.3.1.2]	C-100: The Start vehicle driver must not stop controlling the start vehicle attitude before the next phase is started [H-5.3.1.2]
Start Vehicle (treated as actuator, not controller (no process model, no decision making, at least not one that we will look at	N/A	N/A	N/A	N/A	N/A

Continued on next page

Table D.11: Controller constraints start after takeoff

Table D.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
during the design), therefore analysis in step 4). A risk consciously taken (in this safety assessment)!					
Remote Pilot	Mode	C-101: The Remote Pilot must set the Mode "Waypoints" or "Remote" after getting the "giving back control" command [H-1.1.1, H-4.1.2]	C-102: The Remote Pilot must not set the Mode "Waypoints" before getting the "giving back control" command [H-1.1.1, H-4.1.2] C-102.1: The Remote Pilot must not set the Mode "Remote" before getting the "giving back control" command [H-1.1.1, H-4.1.2] C-103: The Remote Pilot must not set the Mode "Safety" [H-1.1.1, H-4.1.2]	C-104: The Remote Pilot must set the Mode "Waypoints" or "Remote" no later than tbd time after getting the "giving back control" command [H-1.1.1, H-4.1.2]	N/A
Remote Pilot	Waypoints	N/A	N/A	N/A	N/A
Remote Pilot	Flight Parameters	N/A	N/A	N/A	N/A
Remote Pilot	Start command	N/A	C-105: The Remote Pilot must not give start command to the Safety Pilot [tbd]	N/A	N/A
Remote Pilot	Landing command	N/A	C-106: The Remote Pilot must not give landing command to the Safety Pilot [tbd]	N/A	N/A
Remote Pilot	Collision Avoidance command	C-107: The Remote Pilot must give Collision avoidance command to the Safety Pilot after	C-108: The Remote Pilot must not give collision avoidance command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.1, H-2.1, H-4.1.2.1, H-4.2.2.1, H-	C-109: The Remote Pilot must give collision avoidance command to the Safety Pilot no later than tbd time after receiving a warning	N/A

Continued on next page

Table D.12: Controller constraints start after takeoff

Table D.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		receiving a warning from Test Range Control and collision avoidance is appropriate [H-1.1.2 H-5.3.2]	5.3.1, H-6.3, H-8.1]	from Test Range Control and collision avoidance is appropriate [H-1.1.2 H-5.3.2]	
Remote Pilot	Abort command	C-110: The Remote Pilot must give abort command to the Safety Pilot after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2 H-5.3.2]	C-111: The Remote Pilot must not give abort command to the Safety Pilot when collision avoidance is inappropriate in tbd way [H-1.1.1, H-2.1, H-4.1.2.1, H-4.2.2.1, H-5.3.1, H-6.3, H-8.1]	C-112: The Remote Pilot must give abort command to the Safety Pilot no later than tbd time after receiving a warning from Test Range Control and abort is appropriate [H-1.1.2 H-5.3.2]	N/A
Remote Pilot	Start clearance	N/A	N/A	N/A	N/A
Remote Pilot	Landing clearance	N/A	N/A	N/A	N/A
Automated Controller	Attitude	N/A	C-113: The automated controller must not control the aircraft attitude [H-1.1.1, H-4.1.2]	N/A	N/A
Automated Controller	Acceleration	N/A	C-114: The automated controller must not control the aircraft acceleration [H-1.1.1, H-4.1.2, H-8.1]	N/A	N/A
Flight Test Engineer (treated as a sensor, does not send any control actions, only feedback)	N/A	N/A	N/A	N/A	N/A
Flight Director	Start command	N/A	C-115: The Flight Director must not give start command to the Remote Pilot [tbd]	N/A	N/A

Continued on next page

Table D.13: Controller constraints start after takeoff

Table D.2 – continued from previous page

Controller	Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Flight Director	Landing command	N/A	C-116: The Remote Pilot must not give landing command to the Remote Pilot [tbd]	N/A	N/A
Flight Director	Termination	C-117: The Flight Director must terminate the flight when termination is tbd appropriate [tbd]	C-118: The Flight Director must not terminate the flight when termination is tbd not appropriate [tbd]	C-119: The Flight Director must terminate the flight no later than tbd time after termination is tbd appropriate [tbd]	N/A
Test Range Control	Landing clearance	N/A	N/A	N/A	N/A
Test Range Control	Start clearance	N/A	N/A	N/A	N/A

Table D.14: Controller constraints start after takeoff

E Loss Scenarios type a UCA-1 to UCA-6

E.1 Loss Scenarios type a UCA-1

Type a scenarios for UCA-1: The Safety Pilot does not control the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-1: The safety pilot has a medical condition during start before takeoff, including having to use a toilet or conditions caused by the Safety Pilot's environment for example particles in eye, insect bites, wind in eyes, struck by lightning etc., causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical checks right before start, protective gear: sunglasses/shaded airtight safety glasses, insects protection, being well hydrated, providing the possibility to use a toilet or similar, no start during lightning conditions.

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-1 are shown in E.1.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Safety Pilot		X	The Safety Pilot believes the Safety Pilot does not need to control the aircraft attitude during Start Phase when the current action is no action (start vehicle not moving before or after one of the other actions), regular start, abort or collision avoidance.
MM-2	Automated Controller	X		The Safety Pilot believes the Automated Controller is not in Safety Mode and so controls the aircraft attitude, when the Automated Controller is in Safety Mode and does not control the aircraft attitude.
MM-3	Automated Controller		X	The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude and so the Safety Pilot in Safety Mode does not need to control the aircraft attitude.
MM-4	Flight Director	X		The Safety Pilot believes the Flight Director Terminated the flight and so the Safety Pilot does not need to control the aircraft attitude, when the Flight Director did not terminate the flight.

Table E.1: Safety Pilot mental model flaws for UCA-1

Scenario 2 for UCA-1: The Safety Pilot believes the Safety Pilot does not need to control the aircraft attitude during start before takeoff, when the current action is: no action, regular start, abort or collision avoidance [MM-1], causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot about the need to control the aircraft attitude when the current action is no action, regular start, abort or collision avoidance [MM-1] during start before takeoff, even when the start vehicle is not moving before the start or after abort or collision avoidance.

Scenario 3 for UCA-1: The Safety Pilot believes the Automated Controller is not in Safety Mode and so controls the aircraft attitude, when the Automated Controller is in Safety Mode and does not control the aircraft attitude [MM-2] during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot that the Automated Controller is in Safety Mode during start before takeoff.

Scenario 4 for UCA-1: The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude and so the Safety Pilot in Safety Mode does not need to control the aircraft attitude [MM-3] during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot that the Automated Controller in Safety Mode does not control the aircraft attitude.

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 5 for UCA-1: The Safety Pilot gets the impression from the aircraft behavior that there is no need for the Safety Pilot to control the aircraft attitude during the start before takeoff when the current action is no action, regular start, abort or collision avoidance. [MM-3] This causes the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Train the Safety Pilot about the need to always control the aircraft attitude during start before takeoff, no matter the Safety Pilot's impressions of the aircraft dynamics during simulator training. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 6 for UCA-1: The Safety Pilot gets the command from the Remote Pilot that there is no need for the Safety Pilot to control the aircraft attitude during the start before takeoff when the current action is no action, regular start, abort or collision avoidance. [MM-3] This causes the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Train the Safety Pilot about the control hierarchy and control actions, such that he is aware to ignore invalid commands from other controllers.

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

Scenario 7 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but he decides, due to personal experience with similar aircraft, lack of training with this aircraft, training with this aircraft that indicated to him he does not need to control the attitude etc., that it is safe not to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator training that shows the Safety Pilot that it is needed. Telling the Safety Pilot about this causal scenario and making him understand it.

If simulators are used, they provide new hazards, such as differences in model and reality, simulator software flashed on flight hardware etc., which have to be analyzed in another STPA.

Scenario 8 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but he decides the sight attitude feedback received makes it unclear if controlling the attitude actually causes more harm than to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Training the Safety Pilot about how to judge the received feedback, simulator practice with similar to reality attitude sight feedback.

Scenario 9 for UCA-1: The Safety Pilot knows he is supposed to control the aircraft attitude but the Safety Pilot has too much to do or the Safety Pilot did not get enough training,for example just read a manual once, that the Safety Pilot forgets or decides not to control the aircraft attitude during start before takeoff, causing the Safety Pilot to not provide the attitude control action [UCA-1]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with evaluation if the Safety Pilot provided all control actions.

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers.“ [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

Not **A**pplicable (N/A), if the sight is disturbed this only leads to UCA-2, for sensor problems see Scenario 1

2) Inadequate feedback is received

N/A, stopping to control the aircraft attitude is UCA-6

Type b scenarios for the Safety Pilot's attitude (pitch, roll, yaw) control action

It might be useful to give all control actions a number, just as the unsafe control actions, to make it easier to track if all control actions where analyzed regarding loss scenarios of type b. Also some type of software that raises awareness of some kind if there are no type b loss scenarios for a control action yet, is to recommend to avoid human errors.

There needs to be a too late/to early, stopped too soon/applied too long, too fast/too slow, for example angle change rate control surfaces, category for type b scenarios. Even if there is no controller, so no decision making, involved, these are needs the intended design will have to fulfill.

For the case b scenarios no possible actions are given to mitigate the risks, as the actual design was not analyzed here, rather the needs an intended design will have to fulfill.

b1) Scenarios involving the control path

1) Control action not executed

Scenario 1: The Safety Pilot changes the sticks on the remote control to provide the attitude control action, but there is no attitude control signal sent from the remote control, for example because it is turned off, it has no power, it is broken, there is a design error etc., which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 2: The attitude control signal is sent from the remote control, but not received from the actuator system, because the signal is too weak, disturbances on the way to the receiver, inadequate receiver, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 3: The attitude control actuator system received the signal but does but not react to it due to inadequate design or malfunction, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

2) Control action improperly executed, executed when it should not have been, too late, too soon, too long, to short, wrong rates: too fast, too slow etc

Scenario 4: The Safety Pilot changes the sticks on the remote control to provide the attitude control action, but there is an inadequate attitude control signal sent from the remote control as in signal sent too late, control action represented by signal is too long, to short, wrong change rates , for example because the remote control has no power, it is broken, there is a design error etc., causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 5: The Safety Pilot does not change the sticks on the remote control, but there is an attitude control signal sent from the remote control causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 6: The attitude control signal is sent from the remote control, but inadequately received from the actuator system as in signal received too late, control action represented by signal is too long, to short, wrong change rates etc., for example because the signal is too weak, disturbance on the way to the receiver, receiver inadequate etc., causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 7: The signal is not sent from the remote control, but the actuator system receives a signal, which it interprets as valid attitude control signal, for example random signal wrongly interpreted as attitude control signal or attitude control signal from a different transmitter, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 8: The attitude control actuator system received the signal but reacts inadequately as in reaction too late, applied too long, to short, wrong change rates etc. because of inadequate design or a malfunction, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 9: The actuator system did not receive an attitude control signal but acts as if an attitude control signal would have been received because of a malfunction or a design error, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

b2) Scenarios related to the controlled process

1) Control action not executed

Scenario 10: The actuator system does apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does not react because there is not enough power of the control action, environmental disturbances to the control action, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 11: The actuator system does apply the attitude control action, the process, here the control surfaces and probably rotor rpm if used for attitude control, does react to the control action, but the aircraft attitude does not change because of a control surfaces design error or environmental disturbances, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

2) Control action improperly executed, executed when it should not have been, too late, too soon, too long, to short, wrong rates: too fast, too slow etc.

Scenario 12: The actuator system does apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does not react adequately as in too long, to short, wrong change rates etc. to the control action because there is not enough power of the control action or because of environmental disturbances, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 13: The actuator system does apply the attitude control action, the process, here the control surfaces and probably rotor rpm if used for attitude control, does react to the control action, but the aircraft attitude change improperly because of a control surfaces design error or environmental disturbances, which causes the attitude control action not to be executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Scenario 14: The actuator system does not apply the attitude control action, but the process, here the control surfaces and probably rotor rpm if used for attitude control, does react as if the control action would have been applied due to environmental disturbances, causing insufficient/exceeding attitude control being executed. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

E.2 Loss Scenarios type a UCA-2

Type a scenarios for UCA-2: The Safety Pilot controls the aircraft attitude tbd insufficiently/exceeding [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-2: The safety pilot has a medical condition (including insufficient eyesight or conditions caused by the Safety Pilot environment for example particles in eye, insect bites, wind in eyes etc.) during start before takeoff, causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical screening including eyesight test, being well hydrated, protective gear (sunglasses/shaded airtight safety glasses), insects protection

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-2 are shown in E.2.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Aircraft	X		The Safety Pilot believes the Aircraft is still attached to the Start Vehicle when it is already in flight or vice versa.
MM-2	Aircraft	X		The Safety Pilot has an incorrect believe about the current position (xyz) of the aircraft.
MM-3	Aircraft	X		The Safety Pilot has an incorrect believe about the current attitude (pitch, roll, yaw) of the aircraft.
MM-4	Aircraft	X		The Safety Pilot has an incorrect believe about the current acceleration (xyz) of the aircraft.
MM-5	Aircraft	X		The Safety Pilot has an incorrect believe about the current rotor rpm of the aircraft.
MM-6	Aircraft	X		The Safety Pilot has an incorrect believe about the current control surfaces position.
MM-7	Aircraft		X	The Safety Pilot has an incorrect believe about the attitude change of the aircraft depending on his stick movement
MM-8	Remote Pilot	X		The Safety Pilot has an incorrect belief about the current state of the Remote Pilot (No Action, Start, Abort, Collision Avoidance)
MM-9	Automated Controller		X	The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude at least partially (for example stabilizing)
MM-10	Start Vehicle Driver		X	The Safety Pilot has false beliefs about the kind of attitude control the start vehicle driver is able to provide
MM-11	Airspace Environment	X		The Safety Pilot has false beliefs about the airspace environment
MM-12	Airspace Environment		X	The Safety Pilot has false beliefs about the change of the airspace environment
MM-13	Safety Pilot		X	The Safety Pilot has false beliefs about the needed aircraft attitude control provided by the safety Pilot during No Action, Start, Abort or Collision Avoidance

Table E.2: Safety Pilot mental model flaws for UCA-2

Scenario 2 for UCA-2: The Safety Pilot has an incorrect believe about the current control surfaces position [MM-6] (for example the control surface position is not in a defined position when there has no initial stick movement been yet, the Safety Pilot assumes a different defined position etc.), causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: The control surface position must be actuated to a defined position in safety mode when the sticks are in neutral position (meaning the control surfaces are not actuated relative to stick change, but stick position), the Safety Pilot has to know this position.

Scenario 3 for UCA-2: The Safety Pilot has an incorrect believe about the attitude change of the aircraft depending on his stick movement [MM-7], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with a change rate similar to the real system, such that the Safety Pilot knows how and how fast the aircraft will react to his stick movement.

Scenario 4 for UCA-2: The Safety Pilot has an incorrect belief about the current state of the Remote Pilot (No Action, Start, Abort, Collision Avoidance) [MM-8], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: The Safety Pilot needs to be trained about the initial state of the Remote Pilot and the possible state changes.

Scenario 5 for UCA-2: The Safety Pilot believes the Automated Controller in Safety Mode controls the aircraft attitude at least partially (for example stabilizing) [MM-9], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Teaching the Safety Pilot that the automated controller does not control the aircraft attitude in Safety Mode.

Scenario 6 for UCA-2: The Safety Pilot has false beliefs about the kind of attitude control the start vehicle driver is providing [MM-10], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with similar to real system attitude control provided by the simulated start vehicle driver.

Scenario 7 for UCA-2: The Safety Pilot has false beliefs about the airspace environment [MM-11] and so false beliefs about the impact the airspace environment has on the needed attitude control, causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Safety Pilot must get briefed about the expected airspace environment before the start.

Scenario 8 for UCA-2: The Safety Pilot has false beliefs about the change of the airspace environment [MM-12], causing the Safety Pilot to not monitor the airspace environment, which causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Safety Pilot must get briefed about the expected airspace environment change before the start.

Scenario 9 for UCA-2: The Safety Pilot has false beliefs about the needed aircraft attitude control provided by the safety Pilot during No Action, Start, Abort or Collision Avoidance [MM-13], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Inform the Safety Pilot about the needed attitude control during No Action, Start, Abort or Collision Avoidance before takeoff, simulator practice focusing on attitude control during No Action, Start, Abort or Collision Avoidance before takeoff

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 10 for UCA-2: The Safety Pilot does not know how the stick position of the remote control relates to the current control surfaces position [MM-6], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: The Safety Pilot must be trained about how the stick position on the remote control relates to the current control surfaces position.

Scenario 11 for UCA-2: The Safety Pilot develops false beliefs about the needed aircraft attitude control provided by the safety Pilot during No Action, Start, Abort or Collision Avoidance (for example because he usually only flies in certain environmental conditions, which need less attitude control) [MM-13], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Repeat simulator practice continuously, even if Safety Pilot is well experienced with real system. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 12 for UCA-2: The Safety Pilot develops false beliefs about the attitude change of the aircraft depending on his stick movement [MM-7], causing the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Repeat simulator practice after maintenance/payload change with new dynamics, inform the Safety Pilot about the dynamics change

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

Scenario 13 for UCA-2: The Safety Pilot does not know about the attitude envelope the aircraft has to stay in during No Action, Start, Abort or Collision Avoidance during start before takeoff , which causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Safety Pilot must be trained about the attitude envelope the aircraft has to stay in during No Action, Start, Abort or Collision Avoidance during start before takeoff

Scenario 14 for UCA-2: The Safety Pilot does not have the skills (for example not enough training, too many things to do at once etc.) to keep the aircraft in the attitude envelope during No Action, Start, Abort or Collision Avoidance during start before takeoff including the impact of (and the change of) the environmental conditions, which causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Attitude control simulator training with reality equivalent tasks (control actions, monitoring and feedback) with changing environmental conditions and their impact on the attitude control dynamics. It must be monitored and evaluated if the Safety Pilot delivers all his tasks adequately. Put environmental constraints regarding attitude control on the start command (probably flight director).

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers.“ [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

Scenario 15 for UCA-2: The Safety Pilot must look down to the remote control to check the stick positions, which causes him to get no feedback from the aircraft and the start vehicle and vice versa. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice where the Safety Pilot can also only get feedback from the remote control or the aircraft/start vehicle, but not both at the same time.

2) Inadequate feedback is received

Scenario 16 for UCA-2: The sight of the Aircraft together with the sight of the Start Vehicle are insufficient in general or due to sun, rain, fog, hail, snow for the Safety Pilot to see if the Start Vehicle and the Aircraft are still attached, causing the Safety Pilot to believe the Aircraft is still attached to the Start Vehicle when it is already in flight or vice versa [MM-1]. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Making sure the start vehicle is not in the line of sight of the Safety Pilot to the aircraft connection points. Making sure the eyesight is sufficient to detect the takeoff (reacting too late is UCA-65). The Safety Pilot needs sunglasses and should be positioned with the sun in the back if possible. Put environmental constraints to the start command (Flight Director) regarding to sight sufficiency for Safety Pilot attachment feedback for attitude control. Simulator training with reality equivalent line of sight attachment point feedback.

Scenario 17 for UCA-2: The sight of the Aircraft together with the sight of the Start Vehicle are insufficient in general or due to sun, rain, fog, hail, snow for the Safety Pilot to monitor the current attitude (pitch, roll, yaw) of the aircraft [MM-3]. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Making sure the eyesight is sufficient to detect the aircraft attitude (reacting too late is UCA-65). Put environmental constraints to the start command (Flight Director) regarding to sight sufficiency for Safety Pilot attitude feedback for attitude control. Simulator training with reality equivalent line of sight attitude feedback.

Scenario 18 for UCA-2: The sight of the Aircraft together with the sight of the Start Vehicle are insufficient in general or due to sun, rain, fog, hail, snow for the Safety Pilot to monitor the current acceleration (xyz) of the aircraft [MM-4]. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Making sure the eyesight is sufficient to monitor the aircraft acceleration (reacting too late is UCA-65). Put environmental constraints to the start command (Flight Director) regarding to sight sufficiency for Safety Pilot acceleration feedback for attitude control. Simulator training with reality equivalent line of sight attitude feedback.

Scenario 19 for UCA-2: The provided feedback leads the Safety Pilot to an incorrect believe about the current rotor rpm of the aircraft. [MM-5]. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1]. What feedback is provided to the Safety Pilot about the rotor rpm? Is it relevant for attitude control? Is the rpm of each of the two rotors individually controllable?

Scenario 20 for UCA-2: The Safety Pilot senses the wind state, but there a different wind state at the aircraft position. [MM-11]. This causes the Safety Pilot to provide insufficiently/exceeding attitude control [UCA-2]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Moving the Safety Pilot as close as possible to the aircraft.

E.3 Loss Scenarios type a UCA-3

UCA-3: The safety Pilot controls the aircraft attitude such that it is unfavorable in a tbd way during the transition to the next flight phase/for the start of the next flight phase [tbd]

This is only different from UCA-2 if it is possible that the aircraft attitude stays inside the designated (designed) envelope and is still unfavorable for the transition to the next flight phase/for the start of the next flight phase. This UCA can be prevented through the design of the attitude envelope, then no scenario creation for UCA-3 is necessary, because the scenarios are the same as the UCA-2 scenarios. UCA-3 is still important to point out this decision must either be made during the attitude envelope design or scenarios for UCA-3 must be created.

For this work it is assumed the designed attitude envelope is designed such, that staying in the attitude envelope will make sure that the aircraft attitude is favorable for the transition to the next flight phase/for the start of the next flight phase.

E.4 Loss Scenarios type a UCA-4

Type a scenarios for UCA-4: The Safety Pilot controls the aircraft attitude tbd time after the start vehicle accelerates (xy) [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-4: The safety pilot has a medical condition (including conditions caused by the Safety Pilot environment for example particles in eye, insect bites, wind in eyes etc.) during start before takeoff, which lowers the Safety Pilot's reaction time, causing the Safety Pilot to provide attitude control tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical screening regarding reaction time regarding reaction to acceleration of start vehicle, being well hydrated, protective gear (sunglasses/shaded airtight safety glasses), insects protection

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-4 are shown in E.3.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Aircraft		X	The Safety Pilot believes it takes less time until the aircraft attitude is changed after the Safety Pilot moved the sticks on the remote control than it actually takes
MM-2	Start Vehicle Driver		X	The Safety Pilot believes it takes more time until the Start Vehicle Driver changes the Start Vehicle acceleration after the Safety Pilot gives Start, Abort or Collision Avoidance command to the Start Vehicle Driver
MM-3	Start Vehicle	X		The Safety Pilot has false beliefs about the current Start Vehicle acceleration
MM-4	Airspace Environment		X	The Safety Pilot has false beliefs about the way the airspace environment influences the system response time (see MM-1)

Table E.3: Safety Pilot mental model flaws for UCA-4

Scenario 2 for UCA-4: The Safety Pilot believes it takes less time until the aircraft attitude is changed after the Safety Pilot moved the sticks on the remote control than it actually takes [MM-1], causing the Safety Pilot to provide attitude control tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with reality equivalent aircraft attitude change response time to stick movements

Scenario 3 for UCA-4: The Safety Pilot believes it takes more time until the Start Vehicle Driver changes the Start Vehicle acceleration after the Safety Pilot gives Start, Abort or Collision Avoidance command to the Start Vehicle Driver [MM-2] than it actually takes, causing the Safety Pilot to provide attitude control tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with reality equivalent Start Vehicle Driver response time to Safety Pilot commands. Training the Safety Pilot to be ready for start vehicle acceleration as soon as the Safety Pilot has given Start, Abort or Collision Avoidance command.

Scenario 4 for UCA-4: The Safety Pilot has false beliefs about the way the airspace environment influences the system response time for attitude change (see MM-1) [MM-4], which leads to scenario 2 fur UCA-4.

Possible action: Simulator practice with reality equivalent aircraft attitude change response time to stick movements including airspace environment influences on said response time. Training the Safety Pilot about the airspace environment influences on the system response time.

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 5 for UCA-4: The Safety Pilot develops false believes about the time needed until the Start Vehicle Driver changes the Start Vehicle acceleration after the Safety Pilot gives Start, Abort or Collision Avoidance command to the Start Vehicle Driver [MM-2], which leads to Scenario 3 for UCA-4 (for example because the Start Vehicle Driver reacts slowly a couple times, but then acts quicker).

Possible action: Repeat simulator practice continuously with quick start vehicle driver response time, even if Safety Pilot is well experienced with real system. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 6 for UCA-4: The Safety Pilot develops false beliefs about the way the airspace environment influences the system response time for attitude change (see MM-1) [MM-4] (for example because the Safety Pilot gets used to flying in only one certain environmental airspace condition and forgets about the influence of other environmental airspace conditions), which leads to scenario 2 fur UCA-4.

Possible action: Repeat simulator practice continuously with all the different reality equivalent environmental airspace condition influences on the system response time for attitude change. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

Scenario 7 for UCA-4: The Safety Pilot does not have the skills (for example not enough training, too many things to do at once, reaction time etc.) to provide attitude control in tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Attitude control simulator training with reality equivalent tasks (control actions, monitoring and feedback) with changing environmental conditions and their impact on the attitude control dynamics. It must be monitored and evaluated if the Safety Pilot delivers all his tasks in tbd time.

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers.“ [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

Scenario 8 for UCA-4: The Safety Pilot must look down to the remote control to check the stick positions, which causes him to get no feedback from the aircraft and the start vehicle and vice versa, which leads to the Safety Pilot having false beliefs about the current Start Vehicle acceleration (xy) [MM-3]. This causes the Safety Pilot to provide attitude control tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice where the Safety Pilot can also only get feedback from the remote control or the aircraft/start vehicle, but not both at the same time. Safety Pilot attitude control response time to acceleration monitoring and evaluation during this simulator practice.

2) Inadequate feedback is received

Scenario 9 for UCA-4: The sight of the Aircraft together with the sight of the Start Vehicle are insufficient in general or due to sun, rain, fog, hail, snow for the Safety Pilot to monitor the current start vehicle acceleration (xy) [MM-3]. This causes the Safety Pilot to provide attitude control tbd time after the start vehicle accelerates (xy) [UCA-4]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Making sure the eyesight is sufficient to detect the aircraft acceleration in tbd time to react in tbd time. Put environmental constraints to the start command (Flight Director) regarding sight sufficiency for Safety Pilot attitude feedback for attitude control response time. Simulator training with reality adequate line of sight feedback of start vehicle acceleration. Safety Pilot attitude control response time to acceleration monitoring and evaluation during this simulator practice.

E.5 Loss Scenarios type a UCA-5

Type a scenarios for UCA-5: The safety Pilot controls the aircraft attitude tbd time after external forces act on the aircraft [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-5: The safety pilot has a medical condition (including conditions caused by the Safety Pilot environment for example particles in eye, insect bites, wind in eyes etc.) during start before takeoff, which lowers the Safety Pilot's reaction time, causing the Safety Pilot to provide attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical screening regarding reaction time regarding reaction to external forces acting on the aircraft (in control algorithm needed response time), being well hydrated, protective gear (sunglasses/shaded airtight safety glasses), insects protection

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-5 are shown in E.4.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Aircraft		X	The Safety Pilot believes it takes less time until the aircraft attitude is changed after the Safety Pilot moved the sticks on the remote control than it actually takes
MM-2	Airspace Environment		X	The Safety Pilot has false beliefs about the way the airspace environment influences the system response time (see MM-1)
MM-3	Airspace Environment	X		The Safety Pilot has false beliefs about the current airspace environment
MM-4	Airspace Environment		X	The Safety Pilot has false beliefs about the change of the airspace environment

Table E.4: Safety Pilot mental model flaws for UCA-5

Scenario 2 for UCA-5: The Safety Pilot believes it takes less time until the aircraft attitude is changed after the Safety Pilot moved the sticks on the remote control than it actually takes [MM-1], causing the Safety Pilot to provide attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice with reality equivalent aircraft attitude change response time to stick movements.

Scenario 3 for UCA-5: The Safety Pilot has false beliefs about the way the airspace environment influences the system response time for attitude change (see MM-1) [MM-2], which leads to scenario 2 fur UCA-5.

Possible action: Simulator practice with reality equivalent aircraft attitude change response time to stick movements including airspace environment influences on said response time. Training the Safety Pilot about the airspace environment influences on the system response time.

Scenario 4 for UCA-5: The Safety Pilot has false beliefs about the current airspace environment [MM-3], which causes the Safety Pilot to having false beliefs about the way the airspace environment influences the system response time for attitude change (see MM-1) [MM-2], which leads to scenario 2 for UCA-5. Possible action: Briefing the Safety Pilot about initial environmental airspace conditions. Training the Safety Pilot how to evaluate initial environmental airspace conditions.

Scenario 5 for UCA-5: The Safety Pilot has false beliefs about the change of the airspace environment [MM-4], which causes the Safety Pilot to monitor the change of the airspace environment insufficiently, which leads to the Safety Pilot providing attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Briefing the Safety Pilot about possible environmental airspace condition changes. Simulator practice with reality equivalent environmental airspace condition changes, evaluating the Safety Pilot's monitoring of said changes.

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 6 for UCA-5: The Safety Pilot develops false believes about the time it takes until the aircraft attitude is changed after the Safety Pilot moved the sticks on the remote control [MM-1], causing the Safety Pilot to provide attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Repeat simulator practice continuously with reality equivalent aircraft attitude change response time to stick movements, even if Safety Pilot is well experienced with real system. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 7 for UCA-5: The Safety Pilot develops false beliefs about the way the airspace environment influences the system response time for attitude change (see MM-1) [MM-2] (for example because the Safety Pilot gets used to flying in only one certain environmental airspace condition and forgets about the influence of other environmental airspace conditions), which leads to scenario 2 for UCA-5.

Possible action: Repeat simulator practice continuously with reality equivalent aircraft attitude change response time to stick movements including airspace environment influences on said response time. Repeat training the Safety Pilot about the airspace environment influences on the system response time continuously. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

Scenario 8 for UCA-5: The Safety Pilot develops false beliefs about the change of the airspace environment [MM-4], which causes the Safety Pilot to monitor the change of the airspace environment insufficiently, which leads to the Safety Pilot providing attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Continuously repeating simulator practice with reality equivalent environmental airspace condition changes, evaluating the Safety Pilot's monitoring of said changes. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

3) Inadequate control algorithm

Extension 4: Identify unsafe Control Action Selections

Scenario 9 for UCA-5: The Safety Pilot does not have the skills (for example not enough training, too many things to do at once, reaction time) to provide attitude control in tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamic loads act on the aircraft structure [H-4.1.2.1].

Possible action: Attitude control simulator training with reality equivalent tasks (control actions, monitoring and feedback) with changing environmental conditions and their impact on the attitude control dynamics. It must be monitored and evaluated if the Safety Pilot delivers all his tasks in tbd time.

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers.“ [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate feedback and information

1) Feedback or information not received

Scenario 10 for UCA-5: The Safety Pilot must look down to the remote control to check the stick positions, which causes him to get no feedback from the aircraft and the start vehicle and vice versa, which leads to the Safety Pilot having false beliefs about the current airspace environment [MM-3]. This causes the Safety Pilot to provide attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Simulator practice where the Safety Pilot can also only get feedback from the remote control or the aircraft/start vehicle, but not both at the same time. Safety Pilot attitude control response time to external forces acting on the aircraft monitoring and evaluation during this simulator practice.

2) Inadequate feedback is received

Scenario 11 for UCA-5: The sight of the aircraft is insufficient in general or due to sun, rain, fog, hail, snow for the Safety Pilot to monitor the current environmental conditions [MM-3]. This causes the Safety Pilot to provide attitude control tbd time after external forces act on the aircraft [UCA-5]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Making sure the eyesight is sufficient to detect the environmental conditions in tbd time to react in tbd time after external forces act on the aircraft. Put environmental constraints to the start command (Flight Director) regarding sight sufficiency for Safety Pilot attitude feedback for attitude control response time regarding external forces acting on the aircraft. Simulator training with reality adequate line of sight feedback of environmental conditions. Safety Pilot attitude control response time to external forces acting on the aircraft monitoring and evaluation during this simulator practice.

E.6 Loss Scenarios type a UCA-6

Type a scenarios for UCA-6: The Safety Pilot stops controlling the aircraft attitude [H-5.1.1.1.9, H-4.1.2.1]

a1) Identifying scenarios that lead to Unsafe Control Actions - Unsafe controller behavior

1) Failures involving the controller, hardware failures for physical controllers, medical condition for human controllers

Scenario 1 for UCA-6: The safety pilot has a medical condition (including conditions caused by the Safety Pilot environment for example particles in eye, insect bites, wind in eyes etc.) during start before takeoff, causing the Safety Pilot to stop providing attitude control [UCA-6]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Medical screening, being well hydrated, protective gear (sunglasses/shaded airtight safety glasses), insects protection.

2) Inadequate process model

Extension 1: Identify Mental Model Variables

See table 5.4

Extension 2: Identify Mental Model Flaws, identify all possible flaws for this UCA, identify scenarios with flaws initially existing in the mental model

The identified mental model flaws for UCA-6 are shown in E.5.

Number of Mental Model Flaw	Mental Model	State	Behavior	Description
MM-1	Safety Pilot		X	The Safety Pilot believes the Safety Pilot does not need to control the aircraft attitude during Start Phase when the current action is no action, regular start, abort or collision avoidance

Table E.5: Safety Pilot mental model flaws for UCA-6

Scenario 2 for UCA-6: Safety Pilot beliefs the start phase ended after the Safety Pilot sent the take back control command to the Remote Pilot [MM-1] This causes the Safety Pilot to stop providing attitude control [UCA-6]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Train the Safety Pilot that the start phase ends when the control taken command is received

Extension 3: Identify flaws in Mental Model Updates that lead to the identified Mental Model flaws, identify scenarios with flaws where the controller receives the needed feedback/input to update but does not update correctly or does update incorrectly due to other factor besides the feedback. Scenarios where the necessary feedback is not provided to the controller are analyzed in a2

Scenario 3 for UCA-6: The Safety Pilot develops false beliefs about the Safety Pilot's need to control the aircraft attitude during Start Phase when the current action is no action, regular start, abort or collision avoidance [MM-1] (for example because the Safety Pilot has the impression that there is no need to control the attitude, when the Start Vehicle is standing still or the Safety Pilot gets the impression that the aircraft is stable enough to stay in the attitude envelope without the Safety Pilot controlling the aircraft attitude, the Safety Pilot is only used to fly in one certain airspace environment etc.). This causes the Safety Pilot to stop providing attitude control [UCA-6]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Repeat simulator practice continuously with reality equivalent aircraft attitude control needs under different environmental influences especially when start vehicle is standing still, even if Safety Pilot is well experienced with real system. Explaining the Safety Pilot that this behavior is a typical accident scenario. Showing the Safety Pilot examples of accidents which had similar causes.

3) Inadequate control algorithm

Scenario 4 for UCA-6: The Safety Pilot does not have the skills (for example not enough training, too many things to do at once) to provide all his tasks correctly, so he stops controlling the aircraft attitude, because he believes this control action is not as important [UCA-6]. As a result, the aircraft could be tilted towards the start vehicle or ground [H-5.1.1.1.9] and the aircraft could violate maneuver constraints, such that exceeding aerodynamical loads act on the aircraft structure [H-4.1.2.1].

Possible action: Attitude control simulator training with reality equivalent tasks (control actions, monitoring and feedback) with changing environmental conditions and their impact on the attitude control dynamics. It must be monitored and evaluated if the Safety Pilot delivers all his tasks (control actions, monitoring and feedback) in tbd time.

Extension 4: Identify unsafe Control Action Selections

4) Unsafe control input from another controller

„Unsafe control inputs from other controllers can also cause UCAs. These can be found during the previous step when identifying Unsafe Control Actions for other controllers.“ [8]

a2) Identifying scenarios that lead to Unsafe Control Actions - Causes of inadequate

feedback and information

1) Feedback or information not received

N/A

2) Inadequate feedback is received

N/A