NASA/CR-20210026909

Run Time Assurance for Electric Vertical Takeoff and Landing Aircraft

Michael DeVore and Jared Cooper
Barron Associates, Inc., Charlottesville, Virginia

Andy Wallington, Robert Crouse, Gust Tsikalas, Komal Verma
Electron International II Inc., Phoenix, Arizona

Cody H. Fleming
Iowa State University, Ames, Iowa

Greg Carr and Newton Kirby
Architecture Technology Corporation, Campbell, California

March 2022

NASA STI Program Report Series

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- Help desk contact information:

https://www.sti.nasa.gov/sti-contact-form/
and select the "General" help request type.

NASA/CR-20210026909

Run Time Assurance for Electrical Vertical Takeoff and Landing Aircraft

Michael DeVore and Jared Cooper
Barron Associates, Inc., Charlottesville, Virginia

Andy Wallington, Robert Crouse, Gust Tsikalas, Komal Verma
Electron International II Inc., Phoenix, Arizona

Cody H. Fleming
Iowa State University, Ames, Iowa

Greg Carr and Newton Kirby
Architecture Technology Corporation, Campbell, California

National Aeronautics and
Space Administration

NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

March 2022

The use of trademarks or names of manufacturers in this report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Acknowledgments

This research work was awarded by NASA under Basic and Applied Aerospace Research and Technology (BAART) Contract No. NNL16AA12B, Task Order No. 80LARC20F0089. This research builds upon our prior research effort titled “Effectiveness of Alternate Concepts to Contemporary Development Assurance Processes.” [NASA-CR-2020-220586]

The authors would like to thank Dr. Terry Morris and the NASA System Wide Safety Project for sponsoring this research effort.

The NASA technical monitor for this task is Mr. Wilfredo Torres-Pomales. We’d like to thank Wilfredo and Paul Miner of NASA for their patience, guidance, and feedback throughout the course of this research effort.

We’d like to thank Eric Peterson, Srini Mandalapu, and Barbara Lingberg of the FAA, and John Schierman of the AFRL for acting as external reviewers for our research project.

The authors would like to acknowledge Jacek Kawecki of Uber Elevate for providing a distributed electric propulsion vehicle concept with distributed control architecture for an Urban Air Mobility concept of operations.

Table of Contents

Table of Figures

Table of Tables

Table of Acronyms

AAM	Advanced Air Mobility
ACAH	Attitude Command, Attitude Hold
ACAS	Automated Collision Avoidance System
AcCVH	Acceleration Command, Velocity Hold
AFHA	Aircraft Functional Hazard Assessment
AHRS	Attitude Heading and Reference System
ANLDI	Adaptive Nonlinear Dynamic Inversion
ARP	Aerospace Recommended Practice
ASA	Aircraft System Assessment
ASMP	Assumption
ATM	Air Traffic Management
BAART	Basic and Applied Aerospace Research and Technology
CFIT	Controlled Flight Into Terrain
CG	Center of Gravity
CMA	Common Mode Analysis
CV	Controlled Variables
DAA	Detect and Avoid
DAL	Development Assurance Level
DD	Dependence Diagram
DEP	Distributed Electric Propulsion
DI	Dynamic Inversion
DRP	Dynamic Reactive Planning
EASA	European Union Aviation Safety Agency
eVTOL	Electric Vertical Takeoff and Landing
FAR	Federal Aviation Regulations

FCC	Flight Control Computer
FDAL	Function Development Assurance Level
FFS	Functional Failure Set
FHA	Functional Hazard Assessment
FMEA/FMES	Failure Modes and Effects Analysis/Summary
FMS	Flight Management System
FPA	Flight Path Angle
FPC	Flight Path Command
FTA	Fault Tree Analysis
GPS	Global Positioning System
HC	High Confidence
IDAL	Item Development Assurance Level
IFR	Instrument Flight Rules
INS	Inertial Navigation System
LC	Low Confidence
LOC-I	Loss of Control - Inflight
LHI	Left-Hand Inceptor
LRU	Line-Replaceable Unit
MOC	Means of Compliance
MRAC	Model Reference Adaptive Control
NASA	National Aeronautics and Space Administration
NEU	North-East-Up
NLDI	Nonlinear Dynamic Inversion
NMPC	Nonlinear Model Predictive Control
OFN	Obstacle Field Navigator
PFCS	Primary Flight Control System
PH	Position Hold

PIC	Pilot in Command
PID	Proportional-Integral-Derivative
PRA	Particular Risks Analysis
PSSA	Preliminary System Safety Assessment
PSU	Providers of Services to UAM
RCDH	Rate Command, Direction Hold
RCHH	Rate Command, Height Hold
RHI	Right-Hand Inceptor
RSL	Roughness Sublayer
RTA	Run Time Assurance
SFHA	System Functional Hazard Assessment
SSA	System Safety Assessment
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
sUAS	Small Unmanned Air Systems
SVO	Simplified Vehicle Operations
TC/AOS	Turn Coordination/Angle of Sideslip
TCAS	Traffic Collision Avoidance System
TOLA	Takeoff and Landing Areas
TRC	Translational Rate Command
UAM	Urban Air Mobility
UAS	Unmanned Air System
UBL	Urban Boundary Layer
UCL	Urban Canopy Layer
UTM	UAS Traffic Management
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions

VTOL	Vertical Takeoff and Landing
Vx	Translational velocity in x axis
Vy	Translational velocity in y axis
ZSA	Zonal Safety Analysis

Executive Summary

NASA is conducting and supporting research to demonstrate and evaluate the application of Run Time Assurance (RTA) as a means to assure safety in Electric Vertical Takeoff and Landing (eVTOL) aircraft with highly automated or autonomous flight capability supervised by a single onboard pilot.

In 2018, NASA awarded Architecture Technology Corporation (ATCorp), Electron International II Inc., and Barron Associates a contract to conduct research into the Effectiveness of Alternate Concepts to Contemporary Development Assurance Processes. Using a baseline of existing industry-standard approaches to system safety assurance, this research explored alternate concepts and evaluated their effectiveness against current industry practices. During the execution of this research effort the ATCorp Team focused on evaluation of RTA as an alternate concept applied to a novel, airborne system architecture. In particular, the ATCorp Team illustrated the application of an RTA design pattern (with a high automation control mode and a low automation recovery mode) to a notional integrated flight and propulsion control system for a Distributed Electric Propulsion (DEP) Vertical Takeoff and Landing (VTOL) aircraft. This research focused on the application of RTA to one flight control sub-function of a notional eVTOL aircraft design. The assumptions, methods, and results of this work were published in a NASA Contractor's Report in May 2020 [Peterson 2020].

In 2020 NASA awarded Architecture Technology Corporation, Electron International II Inc., Barron Associates, and Dr. Cody H. Fleming a contract to expand on the research into run-time assurance for increasingly autonomous systems. The work described in this report demonstrates a broader application of RTA and examines the implications for design and analysis of aircraft functions and systems; aircraft safety hazards; safety assurance; development assurance; and pilot tasks and performance. This research effort also seeks to assess the efficacy of the combined application of traditional Functional Hazard Analysis (FHA) and the more modern System Theoretic Process Analysis (STPA) techniques to perform hazard analyses on aircraft with complex automated and autonomous systems and an onboard pilot.

The scope of this research is to focus on eVTOL aircraft intended for Urban Air Mobility (UAM) operations with airworthiness requirements from standard certification regulations for Part 23 and Part 27 normal category aircraft as applicable. The scope of the task includes the design and safety assessment at the aircraft function level and system level as discussed in the SAE standards APR4754A and ARP4761, and the ASTM standards F3264, F3061, and F3230. The scope also includes the definition and safety assessment of tasks allocated to the onboard aircraft pilot, as well as the STPA hazard analysis technique.

The objectives of this research effort are:

- To demonstrate and evaluate the application of the RTA-based assurance concept to assure the safety of flight control functions of an eVTOL aircraft with highly automated or autonomous flight capability and a single onboard pilot.
- To demonstrate and assess the effectiveness of FHA and STPA combined as complementary hazard analysis techniques for an eVTOL aircraft with highly automated or autonomous flight capability and a single onboard pilot.

For this current study we build on our prior research effort, and we leverage other NASA, FAA, and industry research related to design and analysis of aircraft functions and systems;

aircraft safety hazards; safety assurance; development assurance; and pilot tasks and performance.

As discussed in the previous study report [Peterson 2020], the control system architecture for many of the UAM aircraft designs, including the eVTOL vehicles that are the object of this study, will necessarily be much more complex than for existing commercial, general aviation, and rotary wing aircraft. The large number of rotational components and control surfaces, together with inherent dynamic instability, mean that piloting in a traditional “stick-to-surface” manner will not be feasible. Not only must the control system manage this complexity, but it must also accommodate the limitations of minimally certificated pilots in command. A key question of this research is whether the control-centric approach adopted by STPA can be a valuable complement to traditional safety assurance processes for these systems.

One of the strengths of FHA is that it relies only on functional breakdowns of the aircraft and its systems, without relying on detailed design information about the components that will ultimately comprise the aircraft. One of the strengths of STPA is that it focuses on modeling interactions between functions and how these interactions can lead to unsafe control of the overall system. This research effort seeks to identify and characterize the potential synergy between these two approaches. For example, being more aware of the coupling between functions, an analyst conducing FHA might be able to identify additional and novel, failure conditions. Likewise, being more aware of different types of failure conditions, usage of STPA might identify novel pathways and cascading scenarios that lead to unsafe control.

A key research question that arises is whether the effectiveness of the two methods occurs at different levels of abstraction. For example, for STPA to be most effective, it might require implementation details that a conventional FHA otherwise may not. To answer this and other questions of how FHA and STPA can be used jointly to improve the assurance processes for UAM applications, we explore several specific notions of hazardous behaviors that many of the advanced subsystems may exhibit. We also model several control functions in STPA, as well as the coupling between them, to identify hazardous scenarios that arise due to interactions between pilots and automation.

During the research effort we developed architectural designs of two alternate eVTOL aircraft, generally following the process characterized in the SAE standards ARP4754 and ARP4761. The design has focused on the control architectures of these aircraft, which are identical except that one incorporates RTA techniques to reduce the criticality of some key software components. Artifacts of this process include a taxonomy of aircraft-level functions, aircraft-level architecture diagrams, aircraft-level functional hazard assessments (AFHA), function allocations onto aircraft systems and subsystems, functional block diagrams for a select set of control-related functions, and system-level functional hazard assessments (SFHA) for those functions.

These artifacts are identical for both vehicles, except for some low-level architectural additions to accommodate the RTA components in one of the vehicles. In an actual aircraft development process, these additions would necessitate a new set of SFHAs. However, the nature of the RTA architecture is such that the impact of these additions on the SFHAs performed for the baseline aircraft will be minimal. Rather than duplicating all the effort and pages of nearly redundant documentation that would be produced by performing SFHAs on both vehicles, we simply note any differences that would arise for the RTA-equipped vehicle.

In parallel, the team developed STPA artifacts for the same aircraft architecture and system designs. These artifacts are very detailed for the lowest level control functions, which the team believes is sufficient to illustrate the differences between STPA and traditional safety engineering approaches. There appears to be only minimal value in continuing that same level of detail for the higher-level control functions. As a result, STPA activities for these functions has only the more interesting aspects of their design.

One of the things we have learned through these activities is that STPA partially overlaps with many of the intents behind SFHA, though with a different set of techniques. It has also become apparent that STPA partially overlaps with many of the intents behind preliminary system safety assessment (PSSA), again through a different set of techniques. In this research effort we explore where they overlap and where they are orthogonal, particularly in the case of hierarchical RTA-equipped control systems. While we had not originally planned, nor are their resources to conduct, a full PSSA for this aircraft, we think there is significant research value in at least a qualitative exploration of their relationships. Rather than performing in parallel a full PSSA and STPA of the entire control system design, the approach we take is to document what activities each of these two processes would entail for this design and the intents behind those activities. We think that a comparison at this level is likely to be more valuable than the specific details contained in the worksheets that would be generated by those activities.

As noted above, the primary objectives of this research effort included demonstration and evaluation of RTA-based assurance to an eVTOL aircraft in an UAM application; and demonstration and evaluation of the effectiveness of FHA and STPA combined as complementary hazard analysis techniques.

This project has highlighted the notion that Development Assurance Level (DAL) D is something of a sweet spot for low-confidence controllers in an RTA-based design. This observation was initially made in the previous BAART task order [Peterson 2020], based on a count of the number of required development activities involved with different DAL assignments. In this project, the team investigated more closely the specific DO-178C [RTCA/DO-178C] development activities that can be eliminated from the process and their relevance to the kinds of advanced controllers considered for the eCRM-001 design. Among the many activities described in DO-178C, the activities related to requirement verifiability, algorithmic accuracy, and test coverage can be the most challenging for the kinds of advanced control techniques that may be desirable in novel UAM designs, such as adaptive control, machine-learning, artificial intelligence, numerical search, and Monte Carlo based algorithms. Moreover, the standard requires that development teams demonstrate that errors leading to unacceptable failure conditions have been removed from the software. The RTA architecture, which cordons off the low-confidence function, makes it much easier to show this for these kinds of algorithms.

It is expected that the UAM community will not have the same degree of institutionalized knowledge regarding the target operating environment that has existed for decades among more traditional aircraft operations. There may be a much wider variety of aircraft configurations, and developers of these novel designs will not have nearly the same level of experience with their vehicles as do those of more traditional aircraft. Moreover, the urban turbulence environment is generally much more complex than that above the atmospheric boundary layer or above rural areas, in which most traditional aircraft spend most of their flight time. Turbulence models and corresponding simulation capabilities for this environment are not as widely available. Finally, operations within the urban environment may evolve rapidly in the initial years as the market develops and the various stakeholders must adapt to accommodate each other.

As a result, it is likely that companies may seek to roll out multiple control system updates to optimize aircraft performance, handling qualities, and piloting performance as the community gains experience in this environment. Even if it is not needed to facilitate certification of the original control system software, the RTA architecture may be an extremely valuable design choice to facilitate these future upgrades. New software versions could be developed to DAL D, then deployed to the fleet as low-confidence components, with protection provided by an RTA monitor and corresponding high-confidence variant that was developed to DAL B during the initial vehicle design. The previous BAART task order [Peterson 2020] demonstrated a tremendous savings in development effort for updates performed in this manner.

With regard to the use of STPA and FHA as complementary hazard analysis techniques, our research effort led us to the following conclusion and recommendations. We advocate for the use of STPA in the following ways. First, it should be used to derive requirements for hardware and software systems and/or components. Based on criticality and other aspects or outputs of the PSSA, these would get fed into the development activities prescribed by the appropriate standard (e.g., DO-178C, DO-255, etc.), where requirements would then be verified accordingly. Second, STPA is a natural complement to other processes in ARP4754A involving design studies and iteration. STPA results can be used to initiate design trade studies, for example by adding or deleting connections/signals in the communications or software architecture, which would then trigger an iteration of PSSA, or possibly be fed back up the chain and result in higher level safety assessments like FHAs or SFHAs.

1.0 Introduction

In 2016 Uber Elevate (now part of Joby Aviation) published a whitepaper describing a vision for on-demand aviation that would use eVTOL aircraft to "enable rapid, reliable transportation between suburbs and cities and, ultimately, within cities." [Uber 2016] The Uber vision for on-demand transportation was predicated on the ability to operate a large number of eVTOL aircraft at high-tempo (many aircraft operating concurrently) in urban areas in order to make the costs to the manufacturers, operators, and travelling public affordable. The Uber whitepaper described a number of challenges that must be overcome to realize the use of eVTOLs for UAM. One of these challenges is related to the need to have a large number of pilots qualified to fly the eVTOL aircraft. Uber proposed to try to reduce the amount of time and cost associated with training pilots by using automation to augment pilot functions and thereby reduce the skills required for pilot tasks such as aviate and navigate. From [Uber 2016]:

> *Pilot Training. Training to become a commercial pilot under FAR Part 135 is a very time-intensive proposition, requiring 500 hours of pilot-in-command experience for VFR and 1200 hours for IFR. As on-demand VTOL service scales, the need for pilots will rapidly increase, and it's likely that with these training requirements, a shortage in qualified pilots will curtail growth significantly. In theory, pilot augmentation technology will significantly reduce pilot skill requirements, and this could lead to a commensurate reduction in training time…*
>
> *As described in the safety section, VTOLs with autonomous capabilities will significantly shift pilot skill requirements. Presently, pilots must monitor both the vehicle's trajectory in relation to the desired path and also adjust many vehicle state parameters to force the trajectory to conform to the desired route. Autonomy refers to the ability of the vehicle to make these adjustments itself; pilot inputs are limited to commanding a desired trajectory rather than the means to achieve it.*
>
> *While we have planned initially for commercial pilots operating under today's Part 135 rules and their equivalents outside the US, we anticipate that demonstrating successful operation with early vehicles will reduce the requirements for pilot experience in conventional aircraft based on reduced pilot task-loading, and more fundamentally, the reduced scope of tasks for which the pilot is responsible. This is similar to what the FAA has done in the definition of the light-sport pilot license which requires roughly half the time that a private pilot license does. Not only must the FAA be convinced, but the insurers who cover the risk of the operation will need to see that pilot skill and experience requirements are reduced.*

In a 2018 study Feary looked more closely at some of the challenges associated with the need for large numbers of pilots to support the UAM concept, pilot training requirements, and the possible use of increased autonomy to reduce required pilot skills and training requirements while maintaining or increasing safety [Feary 2018]. In this paper Feary proposes a model to help frame flight crew functions for evaluation of future operational requirements regardless of whether the functions are performed by human or artificial agent. Feary identifies a number of issues and research challenges associated with the goal of reducing pilot training requirements while increasing the use of automation to support pilot functions. From [Feary 2018]:

> *The transition to greater use of automated systems will generate additional challenges. A phased transition should help to mitigate some safety issues, but in the short term the industry will still have a requirement to provide large numbers of safe and capable pilots. The industry is projecting a shortage of pilots for traditional airline operations, and new flight crew training and performance requirements will likely be necessary.*
>
> *It also appears that if the UAM concept is successful, there may be operators of fleets of eVTOLs that are much larger than the fleet sizes of current on-demand aviation operators today, which will likely require more formal implementation of management processes and operational models that may be more similar to §121 airlines than most §135 operations today.*
>
> *The mid- to long-term vision for UAM is more interesting from a perspective of research into Human- Automation Teaming, as more authority is given to autonomous functions. This will change the nature of piloting, as more aircraft control is likely to be given to the aircraft while decision making authority and response to unusual situations will be some of the last functions to be automated.*

The business imperative to scale operations while reducing pilot training time and costs has given rise to idea of "minimally-trained" pilots operating complex eVTOL aircraft in a challenging operating environment with support from automation and autonomy. Although there are concepts for providing offboard (ground-based) automation and autonomy, we assume for this study that this automation and autonomy are onboard the aircraft. In Section 2, we describe an aircraft that has the capabilities needed to support the eVTOL UAM concept, carries a pilot + 4 passengers, has a minimally trained pilot, operates in a congested airspace, provides turbulence rejection, energy efficiency and efficient path following through automation.

In our previous research effort, we developed a notional airborne system for a new and novel DEP VTOL based on Uber Elevate's eVTOL Common Reference Model (eCRM). The aircraft is a powered-lift vehicle to be developed and certificated under Normal, Utility, Acrobatic and Commuter Category Airplane regulations for VFR day use. Aircraft functions were defined only to a level of detail necessary to support the case study application of RTA to protect a specific flight control function [Peterson 2020].

In this current effort we use the same overall aircraft design (eCRM-001), but we expand on system and sub-system functional definitions to support the hazard analyses and application of RTA. We explore broader application of RTA as well as the implications of pilot-automation interactions. In particular, we focus on defining a number of automation functions in the flight and propulsion control architecture that span from inner-loop to outer-loop control and are candidates for the application of RTA. We consider variable automation that would allow the pilot to partially or totally transfer responsibility to onboard systems for flight control tasks. The human pilot can control the aircraft by manipulating inceptors for direct but highly augmented control modes. Alternatively, the human pilot can provide high-level mission commands, such as waypoints or final destinations, with automation providing path generation and following. In addition, we automated collision avoidance to ensure separation from buildings and other aircraft. It is assumed that these types of functions are required to support the concept of minimally trained pilots operating complex eVTOL aircraft in a high-tempo urban environment such as that envisioned for UAM (Figure 1).

Figure 1. Notional depiction of a UAM operating environment including multiple vehicle types operating in a dense urban environment.[1]

Since the publication of the Uber whitepaper, NASA, the FAA, and industry have published numerous technical studies, vision documents, white papers and concepts of operations for Urban Air Mobility. UAM is a subset of the Advanced Air Mobility (AAM), a National Aeronautics and Space Administration (NASA), FAA, and industry initiative to develop an air transportation system that moves people and cargo between local, regional, intraregional, and urban places previously not served or underserved by aviation using revolutionary new aircraft. While AAM supports a wide range of passenger, cargo, and other operations within and between urban and rural environments, UAM focuses on the transition from the traditional management of air traffic operations to the future passenger or cargo-carrying air transportation services within an urban environment [FAA 2020]. NASA published a Vision ConOps in 2020 intended as a foundation to engage members of the UAM community and provide a consensus on the future vision of UAM operations. It provides a concept for more detailed discussion and a basis for the exploration of ideas using a common framework to inform the continued development and integration of UAM as part of the broader transportation system [NASA 2020].

The present work follows assumptions regarding the UAM operating environment outlined in a 2020 NASA study [Graydon 2020] that investigated the application of FHA and STPA to an eVTOL aircraft operating in a UAM passenger carrying reference scenario. These assumptions regarding the environment, aircraft, and operating scenario are reproduced below: From [Graydon 2020]:

Environment Features:

[1] https://www.nasa.gov/sites/default/files/thumbnails/image/aam-design4-new-image-2-24-2021-3.jpg

- *A service area focused on a large modern city with features including an urban metropolitan landscape, high-rise buildings, a major airport hub, and active construction including large equipment and cranes*
- *Airspace shared with other manned and unmanned air traffic, VTOL and otherwise, and some form of Air Traffic Management (ATM)/UAS Traffic Management (UTM) in place*
- *A weather continuum spanning northern US winters and southern US summers, with representative temperature ranges, precipitation types and rates, and wind profiles*
- *Infrastructure sufficient to battery charging, dispatch, passenger management, and other associated needs, which can include takeoff and landing areas (TOLAs) ranging from cleared fields to purpose-built vertiports*

Aircraft Features

- *Distributed electric propulsion (DEP) realized by 6–8 independently controllable motor/rotor pairs*
- *Vertical takeoff and landing capability combined with wing-borne forward flight, enabled by a combination of rotors and wings which may be fixed or tilting*
- *Piloted control with possible limited autonomous capability (i.e., intermediate-stage UAM capability maturity)*
- *Design/configuration for passenger transit, up to five persons of which one will be the pilot*
- *Commuter distance flight ranges within and across metropolitan areas, up to 50 nautical miles and altitude of less than 10,000 ft*
- *Position reporting and communications appropriate to support ATM/UTM in a form to be determined*
- *Navigation appropriate to support precision route-following within the reduced separation minima likely to characterize the target urban environments*
- *Sensing appropriate to support encounter/conflict detection*
- *Transponding appropriate to support cooperative conflict management*

Operational Scenario

1. *Lift to hover (takeoff). The aircraft departs vertically from the pad at the origin TOLA and attains altitude appropriate to transition.*
2. *Transition to forward flight. The aircraft transitions from reliance on a vertical lift mechanism(s) to reliance on a fixed wing lift mechanism(s). This transition might involve a reconfiguration such as rotor or wing tilt.*
3. *Climb to en route. The aircraft continues gaining altitude until reaching the target altitude for en route flight.*
4. *En route. The aircraft flies its course at target altitude.*
5. *Avoidance. The aircraft maneuvers to deconflict with a detected collision hazard. Note conflict detection can rely on some degree of autonomy, depending on the concept. In this demonstration, the onboard pilot has the responsibility to see and avoid in accordance with 14 CFR §91.113.*

6. *Approach. The aircraft decreases altitude until reaching the target altitude for transition.*
7. *Transition to hover. The aircraft transitions from reliance on a fixed wing lift mechanism(s) to reliance on a vertical lift mechanism(s). This transition might involve a reconfiguration such as rotor or wing tilt.*
8. *Set down (land). The aircraft completes a vertical descent to land on the pad at the destination TOLA.*

1.1 Research Scope and Objectives

In a previous NASA-funded research effort, a team comprising Architecture Technology Corporation, Electron International II Inc., and Barron Associates identified, demonstrated, and evaluated RTA as an effective alternate concept to contemporary development assurance processes [Peterson 2020]. That research effort focused on a limited application of RTA to one flight control sub-function of a notional eVTOL aircraft. Other NASA-funded research developed considerations in assuring increasingly autonomous systems [Alves 2018]. Anderson, Fannin, and Nelson have proposed a taxonomy of flight automation system levels [Anderson 2018].

The work described in this report continues the research into run-time assurance for increasingly autonomous systems by demonstrating a broader application of RTA and examining the implications on: design and analysis of aircraft functions and systems; aircraft safety hazards; safety assurance; development assurance; and pilot tasks and performance. This work also examines the combined application of traditional FHA and the more modern STPA techniques to perform hazard analyses on aircraft with complex automated and autonomous systems and an onboard pilot [SAE 1996] [Leveson 2016] [Graydon 2020].

The scope of this research is to focus on eVTOL aircraft intended for UAM operations with airworthiness requirements from standard certification regulations for Part 23 and Part 27 normal category aircraft as applicable. The scope of the task includes the design and safety assessment at the aircraft function level and system level as discussed in SAE standards ARP4754A [SAE 2010] and ARP4761 [SAE 1996], as well as ASTM standards F3264 [ASTM F3264], F3061 [ASTM F3061], and F3230 [ASTM F3230]. The scope also includes the definition and safety assessment of tasks allocated to the onboard aircraft pilot, as well as the STPA hazard analysis technique.

The objectives of this research effort are:

- To demonstrate and evaluate the application of the RTA-based assurance concept to assure the safety of flight control functions of an eVTOL aircraft with highly automated or autonomous flight capability and a single onboard pilot.
- To demonstrate and assess the effectiveness of FHA and STPA combined as complementary hazard analysis techniques for an eVTOL aircraft with highly automated or autonomous flight capability and a single onboard pilot.

For this current study we build on our prior research effort [Peterson 2020], and we leverage other NASA, FAA, and industry research related to design and analysis of aircraft functions and systems; aircraft safety hazards; safety assurance; development assurance; and pilot tasks and performance.

Our prior research effort established a basic process for using RTA techniques to facilitate certification of an autonomous control component. That work focused on depth of analysis in consideration of a particular control function (automated landing), the design and application of appropriate control laws, the application of the RTA element to the flight/propulsion control system, and the performance of detailed hazard analysis (FHA/PSSA and Fault Tree Analysis) for the notional design. In this study, we expand that basic RTA process in both breadth and depth, along a number of dimensions including: 1) multiple interacting RTA-protected functions across various levels of automation; 2) interactions between the pilot, vehicle, and RTA-protected functions as well as pilot task loading and saturation; 3) application of RTA techniques to mitigate hazards associated with pilot error; and 4) hybrid analysis techniques to ensure that the resulting system is consistent with the assigned DAL.

As discussed in the previous study report [Peterson 2020], the control system architecture for many of the UAM aircraft designs, including the eVTOL vehicles that are the object of this study, will necessarily be much more complex than for existing commercial, general aviation, and rotary wing aircraft. The large number of rotational components and control surfaces, together with inherent dynamic instability, mean that piloting in a traditional “stick-to-surface” manner will not be feasible. Not only must the control system manage this complexity, it must also accommodate the limitations of minimally certificated pilots in command. A key question of this research is whether the control-centric approach adopted by STPA can be a valuable complement to traditional safety assurance processes for these systems.

One of the strengths of FHA is that it relies only on functional breakdowns of the aircraft and its systems, without relying on detailed design information about the components that will ultimately comprise the aircraft. One of the strengths of STPA is that it focuses on modeling interactions between functions and how these interactions can lead to unsafe control of the overall system. This research effort seeks to identify and characterize the potential synergy between these two approaches. For example, being more aware of the coupling between functions, an analyst conducing FHA might be able to identify additional and novel failure conditions. Likewise, being more aware of different types of failure conditions, usage of STPA might identify novel pathways and cascading scenarios that lead to unsafe control.

One of the key research questions that arises is whether the effectiveness of the two methods occurs at different levels of abstraction. For example, for STPA to be most effective, it might require implementation details that a conventional FHA otherwise may not. To answer this and other questions of how FHA and STPA can be used jointly to improve the assurance processes for UAM applications, we explore several specific notions of hazardous behaviors that many of the advanced subsystems may exhibit. We also model several control functions in STPA, as well as the coupling between them, to identify hazardous scenarios that arise due to interactions between pilots and automation.

1.2 Assurance Techniques

This research effort investigates safety engineering processes that may be well-suited for certification of UAM aircraft. We note that current aircraft safety engineering processes (SAE, ASTM, etc.) have served the public extremely well for decades but may not be well-suited for application to novel vehicle architectures that arise from future UAM visions. Still, there is no compelling reason to dismantle the framework they provide. Rather than fundamentally disrupting current processes, we seek to enhance them by investigating how integrating STPA and RTA may make current processes amenable to future aviation systems and aircraft designs. We explore these questions through development of two conceptual vehicle designs: 1) a baseline vehicle that leverages traditional processes and architectures to realize a UAM vehicle concept; and 2) an alternative vehicle design that leverages RTA architectures to (potentially) reduce the time/expense of those safety assurance and certification processes. Since both vehicles are intended to realize the same operational capabilities, most of the design is common to both vehicles.

1.2.1 Aerospace Recommended Practice

SAE ARP4754 [SAE 2010] was originally developed in response to a request from the FAA. The FAA requested that SAE define the appropriate nature and scope of system-level information for demonstrating regulatory compliance for highly integrated or complex avionics systems.

The guidelines in the document were developed in the context of US Title 14 Code of Federal Regulations (14CFR) Part 25. It was recognized at that time they may be applicable in the context of other regulations, such as Parts 23, 27, 29, 33, and 35.

The document is intended to be used in conjunction with ARP4761 and is supported by other aerospace standards such as RTCA DO-178B/C, DO-254 and DO-297, as illustrated in Figure 2.

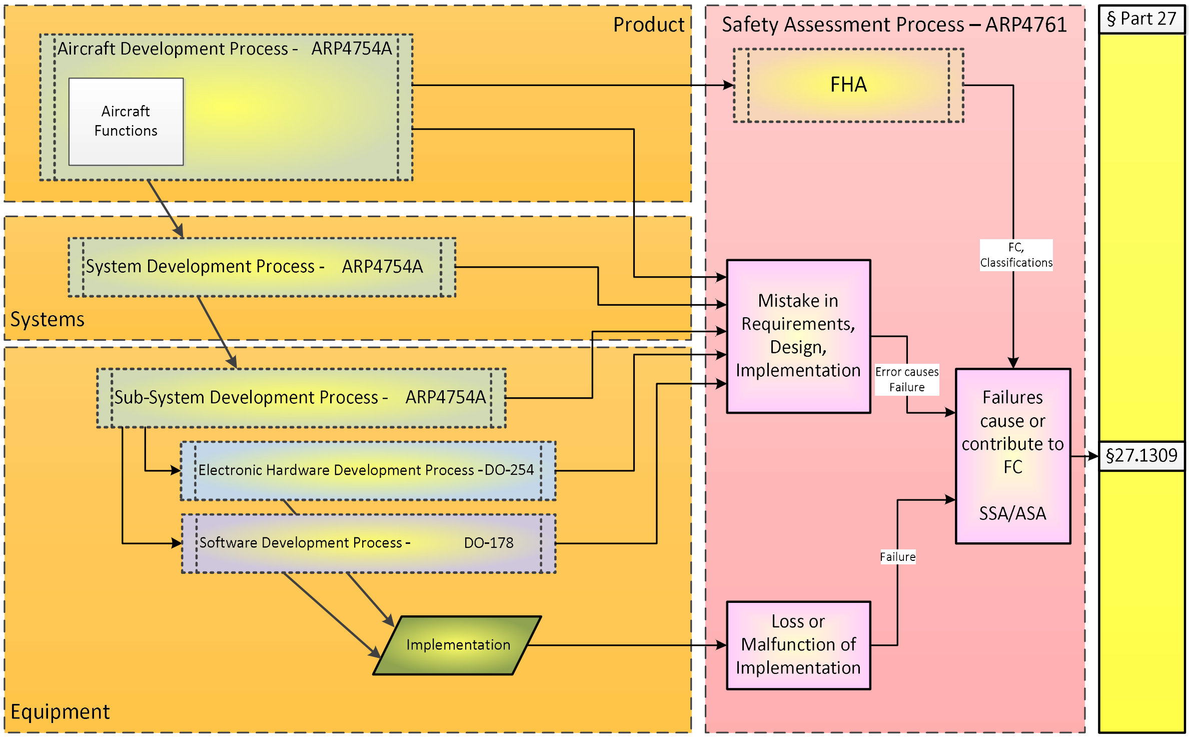

Product
Aircraft Development Process - ARP4754A
Aircraft Functions
Systems
System Development Process - ARP4754A
Equipment
Sub-System Development Process - ARP4754A
Electronic Hardware Development Process -DO-254
Software Development Process - DO-178
Implementation
Safety Assessment Process – ARP4761
FHA
FC, Classifications
Mistake in Requirements, Design, Implementation
Error causes Failure
Failures cause or contribute to FC
SSA/ASA
Failure
Loss or Malfunction of Implementation
§ Part 27
§27.1309

Figure 2. Traditional Development and Safety Assessment Process Link

ARP4754 provides recommendations for the development of aircraft and systems, considering aircraft functions and operating environment. It provides practices for ensuring the safety of the overall aircraft design, showing compliance with regulations, and assisting a company in developing and meeting its own internal standards. These practices include validation of requirements and verification of the design implementation for safety, certification, and product assurance.

Revision A of the document (ARP4754A) contains lessons learned from practitioner feedback and considers the evolution of the industry since ARP4754 was published. The relationship between ARP4754A and ARP4761, as well as their relationship with DO-178B/C and DO-254 are strengthened and discrepancies between the documents identified and addressed.

ARP4754A also explains the top-down development assurance concept for application at the aircraft and system levels. For aircraft and systems, Functional Development Assurance Level (FDAL) is introduced, and the term Item Development Assurance Level (IDAL) is used to describe the level of rigor of development assurance tasks performed on item(s). IDAL, referred to as ''Software Level'' in DO-178B/C and ''Design Assurance Level'' in DO-254, determines the development objectives that need to be satisfied for an item.

Following its publication, the FAA has recognized ARP4754A as an acceptable method for establishing a development assurance process in AC 20-174, Development of Civil Aircraft and Systems.

ARP4761 presents guidelines for performing safety assessments of civil aircraft, systems, and equipment consisting of the Aircraft Functional Hazard Assessment (AFHA), System Functional Hazard Assessment (SFHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Aircraft Safety Assessment (ASA) processes. Figure 3 illustrates the development process from ARP4754A and ARP4761 standards, as adapted for this effort.

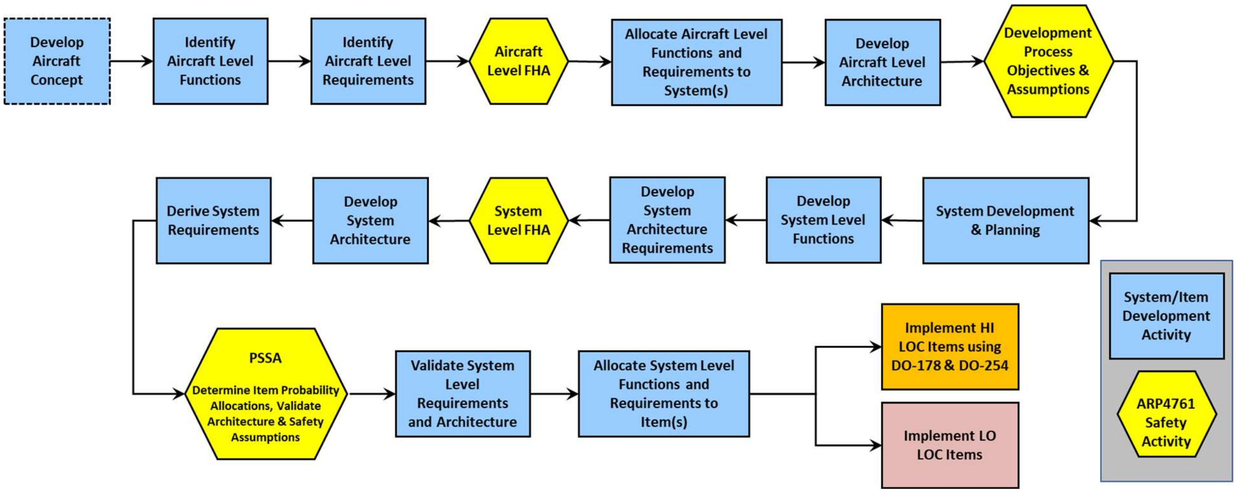

Develop Aircraft Concept
Identify Aircraft Level Functions
Identify Aircraft Level Requirements
Aircraft Level FHA
Allocate Aircraft Level Functions and Requirements to System(s)
Develop Aircraft Level Architecture
Development Process Objectives & Assumptions
System Development & Planning
Develop System Level Functions
Develop System Architecture Requirements
System Level FHA
Develop System Architecture
Derive System Requirements
PSSA
Determine Item Probability Allocations, Validate Architecture & Safety Assumptions
Validate System Level Requirements and Architecture
Allocate System Level Functions and Requirements to Item(s)
Implement HI LOC Items using DO-178 & DO-254
Implement LO LOC Items
System/Item Development Activity
ARP4761 Safety Activity

Figure 3. Case Study Development Process Adapted from SAE Standards

These guidelines may be used when addressing compliance with certification requirements such as 14CFR Parts 23, 25, 27, 29, 33 and 35. It may also be used to assist a company in meeting its own internal standards for safety assessments.

ARP4761 also presents information on the safety analysis methods that may be used to conduct the safety assessment process. These methods include Fault Tree Analysis (FTA), Dependence Diagram (DD), Failure Modes and Effects Analysis/Summary (FMEA/FMES), Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), and Common Mode Analysis (CMA).

The SAE S-18 Aircraft and System Development and Safety Assessment Committee, responsible for revisions to both ARP4754 and ARP4761, are working on updates to ARP4754A and ARP4761 and plan to release both, concurrently, in 2022.

1.2.2 Systems Theoretic Process Analysis

System-Theoretic Accident Model and Processes (STAMP) was created to treat safety as a control problem as opposed to a failure or chain-of-events type of problem and provides the basis for STPA. In the STAMP model of accident causality, accidents arise due to complex dynamic processes that may operate concurrently and interact to create unsafe situations, and accidents can then be prevented by identifying and enforcing constraints on component behavior and their interactions. This model attempts to capture accidents due to component failure, but also attempts to explain increasingly common component interaction accidents that occur in complex systems without any (or many) traditional component "failures." For example, software can create unsafe situations by behaving exactly as instructed or operators and automated controllers can individually perform as intended but together, they may create unexpected or dangerous conditions.

Control processes operate throughout the hierarchy whereby commands or control actions are issued from higher levels to lower levels and feedback is provided from lower levels to higher levels. Accidents arise from inadequate enforcement of safety constraints, for example due to missing or incorrect feedback, inadequate control actions, component failure, uncontrolled disturbances, or other flaws. STAMP defines four types of unsafe control actions that must be eliminated or controlled to prevent accidents:

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

One potential cause of a hazardous control action in STAMP is an inadequate process model used by human or automated controllers. A process model contains the controller's understanding of 1) the current state of the controlled process, 2) the desired state of the controlled process, and 3) the ways the process can change state. This model is used by the controller to determine what control actions are needed.

In software (and in general in automatic control systems), the process model is usually implemented in variables and embedded in the program's algorithms. For humans, the process model is often called the "mental model." Software and human errors frequently result from incorrect process models. Accidents like this can occur when an incorrect or incomplete process model causes a controller to provide control actions that are hazardous. While process model flaws are not the only cause of accidents in STAMP, they are major contributors.

STPA is a hazard analysis technique based on the STAMP accident causality model that is typically performed during the design of a system. STPA attempts to explain in a prospective way why an accident might occur, and these causal analysis results can then be fed back into the design to make it safer. Section 3.9 explains the processes used to perform STPA in more detail.

1.2.3 *Run-Time Assurance*

RTA can be thought of as an architectural design pattern that can allow the use of an advanced but untrusted algorithm to be used in an application that has high safety requirements. The architecture is illustrated in Figure 4, which shows an RTA-protected function that is constructed out of two alternative implementations of the same basic capability, one that is designated “low-confidence” and the other “high-confidence.” An RTA monitor is responsible for switching between these two implementations in a way that ensures safety of the system being controlled. In a typical application, the intent is to use the low-confidence implementation to the greatest extent possible, switching to the high-confidence alternative only when necessary.

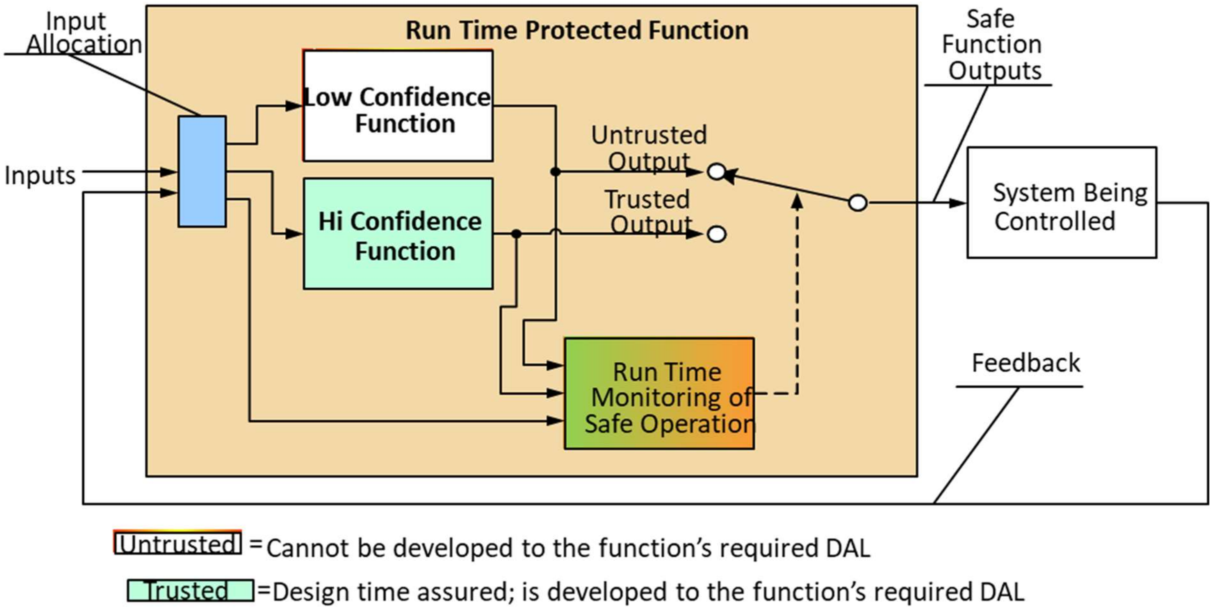

Input Allocation
Inputs
Run Time Protected Function
Low Confidence Function
Hi Confidence Function
Untrusted Output
Trusted Output
Run Time Monitoring of Safe Operation
Safe Function Outputs
System Being Controlled
Feedback
Untrusted =Cannot be developed to the function’s required DAL
Trusted =Design time assured; is developed to the function’s required DAL

Figure 4. General RTA Architecture

In the UAM applications addressed in this report, the low-confidence function corresponds to an advanced, adaptive, or otherwise difficult to certify algorithm. That is, the low-confidence function is one for which the time and or cost associated with developing it to the required functional DAL is prohibitive. In contrast, the high-confidence function corresponds to some more traditional algorithm that is readily developed to the required functional DAL. If the RTA monitor is defined and implemented correctly, the overall RTA-protected function can achieve the required functional DAL. Ultimately, the goal is to make an argument that the RTA protected system is equivalent in terms of safety to a system that consists of a single function implementation developed to the required DAL.

To support this goal, the RTA monitor must ensure that the controlled system always remains within a well-defined safe state space. This space is referred to as the Type I Safe Region and is illustrated in Figure 5. In general, the system being controlled will have some momentum, so the RTA monitor must switch from the low-confidence to high-confidence implementations before the state reaches the edge of the Type I Safety Region. The term Type II Safety Region refers to a subset of Type I space that carves out a “setback” that accounts for this momentum. The high-confidence controller must be engaged before the vehicle state leaves the Type II Safety Region in order to guarantee that the vehicle’s momentum will not carry it outside the original Type I space. Finally, the RTA monitor is typically implemented on a discrete-time computation system and is not capable of instantly checking safety associated with the vehicle’s state. The Type III Safety region accounts for potential time lag between successive checks performed by the RTA monitor. It carves out an additional setback from the Type II region that accounts for potentially erroneous behavior of the low-confidence controller between checks. The RTA monitor is designed to continually check whether the vehicle state is in the Type III Safety Region, and immediately switches to the high-confidence controller if the state is found to be outside this region.

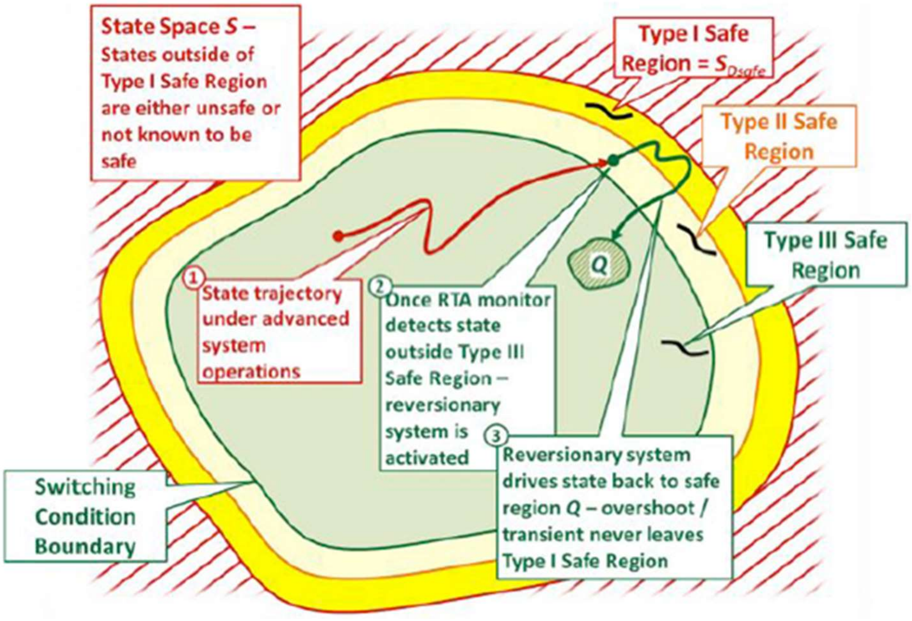

State Space S – States outside of Type I Safe Region are either unsafe or not known to be safe
Type I Safe Region = S_{Dsafe}
Type II Safe Region
Type III Safe Region
Q
1 State trajectory under advanced system operations
2 Once RTA monitor detects state outside Type III Safe Region – reversionary system is activated
3 Reversionary system drives state back to safe region Q – overshoot / transient never leaves Type I Safe Region
Switching Condition Boundary

Figure 5. Type I, II, and III Safety Regions [Schierman 2015]

For detailed discussions of the RTA, its application in aircraft control, and construction of these various safety regions, see [Schierman 2020], [Peterson 2020], and [Schierman 2015].

1.3 Task Order Structure

The task order for this research effort was titled “Run-Time Assurance for Electrical Vertical Takeoff and Landing Aircraft.” The task order was structured by NASA to facilitate examination of the research questions related to the application of ARP-based and STPA-based hazard analysis techniques to complex eVTOL aircraft functions both with and without the use of Run-Time Assurance. Figure 6 below is a notional depiction of the structure of the tasks for this research effort.

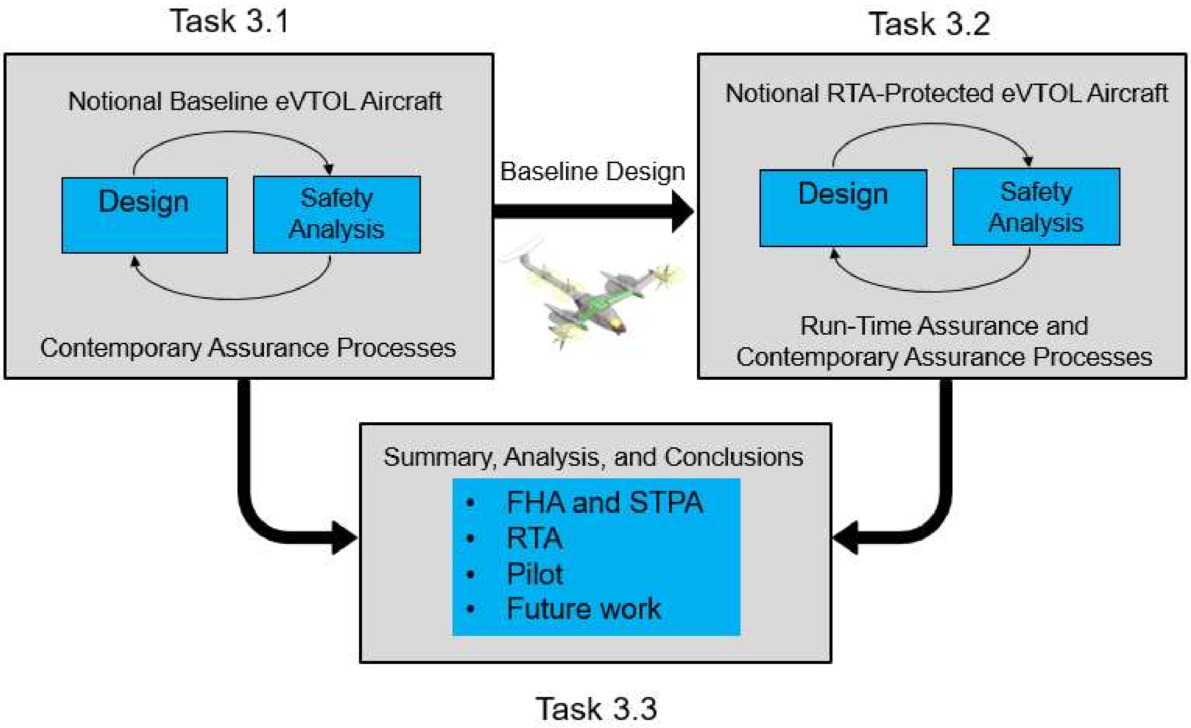

Task 3.1
Notional Baseline eVTOL Aircraft
Design
Safety Analysis
Contemporary Assurance Processes
Baseline Design
Task 3.2
Notional RTA-Protected eVTOL Aircraft
Design
Safety Analysis
Run-Time Assurance and Contemporary Assurance Processes
Summary, Analysis, and Conclusions
• FHA and STPA
• RTA
• Pilot
• Future work
Task 3.3

Figure 6. The task order structure specified by NASA enables a study of the application of ARP and STPA hazard analysis techniques to an eVTOL aircraft with and without RTA-protected functions.

For the sake of completeness and to enable readers to correlate descriptions of work performed with the task structure, we include a synopsis of the primary task descriptions and assumptions specified by NASA for this research effort.

Task 3.1 Notional Baseline eVTOL Aircraft

3.1.1 Define Notional Baseline eVTOL Aircraft

Define a notional baseline eVTOL aircraft with the following characteristics and considerations:

- Electrically powered
- Distributed electric propulsion
- Vertical takeoff and landing capability
- One onboard pilot with level of proficiency comparable to the requirements (knowledge, skill, and experience) for a single engine pilot’s license
- Seating capacity in the range of 4 to 6 passengers and one pilot
- Automated or autonomous flight capabilities
- Capable of operation under visual flight rules (VFR)

Assume operation in controlled airspace over an urban environment with prepared takeoff and landing zones (e.g., vertiports). The notional aircraft definition shall include information processing tasks performed by the pilot, such as the following:

- Aviate: control the aircraft speed and flight path (i.e., fly the aircraft)
- Navigate: determine the location and required course (i.e., fly the aircraft in the right direction)
- Communicate: manage radios and send and receive information (i.e., state the aircraft condition and intentions to ATC and other aircraft)
- Manage Onboard Systems: take care of batteries, electronics, sensors, automation systems, etc.
- Manage the Mission: plan the mission, be aware of the outcome of other tasks, and re-plan as necessary

The aircraft's automated and autonomous flight capabilities shall enable the pilot to transfer partial or complete responsibility to the onboard computers for the Aviate and the Navigate tasks. Automated and autonomous capability for the Communicate, Manage Onboard Systems, and Manage the Mission tasks is not required. Assume that the equivalent of a conventional VFR, single engine pilot's license would be required to operate the vehicle, and therefore standard mitigations currently attributed to an in-situ pilot in control (PIC) context would be applicable. However, given VTOL flight capabilities, assume that the aircraft will not have passive stability and control and that active fly-by-wire strategies will be required to prevent a catastrophic accident scenario.

For the notional baseline aircraft definition, contemporary development assurance processes and cockpit procedures (i.e., pilot tasks) should be used to assure operational flight safety. The notional baseline aircraft definition does not make use of the RTA concept as described in [Peterson 2020] to assure system and operational flight safety.

3.1.2 Perform Hazard Analysis using FHA and STPA

Perform a hazard analysis of the notional baseline eVTOL aircraft. The FHA and the STPA techniques shall be used for this hazard analysis as well as the System Safety Analysis SSA technique, if needed. In addition to hazard identification, the analysis shall determine the required Development Assurance Level (DAL) for the functions, systems, and items in the notional baseline aircraft definition.

Task 3.2 Notional RTA-Protected eVTOL Aircraft

3.2.1 Define Notional RTA-Protected eVTOL Aircraft

Apply the RTA concept as described in [Peterson 2020] to the notional baseline eVTOL aircraft. The notional baseline aircraft shall be modified by applying the RTA concept as a means to assure the safety of the flight control functions (i.e., mitigate hazards related to automated/autonomous flight capability, and the Aviate and Navigate pilot tasks). The RTA concept could be applied, for instance, to provide safety assurance for highly capable automation/autonomous systems, mitigate possible system development errors, and to provide protection against pilot error.

3.2.2 Perform Hazard Analysis using FHA and STPA

Perform a functional hazard analysis of the notional RTA-protected eVTOL aircraft. The FHA and the STPA techniques shall be used to perform the hazard analysis on the notional RTA-protected eVTOL aircraft as well as the System Safety Analysis SSA technique if needed. In addition to hazard identification, the analysis shall determine the required Development Assurance Level (DAL) for the various functions, systems, and items in the notional RTA-protected aircraft definition.

Task 3.3 Summary, Analysis, and Recommendations

3.3.1 Summarize the outcome of the research and provide recommendations for further investigation to advance the concept of run-time safety assurance. Include in this summary 1) a discussion on the effectiveness of FHA and STPA combined as complementary hazard analysis techniques; 2) a discussion of the efficacy of the RTA concept for safety assurance and the implications regarding design, analysis, and assurance of aircraft functions and systems; and 3) a discussion of any relevant safety-related considerations and implications of relying on the pilot to perform a role in the presumably high confidence backup functional paths of one or more RTA-protected function.

2.0 Aircraft Concept

2.1 eCRM-001 Aircraft Concept

Table 1. Notional eCRM-001 Vehicle Key Characteristics

Parameter	Characteristic
Crew	1
Passenger	4
Payload	900 lbs (408 kg)
Takeoff Gross Weight (TOWG)	5,130 lbs (2327 kg)
Range	60 miles (97 km)
Cruise Speed	130 kts (150 mph)
Stall Speed (airplane mode)	80 kts (92 mph)
Operation	Visual Flight Rules (VFR)
Average Flight Duration	30 minutes

The ATCorp Team developed this notional aircraft and example case study framework for a DEP VTOL vehicle based on Uber Elevate’s eVTOL Common Reference Model (eCRM-001). This example aircraft and system definitions are further expanded in this section to support the needs of the program in developing and assessing certification and safety assurance methods using RTA and STPA. The eVTOL aircraft is a powered-lift vehicle to be developed and certificated under Normal, Utility, Acrobatic and Commuter Category Airplane regulations for

VFR day use. The aircraft will be referred to as the eCRM-001 vehicle and has the key characteristics identified in Table 1.

The eCRM-001 eVTOL concept is shown in Figure 7. The eCRM-001 is sized for a single pilot and four passengers in a conventional two by two seating arrangement. The aft row is raised for a stadium seating arrangement. The center of gravity (CG) and center of thrust are located near the aft passenger row, and the design features a lifting tail to dynamically control the aerodynamic center. Batteries are located in the wings to help with span loading weight as well as wing root bending moments. The eCRM-001 is equipped with a single conventional pilot control and display to facilitate certificated and type rated pilots' control of vehicle functionality. The eCRM-001 is planned for use in urban air mobility-air taxi scenarios.

The eCRM-001 features a tilt rotor design augmented by multiple, retractable stacked lifting rotors for vertical flight, as illustrated in Figure 8. A conventional wing with a lifting T-tail is provided for forward flight. The vehicle features four pairs of stacked-rotors, two of which are wing-mounted and two pairs are mounted on the empennage. The stacked-rotor concept is designed to increase thrust, provide counter-torque function, and attenuate noise compared to a single rotor or counter-rotating rotor designs.

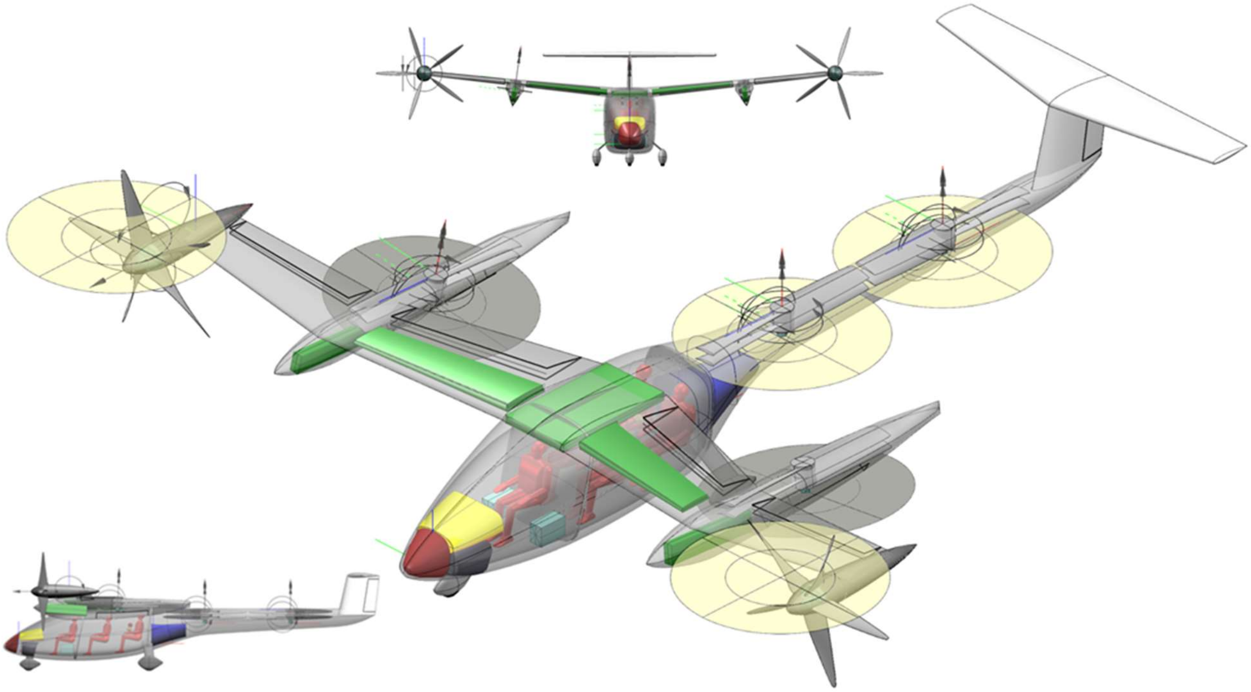


Figure 7. eCRM-001 Notional eVTOL Vehicle

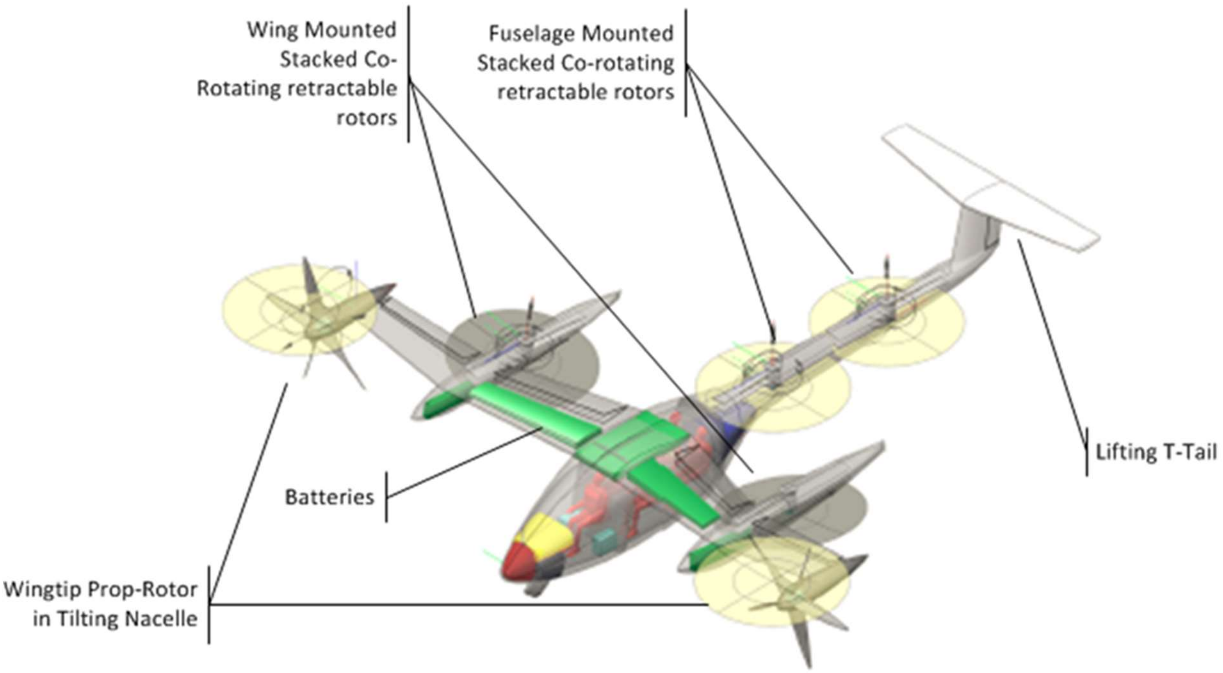

Wing Mounted Stacked Co-Rotating retractable rotors
Fuselage Mounted Stacked Co-rotating retractable rotors
Lifting T-Tail
Batteries
Wingtip Prop-Rotor in Tilting Nacelle

Figure 8. Key Configuration Elements of the eCRM-001

The eCRM-001 power train architecture is presented in Figure 9. Each wing tip propeller is driven by independent dual motors with dual controllers integrated using sprag clutches. Six high voltage battery busses provide redundant electric power to the wingtip and stacked rotor effectors.

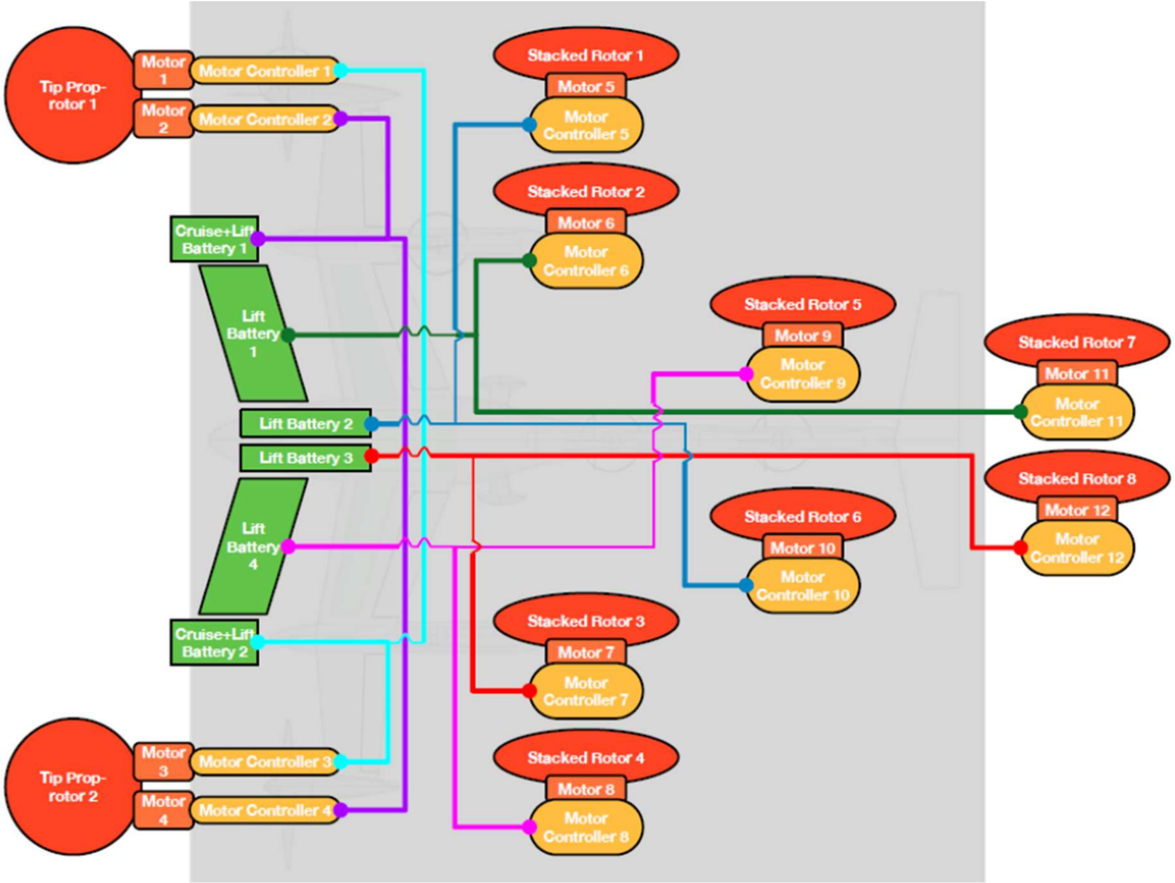


Figure 9. eCRM-001 Powertrain Architecture

2.2 Pilot Assumptions

This work assumes that UAM providers will initially deploy aircraft operated by highly trained pilots who have significant flight experience. Over time, however, UAM operators will transition to operations by minimally trained pilots as defined by the FAA and EASA. This will require a corresponding increase in the level of flight control automation, permitting these lesser trained pilots to handle the complexity of hover and transition flight modes associated with UAM operations [Wing 2020]. This increased automation will require certification of flight control software that is significantly different than previous Part 23 designs, and it is expected that the engineering expertise to directly produce and evaluate high-DAL implementations of this software may be underdeveloped. NASA has developed a timeline and concept called Simplified Vehicle Operations (SVO) that describes the transition from highly trained pilots to lesser trained pilots, with a corresponding increase in autonomy and system complexity [Goodrich 2015]. SVO investigates novel combinations of control strategies, inceptors, displays and automated systems technologies to decrease pilot workload and increase safety.

2.3 Unified Control Architecture

A nominal Primary Flight Control System (PFCS) architecture and corresponding pilot interaction is described in this section. The PFCS architecture describes the lowest level of control we expect the pilot to exercise when operating an UAM aircraft. The level of PFCS control utilizes relatively high control augmentation to help pilots of varying skill levels safely operate the UAM aircraft in a dense urban environment. Additional levels of autonomy are added to implement functions such as autonomous landings and takeoff, autonomous trajectory generation and tracking, obstacle avoidance, decelerate to hover, and flight planning.

The importance of a well-defined pilot interface and control architecture is amplified when considering safety aspects of current operations with expert pilots. Figure 10 shows that Loss of Control - Inflight (LOC-I) is the leading cause of transport category aircraft accidents, with similar trends for smaller aircraft [Boeing 2021]. This indicates pilot control difficulties are a major safety concern in current operations and it is anticipated that these difficulties will continue or may increase for UAM operations, where there will be an increase in air traffic density and obstacles. Note that many UAM manufacturers are proposing flight envelope protection to address LOC-I accidents. This requires additional software to be certified. The increased autonomy and other systems, such as envelope protection, expected for SVO is accompanied by an increase in system complexity and safety requirements. Note also that the second leading contributor to incidents is Controlled Flight Into Terrain (CFIT), which may be influenced by situational awareness, and the fourth reason is operations on the runway (takeoff or excursion).

The control architecture heavily leverages the so-called unified control concept that was most recently implemented on the F-35B aircraft and developed through a series of experimental test programs. The unified control concept is based on four fundamental principles [Lombaerts 2020]:

1. The inceptors should generally control aircraft movement in the same direction as inceptor movement.
2. The number of inceptors operated by each hand should be minimized.
3. Cockpit workload should be equally divided between the left and right hands.
4. It should not be necessary to remove either hand from the inceptors during the most critical phases of flight, including take-off and landing.

2.3.1 F-35 Unified Control Paradigm

The F-35B implemented these principles, resulting in a cockpit design with 3 inceptors, where the pilot commands different aircraft states depending on the flight regime. The flight regimes correspond to wing-borne flight, transition, and jet-borne (hover or vertical) flight. The pilot commands are summarized in Figure 11 [Walker 2013] and vary based on a combination of airspeed and groundspeed. Note that regardless of the specific state controlled by the pilot in different flight regimes, inceptor movement in each axis always commands aircraft motion in the same axis. This reduces pilot workload by eliminating the need for conscious mode switches throughout the flight envelope. The right-hand inceptor (RHI) is a two-axis active sidestick that controls motion in the vertical axis and lateral axis, see Figure 12. At high speeds in wing-borne flight, forward and aft movement of the RHI controls altitude via a flight path rate - flight path hold command response type. In jet-borne / hover mode, RHI longitudinal motion control height rate and the control laws implement a rate command, height hold (RCHH) command response type. These command response types are blended between 45-55 knots (airspeed).

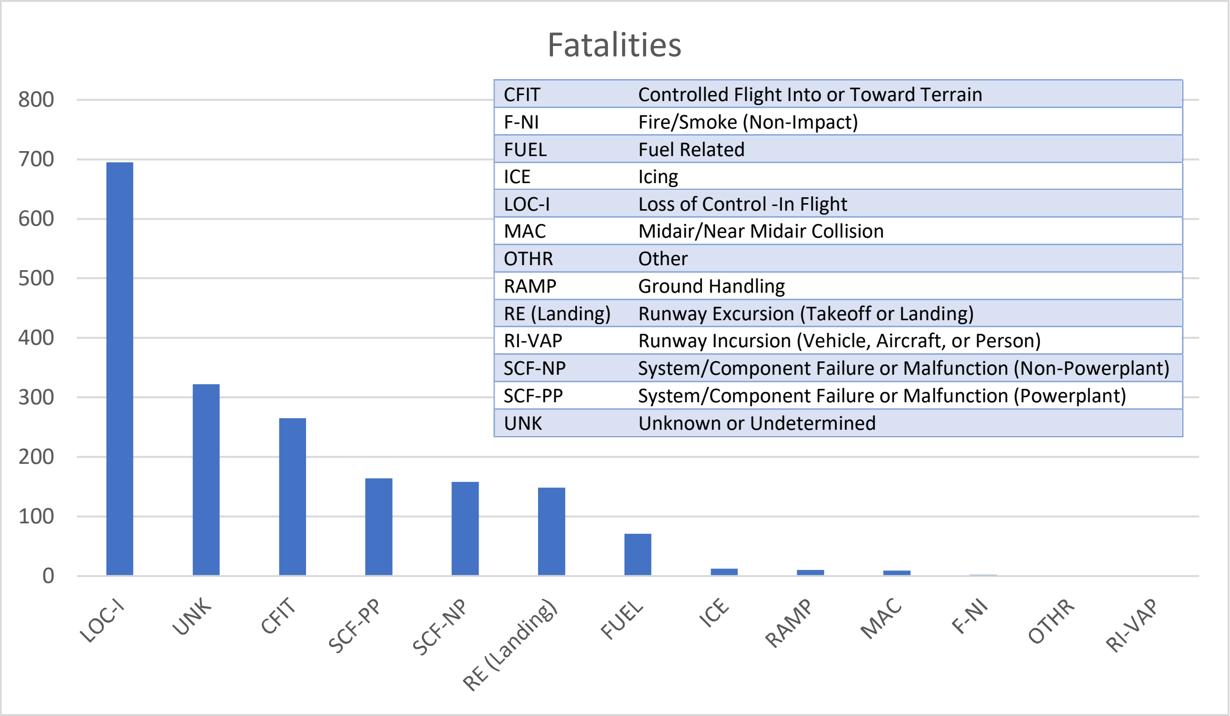


Figure 10. Fatal Occurrences in the Worldwide Commercial Fleet (2011-2020)

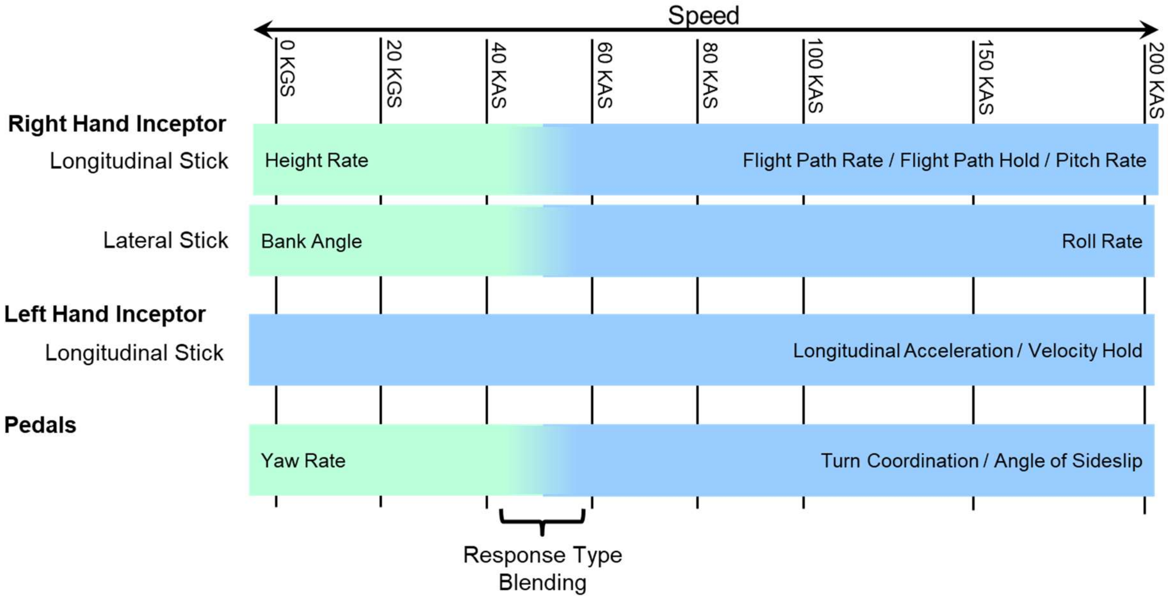


Figure 11. F-35 Pilot command response type blending

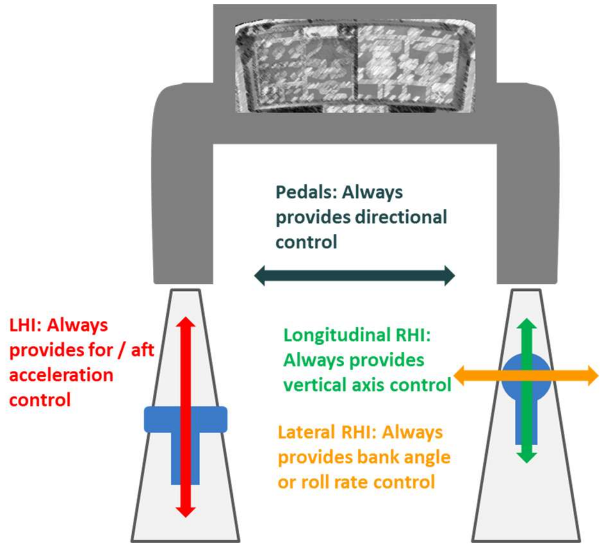

Pedals: Always provides directional control
LHI: Always provides for / aft acceleration control
Longitudinal RHI: Always provides vertical axis control
Lateral RHI: Always provides bank angle or roll rate control

Figure 12. F-35 Pilot Inceptors

Lateral movement of the RHI commands roll rate at high airspeeds and transitions to bank angle command and hold (attitude command, attitude hold ACAH) response type in jet-borne flight. The pedals always control the yaw motion of the aircraft. At high airspeeds pedal motion is used to command sideslip and otherwise used in a Turn Coordination control law. This command is blended to a rate command, direction hold (RCDH) response type in jet-borne flight. The left-hand inceptor (LHI) always controls motion in the longitudinal axis and implements an acceleration command, velocity hold (AcCVH) response type throughout the flight envelope. The pilot also has the option to activate a Translational Rate Command (TRC) command response type in jet-borne flight where the LHI and lateral motion of the RHI command longitudinal and lateral velocity, respectively. This is a velocity command, velocity hold response type. A consequence of this inceptor layout is in hover mode, the pilot is required to use two inceptors to command motion in the horizontal plane, departing from the helicopter paradigm of using a single inceptor for horizontal motion.

2.3.2 Unified Control Architectures for UAM

The F35 unified control architecture was designed, tested, and is operated by professionally trained, expert pilots. Additional research and experimentation are warranted to determine if the control response types implemented in the F-35 are suitable for eVTOL UAM vehicles with pilots of varying skill and training. One such study was recently conducted by NASA to study different SVO implementations, including control architectures that featured different pilot inceptor-to-command mappings [Lombaerts 2020]. In this study, three command structures of pilot interaction were evaluated, summarized in Table 2. The pilot commands are parameterized by the variables $(\delta_{lon}, \delta_{lat}, \delta_{ped}, \delta_{col})$, typically found in rotorcraft controllers. The pilot command variables are mapped to inceptor motion at the beginning of the table, where $(\delta_{lon}, \delta_{lat})$ are from the right-hand inceptor, δ_{col} from the left-hand inceptor, and δ_{ped} from the pedals or a twisting / rotation of the RHI. The conventional controller implements what can be thought of as a controller that could be found in a traditional rotary-wing vehicle. At hover it employs TRC in the longitudinal and lateral axes, RCHH in the vertical axis, and RCDH in the yaw axis. In forward flight, the control transitions to a rate command system with turn coordination and direct control of sideslip with the pedals. The Unified control concept follows the F-35 architecture. The EZ-Fly concept is a design implemented and tested by NASA in the 1990s. It exhibits the fewest control mode changes of the three concepts. Based on initial testing conducted in this study in the NASA ACELeRATE lab, the Unified control architecture was selected for additional testing in the NASA Vertical Motion Simulator.

Table 2. Pilot inceptor mappings for different control architectures [Lombaerts 2020]

	Inceptor Motion	RHI - lon	RHI - lat	Pedal	LHI
Controller	Flight Mode	δ_{lon}	δ_{lat}	δ_{ped}	δ_{col}
Conventional	Hover	u_x	v_y	$\dot{\psi}$	$\dot{h}$
	Transition	θ	ϕ	$\dot{\psi}$ / β	$\dot{h}$
	Forward	$\dot{\theta}$	$\dot{\phi}$	β	$\dot{h}$
Unified	Hover	$\dot{h}$	v_y	$\dot{\psi}$	$\dot{u}_x$
	Transition	γ	ϕ	β	$\dot{V}_{grd}$
	Forward	γ	$\dot{\phi}$	β	$\dot{V}_{CAS}$
EZ-Fly	Hover	$\dot{h}$	$\dot{\psi}$	v_y	$\dot{u}_x$
	Transition	$\dot{h}$	$\dot{\psi}$	v_y	$\dot{V}_{grd}$
	Forward	$\dot{h}$	$\dot{\psi}$	v_y	$\dot{V}_{CAS}$

2.3.3 Pilot Interaction and Control Architecture for eCRM-001 Aircraft

Based on the literature review summarized in the prior sections and acknowledging that eVTOL control and pilot interface is an active and ongoing research topic, a representative control architecture will leverage the unified control concept used in the F-35B and studied in [Lombaerts 2020]. Proposed modifications to the architecture include:

- Hover mode: For the pitch and roll axes make TRC the primary (default) control mode and use ACAH as a backup control mode the pilot can select with a switch or if there is a failure somewhere in the system that would cause TRC to be unreliable.
- Hover mode: Add position hold control to the TRC controller.

The control architecture is summarized in Table 3 and Table 4, which present the pilot-inceptor mapping and command response type, respectively, for the different flight regimes. Figure 13 illustrates the response types and blending between flight regimes. The transition between different control modes is scheduled with a combination of commanded ground speed and airspeed and is transparent to the pilot. Mode annunciation and visual cues indicate the current control mode and flight regime. The angle of the nacelles is also a function of commanded speed.

Table 3. eCRM-001 pilot inceptor mapping

	Inceptor Motion	RHI - lon	RHI - lat	Pedal	LHI
Controller	Flight Mode	δ_{lon}	δ_{lat}	δ_{ped}	δ_{col}
eCRM-001 Unified	Hover	$\dot{h}$	$v_y(\phi \text{ backup})$	$\dot{\psi}$	$u_x(\theta \text{ backup})$
	Transition	γ	ϕ	β	$\dot{V}_{grd}$
	Forward	γ	$\dot{\phi}$	β	$\dot{V}_{CAS}$

Table 4. eCRM-001 Command Response Type

Controller	Flight Mode	Vertical	Roll	Yaw	Pitch
eCRM-001 Unified	Hover	RCHH	TRC (ACAH backup)	RCDH	TRC (ACAH backup)
	Transition	FPC	ACAH	TC / AOS	AcCVH
	Forward	FPC	RCAH	TC / AOS	AcCVH

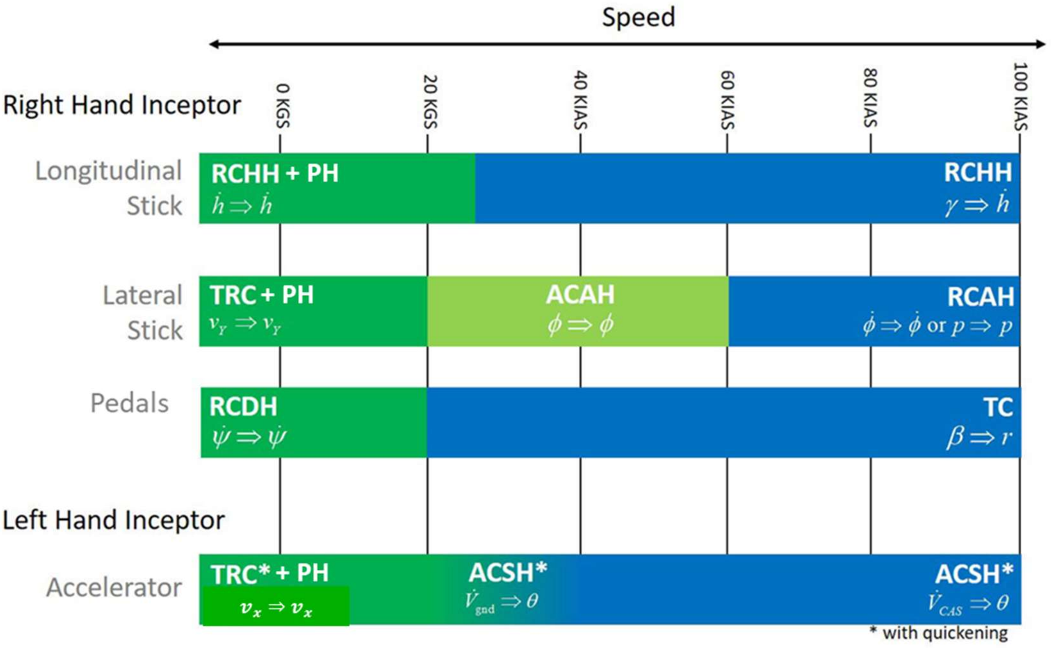


Figure 13. eCRM-001 pilot command response type blending

2.4 Turbulence Mitigation

UAM operations will occur in urban settings featuring complex operating environments that involve complicated wind patterns and gusts. Wind flow and gust models are less developed for urban environments, particularly regarding impacts on the new UAM vehicle designs, than at higher altitudes for commercial fixed-wing aircraft. Development of wind flow and gust models in the urban atmosphere has been slow in large part because of experimental difficulties. A major challenge is the large degree of spatial and temporal heterogeneity of these flows that makes data collection a challenge. Air flow in the roughness sublayer (RSL) is strongly influenced by the wakes of roughness elements such as individual buildings. The resulting spatiotemporal variability is challenging to sample in three dimensions at sufficient resolution. Moreover, many of the most commonly employed turbulence models include assumptions (e.g., horizontal homogeneity) that do not hold in urban environments. Consequently, atmospheric models have poor performance at the scale of urban buildings.

For this reason, computational fluid dynamics (CFD) models have been developed in recent years with some comparisons to empirical data [Hanna 2006], including large-eddy simulations that can resolve the wind flow to a scale sufficiently small to apply to UAM aircraft. The challenges with modeling the ambient wind flow and turbulence has a direct impact on UAM operations and design, as developers and control law designers must cope with a large degree of uncertainty in wind and gust models used to evaluate a design in simulation. Common gust models such as the Dryden and Von Karman spectra are applied to fixed-wing aircraft operating at a speed much greater than the ambient wind speed, allowing the assumption of a *frozen gust field*. This assumption does not apply when operating at slow speeds such as the transition and hover flight regimes of UAM vehicles.

The urban setting complicates wind flow owing to the heterogeneity of the building profiles. A classification of various zones in the atmosphere over urban areas consists of the urban boundary layer (UBL), urban canopy layer (UCL), and RSL [Rotach 1999, Fernando 2010]. Figure 14 graphically depicts these different zones. The UCL extends to the average building height while the RSL extends to multiple (2-5) times the average building height. The flow and dispersion complexity increase as height decreases, caused by the roughness of the urban topology and resulting turbulence. There are large flow variations downstream of buildings and in street canyons caused by wakes, vortices, and channeling effects. Stagnation points on the windward side of buildings can cause significant updrafts at the building edge. In addition to ambient winds, vortices generated by aircraft in wing-borne flight and rotor wakes in hover mode further exacerbate the potential disturbances when aircraft operate in close proximity to each other. Vehicle-to-vehicle wake interaction modeling for UAM operations was recently presented in [Nguyen 2021].

Due to the complex flow environment expected for UAM operations and the reduction in pilot training over time as envisioned in the SVO development plan, a control strategy that seeks to reduce turbulence effects, improve ride quality, improve handling qualities, and reduce pilot workload is a critical design element. In the control design for this project, an adaptive TRC controller is proposed to achieve these objectives and is described in subsequent sections.

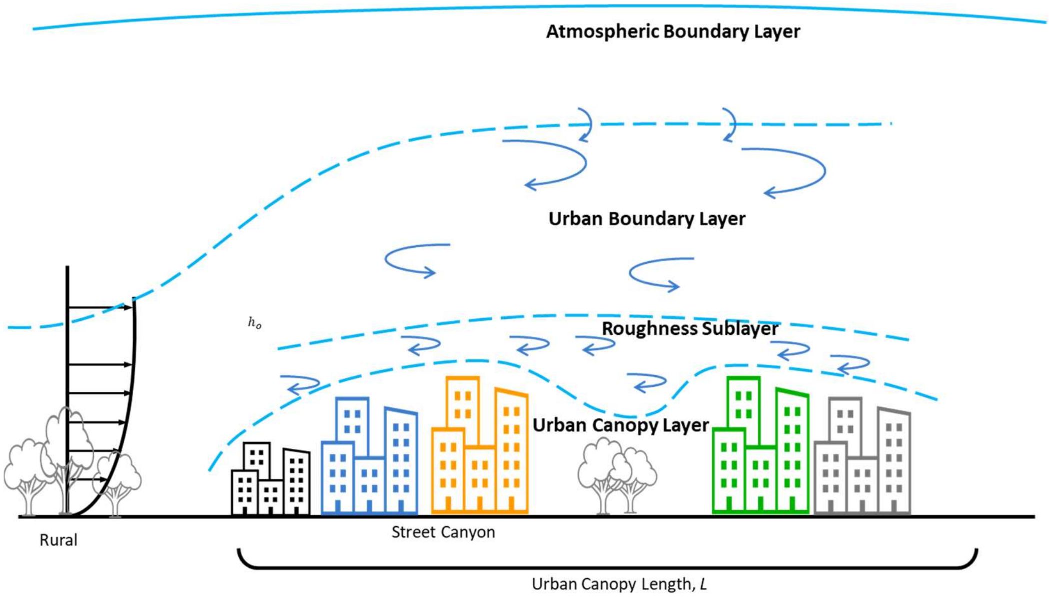


Figure 14. Depiction of atmospheric layers

2.5 Path Efficiency

The AAM initiative envisions extensive use of novel vehicle designs of varying sizes and a significant use of complex autonomous systems to achieve a variety of missions ranging from regional transport to intra-city passenger and goods transport, to autonomous package delivery. Considering the different phases of flight for different types of missions and vehicles operating under the AAM umbrella, this project focuses on what can be considered the most challenging mission: safe intra-city passenger transport. These operations will be conducted almost entirely above populated areas at low altitudes and eventually with reduced pilot training, as autonomous systems gradually are certified to perform piloting tasks.

The density of air traffic is expected to increase significantly, particularly in the low-altitude urban regions. Any required collision avoidance maneuvers will be performed in an environment with complex spatial and temporal constraints, which arise from the cluttered and dynamic operating space, obstructions and obstacles that may be permanent or changing (e.g., flocks of birds or construction cranes), permanent or dynamic flight restrictions in certain areas, noise concerns, and environmental impacts (e.g., ecosystem impact of increased vehicle operations). Moreover, these regions are associated with complex wind and turbulence environments that differ greatly from those experienced at higher altitudes, due to the roughness of urban features, thermal variation, vehicle-generated wakes, and a variety of other factors.

In this complex setting the ability to accurately track a given trajectory (a 3D spatial path with time constraints) is a critical capability. Additionally, the ability to satisfy stringent performance requirements coupled with a desire to minimize power expenditure creates a challenging space to both generate safe and efficient paths and then track them in an optimal manner. The traditional approach of tracking a series of waypoints through a series of connected lines and arc segments may not be adequate for AAM and UAM operations. Such a system should be robust and resilient to the aforementioned challenges in urban operations and be adept to quickly respond to nonlinear dynamics germane to many of the novel AAM / UAM vehicle designs. To summarize, a trajectory tracking control approach should consider the following, which we note is only a subset of a full requirements list: changing vehicle dynamics, external disturbances, nonlinear dynamics, optimize against multiple and potentially competing criteria, (e.g., tracking error, actuator usage, energy consumption), explicitly account for input, output, and state constraints, provide accurate tracking needed for congested areas, and accurately track more complex paths, (i.e., not just waypoints linked by line and arc segments).

2.6 Collision Avoidance

A robust collision avoidance system is a key element in safe AAM operations. As the level of autonomy increases and the training and experience of pilots lessens as envisioned by the SVO concept, a resilient collision avoidance system that is independent of external aircraft systems (i.e., systems not hosted on the aircraft) will be critical to system and operational safety. This is especially true during the take-off and landing flight phases where aircraft density can be expected to increase, obstacles are greater, and the vehicle may be buffeted by winds and turbulence not typically experienced by high-altitude flight. In [Wing 2020] the authors note the importance of achieving a high level of autonomy in the onboard vehicle systems:

> *Achieving such resiliency calls for AAM to incorporate goals for vehicle autonomy, in which the capability for a high degree of operational independence is integrated into the vehicle's onboard flight management functional design.*

We extend this recommendation to include collision avoidance between cooperative and non-cooperative vehicles or objects. While ground-based sensors may provide additional data of operating aircraft, this is susceptible to communication delays and failures and does not account for non-flying objects, e.g., power lines, cranes, etc., ground-based objects, and may not offer sufficient situational awareness to the PIC or collision avoidance system.

There is a distinction between flight management / flight planning and collision avoidance. There is also a distinction between pre-flight planning and inflight planning or management, although each of these functions deals with the flight path of the vehicle. In [Wing 2020] the authors categorize different functions in the following primary groups:

- Mission Management: These functions "…are monitoring the mission itself, assessing the likelihood of successful completion and preparing contingencies." Example functions include flight planning and contingency planning.
- Flightpath Management: These functions are "…associated with achieving the current mission in the most effective way. It acts upon 'non-hazard' changes in the operating environment where successful mission completion is likely." Examples of these functions include flight optimization, constraint conformance, conflict detection and resolution, and flight replanning to recover a nominal path or reengage the mission.
- Tactical Operations: These functions act on immediate hazards with a shorter time to resolve a hazard and typically involves ignoring mission parameters and objectives for a time while the hazard is resolved. The collision avoidance function is in this category.

During pre-flight planning, separation assurance between UAM vehicles is enforced with temporal and spatial route deconfliction and adherence to performance standards specified for operation in UAM corridors. As stated in the FAA CONOPS for UAM operations [FAA 2020],

> *Separation of operations within UAM Corridors is assured through various strategic and tactical methods. The primary method is strategic deconfliction based on collaborative flight intent sharing. Tactical separation is allocated to the UAM operators, including PIC and aircraft capabilities, and may include support from the PSUs.*

Preflight planning can be categorized as a strategic measure. Tactical methods for separation assurance include inflight planning / flight management and collision avoidance capability. As further stated in [FAA 2020],

> *In addition to strategic deconfliction within UAM Corridors that occurs during UAM flight planning, responsibilities also exist for in-flight coordination to ensure tactical separation is maintained. The PIC, supported by the UAM aircraft's capabilities (e.g., DAA) and possibly PSU services (e.g., flight data from active operations in the UAM Corridor), maintains separation from other operations within the UAM Corridor.*

In this context inflight planning or management can include the ability to adjust or replan the flight path to accommodate obstacles or hazards that have a relatively "long" time to closest point of approach (τ_{CPA}). The replanned path avoids the hazard / obstacle but has sufficient time to make "comfortable" flight maneuvers to maintain a high degree of ride quality. Once clear of the hazard, the replanner recovers the nominal / original path. Collision avoidance considers a more immediate hazard, or smaller τ_{CPA} and generally requires a more aggressive maneuver to maintain separation. The safety of passengers is endangered and requires a fast response. The maneuver may reduce passengers' comfort and the primary importance is to maintain safety of the vehicle and passengers. In both cases of strategic flight management and tactical collision avoidance, cooperative and non-cooperative hazards can be encountered.

A cooperative hazard is one which communicates pertinent information to other UAM vehicles and PSUs. The shared information may include vehicle identification number, state information, and intent information that can be utilized to perform a cooperative hazard resolution maneuver. Non-cooperative hazards or objects are aircraft that do not communicate such information or are other objects such as avian, cranes, sUAS, etc. ATC coordination is not anticipated to assist with separation assurance while vehicles operate in the UAM corridors but in contingency scenarios when the UAM vehicle is forced to exit the UAM corridor, then ATC should be notified and the UAM operator should activate ADS-B out [FAA 2020]. For each case considered it is envisioned that a vehicle-to-vehicle communication system will exist for UAM operations, similar to Mode S transponders for current commercial aircraft, and that exteroceptive onboard vehicle sensing is available for the UAM vehicles. The exteroceptive sensors should be able to sense air and ground hazards at a minimum performance level and could be implemented with a multi-modal sensor suite featuring LIDAR, radar, and EO/IR sensors. These sensors are a critical element in detection, tracking, and identification of non-cooperative / non-communicative aircraft, airborne hazards, and ground hazards.

In the case of non-cooperative aircraft, a form of *implied cooperation* can be utilized by the collision avoidance system by following established *rules-of-the-air* in determining the avoidance maneuver. These rules-of-the-air can be added as hard or soft constraints in the collision avoidance algorithm to guide expected behavior of the ownship and hazard aircraft. For example, if two aircraft are converging in a head-on trajectory then each vehicle should maneuver laterally to its right. In another case with sufficient altitude to perform a vertical maneuver, the vehicles should climb or descend so as to not cross altitude paths.

Design standards for detect and avoid (DAA) systems for UAM Vehicles used for collision avoidance systems are still in development and are expected to be included in the release of the ACAS-Xr standard. Additionally, as autonomous systems mature and certification approaches are developed to certify highly autonomous or fully autonomous systems, the PIC may become a remote PIC or supervisor managing the operation of multiple aircraft. In this scenario, the remote PIC has degraded situational awareness compared to an onboard PIC. This motivates the design and analysis of an onboard collision avoidance system that can function independently of any systems or data sources external to the aircraft. This is the class of collision avoidance functions analyzed in this report. We also restrict our attention to UAM operations and limit analysis of interoperability between systems like TCAS II or ACAS-Xa, other than to require that the onboard collision avoidance system be able to work with other collisions avoidance systems in resolving conflicts.

3.0 Baseline Aircraft Development

This section describes development of the baseline aircraft. It focuses on three functions within the control hierarchy of the eCRM-001 aircraft: control of the vehicle's horizontal velocity when in hover mode, path following (autopilot) control, and automated collision avoidance. These functions were chosen to permit an investigation of issues surrounding certification of advanced control algorithms, the advantages of RTA-protection for such algorithms, and the potential usefulness of STPA as a technique to support more traditional aircraft development processes.

3.1 Certification Basis and Means of Compliance

The eCRM-001 aircraft is the same as that used in the previous task study [Peterson 2020]. As noted in that task study report, there is no airworthiness standard in the Code of Federal Regulations Title 14 (14CFR) Part for an eVTOL aircraft. However, in light of the new and novel nature of eVTOL aircraft, the FAA Policy and Innovation Branch is currently working with a number of manufacturers seeking type certification of their eVTOL aircraft to determine certification basis and Means of Compliance (MOC). In common with most of the ongoing and imminently expected eVTOL type certification programs, the proposed eCRM-001 type certification path is under 14CFR 21.17(b). The certification basis is primarily under regulations in 14CFR 23 Amendment 23-64 (Airworthiness Standards: Normal Category Airplane), with additional applicable regulations from 14CFR Parts 27 (Airworthiness Standards: Normal Category Rotorcraft) and Part 35 (Airworthiness Standards: Propellers).

The FAA advisory circular AC23.2010.1 references the ASTM consensus standards which form the MOC to the regulations in14CFR Amendment 23-64 In addition to the ASTM standards, SAE ARP4754A, as invoked by FAA AC20-174, provides additional rigor in the eCRM-001 development assurance process, and is used in assigning appropriate development assurance levels.

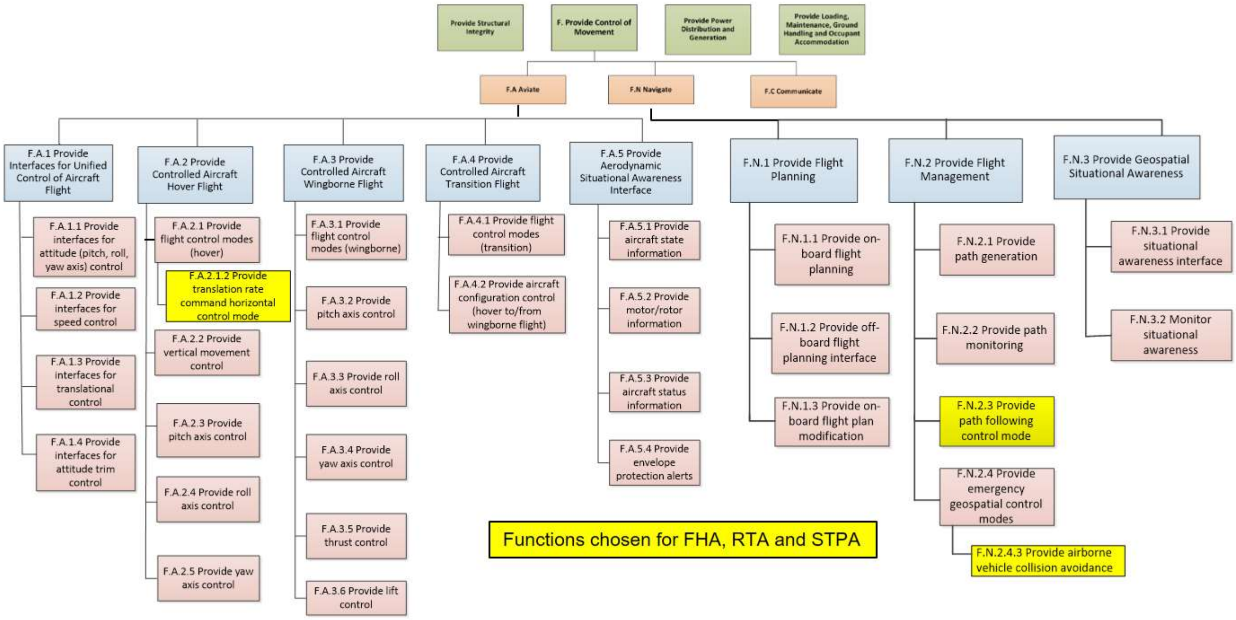
3.2 Aircraft-Level Functions and Functional Hazards

Much discussion has focused on how to define an appropriate list of aircraft functions for UAM. Difficulties stem from aircraft novelty, new kinds of automation, and misunderstanding of function lists. Function list focuses on what a thing (aircraft or system) must do, not what it has. This is because you cannot know how a thing may fail unless you know what it is supposed to do. FHAs explore the various senses in which a function may not be fully provided and the resulting safety consequences. These result in lists of failure conditions, anticipated effects, and classification. Aircraft function list and AFHA are devoid of references to the architecture, systems, and components that comprise the aircraft, excepting only those that are fundamental to the aircraft concept.

The FHA worksheets traditionally evaluate failure conditions as to their effect on the A-aircraft, B-crew and C-occupants. Expanding the safety hazard space to include effects external to the aircraft such as people on the ground, buildings and other aircraft has been the topic of research in both the FAA and NASA communities. As such, expanding this particular FHA to include the effects on D-other aircraft, E-people on the ground and F- property on the ground was not performed, especially considering that for the functions chosen, they already lead to catastrophic losses.

3.2.1 Aircraft Level Functions

Figure 15 gives the functional decomposition used for this task study. The top-level functions as shown (green boxes) are the same as the previous task study. Similar to the previous task study, the top-level function of “Provide Control of Movement” is used. For this task study, the next levels down are decomposed into Aviate, Navigate and Communicate, in order to facilitate the role of the pilot and automation in the eVTOL aircraft and its environment. Further functional decomposition is shown for the Aviate and Navigate functions as they are the functions of interest for this task study. The three sub-functions used for analysis for this task study are shown in the yellow boxes in Figure 15.



Provide Structural Integrity
F. Provide Control of Movement
Provide Power Distribution and Generation
Provide Loading, Maintenance, Ground Handling and Occupant Accommodation
F.A Aviate
F.N Navigate
F.C Communicate
F.A.1 Provide Interfaces for Unified Control of Aircraft Flight
F.A.2 Provide Controlled Aircraft Hover Flight
F.A.3 Provide Controlled Aircraft Wingborne Flight
F.A.4 Provide Controlled Aircraft Transition Flight
F.A.5 Provide Aerodynamic Situational Awareness Interface
F.N.1 Provide Flight Planning
F.N.2 Provide Flight Management
F.N.3 Provide Geospatial Situational Awareness
F.A.1.1 Provide interfaces for attitude (pitch, roll, yaw axis) control
F.A.1.2 Provide interfaces for speed control
F.A.1.3 Provide interfaces for translational control
F.A.1.4 Provide interfaces for attitude trim control
F.A.2.1 Provide flight control modes (hover)
F.A.2.1.2 Provide translation rate command horizontal control mode
F.A.2.2 Provide vertical movement control
F.A.2.3 Provide pitch axis control
F.A.2.4 Provide roll axis control
F.A.2.5 Provide yaw axis control
F.A.3.1 Provide flight control modes (wingborne)
F.A.3.2 Provide pitch axis control
F.A.3.3 Provide roll axis control
F.A.3.4 Provide yaw axis control
F.A.3.5 Provide thrust control
F.A.3.6 Provide lift control
F.A.4.1 Provide flight control modes (transition)
F.A.4.2 Provide aircraft configuration control (hover to/from wingborne flight)
F.A.5.1 Provide aircraft state information
F.A.5.2 Provide motor/rotor information
F.A.5.3 Provide aircraft status information
F.A.5.4 Provide envelope protection alerts
F.N.1.1 Provide on-board flight planning
F.N.1.2 Provide off-board flight planning interface
F.N.1.3 Provide on-board flight plan modification
F.N.2.1 Provide path generation
F.N.2.2 Provide path monitoring
F.N.2.3 Provide path following control mode
F.N.2.4 Provide emergency geospatial control modes
F.N.2.4.3 Provide airborne vehicle collision avoidance
F.N.3.1 Provide situational awareness interface
F.N.3.2 Monitor situational awareness
Functions chosen for FHA, RTA and STPA

Figure 15. Aircraft Functional Decomposition

The subfunctions chosen allow for comparisons of how the STPA driven processes compare with the traditional aerospace ARP 4754A/4761 driven processes and how RTA designs and concepts can be incorporated and evaluated for these safety processes.

- Provide translational rate command horizontal control mode: This subfunction addresses the manual piloting scenario. It requires inertial velocity measurements, typically provided by INS. Failure of INS could require a transition to a lower level of control (e.g., ACAH). This allows opportunity to address interactions with fault detection and isolation in addition to interesting human factors interactions.

- Provide path following control mode: This subfunction addresses the automated-piloting scenario. It has many properties that are similar to Autoland, explored in the previous effort [Peterson 2015].
- Provide airborne vehicle collision avoidance: This subfunction addresses the shared human-automated piloting scenarios. It has rich interactions between pilot and automation.

The definitions of the primary functions are as follows: (A comprehensive list of functions and subfunctions is contained in Appendix A.)

F - Control of Aircraft Movement. This is the major function required to control the movement of the aircraft along the flight profile. It is decomposed into the functions of aviate, navigate, and communicate. Note that the functions under aviate, navigate, and communicate include references to automation. More detailed information regarding what automation is defined for each phase of the flight profile is typically developed during the system allocation process, which includes the system architecture and considerations for the system operation

F.A – Aviate. These are functions related to controlling the aircraft's aerodynamic state. The structure of the functional decomposition for Aviate is as follows:

Basic Control of the Aircraft in Pitch, Roll, Yaw Axes and Speed

F.A.1 Provide Interfaces for Unified Control of Aircraft Flight. The aircraft must provide interfaces by which the pilot can control the aircraft. The aircraft movement is controlled around the pitch, roll and yaw axes as well as speed. These include the left- and right-hand inceptors, rudder pedals, trim switches and mode controls and as well as their interfaces to the other aircraft systems. Unified control makes pilot control of the vehicle consistent throughout the various flight modes, including transitions.

Control Under Specific Flight Modes

F.A.2 Provide Controlled Aircraft Hover Flight

F.A.2.1.2 Provide translation rate command horizontal control mode. The aircraft must provide a control mode for translational rate command horizontal control in hover.

F.A.3 Provide Controlled Aircraft Wingborne Flight. The aircraft must provide the capacity for a controlled wingborne flight.

F.A.4 Provide Controlled Aircraft Transition Flight. The aircraft must provide the capacity for a controlled flight during transition between hover and wingborne flight.

Aviate Situational Awareness

F.A.5 Provide Aerodynamic Situational Awareness Interface. The aircraft must provide an interface to the pilot to provide aerodynamic situational awareness. This typically takes the form of displays, lights, aural caution and warning and tactile feedback.

F.N – Navigate. These are functions related to controlling the aircraft's geospatial state. The structure for the functional decomposition for Navigate is as follows:

Perform Flight Planning

F.N.1 Provide Flight Management Planning. The aircraft must provide the capacity to perform flight planning, including origin, destination, and route of flight.

Control Modes Required to Follow Paths

F.N.2 Provide Flight Management. The aircraft must provide the capacity for the management of the flight plan.

F.N.2.1 Provide path generation. The aircraft must provide the capacity to generate the flight plan path that the aircraft will need to follow.

F.N.2.2 Provide path monitoring. The aircraft must provide the capacity to monitor that the aircraft is following the generated flight path within the specified tolerances.

F.N.2.3 Provide path following control mode. The aircraft must provide the capacity for vertical and lateral control along the navigational route (flight plan). This includes any failure or warning annunciations to the pilot.

F.N.2.4 Provide emergency geospatial control modes

F.N.2.4.3 Provide airborne vehicle collision avoidance. The aircraft must provide the capacity to avoid collisions with other aircraft, terrain and fixed structures, such as buildings. This includes the emergency maneuver required once an imminent collision is detected.

Navigation Situational Awareness

F.N.3 Provide Geospatial Situational Awareness. The aircraft must provide the capacity for the pilot to achieve and maintain situational awareness of the geospatial flight and the surroundings. This includes how the aircraft is following the flight path trajectory as well as any imminent threats of collisions with other aircraft or structures.

F.C Communicate. These are functions related to controlling communications on the aircraft and to and from the aircraft.

3.2.2 Aircraft Functional Hazard Assessment (AFHA)

The Aircraft Functional Hazard Assessment (AFHA) is presented in Appendix B. The AFHA for this study evaluates three aircraft level functions:

- Provide Translation Rate Command Horizontal Control Mode
- Provide Path Following Control Mode

- Provide Airborne Vehicle Collision Avoidance

Catastrophic and Hazardous Failure Conditions for these three functions are summarized in Table 5, Table 6, and Table 7.

At the aircraft level, the AFHA examines how the function can fail without regards to any specific implementation and/or interface. Basic categories of function failure include:

- Loss of the function – failure of function to "activate" when the design calls for activation. This is normally in conjunction with the system alerting the pilot to the failure
- Erroneous control function (malfunction) – malfunctions of the control function resulting in erroneous vehicle control. Annunciation of the malfunction to the pilot is considered as well as non-annunciation of the malfunction to the pilot. In cases where the flight phase is a low altitude flight phase, pilot annunciation may not be considered since the pilot may not have sufficient time to recover.
- Uncommanded engagement (activation) of the function – function engages (activates) during conditions where the design does not call for activation. Again, pilot annunciation is considered

Phase of flight is considered for all failure conditions. Phase of flight is defined in Appendix B and includes phases such as taxi, takeoff, climb, cruise, descent, approach, and landing. Failures which occur during the low altitude phases of flight are usually more severe than at higher altitudes.

This study considers operation of the vehicle by the so-called "minimally trained pilot". As such, failures in some cases are classified with a more severe classification due to assumptions around the ability of a pilot with lesser training to recognize and recover from a failure condition (particularly during vehicle operation at low altitude such as takeoff, approach, and landing). Assumptions made of the "minimally trained pilot", as well as other assumptions made in carrying out the AFHA (and later the SFHA), are documented in Appendix B.

Table 5 Provide Translation Rate Command Horizontal Control Mode Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App A Failure Condition Number	Classification
Loss of TRC Control Mode (with or without annunciation to the pilot)	F.A.2.1.2.TL1	Catastrophic
Erroneous TRC control	F.A.2.1.2.MF1	Catastrophic
Erroneous TRC engagement	F.A.2.1.2.MF2	Catastrophic

Table 5 provides the AFHA summary for TRC control. Since TRC is a low-altitude control mode, and the pilot is considered "minimally trained", failures are considered catastrophic. For function failures deemed Catastrophic, the design needs to satisfy two objectives:

- Probability of failure less than 10^{-8} (cf. Table 16)
- No single fault can lead to the top-level failure condition

(DAL assignments for systems implementing these functions depend on architectural details, and these are discussed in Section 3.8.) The baseline eCRM-001 vehicle has two installed combined INS/GPS line replaceable units (LRU). Unresolvable mis-compare of the input feedback parameters will represent a single point of failure and will need to be addressed by the design irrespective of RTA. This may require installation of a third INS.

Table 6 Provide Path Following Control Mode Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App A Failure Condition Number	Classification
Loss of Lateral Path Following Control Mode during flight without annunciation to the pilot	F.N.2.3.TL2	Hazardous
Loss of Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	F.N.2.3.TL3	Catastrophic
Erroneous Lateral Path Following Control Mode without annunciation to the pilot	F.N.2.3.MF2	Hazardous
Erroneous Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	F.N.2.3.MF3	Catastrophic
Uncommanded engagement of Lateral Flight Path Control Mode during flight	F.N.2.3.MF5	Catastrophic
Loss of Vertical Path Following Control Mode during flight without annunciation to the pilot	F.N.2.3.TL5	Hazardous
Loss of Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	F.N.2.3.TL6	Catastrophic
Erroneous Vertical Path Following Control Mode without annunciation to the pilot	F.N.2.3.MF7	Hazardous
Erroneous Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	F.N.2.3.MF8	Catastrophic
Uncommanded engagement of Vertical Flight Path Control Mode during flight	F.N.2.3.MF10	Catastrophic

Table 6 provides the AFHA summary of Hazardous and Catastrophic failure conditions for the Path Following Control mode. As with TRC above, the design will need to be compliant with probability requirements for the Catastrophic failure conditions as well as the “no single fault” requirement. Hazardous failure conditions probability requirements are 10^{-7} and are not subject to the “no single fault” requirement.

Table 7 Provide Airborne Vehicle Collision Avoidance Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App A Failure Condition Number	Classification
Loss of collision avoidance not annunciated to the pilot	F.N.2.4.3.TL2	Catastrophic (Note 1)
Collision avoidance activation with erroneous avoidance maneuver (legitimate collision threat detected)	F.N.2.4.3.MF2	Catastrophic
Collision avoidance activation without annunciation to the pilot (legitimate collision threat detected)	F.N.2.4.3.MF3	Catastrophic

Note 1 – Assumes probability of collision is 1.

Table 7 provides the AFHA summary of the Vehicle Collision Avoidance mode. Catastrophic failure conditions are un-annunciated loss of function, as well as two identified control faults. The Vehicle Collision Avoidance mode is considered a safety mode with no RTA backup other than pilot monitoring of the function.

3.3 Aircraft-Level Architecture

The aircraft level architecture from the previous BAART task order is also used in this work, as shown in Figure 16. The effectors are shown in the dark blue box, the electrical power system in the red box, aircraft sensors in the green box, flight deck annunciations and controls in the gray box, and pilot flight and propulsion controls interfaces in the turquoise box. While the prior task order detailed low-level control of the aircraft effectors, this task order significantly expands and adds detail to the Flight and Propulsion Control Electronics portrayed as the orange system.

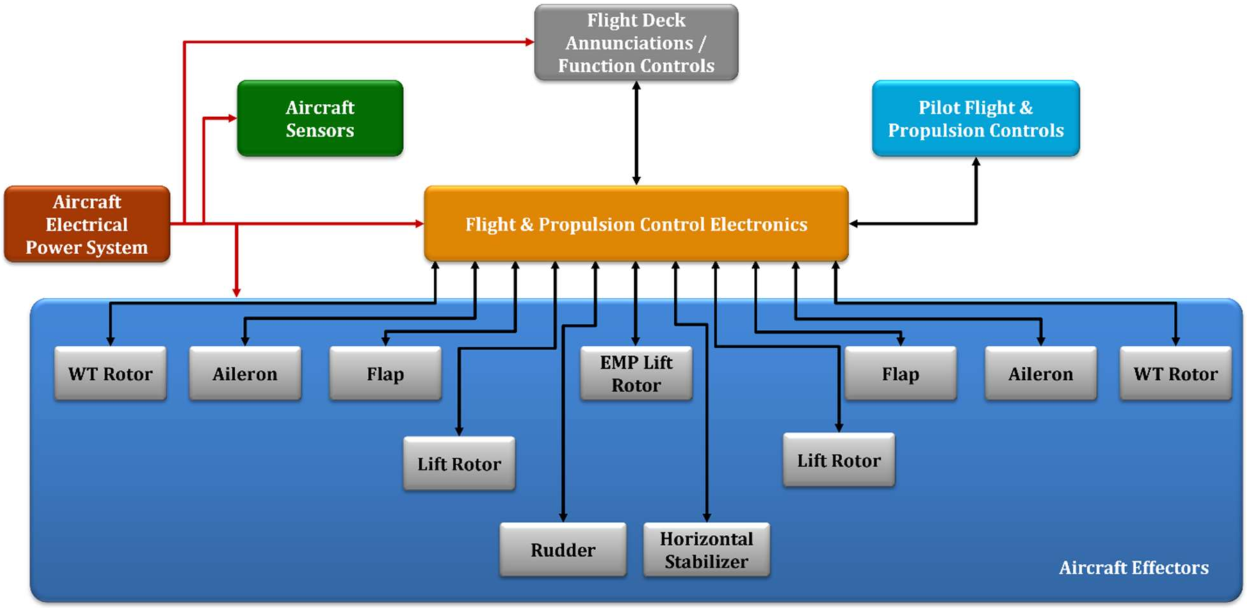

Flight Deck Annunciations / Function Controls
Aircraft Sensors
Pilot Flight & Propulsion Controls
Aircraft Electrical Power System
Flight & Propulsion Control Electronics
WT Rotor
Aileron
Flap
EMP Lift Rotor
Flap
Aileron
WT Rotor
Lift Rotor
Lift Rotor
Rudder
Horizontal Stabilizer
Aircraft Effectors

Figure 16. Aircraft Level Architecture Focused on Flight and Propulsion Control

An additional level of description for systems other than the Flight and Propulsion Control Electronics is shown in Figure 17. Here, the primary subsystem for each parent system is summarized. The main inceptors for pilot control follow the unified control concept and include left and right-hand inceptors, pedals, flap control, nose wheel steering and other ground controls, and the mission computer interface. The Flight Deck Annunciations and Function Controls include systems for situational awareness including displays, inceptor feedback, automation mode controls, and caution / warning systems. The proprioceptive aircraft sensors are listed as are the main subsystems for the effectors.

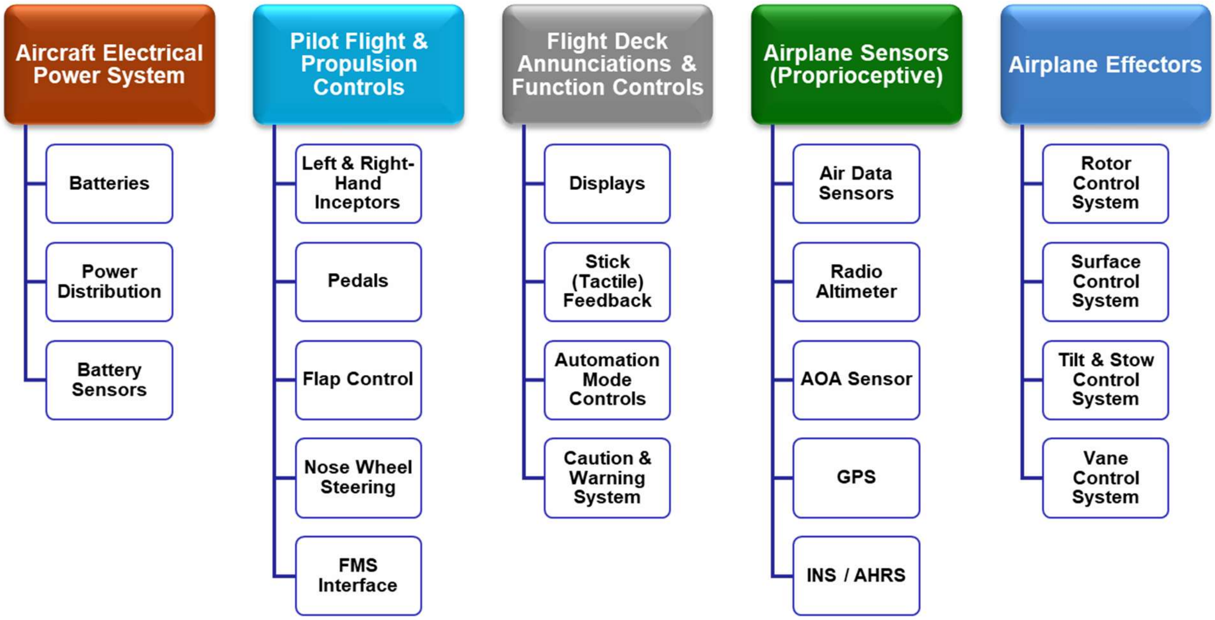


Figure 17. Aircraft Systems and Subsystems

3.4 Aircraft-Level Systems and Subsystems

The primary subsystems of the Flight and Propulsion Control Electronics are shown in Figure 18. The primary subsystems and functions are grouped according to respective hardware. For example, the Flight Control Computer (FCC) provides the computational support for a human pilot to manually fly the aircraft. It hosts functions such as state estimation, flight path command control, and tracking control. The Flight Management System (FMS) provides the computational support for automated flying and hosts functions such as multiple path generation options and maintenance of the World Map to assist with navigation and situational awareness. The Collision Avoidance Systems is a group consisting of multiple LRUs that provide monitoring and notification of potential collisions or urgent hazards using cooperative technologies, such as ADS-B and TCAS. The Exteroceptive Sensors is a group consisting of multiple LRUs that provide sensing of the environment outside the aircraft, such as RADAR, LIDAR, synthetic vision, etc. Details of the various flight and propulsion functions are given in the following section.

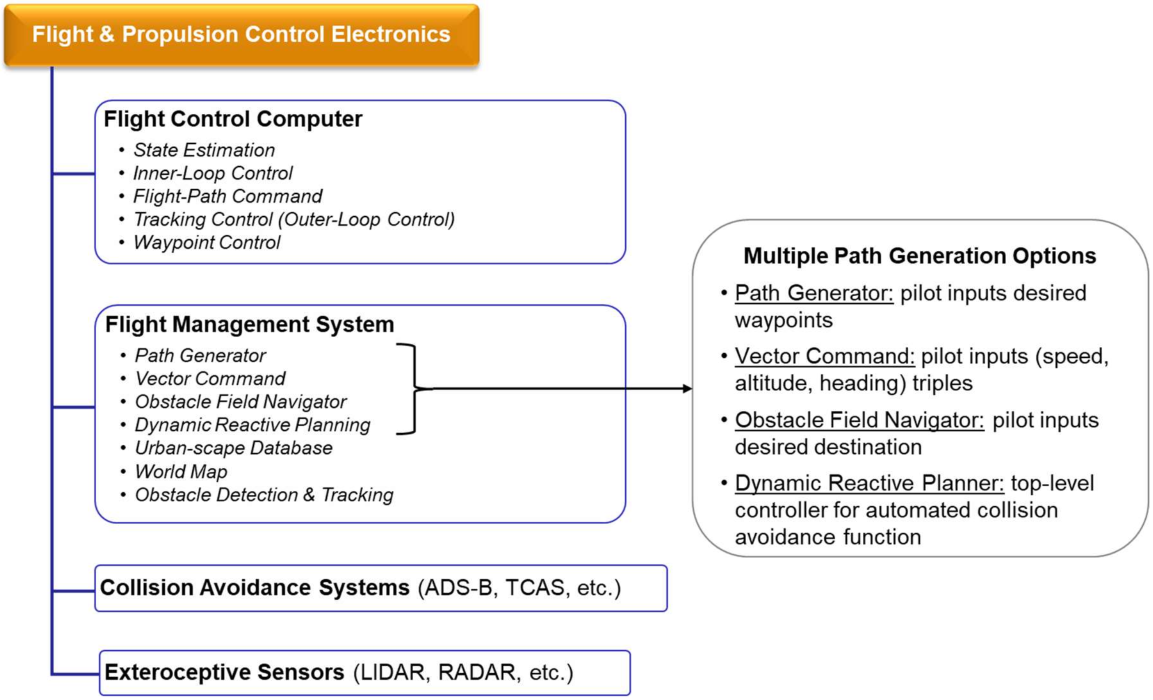

Flight & Propulsion Control Electronics
Flight Control Computer
• State Estimation
• Inner-Loop Control
• Flight-Path Command
• Tracking Control (Outer-Loop Control)
• Waypoint Control
Flight Management System
• Path Generator
• Vector Command
• Obstacle Field Navigator
• Dynamic Reactive Planning
• Urban-scape Database
• World Map
• Obstacle Detection & Tracking
Multiple Path Generation Options
• Path Generator: pilot inputs desired waypoints
• Vector Command: pilot inputs (speed, altitude, heading) triples
• Obstacle Field Navigator: pilot inputs desired destination
• Dynamic Reactive Planner: top-level controller for automated collision avoidance function
Collision Avoidance Systems (ADS-B, TCAS, etc.)
Exteroceptive Sensors (LIDAR, RADAR, etc.)

Figure 18. Flight and Propulsion Control Subsystems

Additional detail of the effector layout and control for the effectors is provided in Figure 19, which shows the Flight Propulsion Control Functional Block Diagram. For system definition purposes, the functionality is organized into five groups: Central Controller, Rotor Control, Surface Control, Tilt and Stow Control, and Vane Control.

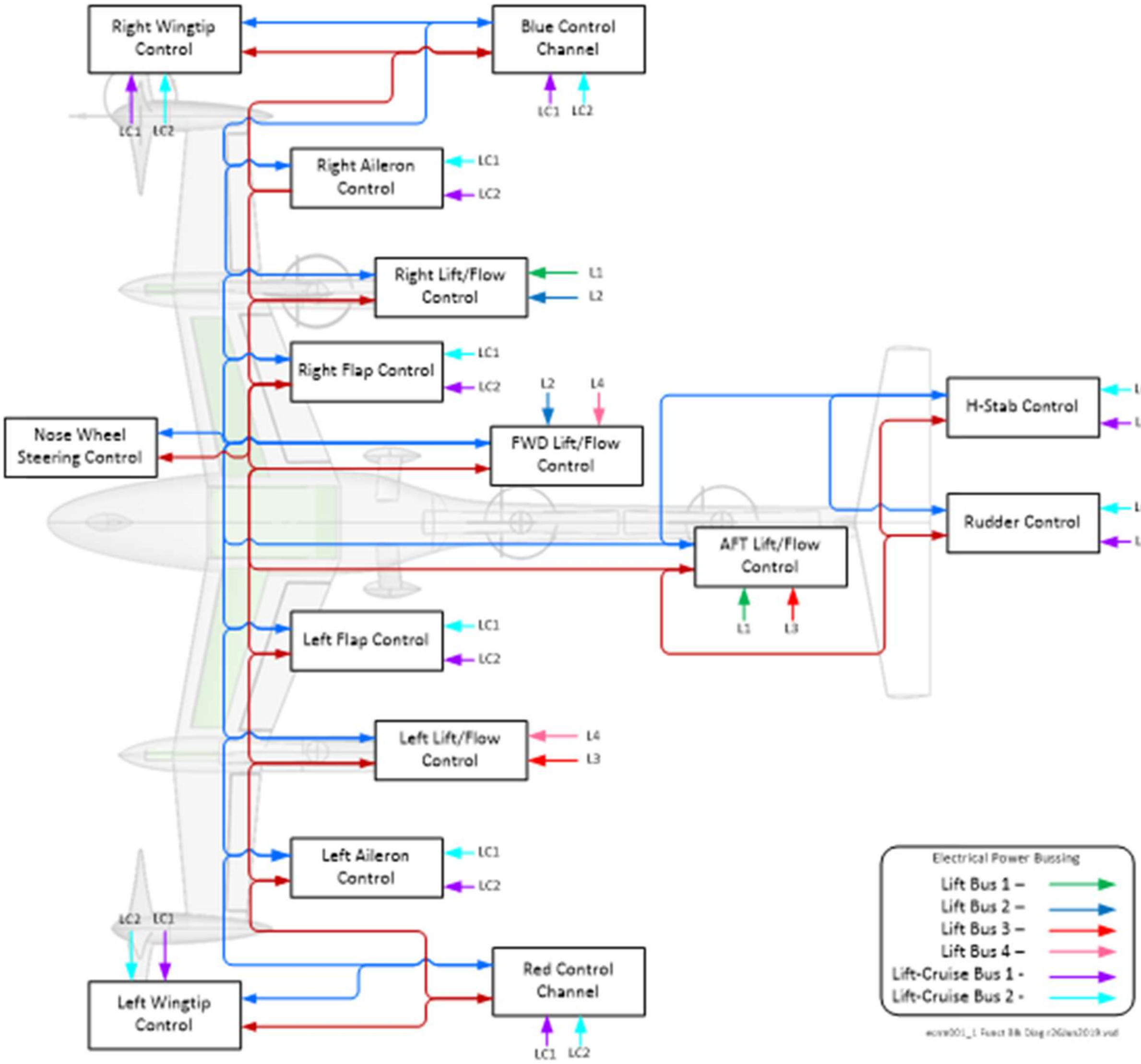


Figure 19. Flight-Propulsion Control Functional Block Diagram

3.5 Flight and Propulsion Control Architecture

A high-level architecture of the integrated flight and propulsion control system is shown in block-diagram form in Figure 20**.** It is largely based on a variable-autonomy control architecture for rotorcraft presented in [Takahashi 2017]. This diagram focuses on the different control systems used for both manual and autonomous flight and the pilot's interaction with these systems. Note that the response type for manual flight is at a higher level of augmentation than may be typical for other rotorcraft and fixed-wing vehicles. As discussed in Section 2.3.2, in hover mode there is a TRC response type in the lateral and longitudinal axes and a vertical rate command in the heave axis. Typically, rotorcraft feature an attitude command / attitude hold (ACAH) or rate command response type in these axes when operated by expert pilots. The TRC response type may be more suitable for pilots with varying levels of training and may also reduce pilot workload. The PFCS is responsible for manual flight and accepts pilot inceptor commands as outlined in Table 3. There is an optional reversionary mode where the pilot would interact with an ACAH in the lateral and longitudinal axes, but this mode is not analyzed in detail in this project.

The blocks with red highlighting represent the control components primarily responsible for the three functions selected for detailed examination in this study. These include the Dynamic Reactive Planner (DRP), Tracking Control, and Flight Path Command (FPC) controller.

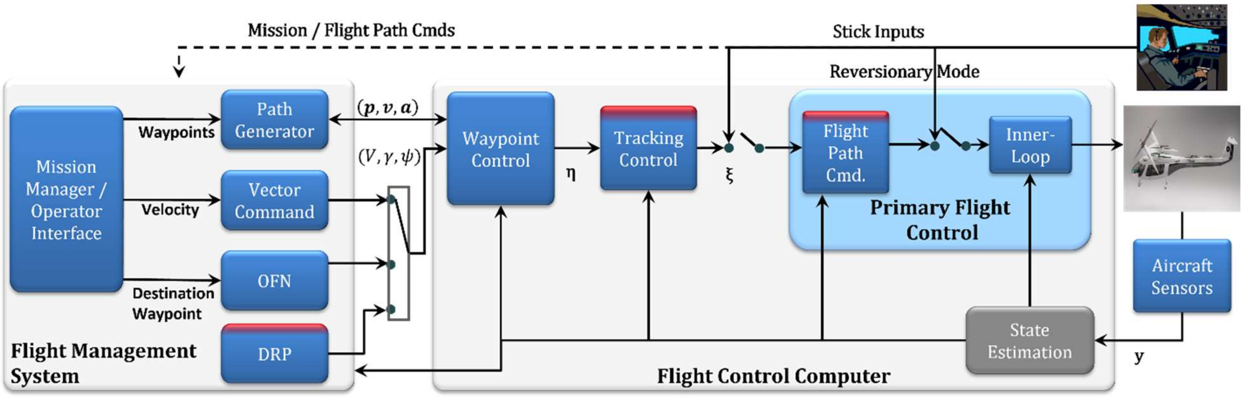


Figure 20. Integrated Flight and Propulsion Control Architecture

Recall from the discussion of the Unified Control Concept in Section 2.3 that the pilot inceptor issues a different command based on flight regime (e.g., hover, transition, or fixed-wing flight mode). These different systems are embedded in the corresponding blocks in Figure 20. For example, the TRC controller is part of the FPC block and is active during hover mode flight. Higher levels of autonomy and pilot augmentation are provided in the FMS in the form of different path generation functions, namely, the Path Generator, Vector Command, and Obstacle Field Navigator (OFN). These functions are used as part of the mission planning and management system to generate a path or trajectory meeting different flight objectives. Additional details are provided in Section 3.7.

When the vehicle is operated in a highly autonomous manner, the pilot or a ground-based function provides a mission or flight plan and the onboard systems monitor the progress of the plan and execute it. The pilot can specify a flight plan or path using different functions implemented on the FMS, including the Path Generator, Vector Command, and OFN. Each of these functions parameterizes a path that is input to the Waypoint Control block, which transforms the different path parameterizations to a common inertial reference path with accompanying velocity and acceleration profiles. This encoding of the path is then sent to the Tracking Control which acts as an autopilot and issues a command vector, ξ, to follow the path. Note that this is the insertion point for the pilot inceptor commands and the remaining downstream components are the same for both automated and manual flight.

3.6 Aircraft-Level Function Allocation

The aircraft system development process allocates the high-level airplane functions to various planned aircraft systems or specific system elements in one system. Table 8 is an excerpt of the complete function allocation matrix that focuses on three functions selected for analysis: Provide TRC Horizontal Control Mode, Provide Path Following Control Mode, and Provide Airborne Vehicle Collision Avoidance. The table indicates the primary systems that work together to provide each function.

Table 8. Aircraft Function Allocation (excerpt)

Systems	TRC	Path Following	Collision Avoidance
Pilot Flight & Propulsion Controls			
Pilot Left & Right-Hand Inceptors	X	X	X
Pilot Pedals	X	X	X
FMS Interface		X	
Airplane Sensor (proprioceptive)			
GPS	X	X	X
INS / AHRS	X	X	X
Flight Propulsion & Control Electronics			
Flight Control Computer			
Inner-loop Control	X	X	X
Flight Path Command	X	X	X
Tracking Control (outer-loop)		X	X
Waypoint Control		X	X
Mission Computer			
Path Generator		X	
Vector Command		X	
Obstacle Field Navigator		X	
Dynamic Reactive Planning			X
Exteroceptive Sensors		X	X

The TRC function provides manual flight control capabilities to the pilot and also accepts a command vector from the Tracking Control block while in automated flight mode. The TRC controller is active while the vehicle is in hover mode and is designed to provide increased handling qualities and reduced pilot workload. The functional diagram of the TRC function is shown in Figure 21. A switch depicted near the top left of the FCC-1 block indicates the reference command sent to the Hover Mode Controller system can come from either the pilot inceptor or Tracking Control depending on the state of the AutoPilot Engage (AP Engage) signal which is sent from the Mode Control Panel. The Hover Mode Controller uses feedback from the aircraft sensors to provide closed-loop tracking on the reference signals and disturbance rejection to external disturbances. The Hover Mode Controller is composed of the TRC / Position Hold Controller which acts in the lateral and longitudinal axes and a Vertical and Yaw Controller that operates on the heave and directional axes. The output commands are then transmitted to the Inner-Loop Controller. The Position Hold functionality operates on all four axes and provides the ability to maintain a geo-referenced position and heading when the inceptors are at neutral. Pilot inceptor motion then commands translational velocities in the lateral, longitudinal, and heave axes and a yaw rate command in the directional axis.

Flight mode transition between hover and wingborne flight mode is scheduled based on a combination of ground-speed and airspeed as described in Figure 13. This signal comes from the Mode Logic block and activates the switch in the middle right of the FCC-1 block that determines which signal is sent to the Inner-Loop block. In hover mode, the output of the Hover Mode Controller is the vector of commands $\{\phi_c, \theta_c, v_{zc}, r_c\}$ that provide reference signals of the desired roll angle, pitch angle, vertical rate, and yaw rate to follow the reference commands input to the Hover Mode Controller. Different reference commands originate from the Transition Mode Controller and Wingborne Mode Controller. The Flight Path Command controller is comprised of the Hover, Transition, and Wingborne Mode controllers. This controller is not labelled in the figure to focus on the TRC function.

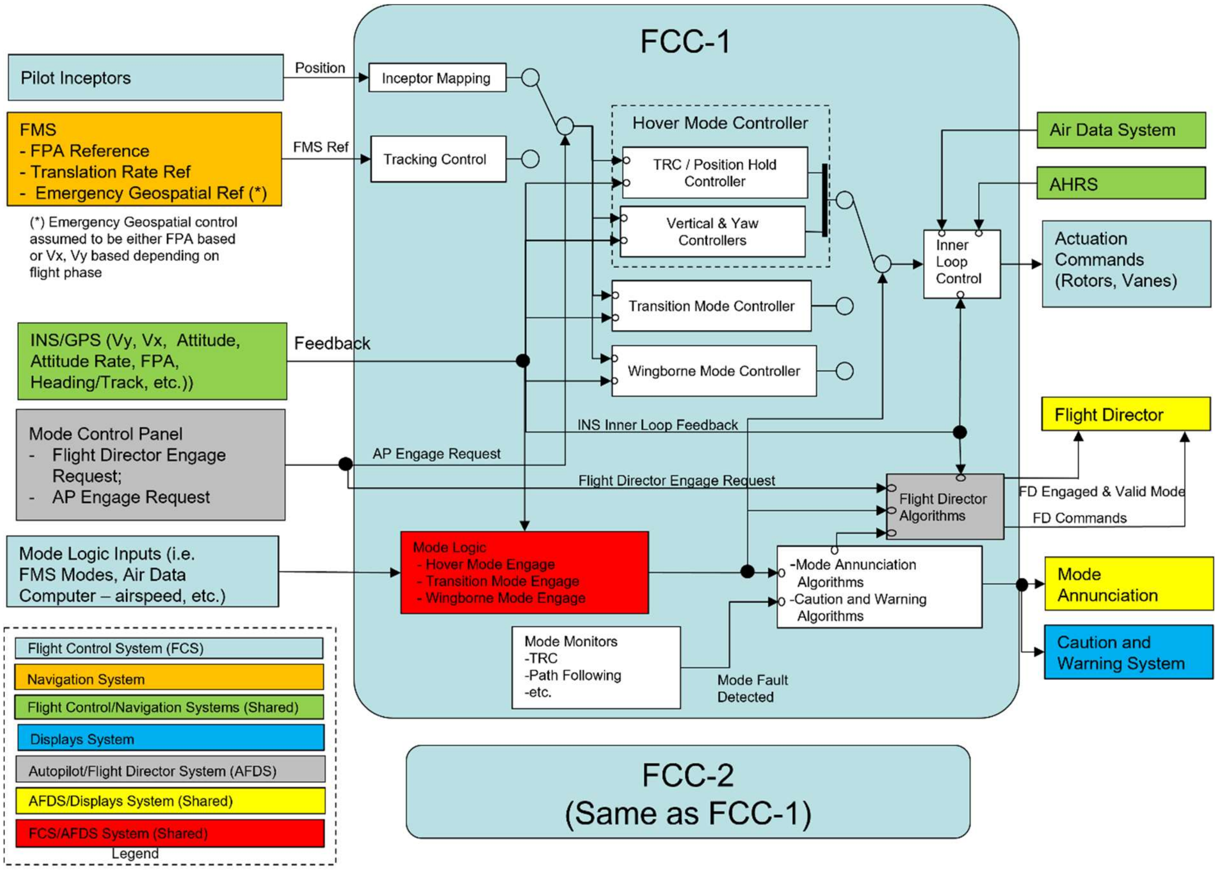

FCC-1
Pilot Inceptors
Position
Inceptor Mapping
FMS
- FPA Reference
- Translation Rate Ref
- Emergency Geospatial Ref (*)
FMS Ref
Tracking Control
(*) Emergency Geospatial control assumed to be either FPA based or Vx, Vy based depending on flight phase
Hover Mode Controller
TRC / Position Hold Controller
Vertical & Yaw Controllers
Air Data System
AHRS
Inner Loop Control
Actuation Commands (Rotors, Vanes)
Transition Mode Controller
Wingborne Mode Controller
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Feedback
INS Inner Loop Feedback
Flight Director
Mode Control Panel
- Flight Director Engage Request;
- AP Engage Request
AP Engage Request
Flight Director Engage Request
Flight Director Algorithms
FD Engaged & Valid Mode
FD Commands
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
-Mode Annunciation Algorithms
-Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
Mode Monitors
-TRC
-Path Following
-etc.
Mode Fault Detected
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)
Legend
FCC-2
(Same as FCC-1)

Figure 21. Functional Block Diagram for the TRC Function

The functional block diagram for the Path Following function is shown in Figure 22. This function is responsible for generating a path, or trajectory, and tracking the path. The systems not included in this function are greyed out in the figure. The data flow of the function starts in the FMS block with World Map and Path Generator systems. The World Map system is responsible for maintaining an updated synthetic description of the sensed external environment. A notional architecture is shown in Figure 23. It combines known data from an urban-scape database (e.g., building layouts, road grids, restricted fly zones, etc.), combined with live sensor data collected from the environment. Flight tracks and positions of other vehicles in the vicinity can be included from cooperative aircraft (defined as those with communicating transponders). Exteroceptive sensing systems feed into the World Map to update a map of the external world and identify and track any identified obstacles or hazards (e.g., birds, non-cooperative aircraft, temporary construction cranes, etc.). A synthetic view of the map can be made available to the pilot to assist with planning and situational awareness.

The description and analysis of the Path Following function focuses on use of the Path Generator system, although the other path generation blocks could also be used. The Path Generator was chosen as it represents a common planning procedure that creates the path from a series of waypoints and meta-data specified by the pilot. This waypoint information is then sent to the Waypoint Control which is responsible for filtering and transforming path represented by different formats and possibly different frames to a continuous inertial path, $\eta = \{X_c, Y_c, h_c, \psi_c\}$ along with velocity and acceleration profiles. This path encoding is then sent to the Tracking Control which acts as an autopilot and generates commands to track the path. The proprioceptive sensing systems, various mode logic and monitors, mode annunciation, and navigation displays also support the Path Following function.

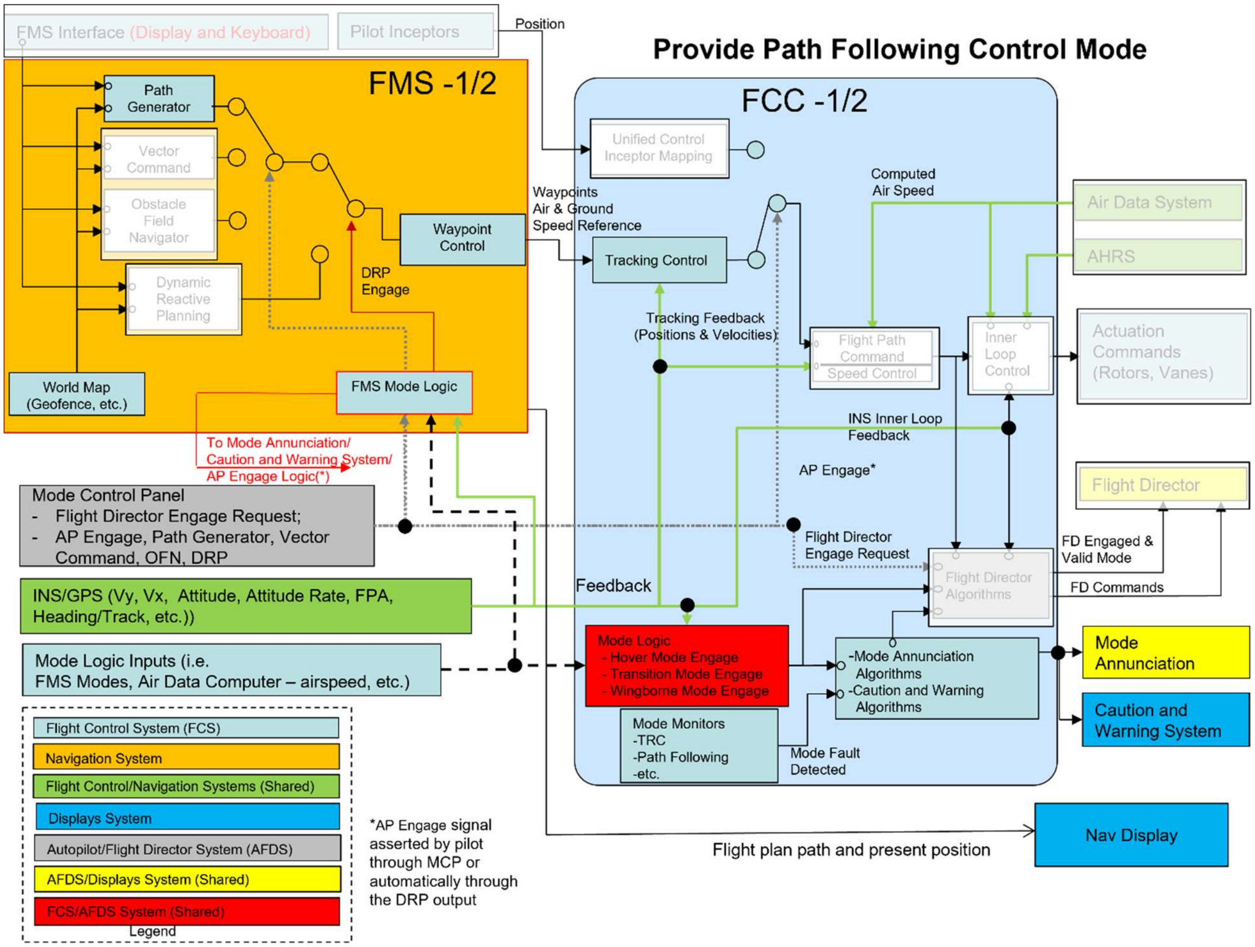

FMS Interface (Display and Keyboard)
Pilot Inceptors
Position
Provide Path Following Control Mode
FMS -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Dynamic Reactive Planning
Waypoint Control
DRP Engage
World Map (Geofence, etc.)
FMS Mode Logic
To Mode Annunciation/ Caution and Warning System/ AP Engage Logic(*)
FCC -1/2
Unified Control Inceptor Mapping
Waypoints Air & Ground Speed Reference
Tracking Control
Computed Air Speed
Air Data System
AHRS
Tracking Feedback (Positions & Velocities)
Flight Path Command Speed Control
Inner Loop Control
Actuation Commands (Rotors, Vanes)
INS Inner Loop Feedback
AP Engage*
Flight Director
Flight Director Engage Request
FD Engaged & Valid Mode
Flight Director Algorithms
FD Commands
Feedback
Mode Control Panel
- Flight Director Engage Request;
- AP Engage, Path Generator, Vector Command, OFN, DRP
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
-Mode Annunciation Algorithms
-Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
Mode Monitors
-TRC
-Path Following
-etc.
Mode Fault Detected
Nav Display
Flight plan path and present position
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)
Legend
*AP Engage signal asserted by pilot through MCP or automatically through the DRP output

Figure 22. Functional Block Diagram for the Path Following Function

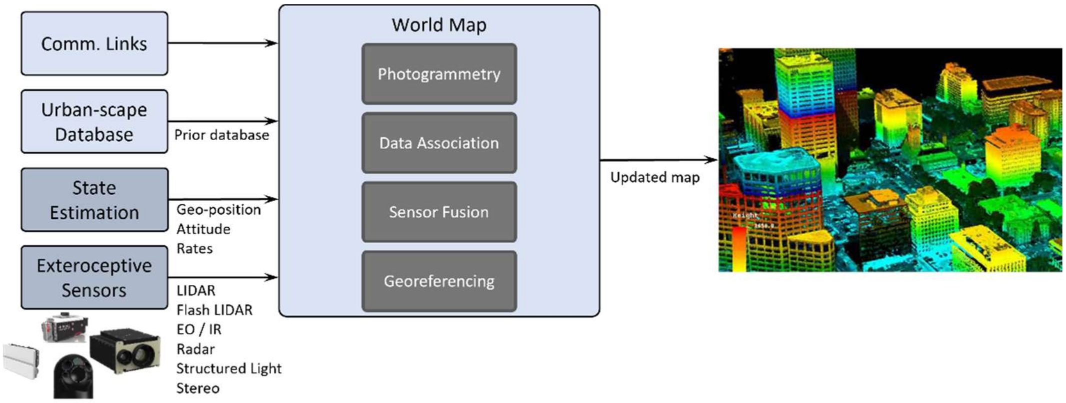
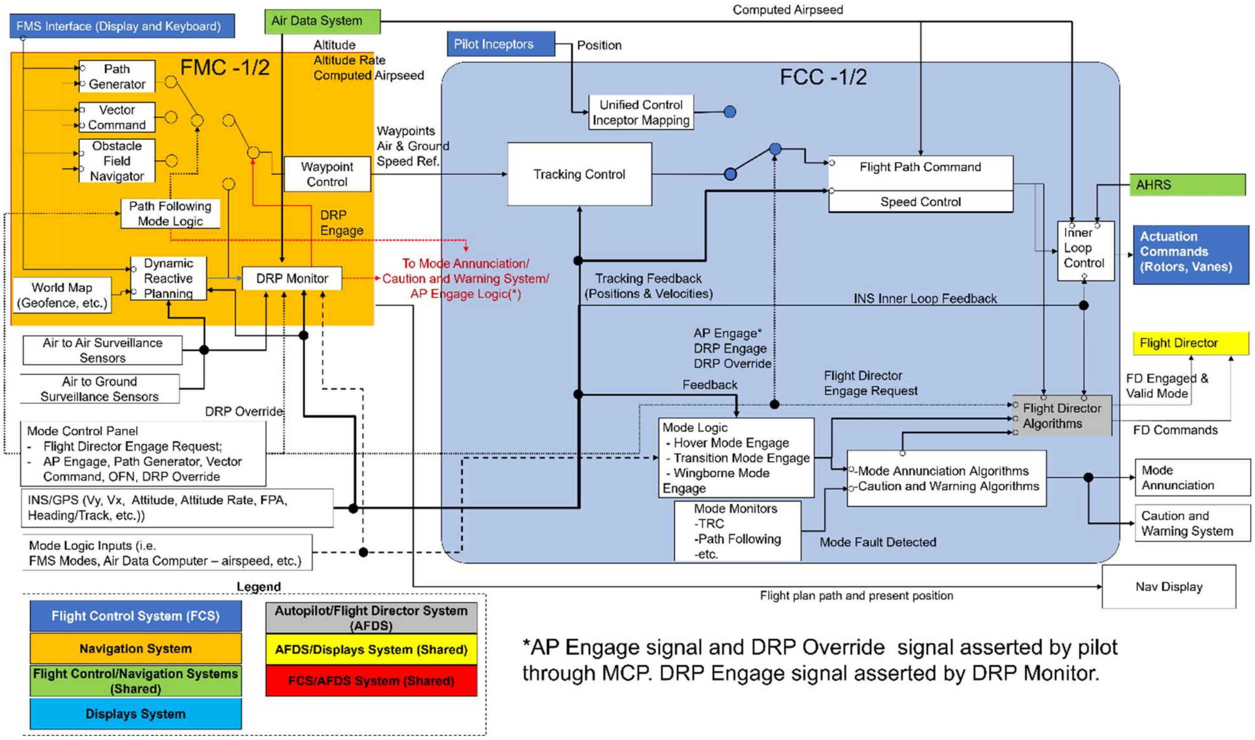


Figure 23. Notional World Map Architecture

The functional block diagram for the Collision Avoidance function is shown in Figure 24. As with the other functional diagrams, only the systems involved in implementing the function are shown in the figure. The Collision Avoidance function is perhaps the most complex function analyzed in this work as it includes a greater breadth of systems such as the exteroceptive sensors, the World Map, all three path generation blocks, pilot interaction, mode logic and monitors, the DRP, mode annunciation and warning systems, and the complete automated path following and control functions ranging from the Waypoint Control to the inner-loop and effector commands. The Flight Director and Navigation Displays are also active and relevant to this analysis.


FMS Interface (Display and Keyboard)
Air Data System
Computed Airspeed
Altitude
Altitude Rate
Computed Airspeed
Pilot Inceptors
Position
FMC -1/2
FCC -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Path Following Mode Logic
Waypoint Control
Waypoints Air & Ground Speed Ref.
DRP Engage
Dynamic Reactive Planning
DRP Monitor
World Map (Geofence, etc.)
To Mode Annunciation/ Caution and Warning System/ AP Engage Logic(*)
Unified Control Inceptor Mapping
Tracking Control
Flight Path Command
Speed Control
AHRS
Inner Loop Control
Actuation Commands (Rotors, Vanes)
Tracking Feedback (Positions & Velocities)
INS Inner Loop Feedback
Flight Director
AP Engage* DRP Engage DRP Override
Feedback
Flight Director Engage Request
FD Engaged & Valid Mode
Flight Director Algorithms
FD Commands
Air to Air Surveillance Sensors
Air to Ground Surveillance Sensors
DRP Override
Mode Control Panel
- Flight Director Engage Request;
- AP Engage, Path Generator, Vector Command, OFN, DRP Override
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
Mode Annunciation Algorithms
Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
INS/GPS (Vy, Vx, Altitude, Altitude Rate, FPA, Heading/Track, etc.))
Mode Monitors
-TRC
-Path Following
-etc.
Mode Fault Detected
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Flight plan path and present position
Nav Display
Legend
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)

*AP Engage signal and DRP Override signal asserted by pilot through MCP. DRP Engage signal asserted by DRP Monitor.

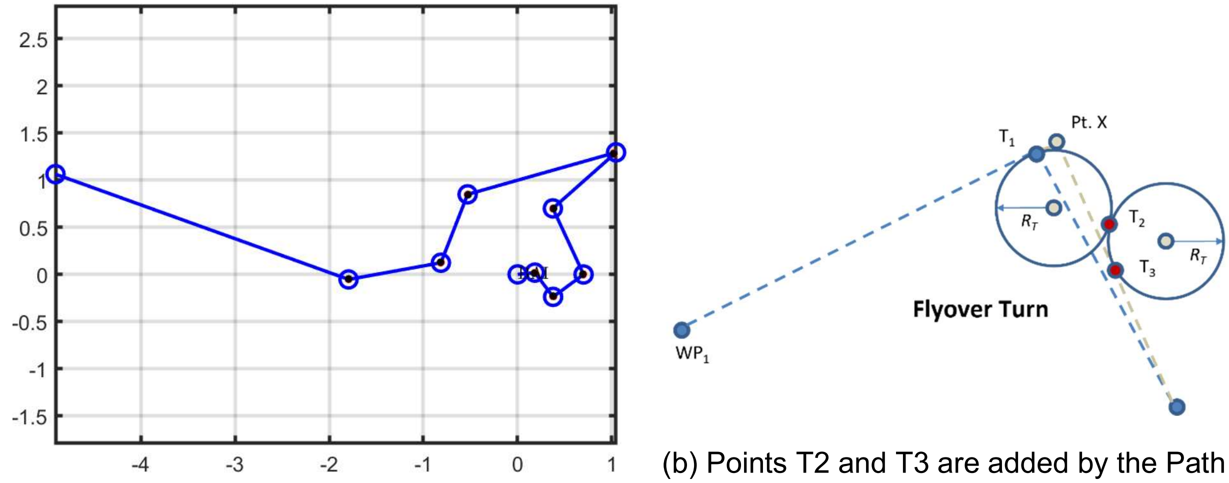
Figure 24. Functional Block Diagram for the Collision Avoidance Function

As described in Section 2.6, there is a distinction between flight planning, flight replanning, and collision avoidance. The Collision Avoidance function is concerned with immediate hazards with a shorter time to resolve a hazard and typically involves ignoring mission parameters and objectives for a time while the hazard is resolved. The collision avoidance function belongs to the category of *tactical operations*. TCAS II and ACAS-XA are examples of systems that help form the Collision Avoidance function for present commercial aircraft. UAM aircraft are expected to utilize systems that adhere to the ACAS-Xr standard, still in development. As shown in Figure 24, air-to-air surveillance sensors (i.e., exteroceptive sensors and communication links between UAM vehicles) are used in combination with air-to-ground surveillance sensing systems to help inform the DRP and DRP Monitor of potential threats and provide information to assist in determining the degree of those threats. This would include both cooperative and uncooperative aircraft. Examples of currently available technologies include TCAS/ACAS, Mode S transponders, and ADS-B. Air-to-Ground Surveillance Sensors is a group of sensors capable of detecting ground-based threats (such as buildings) and providing information to assist in determining the degree of those threats. Examples of currently available technologies include LIDAR, radar, synthetic vision, etc. The DRP Monitor continuously monitors the environment for any threats from air-to-air collisions or air-to-ground collisions, and it switches the flight plan accordingly to dynamic reactive planning (collision avoidance path), after first allowing a short time for a pilot override. Additional description of the DRP Monitor is provided in Section 3.7.3. The DRP continuously computes a 4D path from the vehicle’s current location that will avoid any pending air to air or air to ground threats. The Pilot Override allows the pilot to override a collision avoidance maneuver.

3.7 System-Level Functions and Architecture

This section provides additional detail on the system and architecture of the integrated flight and propulsion control architecture presented in Figure 20. The design features a high-level of autonomy and autonomous systems as envisioned by the SVO concept. At any point during flight when the autonomy is active, such as during autonomous path following, the pilot may regain manual control by manipulating the inceptors. Smooth transition is provided to eliminate unwanted transients during the return to manual flight. The pilot interacts with autonomous systems hosted on the FMS. There are three different functions the pilot may use to plan a path as outlined in the figure. These are summarized in the following.

Path Generator: The Path Generator allows the pilot to enter waypoints (spatial locations) representing a predetermined path with macro-level parameters such as velocity limits, climb rate and acceleration limits, etc. It produces a smoothed spatial path with a corresponding velocity profile such that the aircraft will achieve the desired waypoints within a specified capture radius. The Path Generator may insert additional waypoints to follow kinematic or dynamic constraints. Additionally, each waypoint is parameterized with a radius defining a 3D corridor the vehicle must stay in when transiting between successive waypoints. The Path Generator produces a path that may be associated with conventional waypoint following, as shown in Figure 25(a), which shows a notional list of waypoints that could be entered by the pilot. To provide a smooth transition between waypoints, the Path Generator may add points T2 and T3 as shown in subfigure (b) which define transition points between two circular segments that help align the path with the current active waypoint. The radii of the two circles shown in subfigure (b) are a function of the commanded airspeed and maximum bank angle. This type of turn depicted in the figure is a *Flyover Turn* because the vehicle is commanded to fly directly over the active waypoint before transitioning to the next point. Verifying that consecutive waypoints are spaced sufficiently far apart to allow for this type of "arc-arc" transitioning constrained by the maximum bank angle is also part of the Path Generator.



(a) Notional waypoints input by pilot

(b) Points T2 and T3 are added by the Path Generator to provide smooth profile

Figure 25. Path Generator Example

Vector Command: The Vector Command allows the pilot to enter discrete changes in the velocity vector to command the motion of the aircraft. The velocity changes can be described as commanded speed (V), flight path (γ), and heading (ψ). The command variables are held constant for some amount of time as specified by the pilot. The Vector Command then processes the commands entered by the pilot and checks the mission progress to send updated commands (speed, glideslope, heading triplets) to the Waypoint Control.

Obstacle Field Navigator: The OFN block allows the pilot to enter a single destination waypoint. Based on the vehicle's current position, OFN will generate a path to the final destination that adheres to mission parameters. OFN generates the path based on current world knowledge and may need to refine the path if previously unknown obstacles or hazards are detected. OFN outputs a stream of (speed, flight path, heading) triplets to the Waypoint Control in the same manner as Vector Command.

The Dynamic Reactive Planner also outputs a triplet of (speed, flight path, heading). The Waypoint Control is configured to accept the waypoint encoded path from the Path Generator or the vector triplet. The Waypoint Control is responsible for filtering and transforming paths represented by different formats and possibly different frames to a continuous inertial path, $\eta = \{X_c, Y_c, h_c, \psi_c\}$ along with velocity and acceleration profile. This path encoding is then sent to the Tracking Control which acts as an autopilot and generates commands to track the path.

3.7.1 Translation Rate Command

The TRC controller is active while the vehicle is in hover mode and is designed to provide increased handling qualities and reduced pilot workload. This is particularly important for AAM operations implementing the SVO vision of employing pilots with minimal training to pilot the aircraft. Minimally-trained pilots are expected to be more vulnerable to fatigue resulting from lower handling qualities produced with lower levels of augmentation. This is compounded with the complex, dynamic, and congested operating environment of UAM operations and is further compounded as the tempo of UAM operations increases. The TRC controller is designed to help alleviate workload, increase handling qualities, and reduce cognitive workload allowing the pilot to better perform secondary tasks and enjoy a greater capacity to monitor the flight and provide oversight of other automated or autonomous systems. The design of the TRC controller also seeks to provide desired performance while providing robustness to uncertainties and external disturbance. Additionally, the TRC seeks to maximize passenger comfort, which may be critical for customer acceptance of UAM services.

The TRC control design is based on an adaptive nonlinear dynamic inversion (ANLDI) design. NLDI has been implemented on a number of systems including fixed-wing vehicles, rotorcraft, and fighters like the F35. A number of benefits make it appealing to the novel UAM vehicle concepts which feature drastically changing dynamics, numerous control effectors (surface effectors and rotors), and highly nonlinear responses. Traditional control design using gain scheduled techniques are likely to introduce high costs for vehicles of this nature. NLDI separates the control design from the vehicle dynamics allowing a full-envelope controller to be efficiently designed even for vehicles with changing configurations such as nacelle / rotor tilt which introduce vastly differing dynamic response. Overall, the NDLI design can reduce system complexity and cost. The adaptive augmentation addresses modeling uncertainties, errors in tracking the desired dynamics, external disturbances, failures, impairments, etc. A general description of NLDI is provided, which includes a broad view of the TRC and Inner-Loop controllers, followed by inclusion of the adaptive element. Note that the Inner-loop controller also employs a NLDI design using an ACAH response type and will be referred to as ACAH or the inner-loop controller in the following discussion.

The TRC / ACAH flight control architecture is shown in Figure 26. The pilot commands may originate from the pilot inceptors or the Guidance law but are shown coming from the pilot in this figure. Reference commands controlling lateral velocity (V_{yc}), longitudinal velocity (V_{xc}), vertical velocity (V_{zc}), and yaw rate (r_c) are issued to the TRC module. The TRC passes the vertical velocity and yaw rate command directly to the ACAH controller and determines the required roll (ϕ_c) and pitch (θ_c) attitude commands to track the velocity command. The ACAH controller determines the control signal, $\boldsymbol{u}$, that follows the commanded attitudes, vertical velocity, and yaw rate. A mixing, or control allocation, system then maps the command signal to individual surfaces depending on the vehicle configuration and flight mode. Aircraft states, $\boldsymbol{x}$, and measurements, $\boldsymbol{y}$, are provided to the controllers.

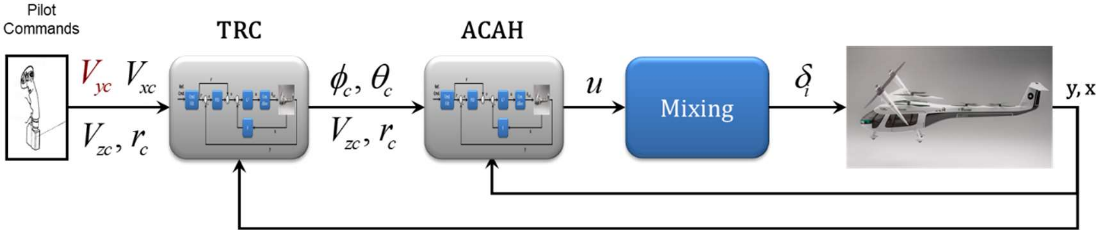


Figure 26. TRC / ACAH architecture

A general architecture for dynamic inversion is shown in Figure 27. Dynamic inversion controllers generate a command, $\boldsymbol{u}$, that follows a reference command generated by a command filter. The NLDI control approach includes nonlinear kinematics in the inversion approach and can streamline the control design process by reducing the need for gain scheduling. The NLDI approach is based on the concept of feedback linearization [Slotine 1991] wherein the actual plant dynamics are inverted, or approximately so, to command the plant to follow a set of *desired dynamics.* DI has been successfully applied to fixed-wing vehicles [Enns 1994, Harris 2018], rotorcraft [Horn 2019], and tiltrotors [Cooper 2010]. Consider a system described by:

$$\begin{gathered} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{gathered} \qquad (1)$$

where $\boldsymbol{x} \in \mathfrak{R}^n$ are the states, $\boldsymbol{u} \in \mathfrak{R}^m$is the control vector, and $\boldsymbol{y} \in \mathfrak{R}^m$ is a vector of measured outputs called the controlled variables (CV). The number of outputs equals the number of control elements in $\boldsymbol{u}$**,** and full-state feedback is required in addition to the measurement vector. The reference command passes through a command filter, sometimes called a flying qualities model, that generates the reference command used in the design, $\boldsymbol{r}$, and derivative. The command filter generates a desired response to pilot inputs and is designed following handling quality (HQ) standards like ADS-33 [USAAMC 2000] for the vertical flight phases and MIL-STD-1797 for flight operating as a fixed-wing aircraft. The DI controller follows the reference command by calculating the control signal $\boldsymbol{u}$:

$$u = G^{-1}(x)(\nu - F(x)) \qquad (2)$$

The closed-loop dynamics are expressed by $\dot{x} = \nu$, where ν is called a pseudo-control. Here, $F(\boldsymbol{x})$ and $G(\boldsymbol{x})$ are approximations to the actual dynamics. If the vehicle dynamics were perfectly modeled and there were no disturbances, the vehicle would follow the desired response, ν. In practice, these assumptions do not exist and a linear proportional-integral-derivative (PID) compensator, K, is added to ν to track the desired signal and govern disturbance compensation.

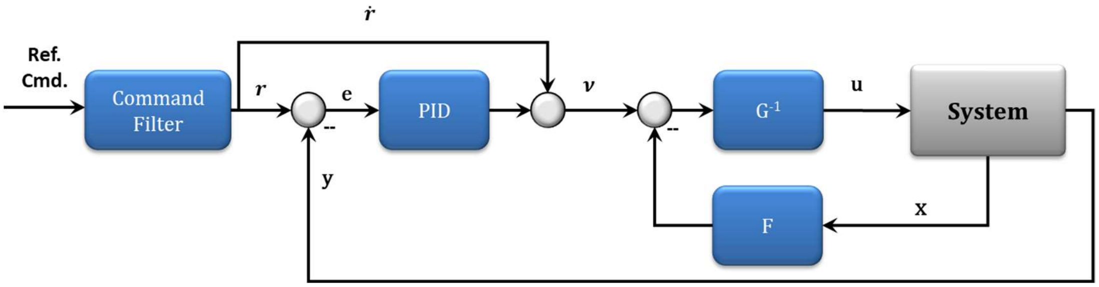


Figure 27. Dynamic inversion architecture

The DI scheme requires the output vector, $\boldsymbol{y}$, to be differentiated until the control signal appears in the resulting equation and that $G(\boldsymbol{x})$ is invertible. Differentiating $\boldsymbol{y}$ results in:

$$\begin{gathered}\dot{y} = \frac{\partial h}{\partial x}(x)\dot{x} = F(x) + G(x)u \\ F(x) \triangleq \frac{\partial h}{\partial x}(x)f(x), \quad G(x) \triangleq \frac{\partial h}{\partial x}(x)g(x)\end{gathered} \tag{3}$$

where $F(\boldsymbol{x})$ and $G(\boldsymbol{x})$ are the Jacobians of the nonlinear system evaluated at different flight conditions. Substituting Eq. (2) into Eq. (3) results in a system of decoupled integrators, $\dot{y} = \nu$. The pseudo-control, ν, is defined by the reference signal and a linear compensator acting on the error signal:

$$\begin{gathered}\nu = \dot{r} + K(s)e \\ e \triangleq r - y\end{gathered} \tag{4}$$

The error dynamics determine the response to disturbances and modeling errors and are described as:

$$\dot{e} = \dot{r} - \dot{y} \;\rightarrow\; \nu - \dot{r} \tag{5}$$

The error dynamics are therefore stable with a proper choice of ν and compensator K(s), which depends on the choice of controlled variables composing the output vector $\boldsymbol{y}$.

The TRC loop employs this architecture and is augmented to include position-hold functionality. As the pilot manipulates the inceptors, velocities are commanded in the longitudinal and lateral axes in the *vehicle heading* frame, vertical rate in the heave axis, and heading rate in the yaw axis. If the inceptors are at trim, the current 3D position and heading angle are maintained. The vehicle heading frame is the NEU frame rotated to align with the UAS's current heading. The x-axis in the vehicle heading frame points in the current heading and the y-axis points out the right wing. In this case, the inertial North (N), East (E), and Up (U) position are controlled. A schematic of the controller for the N position is shown in Figure 28.

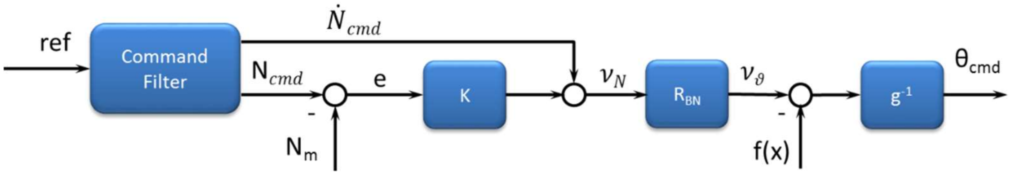


Figure 28. TRC / position hold architecture

The vehicle dynamics describing translational motion are based on pitch and roll changes from trim:

$$\begin{aligned} \dot{V}_x^{vh} &\approx -g\theta \\ \dot{V}_y^{vh} &\approx g\phi \end{aligned} \tag{6}$$

Using this model, the pitch and roll attitude are used as commands to the inner-loop controller to regulate inertial position. The control signals are given by:

$$\begin{aligned} \theta_{cmd} &= -\frac{1}{g}(K_{Px}\tilde{x} + K_{Ix}\int \tilde{x}\,\mathrm{dt} + \mathrm{K}_{Dx}\dot{\tilde{x}}) \\ \phi_{cmd} &= \frac{1}{g}(K_{Py}\tilde{y} + K_{Iy}\int \tilde{y}\,\mathrm{dt} + \mathrm{K}_{Dy}\dot{\tilde{y}}) \end{aligned} \tag{7}$$

Here $\tilde{x}$ and $\tilde{y}$ are the North and East errors rotated in the vehicle heading frame. These commands are input to the inner-loop controller which calculates actuator commands to track the commanded pitch and roll attitudes.

The general NLDI architecture shown in Figure 27 is augmented with an adaptive element resulting in the architecture shown in Figure 29. The Adaptive Command Filter performs a similar function as the NLDI Command Filter. The Adaptive Augmentation block represents an adaptive scheme that could be based on any number of approaches; Model Reference Adaptive Control (MRAC) is chosen for this design. The adaptive element adjusts parameters of the control law and provides function approximation to account for unknown dynamics, errors, external disturbances, impairments, etc. The output of the adaptive element adds to the pseudo-control, ν, produced by the NLDI controller.

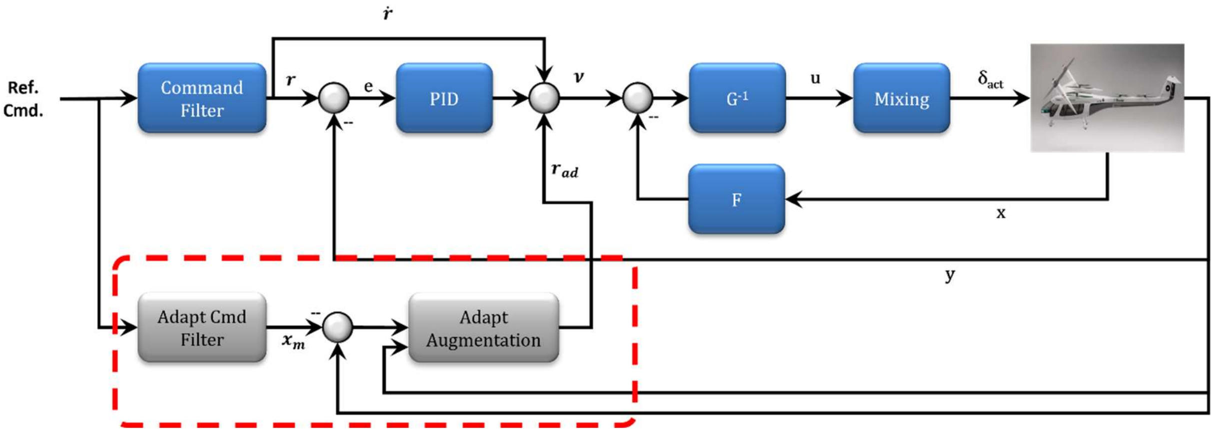


Figure 29. Dynamic inversion architecture with adaptive element

3.7.2 Tracking Control

The Tracking Control system generates the required commands to track a provided trajectory or path and effectively acts as an autopilot. The architecture is shown in Figure 30 and features a nonlinear model predictive control (NMPC) design augmented with an adaptive prediction horizon based on the path characteristics. The adaptive prediction horizon algorithm is implemented in the Path Characteristics block. The NMPC design features a number of benefits that make it appealing when operating in the demanding UAM theater. To summarize a few of these benefits, the NMPC design accounts for changing dynamics, disturbances, and constraints in a rigorous manner; includes nonlinear dynamics yielding increased tracking performance; solves a multi-objective cost function that can optimize over multiple criteria, e.g., tracking error, actuator usage, energy consumption; and explicitly accounts for input, output, and state constraints.

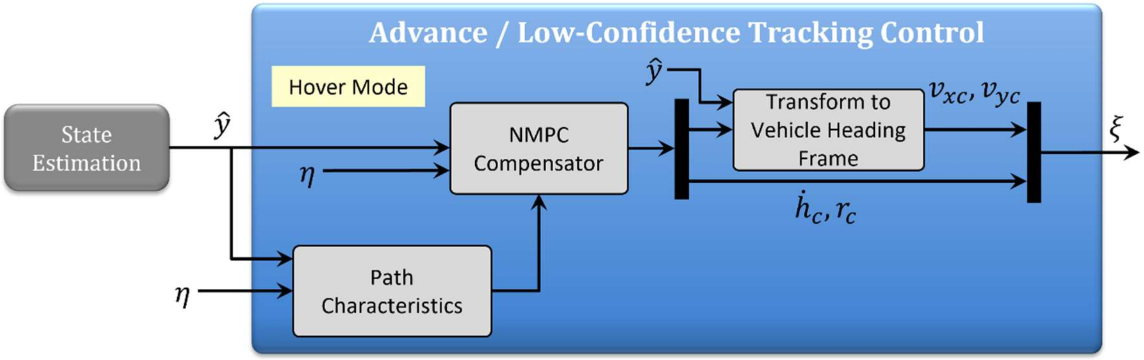


Figure 30. Low-confidence Tracking Control Architecture

The main idea behind NMPC is to solve an optimal control problem at a future time, called the prediction horizon, and then integrate backwards in time until reaching the current time step. In the problem formulation the boundary conditions are specified at the prediction horizon and so the solution must be computed there. The control input at the current time step is used and the process repeats at the next control update. By finding the optimal solution at the prediction horizon, the controller generally exhibits improved performance and reduced transient response. The cost function includes terminal cost, along-the-path cost, and constraints. It can take an arbitrary form, in general, but a quadratic cost function can be used to efficient solution using optimization approaches like gradient descent. A general cost function has the form:

$$F = \underbrace{\Psi_{N_p}\left(x(N_p)\right)}_{\text{Terminal Cost}} + \underbrace{\sum_{i=0}^{N_p-1} L\left(x(i), u(i)\right)}_{\text{Along-Path Cost}} + \underbrace{\lambda_{i+1}^{T}\left(f\left(x(i), u(i)\right) - x(i+1)\right)}_{\text{Constraints w/Lagrange multipliers}} \tag{8}$$

The advanced Tracking Control also has the ability to adjust the prediction horizon based on the characteristics of the path, which can be described based on the curvature and torsion that relate to accelerations. This allows more powerful and flexible representations of the path such as polynomials, B-splines, or Bezier curves. For example, Figure 31 displays a path originally represented as a series of waypoints that has been parameterized as a B-spline curve with smooth and continuous transitions between waypoints. The B-spline curve can be constrained to lie within some constraint distance of each waypoint, or to pass directly through the waypoints, although that was not enforced in the example figure shown below. A parallel transport frame is also shown with origin at a desired point, P. This point is the desired point where the vehicle should be at the current time step and is propagated along the path by a desired, and possibly varying, propagation rate. The error, e, is determined from the vehicle's current position and desired point, P. Given a prediction horizon, with N_p points in the future, a series of desired points, $\{P_{i(s_i)}\}_{i=1}^{N_p}$, can be calculated. This set of points and their derivatives are the reference commands used in the NMPC formulation. Then, based on the path curvature and vehicle performance limits, the prediction horizon can be adapted to improve tracking performance and robustness. Effectively this changes the location along the path where the boundary condition and optimal solution is found in the NMPC formulation.

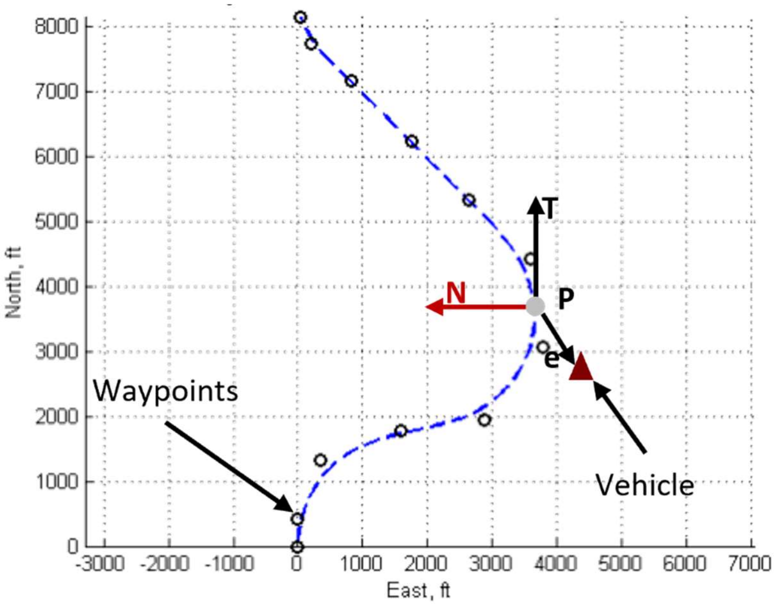


Figure 31. Complex Path Represented as a B-spline Curve

3.7.3 Dynamic Reactive Planning

The DRP controller is the top-level control system responsible for providing the Collision Avoidance function. It continuously computes a collision avoidance solution that may temporarily disregard mission objectives to maintain passenger and aircraft safety. The DRP adheres to a set of hierarchical constraints with different priorities. A notional constraint set is depicted in Figure 32. Here, the most critical constraint is to maintain minimum separation between other aircraft and obstacles, followed by adherence to ACAS or other resolution advisory standards. The Right-of-Way constraint can be interpreted to include adherence to established *rules-of-the-air* and other expected behaviors, including cooperative behaviors. A model of expected cooperative behavior can be extremely beneficial in the case of non-cooperative / non-communicative aircraft. The remaining constraints address a desire to maintain safety against an aircraft or obstacle with a dynamic flight path; maintain a well clear distance with obstacles; keep the highest threat in the sensor field of view; and stay within the flight corridor. This last constraint has particular importance in airspace with congested or dense flight operations, because if one vehicle must deviate from a defined safe corridor it will have a ripple effect on other aircraft. In this case, communication infrastructure must be used to alert pilots of nearby aircraft. Onboard decentralized cooperative collision avoidance algorithms could be a strong advance in safety during these conditions.

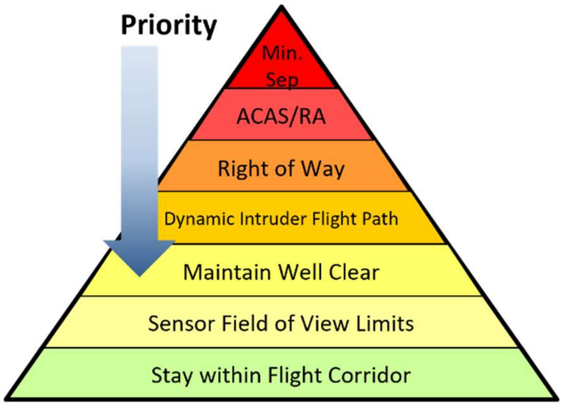

Priority
Min. Sep
ACAS/RA
Right of Way
Dynamic Intruder Flight Path
Maintain Well Clear
Sensor Field of View Limits
Stay within Flight Corridor

Figure 32. Notional DRP Hierarchical Constraints

A notional DRP architecture is adopted from prior work by Barron Associates [Cooper 2014] and shown in Figure 33. The DRP accepts data from the World Map and Obstacle Detection and Tracking system as well as ownship state estimates. The closest time to approach (τ_{CPA}) is computed based on the well-clear volume depicted as the yellow cylinder in the figure. If the projected future flight path of the intruder aircraft violates the well-clear volume within some future time window, then the pilot is alerted of the impending breach and is also provided with the avoidance maneuver. The final form of the avoidance maneuver is encoded as a series of (speed, flight path, and heading) triplets that are compatible with downstream Waypoint Control and Tracking Control components. The avoidance maneuver is shown as the green curve in the figure. For cooperative aircraft, the Collision Avoidance function should rarely be called. With adequate time and communication abilities, flight planning and flight replanning can and should occur prior to invocation of the Automated Collision Avoidance function. Nevertheless, this relies on reliable communication links and other critical systems performing properly, so the Automated Collision Avoidance design should account for all possible scenarios. Once the hazard has been cleared, the flight replanning function should be called to either regain the original flight path or plan a new path to the goal. The DRP automatically generates an avoidance solution, and this maneuver is executed autonomously, unless the pilot takes a positive action to stop the maneuver.

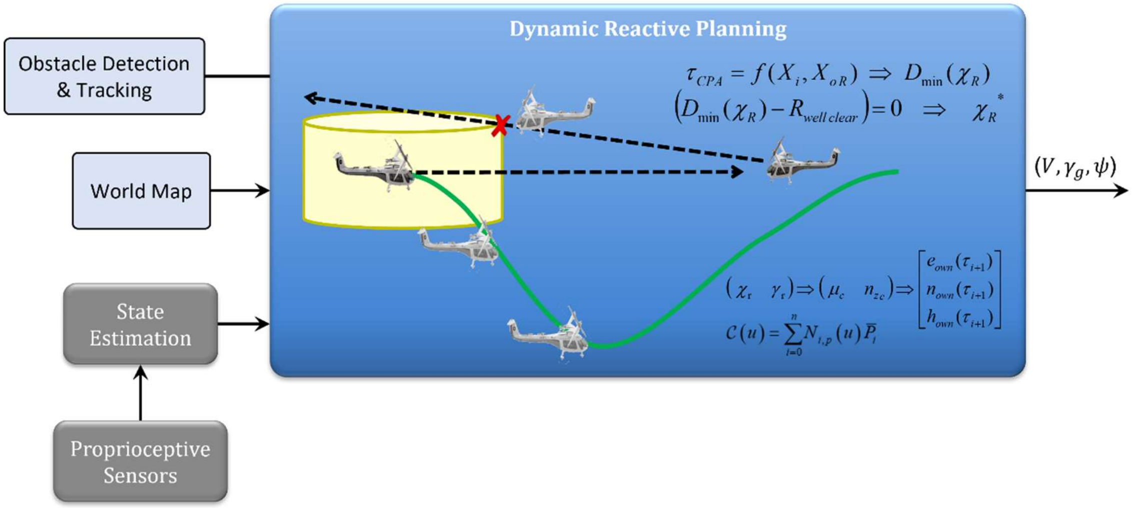

Dynamic Reactive Planning
Obstacle Detection & Tracking
World Map
State Estimation
Proprioceptive Sensors
$\tau_{CPA} = f(X_i, X_{oR}) \Rightarrow D_{\min}(\chi_R)$
$\left(D_{\min}(\chi_R) - R_{well\,clear}\right) = 0 \Rightarrow \chi_R^*$
$(\chi_r \quad \gamma_r) \Rightarrow (\mu_c \quad n_{zc}) \Rightarrow \begin{bmatrix} e_{own}(\tau_{i+1}) \\ n_{own}(\tau_{i+1}) \\ h_{own}(\tau_{i+1}) \end{bmatrix}$
$C(u) = \sum_{i=0}^{n} N_{i,p}(u)\bar{P}_i$
(V, γ_g, ψ)

Figure 33. Notional DRP Architecture

There are four primary signals for this case that determine the "flight mode" and behavior of the DRP:

1. AP Engage - if true engages the autopilot which leads to automated path following for our case
2. RA Issued - true if the DRP Monitor issues an RA
3. DRP Engage - if true commands the autopilot to follow the RA
4. DRP Override - commanded by the pilot and if true does not follow the RA. The state of the AP Engage depends on when the DRP Override was issued as explained below.

We reiterate that at any point in flight, including during a collision avoidance maneuver, the pilot may turn off the autopilot and regain manual control of the vehicle. When the DRP Monitor issues an RA (resolution advisory - this is the command maneuver to avoid the hazard), the pilot is given a time window, ΔT, to override the DRP RA by setting the DRP Override signal to true. If the pilot does not set DRP Override to true within the time window, then both the DRP Engage and AP Engage are set to true, which cause the RA to be automatically followed. This scenario is depicted in Figure 34.

If the pilot sets DRP Override to true within the ΔT window - prior to the start of the DRP RA maneuver - the current flight mode is maintained. If pilot had manual control of the aircraft (AP Engage was false), the pilot maintains manual control. If autopilot was engaged (AP Engage was true), this is maintained and DRP Engage is not set to true. Appropriate systems like the DRP Monitor or World Map continues to monitor and track the object that caused the RA to be issued. This scenario is depicted in Figure 35.

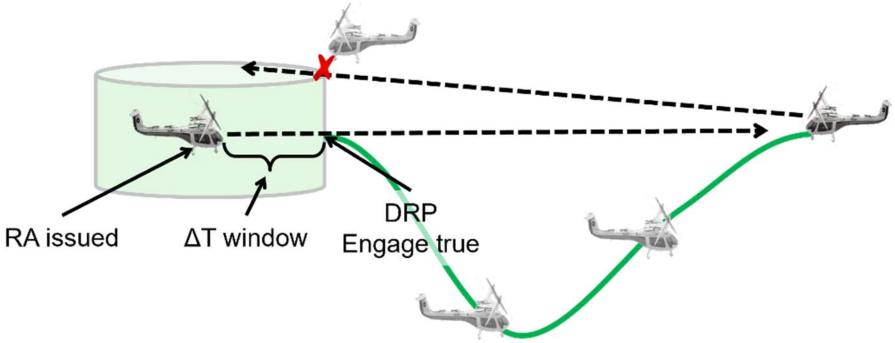


Figure 34. DRP Engagement Logic (Case 1)

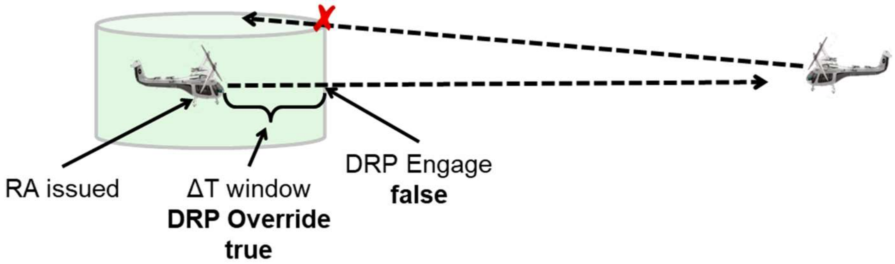


Figure 35. DRP Engagement Logic (Case 2)

If the pilot sets DRP Override true after the ΔT window has passed (i.e., after the RA maneuver has already begun), then both AP Engage and DRP Engage are set to false. The pilot then regains manual control of the aircraft. At this point the pilot can task the flight planner to replan a route (this is strategic flight replanning) to complete mission objectives. Note that this could cause confusion with the pilot because setting DRP Override true has different behavior depending on if it is set within the ΔT window or not. Pilot cues - audio and visual - are needed to ensure the pilots know they have manual control. This scenario is depicted in Figure 36.

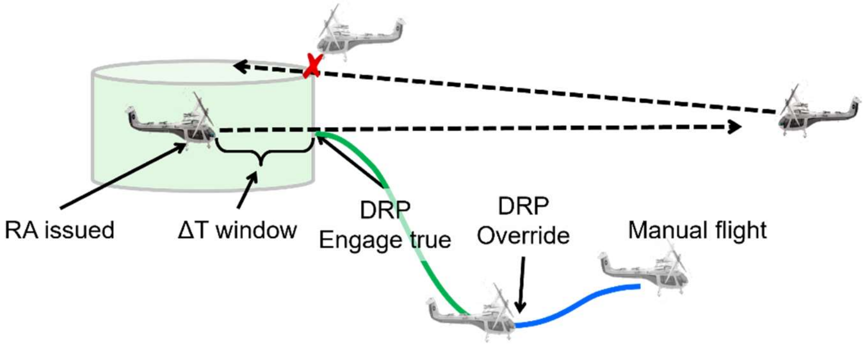


Figure 36. DRP Engagement Logic (Case 3)

Once the pilot issues a DRP Override for a certain case (hazard presumably caused by an intruder aircraft or other flying object, e.g., birds), DRP Monitor does not issue another RA for that hazard unless the object no longer requires an RA for some amount of time, but then does require an RA at a future time. The discussion to this point has not focused specifically on either cooperative or non-cooperative traffic but a note on cooperative traffic is warranted. Non-cooperative traffic refers to vehicles or objects that do not actively communicate with other aircraft through some type of transponder or ADS-B or other system UAM vehicles will use to cooperate and share information. Recent work at NASA has considered cooperative flight planning and replanning, which are related to our work on Collision Avoidance. In considering cooperative collision avoidance there are a number of useful signals that may be used in a cooperative and decentralized collision avoidance function, including:

- Flight mode - automated or manual (pilot control)
- State information - altitude, speed, heading, etc.
- Planned path
- Performance of tracking a flight path
- Expected performance bounds in tracking a path
- Knowledge of “safe corridors” - these are corridors the vehicles are expected to be in (accounts for tracking performance)
- Environmental conditions - is there wind or turbulence making it more difficult to track a path
- Indication of sensor and vehicle health

Finally, it is worth noting that the DRP controller and monitor are architected in a manner that is very similar to the general RTA architecture discussed in Section 1.2.3. This is emphasized in Figure 37 which is an excerpt of the Collision Avoidance functional block diagram. Comparing this diagram to that of Figure 4, it can be seen that the DRP controller fills the role of a high-confidence controller in the general RTA architecture, and the DRP Monitor fills the role of an RTA monitor. Together, the DRP components protect against potential safety violations by the other path-planning components or by the pilot, ensuring safe separation from buildings and other aircraft.

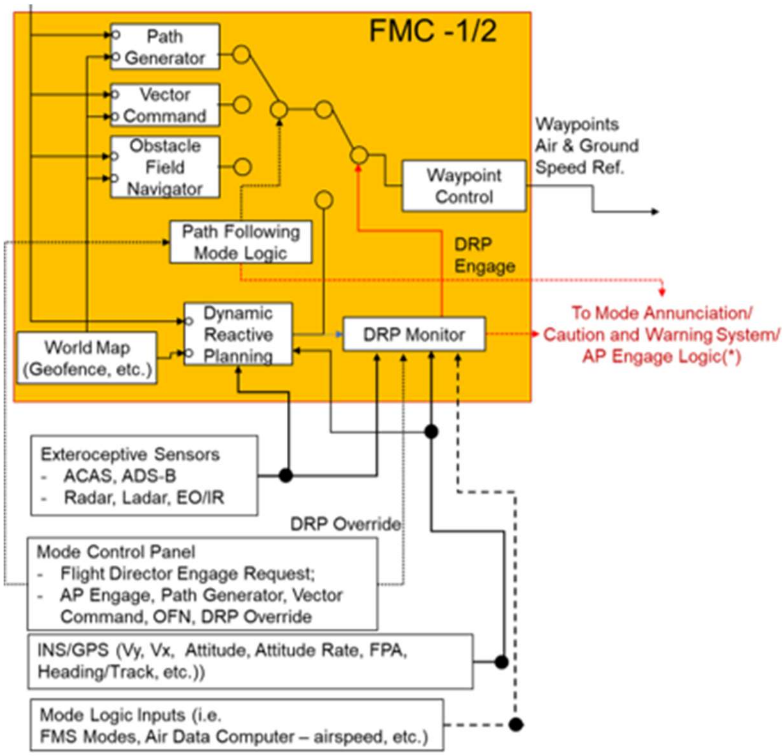

FMC -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Path Following Mode Logic
Waypoint Control
Waypoints Air & Ground Speed Ref.
DRP Engage
To Mode Annunciation/ Caution and Warning System/ AP Engage Logic(*)
Dynamic Reactive Planning
DRP Monitor
World Map (Geofence, etc.)
Exteroceptive Sensors
- ACAS, ADS-B
- Radar, Ladar, EO/IR
DRP Override
Mode Control Panel
- Flight Director Engage Request;
- AP Engage, Path Generator, Vector Command, OFN, DRP Override
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)

Figure 37. DRP as an Application of the RTA Design Pattern

3.8 System Functional Hazard Assessment

The System Functional Hazard Assessment is presented in Appendix C. The required functional design assurance levels are listed in the “Remarks” section of the SFHA tables. Note that the “Remarks” listing of DALs is for convenience, as DALs would normally be documented in program plans such as the “Plan for Software Aspects of Certification” (PSAC) and “Plan for Hardware Aspects of Certification” (PHAC). Catastrophic and Hazardous Failure Conditions are summarized in Table 9, Table 10, and Table 11 for the three selected aircraft functions (TRC Control, Path Following, and Automated Collision Avoidance).

With the list of desired vehicle functions and the results of the AFHA, a system architecture is proposed. The system architecture is a functional block diagram which depicts actual Systems and/or subfunction blocks intended to be implemented in hardware and software. Signal flow and interfaces between Systems and Subfunctions are also depicted.

The SFHA then examines failures of Systems, Subfunctions, signal paths/interfaces and their impact on the function being supported. As an example, the TRC function provides interfaces to the pilot controls (inceptors) to allow manual TRC control. The SFHA then examines the effects of inceptor failures on the TRC function. The SFHA then becomes the next level of hazard analysis, more detailed and one step below the AFHA.

Table 9 provides a summary of catastrophic failure conditions of the TRC function. A functional block diagram of this function can be found in Figure 55.

Due to its use primarily as a low altitude takeoff and landing control mode, all failures at low altitude are considered catastrophic. This requires a FDAL assignment of level B, as well as analysis to show that no single fault in the design can cause any of these failure conditions. An example of a single fault is a mis-compare of the data from the two installed INS/GPS units which cannot be isolated to either of the two INS/GPS units. For this case, possible mitigation includes installation of a third INS/GPS unit. Since the TRC control mode controls lateral and longitudinal ground speed, an additional third source of ground speed may be found in the GPS unit, if powered independently and otherwise independent of its collocated INS. Some additional work must be done before contemplating use of GPS as a third source:

- Satellite RF Multi path degrading the quality of GPS velocity when operating below the city skyline
- Loss of satellite reception when operating below the city skyline
- Any bandwidth limitations of the GPS velocity inputs

Since TRC failures include catastrophic failure conditions, then at the functional level, the functional design assurance level (FDAL) is level B.

Table 9 Provide Translation Rate Command Horizontal Control Mode Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App B Failure Condition Number	Classification
Loss of (left/right) hand inceptor (control of Vx, Vy. Vz velocities in manual flight)	FCS.1.1.TL1	Catastrophic
Erroneous (left/right) inceptor position outputs	FCS.1.1.MF1	Catastrophic
Loss of FCC TRC mode during takeoff or landing due to loss of or incorrect mode logic inputs (prematurely exits TRC mode to another mode):	FCS.1.1.TL2	Catastrophic
Loss of FCC TRC control computational capability causes loss of TRC function	FCS.1.1.TL3	Catastrophic
Loss of Autopilot during takeoff or landing not annunciated to the pilot	FCS.1.1.TL5	Catastrophic
Inability to disengage autopilot	FCS.1.1.TL8	Catastrophic
Inadvertent/erroneous autopilot engagement (system not yet providing valid guidance commands to autopilot/pilot not expecting autopilot engagement)	FCS.1.1.MF6	Catastrophic

Failure Condition	App B Failure Condition Number	Classification
Erroneous FCC TRC control computational capability causes incorrect TRC control	FCS.1.1.MF2	Catastrophic
Erroneous FCC flight director display output while in manual flight	FCS.1.1.MF3	Catastrophic
Erroneous FCC mode annunciation computation during takeoff or landing	FCS.1.1.MF4	Catastrophic
Erroneous TRC engagement	FCS.1.1.MF5	Catastrophic
Loss INS/GPS feedback signals to TRC controller causes loss of TRC function	NAV.1.1.TL1	Catastrophic
Loss of FMS TRC mode not annunciated to the pilot	NAV.1.1.TL3	Catastrophic
Erroneous INS/GPS feedback signals to TRC controller causes incorrect TRC control	NAV.1.1.MF1	Catastrophic
Undetected erroneous FMS generated flight path references cause incorrect TRC control	NAV.1.1.MF2	Catastrophic
Loss of ability of the pilot to bias the FMS TRC path when needed due to loss of either inceptor	NAV.1.1.PL1	Catastrophic
Erroneous FMS TRC path bias applied due to erroneous inceptor outputs	NAV.1.1.MF4	Catastrophic
Erroneous flight director display while in manual flight (also unannunciated loss of flight director)	DSP.1.1.MF1	Catastrophic
Loss of TRC mode annunciation (TRC still engaged)	DSP.1.1.TL2	Catastrophic
Erroneous mode annunciation during takeoff or landing (TRC mode engaged)	DSP.1.1.MF2	Catastrophic
Loss of autopilot disengage warning	DSP.1.1.MF3	Catastrophic

Table 10 provides a summary of Catastrophic and Hazardous failure conditions for the Path Following Control mode. A functional block diagram of this function can be found in Figure 56.

For flight phases other than cruise (i.e. takeoff, approach, landing), the Path Following Control mode needs to remain operational (fail-op) after a single failure, since loss of or malfunction (erroneous) operation is catastrophic at these lower altitudes due to potential for collisions and/or unsafe maneuvers. This would typically require dual fully monitored FMSs and FCCs, and triple INS.

"Minimally Trained Pilot" assumptions necessitate that some failures are deemed more severe than they otherwise would be for more highly trained and experienced pilots. If the "Minimally Trained Pilot" can be assumed to respond properly to annunciated loss of the Path Following Control mode, then it may be possible to implement a system with a single fully monitored FMS. Un-annunciated loss of mode would still need to be shown to occur at less than 10^{-8} per flight hour, along with the "no single fault" criteria for un-annunciated loss of mode.

Required FDAL for the Path Following Control mode is level B.

Table 10 Provide Path Following Control Mode Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App B Failure Condition Number	Classification
Undetected/un-annunciated loss of waypoint data (failure is in FCC)	FCS.2.1.TL2	Hazardous
Undetected/unannunciated erroneous waypoint data(failure is in FCC)	FCS.2.1.MF2	Hazardous
Loss of waypoint data with or without detection/annunciation to the pilot (failure is in FCC)	FCS.2.1.TL3	Catastrophic
Erroneous waypoint data with or without detection/annunciation to the pilot (failure is in FCC)	FCS.2.1.MF3	Catastrophic
Undetected/unannunciated loss of INS data to Tracking Controller	FCS.2.1.TL5	Hazardous
Undetected/un-annunciated erroneous feedback data from INS to tracking controller	FCS.2.1.MF5	Hazardous
Loss of INS data to Tracking Controller with or without detection/annunciation to the pilot	FCS.2.1.TL6	Catastrophic
Erroneous feedback data from INS to tracking controller with or without detection/annunciation to the pilot	FCS.2.1.MF6	Catastrophic
Undetected/un-annunciated loss of Path Mode (Mode logic error)	FCS.2.1.TL8	Hazardous
Loss of Path Mode (FCC path mode disengages) with or without detection/annunciation to the pilot	FCS.2.1.TL9	Catastrophic
Tracking Control algorithm calculates erroneous outer loop control data undetected/un-annunciated	FCS.2.1.MF8	Hazardous

Failure Condition	App B Failure Condition Number	Classification
Tracking Control algorithm calculates erroneous outer loop control data with or without detection/annunciation to the pilot	FCS.2.1.MF9	Catastrophic
Undetected/un-annunciated loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS)	NAV.2.1.TL2	Hazardous
Undetected/un-annunciated erroneous Path Generation/Waypoint Control data	NAV.2.1.MF3	Hazardous
Loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS) with or without detection/annunciation to the pilot	NAV.2.1.TL3	Catastrophic
Erroneous Path Generation/Waypoint Control data with or without detection/annunciation to the pilot	NAV.2.1.MF4	Catastrophic
Uncommanded Path Mode engagement	NAV.2.1.MF1	Catastrophic

Table 10 provides a summary of Catastrophic failure conditions for the Airborne Vehicle Collision Avoidance function (there are no failure conditions deemed hazardous). Two main components in the navigation system provide the collision avoidance function. The first is a monitor to determine if a collision or threat is imminent and the second is the maneuver required to avoid the collision/threat. A functional block diagram of this function can be found in Figure 57.

Two strategies are employed to avoid collisions. The first is the flight plan itself which considers the locations and heights of buildings and other obstacles in the construction of a flight path to avoid these obstacles (the “geo-fence”), as well as knowledge of other co-operative aircraft flight plans. The second strategy employs a sophisticated array of vehicle real time sensors to provide the necessary information for both air and ground threats for real time detection and avoidance.

The pilot is given a means to cancel the collision avoidance maneuver if the pilot deems prudent.

Since the FMS navigation function contains the collision avoidance function, the FMS needs to be high integrity (example fully monitored com/mon architecture) to mitigate errors. The vehicle real time sensors will also need some form or error mitigation including common cause aspects. As long as the pilot is deemed able to take over the collision detection and avoidance in case of annunciated loss of function, then there are no redundancy requirements of the FMS.

The collision avoidance function is potentially a very complex function, as there will be requirements for error free operation and full coverage of the airspace around the vehicle with the ability to assess and avoid multiple threats. The required FDAL of the function is level B. Corresponding IDALs for the FMS and vehicle sensor array will also be level B.

The level B collision avoidance function may be considered a form of RTA and therefore used as a RTA mitigation for other functions whose erroneous operation may result in collision threats.

Table 11 Provide Airborne Vehicle Collision Avoidance Catastrophic/Hazardous Flight Conditions Summary

Failure Condition	App B Failure Condition Number	Classification
Loss of DRP Monitor/Planner (threat detection capability) due to external sensor failure or FMS input failure, undetected/unannunciated	NAV.3.1.TL2	Catastrophic
Loss of DRP Monitor/Planner (threat detection capability) due to DRP Monitor computation failure undetected/un-annunciated	NAV.3.1.TL4	Catastrophic
Erroneous DRP Monitor/Planner	NAV.3.1.MF1	Catastrophic

3.9 Systems Theoretic Process Analysis

This section provides an overview of the work conducted as well as sample artifacts for STPA of the baseline aircraft design. This analysis is conducted with the intent to identify how STPA may complement ARP hazard analysis processes. The process and results from STPA consideration of the TRC function are outlined in this section. Additional results with unsafe control actions and loss scenarios from the STPA work can be found in Appendix D.

The eVTOL aircraft's operational environment is assumed similar to those used in [Graydon 2020]. First, it is assumed that the aircraft is operating in a large metropolitan landscape (i.e. high-rise buildings, busy airport, etc.). Second, a shared airspace with other manned and unmanned air traffic is assumed.

The STPA process described in [Leveson 2018] is adapted for this analysis and the development of STPA artifacts. The conducted work is not a complete STPA analysis of an aircraft's control system. Instead, select examples are produced at each step for illustrative purposes. The employed process is outlined below:

1. Define the Purpose of the Analysis
   A. Identify things that are important to potential stakeholders, and define associated losses. These losses facilitate the identification of hazards and constraints.
   B. Identify and define system-level hazards from the losses. The hazards describe aircraft states that may result in a loss when the aircraft is operating in worst-case environmental conditions.

   C. Identify and define system-level constraints from the system-level hazards. These constraints must be met to avoid losses.

2. Model the Control Structure
   A. Identify functions of interest for analysis.
   B. Develop a hierarchical control system architecture.
   C. Determine functional relationships and interactions within the control architecture in order to identify which sub-systems must be analyzed.
   D. Identify inputs and outputs to sub-systems within the control architecture. Some of the inputs/outputs are considered as being control actions, and they facilitate the identification of unsafe control actions.
3. Identify Unsafe Control Actions
   A. Identify unsafe control actions by analyzing the various control actions (CAs) to determine whether they could lead to hazards/losses. Consider various types of control actions (e.g., not providing CA, providing CA, providing CA to soon/late/out-of-sequence, and applying CA too briefly/long leads to loss)
4. Identify Loss Scenarios
   A. Identify a control system component (e.g., tracking controller) and one or more of its unsafe control actions for analysis.
   B. Define the control loop for the chosen control system component.
   C. Identify potential causal factors for the chosen unsafe control action at each point in the control loop. Loss scenarios describe causal factors for unsafe control actions that may elicit hazards/losses.
   D. Repeat this step for all control system components and unsafe control actions that are of interest.

The losses defined in Table 12 are borrowed from the UAM hazard analysis research paper [Graydon 2020]. These losses are intended to provide a foundation for the STPA analysis. All developed STPA artifacts can be traced back to at least one of these losses. This list is not necessarily comprehensive, and certain losses, such as environmental loss, are not considered for the purposes of this analysis.

Table 12. STPA Losses

ID	Loss Description
L-1	Death of or injury to a human (aircrew, groundcrew, passenger, or third party).
L-2	Loss of or damage to an aircraft (ownship or other).
L-3	Loss of or damage to ground structures.

Hazards that were borrowed from [Graydon 2020] for the STPA analysis are defined in Table 13. The hazards describe aircraft states that may result in a loss during worst-case environmental conditions. Each of the hazards can be traced back to one or more losses. The list of hazards below satisfies the purposes of this analysis, though it is not necessarily comprehensive.

Table 13. STPA Hazards

ID	Hazard Description	Corresponding Loss
H-1	Ownship violates minimum separation standards in flight.	L-1, L-2
H-2	Ownship is operating in environment or flight regime (e.g., altitude, airspeed, or weather concerns) that is beyond its operating limits.	L-1, L-2, L-3
H-3	Ownship is not at a safe distance from terrain or an obstacle.	L-1, L-2, L-3
H-4	Ownship motion exceeds limits for occupant health and comfort.	L-1

System-level constraints are derived from the hazards above to define conditions that the aircraft must meet in order to avoid losses. These constraints are listed in Table 14.

Table 14. STPA System-Level Constraints

ID	System-Level Constraint Description	Corresponding Hazard
SC-1	Ownship must maintain minimum separation standards in flight.	H-1
SC-2	Ownship must operate only in environments and flight regimes (e.g., altitude, airspeed, weather concerns) that are within its operating limits.	H-2
SC-3	Ownship must maintain safe distance from terrain and obstacles.	H-3
SC-4	Ownship must move at rates appropriate for occupant health and comfort.	H-4

A hierarchical control structure is developed to organize the control systems in a way that is conducive to STPA analysis. This model was first adapted from a control architecture in [Takahashi 2017] prior to the initial completion of our aircraft's control system design. It has been iteratively modified to conform to our aircraft's control system design as the design developed. Figure 38 delineates the STPA Control architecture relevant to the TRC system.

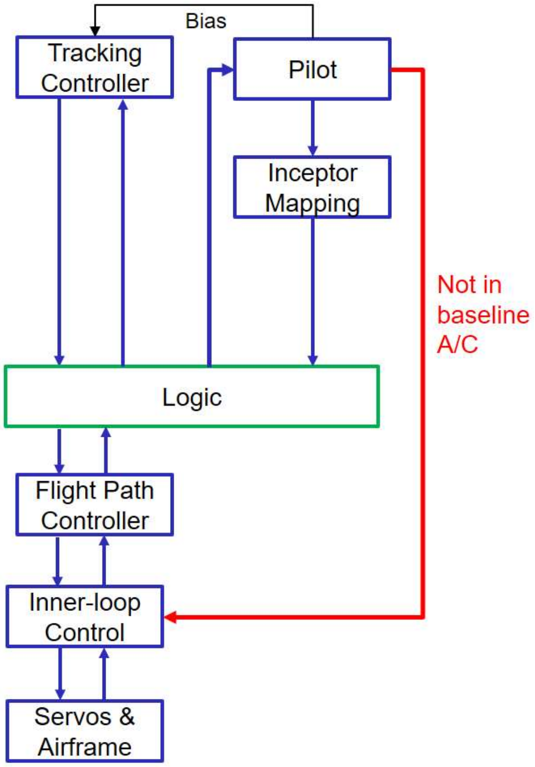


Figure 38. STPA Control Architecture for the TRC Function

STPA analysis is conducted on multiple systems in this hierarchical model. TRC is primarily analyzed in the tracking controller for the aircraft's hover mode configuration. However, unsafe control actions and loss scenarios are also developed for the flight path controller and for the inner-loop control system.

The logic block in this control structure identifies and disseminates information regarding the aircraft's flight mode (i.e., hover, wingborne, or transition) and automation mode (i.e., auto or manual). A bias input is included from the pilot to the tracking controller. The bias signal modifies the aircraft's trajectory when the pilot moves the stick while the autopilot is flying. Its components are consistent with the waypoint controller's output.

Unsafe control actions (UCAs) are identified for each of the blue blocks in the STPA hierarchical control structure. In the case of the FMS, UCAs were identified for its sub-systems: path generator, DRP, and waypoint control. A UCA is a control action that will result in a hazard under worst-case environmental conditions. Identified UCAs were organized into tables where the row indicates the control variable, and the column indicates the UCA's category. As an example of one of the developed UCA tables, the UCAs for the aircraft's TRC function are shown in Table 15.

Table 15. TRC Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing Too Soon, too Late, or Out of Sequence

Velocity	**UCA.TRC.1** No command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3]	**UCA.TRC.2** Velocity command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3] **UCA.TRC.3** Velocity command given when in hover leads to rapid acceleration [H-4] **UCA.TRC.4** Command provided during wingborne flight [H-2] **UCA.TRC.5** Velocity command results in exceedance of flight envelope [H-2]	**UCA.TRC.6** Velocity command applied too late to avoid other aircraft or terrain/obstacle when in hover [H-1,3] **UCA.TRC.7** Command sent too late in the case that the aircraft has already switched to transition or wingborne mode [H-2]
Yaw Rate		**UCA.TRC.8** Yaw rate command given when in hover leads to rapid angular acceleration of the aircraft [H-4] **UCA.TRC.9** Command provided during wingborne flight [H-2]	**UCA.TRC.10** Command sent too late in the case that the aircraft has already switched to transition or wingborne mode [H-2]

Each of the UCAs is mapped to one or more of the hazards in Table 13. They are categorized in columns according to how the control action is unsafe. The example above only shows three of these categories, but the following four categories are considered for each control system block:

- Not providing causes hazard
- Providing causes hazard
- Providing too soon, too late, or out of sequence causes hazard
- Stopping too soon, applying too long causes hazard

Figure 39 shows a control loop for the TRC function along with corresponding loss scenarios at each input/output. These loss scenarios describe factors causing UCA.TRC.2 and UCA.TRC.3, shown in red in Table 15, to occur. As recommended by [Leveson 2018], loss scenarios fitting the following cases are identified for TRC as well as the other analyzed functions in Appendix D.

- Scenarios that lead to unsafe control actions
    - Unsafe controller behavior

    - Causes of inadequate feedback and information
- Scenarios in which control actions are improperly executed or not executed
    - Scenarios involving the control path
    - Scenarios related to the controlled process

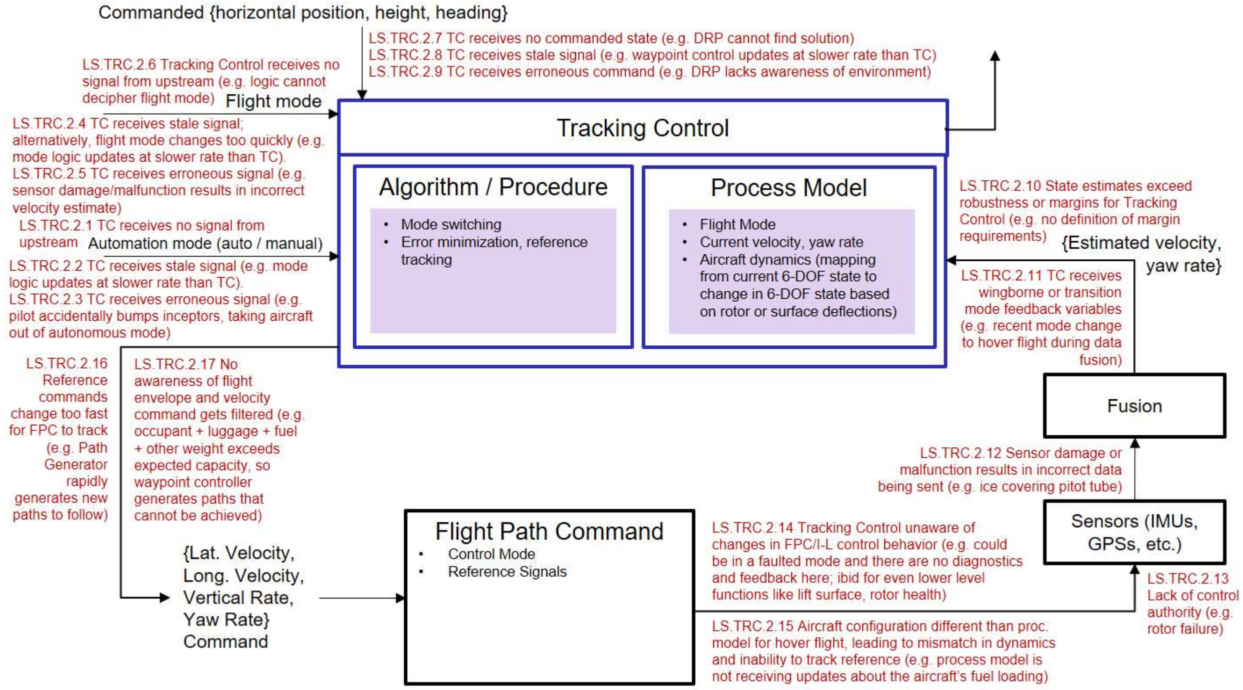

Commanded {horizontal position, height, heading}
LS.TRC.2.7 TC receives no commanded state (e.g. DRP cannot find solution)
LS.TRC.2.8 TC receives stale signal (e.g. waypoint control updates at slower rate than TC)
LS.TRC.2.9 TC receives erroneous command (e.g. DRP lacks awareness of environment)
LS.TRC.2.6 Tracking Control receives no signal from upstream (e.g. logic cannot decipher flight mode)
Flight mode
LS.TRC.2.4 TC receives stale signal; alternatively, flight mode changes too quickly (e.g. mode logic updates at slower rate than TC).
LS.TRC.2.5 TC receives erroneous signal (e.g. sensor damage/malfunction results in incorrect velocity estimate)
LS.TRC.2.1 TC receives no signal from upstream
Automation mode (auto / manual)
LS.TRC.2.2 TC receives stale signal (e.g. mode logic updates at slower rate than TC).
LS.TRC.2.3 TC receives erroneous signal (e.g. pilot accidentally bumps inceptors, taking aircraft out of autonomous mode)
Tracking Control
Algorithm / Procedure
• Mode switching
• Error minimization, reference tracking
Process Model
• Flight Mode
• Current velocity, yaw rate
• Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections)
LS.TRC.2.10 State estimates exceed robustness or margins for Tracking Control (e.g. no definition of margin requirements)
{Estimated velocity, yaw rate}
LS.TRC.2.11 TC receives wingborne or transition mode feedback variables (e.g. recent mode change to hover flight during data fusion)
Fusion
LS.TRC.2.12 Sensor damage or malfunction results in incorrect data being sent (e.g. ice covering pitot tube)
Sensors (IMUs, GPSs, etc.)
LS.TRC.2.13 Lack of control authority (e.g. rotor failure)
LS.TRC.2.16 Reference commands change too fast for FPC to track (e.g. Path Generator rapidly generates new paths to follow)
LS.TRC.2.17 No awareness of flight envelope and velocity command gets filtered (e.g. occupant + luggage + fuel + other weight exceeds expected capacity, so waypoint controller generates paths that cannot be achieved)
{Lat. Velocity, Long. Velocity, Vertical Rate, Yaw Rate} Command
Flight Path Command
• Control Mode
• Reference Signals
LS.TRC.2.14 Tracking Control unaware of changes in FPC/I-L control behavior (e.g. could be in a faulted mode and there are no diagnostics and feedback here; ibid for even lower level functions like lift surface, rotor health)
LS.TRC.2.15 Aircraft configuration different than proc. model for hover flight, leading to mismatch in dynamics and inability to track reference (e.g. process model is not receiving updates about the aircraft's fuel loading)

Figure 39. TRC Loss Scenarios (LS.TRC.2)

Examples for how the loss scenarios might occur are organized into the following three categories:

- Cannot track the commanded velocity due to lower-level controller failure
- Commanded velocity exceeds the flight envelope (either commanded velocity exceeds limit or the flight envelope unexpectedly changes)
- Commanded velocity leads to LOS, and it is tracked

These three categories have implications on the design as well as what the pilot should or should not be able to do. It is assumed that the pilot is acting primarily in a monitoring function vs. actively flying the aircraft at all times. This aligns with assumption that pilot can turn aviate/navigate tasks over to automation. The examples below show that the tracking controller may need vehicle health information, sensor status, and other data. Examples for how the TRC loss scenarios in Figure 39 may occur are listed below. Each example is traced back to its corresponding loss scenario. Similarly, the higher-level bullet points that categorize the examples are traced back to a corresponding UCA.

- TRC commands velocity that would maintain separation, but the system cannot adhere to this velocity [UCA.TRC.2]
    - Flight mode logic updates at slower rate than TC [LS.TRC.2.4]

    - Flight mode logic cannot decipher flight mode [LS.TRC.2.6]
    - Waypoint controller rapidly generates new paths to follow, resulting in reference commands changing too quickly for FPC to track [LS.TRC.2.16]
    - Lower-level controller or aircraft component is in a faulted mode that the TC is unaware of [LS.TRC.2.14]
    - Rotor failure results in lack of control authority [LS.TRC.2.13]
- TRC commands velocity that would maintain separation, but this velocity exceeds the flight envelope [UCA.TRC.5]
    - Commanded velocity exceeds maximum allowable velocity (commanded waypoint has an unrealistic time constraint)
        - Process model is not receiving updates about the aircraft's fuel loading [LS.TRC.2.15]
    - Flight envelope changes due to external causes
        - Occupant + luggage + fuel + other weight exceeds expected capacity, so waypoint controller generates paths that cannot be achieved [LS.TRC.2.17]
        - Damage, or wear and tear to rotors impairs vehicle performance [LS.TRC.2.17]
- Commanded velocity itself leads to LOS, and the velocity is tracked [UCA.TRC.2]
    - DRP cannot find solution [LS.TRC.2.7]
    - Waypoint Control updates at slower rate than TC, resulting in TC receiving stale signal [LS.TRC.2.8]
    - DRP lacks awareness of environment, resulting in TC receiving erroneous command [LS.TRC.2.9]
    - Pilot accidentally bumps inceptors, taking the aircraft out of autonomous mode [LS.TRC.2.3]
    - Sensor damage/malfunction (e.g., ice covering pitot tube) results in incorrect state estimate [LS.TRC.2.12]

4.0 RTA-Protected Aircraft Development

This section addresses the design of the RTA-protected aircraft variant. As most of the architecture is identical for both the baseline and RTA-protected designs, the focus here is on the differences between the two and the safety implications of those differences. A key result is that the RTA architecture allows the advanced control algorithms implementing TRC and Tracking Control to be assigned a much lower IDAL, which may be critical for certification of these components.

4.1 RTA-Protected TRC

The TRC controller is active while the vehicle is in hover mode and is designed to provide increased handling qualities and reduced pilot workload. The RTA-protected aircraft variant incorporates the same ANLDI TRC controller as the baseline aircraft, which was discussed in detail in Section 3.7.1. However, in the RTA-protected variant, this controller is coupled with a more traditional (high-confidence) TRC implementation and an RTA monitor to switch between the two. The high-confidence implementation follows a gain-schedule PID approach. The gains are scheduled as functions of ground speed and airspeed, with additional schedules governing the use of certain effectors (rotors and aerodynamic surfaces) and the angle of the wing-tip rotors. The PID-based controller will not provide many of the benefits that come from the ANLDI-based controller, such as turbulence mitigation, improved ride quality, improved handling qualities, etc. However, it is intended for use only in the (hopefully rare) case that the ANLDI-based controller fails to meet safety or performance requirements. By including the PID-based controller as a reversionary system, the ANLDI-based controller can be assigned a lower DAL than in the baseline vehicle case, significantly reducing the time and cost associated with its development.

The RTA architecture for the TRC controller is shown at a high-level in Figure 40, which reproduces the TRC functional block diagram from Figure 21 but highlights two alternatives for the TRC controller. The Baseline Vehicle design, which was developed in Section 3.0, contains a single TRC implementation featuring the ANLDI design. This alternative is illustrated on the left side of the figure. The RTA-Protected Vehicle design contains both ANLDI and gain-scheduled PID implementations. The ANLDI implementation fills the role of a low-confidence controller, and it is intended to receive a lower DAL assignment than the high-confidence PID implementation. The RTA Monitor and Switch is responsible for confirming correct operation of the ANLDI design, and if incorrect operation is detected, it switches to the high-confidence gain-schedule PID design. The intended IDAL assignments for each of the control architectures and RTA monitor are also shown in the figure. Note that these are *intended* IDAL assignments; actual IDAL assignments must be determined through the SFHA and PSSA activities.

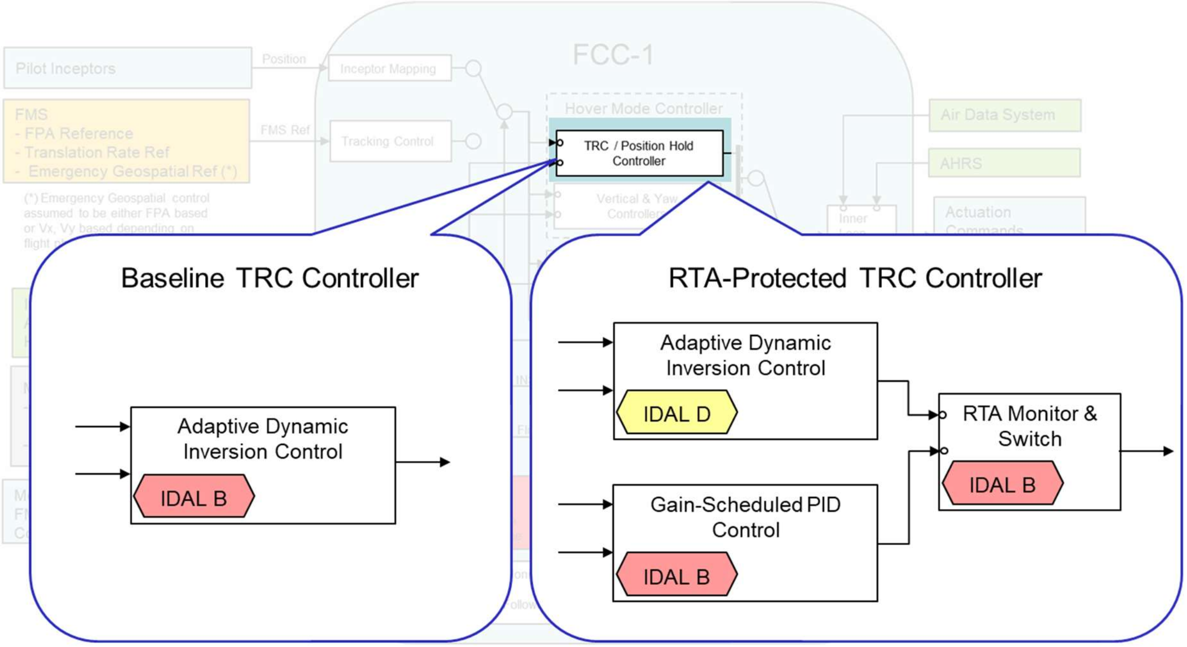

FCC-1
Pilot Inceptors
Position
Inceptor Mapping
FMS
- FPA Reference
- Translation Rate Ref
- Emergency Geospatial Ref (*)
FMS Ref
Tracking Control
(*) Emergency Geospatial control assumed to be either FPA based or Vx, Vy based depending on flight
Hover Mode Controller
TRC / Position Hold Controller
Vertical & Yaw Controller
Air Data System
AHRS
Inner
Actuation Commands
Baseline TRC Controller
Adaptive Dynamic Inversion Control
IDAL B
RTA-Protected TRC Controller
Adaptive Dynamic Inversion Control
IDAL D
Gain-Scheduled PID Control
IDAL B
RTA Monitor & Switch
IDAL B

Figure 40. RTA Architecture for the TRC Controller

A detailed design of switching conditions for the RTA system is beyond the scope of this effort but an example of the switching condition with the vehicle in hover mode, focused on staying outside the domain defining the vortex ring state, was performed in the prior BAART task. That example performed a conceptual analysis of one type of aerodynamic condition (vortex ring state) that would be included in the design of an RTA system for an actual vehicle. Beyond aerodynamic states there are also structural, sensors, power systems, etc., that should be considered. In general, the RTA system checks conditions that relate to safety requirements, performance metrics, and content of the signals communicated between systems. A subset of the checks the RTA monitor would perform include: confirming that the vehicle is in the Type III safety region, confirming that minimum tracking performance on reference signals is achieved, checking that peak transient errors are appropriately bounded, checking that limit cycle oscillations are not present, and verifying that the mean-squared error (MSE) is appropriately bounded over some past time window. The RTA system would also ensure the output commands from ANLDI system are within specified limits of the inner-loop system receiving these commanded signals. Any switch to the PID-based implementation must be timely enough to ensure that all safety requirements are satisfied at all times.

Specifically, for the TRC controller, the input command signals for lateral and longitudinal velocity should be inspected to ensure the signal magnitude and qualities (e.g., rates, frequency limits, etc.) are within bounds. The bounds of these reference signals should also be checked in combination with other signals, such as vertical rate, to ensure aerodynamic states like vortex ring state, and aeroelastic instabilities are not encountered. Performance metrics, as previously, mentioned should be checked using metrics such as MSE, transient response, etc. The output signals of the TRC controller are roll and pitch attitude, computed to track the reference lateral and longitudinal velocities, respectively. Limit checking on these signals should also be performed.

4.2 RTA-Protected Tracking Control

The Tracking Control system generates the required commands to track a provided trajectory or path and effectively acts as an autopilot. Tracking Control for the RTA-protected aircraft variant incorporates the same adaptive NMPC algorithm that was used for the baseline vehicle design, which was discussed in detail in Section 3.7.2. However, in the RTA-protected variant, this implementation is coupled with a more traditional (high-confidence) tracking control implementation and an RTA monitor to switch between them. The high-confidence implementation follows a gain-scheduled PID approach. The PID-based controller will not provide many of the benefits that come from the NMPC-based controller, such as minimum energy consumption, high tracking accuracy, etc. However, it is intended for use only in the (hopefully rare) case that the NMPC-based controller fails to meet safety or performance requirements. By including the PID-based controller as a reversionary system, the NMPC-based tracking controller can be assigned a lower DAL than in the baseline vehicle case, significantly reducing the time and cost associated with its development.

The RTA architecture for the Tracking Control system is shown at a high-level in Figure 41, which reproduces the Tracking Control functional block diagram from Figure 22 but highlights two alternatives for the Tracking Control system. The Baseline Vehicle design, which was developed in Section 3.0, contains a single Tracking Control implementation featuring the adaptive NMPC design. This alternative is illustrated on the left side of the figure. The RTA-Protected Vehicle design contains both the adaptive NMPC and gain-scheduled PID implementations. The NMPC implementation fills the role of a low-confidence controller in the RTA design pattern, and it is intended to receive a lower DAL assignment than the high-confidence PID implementation. The RTA Monitor and Switch is responsible for confirming correct operation of the NMPC design, and if incorrect operation is detected, it switches to the high-confidence gain-scheduled PID design. The intended IDAL assignments for each of the tracking control architectures and RTA monitor are also shown in the figure. Note that these are *intended* IDAL assignments; actual IDAL assignments must be determined through the SFHA and PSSA activities.

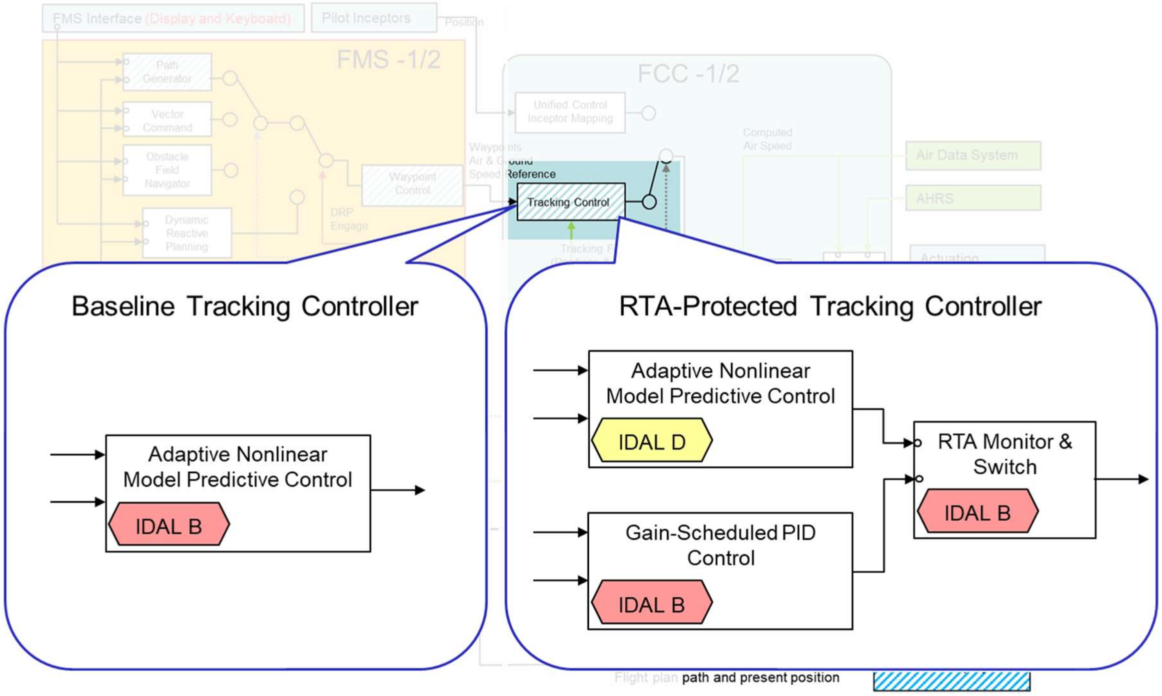

FMS Interface (Display and Keyboard)
Pilot Inceptors
Position
FMS -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Dynamic Reactive Planning
DRP Engage
Waypoint Control
FCC -1/2
Unified Control Inceptor Mapping
Waypoints Air & Ground Speed Reference
Tracking Control
Computed Air Speed
Air Data System
AHRS
Actuation
Baseline Tracking Controller
Adaptive Nonlinear Model Predictive Control
IDAL B
RTA-Protected Tracking Controller
Adaptive Nonlinear Model Predictive Control
IDAL D
Gain-Scheduled PID Control
IDAL B
RTA Monitor & Switch
IDAL B
Flight plan path and present position

Figure 41. RTA Architecture for the Tracking Controller

The inputs to the Tracking Controller consist of a finely spaced sequence of waypoints with timing information that the vehicle must follow. The RTA monitor continually checks whether the adaptive NMPC implementation is causing the vehicle to accurately traverse these waypoints, switching to the PID-based implementation if a violation of the tracking accuracy or other performance requirements is imminent. The outputs of the Tracking Controller in hover mode are lateral velocity, longitudinal velocity, vertical rate, and yaw rate and are the commands computed to track the reference trajectory. The RTA monitor performs continual checks on the outputs computed by the NMPC-based implementation, confirming that they are within the allowable limits of the downstream TRC controller, have a spectral content that is within appropriate bounds, etc. It switches to the PID-based implementation if a violation of any output requirements of the Tracking Controller is imminent. Any switch to the PID-based implementation must be timely enough to ensure that all safety requirements are satisfied at all times.

The high-confidence Tracking Control architecture is presented in Figure 42 for both Hover and Forward Flight modes. Depending on the flight mode, different frames of reference are used: the vehicle heading frame for hover mode and an inertial *path aligned frame* for forward flight mode. The vehicle heading frame is a local geodetic frame rotated to align with the heading of the aircraft. The path aligned frame is an orthonormal frame attached to 3D spatial path and is composed of a tangent vector and two normal vectors. The parallel transport frame is one representation of a path aligned frame. The basic structure is the same for both modes and employs a traditional gain-scheduled PID design.

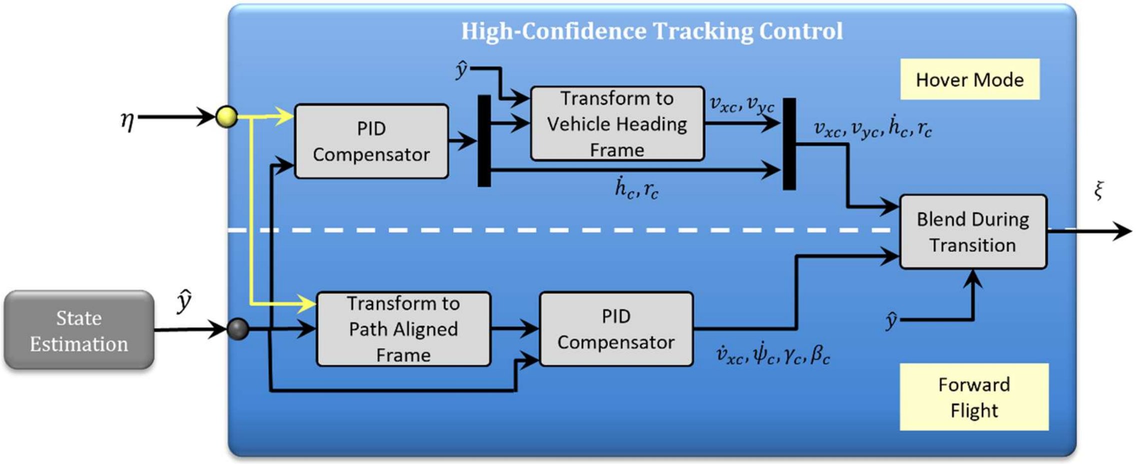

High-Confidence Tracking Control
Hover Mode
Forward Flight
η
$\hat{y}$
PID Compensator
Transform to Vehicle Heading Frame
v_{xc}, v_{yc}
$v_{xc}, v_{yc}, \dot{h}_c, r_c$
$\dot{h}_c, r_c$
Blend During Transition
ξ
State Estimation
Transform to Path Aligned Frame
PID Compensator
$\dot{v}_{xc}, \dot{\psi}_c, \gamma_c, \beta_c$

Figure 42. High-confidence Tracking Control Architecture

4.3 DRP as an RTA Application

The DRP Controller fills a role in the design that is somewhat different than that of the TRC and Tracking Controllers, which have the RTA monitor switching between advanced (low-confidence) and traditional (high-confidence) implementations. In contrast, the novelty of the DRP controller functionality is such that there are no “traditional” implementations to be leveraged in this design, save for the pilot who has ultimate authority to override DRP and choose an alternative collision avoidance maneuver. That is, the DRP Controller and DRP Monitor implement the RTA design pattern at this level of the control hierarchy, and they are not themselves the subject of RTA protection. As a result, the DRP design for the RTA-protected vehicle is identical to that of the baseline vehicle.

4.4 RTA Subsystem Interactions

As discussed in Section 1.2.3, the monitors in an RTA-protected architecture must continually check the state of the aircraft to see if it has crossed the boundary of the Type III Safety Region, and immediately switch to the high-confidence controller if so. That boundary accounts for the ability of the high-confidence controller to quickly drive the aircraft into a desired recovery region of the state space. As a result, the boundary depends in large part on the dynamic response of all systems that are downstream of the RTA-protected controller.

When multiple RTA-protected controllers are included in an aircraft design, the dynamic response that one RTA monitor should anticipate depends upon the reversionary state of downstream RTA-protected subsystems. This is because the downstream high-confidence and low-confidence controllers may have different performance properties, different input limitations, different output ranges, etc. This difference in Type III safety regions is illustrated in Figure 43. The left side of the figure shows a notional Type III safety region for a top-level RTA-protected controller assuming that all downstream RTA-protected controllers are using their low-confidence implementations (i.e., are providing the highest possible performance). The right side of the figure shows a notional Type III safety region assuming that all downstream RTA-protected controllers have switched to their high-confidence implementations (i.e., are collectively providing lower overall performance). The boundary of this safety region is pulled inward because the lower performance provided by downstream controllers will necessitate an increased recovery time for the top-level controller.

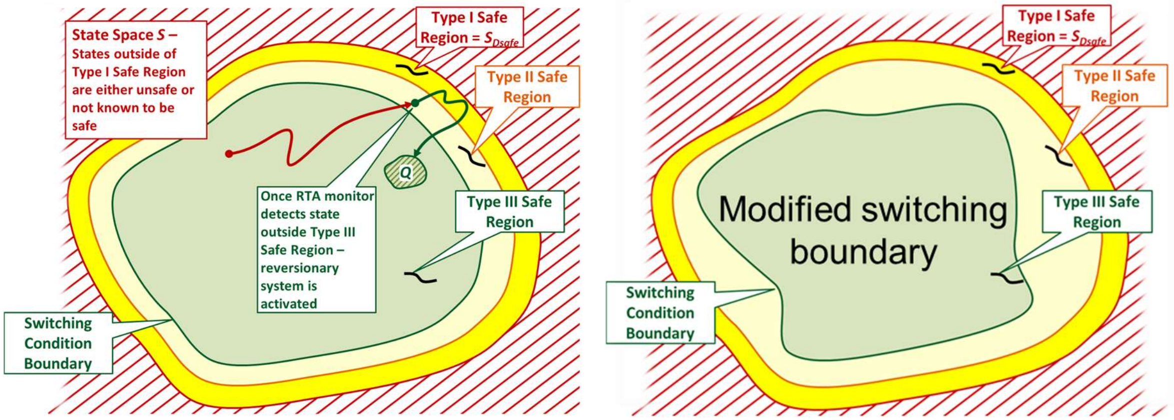

State Space S – States outside of Type I Safe Region are either unsafe or not known to be safe
Type I Safe Region = S_{Dsafe}
Type II Safe Region
Q
Once RTA monitor detects state outside Type III Safe Region – reversionary system is activated
Type III Safe Region
Switching Condition Boundary
Type I Safe Region = S_{Dsafe}
Type II Safe Region
Modified switching boundary
Type III Safe Region
Switching Condition Boundary

Figure 43. Differences in Type III Safety for Alternate Controller Implementations

In the eCRM-001 design, this difference in Type III boundaries is relevant for the:

- Tracking Controller – the output of the Tracking Controller is input to the TRC Controller when the aircraft is in hover mode. Performance differences between the high-confidence and low-confidence TRC Controller implementations will affect the high-confidence Tracking Controller's ability to quickly reduce any path following error.
- DRP Controller – the output of the DRP Controller is input to the Tracking Controller. Performance differences arising from the four different combinations of high- and low-confidence Tracking Controller and high- and low-confidence TRC Controller will affect the DRP Controller's ability to avoid collisions.

Rather than having the switching boundaries of these RTA monitors vary over time based on the state of downstream RTA-protected systems, the eCRM-001 design is such that each RTA monitor makes a worst-case assumption about the performance that downstream RTA-protected functions will provide. That is, each RTA monitor employs a constant Type III safety region that will ensure safe operation regardless of the state of any down-stream RTA-protected system. This is a conservative approach that may reduce the Type III safety region of the Tracking Controller and DRP controller, resulting in a larger safety margin than would be strictly required. However, this approach has the advantage of avoiding the architectural and algorithmic complexity required to synchronize RTA monitors across these different systems.

4.5 Updates to AFHA and SFHA

This section provides the updates on aircraft and system safety for introducing the changes to incorporate RTA protection to the baseline eCRM-001 aircraft using the processes established by ARP4754A and ARP4761. This is performed for the three (3) functions used for the task study. Figure 44 shows a depiction of the RTA protections for those functions.

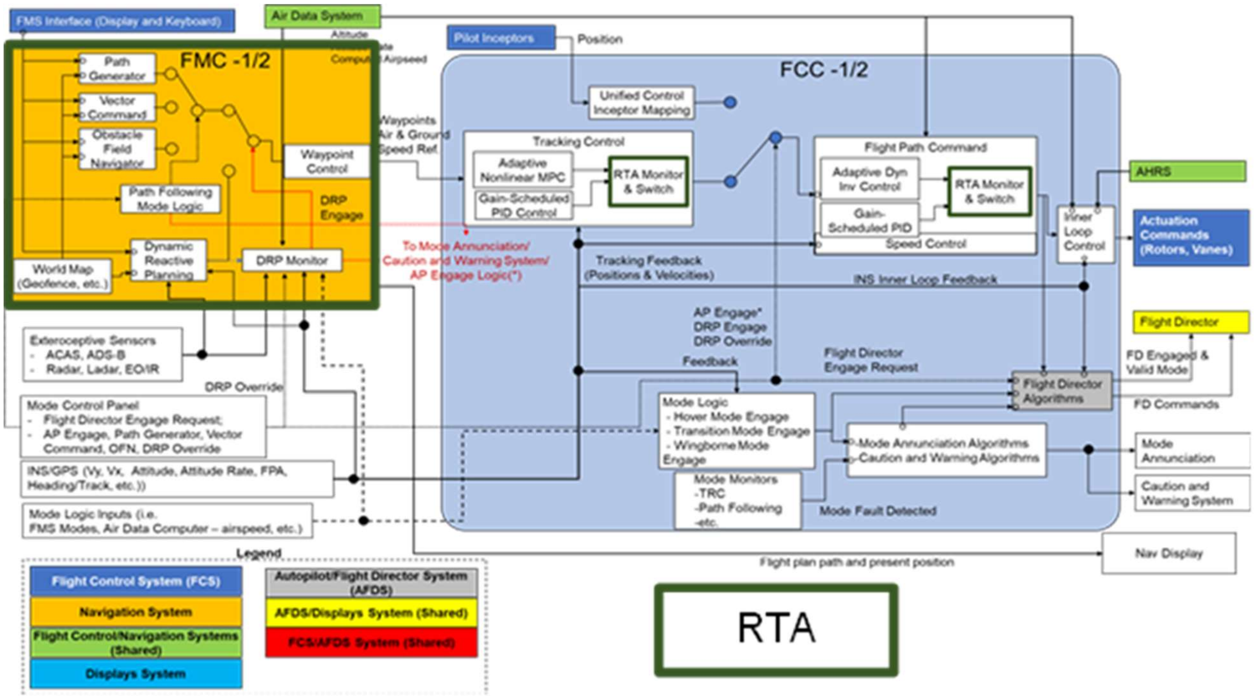


Figure 44. Control System Block Diagram Depicting RTA Components

4.5.1 FAA eVTOL Certification Assumptions

The FAA's Blueprint for Air Transformation describes the term Safety Continuum as [FAA 2017]:

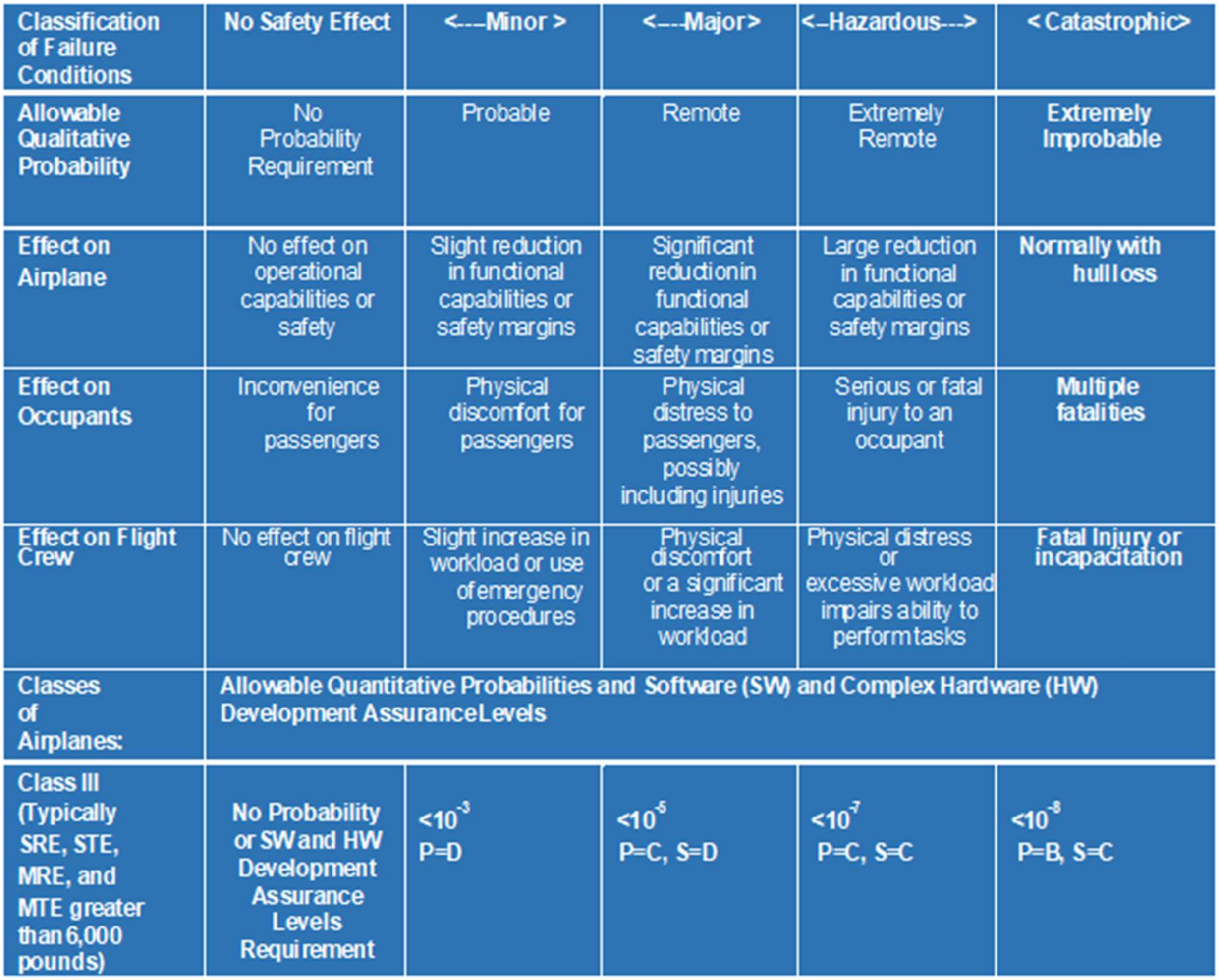
> *Safety Continuum – The level of safety established by regulation, guidance and oversight that change based on risk and societal expectations of safety. The safety continuum applies an appropriate level of safety from small UAS to large transport category aircraft. The differing level of safety balances the needs of the flying public, applicants and operators while facilitating both the advancement of safety and the encouragement of technological innovation*

Table 16 shows the FDAL assignments from AC 23.1309-1E.

Current (as of 2021) eVTOL certification programs are as follows:

- 14CFR 21.17(a) certification based on 14CFR 23, Amendment 23-64
- eCRM-001 as Class II aircraft
- Class III DAL requirements for FCS and propulsion systems

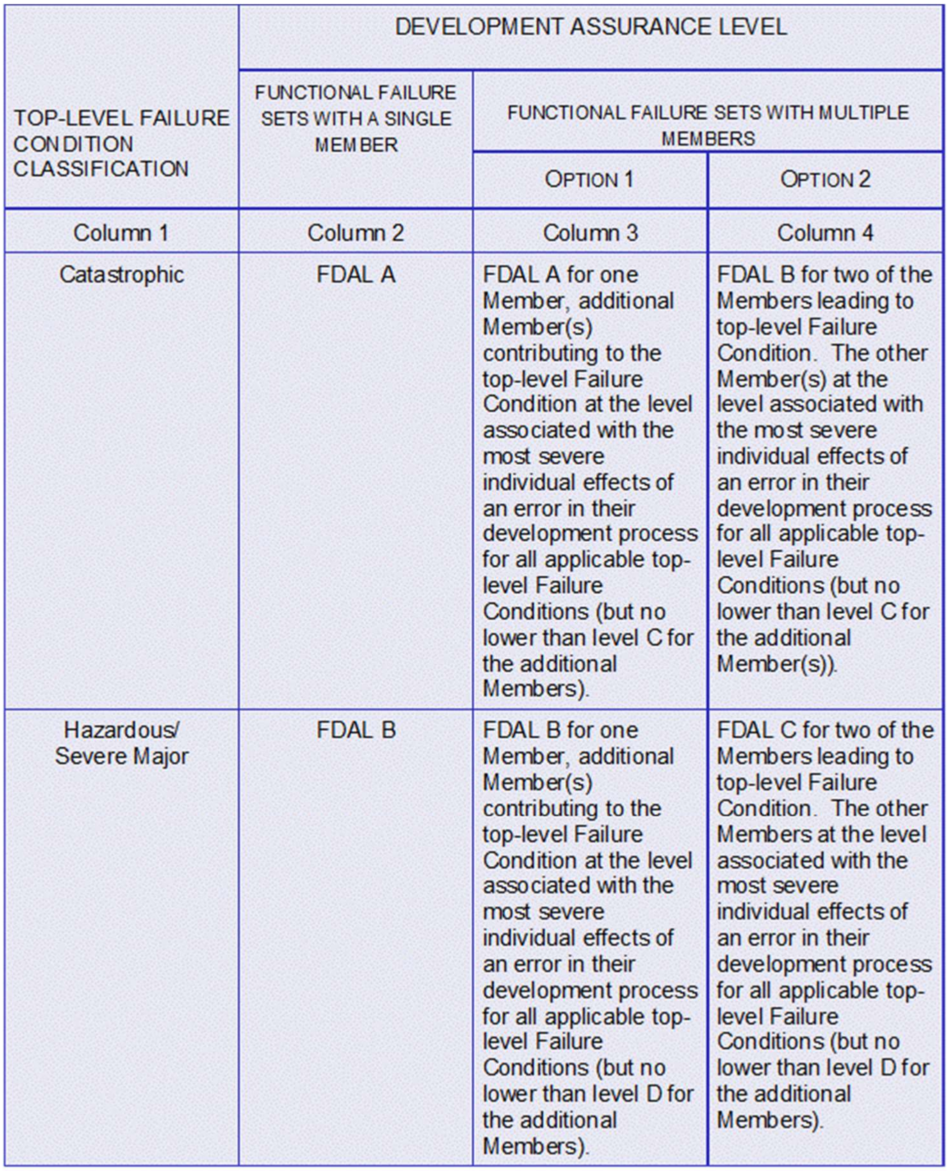
Table 16. FDAL Assignment from AC 23.1309-1E



Classification of Failure Conditions	No Safety Effect	<---Minor >	<---Major>	<--Hazardous--->	< Catastrophic>
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reductionin functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hullloss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to performtasks	Fatal Injury or incapacitation
Classes of Airplanes:	Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development AssuranceLevels				
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ P=D	$<10^{-5}$ P=C, S=D	$<10^{-7}$ P=C, S=C	$<10^{-8}$ P=B, S=C

The previous report, NASA/CR-2020-220586, Appendix A proposes a Very High Confidence (VHC) IDAL A and a Low Confidence (LC) IDAL D, to provide FDAL A. Currently it is understood that this topic is under discussion at FAA. Given current active eVTOL TC programs, HC IDAL B and LC IDAL D for this research project are assumed to meet ARP4754A Table 3 Option 1 (AC 20-174) for Hazardous/Severe Major Top-Level Failure Condition Classification (see Table 17). Note that ARP4754A is written specific to Part 25 aircraft certification – the Hazardous/Severe Major Part 25 DAL assignment is assumed equivalent to Part 23 Catastrophic DAL assignment.).

Table 17. ARP4754A DAL Assignment (cf. Part 25)



TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1	OPTION 2
Column 1	Column 2	Column 3	Column 4
Catastrophic	FDAL A	FDAL A for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Members).	FDAL B for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).

4.5.2 RTA and Software Considerations

For the purposes of this analysis, these certification assumptions justify the software to be developed to IDAL D for the low confidence part of the RTA design as long as the high confidence part along with the RTA monitor meet IDAL B for FDAL B assignments. Per DO-178C this relaxes required activities for IDAL D related to verifiability of requirements, accuracy and behavior of algorithms and test coverage. These are the kinds of activities that cause difficulty for adaptive control, machine learning, AI, numerical search, Monte Carlo techniques, etc.

In the PSSA, this would be documented as the justification for the RTA-based design. The resultant integrity and availability safety requirements would need to be shown as met in the

PSSA, as would an analysis that errors leading to unacceptable failure conditions have been removed. RTA protection should make it much easier to show this for these kinds of algorithms. Bear in mind, that to reduce FDALs/IDALs from their top level FDAL it must be shown that the corresponding FDAL/IDAL functional failure sets (FFS) are independent (no common mode faults exist). Functions, subfunctions and Items not independent must be developed to the top-level DAL.

PSSA would need to consider the inputs to the high confidence (HC) and low confidence (LC) control laws, as well as the (high confidence) RTA monitor and switch, including the software/design failures that may be in control laws and RTA monitor. Top level fault tree may consider failures such as: LC control law software/design failure AND (RTA monitor fails to detect OR fails to switch). RTA failure to detect or failure to switch is treated as separate software failures. This would have two FFS.

- Set 1 – LC control law software/design failure, RTA monitor failure to detect
- Set 2 – LC control law software/design failure, RTA monitor fails to switch

The RTA failure to detect and failure to switch may alternately be treated as just a single RTA monitor failure, as opposed to the two failure sets above. The fault tree showing these failures would simply show the relationship of how these failures could occur, combine, and cause a hazard, but without assigning a particular failure rate to any of these since software/design related failure rate cannot be known.

Relevant key definitions are (see ARP4761 for more details):

- Independence – A concept that minimizes the likelihood of common mode errors between aircraft/system functions or items. Separation of responsibilities that assures the accomplishment of objective evaluation, e.g., validation activities not performed solely by the developer of the requirement of a system or item.
- Functional Failure Set – A single member or multiple members (systems or items) that lead to a top-level failure condition. The top-level failure condition would be the hazard and below that is the particular set of failures from the member(s) that lead to that hazard.

IDAL assignments consider functional independence, item development independence, and number of members.

4.5.3 Notional PSSA Process

The PSSA is part of the ARP4754A/4761 safety process and pertinent aspects of it are described in this section for purposes of understanding its scope and use. The purpose of the preliminary assessment is to evaluate the proposed system/architecture such that safety requirements can be identified/defined and allocated at the system and item level to meet defined safety levels/requirements. This section identifies, at a high level, the basic process. Process details can be found in ARP 4754A/4761. Salient points are as follows:

- Safety levels are defined in the FHA/SFHA as hazard conditions and classifications of the various system functions
- PSSA is used to establish safety requirements flowed to both system and item safety requirements

- Safety requirements typically include independence requirements, probabilistic availability/integrity requirements, “no single fault” criteria, operational/maintenance limitations (flowed down to OEM maintenance manuals/flight manuals), development assurance levels for hardware and software components (DO-178 for S/W, DO-254 for H/W) and fault detection (monitoring)

Inputs to the PSSA process are:

- Aircraft and System Functional Hazard Analysis (AFHA/SFHA)
- Preliminary system design and architecture
- Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), and Common Mode Analysis (CMA)

Outputs from the PSSA process are:

- System and Item Safety Requirements
- Item Design Assurance Levels for hardware and software
- Additional Failure Conditions, Effects, and Classifications

The PSSA is a “living document” and is updated regularly as the system development/design progresses. Updates may impose new or modified safety requirements and ultimately serves as the basis for the System Safety Assessment (SSA) which is submitted to the certification authorities as validation/evidence that system safety requirements have been met.

4.5.3.1 PSSA Analysis Tools

The three primary tools are the FTA, FMEA, and CMA. They comprise a systematic examination of the proposed architecture/design to evaluate how failures of the proposed architecture/design could cause failures as defined in the AFHA/SFHA. The analysis is not necessarily done in sequence but can be in parallel. Additional analysis includes particular risk analysis/zonal analysis. Particular Risk looks at how events outside of the system errors can lead to hazards, such as rotor burst causing simultaneous damage to redundant LRU’s. Zonal analysis examines the effect of equipment installation within established zones of the aircraft to such effects as compartment overheating, mutual interference between co-located LRUs, etc.

4.5.3.1.1 Fault Tree Analysis

FTA is a quantitative and/or qualitative analysis showing how individual failures and failure combinations can combine to create a system or aircraft level hazard. Quantitative analysis is used to show probability of occurrence of an event or failure condition. Qualitative analysis may be used to show independence when failure rates are not established, such as when software or design failures are considered. The preliminary FTA may make assumptions about item independence, item (or LRU) failure rates, exposure times to item/LRU failure, etc. All assumptions must be validated early in the design. The FTA starts with the top-level hazard defined in the FHAs and works its way down to “Basic Event” failures, which comprise the individual items, piece parts, or LRUs as appropriate. It is expressed as a probability of the hazard occurring on a “per flight hour” basis.

4.5.3.1.2 Common Mode Analysis (CMA)

The CMA is used to validate independence claims used to support other analysis, such as the FTA. Part of the “Common Cause Analysis” includes the “Particular Risk” and “Zonal” analysis. Each independence claim/requirement identified in other analysis and design documentation is subject to a qualitative review to establish that the claim is valid. Examples of common mode failure include:

- Common cause failure – such as independence between two LRUs (such as INS) being violated due to being powered from the same power bus
- Common cause error – such as a design error in a redundant system using identical software

4.5.3.1.3 Failure Modes and Effects Analysis

The FMEA is a bottom-up analysis of system failure modes. The FMEA can be performed at the piece part level, function/subfunction level, and LRU level. It identifies failure effects from single failures and may be used to support other analysis such as FTA.

4.5.4 Approach

The approach used to analyze the RTA protected eCRM-001 aircraft is to first review the baseline AFHA worksheets for the baseline aircraft while considering the RTA protections proposed. The assumptions documented in the AFHA for the baseline eCRM-001 aircraft are also reviewed for the RTA protected aircraft. The next step is to validate the SFHA for the system design implementation of the RTA protected eCRM-001 aircraft against the baseline aircraft system design, including any applicable effects of the RTA monitor. The assumptions documented in the SFHA worksheets are also reviewed. The final step is to expand the evaluation to include the PSSA, as the RTA protection is most likely to be assessed at this level of the ARP safety process.

4.5.5 Update for “Provide Translation Rate Command Horizontal Control Mode”

4.5.5.1 RTA Application

The RTA-protected aircraft and the Baseline aircraft are the same for this function. The function design assumes fixed nacelles in hover operating mode. Figure 45 illustrates application of the RTA pattern is to the “Flight Path Command” block in the FCC. The Flight Path Command block accepts translational inertial velocity commands from either the pilot or automation and outputs pitch and roll attitude commands to the inner loop control law. Within the Flight Path Command block there is a low confidence (LC) controller, a high confidence (HC) controller and an RTA monitor and switch. The low confidence control law (adaptive dynamic inversion control) is more complex. The high confidence control law (gain scheduled PID) is less complex.

The required reference signals for both the LC and HC control laws are desired longitudinal (Vx) and lateral (Vy) inertial speeds. The LC control law would additionally need angular rates (p, q, r).

Both designs would also require limits on the attitude commands and rates of change for these commands.

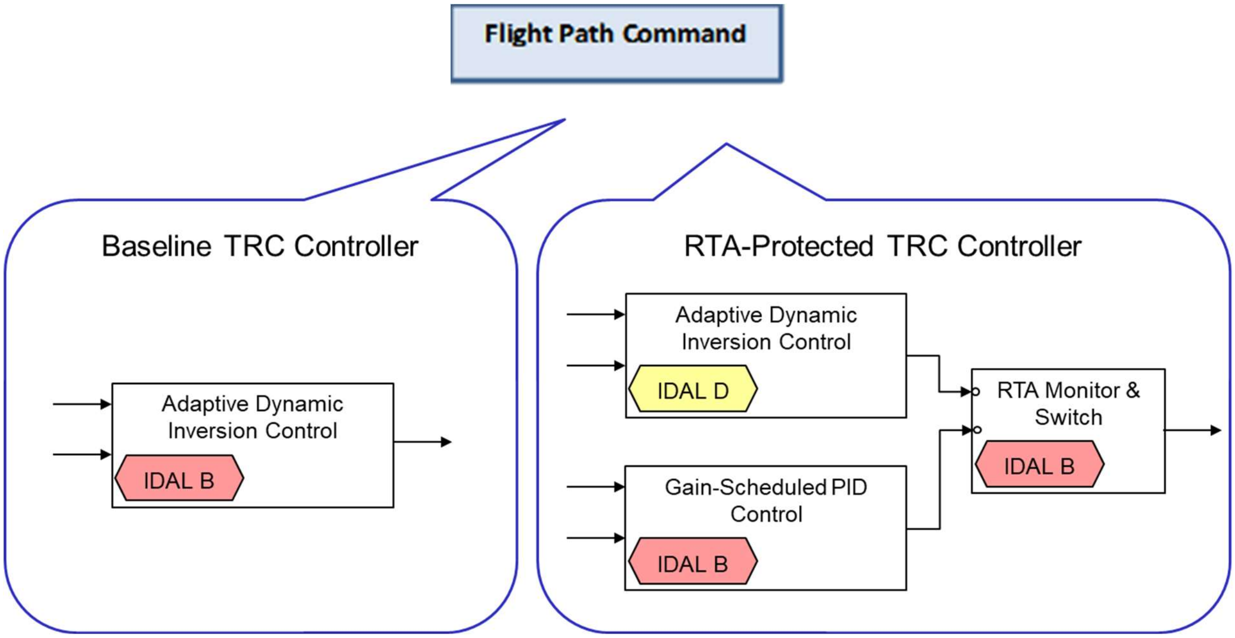

Flight Path Command
Baseline TRC Controller
Adaptive Dynamic Inversion Control
IDAL B
RTA-Protected TRC Controller
Adaptive Dynamic Inversion Control
IDAL D
Gain-Scheduled PID Control
IDAL B
RTA Monitor & Switch
IDAL B

Figure 45. Baseline and RTA-Protected TRC Controllers

4.5.5.2 RTA-Protected Aircraft Update

The function is determined to be FDAL B due to the severity of the hazard (from the SFHA). This FDAL can be implemented by having the “Adaptive Dynamic Inversion Control” shown above in the baseline TRC controller developed to IDAL B software standards, or by having a high confidence controller developed to IDAL B software standards (Gain scheduled PID control in the above figure) with an RTA monitor and switch also developed to IDAL B, which allows the “Adaptive Dynamic Inversion Control” to be developed to IDAL D software standards.

The AFHA and SFHA were validated as having no impact due to the RTA implementation noted above. The primary impact would be in the PSSA, as the implementation would need to show how it meets the FDAL B assignment.

4.5.6 Update for “Provide Path Following Control Mode”

4.5.6.1 RTA Application

The RTA-protected aircraft and the Baseline aircraft are the same for this function. Figure 46 illustrates application of the RTA pattern to the “Tracking Control” block in the FCC. The Tracking Control block accepts flight path commands from the FMS and outputs translational velocities to the Flight Path Command block, also in the FCC. Within the Tracking Control block there is a low confidence (LC) controller, a high confidence (HC) controller and an RTA monitor and switch. The low confidence control law (adaptive nonlinear model predictive control) is more complex. The high confidence control law (gain scheduled PID) is less complex.

The required signals for both the LC and HC control laws are envisioned as the same.

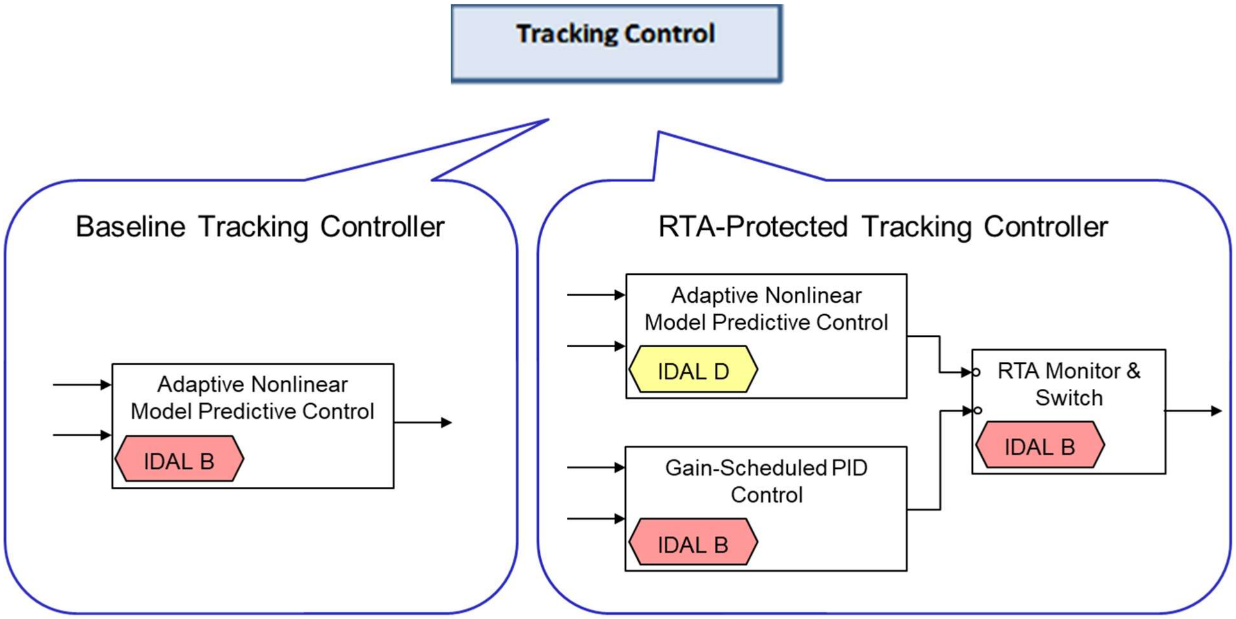

Tracking Control
Baseline Tracking Controller
Adaptive Nonlinear Model Predictive Control
IDAL B
RTA-Protected Tracking Controller
Adaptive Nonlinear Model Predictive Control
IDAL D
RTA Monitor & Switch
IDAL B
Gain-Scheduled PID Control
IDAL B

Figure 46. Baseline and RTA-Protected Tracking Controllers

4.5.6.2 RTA-Protected Aircraft Update

The function is determined to be FDAL B due to the severity of the hazard (from the SFHA). This FDAL can be implemented by having the “Adaptive Nonlinear Model Predictive Control” shown above in the baseline Tracking Controller developed to IDAL B software standards, or by having a high confidence controller developed to IDAL B software standards (Gain scheduled PID control in the figure) with an RTA monitor and switch also developed to IDAL B, which allows the “Adaptive Nonlinear Model Predictive Control” to be developed to IDAL D software standards.

The AFHA and SFHA were validated as having no impact due to the RTA implementation noted above. The primary impact would be in the PSSA, as the implementation would need to show how it meets the FDAL B assignment.

4.5.7 Update for “Provide Airborne Vehicle Collision Avoidance”

4.5.7.1 RTA Application

Unlike the RTA for Tracking Controller and TRC, which has the RTA monitor switching the Low Confidence and High Confidence controllers, the DRP and the DRP Monitor itself act as an RTA mechanism. This is since it monitors functionality of other path generation and tracking systems, monitors for collisions / loss of well-clear when in piloted mode and interacts with Autopilot Engage logic.

4.5.7.2 RTA-Protected Aircraft Update

In this context, the RTA-Protected aircraft and the baseline aircraft are the same, as is the system design, and no further analysis is required for the difference between the two.

4.5.8 Summary

RTA protection for these three subfunctions are fully implemented in the software and do not have any observable unique sensor inputs or outputs, thus nothing different from the baseline aircraft. The difference is in the software implementation of the particular control laws in tracking control and flight path command blocks, allowing for IDAL D for the more complex control laws. The RTA protection in the PSSA will need to show how these overall blocks meet IDAL B and how errors leading to unacceptable failure conditions have been removed. Although the RTA implementation will require some additional analysis, as there will be two sets of control laws and a monitor, any additional analysis at this stage will be greatly offset by the work saved related to verifiability of requirements, accuracy and behavior of algorithms and test coverage to implement through IDAL D.

4.6 Updates to STPA

This study identified what needs to be adapted or updated in order to conduct STPA on RTA-protected aircraft functions as well as how such an STPA approach to RTA-protected aircraft can support existing aircraft certification processes (the final recommendations of which are included in Section 5.8). The first insight and recommendation involves the fact that STPA can proceed in a typical fashion for RTA-protected functions and that nothing “new” needs to be invented in terms of STPA methodology to support hazard analyses for such functions. Indeed, one potential advantage of STPA is that it is often employed to analyze interactions between and among functions – much of the analysis surrounding the TRC function and the pilot role attempts to do just this (e.g. in Section 3.9 as well as loss scenarios start in Table 41-Table 43 and Table 47 in Appendix E).

Obviously as the complexity of a system increases, so will the complexity of the associated analyses. STPA is no different, but it is encouraging that STPA is inherently grounded in the notion of control and requires one to think about and model interactions between components in a way that is amenable to general notions from control theory. At the risk of abusing concepts from complexity theory, we assert that the complexity of conducting STPA scales “linearly” with the addition of RTA protections into aircraft systems. There is already a fairly rich history of STPA analyses including controllers operating in parallel and/or involve mode-switching [Levson 2018]. The main question we sought to answer was *how to model these systems* in terms of the concept of the STPA control structure, with the assertion that an appropriate modeling abstraction gives the necessary structure to methodically identify unsafe control actions and scenarios along the various control loops that can lead to unsafe control.

We explored three different modeling abstractions, focusing on the TRC function as an exemplar. The first idea is to augment the existing STPA control loop (e.g., the abstraction depicted in Figure 38) with information associated RTA protections and then proceed with the standard loss scenario generation. Figure 47 depicts such a control loop, with differences between baseline function and RTA-protected function highlighted in red text. The idea here is to include all of the architectural details of the RTA concept into the STPA notion of “Algorithm / Procedure,” update the Process Model to include any information required to run more sophisticated controllers, and additional details along the control loop needed to implement RTA. For the TRC function this includes the additional control law of the adaptive model predictive controller, the RTA monitor necessary to switch modes between this predictive controller and a traditional controller, and a delineation of what is meant by “flight mode” as RTA protection of this function results in multiple types of flight modes (in this case, whether the aircraft is in hover or wingborne flight, and whether the aircraft is being controlled by an adaptive MPC law or a gain-scheduled law).

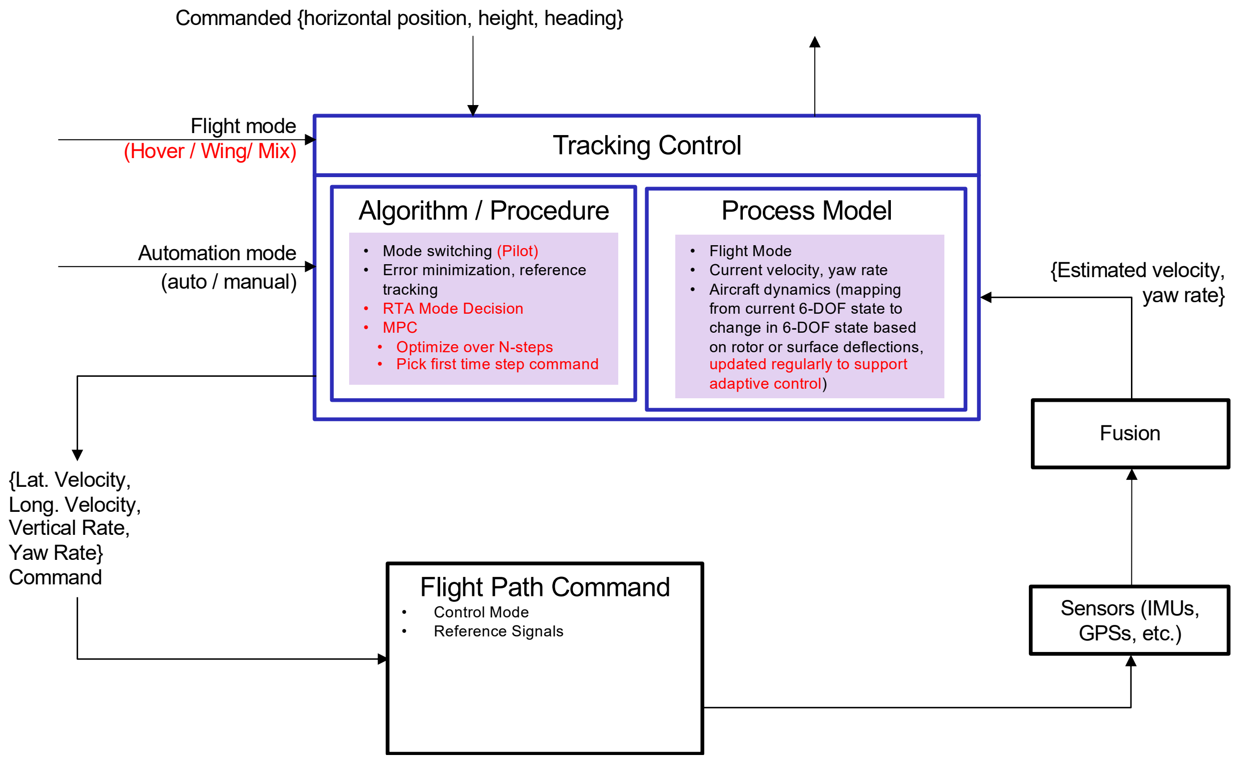

Commanded {horizontal position, height, heading}
Flight mode
(Hover / Wing/ Mix)
Tracking Control
Automation mode
(auto / manual)
Algorithm / Procedure
Mode switching (Pilot)
Error minimization, reference tracking
RTA Mode Decision
MPC
Optimize over N-steps
Pick first time step command
Process Model
Flight Mode
Current velocity, yaw rate
Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections, updated regularly to support adaptive control)
{Estimated velocity, yaw rate}
Fusion
{Lat. Velocity, Long. Velocity, Vertical Rate, Yaw Rate} Command
Flight Path Command
Control Mode
Reference Signals
Sensors (IMUs, GPSs, etc.)

Figure 47. Candidate #1, Updated Feedback Loop Model for STPA Causal Analysis of RTA-Protected Tracking Controller

The issue with this approach is that it makes it opaque and potentially challenging for the analyst to keep track of and reason about the behaviors and possible safety issues for such a system. While all the necessary information *could* be captured in this way, it does not lend itself to thorough, transparent, repeatable analyses. We therefore advocate for explicitly pulling apart these functions and adhering to something conceptually equivalent to Figure 38, which is similar in that there are multiple controllers of the same function possibly working in parallel.

We explored two alternatives for modeling the interacting nature of RTA-protected functions in a more explicit way than in Figure 47. In either case, one can proceed with STPA in the usual way, first analyzing each parallel control loop individually, identifying unsafe control actions and causal scenarios as if they are the only part of the control loop – these results would look similar to any of the tables in Appendix E. One thing to note in the following diagrams, Figure 48 and Figure 49, is that not only do the baseline controller and the more sophisticated model predictive controller have different control algorithms, but in the context of STPA, these two controllers also have different “Process Models,” which will result in potentially different causal factors.

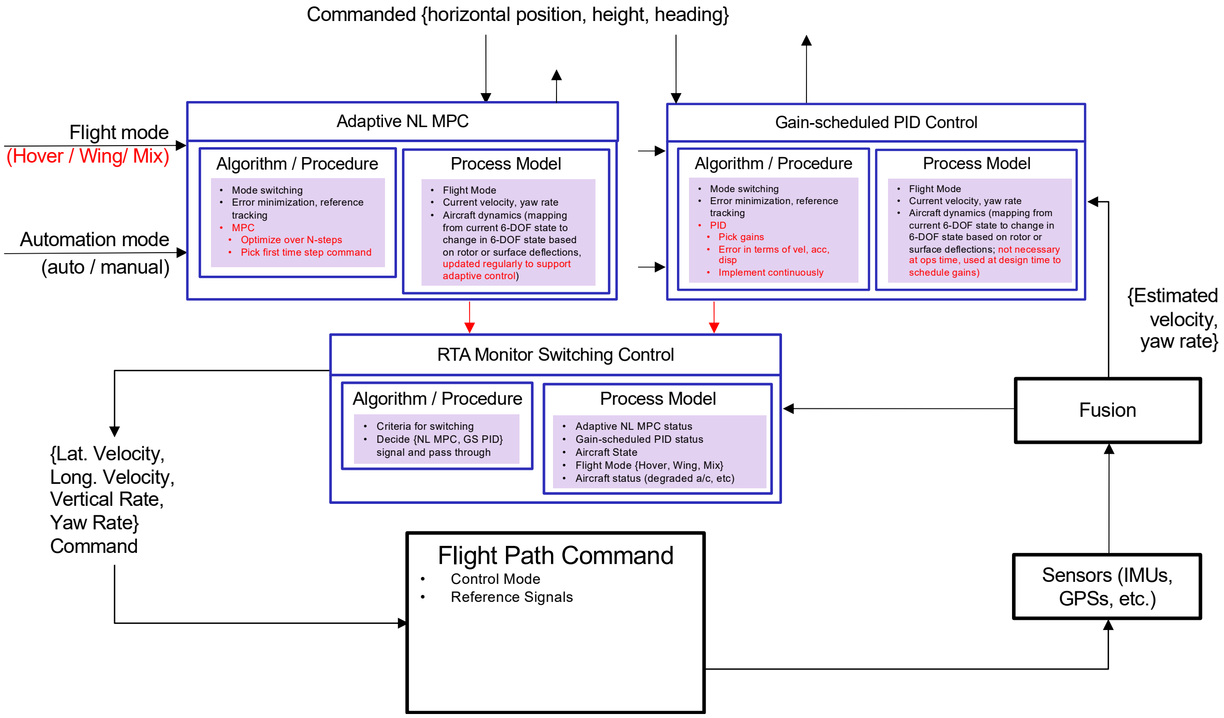

Commanded {horizontal position, height, heading}
Flight mode
(Hover / Wing/ Mix)
Automation mode
(auto / manual)
Adaptive NL MPC
Algorithm / Procedure
Mode switching
Error minimization, reference tracking
MPC
Optimize over N-steps
Pick first time step command
Process Model
Flight Mode
Current velocity, yaw rate
Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections, updated regularly to support adaptive control)
Gain-scheduled PID Control
Algorithm / Procedure
Mode switching
Error minimization, reference tracking
PID
Pick gains
Error in terms of vel, acc, disp
Implement continuously
Process Model
Flight Mode
Current velocity, yaw rate
Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections; not necessary at ops time, used at design time to schedule gains)
{Estimated velocity, yaw rate}
RTA Monitor Switching Control
Algorithm / Procedure
Criteria for switching
Decide {NL MPC, GS PID} signal and pass through
Process Model
Adaptive NL MPC status
Gain-scheduled PID status
Aircraft State
Flight Mode {Hover, Wing, Mix}
Aircraft status (degraded a/c, etc)
Fusion
{Lat. Velocity, Long. Velocity, Vertical Rate, Yaw Rate} Command
Flight Path Command
Control Mode
Reference Signals
Sensors (IMUs, GPSs, etc.)

Figure 48. Candidate #2, Updated Feedback Loop Model for STPA Causal Analysis of RTA-Protected Tracking Controller

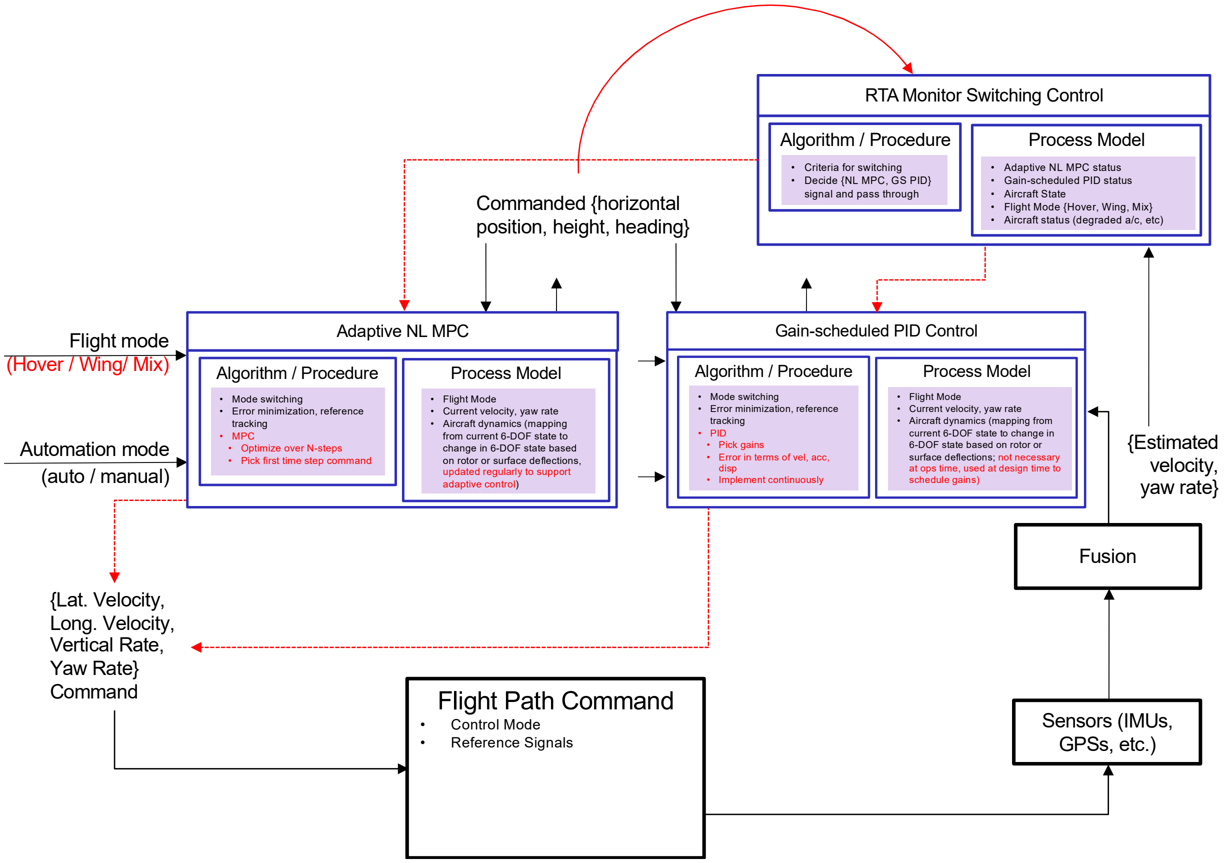

RTA Monitor Switching Control
Algorithm / Procedure
Criteria for switching
Decide {NL MPC, GS PID} signal and pass through
Process Model
Adaptive NL MPC status
Gain-scheduled PID status
Aircraft State
Flight Mode {Hover, Wing, Mix}
Aircraft status (degraded a/c, etc)
Commanded {horizontal position, height, heading}
Flight mode
(Hover / Wing/ Mix)
Automation mode
(auto / manual)
Adaptive NL MPC
Algorithm / Procedure
Mode switching
Error minimization, reference tracking
MPC
Optimize over N-steps
Pick first time step command
Process Model
Flight Mode
Current velocity, yaw rate
Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections, updated regularly to support adaptive control)
Gain-scheduled PID Control
Algorithm / Procedure
Mode switching
Error minimization, reference tracking
PID
Pick gains
Error in terms of vel, acc, disp
Implement continuously
Process Model
Flight Mode
Current velocity, yaw rate
Aircraft dynamics (mapping from current 6-DOF state to change in 6-DOF state based on rotor or surface deflections; not necessary at ops time, used at design time to schedule gains)
{Estimated velocity, yaw rate}
Fusion
{Lat. Velocity, Long. Velocity, Vertical Rate, Yaw Rate} Command
Flight Path Command
Control Mode
Reference Signals
Sensors (IMUs, GPSs, etc.)

Figure 49. Candidate #3, Updated Feedback Loop Model for STPA Causal Analysis of RTA-Protected Tracking Controller

Perhaps more interesting is the modeling abstraction used for the RTA monitor, which is the primary difference between Figure 48 and Figure 49. One can think of RTA monitor and switching function as either a “pass-through” or a “controller.” In the former concept, the RTA monitor acts as a filter and simply lets one of the two signals pass through to the next layer of the control stack. In the latter concept, the RTA monitor manages the two controllers. Based on Figure 49, one could image designs where the RTA monitor preconditions the reference input before passing to and selecting the appropriate controller. One could even imagine designs where the monitor literally turns one controller off while the other operates.

In addition, placing the RTA monitor “above” the high-confidence and low-confidence controllers in the control hierarchy engenders several other questions. Does this function need to have access to other aircraft information, or does it only need access to information about the envelope of the IDAL D controller? For example, does the monitor itself need current aircraft inertial states, health states of components up and downstream in the control hierarchy? Does the monitor need the reference signal that the two controllers are working towards achieving? Note that we are not advocating for these ideas and more detail on RTA design considerations is already provided in Section 4.4 and elsewhere. Rather, the point we are trying to make here is that STPA naturally helps the analyst start working through some of these questions before the detailed design has even begun. That is, the modeling step of STPA elicits several interesting questions about architecture and design, supporting a conclusion that STPA potentially supports assurance activities like PSSA for these complex control functions. Section 5.8 provides more detail about this conclusion.

5.0 Summary, Analysis, and Recommendations

5.1 Certification Basis Alternatives

5.1.1 Certification Basis and MOC

The certification authority approves an aircraft manufacturer's design (referred to as the applicant's type design) using the Type Certification (TC) process. In the United States, the certification authority is the FAA, and the regulations for aircraft certification are provided in the Code of Federal Regulations Title 14 (14CFR) Chapter 1, Department of Transportation, Subchapter C, Aircraft, as follows:

- Part 21 Certification Procedures for Products and Articles
- Part 23 Airworthiness Standards: Normal Category Airplanes (19 or less passengers)
- Part 27 Airworthiness Standards: Normal Category Rotorcraft (9 or less seats)
- Part 33 Airworthiness Standards: Aircraft Engines
- Part 35 Airworthiness Standards: Propellers

The FAA has worked with industry to produce The FAA and Industry Guide to Product Certification [FAA CPI 2017]. This guideline is applicable to all TC applicants and certification projects and describes the TC process.

The definition of the aircraft certification basis (the applicable rules), and the associated MOC, or how to show compliance with the rules, is a negotiation process between the certification authority and the applicant. For the eCRM-001, the subject in this case study, the certification authority is the FAA, and the applicant is the eCRM-001 aircraft manufacturer.

5.1.2 Certification Authority and Applicant approaches for eVTOL aircraft

Currently there are differing authority approaches for the type certification of eVTOL aircraft between the FAA and EASA. Also, different industry standards (ASTM, SAE). In common with the approach currently being taken by many of the eVTOL aircraft manufacturers in the US, who have either applied for a type certificate (TC), or who are in the process of applying for a TC, for this task study the assumption has been made that the eCRM-001 will be certificated to 14CFR 21.17(a)(1). Additionally, it has been assumed the certification basis will be 14CFR Part 23 latest amendment (amendment 23-64), with additional regulations from 14CFR Parts 27, 33 and 35, as applicable.

In accordance with the FAA guidance contained in advisory circular AC20-174, Development of Civil Aircraft and Systems, SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, has been used as the MOC for 14CFR 23.2510, Equipment, systems and operation.

5.1.3 The Safety Continuum, and FAA Reorganization

Part 23 Amendment 23-64 resulted directly from FAA recognition of the safety continuum. The purpose of the Part 23 rewrite was to replace the prescriptive design requirements in Amendment 23-63 with performance-based airworthiness standards.

The FAA reorganization introduced the role of the FAA Policy and Innovation department in the TC process. The applicant is now able to begin the certification basis and MOC negotiation process prior to making an application for aircraft TC.

5.2 RTA to Enable Advanced UAM Control

This project has highlighted the notion that DAL D is something of a sweet spot for low-confidence controllers. This observation that was initially made in the previous BAART task order [Peterson 2020], based on a count of the number of required development activities involved with different DAL assignments. In this project, the team investigated more closely the specific DO-178C [RTCA/DO-178C] development activities that can be eliminated from the process and their relevance to the kinds of advanced controllers considered for the eCRM-001 design. These activities relate to:

- Verifiability of requirements (e.g., Activities 6.3.1.d and 6.3.2.d in DO-178C)
- Accuracy and behavior of algorithms (e.g., Activities 6.3.1.g and 6.3.2.g in DO-178C)
- Test coverage (e.g., Activity 6.4.4.b in DO-178C)

Among the many activities described in DO-178C, it is these activities that can be the most challenging for the kinds of advanced control techniques that may be desirable in novel UAM designs, such as adaptive control, machine-learning, artificial intelligence, numerical search, and Monte Carlo based algorithms. Moreover, the standard requires that development teams demonstrate that errors leading to unacceptable failure conditions have been removed from the software. The RTA architecture, which cordons off the low-confidence function, makes it much easier to show this for these kinds of algorithms.

5.3 RTA to Support Incremental UAM Control Revisions

It is expected that the UAM community will not have the same degree of institutionalized knowledge regarding the target operating environment that has existed for decades among more traditional aircraft operations. There may be a much wider variety of aircraft configurations, and developers of these novel designs will not have nearly the same level of experience with their vehicles as do those of more traditional aircraft. Moreover, the urban turbulence environment is generally much more complex than that above the atmospheric boundary layer or above rural areas, in which most traditional aircraft spend most of their flight time. Turbulence models and corresponding simulation capabilities for this environment are not as widely available. Finally, operations within the urban environment may evolve rapidly in the initial years as the market develops and the various stakeholders must adapt to accommodate each other.

As a result, it is likely that companies may seek to roll out multiple control system updates to optimize aircraft performance, handling qualities, and piloting performance as the community gains experience in this environment. Even if it is not needed to facilitate certification of the original control system software, the RTA architecture may be an extremely valuable design choice to facilitate these future upgrades. New software versions could be developed to DAL D, then deployed to the fleet as low-confidence components, with protection provided by an RTA monitor and corresponding high-confidence variant that was developed to DAL B during the initial vehicle design. The previous BAART task order [Peterson 2020] demonstrated a tremendous savings in development effort for updates performed in this manner.

5.4 Multiple Recovery Controllers

The ASTM standard F-3269-17 [ASTM F3269] explicitly considers the possible use of multiple high-confidence controllers within an RTA-protected component that might become active when the RTA monitor triggers a switch from the low-confidence algorithm, depending on the aircraft state. (These are termed “recovery control functions” in that document.) This concept is also described at length in [Schierman 2015], which provides quantitative examples involving reversionary control of aircraft with morphing wing structures. In that example, the RTA monitor selects a high-confidence function based on the current wing configuration.

This current project has not explicitly addressed the potential use of multiple high-confidence controllers in this manner; however, the development herein does not preclude such designs for the eCRM-001 aircraft. In some sense, the distinction between an architecture with multiple high-confidence controllers and an architecture with a single complex high-confidence controller is semantic. In this application, the distinction likely would not be relevant until several more design iterations have taken place, and the control systems have more detail developed.

For example, the eCRM-001 design explored in this work contains a high-confidence TRC controller that employs linear gain scheduled control to accommodate the non-linear aircraft dynamics. In practice, this would involve the construction of a table of control parameters, each row of which would be tuned to a particular operating point. This effectively creates a large number of individual controllers, switched in and out by the selection of a row from the table. Early in the design, it is very common to consider this as a single non-linear controller, with details worked out at a much later time, during the implementation activities governed by DO-178C.

As a contrasting example, the eCRM-001 design includes a DRP controller that provides high-level control functions in collision avoidance scenarios. In practice, this controller would almost certainly employ multiple discrete control components that would be switched in and out during operation, depending upon the current flight mode of the aircraft. For example, collision avoidance in hover mode will necessarily involve very different strategies, and likely comply with different set of regulations, than collision avoidance in forward flight mode. These details will likely be addressed at an earlier phase of the development cycle, prior to the software development activities of DO-178C.

5.5 Temporary vs. Terminal Recovery Control

The ASTM standard F-3269-17 [ASTM F3269] makes a distinction between high-confidence control functions that are intended for use on a temporary basis, meaning that the RTA monitor will switch back to the low-confidence controller when conditions allow, and those that are intended for terminal use, meaning that they remain active until the conclusion of the flight. Examples of this concept are explored in detail in [Schierman 2015], for situations in which it is desirable to leverage the high-performance offered by a low-confidence function to the greatest possible extent.

For the eCRM-001 design considered in the present effort, the DRP controller is intended to be employed on a temporary basis, with control reverting to the pilot or autopilot once the threat of a collision has been avoided. On the other hand, it is anticipated that the high-confidence implementations of TRC and Tracking Control functionality would be considered terminal functions. For the UAM application, the improved performance, handling qualities, and passenger comfort provided by the low-confidence implementations are secondary considerations to the safety of passengers and crew. Should the RTA monitor effect a switch from the low- to high-confidence implementations, the ability of the low-confidence controller to safely control the aircraft would be in question. Such an occurrence would likely entail some maintenance process after landing to document the event, capture the conditions that caused the switch, perform some checkout operations, etc.

This perspective may be quite different in a military setting. For situations in which the aircraft may be under direct assault by a hostile adversary, the performance and/or robustness afforded by a low-confidence control algorithm may be fundamental to the crew's safety. In such a case, it may be preferable for the RTA monitor to switch back to the low-confidence controller as quickly as possible.

5.6 RTA Subsystem Interactions

In an RTA-protected architecture, the RTA monitor ensures that the aircraft state remains within a defined safety region by switching to a high-confidence implementation if the state crosses the corresponding switching boundary (i.e., the boundary of Type III safety region). The exact placement of this boundary depends, in part, on the combined dynamics of the aircraft and any down-stream controllers. If those downstream controllers also employ RTA protection, those dynamics could change depending on whether the downstream controllers currently employ their low-confidence or high-confidence variants. Each RTA monitor must in some way account for those differences.

In [Schierman 2015], the authors develop a contract-based communication scheme between the various RTA monitors in a hierarchical control design to dynamically negotiate the safety boundaries each will enforce. They introduce a Global RTA Manager component to coordinate these negotiations, as shown in Figure 50. While this negotiation and the architecture to support it can involve a significant amount of complexity, it can maximize the use of high-performance (low-confidence) controllers that are active at any point in time within that control hierarchy. As previously noted, in a military setting involving hostile actors, maximizing the use of these high-performance controllers may be critical for ensuring crew safety.

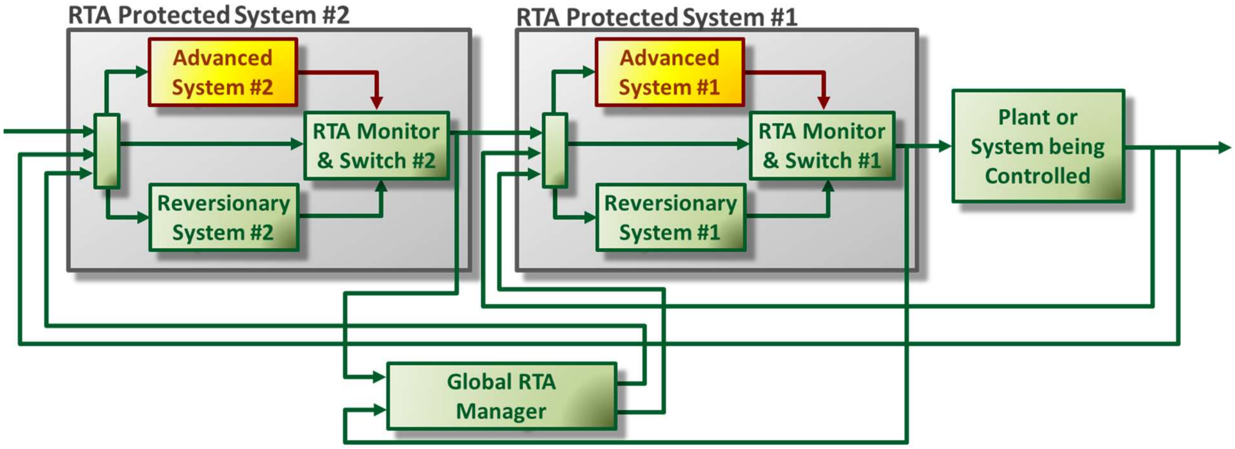


Figure 50. Coordination of RTA Protected Systems (from [Schierman 2015])

In a civilian UAM setting, however, the complexity associated with such a design is less desirable. An alternative and much simpler design would have each RTA monitor use a switching boundary defined relative to the worst-case performance dynamics of all down-stream control components, as was done for the eCRM-001 design explored in this work. This approach allows all RTA monitors to perform their functions independently of one another, switching to their respective low-confidence controllers based upon locally available information. The potential drawback is that the safety boundaries being enforced would be more conservative, potentially increasing the likelihood that a monitor would trigger a switch to its high-confidence system. In the UAM environment, in which switching to the high-confidence controller does not decrease safety, this tradeoff of decreased complexity for increased conservatism is likely to be well accepted.

As an example, consider the collision avoidance function, for which high-level control is provided by the DRP controller. If the state of RTA monitors at the Tracking Control and TRC Control levels are not known to the DRP monitor, it must assume a worst-case scenario in which the lower performing (high-confidence) controllers are operating at those lower levels. It would thus engage the DRP controller (i.e., issue a collision avoidance RA) earlier than might otherwise be necessary. If, in fact, the downstream Tracking Control and TRC monitors were still using their high-performance (low-confidence) control implementations, the result would be a slightly increased number of RAs issued and a greater separation from nearby aircraft than would be strictly necessary. While an increased rate of RAs may have some safety implications, the corresponding decrease in design complexity (and potential reduction in hazards stemming from design or implementation flaws) may more than compensate.

5.7 RTA in an ARP4754-based Process

In the previous BAART task order [Peterson 2020], a process for incorporating RTA protection within an aircraft design was explored. This process implicitly assumed that the potential utility of RTA protection was anticipated early in the overall aircraft design process, which may well be the case if the need for advanced control techniques is recognized at that stage. Process elements for including RTA designs included an elaboration of RTA approach and goals, allocation of functionality to RTA components and related controllers, and formal specification of safety regions and switching boundaries. These are illustrated in Figure 51, along with the traditional SAE-based development process.

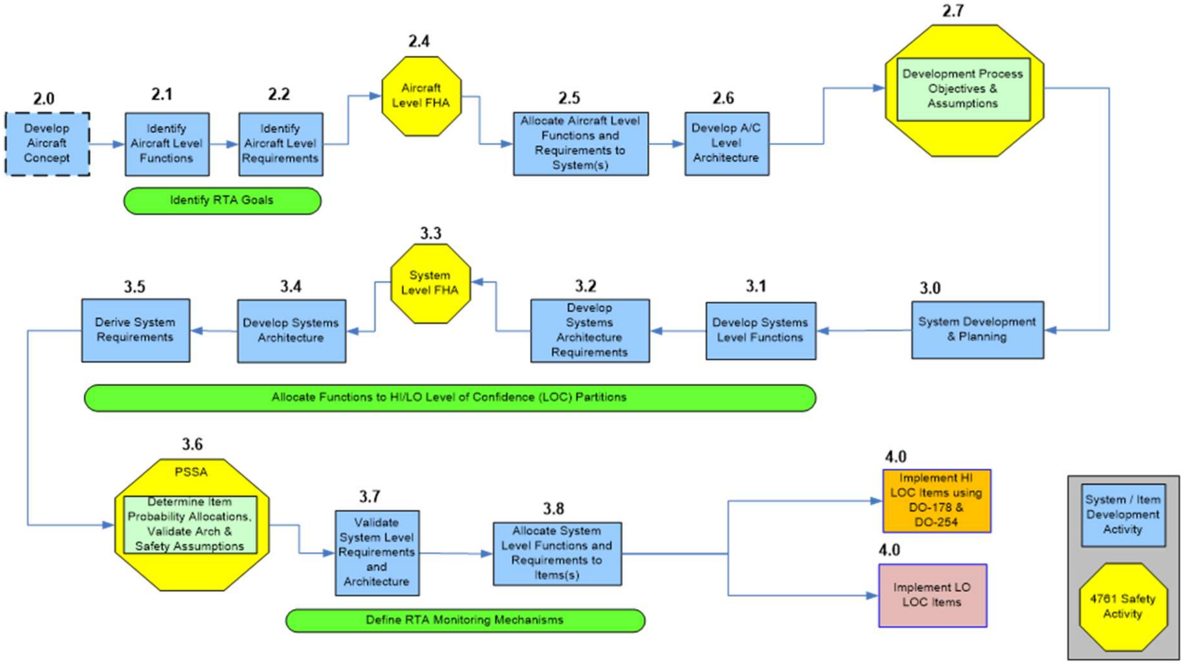

2.0
Develop Aircraft Concept
2.1
Identify Aircraft Level Functions
2.2
Identify Aircraft Level Requirements
Identify RTA Goals
2.4
Aircraft Level FHA
2.5
Allocate Aircraft Level Functions and Requirements to System(s)
2.6
Develop A/C Level Architecture
2.7
Development Process Objectives & Assumptions
3.0
System Development & Planning
3.1
Develop Systems Level Functions
3.2
Develop Systems Architecture Requirements
3.3
System Level FHA
3.4
Develop Systems Architecture
3.5
Derive System Requirements
Allocate Functions to HI/LO Level of Confidence (LOC) Partitions
3.6
PSSA
Determine Item Probability Allocations, Validate Arch & Safety Assumptions
3.7
Validate System Level Requirements and Architecture
3.8
Allocate System Level Functions and Requirements to Items(s)
Define RTA Monitoring Mechanisms
4.0
Implement HI LOC Items using DO-178 & DO-254
4.0
Implement LO LOC Items
System / Item Development Activity
4761 Safety Activity

Figure 51. Case Study Process Flow from [Peterson 2020]

However, it may happen that the need for RTA protection is not anticipated at the start of aircraft design, while the required aircraft functionality is being defined. The design pattern of RTA explored for the Tracking Controller and TRC Controller in the current effort provides insight into how such use cases might be identified. For these controllers, the SFHA activities indicated that the functionality required at these levels in the control hierarchy must be at least FDAL B. However, the requirements for those functions (e.g., adaptability, turbulence rejection, nonlinear tracking, etc.) led to the selection of algorithms that are unlikely to be developed to DAL B. An RTA-based architecture was used to accommodate these requirements for as long as the RTA monitor determines it is safe to do so, while achieving the indicated DAL B.

More generally, RTA may be a useful design alternative for cases in which system functions assigned DALs higher than level D have requirements that are best satisfied by algorithms that cannot be practically developed above DAL D.

5.8 STPA in an ARP4754-based Process

Several studies and working groups have addressed the relationship between STPA and existing standards. For example, standards committees have been and/or are investigating the notion of using STPA during development and safety assessment of general civil aircraft types. In addition, several papers in the academic literature have addressed similarities and differences between STPA and other hazard analysis techniques [Abdulkhaleq 2015] as well as comparisons of the types of results produced by STPA and other methods [Sulaman 2019].

In addition, due to the unique nature of aircraft such eCRM-001, as well as the unique types of operations required for urban air mobility concepts [FAA 2020], the following recommendations for integrating STPA into ARP4754-based processes are intentionally focused and scoped in several ways. We have been focused on answering the following questions:

1. Is STPA a useful framework for supporting an ARP4754-driven development process for eVTOL aircraft with *highly complex, highly automated, hierarchical control systems*?
2. If it is useful, how should STPA be integrated with the various processes described in ARP4754 and its related standards?

Although documentation on STPA does include descriptions and discussions about integrating STPA into a larger engineering process [Leveson 2016, Leveson 2018], these descriptions are very abstract in the sense that they are not tied directly to any application domains. In particular, the general documentation describing the STPA methodology is not specific to the aircraft development industry and its associated standards.

Furthermore, STPA is at its core an *analysis* technique, not necessarily a development process. ARP4754A and related standards (ARP4761, DO-178C, DO-254, etc.) are fundamentally about the process of engineering aircraft. These processes include multiple assessments at important points in the development cycle, and furthermore these assessments include recommendations about specific analysis techniques and other activities. These processes are specifically tailored to the design and certification commercial aircraft.

5.8.1 Background on ARP4754A Processes

Before describing specific guidance on recommendations for how STPA could be integrated into processes for aircraft certification, it is instructive to consider several relevant definitions from ARP4754A. First, note that System Level FHA

> *Examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific failure conditions [SAE 2010]*

The system architecture and system requirements are then derived based on these system level functional hazard assessments. It is on these architectures and requirements that one then performs a Preliminary System Safety Assessment (PSSA), determining item probability allocations, validating architecture and safety assumptions, and other activities. In particular, the PSSA involves a

> *systematic examination of a proposed architecture(s) to determine how failures could cause the Failure Conditions identified by the FHA*

The purpose of a PSSA is to, among other things, (1) provide an overview of the system and its modes of operation, (2) provide an assessment of meeting availability requirements, (3) provide an assessment of meeting integrity requirements, and (4) ensure that design assurance levels (DALs) are assigned appropriately. A PSSA includes Reliability Analysis, Maintainability Analysis, Preliminary Fault Tree Analysis, hazard analysis considerations, as well as DALs. To support more detailed analysis, a PSSA may include a system/product block level FMEA that seeks to identify what failures may result from the system/product design blocks, what their effects are, and how they would be mitigated by the design.

It is for this *systematic examination of a proposed architecture* that we recommend STPA as a particularly useful role in the context of PSSA. In particular, STPA could be useful due to the inherent complexity of the control architectures required to operate novel aircraft like eCRM-

001, where not only is each control function potentially complex but also due to the coupling within and across the hierarchical control structures of such aircraft.

STPA is similar in spirit to the system architecture FMEA portion of the PSSA in that it seeks to identify how and why hazardous behaviors may arise. However, unlike FMEA and other analysis techniques in ARP4761, STPA is explicitly a control-focused technique that seeks to identify unsafe control actions anywhere in the control hierarchy. STPA systematically addresses each control signal, examining possible hazards due to problems with signal content, timing, coupling due to feedback, etc. STPA is useful for identifying control mishaps, identifying design gaps, modifying or augment control architectures, and deriving safety requirements. To reach its full potential, and to help certify novel aircraft under novel operational conditions, one must address the interface between safety assessment and STPA.

5.8.2 Integration of STPA into ARP4754 Processes

Although STPA *could* be used to support Preliminary Aircraft Safety Assessment (PASA) and possibly other aspects of the safety assessment process, for the reasons described in the previous sub-section we focus here on recommendations for *how to integrate STPA with PSSA*. To illustrate how to integrate STPA into the appropriate standards, we will again notionally depict the STPA process and identify what artifacts should come “from” the various standards’ processes to support STPA, and then identify what artifacts STPA should produce and give “to” the appropriate processes.

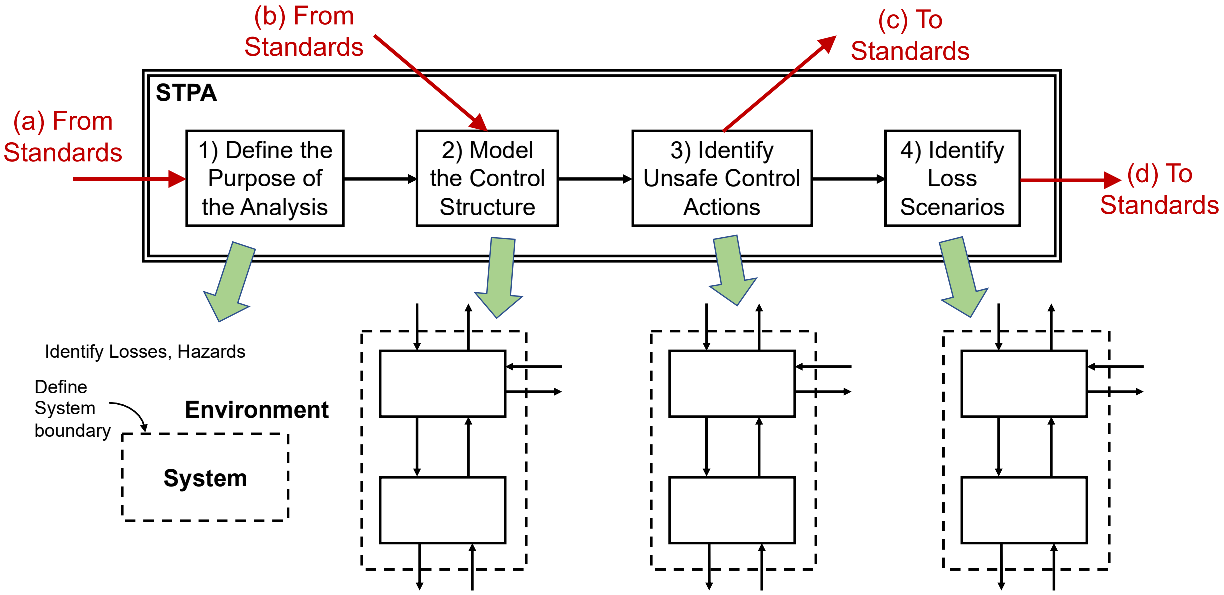


Figure 52. Graphical Depiction of mapping from Standards to and from STPA

The four labels in Figure 52 represent the following:

- Define the Purpose of the Analysis in STPA: The general systems engineering process in ARP4754, including identification of hazards, operational assumptions, etc. represents the input into the first step of STPA; i.e. the standards form an input *to* STPA.
- Model the Control Structure in STPA: the functional breakdown that is undertaken as part of a Functional Hazard Assessment in ARP4761, as well as block diagrams from

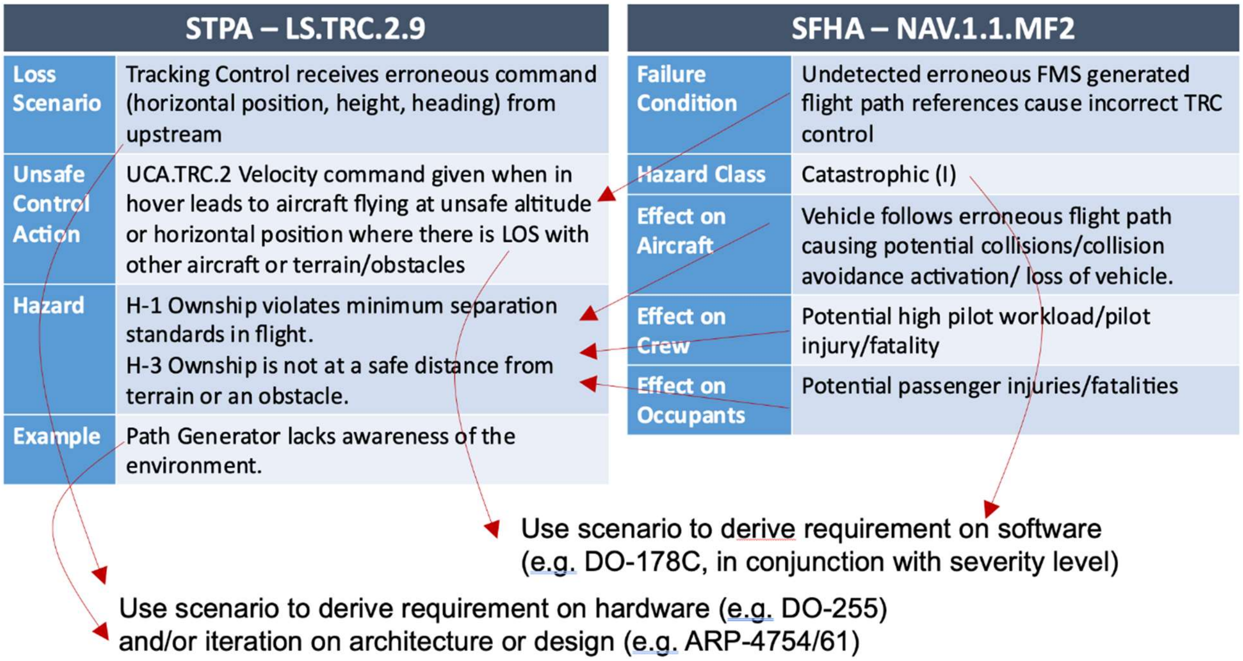
system FHAs represent an input into STPA and helps to form the control structure. In addition, Concepts of Operations documents and control system diagrams can be used to inform this step when available.

- Identify Unsafe Control Actions in STPA: this step represents an input *from STPA to the existing standards*. In particular, the unsafe control actions should be used to derive requirements on controller behavior and related software requirements; in other words, this output should feed into DO-178C.
- Identify Loss Scenarios in STPA: this step results in derived requirements on subsystem and/or component behavior as well as software requirements, feeding in DO-178C and other standards. In addition, this step can result in modified architectures or designs, feeding back into ARP4754 and/or ARP4761.

Figure 53 illustrates these connections in more detail, with specific example results coming out of our analysis of the tracking controller functionality in the notional eCRM-001 type aircraft. In particular, note that the effects on aircraft, crew, and occupants provide guidance on the types of “hazards” (hazard here is defined according to the STPA definition [Leveson 2016]) considered in the STPA analysis. This represents a snapshot of “Define the Purpose of Analysis” in STPA. The control structure models are described in Section 3.9, which were developed based on a combination of the functional breakdown and/or block diagrams, as well as control architecture diagrams [Takahashi 2017].

The unsafe control action should then be translated into a requirement, i.e., velocity command should not be given in that particular scenario, and these scenarios can be further refined based on the operational concept, subject matter expertise, and other information sources. These derived requirements are then combined with the hazard class identified in the SFHA to form the appropriate guidance and processes used to certify that particular subsystem.

In addition, the failure condition identified in the SFHA often represents a type of unsafe control action that would be identified by STPA; this represents a possible synergy or extra set of guidance on which unsafe control actions merit the most attention in the next step, which involves identifying loss scenarios, or scenarios that may lead to an unsafe control action. Finally, the loss scenarios in STPA result in identification of additional design requirements, particularly on those components that are necessary for a controller to perform its function. In cases where the loss scenarios cannot be eliminated or mitigated through the imposition of requirements, these loss scenarios can also trigger a modification of the design or controller architecture.



STPA – LS.TRC.2.9	
Loss Scenario	Tracking Control receives erroneous command (horizontal position, height, heading) from upstream
Unsafe Control Action	UCA.TRC.2 Velocity command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is LOS with other aircraft or terrain/obstacles
Hazard	H-1 Ownship violates minimum separation standards in flight. H-3 Ownship is not at a safe distance from terrain or an obstacle.
Example	Path Generator lacks awareness of the environment.

SFHA – NAV.1.1.MF2	
Failure Condition	Undetected erroneous FMS generated flight path references cause incorrect TRC control
Hazard Class	Catastrophic (I)
Effect on Aircraft	Vehicle follows erroneous flight path causing potential collisions/collision avoidance activation/ loss of vehicle.
Effect on Crew	Potential high pilot workload/pilot injury/fatality
Effect on Occupants	Potential passenger injuries/fatalities

Use scenario to derive requirement on software (e.g. DO-178C, in conjunction with severity level)
Use scenario to derive requirement on hardware (e.g. DO-255) and/or iteration on architecture or design (e.g. ARP-4754/61)

Figure 53. Illustration of connections between FHA, STPA, and Certification Standards

In summary, we advocate for the use of STPA in the following ways. First, it should be used to derive requirements for hardware and software systems and/or components. Based on criticality and other aspects or outputs of the PSSA, these would get fed into the appropriate standard processes, e.g. DO-178C, DO-254, DO-255, and DO-297, where requirements would then be verified accordingly. Second, STPA is a natural complement to other processes in ARP4754A involving design studies and iteration. STPA results can be used to initiate design trade studies, for example by adding or deleting connections/signals in the communications or software architecture, which would then trigger an iteration of PSSA, or possibly be fed back up the chain and result in higher level safety assessments like FHAs or SFHAs.

5.9 STPA for RTA-Protected Systems

Results from the current and previous task orders show that the inclusion of RTA protection for advanced control components can significantly decrease the amount of development effort by eliminating the requirement to perform key activities from DO-178C for those components. However, the RTA architecture does result in an increased system complexity that can increase the effort associated with performing STPA activities for these systems. Team experience in the current task order suggests that this increase is not drastic because of the parallel structure that exists between the low-confidence and high-confidence controllers.

While the RTA monitoring and switching components require additional analysis, the introduction of a second parallel controller (in this case, the high-confidence controller) does not necessarily increase the number of unsafe control actions or causal factors that must be addressed during the STPA. Since both low- and high-confidence controllers are controlling the same process, there will be significant commonality in the available control actions and in the subsets of those that are unsafe. (Depending, of course, on the level of abstraction used to model these controllers.) Thus, the inclusion of STPA as part of the PSSA activities is likely not an impediment to the use of RTA protection.

5.10 Pilot as a System Component

An aircraft development process based on ARP4754A and related standards explicitly considers the pilot and piloting capabilities early in development, from the aircraft function development through SFHA activities. The primary considerations addressed during AFHA and SFHA is the impact hazards will have upon the pilot and the pilot's ability to safely perform required tasks. These considerations lead to the assignment of FDALs, which ultimately determine the development rigor that must attend the components implementing those functions. Typically, the pilot's capabilities and/or limitations are not explicitly considered after FDAL assignments have been made. (Occasionally, references to specific pilot errors might appear in an FTA, but these do not generally contribute quantitatively to the FTA result.)

In contrast, a typical STPA formulation will explicitly model the pilot as part of the aircraft system. This permits very explicit consideration regarding erroneous actions the pilot may take and how those actions might affect safety. Inclusion of STPA as a supporting analysis within the PSSA would provide a structured way to address the impact of potential pilot errors within the traditional safety engineering process. This may provide highly valuable support for the design of UAM aircraft, which will involve novel designs and environments with the potential for:

- Highly complex pilot-automation interactions that may result in novel failure modes;
- A lack of strong institutionalized knowledge regarding the demands likely to be placed on the pilot
- Wide variation in piloting skills.

The ability to explicitly model the effects of pilot errors may also be very valuable for the design of training materials. That is, it can potentially help identify piloting errors that have significant negative consequence and that cannot be adequately mitigated by components within the aircraft. These are strong candidates for explicit inclusion in training materials.

It is worth noting that STPA is not quantitative, in the sense that it does not assign probabilities to erroneous actions that a pilot might take. Thus, its use in conjunction with other PSSA activities would address pilot errors in much the same way as software development errors are currently addressed. In particular, STPA results may not directly support quantitative fault tree analyses and other techniques that deal directly with hazard probabilities. To support this level of integration, safety assessments would need to be augmented with quantitative human performance models capable of generating plausible pilot error rates.

6.0 Recommendations for Future Research

During the course of our current study, we identified a number of issues and questions that would merit further research. This list is not exhaustive but includes brief descriptions of future research efforts that could build upon the current research effort and contribute to government and industry efforts related to Run-Time Assurance, and the design, certification, and safety analysis of novel aircraft designs such as those being planned for UAM applications.

- **Conduct PSSA for the eCRM-001:** This current project completed AFHA/SFHA for the Baseline Aircraft design and noted the implications on AFHA/SFHA for the RTA-Protected Aircraft. We also completed an STPA analysis for the Baseline Aircraft design, which was recommended as a supporting analysis for PSSA. PSSA would continue safety analysis of the aircraft and its control system. We would also further explore interactions between aircraft sub-functions, and explore in more detail how STPA can add value to traditional analyses such as FTA, FMEA, etc.

- **Collision Avoidance Functionality:** In this effort we would develop collision avoidance requirements and candidate designs specifically for UAM. Current collision avoidance systems contemplate more traditional aircraft operations. UAM will be a very different operational environment with unique challenges. Government and industry will need consensus on exactly what CAS in this environment should comprise. Research into CAS design and development for UAM could include: 1) Development of detailed collision avoidance scenarios; 2) Considerations for dealing with rogue actors; 3) Equipage necessary to support CAS; 4) Candidate algorithms to process data streams; 4) Pilot interfaces for situational awareness; and 5) High-level automated control algorithms.
- **RTA Theory and Practice:** Perform research to answer questions of practical relevance for RTA implementations. The previous task order included computational example of RTA boundary development for a simplified control component. The current task order developed control concepts in much more detail. Government and industry would benefit from more complete RTA algorithmic development for these, with example plans for software certification. Key items that need to be developed include: 1) Formal specification of RTA boundary for control elements developed in this task order, with candidate plans for DO-178C activities; 2) Demonstrating requirement verifiability, algorithm accuracy, test coverage, etc.; 3) Detailed requirements for RTA behavior following equipment failures; and 4) Interactions between RTA and health monitoring, desired behavior following a failure, pilot interfaces to affect desired behavior, etc.
- **RTA Development:** Explore implementations of RTA algorithmic components that could support deeper analysis & experimentation. This study examined several systems for which RTA-protection could be valuable and how the RTA components might operate. Investigation beyond PSSA level would benefit from candidate implementations of those components. Government and industry would benefit from development of a reusable software framework implementing common algorithmic components such as: 1) General software architecture for RTA-protection within an autonomous GNC hierarchy; 2) Tools supporting RTA monitoring within that architecture; and 3) Tools for implementing high-confidence recovery functions.
- **Proof of Concept Study:** Government and industry would benefit from case studies that look at actual RTA performance in related systems. Our current research work has examined realistic candidate applications of RTA. We have identified specific algorithms for both low-confidence and high-confidence components. Software implementations of these algorithms exist and could be leveraged in future research. With additional development, the RTA design could be realized in software to support detailed case studies. This could be accomplished through an incremental development/test approach: 1) Simulation environment and algorithmic implementation that would support large-scale batch simulation studies; 2) Human-in-the-loop simulation of that architecture to enable studies of pilot interactions of such systems; and 3) Flight testing of these in an unmanned eVTOL aircraft.
- **Pilot as a System Component:** One of our key findings and recommendations from our current research effort is that STPA activities be included in the PSSA to address potential piloting errors. However, STPA is not quantitative and does not incorporate models of the pilot. Considerable research has investigated quantitative pilot models

including treating the pilot as a feedback control component and more general human factors measures of performance. Government and industry would benefit from studies that look at how these models might be incorporated more directly into the safety engineering process. This could provide a more rigorous basis for determining likely failure rates traceable to pilot errors for a given design. We also propose to include these models early in the design process, helping to ensure safe designs that account for limitations of human performance.

Appendix A. Aircraft Function List

F – Provide control of aircraft movement

This is the major function required to control the movement of the aircraft along the flight profile. It is decomposed into the functions of aviate, navigate and communicate. Note that the functions under aviate, navigate and communicate include references to automation. More detailed information regarding what automation is defined for each phase of the flight profile is typically developed during the system allocation process, which includes the system architecture and considerations for the system operation

F.A - Aviate

These are functions related to controlling the aircraft's aerodynamic state. The functional decomposition includes 1) the functions required for the pilot controls (i.e., the interface to the other systems) to manually control the aircraft (F.A.1); 2) the functions for the systems required to automatically or manually (by direct pilot input) control the flight profile including hover, wingborne, and transition between hover and wingborne flight (F.A.2, 3 and 4); and 3) the functions for the systems required to provide situational awareness to the pilot for the aviate function (F.A.5). These are for awareness of the aerodynamic situation, as opposed to the navigation/geospatial situational awareness discussed under F.N - Navigate.

F.A.1 Provide interfaces for unified control of aircraft flight

The aircraft must provide interfaces by which the pilot can control the aircraft. The aircraft movement is controlled around the pitch, roll and yaw axes as well as speed. These include the left- and right-hand inceptors, rudder pedals, trim switches and mode controls and as well as their interfaces to the other aircraft systems. Unified control makes pilot control of the vehicle consistent throughout the various flight modes, including transitions.

F.A.1.1 Provide interfaces for attitude (pitch, roll, yaw axis) control

The aircraft must provide interfaces by which the pilot can control the aircraft pitch, roll and yaw axes.

F.A.1.1.1 Provide attitude control interfaces for hover flight

The aircraft must provide interfaces by which the pilot can control attitude in hover flight.

F.A.1.1.1.1 Provide manual attitude control interfaces for hover flight

The aircraft must provide interfaces by which the pilot can manually control attitude in hover flight.

F.A.1.1.1.2 Provide automation attitude control interfaces for hover flight

The aircraft must provide interfaces by which the pilot can enable automation to control attitude in hover flight.

F.A.1.1.2 Provide attitude control interfaces for wingborne flight

The aircraft must provide interfaces by which the pilot can control attitude in wingborne flight.

F.A.1.1.2.1 Provide manual attitude control interfaces for wingborne flight

The aircraft must provide interfaces by which the pilot can manually control attitude in wingborne flight.

F.A.1.1.2.2 Provide automation attitude control interfaces for wingborne flight

The aircraft must provide interfaces by which the pilot can enable automation to control attitude in wingborne flight.

F.A.1.1.3 Provide attitude control interfaces for transition flight

The aircraft must provide interfaces by which the pilot can control attitude for transition between hover and wingborne flight, and between wingborne and hover flight.

F.A.1.1.3.1 Provide manual attitude control interfaces for transition flight

The aircraft must provide interfaces by which the pilot can manually control attitude for transition between hover and wingborne flight, and between wingborne and hover flight.

F.A.1.1.3.2 Provide automation attitude control interfaces for transition flight

The aircraft must provide interfaces by which the pilot can enable automation to control attitude for transition between hover and wingborne flight, and between wingborne and hover flight.

F.A.1.2 Provide interfaces for speed control

The aircraft must provide interfaces by which the pilot can control the speed of the aircraft.

F.A.1.3 Provide interfaces for translational control

The aircraft must provide interfaces by which the pilot can control the translational axes of the aircraft.

F.A.1.3.1 Provide interfaces for vertical control

The aircraft must provide interfaces by which the pilot can control the vertical axis of the aircraft.

F.A.1.3.2 Provide interfaces for horizontal control

The aircraft must provide interfaces by which the pilot can control the horizontal axes of the aircraft.

F.A.1.4 Provide interfaces for attitude trim control

The aircraft must provide interfaces by which the pilot can control attitude trim of the aircraft.

F.A.2 Provide controlled aircraft hover flight

The aircraft must provide the capacity for a controlled hover flight.

F.A.2.1 Provide flight control modes (hover)

The aircraft must provide modes to control hover flight.

F.A.2.1.1 Provide rate command/height hold vertical control mode

The aircraft must provide a control mode for rate command/height hold control in hover.

F.A.2.1.2 Provide translation rate command horizontal control mode

The aircraft must provide a control mode for rate command horizontal control in hover.

F.A.2.1.3 Provide rate command/direction hold yaw control mode

The aircraft must provide a control mode for rate command/direction hold yaw control in hover.

F.A.2.2 Provide vertical movement control

The aircraft must provide a control mode for vertical movement control in hover.

F.A.2.2.1 Control wingtip, RT/LT wing, FWD/AFT fuselage rotors

The aircraft must provide the capacity to control the wingtip, RT/LT wing and FWD/AFT fuselage rotors for vertical movement in hover.

F.A.2.2.2 Control vertical rate

The aircraft must provide the capacity to control vertical rate in hover.

F.A.2.3 Provide pitch axis control

The aircraft must provide the capacity to provide pitch axis control in hover.

F.A.2.3.1 Control wingtip rotors, FWD/AFT fuselage rotor

The aircraft must provide the capacity to control the wingtip rotors and FWD/AFT fuselage rotor for pitch axis control in hover.

F.A.2.3.2 Control pitch rate

The aircraft must provide the capacity to control pitch rate in hover.

F.A.2.4 Provide roll axis control

The aircraft must provide the capacity for roll axis control in hover.

F.A.2.4.1 Control wingtip rotors, RT/LT wing rotors

The aircraft must provide the capacity to control the wingtip rotors and RT/LT wing rotor for roll axis control in hover.

F.A.2.4.2 Control roll rate

The aircraft must provide the capacity to control roll rate in hover.

F.A.2.5 Provide yaw axis control

The aircraft must provide the capacity for yaw axis control in hover.

F.A.2.5.1 Control rotor flow effectors

The aircraft must provide the capacity to control the rotor flow effectors for yaw axis control in hover.

F.A.2.5.2 Control yaw rate

The aircraft must provide the capacity to control yaw rate in hover.

F.A.3 Provide controlled aircraft wingborne flight

The aircraft must provide the capacity for a controlled wingborne flight.

F.A.3.1 Provide flight control modes (wingborne)

The aircraft must provide modes to control wingborne flight.

F.A.3.1.1 Provide flight path command vertical control mode

The aircraft must provide a flight path command vertical control mode for wingborne flight.

F.A.3.1.2 Provide rate command/attitude hold roll control mode

The aircraft must provide a rate command/attitude hold roll control mode for wingborne flight.

F.A.3.1.3 Provide turn coordination/angle-of-sideslip yaw control mode

The aircraft must provide a turn coordination/angle-of-sideslip yaw control mode for wingborne flight.

F.A.3.1.4 Provide acceleration command/velocity hold pitch control mode

The aircraft must provide an acceleration command/velocity hold pitch control mode for wingborne flight.

F.A.3.2 Provide pitch axis control

The aircraft must provide the capacity for pitch axis control in wingborne flight.

F.A.3.2.1 Control elevator

The aircraft must provide the capacity to control the elevator for pitch axis control in wingborne flight.

F.A.3.2.2 Control pitch rate

The aircraft must provide the capacity to control pitch rate in wingborne flight.

F.A.3.3 Provide roll axis control

The aircraft must provide the capacity for roll axis control in wingborne flight.

F.A.3.3.1 Control ailerons

The aircraft must provide the capacity to control the ailerons for roll axis control in wingborne flight.

F.A.3.3.2 Control roll rate

The aircraft must provide the capacity to control roll rate in wingborne flight.

F.A.3.4 Provide yaw axis control

The aircraft must provide the capacity for yaw axis control in wingborne flight.

F.A.3.4.1 Control rudder

The aircraft must provide the capacity to control the rudder for yaw axis control in wingborne flight.

F.A.3.4.2 Control yaw rate

The aircraft must provide the capacity to control yaw rate in wingborne flight.

F.A.3.5 Provide thrust control

The aircraft must provide the capacity for thrust control in wingborne flight.

F.A.3.5.1 Control wingtip rotors

The aircraft must provide the capacity to control the wingtip rotors to provide thrust control in wingborne flight.

F.A.3.6 Provide lift control

The aircraft must provide the capacity for lift control in wingborne flight.

F.A.4 Provide controlled aircraft transition flight

The aircraft must provide the capacity for a controlled flight during transition between hover and wingborne flight.

F.A.4.1 Provide flight control modes (transition)

The aircraft must provide modes to control flight during transition.

F.A.4.1.1 Provide flight path command vertical control mode

The aircraft must provide a flight path command vertical control mode for transition flight.

F.A.4.1.2 Provide attitude command/attitude hold roll control mode

The aircraft must provide an attitude command/attitude hold roll control mode for transition flight.

F.A.4.1.3 Provide turn coordination/angle-of-sideslip yaw control mode

The aircraft must provide a turn coordination/angle-of-sideslip yaw control mode for transition flight.

F.A.4.1.4 Provide acceleration command/velocity hold pitch control mode

The aircraft must provide an acceleration command/velocity hold pitch control mode for transition flight.

F.A.4.2 Provide aircraft configuration control (transition)

The aircraft must provide aircraft configuration control for transition flight.

F.A.4.2.1 Control wingtip rotor tilt vs. speed

The aircraft must provide the capacity to control wingtip rotor tilt vs. speed for transition flight.

F.A.4.2.2 Control fuselage/wing rotor stow and unstow

The aircraft must provide the capacity to stow and deploy rotors when transitioning between hover and forward flight.

F.A.5 Provide aerodynamic situational awareness interface

The aircraft must provide an interface to the pilot to provide aerodynamic situational awareness. This typically takes the form of displays, lights, aural caution and warning and tactile feedback.

F.A.5.1 Provide aircraft state information

The aircraft systems required to provide the pilot with information concerning the aircraft’s state.

F.A.5.1.1 Provide attitude

The aircraft must provide the pilot with information concerning the aircraft attitude.

F.A.5.1.2 Provide altitude

The aircraft must provide the pilot with information concerning the aircraft altitude.

F.A.5.1.3 Provide heading

The aircraft must provide the pilot with information concerning the aircraft heading.

F.A.5.1.4 Provide airspeed

The aircraft must provide the pilot with information concerning the aircraft airspeed.

F.A.5.2 Provide motor/rotor information

The aircraft must provide the pilot with information concerning the aircraft motor/rotor information. This typically includes operational and position data.

F.A.5.3 Provide aircraft status information

The aircraft must provide the pilot with information concerning the aircraft status. This typically includes information of aircraft systems capability and operational/failure status.

F.A.5.4 Provide envelope protection alerts

The aircraft must provide alerts to the pilot for envelope protection of the aircraft.

F.A.5.4.1 Provide attitude limits

The aircraft must provide alerts to the pilot for when the aircraft is at, nearing or going to exceed the attitude limits of the aircraft.

F.A.5.4.2 Provide speed limits (longitudinal and vertical speed limits)

The aircraft must provide alerts to the pilot when the aircraft is at, nearing, or going to exceed the speed limits (longitudinal and vertical speed limits) of the aircraft.

F.A.5.4.3 Provide hover limits (vortex ring state)

The aircraft must provide alerts to the pilot for when the aircraft is at, nearing or going to exceed the hover limits (vortex ring state)) of the aircraft.

F.A.5.4.4 Provide alpha limits

The aircraft must provide alerts to the pilot for when the aircraft is at, nearing or going to exceed the alpha (angle of attack stall) limits of the aircraft.

F.N - Navigate

These are functions related to controlling the aircraft's geospatial state. The functional decomposition for Navigate includes: 1) the functions required for planning of the navigation route (F.N.1); 2) the functions required for the execution of the entered flight plan (F.N.2); and 3) the functions required for the pilot to be aware of how the flight plan is being followed along with any anomalies (F.N.3).

F.N.1 Provide flight planning

The aircraft must provide the capacity to perform flight planning, including origin, destination, and route of flight.

F.N.1.1 Provide on-board flight planning

The aircraft must provide the capacity to perform the flight planning function on-board the aircraft.

F.N.1.1.1 Provide interface to specify a flight plan

The aircraft must provide the capacity to specify and enter a flight plan, either manually by the pilot or through automation.

F.N.1.1.1.1 Provide manual pilot interface to specify a flight plan

The aircraft must provide the capacity for the pilot to enter a flight plan on-board the aircraft.

F.N.1.1.1.2 Provide automation interface to specify a flight plan

The aircraft must provide the capacity to upload/download a flight plan to/from the flight management automation system.

F.N.1.2 Provide off-board flight planning interface

The aircraft must provide the capacity to enter a flight plan off-board the aircraft.

F.N.1.3 Provide on-board flight plan modification

The aircraft must provide the capacity to modify the existing flight plan on-board the aircraft.

F.N.2 Provide flight management

The aircraft must provide the capacity for the management of the flight plan.

F.N.2.1 Provide path generation

The aircraft must provide the capacity to generate the flight plan path that the aircraft will need to follow.

F.N.2.2 Provide path monitoring

The aircraft must provide the capacity to monitor that the aircraft is following the generated flight path within the specified tolerances.

F.N.2.3 Provide path following control mode

The aircraft must provide the capacity for vertical and lateral control along the navigational route (flight plan). This includes any failure or warning annunciations to the pilot.

F.N.2.3.1 Provide automated path following control mode

The aircraft must provide a control mode for the aircraft to automatically follow the generated flight plan path.

F.N.2.3.2 Provide variable-autonomy path following control mode

The aircraft must provide a control mode for the aircraft to follow the generated flight plan path with variable-autonomy.

F.N.2.4 Provide emergency geospatial control modes

The aircraft must provide emergency modes when geospatial envelopes or conditions are violated or in danger of being violated. This includes failure or warning annunciations to the pilot.

F.N.2.4.1 Provide geo-fence protection

The aircraft must provide mitigation against violation of geo-fence boundaries. An emergency maneuver may be required to keep the aircraft at a safe distance from such boundaries.

F.N.2.4.2 Provide minimum safe altitude

The aircraft must provide a minimum safe altitude for the aircraft to operate. An emergency maneuver may be required to keep the aircraft at a safe altitude.

F.N.2.4.3 Provide airborne vehicle collision avoidance

The aircraft must provide the capacity to avoid collisions with other aircraft, terrain and fixed structures, such as buildings. This includes the emergency maneuver required once an imminent collision is detected.

F.N.3 Provide Geospatial Situational Awareness

The aircraft must provide the capacity for the pilot to achieve and maintain situational awareness of the geospatial flight and the surroundings. This includes how the aircraft is following the flight path trajectory as well as any imminent threats of collisions with other aircraft or structures.

F.N.3.1 Provide situational awareness interface

The aircraft must provide interfaces by which a pilot can achieve and maintain geospatial situational awareness. This typically takes the form of physical displays, lights, aural cautions and warnings, and tactile feedback.

F.N.3.2 Monitor situational awareness

The aircraft must provide the capacity for the pilot to monitor geospatial situational awareness. This typically takes the form of graphical/logical displays, lights, aural cautions and warnings, and tactile feedback.

F.C – Communicate

These are functions related to controlling communications on the aircraft and to and from the aircraft. The structure for the functional decomposition for Communicate includes 1) air-to-ground communication (F.C.1), 2) air-to -air communication (F.C.2), and 3) onboard communication (F.C.3).

F.C.1 Provide air-ground communication

The aircraft must provide the capacity for communications between the air and the ground.

F.C.1.1 Provide vehicle to/from airspace control authority

The aircraft must provide the capacity for communications between the air and the ground related to the airspace control authority.

F.C.1.1.1 Provide ATC communication (voice, data)

The aircraft must provide the capacity for communications between the air and the ground related to Air Traffic Control (ATC). This includes both voice and data.

F.C.1.1.2 Provide vertiport communication (voice, data)

The aircraft must provide the capacity for communications between the air and the ground related to Vertiport Control Authority. This includes both voice and data.

F.C.1.2 Provide vehicle to/from company operations

The aircraft must provide the capacity for communications between the aircraft and the company operations for that aircraft.

F.C.1.3 Provide vehicle navigation communication

The aircraft must provide the capacity for communications for vehicle navigation.

F.C.2 Provide air-air communications

The aircraft must provide the capacity for communications between the aircraft and other aircraft.

F.C.2.1 Provide vehicle-to-vehicle (data e.g. TCAS)

The aircraft must provide the capacity for data communications between the aircraft and other aircraft. An example is a Traffic Collision and Avoidance System (TCAS).

F.C.2.2 Provide vehicle to-from vehicle (voice)

The aircraft must provide the capacity for voice communications between the aircraft and other aircraft.

F.C.3 Provide vehicle internal communications

The aircraft must provide the capacity for internal communications within the aircraft.

Appendix B. Baseline Aircraft Functional Hazard Assessment

B.1 Introduction

The assessment captured herein represents the airplane level functional hazard assessment (AFHA) for the eCRM-001 VTOL airplane.

B.1.1 References

The following documents are referenced herein.

[1] Peterson, E., DeVore, M., Cooper, J., & Carr, G., “Run-Time Assurance as an Alternate Concept to Contemporary Development Assurance Processes,” NASA, 2020.

[2] 14CFR/CS Part 23, Amendment 23-64

[3] ASTM F3230-17, “Safety Assessment of Systems and Equipment in Small Aircraft”

[4] ASTM F3061-17, “Standard Specification for Systems and Equipment in Small Aircraft”

[5] “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Aircraft Systems and Equipment”

[6] eCRM-001 Airplane Function List (Appendix A)

Editor’s Note: Document reference numbering within an example artifact will be to the documents listed as references in this section rather than the overall report reference list.

B.1.2 Glossary

A glossary that captures specific terms and definitions used within the AFHA is provided in Table 18.

Table 18. Glossary of AFHA Terms

Term	Definition
Uncommanded	Activation of a function without pilot command input or erroneously activated due to equipment failure.
Minimum Acceptable Control (MAC)	An aircraft configuration under which the normal acceptable control performance criteria will still be satisfied and when lost will result in the failure condition effects described.
Loss of Mode/Control	Condition whereby an engaged mode disengages due to failure or otherwise uncommanded by the pilot.

Erroneous control	Failure condition whereby vehicle does not respond to commands in the manner intended
Lateral Deviation Beyond Limits	Lateral limits assume defined as +/- x.xx nautical miles (TBD) either side of planned course. Deviations occurring during the takeoff and landing phases expected to be more stringent than during cruise flight.
Vertical Deviation Limits	1. Vehicle does not level off at assigned altitude within +/- x feet (TBD) 2. Flight path projection predicts altitude constraint will not be met within +/- x feet (TBD) 3. For gamma based vertical paths, altitude on the path not within +/- x feet (TBD) 4. Airspeed more than +/- x knots from speed reference ** Deviations occurring during the takeoff and landing phases expected to be more stringent than during cruise flight.
Available, Availability	Qualitative or quantitative attribute that a system or equipment is in a functioning state at a given point in time.
Integrity	Qualitative or quantitative attribute of a system, equipment, or an item indicating that it can be relied upon to work as intended.
Independence	A design concept which ensures that the failure of one item does not cause a failure of another item (Derived from JAA AMJ 25.1309). (2) Separation of responsibilities that assures the accomplishment of objective evaluation.

B.2 Airplane Description Summary

Refer to Section 2.0 for a description of the eCRM-001 vehicle.

B.3 AFHA Development

The AFHA process accomplished herein is in accordance with ARP4761 [SAE 1996] recommended guidelines.

B.3.1 AFHA Inputs

The airplane development process identified the airplane level functions captured in eCRM-001 Airplane Function List. A subset of these functions will be the subject of the safety evaluation herein.

B.3.1.1 Review & Confirm Airplane Functions

Functions selected for evaluation are described:

- Provide Translation Rate Command horizontal control mode – Active while in hover, longitudinal and lateral inceptor deflections provide longitudinal and lateral velocities proportional to inceptor displacement. When the inceptors are in the neutral/detent position, the vehicle position relative to the ground is maintained (position hold mode). Vertical inceptor commands a vertical rate proportional to inceptor displacement. When the vertical inceptor is in the neutral/detent position, the vehicle maintains a fixed altitude.
- Provide path following control mode – provides vertical and lateral control along the navigational route (flight plan) as entered into the Flight Management System.
- Provide airborne vehicle collision avoidance – provides detection and annunciation to the pilot of airborne and surface threats/obstacles which may pose a collision hazard to the vehicle. Provides automatic maneuvering to avoid potential collision threats.

B.3.2 Determine Failure Conditions

This study examined failure conditions for three selected functions: Provide Translation Rate Command horizontal control mode, Provide Path Following Control Mode, and Collision Avoidance

B.3.2.1 Failure Condition Identification Matrix

A failure condition identification matrix was constructed for three pre-selected functions. This initial matrix is presented in Table 19. Postulated failure condition descriptions are captured for Total Loss of Function, Partial Loss of Function and Malfunction (erroneous operation of function).

Table 19. eCRM-001 Failure Condition Identification Matrix

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
F	Control of Airplane Movement			
F.A	Aviate			
F.A.2	Provide Controlled Aircraft Hover Flight			
F.A.2.1	Provide Flight Control Modes (Hover)			
F.A.2.1.2	Provide Translation Rate Command horizontal control mode	**F.A.2.1.2.TL1** Loss of TRC Control Mode (with or without annunciation to the pilot) **F.A.2.1.2.TL2** Loss of TRC Control Mode availability in cruise annunciated to the pilot	-	**F.A.2.1.2.MF1** Erroneous TRC control **F.A.2.1.2.MF2** Erroneous TRC engagement
F.N	Navigate			
F.N.2	Provide Flight Management			
F.N.2.3	Provide Path Following Control Mode	**F.N.2.3.TL1** Loss of Lateral Path Following Control Mode during flight with annunciation to the pilot **F.N.2.3.TL2** Loss of Lateral Path Following Control Mode during flight without annunciation to the pilot **F.N.2.3.TL3** Loss of Lateral Path Following Control Mode during	-	**F.N.2.3. MF1** Erroneous Lateral Flight Path deviation during flight with annunciation to the pilot **F.N.2.3. MF2** Erroneous Lateral Flight Path deviation during flight without annunciation to the pilot **F.N.2.3. MF3** Erroneous Lateral Flight Path deviation during flight takeoff/landing flight phase (with or without annunciation to the pilot)

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
		takeoff/landing flight phase (with or without annunciation to the pilot)		**F.N.2.3. MF4** Erroneous Lateral Flight Path deviation annunciation to the pilot when no deviation exists **F.N.2.3.MF5** Uncommanded engagement of Lateral Flight Path control mode

F.N.2	Provide Flight Management			
F.N.2.3	Provide Path Following Control Mode	**F.N.2.3.TL4** Loss of Vertical Path Following Control Mode during flight with annunciation to the pilot **F.N.2.3.TL5** Loss of Vertical Path Following Control Mode during flight without annunciation to the pilot **F.N.2.3.TL6** Loss of Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	-	**F.N.2.3. MF6** Erroneous Vertical Flight Path deviation during flight with annunciation to the pilot **F.N.2.3. MF7** Erroneous Vertical Flight Path deviation during flight without annunciation to the pilot **F.N.2.3. MF8** Erroneous Vertical Flight Path deviation during flight takeoff/landing flight phase (with or without annunciation to the pilot) **F.N.2.3. MF9** Erroneous Vertical Flight Path deviation annunciation to the pilot when no deviation exists **F.N.2.3. MF10** Uncommanded engagement of Vertical Flight Path Control Mode during flight

F.N.2.4	Provide Emergency Geospatial Control Modes			

F.N.2.4.3	Provide airborne vehicle collision avoidance	**F.N.2.4.3.TL1** Loss of collision avoidance function annunciated to the pilot **F.N.2.4.3.TL2** Loss of collision avoidance function not annunciated to the pilot	-	**F.N.2.4.3. MF1** Erroneous collision avoidance activation (collision threat annunciated to pilot but no collision threat exists) **F.N.2.4.3. MF2** Collision avoidance activation with erroneous avoidance maneuver (collision threat annunciated to pilot, legitimate collision threat detected) **F.N.2.4.3.MF3** Collision avoidance activation without annunciation to the pilot (legitimate collision threat detected)

B.3.2.2 Pilot Awareness

Editors' Note: Not included in this example for brevity.

B.3.3 Assess Failure Conditions Matrix

The effects of each of the identified failure condition on the aircraft, flight crew and occupants other than the flight crew have been assessed. The effects are captured based on their immediate effect on aircraft, flight crew and occupants during the phase of flight being analyzed.

The captured effects of each failure condition are shown in Column 4 of the AFHA worksheet tables, which are contained in Appendix B.5.

B.3.3.1 eCRM-001 Flight Profile

The eCRM-001 aircraft flight of average duration is presented in Figure 54. eCRM-001 Average Flight Profile. The nominal flight is divided into four flight phase groups, with individual flight phase durations as presented in Table 20. Flight phases and profile are the same used in the previous study [Peterson 2020].

Editor's Note: Not all eCRM-001 operational flight phases have been included in the study example system definition.

Table 20. eCRM-001 Airplane Flight Phases

Flight Phase	Flight Time	Flight Phase Code	Flight Phase
Ground	68s	G1	Taxi Out
	68s		Taxi In
Takeoff	18s	T1	Break ground to Hover
	60s	T2	Transition – Hover to Forward Flight
Forward Flight	91s	F1	Climb
	1212s	F2	Cruise
	91s	F3	Descent
		F4	Go Around
Landing	86s	L1	Transition – Forward Flight to Hover
	40s	L2	Hover – Descend to ground
	1734s	ALL	All flight phases
	30 min		

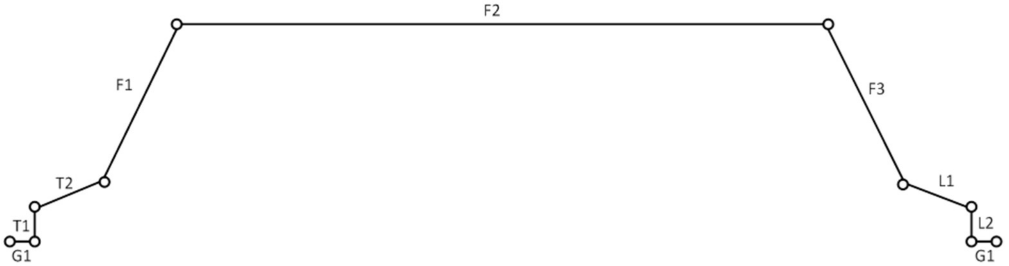


Figure 54. eCRM-001 Average Flight Profile

B.3.3.2 Operational Conditions

Editors’ Note: Not included in this example for brevity, except as identified in Section 1.0.

B.3.3.3 Environmental Conditions

Editors’ Note: Not included in this example for brevity.

B.3.4 Classify Failure Conditions Based on Effect Severity

Each failure condition has been classified based on its effects by applying the qualitative classification criteria provided in Reference [ASTM F3230], as applicable to this type of airplane. The failure condition classifications presented in Reference [ASTM F3230] are reproduced in Table 21 for convenience.

Table 21. F3230-17 Failure Condition Classifications

FC Classification based on Effect Area	Negligible	Minor	Major	Hazardous	Catastrophic
Effect on Aircraft	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal injury or incapacitation
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities

Allowable Qualitative Probability F3230-17	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Allowable Quantitative Probability F3230-17	No Probability Requirement	AW-I ≤ 10^{-3} AW II ≤ 10^{-3}	AW-I ≤ 10^{-4} AW II ≤ 10^{-5}	AW-I ≤ 10^{-5} AW II ≤ 10^{-6}	AW-I ≤ 10^{-6} AW II ≤ 10^{-7}

Note: AW – Airworthiness Level of F3230-17 is based on Assessment Level assigned per F3061-17. For the eCRM-001, the Assessment Level is “II”.

The classification of each failure condition for each flight phase is captured in Column (5) of the AFHA worksheet tables.

B.3.5 AFHA Assumptions

Assumptions made while accomplishing the effect evaluation of each failure condition have been captured and numerically identified for reference. Table 22 presents the analysis assumptions and notes that have been made during the development of this functional hazard assessment. Some assumptions are specifically referenced in the AFHA worksheets. Others are not referenced and are considered global assumptions.

Table 22. AFHA Assumptions and Notes

Assumption Identifier	Description
ASMP 1	The baseline eCRM001 vehicle employs TRC control mode as the only available mode while in hover.
ASMP 2	For the eCRM001 vehicle, dual INS with integrated GPS, INS is expected to be utilized as the source of velocity inputs into the control laws. Since the GPS velocity inputs are probably too slow for use in the control laws, it is expected that the INS acceleration and velocities will be used with the GPS velocities used to monitor the INS. This monitor will require some thought as the GPS is typically used by the INS/GPS to null out INS drift errors, so there may be a potential failure of GPS, which would impact INS outputs (erroneous null bias cancelation due to GPS failure).
ASMP 3	The path following mode is assumed monitored for accurate path tracking, with tracking errors beyond acceptable limits annunciated to the pilot. Full credit is taken for the pilot correctly reacting to the annunciation since basic navigation is a required skill of even relatively untrained pilots. **[Note – flight path monitoring is assumed independent with GPS position compared with INS position. Note that most coupled INS/GPS systems use GPS information to correct for INS drift thus a potential common mode exists which will need to be addressed].**
ASMP 4	Where excessive path following tracking error occurs and the annunciation fails to alert the pilot, no credit is taken for either the pilot or ATC (or equivalent) to

Assumption Identifier	Description
	recognize the path deviation. Hazard class is given assuming collision detection and avoidance is operating normally, hazard class with failed collision detection and avoidance given parenthetically. Note that un-annunciated excessive error also occurs when the Navigation system corrupts a correctly entered flight plan.

Assumption Identifier	Description
ASMP 5	For the case of un-annunciated path following error resulting in “missing” the landing destination, no credit is taken for pilot monitoring so it is assumed an off-vertiport landing will be required with possible crew/passenger injuries and/or fatalities. Due to the unknown urban environment of UAM operations, all forced landings not at a prepared field are presumed hazard class II.
ASMP 6	Path following is analyzed as an outer loop control law. Inner loop control assumed to incorporate attitude and rate limits to protect vehicle from overstress and/or unsafe attitudes due to erroneous outer loop control.
ASMP 7	Flight assumed to be performed only in VMC flight conditions
ASMP 8	Collision with other airborne vehicles mitigated by ADS-B/TCAS. These systems provide annunciation of airborne collision threats and provide avoidance guidance. Guidance commands are assumed coupled to automation, providing automatic flight guidance to avoid potential collisions.
ASMP 9	Collision with the ground or earth based structures is mitigated by vehicle systems using LIDAR and radar altimeter. No credit is taken for passive geo fence based flight planning to mitigate collision, since this AFHA analyzes the active avoidance function only.
ASMP 10	Collision avoidance detection is assumed to be “desensitized” during takeoff and landing to reduce nuisance alerts/maneuver activations with other vehicles/structures in the area. Thus, pilot is required to take on additional responsibility to avoid threats posed by other vehicles and proximity to structures during takeoff and landing.
ASMP 11	**Text Deleted
ASMP 12	Any activation of the collision avoidance maneuver, even in non-failed conditions, is presumed a hazard class III due to potential injuries to passengers who may not be in their seats.
ASMP 13	For un-annunciated loss of the collision warning function, it is assumed that a collision hazard will occur during the flight. This pessimistic assumption, when coupled with the assumption that the pilot will not detect the impending collision leads to a hazard classification of I.
ASMP 14	A “minimally trained” pilot will correctly act on system failures that are annunciated to the pilot. For failures not annunciated pilot is assumed to not recognize the effects of the failure in time to take corrective action. System failure(s) occurring at low altitudes such as takeoff and landing may not be reliably remedied by such a pilot, whether or not the pilot is made aware of the failure due to rapid response times and decision making required.
ASMP 15	Vertical and Lateral Deviation Limits are as provided in Section 1.2 Glossary.
ASMP 16	UAM Operations are conducted with a suitable alternate airfield available for a forward flight landing in the event transition from forward flight to hover flight is not available
ASMP 17	During Cruise (F2) flight phase a specified minimum safe altitude is assumed to provide a safe margin above the highest urban structure in the area.. This altitude margin is assumed sufficient to allow even minimally trained pilots

Assumption Identifier	Description
	enough time to intervene and recover the vehicle in the event annunciated navigation failures causing deviation from the flight plan path.
ASMP 18	Erroneous Navigation autonomy path commands cannot cause greater than a hazard classification of major change in vehicle attitudes and/or attitude rates.
ASMP 19	Minimally trained pilots are assumed capable of navigating to the planned arrival and alternate landing areas in the event of loss of on-vehicle navigation capability. Due to the nature of navigating in an urban environment, such unaided navigation is assumed to constitute a significant increase in pilot workload.
ASMP 20	It is assumed common cause failure (single failure) may cause erroneous waypoint data to simultaneously be used by the FCC tracking control function and the Display function. This can lead to failures not being detectable by the pilot as the erroneous computed path may seem correct on the Nav display. The design will need to preclude this possibility.
ASMP 21	In the Path Following analysis, no credit is taken for the “Dynamic Reactive Planning” (DRP) function to protect the airplane from erroneous path following control. This is to ensure a pessimistic assessment of path mode hazards. Additionally, (sub) function blocks may exist in the FMS and FCC common to both the path mode and DRP signal paths.

B.4 AFHA Output Summary

Table 23 summarizes the Failure Conditions that can lead to Catastrophic or Hazardous effects on the aircraft. For details associated with each failure condition refer to the AFHA worksheets contained in Appendix B.5.

Table 23. eCRM-001 Catastrophic & Hazardous FC Summary

Function	FC #	Failure Condition (Hazard Description)	Flight Phase	Classification
Provide Controlled Aircraft Hover Flight: Provide Translation Rate Command horizontal control mode	F.A.2.1.2.TL1	Loss of TRC Control Mode (with or without annunciation to the pilot)	ALL	Catastrophic
	F.A.2.1.2.MF1	Erroneous TRC control	ALL	Catastrophic
	F.A.2.1.2.MF2	Erroneous TRC engagement	ALL	Catastrophic
Provide Flight Management:				

Function	FC #	Failure Condition (Hazard Description)	Flight Phase	Classification
Provide Path Following Control Mode	F.N.2.3.TL2	Loss of Lateral Path Following Control Mode during flight without annunciation to the pilot	F	Hazardous
	F.N.2.3.TL3	Loss of Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	T, L	Catastrophic
	F.N.2.3.MF2	Erroneous Lateral Path Following Control Mode without annunciation to the pilot	F	Hazardous
	F.N.2.3.MF3	Erroneous Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	T, L	Catastrophic
	F.N.2.3.MF5	Uncommanded engagement of Lateral Flight Path Control Mode during flight	ALL	Catastrophic
	F.N.2.3.TL5	Loss of Vertical Path Following Control Mode during flight without annunciation to the pilot	F	Hazardous
	F.N.2.3.TL6	Loss of Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	T, L	Catastrophic
	F.N.2.3.MF7	Erroneous Vertical Path Following Control Mode without annunciation to the pilot	F	Hazardous
	F.N.2.3.MF8	Erroneous Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot)	T, L	Catastrophic
	F.N.2.3.MF10	Uncommanded engagement of Vertical Flight Path Control Mode during flight	ALL	Catastrophic
Provide Emergency Geospatial Control Modes:	F.N.2.4.3.TL2	Loss of collision avoidance not annunciated to the pilot	ALL	Catastrophic (Note 1)

Function	FC #	Failure Condition (Hazard Description)	Flight Phase	Classification
Provide airborne vehicle collision avoidance	F.N.2.4.3.MF2	Collision avoidance activation with erroneous avoidance maneuver (legitimate collision threat detected)	ALL	Catastrophic
	F.N.2.4.3.MF3	Collision avoidance activation without annunciation to the pilot (legitimate collision threat detected)	ALL	Catastrophic

Note 1 – Assumes probability of collision is 1 (Table 22, ASMP 13)

Editor's Note: For an actual vehicle certification project, each of the AFHA failure conditions would be developed in their entirety. The example system definition herein is developed only to the level of detail necessary to support the goals of the study.

B.5 AFHA Worksheets

The AFHA worksheets are shown on the following pages.

Functional Hazard Assessment						
Function	Provide Translation Rate Command horizontal control mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.A.2.1.2.TL1	Loss of TRC Control Mode (with or without annunciation to the pilot)	T1, T2, T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to inceptor commands causing inability to control flight path. B) Pilot unable to control vehicle. Loss of vehicle with pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	ASMP 1

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Translation Rate Command horizontal control mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.A.2.1.2.TL2	Loss of TRC Control Mode availability in cruise annunciated to the pilot	F	A) Vehicle will not be able to transition from forward flight to hover/TRC mode. Unable to perform vertical landing B) Pilot will need to land at alternate airfield suitable for forward flight landing C) No effect	IV	ASA/SSA	ASMP 1 ASMP 16

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Translation Rate Command horizontal control mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.A.2.1.2.MF1	Erroneous TRC control	T1, T2, T3; L1, L2	A) Vehicle Vx, Vy velocities not consistent with inceptor inputs causing inability to control flight path. B) Pilot unable to control vehicle. Loss of vehicle with pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	ASMP 1 ASMP 2

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Translation Rate Command horizontal control mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.A.2.1.2.MF2	Erroneous TRC engagement	ALL	A) Vehicle control incompatible with current flight control mode, particularly in transition to forward flight and forward flight. Vehicle loss of control. Hull loss. B) Pilot unable to control vehicle. Loss of vehicle with pilot fatality. C) Passenger fatalities	I	ASA/SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL1	Loss of Lateral Path Following Control Mode during flight with annunciation to the pilot	F	A) Vehicle loss of control to lateral flight path. Vehicle may exceed lateral flight path constraints. B) Pilot disengages PATH mode and maneuvers vehicle back to lateral path. C) No effect	IV	ASA/SSA	ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment

Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL2	Loss of Lateral Path Following Control Mode during flight without annunciation to the pilot	F	A) Vehicle flight path exceeds established lateral flight path control limits. Vehicle may “miss” destination. Vehicle may encroach upon other aircraft or structures. Collision avoidance maneuver may activate. B) Significant increase in pilot workload due to either collision avoidance activation or non-arrival at destination. Potential pilot injury due to getting “lost” and requiring possible off-airport landing. C) Potential occupant injuries due to possible off-vertiport landing.	II	ASA/SSA	ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL3	Loss of Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot) (*)	T, L	A) Vehicle flight path exceeds established lateral flight path control limits. Potential hull loss. B) Pilot must quickly disengage PATH mode and maneuver vehicle back to lateral path. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	ASMP 10 ASMP 14 ASMP 15 (*) due to low altitude failure, no credit taken for annunciation to the pilot

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF1	Erroneous Lateral Path Following Control Mode during flight with annunciation to the pilot	F	A) Vehicle flight path may exceed established lateral path control limits. B) Pilot disengages PATH mode and maneuvers vehicle back to lateral path. C) No effect	IV	ASA/SSA	ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF2	Erroneous Lateral Path Following Control Mode without annunciation to the pilot	F	A) Vehicle flight path may exceed established lateral flight path control limits. Vehicle may "miss" destination. Vehicle may encroach upon other aircraft or structures. Collision avoidance maneuver may activate. B) Significant increase in pilot workload due to either collision avoidance activation or non-arrival at destination. Potential pilot injury due to getting "lost" and requiring possible off-airport landing. C) Potential occupant injuries due to possible off-vertiport landing.	II	ASA/SSA	ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF3	Erroneous Lateral Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot) (*)	T, L	A) Vehicle flight path exceeds established lateral flight path control limits. Possible hull loss. B) Pilot must quickly disengage PATH mode and maneuver vehicle back to lateral path. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	ASMP 10 ASMP 14 ASMP 15 (*) due to low altitude failure, no credit taken for annunciation to the pilot

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF4	Erroneous Lateral Flight Path deviation annunciation to the pilot when no deviation exists	ALL	A) No effect B) Increase in pilot workload due to: - determine reason for (erroneous) annunciation - additional pilot effort to monitor NAV performance in absence of automation C) No effect	III	ASA/SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF5	Uncommanded engagement of Lateral Flight Path Control Mode during flight (*)	ALL	A) Vehicle follows unintended flight path. Possible hull loss. B) Pilot unable to control vehicle flight path. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	(*) Worst case uncommanded engagement presumes pilot inability to disengage

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL4	Loss of Vertical Path Following Control Mode during flight with annunciation to the pilot	F	A) Vehicle loss of control to Vertical flight path. Vehicle may exceed Vertical flight path constraints. B) Pilot disengages PATH mode and maneuvers vehicle back to Vertical path. C) No effect)	IV	ASA/SSA	ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL5	Loss of Vertical Path Following Control Mode during flight without annunciation to the pilot	F	A) Vehicle flight path exceeds established Vertical flight path control limits. Vehicle may "miss" destination. Vehicle may encroach upon other aircraft or structures. Collision avoidance maneuver may activate. B) Significant increase in pilot workload due to either collision avoidance activation or non-arrival at destination. Potential pilot injury due to getting "lost" and requiring possible off-airport landing. C) Potential occupant injuries due to possible off-vertiport landing.	II	ASA/SSA	ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.TL6	Loss of Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot) (*)	T, L	A) Vehicle flight path exceeds established Vertical flight path control limits. Potential hull loss. B) Pilot must quickly disengage PATH mode and maneuver vehicle back to Vertical path. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	ASMP 10 ASMP 14 ASMP 15 (*) due to low altitude failure, no credit taken for annunciation to the pilot

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF6	Erroneous Vertical Path Following Control Mode during flight with annunciation to the pilot	F	A) Vehicle flight path may exceed established Vertical path control limits. B) Pilot disengages PATH mode and maneuvers vehicle back to Vertical path. C) No effect	IV	ASA/SSA	ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF7	Erroneous Vertical Path Following Control Mode without annunciation to the pilot	F	A) Vehicle flight path may exceed established Vertical flight path control limits. Vehicle may “miss” destination. Vehicle may encroach upon other aircraft or structures. Collision avoidance maneuver may activate. B) Significant increase in pilot workload due to either collision avoidance activation or non-arrival at destination. Potential pilot injury due to getting “lost” and requiring possible off-airport landing. C) Potential occupant injuries due to possible off-vertiport landing.	II	ASA/SSA	ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	FC Class	Cert Approach	Remarks/ Justification
F.N.2.3.MF8	Erroneous Vertical Path Following Control Mode during takeoff/landing flight phase (with or without annunciation to the pilot) (*)	T, L	A) Vehicle flight path exceeds established Vertical flight path control limits. Potential hull loss. B) Pilot must quickly disengage PATH mode and maneuver vehicle back to Vertical path. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	ASMP 10 ASMP 14 ASMP 15 (*) due to low altitude failure, no credit taken for annunciation to the pilot

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF9	Erroneous Vertical Flight Path deviation annunciation to the pilot when no deviation exists	ALL	A) No effect B) Increase in pilot workload due to: - determine reason for (erroneous) annunciation - additional pilot effort to monitor NAV performance in absence of automation C) No effect	III	ASA/SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Path Following Control Mode					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.3.MF10	Uncommanded engagement of Vertical Flight Path Control Mode during flight (*)	ALL	A) Vehicle follows unintended flight path. Potential hull loss. B) Pilot unable to control vehicle flight path. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	(*) Worst case uncommanded engagement presumes pilot inability to disengage

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Airborne Vehicle Collision Avoidance					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.4.3.TL1	Loss of collision avoidance function annunciated to the pilot	ALL	A) Vehicle unable to detect and respond to impending collision. B) Increased workload due to required monitoring for external threats. C) No effect	III	ASA/SSA	ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Airborne Vehicle Collision Avoidance					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.4.3.TL2	Loss of collision avoidance function not annunciated to the pilot	ALL	A) Vehicle is unable to annunciate to the pilot collision warnings, and is unable to automatically maneuver from an impending collision. Potential hull loss. B) Potential pilot injury or fatality if collision occurs. C) Potential passenger injures or fatalities if collision occurs.	I	ASA/SSA	ASMP 13 ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Airborne Vehicle Collision Avoidance					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.4.3.MF1	Erroneous collision avoidance activation	ALL	A) Vehicle performs collision avoidance maneuver where no collision threat exists. B) Significant increase in workload to determine cause of erroneous warning/activation C) Potential passenger injuries	III	ASA/SSA	ASMP 12 ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Airborne Vehicle Collision Avoidance					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.4.3.MF2	Collision avoidance activation with erroneous avoidance maneuver (legitimate collision threat detected)	ALL	A) Vehicle maneuvers such that threat is not avoided resulting in significant reduction of safety margins and potential collision resulting in hull loss B) Significant pilot workload to identify and avoid collision. Potential pilot fatality if collision occurs. C) Potential passenger fatalities if collision occurs	I	ASA/SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Functional Hazard Assessment						
Function	Provide Airborne Vehicle Collision Avoidance					**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**FC Class**	**Cert Approach**	**Remarks/ Justification**
F.N.2.4.3.MF3	Collision avoidance activation without annunciation to the pilot (legitimate collision threat detected)	ALL	A) Vehicle maneuvers to avoid threat B) Pilot not aware of why activation occurred. Pilot may try and counter collision avoidance maneuver resulting in significant reduction in safety margins. Possible collision and pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	ASMP 14

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise	F5:	L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

Appendix C. Baseline Aircraft System Functional Hazard Assessments

C.1 SFHA Introduction

This document presents the System Functional Hazard Assessment (SFHA) for the eCRM-001 aircraft. It is derived from the Aircraft Functional Hazard Assessment (AFHA) in Appendix B and unless otherwise stated, the assumptions used are the same as the referenced AFHA.

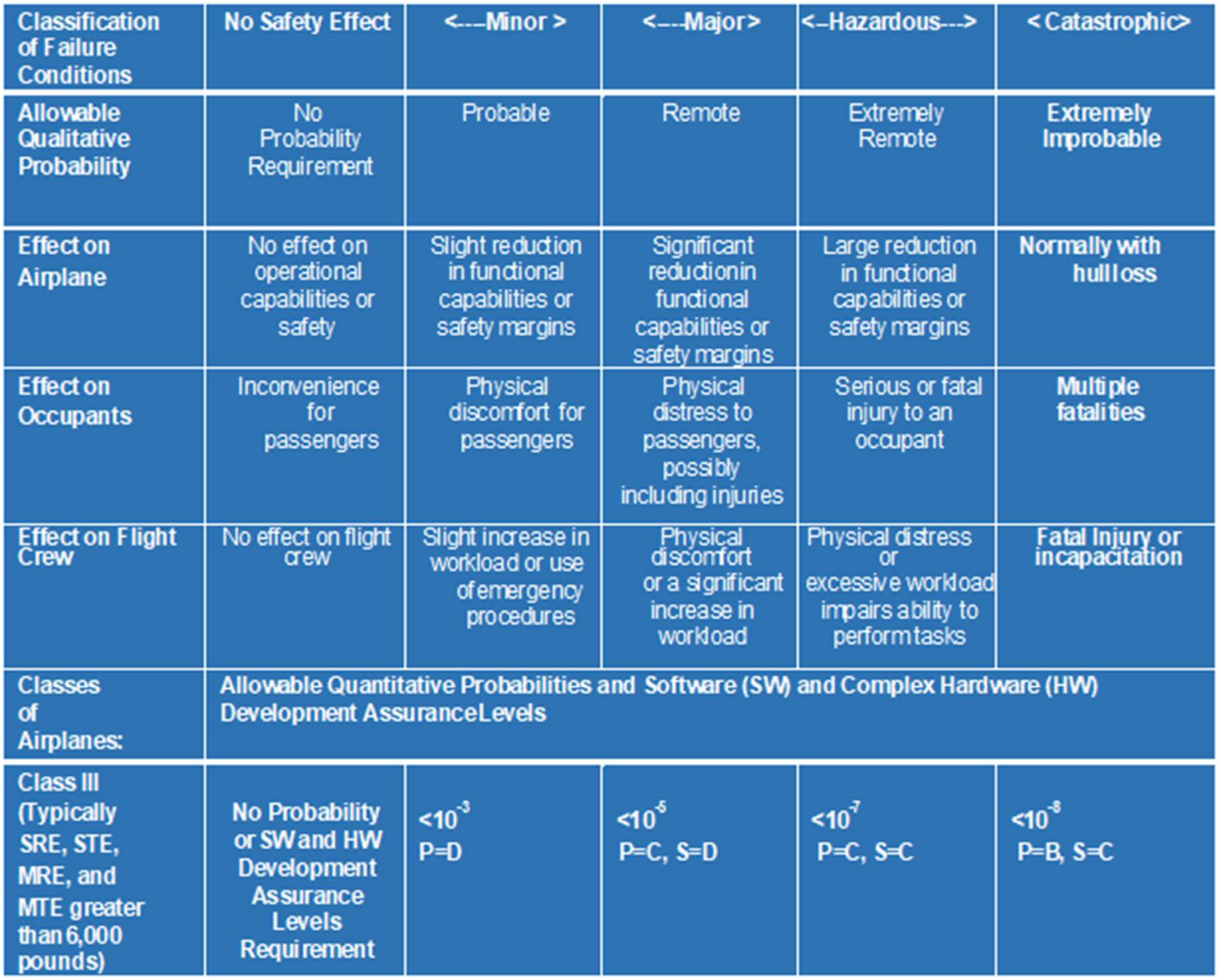
C.1.1 Applicable Safety Objectives used for the SFHA

The applicable safety objectives used for the SFHA for the eCRM-001 aircraft are derived from a combination of FAA advisory circular AC 23.1309-1E and SAE ARP4754A.

AC 23.1309-1E provides the safety effects, classifications, failure probabilities and required development assurance levels of the various part 23 aircraft classes. The eCRM-001 is assumed to be designated as a Class III aircraft.

Supporting the selection of safety objectives used in Table 24 for FDAL Assignment from AC 23.1309-1E. In the table, P stands for Primary system and S stands for Secondary system.

Table 24. Class III Aircraft Design Assurance Levels versus Severity of Failure Condition (extract from AC 23-1309-1E)



Classification of Failure Conditions	No Safety Effect	<---Minor >	<---Major>	<--Hazardous--->	< Catastrophic>
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely Remote	Extremely Improbable
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reductionin functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development AssuranceLevels				
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ P=D	$<10^{-5}$ P=C, S=D	$<10^{-7}$ P=C, S=C	$<10^{-8}$ P=B, S=C

The above tables are consulted to define the top level design assurance levels for the functions analyzed. During the allocation process of functions to software elements (subfunctions and items), the safety analysis process identifies groups of subfunctions and items which can contribute to each top level functional hazard. These groupings are referred to as "Functional Failure Sets" (FFS) in ARP 4754A, and each subfunction and/or item is referred to as a "member" of each set. Within a FFS, ARP 4754A allows a reduction in the DAL to individual members of the set so long as specific conditions are assured:

- Each member contributes to the top level event (that is, the top level hazard is realized only when all members of the set have "failed") and
- Each member is independent of the other members (that is, a single (common) failure or error cannot cause all members of the FFS to fail or become erroneous causing the top level hazard to occur)

The analysis may identify multiple Functional Failure Sets for each top level hazard. For example, the analysis may determine two causes leading to a top level hazard:

1. Software item A erroneous and Software item B erroneous or;
2. Subfunction C failure and Software item D erroneous.

In this example, there are two Functional Failure Sets, (1) Software Item A and Software Item B, and separately (2) Subfunction C and Software Item D. Note that subfunction C may consist of multiple additional software items.

In the above examples, ARP 4754A may allow a reduction in subfunction and item DALs from the corresponding top level DAL; for example, subfunctions and items may be reduced to level D for top level DAL B hazards (note that the reduction in DAL to level D differs with AC23.1309-1E which only allows a reduction in DAL to level C for this case).

If it cannot be shown that the required independence exists, then no DAL reduction is allowed for the members.

Refer to ARP 4754A for more detailed guidance.

C.1.2 SFHA Scope

Although typically each aircraft system is assessed separately for all the affected functions and subfunctions and produced as a standalone document, this particular SFHA will be a combined SFHA for the dominant affected systems for the three (3) subfunctions being assessed. These are the “Provide Translation Rate Command Horizontal Control Mode” subfunction, the “Provide Path Following Control Mode” subfunction and the “Provide Airborne Vehicle Collision Avoidance” subfunction.

This particular combo SFHA is completed for navigation, flight control and display systems for “Provide Translation Rate Command Horizontal Control Mode”. For “Provide Path Following Control Mode” subfunction the combo SFHA was done for the navigation and flight control systems. For the “Provide Airborne Vehicle Collision Avoidance” it is done for the navigation system.

C.1.3 SFHA Overview

This Appendix presents the failure identification matrix and worksheets as would be done for a traditional SFHA. It additionally provides the notes and observations that are pertinent to interpreting the assessment and its derived safety requirements and FDALs and subsequent IDALs, as well as providing design considerations, as appropriate.

As the AFHA provides the failure hazard assessment at the aircraft level, the SFHA provides the failure hazard assessment at the system level. The functions/subfunctions assessed are the same as the aircraft level, but again applied at the system level as opposed to the aircraft level. The functions/subfunctions are assessed for each of the affected systems. As such, the architecture needs to progress sufficiently to identify the systems on the aircraft as well as the relationships (inputs and outputs –signal flow) to each other and their internal logic and computations. In this way the assessment can be performed in a thorough manner and to all systems affected in their individual way.

Bear in mind that in this step of the process (SFHA), the systems architecture needs to be developed as appropriate, but the further development of breaking the systems into Line Replaceable Units (LRUs) and quantity of LRUs is a next step considering the total requirements (operational, performance, maintenance, etc.) as well as the safety requirements (from the assigned FDALs, which lead to IDALs, and the derived safety requirements from the hazard assessments. These tend to be refined during the PSSA process and fault trees.

C.1.4 SHFA Process

As stated, the function list is carried over from AFHA. Each sub-function to be assessed at the system level, has a common "name "from the function list, same as for the AFHA in the worksheets. That is how the linkage is provided for the assessment. Architecturally, the system block diagram for which the sub-function is implemented is used to identify and assess the failures, again using the same assumptions as in the AFHA. A separate assessment for each applicable system (flight control, navigation and display) is performed. Each system block is assessed, looking at its inputs, its outputs and logic/computations for the particular sub-function. Following are the system block diagrams used for the three (3) subfunctions, and descriptions of the boundaries used for the assessments.

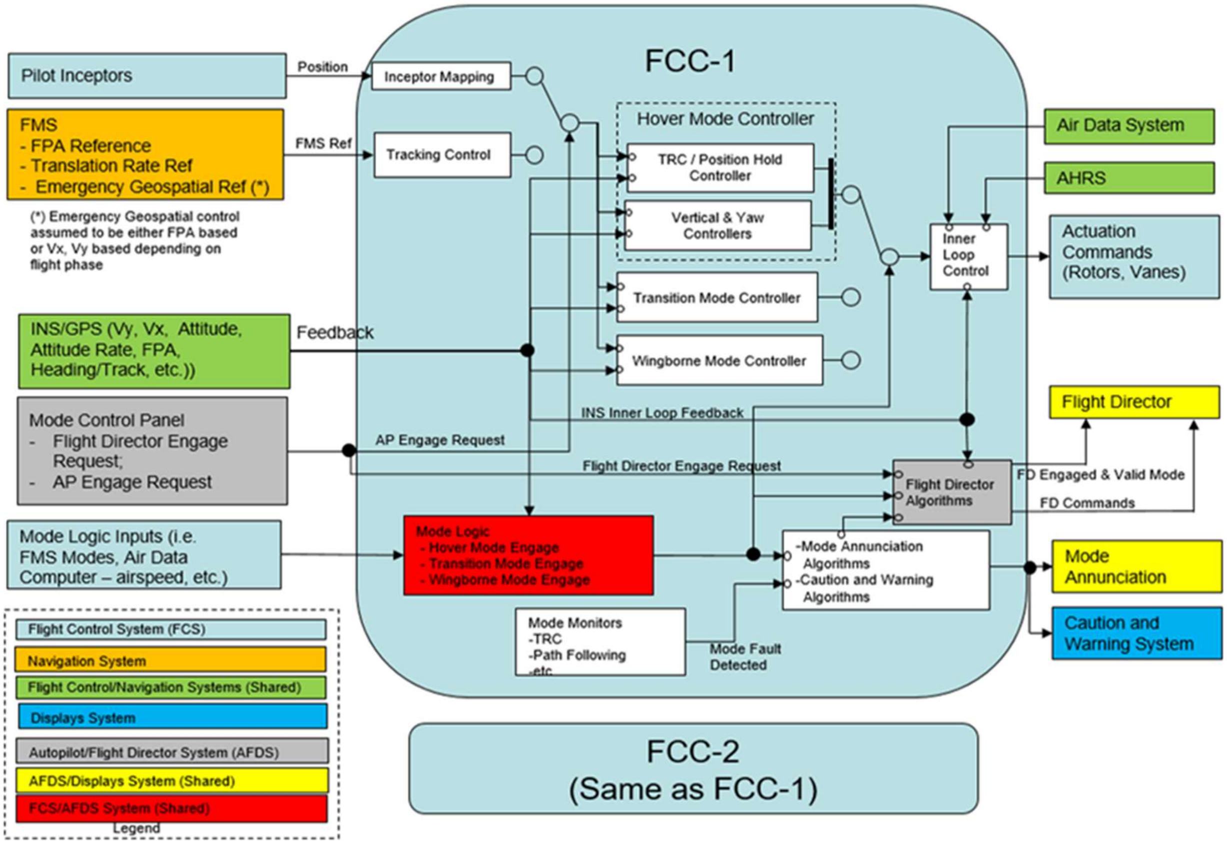
Definitions for the pertinent blocks are as follows:

- Flight Path Command (mode controller) – Accepts outputs from tracking control or from the pilot inceptors and provides the pitch/roll/yaw attitude and rate to the inner loop control needed to achieve those tracking control or pilot inceptor outputs. This is a computational block in the flight control computer.
- Tracking Control – Accepts reference velocities, altitude, and heading from Waypoint Control. Its inputs are actual vehicle state information and it outputs a longitudinal acceleration, flight path angle, heading rate, and beta command to the Flight Path Command (mode controller) block. This is a computational block in the flight control computer.
- Path Generator – provides a series of waypoints to follow a defined flight plan/path from departure to destination. Waypoints are entered by the pilot (or uplinked from a ground station). The path generator provides a "smoothed spatial path with a corresponding velocity profile". This is a computational block in the flight management computer.
- Waypoint Control–computes and outputs desired longitudinal and lateral velocities, target altitude, and heading reference needed to arrive at the next waypoint to flight controls, from the various means of providing a navigation flight path. This is a computational block in the flight management computer.
- DRP Monitor– continuously monitors the vehicle for any threats from air to air collisions or air to ground collisions, and switches the flight plan accordingly to dynamic reactive planning (collision avoidance path), after first allowing a short time for a pilot override. This is a computational block within the flight management computer.
- Dynamic Reactive Planning– continuously computes a 4D path from the vehicle's current location that will avoid any pending air to air or air to ground threats. Defined as a computational block within the flight management computer
- Pilot Override– allows the pilot to override a collision avoidance maneuver.
- Air to Air Surveillance Sensors - group of sensors capable of detecting air to air threats and providing information to assist in the degree of the threat. This would include both cooperative and uncooperative aircraft. Today examples are TCAS/ACAS, Mode S transponders, ADS-B.

- Air to Ground Surveillance Sensors - group of sensors capable of detecting air to ground threats (such as buildings) and providing information to assist in the degree of the threat. Today examples are LADAR, radar and synthetic vision.

C.1.4.1 Provide Translation Rate Command Horizontal Control Mode Process

The boundary of the assessment for the “Provide Translation Rate Command Horizontal Control Mode”, subfunction is from external sensors (FMS, INS, etc.) up to the input to the FCC inner loop (note that the inner loop is common to all flight control modes and is assumed would be separately assessed). Refer to Figure 55.



FCC-1
Pilot Inceptors
Position
Inceptor Mapping
FMS
- FPA Reference
- Translation Rate Ref
- Emergency Geospatial Ref (*)
FMS Ref
Tracking Control
(*) Emergency Geospatial control assumed to be either FPA based or Vx, Vy based depending on flight phase
Hover Mode Controller
TRC / Position Hold Controller
Vertical & Yaw Controllers
Transition Mode Controller
Wingborne Mode Controller
Air Data System
AHRS
Inner Loop Control
Actuation Commands (Rotors, Vanes)
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Feedback
INS Inner Loop Feedback
Mode Control Panel
- Flight Director Engage Request;
- AP Engage Request
AP Engage Request
Flight Director Engage Request
Flight Director
Flight Director Algorithms
FD Engaged & Valid Mode
FD Commands
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
-Mode Annunciation Algorithms
-Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
Mode Monitors
-TRC
-Path Following
-etc
Mode Fault Detected
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)
Legend
FCC-2
(Same as FCC-1)

Figure 55. Functional Block Diagram for Provide Translation Rate Command Horizontal Control Mode

C.1.4.2 Provide Path Following Control Mode Process

Refer to Figure 56 for the “Provide Path Following Control Mode” subfunction. The assessment is predominantly for “Tracking Control” (as it computes the path error) within the FCC, along with its inputs (FMS, INS) and mode logic and annunciations. Since its output to the “Flight Path Command” function is also within the FCC, it is not separately analyzed for this subfunction.

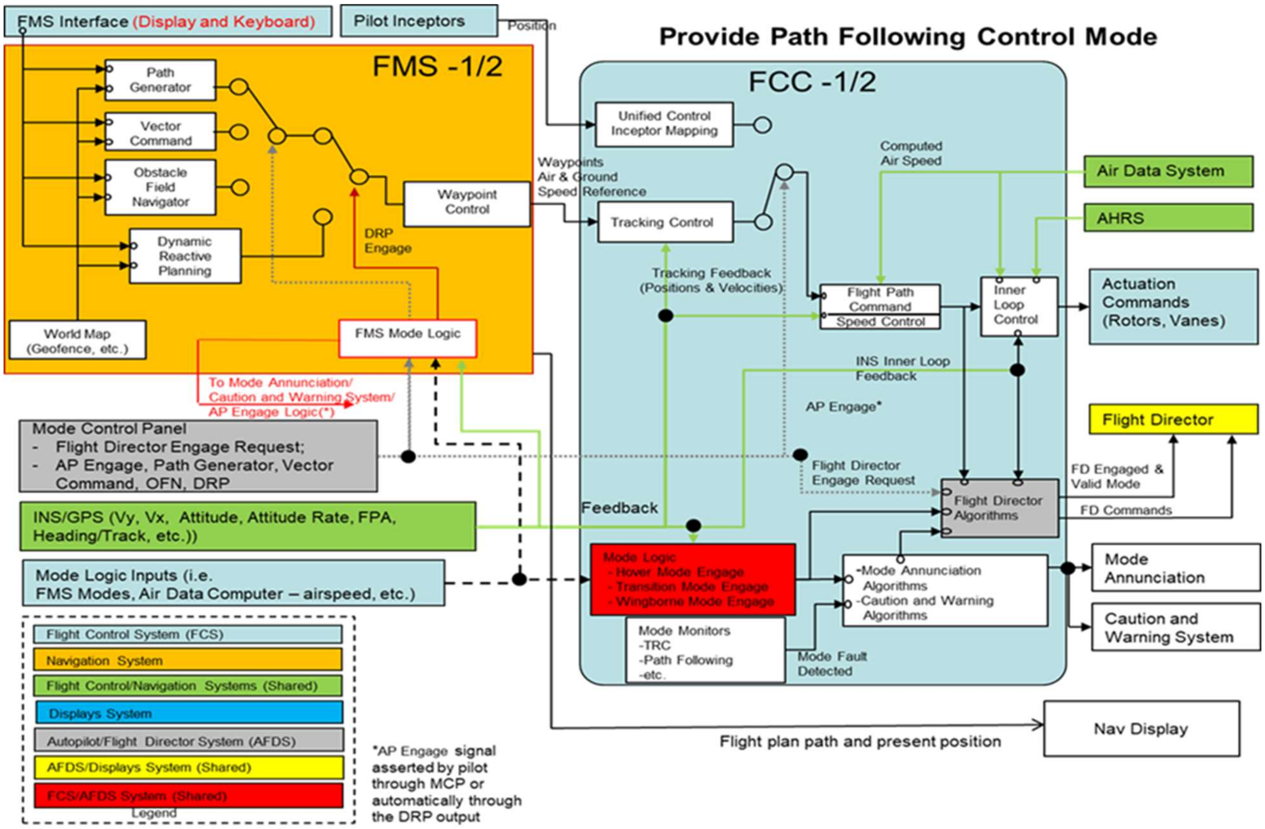
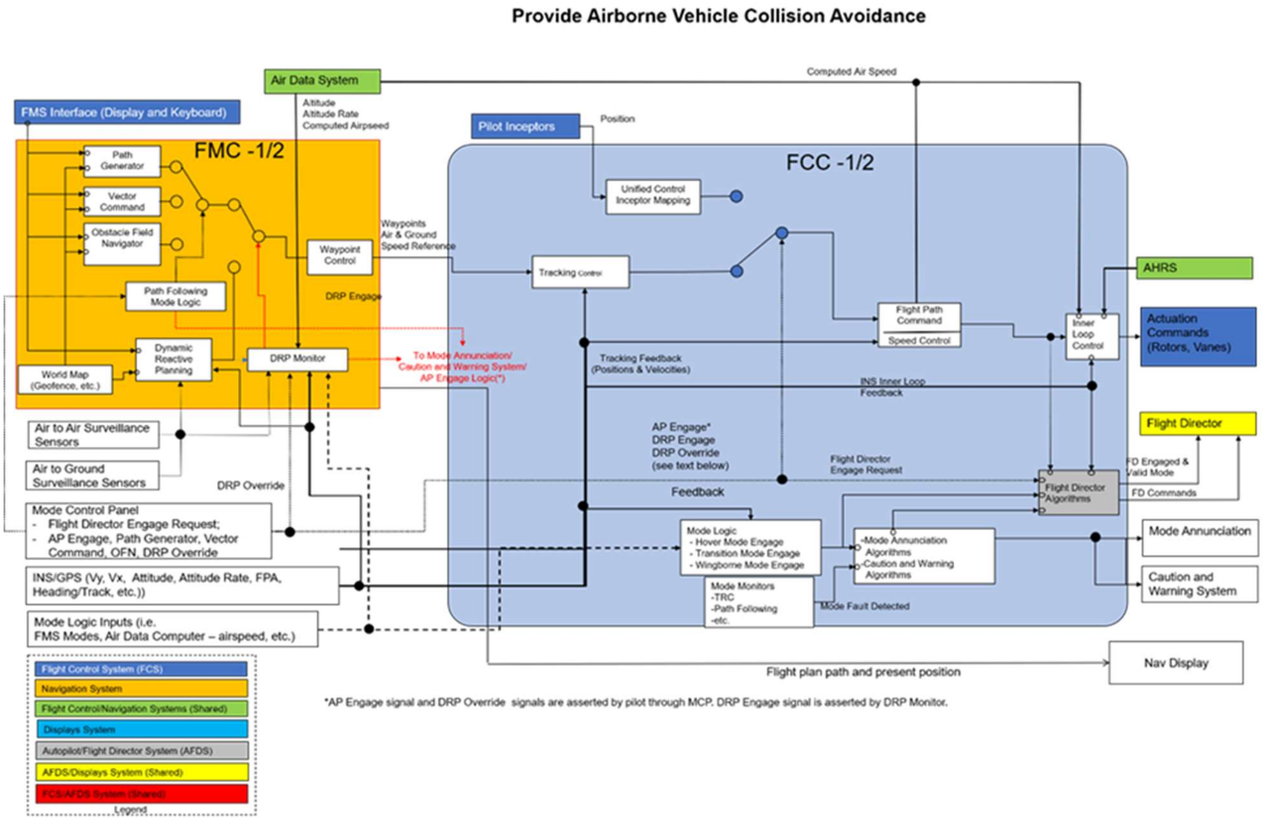

FMS Interface (Display and Keyboard)
Pilot Inceptors
Position
Provide Path Following Control Mode
FMS -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Dynamic Reactive Planning
World Map (Geofence, etc.)
Waypoint Control
DRP Engage
FMS Mode Logic
To Mode Annunciation/ Caution and Warning System/ AP Engage Logic(*)
FCC -1/2
Unified Control Inceptor Mapping
Waypoints Air & Ground Speed Reference
Tracking Control
Computed Air Speed
Air Data System
AHRS
Tracking Feedback (Positions & Velocities)
Flight Path Command
Speed Control
Inner Loop Control
Actuation Commands (Rotors, Vanes)
INS Inner Loop Feedback
AP Engage*
Flight Director
Flight Director Engage Request
FD Engaged & Valid Mode
Flight Director Algorithms
FD Commands
Mode Control Panel
- Flight Director Engage Request;
- AP Engage, Path Generator, Vector Command, OFN, DRP
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Feedback
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
-Mode Annunciation Algorithms
-Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
Mode Monitors
-TRC
-Path Following
-etc.
Mode Fault Detected
Flight plan path and present position
Nav Display
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)
Legend
*AP Engage signal asserted by pilot through MCP or automatically through the DRP output

Figure 56. Functional Block Diagram for Provide Path Following Control Mode

C.1.4.3 Provide Airborne Vehicle Collision Avoidance Process

For the “Provide Airborne Vehicle Collision Avoidance” the assessment is done for dynamic reaction planning (DRP) and the DRP monitor within the navigation system, including sensor inputs as well as the computations, as they monitor real time threats and decide when and how to provide a collision avoidance maneuver. The flight control system is not included as the inputs from waypoint control within the navigation system to the flight control system is the same, as other navigation planning systems. Refer to Figure 57.


Provide Airborne Vehicle Collision Avoidance

Air Data System
Altitude
Altitude Rate
Computed Airpseed
Computed Air Speed
FMS Interface (Display and Keyboard)
FMC -1/2
Path Generator
Vector Command
Obstacle Field Navigator
Path Following Mode Logic
Waypoint Control
Waypoints
Air & Ground
Speed Reference
DRP Engage
Dynamic Reactive Planning
World Map (Geofence, etc.)
DRP Monitor
To Mode Annunciation/
Caution and Warning System/
AP Engage Logic(*)
Air to Air Surveillance Sensors
Air to Ground Surveillance Sensors
DRP Override
Mode Control Panel
- Flight Director Engage Request;
- AP Engage, Path Generator, Vector Command, OFN, DRP Override
INS/GPS (Vy, Vx, Attitude, Attitude Rate, FPA, Heading/Track, etc.))
Mode Logic Inputs (i.e. FMS Modes, Air Data Computer – airspeed, etc.)
Pilot Inceptors
Position
FCC -1/2
Unified Control Inceptor Mapping
Tracking Control
Flight Path Command
Speed Control
Inner Loop Control
AHRS
Actuation Commands (Rotors, Vanes)
Tracking Feedback
(Positions & Velocities)
INS Inner Loop Feedback
AP Engage*
DRP Engage
DRP Override
(see text below)
Flight Director Engage Request
Feedback
Flight Director
FD Engaged & Valid Mode
FD Commands
Flight Director Algorithms
Mode Logic
- Hover Mode Engage
- Transition Mode Engage
- Wingborne Mode Engage
Mode Monitors
-TRC
-Path Following
-etc.
Mode Fault Detected
-Mode Annunciation Algorithms
-Caution and Warning Algorithms
Mode Annunciation
Caution and Warning System
Nav Display
Flight plan path and present position
Flight Control System (FCS)
Navigation System
Flight Control/Navigation Systems (Shared)
Displays System
Autopilot/Flight Director System (AFDS)
AFDS/Displays System (Shared)
FCS/AFDS System (Shared)
Legend

*AP Engage signal and DRP Override signals are asserted by pilot through MCP. DRP Engage signal is asserted by DRP Monitor.

Figure 57. Functional Block Diagram for Provide Airborne Vehicle Collision Avoidance

The failure identification matrix is created to identify the failures (total loss, partial loss or malfunction), with reference numbers assigned to be used in the worksheets. The worksheets are then created for each identified failure, with effects of the failure on the aircraft, crew and passengers, by flight phase. This assessment is then reviewed against the AFHA failure to ensure consistency and coverage. FDALs may be assigned at this level, as well as derived safety requirements; this process is utilized here, for clarity.

As a note, it is then the safety requirements (not the hazard assessment) which are traced throughout the development program to ensure that the design implemented and verified adheres to the defined safety.

The process is iterative and may be updated based on PSSA.

C.2 Failure Assessment

The failure assessment is against the same vehicle and operation as the AFHA, except at the system level. As such not repeated here are the vehicle description, flight phase profile, and failure condition classifications as they are defined in the AFHA developed in Appendix A.

C.2.1 Failure Identification Matrix Description

Postulated failure condition descriptions are captured for Total Loss of function, Partial Loss of Function and Malfunction (erroneous operation) of Function, for each affected system.

Table 25. FCS.1 Provide Flight Control Modes (Hover)

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
FCS.1	Provide Flight Control Modes (Hover)			
FCS.1.1	Provide Translation Rate Command horizontal control mode	**FCS.1.1.TL1** Loss of (left/right) hand inceptor (control of Vx, Vy, Vz velocities in manual flight) **FCS.1.1.TL2** Loss of FCC TRC mode during takeoff or landing due to loss of or incorrect mode logic inputs (prematurely exits TRC mode to another mode): **FCS.1.1.TL3** Loss of FCC TRC control computational capability causes loss of TRC function **FCS.1.1.TL4** Loss of Autopilot during takeoff or landing with annunciation to the pilot **FCS.1.1.TL5** Loss of Autopilot during takeoff or landing not annunciated to the pilot **FCS.1.1.TL6** Loss of FCC TRC mode availability in during cruise annunciated to the pilot **FCS.1.1.TL7** Loss of FCC flight director data while in manual flight **FCS.1.1.TL8** Inability to disengage autopilot	-	**FCS.1.1.MF1** Erroneous (left/right) inceptor position outputs **FCS.1.1.MF2** Erroneous FCC TRC control computational capability causes incorrect TRC control **FCS.1.1.MF3** Erroneous FCC flight director display output while in manual flight **FCS.1.1.MF4** Erroneous FCC mode annunciation computation during takeoff or landing **FCS.1.1.MF5** Erroneous TRC engagement **FCS.1.1.MF6** Inadvertent/erroneous autopilot engagement (system not yet providing valid guidance commands to autopilot/pilot not expecting autopilot engagement)

		FCS.1.1.TL9 Inability to engage autopilot		

Table 26. FCS.2 Provide Flight Control Modes (Path Following)

FCS.2	Provide Flight Control Modes (Path Following)			
FCS.2.1	Provide Path Following Control Mode	**FCS.2.1.TL1** Detected/annunciated loss of waypoint data (failure is in FCC) **FCS.2.1.TL2** Undetected/un-annunciated loss of waypoint data (failure is in FCC) **FCS.2.1.TL3** Loss of waypoint data with or without detection/annunciation to the pilot (failure is in FCC) **FCS.2.1.TL4** Detected/annunciated loss of INS data to Tracking Controller **FCS.2.1.TL5** Undetected/unannunciated loss of INS data to Tracking Controller **FCS.2.1.TL6 Loss** of INS data to Tracking Controller with or without detection/annunciation to the pilot **FCS.2.1.TL7** Detected/annunciated loss of Path Mode (Mode logic error) **FCS.2.1.TL8** Undetected/un-annunciated loss of Path Mode (Mode logic error) **FCS.2.1.TL9** Loss of Path Mode (FCC path mode disengages) with or without detection/annunciation to the pilot	-	**FCS.2.1. MF1** Detected and annunciated erroneous waypoint data (failure is in FCC) **FCS.2.1. MF2** Undetected/unannunciated erroneous waypoint data (failure is in FCC) **FCS.2.1. MF3** Erroneous waypoint data with or without detection/annunciation to the pilot (failure is in FCC) **FCS.2.1. MF4** Detected/annunciated erroneous feedback data from INS to tracking controller **FCS.2.1. MF5** Undetected/un-annunciated erroneous feedback data from INS to tracking controller **FCS.2.1. MF6** Erroneous feedback data from INS to tracking controller with or without detection/annunciation to the pilot **FCS.2.1. MF7** Tracking Control algorithm calculates erroneous outer loop control data detected/annunciated **FCS.2.1. MF8** Tracking Control algorithm calculates erroneous outer loop control data undetected/un-annunciated **FCS.2.1. MF9** Tracking Control algorithm calculates erroneous outer loop control data with or without detection/annunciation to the pilot

Table 27. FCS.3 Provide Emergency Geospatial Control Modes

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
FCS.3	Provide Emergency Geospatial Control Modes			
FCS.3.1	Provide airborne vehicle collision avoidance ** Not analyzed for this study	**	-	**

Table 28. NAV.1 Provide Flight Management

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
NAV.1	Provide Flight Management			
NAV.1.1	Provide Translation Rate Command horizontal control mode	**NAV.1.1.TL1** Loss INS/GPS feedback signals to TRC controller causes loss of TRC function **NAV.1.1.TL2** Loss of FMS TRC mode annunciated to the pilot **NAV.1.1.TL3** Loss of FMS TRC mode not annunciated to the pilot **NAV.1.1.TL4** Loss of INS/GPS feedback signals in cruise causes loss of TRC function availability. Loss of TRC availability is annunciated to the pilot.	-	**NAV.1.1. MF1** Erroneous INS/GPS feedback signals to TRC controller causes incorrect TRC control **NAV.1.1. MF2** Undetected erroneous FMS generated flight path references cause incorrect TRC control **NAV.1.1. MF3** Detected erroneous FMS generated flight path references cause incorrect TRC control **NAV.1.1. MF4** Erroneous FMS TRC path bias applied due to erroneous inceptor outputs.

Table 29. NAV.2 Provide Flight Management

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
NAV.2	Provide Flight Management			
NAV.2.2	Provide Path Following Control Mode	**NAV.2.1.TL1** Detected loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS) **NAV.2.1.TL2** Undetected/un-annunciated loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS) **NAV.2.1.TL3** Loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS) with or without detection/annunciation to the pilot	-	**NAV.2.1. MF1** Uncommanded Path Mode engagement **NAV.2.1. MF2** Detected erroneous Path Generation/Waypoint Control data (FMS detects its own fault and flags data as invalid on the bus; uncommanded annunciated mode change in FMS **NAV.2.1. MF3** Undetected/un-annunciated erroneous Path Generation/Waypoint Control data **NAV.2.1. MF4** Erroneous Path Generation/Waypoint Control data with or without detection/annunciation to the pilot

Table 30. NAV.3 Provide Emergency Geospatial Control Modes

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
NAV.3	Provide Emergency Geospatial Control Modes			

NAV.3.1	Provide airborne vehicle collision avoidance	NAV.3.1.TL1 Loss of DRP Monitor (threat detection capability) due to external sensor failure or FMS input failure detected/annunciated NAV.3.1.TL2 Loss of DRP Monitor (threat detection capability) due to external sensor failure or FMS input failure, undetected/unannunciated NAV.3.1.TL3 Loss of DRP Monitor (threat detection capability) due to DRP Monitor computation failure detected/annunciated NAV.3.1.TL4 Loss of DRP Monitor (threat detection capability) due to DRP Monitor computation failure undetected/un-annunciated		NAV.3.1. MF1 Erroneous DRP Monitor/Planner -non-existent threat detected or -Actual threat detected but avoidance guidance erroneous due to undetected/un-annunciated senor of computation failure

Table 31. DSP.1 Provide Flight Control Modes (Hover)

ID #	Airplane Function	Total Loss	Partial Loss	Malfunction
DSP.1	Provide Flight Control Modes (Hover)			
DSP.1.1	Provide Translation Rate Command horizontal control mode	**DSP.1.1.TL1** Loss of flight director display while in manual flight annunciated **DSP.1.1.TL2** Loss of TRC mode annunciation (TRC still engaged)	-	**DSP.1.1.MF1** Erroneous flight director display while in manual flight (also unannunciated loss of flight director) **DSP.1.1.MF2** Erroneous mode annunciation during takeoff or landing (TRC mode engaged) **DSP.1.1.MF3** Loss of autopilot disengage warning
DSP.2.1	Provide Path Following Control Mode ** Not analyzed for this study	**	**	**
DSP 3	Provide Emergency Geospatial Control Modes			

DSP.3.1	Provide airborne vehicle collision avoidance **Not analyzed for this study	**	-	**

C.3 SFHA Observations and Notes

C.3.1 Provide Translation Rate Command Horizontal Control Mode

C.3.1.1 FDAL Assignment

FDAL assignment for the TRC controller is level B, since the TRC failure is catastrophic (Part 23 Class III aircraft).

C.3.1.2 IDAL Assignment

Item development assurance levels are presented in the SFHA tables using the terminology "DAL (C, B) equivalent". The intent is to present the top level functional DAL requirement (FDAL), from which it may be possible to assign corresponding FDALs for the (sub-)functions, and IDALs for the items, taking into account architectural mitigation per ARP4754A (see section 1.1). Final IDAL assignments are determined after requirements are allocated to software configuration items with corresponding software functions (input processing, monitors, control laws, etc.).

C.3.1.3 Single Point Failures and Mitigation Considerations

Since TRC loss or malfunction is catastrophic, no single fault shall cause loss of or erroneous TRC control (AC 23.1309-1E). Single faults can occur when one of the two INS/GPS systems fails undetected (i.e., monitors detect an unflagged mis-compare between redundant INS/GPS inputs). It is assumed INS ground speed inputs are used in the control laws and that the GPS ground speed inputs update rate is too slow for it to be used. Also a single loss can occur if a single installed FMS has an undetected FMS failure. Single flight director display can have erroneous flight director in manual flight or guidance contrary to autoflight.

Options to mitigate single faults are for the TRC to either be fail-operative or have an alternate mode available in case of TRC failure. The fail-operative case would be triple redundant INS/GPS and dual self-monitored (dual lane) FMS and FCC.

The pilot uses flight director guidance to perform manual vertical landings or to monitor the automation in TRC mode. A single flight director display may represent a single fault risk (display is a single fault). One can assume a minimally trained pilot will mitigate erroneous flight director (flight in VMC only) and therefore it may be possible to reduce the flight director hazard to class II or even III. This is dependent on how much training a minimally trained pilot would have. Another option for mitigation is to implement independent lateral and vertical displacement and "excess displacement" from path warnings.

C.3.2 Provide Path Following Control Mode

For flight phases other than cruise, the path following mode, needs to remain fully operational after a single failure (loss of, or erroneous, Path Following mode catastrophic in this flight phase). This would typically mean dual fully monitored FMSs, dual fully monitored FCCs and triple INS. In addition to an RTA monitor in the tracking controller in the FCC, there may be an opportunity for single (fully monitored) FMS if an RTA backup to the path generation portion of the path following mode is available. This assumes that the RTA backup is independent of primary mode. Loss of both the primary and the RTA backup to the path generation portion of the path following function would need to be shown to be less that 10e-8. Since loss of the path generation portion of the path following mode also means loss of navigation capability (since loss of waypoint data is included in the SFHA as a cause for loss of path generation), then the path generation subfunction itself must be deemed non-critical; that is, not required for continued safe flight and landing. This “non-critical” designation may not be needed if the RTA backup mode is capable of performing the navigation task, but this implies some means of recovering presumably lost or corrupted waypoint data.

Bear in mind that the assumption of “Minimally Trained Pilot” does lead to more severe hazard classifications for some failures than for pilot with exceptional piloting skills.

C.3.3 Provide Airborne Vehicle Collision Avoidance

For airborne vehicle collision avoidance, the main two components are in the navigation system: the first being a monitor to determine if a collision or threat is imminent and the second being the maneuver required to avoid the collision. The pilot is also given a means to override the collision avoidance automatic maneuver if the pilot deems prudent.

There are two lines of defense. The first line of defense is the flight plan itself which considers the geo-fence and possibly other cooperative aircraft’s flight plans. The second line of defense is the collision avoidance imminent threat detection. Sophisticated real-time sensors are needed to provide the necessary information for both air-to-air threats and air-to-ground threats for this detection and avoidance.

The FMS needs to be high integrity (example com/mon architecture) to mitigate errors. The sensor sets additionally will need some form of error mitigation, including common cause. As long as the pilot is deemed to be able to take over the collision detection and avoidance, in case of loss of function in the navigation system, there are no redundancy requirements for availability of the FMS.

Note that this is a very complex function as it requires the ability for sensors to provide this information error free, with full airspace coverage around the vehicle, and the ability to assess multiple threats simultaneous or in sequence. Also, the pilot override logic has additional complexities, as it needs to consider how to ignore legitimate threats involving other aircraft, especially considering minimally trained pilots.

There is a potential issue with the sophistication/complexity of the sensor package, especially its implementation and resultant threat detection computations. The concern is centered on whether it can meet DO-178/DO-254 standards for DAL B due to the technology involved.

C.4 SFHA Worksheets and Descriptions

This section summarizes the failure effects and their associated severity classifications. Again, the assumptions used (ASMP) in the remarks Column 7 are documented in Appendix B.3.5 and not repeated here. Typically, each assessment document would have its own assumptions, but for the purposes of this task study, they are documented in one place. Any text italicized in Column 2 are just examples to help provide insights with the failure condition and any text italicized in column 7 are provided as added clarifications giving what derived requirements could mitigate the failure and some design insights into how the derived requirements could be implemented. In addition, FDALs assigned for the class I, II and III hazards, are consistent with the safety objectives from Section C.1.1.

C.4.1 Translation Rate Command SFHA Worksheets

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL1	Loss of (left/right) hand inceptor (control of Vx, Vy. Vz velocities in manual flight) - *Open wiring* - *Loss of sensor excitation* - *Electrical/mechanical failure of the sensor* - *Mechanical connection between inceptor and inceptor position sensor break*	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to pilot control inputs causing inability to control flight path B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	*Derived Requirement –* *Triple redundant, electrically and mechanically isolated, position sensors for each axis, with in line and comparison monitoring sufficient to isolate a single failed sensor.* *Triplex inceptor monitors FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.MF1	Erroneous (left/right) inceptor position outputs - *Open or shorted inceptor sensor wiring* - *EMI* - *Jammed inceptor (Foreign Object Debris - FOD)*	T1-T3; L1, L2	A) Vehicle does not provide correct Vx, Vy velocity references to pilot control inputs causing inability to control flight path B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	*Derived Requirement -* *Triple redundant, electrically and mechanically isolated, position sensors for each axis, with in line and comparison monitoring sufficient to isolate a single failed sensor.* *Triplex inceptor monitors FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	***Failure Condition (Hazard)***	***Flight Phase***	***Effect of Failure on:*** ***A) Aircraft*** ***B) Crew*** ***C) Occupants***	**Hazard Class**	***Cert Approach***	***Remarks/ Justification***
FCS.1.1.TL2	Loss of FCC TRC mode during takeoff or landing due to loss of or incorrect mode logic inputs (prematurely exits TRC mode to another mode): - *Air Data System* - *Ground speed* - *FCC mode logic computations*	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to inceptor/FMS commands causing inability to control flight path B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	ASMP 1 *Derived Requirement – sufficient redundancy needed for mode logic inputs to meet hazard class* *Redundant FCCs* *Dual lane FCCs with cross lane mode monitoring and reversion to remaining FCC or to back up RTA mode such as ACAH* *Monitors and mode logic FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL3	Loss of FCC TRC control computational capability causes loss of TRC function	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to inceptor/FMS commands causing inability to control flight path B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	ASMP 1 *Derived Requirement – Redundant FCCs* *Dual lane FCCs with cross lane monitoring and reversion to remaining FCC* *FDAL level B equivalent for monitor and TRC controller*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL4	Loss of Autopilot during takeoff or landing with annunciation to the pilot	T1-T3; L1, L2	A) Loss of Autopilot control B) Pilot to recognize loss of autopilot and assume manual control C) No effect	IV	ASA/SSA	ASMP 7 *Autopilot availability FDAL D equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Control System	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.1.1.TL5	Loss of Autopilot during takeoff or landing not annunciated to the pilot	T1-T3; L1, L2	A) Potential damage or vehicle loss due to uncontrolled landing B) Pilot may not recognize loss of automatic control. Potential pilot injury/fatality C) Potential passenger injuries/fatalities	I	ASA/SSA	ASMP 14 *Derived Requirement – redundant and independent autopilot disengage warning* *FDALB equivalent for disengage logic and annunciation*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL8	Inability to disengage autopilot	T1-T3; L1, L2	A) Potential hull loss depending on reason for pilot attempting to disengage autopilot. B) Potential pilot fatality C) Potential passenger injuries/fatalities	I	ASA/SSA	ASMP 14 *Derived Requirement – At least two independent autopilot disengage means* *FDAL B equivalent for disengage logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.MF6	Inadvertent/erroneous autopilot engagement (system not yet providing valid guidance commands to autopilot/pilot not expecting autopilot engagement)	T1-T3; L1, L2	A) Potential hull loss due to incorrect autopilot control B) Potential pilot confusion leading to fatality due to erroneous autopilot control or efforts to override autopilot commands C) Potential passenger injuries/fatalities	I	ASA/SSA	ASMP 14 *Derived Requirement –* *dual independent autopilot engage means* *FDAL B equivalent for autopilot engage logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL9	Inability to engage autopilot	T1-T3; L1, L2	A) No effect B) Pilot observes lack of engagement and continues manually controlled flight C) No effect	IV	ASA/SSA	*Autopilot availability FDAL D equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.MF2	Erroneous FCC TRC control computational capability causes incorrect TRC control	T1-T3; L1, L2	A) Vehicle follows erroneous flight path causing potential collisions/collision avoidance activation/ loss of vehicle. B) Potential high pilot workload/pilot injury/fatality C) Potential passenger injuries/fatalities	I	ASA/SSA	ASMP 1 *Derived Requirement – Redundant FCCs* *Dual lane FCCs with cross lane monitoring and reversion to remaining FCC* *FDAL B equivalent for monitor and reversion logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL6	Loss of FCC TRC mode availability in cruise annunciated to the pilot* - *FCC input receiver failure* - *FCC Input sensor receiver failure* - *FCC computational failure*	F1-F4	A) Vehicle will not be able to transition from forward flight to hover/TRC mode. Unable to perform vertical landing. B) Pilot recognizes annunciation and plans landing at alternate airfield suitable for forward flight landing. C) No effect	III	ASA/SSA	ASMP 1 (*) for un-annunciated failure, refer to mode loss during TO/Landing phase Cruise TRC mode availability FDAL C equivalent

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.TL7	Loss of FCC flight director data while in manual flight	T1-T3; L1, L2	A) No effect B) Pilot loses manual guidance cues resulting in increase in workload to perform own navigation and avoidance for the geo fence/other structures. Note that pilot must monitor navigation data to avoid geo fence and structure. C) No effect	III	ASA/SSA	ASMP 7 *Flight Director availability FDAL C equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Control System	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.1.1.MF3	Erroneous FCC flight director display output while in manual flight	T1-T3; L1, L2	A) Potential loss of vehicle due to pilot following incorrect guidance B) Pilot may follow incorrect guidance into a hazardous condition (collision or landing at extreme attitude). Possible pilot injury/fatality. C) Possible passenger injury/fatality	I	ASA/SSA	ASMP 14 *Derived Requirement – dual lane redundant FCC flight directors with cross lane monitoring and reversion to remaining FCC* *Note – "No single fault" rule may preclude having a single flight director display installed.* *Need secondary lateral/longitudinal displacement display independent of FD cues* *FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment

System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.MF4	Erroneous FCC mode annunciation computation during takeoff or landing	T1-T3; L1, L2	A) Potential damage due to hard or out of envelope landing. B) Pilot confusion with respect to actual engaged mode. Potential pilot injury/fatality C) Possible passenger injury/fatality	I	ASA/SSA	ASMP 1 *Derived Requirement – Redundant FCCs* *Dual lane FCCs with cross lane monitoring and reversion to remaining FCC* *FDAL B equivalent for monitor and reversion logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Control System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.1.1.MF5	Erroneous TRC engagement	ALL	A) Vehicle control incompatible with current flight mode, particularly in transition to forward flight and forward flight. Vehicle loss of control. Hull loss. B) Pilot unable to control vehicle. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	*Derived Requirement – Redundant FCCs* *Dual lane FCCs with cross lane monitoring and reversion to remaining FCC* *FDAL B equivalent for monitor and reversion logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.1.1.TL 1	Loss INS/GPS feedback signals to TRC controller causes loss of TRC function	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to inceptor/FMS commands causing inability to control flight path B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	ASMP 1 *Derived Requirement – sufficient redundancy needed for INS/GPS feedback to meet hazard class* *Monitoring to detect loss of feedback signals* *FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.1.1.TL2	Loss of FMS TRC mode annunciated to the pilot	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to FMS commands causing inability to control flight path B) Pilot observes loss of FMS TRC mode annunciation and reverts to manual TRC control via inceptors. Slight increase in pilot workload. C) No effect	IV	ASA/SSA	ASMP 7 ASMP 14 *FMS TRC Mode availability FDAL D equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Navigation	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.1.1.TL 3	Loss of FMS TRC mode not annunciated to the pilot	T1-T3; L1, L2	A) Vehicle does not provide Vx, Vy velocity control to FMS commands causing inability to control flight path B) Pilot to recognize effects of failure (loss of control). Pilot may not be relied upon to effectively mitigate the failure if it occurs at low altitude, or if recognized late in the approach. This may cause hard landing/loss of vehicle with potential pilot injury/fatality. C) Potential passenger injuries/fatalities.	I	ASA/SSA	ASMP 14 *Derived Requirement –* *(1) Redundant failure detection (i.e., dual lane FMS)* *(2) Dual independent fault annunciation paths* *FDAL B equivalent (Annunciation path and monitor)*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Navigation	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.1.1. TL4	Loss of INS/GPS feedback signals in cruise causes loss of TRC function availability. Loss of TRC availability is annunciated to the pilot.	F1-4	A) Vehicle will not be able to transition from forward flight to hover/TRC mode. Unable to perform vertical landing. B) Pilot recognizes annunciation and plans landing at alternate airfield suitable for forward flight landing. C) No effect	III	ASA/SSA	ASMP 1 *Refer to **NAV.1.1.TL1** for FDAL rationale (loss during takeoff/landing)*

OPERATIONAL FLIGHT PHASES (Col. 3)

<u>GROUND</u>	<u>TAKEOFF</u>	<u>INFLIGHT</u>		<u>LANDING</u>
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.1.1.MF 1	Erroneous INS/GPS feedback signals to TRC controller causes incorrect TRC control - *Feedback signals fail to 0, max range values or other incorrect values*	T1-T3; L1, L2	A) Vehicle Vx, Vy velocities not consistent with inceptor/FMS references causing inability to control flight path. Potential loss of vehicle. B) Pilot unable to control vehicle, Loss of vehicle with potential pilot fatality C) Potential passenger fatalities	I	ASA/SSA	ASMP 1; ASMP 2 *Derived Requirement – sufficient redundancy needed for INS/GPS feedback to meet hazard class (triple redundant allows voting out a failed GPS); Dual redundant with reversionary mode to ACAH (RTA) – using AHRS (AHRS att/att rates monitored with INS)* *FDAL B equivalent for monitors and reversionary logic*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.1.1.MF 2	Undetected erroneous FMS generated flight path references cause incorrect TRC control	T1-T3; L1, L2	A) Vehicle follows erroneous flight path causing potential collisions/collision avoidance activation/ loss of vehicle. B) Potential high pilot workload/pilot injury/fatality C) Potential passenger injuries/fatalities	I	ASA/SSA	*Derived Requirement – need to validate flight plan entry. Once validated, protect with CRC.* *Redundant or dual lane FMS to monitor FMS command outputs resulting from flight plan.* *Flight plan entry validation level B equivalent* *Monitor of flight plan integrity command monitors need to be FDAL B equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Navigation	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.1.1.MF 3	Detected erroneous FMS generated flight path references cause incorrect TRC control	T1-T3; L1, L2	A) For detected failure, vehicle reverts to manual TRC control. B) Potential high pilot workload due to reversion to manual TRC mode. Potential pilot injury for low altitude failure resulting in hard landing or go around C) Potential passenger injuries	III	ASA/SSA	*Derived Requirement – need to validate flight plan entry. Once validated, protect with CRC.* *Redundant or dual lane FMS to monitor FMS command outputs resulting from flight plan.* *FMS data monitor and fault reaction DAL level C equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.1.1.PL1	Loss of ability of the pilot to bias the FMS TRC path when needed due to loss of either inceptor	T1-T3; L1, L2	A) Vehicle follows programmed flight path despite pilot efforts to modify the flight path. Vehicle follows path not intended. B) Pilot may erroneously disengage FMS resulting in loss of control of vehicle. Potential pilot fatality. C) Potential passenger injuries/fatalities	I	ASA/SSA	*Derived Requirement – Triple redundant, electrically and mechanically isolated, position sensors for each axis, with in line and comparison monitoring sufficient to isolate a single failed sensor* *FDAL B equivalent for the triplex monitoring and inceptor voting logic.*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Navigation	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.1.1.MF 4	Erroneous FMS TRC path bias applied due to erroneous inceptor outputs.	T1-T3; L1, L2	A) Vehicle does not follow programmed flight path. Possible collision with other vehicles/structure. Possible loss of vehicle. B) Potential pilot fatality C) Potential passenger injuries/fatalities	I	ASA/SSA	*Derived Requirement – Triple redundant, electrically and mechanically isolated, position sensors for each axis, with in line and comparison monitoring sufficient to isolate a single failed sensor.* *FDAL B equivalent for the triplex monitoring and inceptor voting logic.*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Display System	Function	Provide Translation Rate Command Horizontal Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
DSP.1.1.TL1	Loss of flight director display while in manual flight annunciated	T1-T3; L1, L2	A) No effect B) Pilot loses manual guidance cues resulting in increase in workload to perform own navigation and avoidance for the geo fence/other structures. Note that pilot must monitor navigation data to avoid geo fence and structure. C) No effect	III	ASA/SSA	ASMP 7 *For landing, assume visual landing (no landing aids other than outside visual reference to vertiport)* *Flight Director availability FDAL C equivalent*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Display System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
DSP.1.1.MF1	Erroneous flight director display while in manual flight (also unannunciated loss of flight director)	T1-T3; L1, L2	A) Potential loss of vehicle due to pilot following incorrect guidance B) Pilot may follow incorrect guidance into a hazardous condition (collision or landing at extreme attitude). Possible pilot injury/fatality. C) Possible passenger injury/fatality	I	ASA/SSA	ASMP 14 *Derived Requirement – Redundant independent FCC inputs to displays with comparison monitor in the displays system from input to display output.* *FDAL B equivalent for display resident monitor and FD Fail logic/annunciation* *Need secondary lateral/longitudinal displacement display independent of FD cues*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Display System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
DSP.1.1.TL2	Loss of TRC mode annunciation (TRC still engaged)	T1-T3; L1, L2	A) Potential damage due to hard or out of envelope landing. B) Pilot confusion with respect to actual engaged mode. Pilot may or may not recognize TRC is still engaged with loss of annunciation. Potential pilot injury/fatality C) Possible passenger injury/fatality	I	ASA/SSA	ASMP 14 *Derived Requirement – Redundant independent FCC inputs to displays with independent comparison monitor in the displays system from input to display output.* *FDAL B equivalent for displays resident monitor and FD Fail logic/annunciation*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Display System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
DSP.1.1.MF2	Erroneous mode annunciation during takeoff or landing (TRC mode engaged)	T1-T3; L1, L2	A) Potential damage due to hard or out of envelope landing. B) Pilot confusion with respect to actual engaged mode. Potential pilot injury/fatality C) Possible passenger injury/fatality	I	ASA/SSA	ASMP 14 *Derived Requirement – Redundant independent FCC inputs to displays with comparison monitor in the displays system from input to display output.* *FDAL B equivalent for displays resident monitor and mode annunciation*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Display System**	**Function**	**Provide Translation Rate Command Horizontal Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
DSP.1.1.MF3	Loss of autopilot disengage warning	T1-T3; L1, L2	A) Loss of vehicle control if the autopilot disengages without warning the pilot. Potential hull loss B) Potential pilot injury/fatality if pilot does not assume manual control C) Possible passenger injuries/fatalities	I	ASA/SSA	ASMP 14 *Derived Requirement – Dual independent disengage annunciations/warnings* *FDAL B equivalent for disengage warning*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

C.4.2 Path Following Mode SFHA Worksheets

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.2.1.TL1	Detected/annunciated loss of waypoint data (failure is in FCC)	F2	A) No effect assuming pilot intervenes upon loss of mode B) Pilot recognizes annunciation and intervenes to maintain vehicle in a safe state. Increase in pilot workload. Pilot navigates vehicle to destination. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

- CLASS I CATASTROPHIC
- CLASS II HAZARDOUS
- CLASS III MAJOR
- CLASS IV MINOR
- CLASS V NO EFFECT

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.2.1. MF1.	Detected and annunciated erroneous waypoint data (failure is in FCC)	F2	A) No effect assuming pilot intervenes upon loss of mode. Possible minor exceedance of path control limits B) Pilot recognizes annunciation and intervenes to maintain vehicle in a safe state. Increase in pilot workload. Pilot navigates vehicle to destination. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.2.1.TL2	Undetected/un-annunciated loss of waypoint data (failure is in FCC)	F2	A) Vehicle loses feedback data used in tracking control path calculations. Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene C) No effect	II	ASA/SSA	DAL C ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15 ASMP 17 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment

System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.MF2	Undetected/unannunciated erroneous waypoint data(failure is in FCC)	F2	A) Vehicle follows erroneous path. Possible significant reduction in safety margins. B) Pilot will need to use independent navigation means(visual/GPS/RNAV) to recognize departure from intended path and then intervene. C) No effect	II	ASA/SSA	DAL C ASMP4, 5, 6 ASMP 14, 15, 17, 18 ASMP 19, 20, 21 *Derived requirements:* 1. *FCC COM-MON architecture to mitigate failure to detect* 2. *Display function to receive independent waypoint data from FCC and FMS for monitoring/detection*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL3	Loss of waypoint data with or without detection/annunciation to the pilot (failure is in FCC)	F1, F3, F4, T1, T2, L1, L2	A) Vehicle flight path exceeds established flight path control limits. Potential hull loss. B) Pilot must quickly disengage PATH mode and maneuver vehicle back to the path. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	DAL B ASMP 3, 4, 5, 7 ASMP 10, 14, 15 ASMP 19, 20, 21 *Derived requirements:* 1. *FCC COM-MON architecture to mitigate failure to detect* 2. *Display function to received independent waypoint data from FCC and FMS for monitoring/detection*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF3	Erroneous waypoint data with or without detection/annunciation to the pilot (failure is in FCC)	F1, F3, F4, T1, T2, L1, L2	A) Vehicle follows erroneous path. Vehicle may encroach upon geo fence boundary resulting in collision with structures and loss of vehicle. B) Pilot will need to use independent navigation means(visual/GPS/RNAV) to recognized departure from intended path and then intervene. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	DAL B ASMP 3, 4, 5, 7 ASMP 10, 14, 15, 18 ASMP 19, 20, 21 *Derived requirements:* 1. *FCC COM-MON architecture to mitigate failure to detect* 2. *Display function to received independent waypoint data from FCC and FMS for monitoring/det ection*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

System Functional Hazard Assessment

System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL4	Detected/annunciated loss of INS data to Tracking Controller	F2	A) Aircraft no longer able to autonomously follow intended flight path B) Pilot to recognize annunciation and intervene. Significant increase in workload. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19 *Derived requirements:* *1. On loss of data, autonomy should revert to attitude hold mode*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF4	Detected/annunciated erroneous feedback data from INS to tracking controller	F2	A) Aircraft no longer able to autonomously follow intended flight path B) Pilot to recognize annunciation and intervene. Significant increase in workload. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.2.1.TL5	Undetected/unannunciated loss of INS data to Tracking Controller	F2	A) Vehicle loses feedback data used in tracking control path calculations. Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene C) No effect	II	ASA/SSA	DAL C ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15 ASMP 17 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
FCS.2.1. MF5	Undetected/un-annunciated erroneous feedback data from INS to tracking controller	F2	A) Vehicle flight path may exceed established flight path control limits. Vehicle may "miss" destination. Vehicle may encroach upon other aircraft or structures. Collision avoidance maneuver may activate. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Pilot may not recognize deviation on NAV display resulting in significant reduction in safety margins. C) Potential occupant injuries/fatalities	II	ASA/SSA	DAL C ASMP 4 ASMP 5 ASMP 6 ASMP 14 ASMP 15 ASMP 17 ASMP 18 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Flight Controls	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL6	Loss of INS data to Tracking Controller with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Vehicle loses feedback data used in tracking control path calculations. Vehicle will deviate from intended flight path. Vehicle may encroach upon geo fence boundaries resulting in potential loss of vehicle. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Failure to intervene may result in potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	DALB ASMP 3, 4, 5 ,7 ASMP 10, 14, 15 ASMP 19, 20, 21 No credit taken for DRP function *Derived requirements:* 1. *FCC COM-MON architecture to mitigate failure to detect* 2. *FCC INS monitor compares inputs from the dual INS's*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF6	Erroneous feedback data from INS to tracking controller with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Vehicle flight path exceeds established flight path control limits. Possible hull loss. B Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality Potential pilot fatality. C) Possible injuries and/or fatalities	I	ASA/SSA	DAL B ASMP 3, 4, 5, 7 ASMP 10, 14, 15, 18 ASMP 19, 20, 21 *Derived requirements:* 1. *FCC COM-MON architecture to mitigate failure to detect* 2. *FCC INS monitor compares inputs from the dual INS's*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL7	Detected/annunciated loss of Path Mode (Mode logic error)	F2	A) Aircraft no longer able to autonomously follow intended flight path B) Pilot to recognize annunciation and intervene. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL8	Undetected/un-annunciated loss of Path Mode (Mode logic error)	F2	A) Vehicle loses feedback data used in tracking control path calculations. Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene C) No effect	II	ASA/SSA	DAL C ASMP4 ASMP 5 ASMP 14 ASMP 15 ASMP 17 ASMP 19 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1.TL9	Loss of Path Mode (FCC path mode disengages) with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Vehicle will deviate from intended flight path. Vehicle may encroach upon geo fence boundary resulting in collision with structures and loss of vehicle. B Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	DAL B ASMP 3 ASMP 4 ASMP 5 ASMP 7 ASMP 10 ASMP 14 ASMP 15 ASMP 19 ASMP 20 ASMP 21 *Derived requirement(s):* 1. *FCC COM-MON architecture to mitigate failure to detect*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF7	Tracking Control algorithm calculates erroneous outer loop control data detected/annunciated	F2	A) Vehicle flight path may exceed established path control limits. B) Pilot disengages PATH mode and maneuvers vehicle back to the path. C) No effect	IV	ASA/SSA	DAL D ASMP 5 ASMP 6 ASMP 14 ASMP 15 ASMP 17 ASMP 18 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

CLASS I	CATASTROPHIC
CLASS II	HAZARDOUS
CLASS III	MAJOR
CLASS IV	MINOR
CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF8	Tracking Control algorithm calculates erroneous outer loop control data undetected/un-annunciated	F2	A) Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Significant increase in pilot workload. Pilot may not recognize deviation on NAV display resulting in significant reduction in safety margins. Possible pilot injury due to forced landing C) Potential occupant injuries due to possible off-vertiport landing	II	ASA/SSA	DAL C ASMP 4, 5, 6 ASMP 14 ASMP 15 ASMP 17 ASMP 18 ASMP 19 ASMP 20 ASMP 21 *Derived requirement(s):* 1. *FCC COM-MON architecture to mitigate failure to detect*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Flight Controls**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
FCS.2.1. MF9	Tracking Control algorithm calculates erroneous outer loop control data with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Vehicle flight path exceeds established flight path control limits. Possible hull loss B Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality Potential pilot fatality. C) Potential passenger injuries and/or fatalities	I	ASA/SSA	DAL B ASMP 3, 4, 5, 7 ASMP 10, 14, 15, 18 ASMP 19, 20, 21 *Derived requirement(s):* 1. *FCC COM-MON architecture to mitigate failure to detect*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.2.1.TL 1	Detected loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS)	F2	A) Aircraft no longer able to autonomously follow intended flight path. B) Pilot to recognize failure annunciation and intervene. Significant increase in workload. C) No effect	IV	ASA/SSA	DAL D ASMP 3 ASMP 7 ASMP 14 ASMP 17 ASMP 19

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment

System	Navigation	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.2.1. MF2	Detected erroneous Path Generation/Waypoint Control data (FMS detects its own fault and flags data as invalid on the bus; uncommanded annunciated mode change in FMS)	F2	A) Aircraft no longer able to autonomously follow intended flight path. B) Pilot to recognize failure annunciation and intervene. Significant increase in workload. C) No effect	IV	ASA/SSA	DAL D ASMP 14 ASMP 17 ASMP 19 FCC assumed to monitor FMS inputs and annunciate loss of FMS data

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	TAKEOFF	INFLIGHT		LANDING
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.2.1.TL 2	Undetected/un-annunciated loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS)	F2	A) Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Significant increase in pilot workload. Pilot may not recognize deviation on NAV display resulting in significant reduction in safety margins. C) Potential occupant injuries/fatalities	II	ASA/SSA	DAL C ASMP4 ASMP 5 ASMP 6 ASMP 14 ASMP 15 ASMP 17 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.2.1. MF3	Undetected/un-annunciated erroneous Path Generation/Waypoint Control data	F2	A) Vehicle will deviate from intended flight path. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Significant increase in pilot workload. Pilot may not recognize deviation on NAV display resulting in significant reduction in safety margins C) Potential occupant injuries/fatalities	II	ASA/SSA	DAL C ASMP 4, 5, 6 ASMP 14, 15, 17, 18 ASMP 19, 20, 21 *Derived requirement(s):* 1. *FMS COMMON architecture to mitigate failure to detect*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.2.1.TL 3	Loss of Path Generation/Waypoint Control data to FCC (e.g. due to data bus wiring failure, loss of power to FMS) with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Aircraft no longer able to autonomously follow intended flight path. Potential hull loss. B) Pilot to recognize failure annunciation and intervene. . Low altitude and late recognition may lead to unsafe maneuvers, collision with other vehicles/ground structure/hard landing. Possible pilot injury/fatality C) Possible injuries and/or fatalities	I	ASA/SSA	DAL B ASMP 3 ASMP 4 ASMP 5 ASMP 7 ASMP 10 ASMP 14 ASMP 15 ASMP 19 ASMP 20 ASMP 21

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Path Following Control Mode**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.2.1. MF4	Erroneous Path Generation/Waypoint Control data with or without detection/annunciation to the pilot	F1, F3, F4, T1, T2, L1, L2	A) Vehicle will deviate from intended flight path. Potential hull loss. B) Pilot to recognize departure from intended flight path by observing NAV display data and intervene. Significant increase in pilot workload. Pilot may not recognize deviation on NAV display resulting in significant reduction in safety margins. Possible pilot injury/fatality. C) Potential occupant injuries/fatalities	I	ASA/SSA	DAL B ASMP 3, 4, 5, 7 ASMP 10, 14, 15, 18 ASMP 19, 20, 21 *Derived requirement(s):* 1. *FMS COMMON architecture to mitigate failure to detect*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	Navigation	Function	Provide Path Following Control Mode			Rev Date:
1	2	3	4	5	6	7
Ref. No.	Failure Condition (Hazard)	Flight Phase	Effect of Failure on: A) Aircraft B) Crew C) Occupants	Hazard Class	Cert Approach	Remarks/ Justification
NAV.2.1. MF1	Uncommanded Path Mode engagement (*)	ALL	A) Vehicle follows unintended flight path. Potential hull loss. B) Pilot unable to control vehicle flight path. Potential pilot fatality. C) Potential passenger fatalities	I	ASA/SSA	DAL B (*) Worst case uncommanded engagement presumes pilot inability to disengage *Derived requirement:* *Dual lane COM/MON FMS or dual FMS (with FCC mode mismatch monitor)*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

C.4.3 Provide Airborne Vehicle Collision Avoidance SFHA Worksheets

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Airborne Vehicle Collision Avoidance**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.3.1.TL1	Loss of DRP Monitor/Planner (threat detection capability) due to external sensor failure or FMS input failure detected/annunciated	ALL	A) Aircraft no longer capable of detecting and avoiding collision threats B) Pilot required to visually scan outside cockpit to identify collision threats. Significant increase in workload. C) No effect	III	SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Airborne Vehicle Collision Avoidance**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.3.1.TL2	Loss of DRP Monitor/Planner (threat detection capability) due to external sensor failure or FMS input failure, undetected/unannunciated	ALL	A) Aircraft no longer capable of detecting and avoiding collision threats. Potential hull loss due to collision. B) Pilot unaware of loss of function. Significant reduction in safety margins as pilot may not recognize potential threats or recognize threat late resulting in significant pilot maneuver to avoid collision, or failure to avoid collision. Potential pilot fatality. C) Potential passenger fatalities.	I	SSA	ASMP 13 DAL B

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment

System	**Navigation**	**Function**	**Provide Airborne Vehicle Collision Avoidance**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.3.1.TL3	Loss of DRP Monitor/Planner (threat detection capability) due to DRP Monitor computation failure detected/annunciated	ALL	A) Aircraft no longer capable of detecting and avoiding collision threats B) Pilot required to visually scan outside cockpit to identify collision threats. Significant increase in workload. C) No Effect	III	SSA	

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment

System	**Navigation**	**Function**	**Provide Airborne Vehicle Collision Avoidance**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.3.1.TL4	Loss of DRP Monitor/Planner (threat detection capability) due to DRP Monitor computation failure undetected/un-annunciated	ALL	A) Aircraft no longer capable of detecting and avoiding collision threats. Potential hull loss due to collision. B) Pilot unaware of loss of function. Significant reduction in safety margins as pilot may not recognize potential threats or recognize threat late resulting in significant pilot maneuver to avoid collision, or failure to avoid collision. Potential pilot fatality. C) Potential passenger fatalities.	I	SSA	ASMP 13 DAL B *DR – FMS Com/Mon DRP monitor to detect this failure*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

System Functional Hazard Assessment						
System	**Navigation**	**Function**	**Provide Airborne Vehicle Collision Avoidance**			**Rev Date:**
1	**2**	**3**	**4**	**5**	**6**	**7**
Ref. No.	**Failure Condition (Hazard)**	**Flight Phase**	**Effect of Failure on:** **A) Aircraft** **B) Crew** **C) Occupants**	**Hazard Class**	**Cert Approach**	**Remarks/ Justification**
NAV.3.1.MF1	Erroneous DRP Monitor/Planner *Examples:* *-non-existent threat detected or* *-Actual threat detected but avoidance guidance erroneous* *due to undetected/un-annunciated sensor or computation failure*	ALL	A) Aircraft follows invalid collision avoidance guidance. Possible hull loss if erroneous guidance causes a collision. B) Pilot may not have the information required to assess the validity of the threat. Pilot will probably allow vehicle to execute the erroneous avoidance maneuver, which may create a collision hazard, resulting in possible pilot fatality. C) Potential passenger fatalities.	I	SSA	ASMP 14 DAL B *DR – FMS Com/Mon DRP monitor to detect this failure* *DR – redundant external sensors with common cause analysis of potential redundant sensor to eliminate common system faults or environmental conditions interfering with the sensors.*

OPERATIONAL FLIGHT PHASES (Col. 3)

GROUND	**TAKEOFF**	**INFLIGHT**		**LANDING**
G1: Taxi	T1: Break Ground to Hover	F1: Climb	F4: Go Around	L1: Transition-Fwd to Hover
	T2: Transition-Hover to Fwd	F2: Cruise		L2: Hover Descend to Ground
	T3: Rejected Takeoff	F3: Descent		

HAZARD CLASSIFICATIONS (Col. 5)

• CLASS I	CATASTROPHIC
• CLASS II	HAZARDOUS
• CLASS III	MAJOR
• CLASS IV	MINOR
• CLASS V	NO EFFECT

Appendix D. Baseline Aircraft System Theoretic Process Analyses

As described in Section 3.9 Systems Theoretic Process Analysis, the STPA analysis is conducted on multiple systems in the hierarchical model depicted in Figure 38. TRC is primarily analyzed in the tracking controller for the aircraft's hover mode configuration. However, unsafe control actions and loss scenarios are also developed for the flight path controller, and for the inner-loop control system.

Unsafe control actions are identified for each of the blue blocks in the STPA hierarchical control structure. In the case of the FMS, UCAs were identified for its sub-systems: path generator, DRP, and waypoint control. A UCA is a control action that will result in a hazard under worst-case environmental conditions. Identified UCAs were organized into tables where the row indicates the control variable and the column indicates the UCA's category.

Figure 39 shows a control loop for the TRC function along with corresponding loss scenarios at each input/output. Figures such as this were developed for each of the functions analyzed during the STPA process. For the sake of legibility, rather than including annotated control loops for each of the functions analyzed, in this Appendix we provide tabulated results for the UCAs and loss scenarios. As recommended by [Leveson 2018], we identified loss scenarios fitting the following cases:

- Scenarios that lead to unsafe control actions
  - Unsafe controller behavior
  - Causes of inadequate feedback and information
- Scenarios in which control actions are improperly executed or not executed
  - Scenarios involving the control path
  - Scenarios related to the controlled process

Note that both the identified UCAs and loss scenarios are intended to serve as examples and are not necessarily complete. This is why there are tables in which there is no identified loss scenario for each and every type of case listed above.

Table 32. Inner Loop Controller Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence	Stopping too soon, applying too long
Rotor Control Input	**UCA.ILC.1** Not providing (at all) will lead to loss of control and eventually all hazards in most flight regimes [H-1,2]	**UCA.ILC.2** Spinning up rotors at vertiport before passengers/crew are safely inside or away from aircraft [H-4] **UCA.ILC.3** Commanding rate that saturates or exceeds physical limits [H-2] **UCA.ILC.4** Spinning up when rotor is stowed for forward flight [H-2]	**UCA.ILC.20** Rotor commanded to stop before landing or before transitioning to forward flight [H-2]	**UCA.ILC.5** Stopped too soon during landing phase, leading to LOS [H-2] **UCA.ILC.6** Rotor spun up too long leading to instability or health issues at vertiport [H-2, H-4]
Surface Deflection Input	**UCA.ILC.7** Not changing surface configuration when current trajectory is leading to LOS (with terrain; with aircraft) [H-1, H-3] **UCA.ILC.8** Not changing surface configuration when transitioning to forward flight [H-2]	**UCA.ILC.9** Changing surface deflection when aircraft is near its operating limit, causing stall or over-speed [H-2] **UCA.ILC.10** Changing surface deflection when current trim and aircraft are in stable flight and clear trajectory [H-1,2,3] **UCA.ILC.11** Putting surfaces in forward flight regime during (near) vertical flight [H-2]	**UCA.ILC.12** Ibid w/r/t 20 above	**UCA.ILC.13** Otherwise safe surface input maintained until aircraft hits stall condition [H-2]
Surface & Rotor Input	**UCA.ILC.14** Not updating/changing rotor speed when surface deflections are modified (vice	**UCA.ILC.16** Updating/changing rotor & surface leading to	**UCA.ILC.18** Updating rotor & surface too late leading to unintended trajectory and loss of	**UCA.ILC.19** Stopping rotor rotation too soon resulting in loss of control [H-2]

	versa), initiating unstable flight [H-2] **UCA.ILC.15** Not updating/changing rotor & surface when current trajectory has terrain or other aircraft [H-1,3]	inappropriate aircraft attitude [H-2] **UCA.ILC.17** Updating/changing rotor & surface leading to or initiating path to collision [H-1,3]	safe separation with other aircraft or terrain / obstacles [H-1,3]	

Table 33. Flight Path Controller Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence	Stopping too soon, applied too long
Pitch / Roll / Yaw (PRY) Input *Hover Mode	**UCA.FPC.1** No command given when aircraft in hover dynamic situation, leading to loss of control [H-2] **UCA.FPC.2** No translational (or vertical) updates provided when current velocity profile is leading to collision [H-1,3] **UCA.FPC.3** No PRY commands given during transition leading to improper (no) blending [H-2]	**UCA.FPC.4** PRY command leads to translational rate near building or terrain [H-1] **UCA.FPC.5** PRY command leads to translational rate that will intercept with other aircraft trajectory [H-3] **UCA.FPC.6** PRY leads to combination of translational rates (side, fore/aft) that cannot be stably maintained [H-2]	**UCA.FPC.7** PRY commands started before dynamics hit hover configuration [H-2] **UCA.FPC.8** System not swapped to PRY after aircraft transitions to hover, leading to instability [H-2]	**UCA.FPC.9** PRY stopped too soon on approach, leading to loss of control [H-2] **UCA.FPC.10** PRY commands continued upon touchdown, leading to instability at aircraft/pad interface [H-2]
Pitch / Roll / Side-Slip (PRSS) Input *Forward Flight Mode	**UCA.FPC.11** See above but adjusted/inverted for forward flight	**UCA.FPC.12** Sideslip signal given when aircraft is not in a forward flight dynamic configuration [H-2]	**UCA.FPC.15** See above but adjusted/inverted for forward flight	**UCA.FPC.16** PRSS input applied too long during transition mode, leading to instability at hover [H-2]

		UCA.FPC.13 PRSS command given that inner loop control cannot track [H-2] **UCA.FPC.14** PRSS command given that results in trajectory that will conflict with other aircraft or objects [H-1,3]		
Rotor Input *Forward Flight Mode	**UCA.FPC.17** Lack of rotor command leads to inadequate authority and stall [H-2] **UCA.FPC.18** Lack of rotor stop command provided before stowage [H-4]	**UCA.FPC.19** Rotor inputs provided to rotors that are stowed [H-all] **UCA.FPC.20** Rotor input provided in improper environment (e.g. providing rotor when people are around at port)	**UCA.FPC.21** Rotor commands not updated to reflect change in flight dynamics [H-2]	**UCA.FPC.22** Rotors are stopped too soon before transitioning out of (into) hover flight [H-2]
Lifting Surface Control Input *Forward Flight Mode	**UCA.FPC.23** No command given results in stall and loss of control [H-2]	**UCA.FPC.24** Lifting surface control input leads to loss of control [H-2] **UCA.FPC.25** Command provided during hover flight [H-2]	**UCA.FPC.26** Lifting surface control applied too late, resulting in the aircraft stalling and loss of control [H-2]	**UCA.FPC.27** Lifting surface deflection stopped too soon resulting in stall and loss of control [H-2]

For the purposes of the examples below, the analysis was focused on the following types of hazards: Not Providing Causes Hazard, Providing Causes Hazard, Providing Too Soon/Late or Out of Sequence Causes Hazard. Hazards that may be caused by a control action stopping too soon or lasting too long are not considered and are omitted from the example tables below.

Table 34. TRC Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence

Velocity	**UCA.TRC.1** No command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3]	**UCA.TRC.2** Velocity command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3] **UCA.TRC.3** Velocity command given when in hover leads to rapid acceleration [H-4] **UCA.TRC.4** Command provided during wingborne flight [H-2] **UCA.TRC.5** Velocity command results in exceedance of flight envelope [H-2]	**UCA.TRC.6** Velocity command applied too late to avoid other aircraft or terrain/obstacle when in hover [H-1,3] **UCA.TRC.7** Command sent too late in the case that the aircraft has already switched to transition or wingborne mode [H-2]
Yaw Rate		**UCA.TRC.8** Yaw rate command given when in hover leads to rapid angular acceleration of the aircraft [H-4] **UCA.TRC.9** Command provided during wingborne flight [H-2]	**UCA.TRC.10** Command sent too late in the case that the aircraft has already switched to transition or wingborne mode [H-2]

Table 35. Wingborne Tracking Control Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence
Longitudinal Velocity	**UCA.TRC.11** No command given when in wingborne flight leads to aircraft flying too slow such that it stalls and there is loss of control [H-2] **UCA.TRC.12** No command given when in wingborne flight leads to	**UCA.TRC.13** Longitudinal velocity command given when in wingborne flight leads to aircraft flying too slow such that it stalls and there is loss of control [H-2] **UCA.TRC.14** Longitudinal velocity command given when in wingborne flight leads to aircraft flying too	**UCA.TRC.17** Longitudinal velocity command applied too late when in wingborne flight leads to loss of separation with other aircraft [H-1] **UCA.TRC.18** Command sent too late in the case that the aircraft has already

	aircraft flying too slow/fast and losing separation with other aircraft [H-1]	slow/fast and losing separation with other aircraft [H-1] **UCA.TRC.15** Longitudinal velocity command given when in wingborne flight leads to rapid acceleration [H-4] **UCA.TRC.16** Command provided during hover flight [H-2]	switched to transition or hover mode [H-2]
Flight Path Angle (FPA)	**UCA.TRC.19** No command given when in wingborne flight leads to aircraft stall and loss of control [H-2] **UCA.TRC.20** No command given when in wingborne flight leads to aircraft losing safe separation with other aircraft or terrain / obstacles [H-1,3]	**UCA.TRC.21** FPA command given when in wingborne flight leads to aircraft stall and loss of control [H-2] **UCA.TRC.22** FPA command given when in wingborne flight leads to aircraft losing safe separation with other aircraft or terrain/obstacles [H-1,3] **UCA.TRC.23** FPA command given when in wingborne flight leads to rapid vertical acceleration [H-4] UCA.TRC.24 Command provided during hover flight [H-2]	**UCA.TRC.25** FPA command applied too late leading to loss of safe separation with other aircraft or terrain/obstacles when in wingborne flight [H-1,3] **UCA.TRC.26** Command sent too late in the case that the aircraft has already switched to transition or hover mode [H-2]
Heading Rate	**UCA.TRC.27** No command given when in wingborne flight leads to loss of safe lateral separation with other aircraft or terrain/obstacles [H-1,3]	**UCA.TRC.28** Heading rate command given when in wingborne flight leads to aircraft losing safe lateral separation with other aircraft or terrain/obstacles [H-1,3] **UCA.TRC.29** Heading rate command given when in wingborne flight leads to rapid acceleration [H-4] **UCA.TRC.30** Command provided during hover flight [H-2]	**UCA.TRC.31** Heading rate command applied too late leading to loss of safe lateral separation with other aircraft or terrain/obstacles when in wingborne flight [H-1,3] **UCA.TRC.32** Command sent too late in the case that the aircraft has already switched to transition or hover mode [H-2]

Sideslip Angle		**UCA.TRC.33** Command provided during hover flight [H-2]	**UCA.TRC.34** Command sent too late in the case that the aircraft has already switched to transition or hover mode [H-2]

Table 36. Pilot Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence
Inceptors	**UCA.PIL.1** No command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3] **UCA.PIL.2** No command given when in wingborne flight leads to aircraft stall and loss of control [H-2] **UCA.PIL.3** No command given when in wingborne flight leads to aircraft flying too slow/fast and losing longitudinal separation with other aircraft [H-1]	**UCA.PIL.4** Inceptor command given when in hover leads to aircraft flying at unsafe altitude or horizontal position where there is loss of separation with other aircraft or terrain/obstacles [H-1,3] **UCA.PIL.5** Inceptor command given when in wingborne flight leads to aircraft stall and loss of control [H-2] **UCA.PIL.6** Inceptor command given when in wingborne flight leads to aircraft flying too slow/fast and losing longitudinal separation with other aircraft [H-1] **UCA.PIL.7** Inceptor command given when in wingborne flight leads to loss of lateral separation with other aircraft [H-1] **UCA.PIL.8** Inceptor command given when in hover leads to rapid linear acceleration of the aircraft [H-4]	**UCA.PIL.11** Inceptor command applied too late to avoid other aircraft or terrain/obstacle [H-1,3] **UCA.PIL.12** Command sent too late in the case that the aircraft has already switched flight modes [H-1,2,3]

		UCA.PIL.9 Inceptor command given when in hover leads to rapid angular acceleration of the aircraft [H-4] **UCA.PIL.10** Inceptor command given when in hover results in exceedance of flight envelope [H-2]	

Table 37. Waypoint Controller Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence
Geospatial Positions	**UCA.WPC.1** No command given leads to aircraft losing safe separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.WPC.2** Geospatial positions command results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3] **UCA.WPC.3** Geospatial positions command results in stall and/or loss of control [H-2] **UCA.WPC.4** Geospatial positions command results in rapid acceleration [H-4]	**UCA.WPC.5** Geospatial positions commanded out of sequence results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3] **UCA.WPC.6** Geospatial positions commanded out of sequence results in stall and/or loss of control [H-2]
Headings		**UCA.WPC.7** Heading commands conflict with commanded Geospatial positions [H-2]	

Table 38. Path Generator Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence
Geospatial Positions	**UCA.PGR.1** No command given leads to aircraft losing safe separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.PGR.2** Geospatial positions command results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.PGR.3** Geospatial positions commanded out of sequence results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]
Velocities	**UCA.PGR.4** No command given leads to stall and/or loss of control [H-2]	**UCA.PGR.5** Velocity profile command results in stall and/or loss of control [H-2] **UCA.PGR.6** Velocity profile command results in non-conformance with commanded Geospatial positions, and loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.PGR.7** Velocity profile commanded out of sequence results in stall and/or loss of control [H-2]

Table 39. Collision Avoidance Unsafe Control Actions

Commanded Variable	Not Providing Causes Hazard	Providing Causes Hazard	Providing too Soon, too Late, or Out of Sequence
Velocity	**UCA.DRP.1** No command given leads to stall and/or loss of control [H-2] **UCA.DRP.2** No command given leads to loss of separation with other aircraft [H-1]	**UCA.DRP.3** Velocity profile command results in stall and/or loss of control [H-2] **UCA.DRP.4** Velocity profile command results in loss of separation with other aircraft [H-1]	**UCA.DRP.5** Velocity profile commanded out of sequence results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]

Flight Path Angle	**UCA.DRP.6** No command given leads to stall and/or loss of control [H-2] **UCA.DRP.7** No command given leads to loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.8** Flight path angle command results in stall and/or loss of control [H-2] **UCA.DRP.9** Flight path angle command results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.10** Flight path angles commanded out of sequence results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]
Heading	**UCA.DRP.11** No command given leads to loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.12** Heading command results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.13** Headings commanded out of sequence results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]
Path Generator Engage / Disengage	**UCA.DRP.14** No command given leads to loss of safe separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.15** Engage/disengage command results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]	**UCA.DRP.16** Path generator engage/disengage commanded too late results in loss of separation with other aircraft or terrain/obstacles [H-1, H-3]

The loss scenarios described below can be traced back to the UCAs in the above tables. As an example, the loss scenarios in Table 40 can be traced back to UCA.FPC.4, UCA.FPC.5, and UCA.FPC.6 in Table 33. The hazardous control actions in the loss scenario tables are derived from the combination of a row and column in the UCA tables. In Table 40, the hazardous control action corresponds to the “Pitch/Roll/Yaw (PRY) Input” row, and the “Providing Causes Hazard” column in Table 33. Note that the identified loss scenarios are intended to serve as examples, and are not necessarily complete.

Table 40. Flight Path Controller Loss Scenarios (LS.FPC.1)

	Corresponding UCA: UCA.FPC.4, 5, 6	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information

PRY Not Provided Causes Hazard	LS.FPC.1.1 FPC receives velocity reference during forward flight (or only velocity during transition); or vice versa (Controller incorrectly identifies mode of flight) LS.FPC.1.2 FPC receives stale signal; alternatively, references change too quickly LS.FPC.1.3 FPC receives no signal from upstream LS.FPC.1.4 FPC receives command that directs aircraft to collide with a building or another aircraft LS.FPC.1.5 FPC receives commanded state that is outside of the flight envelope	LS.FPC.1.6 Aircraft achieves attitude tracking (PRY) but not velocity LS.FPC.1.7 FPC receives aircraft attitude instead of rates LS.FPC.1.8 Aircraft velocity estimates do not match actual velocity, exceeding robustness or margins for FPC (what are margin requirements?) LS.FPC.1.9 TRC-style behavior cannot be provided because logic does not exist to track velocity (think, s/w update to eliminate this function in the future) LS.FPC.1.10 Lack of control authority, e.g. degradation of rotor performance, failure of rotor and inability to diagnose which one(s) and adapt, lack of power, icing on surfaces, etc… LS.FPC.1.11 Aircraft configuration different than proc. model for hover flight, leading to mismatch in dynamics and inability to track reference LS.FPC.1.12 FPC unaware of any changes in inner-loop control behavior (e.g. could be in a faulted mode and there are no diagnostics and feedback here; ibid for even lower level functions like lift surface, rotor health) LS.FPC.1.13 Definition of flight modes incorrect for aircraft configuration and state, and/or environment (shifting or out-of-bounds payload, wind shear)

	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process

Velocity Not Provided Causes Hazard	LS.FPC.1.16 Reference commands change too fast for the inner-loop controller to track or stabilize LS.FPC.1.17 Vertical lift rotors and surfaces move too slowly (or not at all) to hover configuration (inability to track translational velocity command)	LS.FPC.1.14 No awareness of flight envelope and P/R/Y command gets filtered LS.FPC.1.15 Flight envelope has changed (or flight envelope protection unavailable)

Table 41. TRC Loss Scenarios (LS.TRC.1)

	Corresponding UCA: UCA.TRC.1	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.TRC.1.1 Tracking Control receives stale automation mode signal; alternatively, automation mode changes too quickly LS.TRC.1.2 Tracking Control receives no automation mode signal from upstream LS.TRC.1.3 Tracking Control receives stale flight mode signal; alternatively, flight mode changes too quickly LS.TRC.1.4 Tracking Control receives no flight mode signal from upstream LS.TRC.1.5 Tracking Control receives no commanded state from upstream	LS.TRC.1.6 Data fusion algorithm updates at too low of a frequency LS.TRC.1.7 Fusion algorithm mishandles null input from sensor LS.TRC.1.8 Sensor damage/malfunction results in no data being sent LS.TRC.1.9 Sensor sample rate is too low, and measurements are sent too late
	b) Identifying scenarios in which control actions are improperly executed or not executed	

Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TRC.1.10 Reference commands are sent too infrequently (FPC updates more frequently than Tracking Control)	

Table 42. TRC Loss Scenarios (LS.TRC.2)

	Corresponding UCA: UCA.TRC.2, 3	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.TRC.2.1 TC receives no automation mode signal from upstream LS.TRC.2.2 TC receives stale automation mode signal LS.TRC.2.3 TC receives erroneous automation mode signal LS.TRC.2.4 TC receives stale flight mode signal; alternatively, flight mode changes too quickly LS.TRC.2.5 TC receives erroneous flight mode signal LS.TRC.2.6 TC receives no flight mode signal from upstream LS.TRC.2.7 TC receives no commanded state from upstream	LS.TRC.2.10 State estimates exceed robustness or margins for Tracking Control (what are margin requirements?) LS.TRC.2.11 Tracking Control receives wingborne or transition mode feedback variables LS.TRC.2.12 Sensor damage or malfunction results in incorrect data being sent

	LS.TRC.2.8 TC receives stale signal from upstream LS.TRC.2.9 TC receives erroneous command from upstream	

	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TRC.2.16 Reference commands change too fast for FPC to track LS.TRC.2.17 No awareness of flight envelope and velocity command gets filtered	LS.TRC.2.13 Lack of control authority LS.TRC.2.14 Tracking Control unaware of changes in FPC/I-L control behavior (e.g. could be in a faulted mode and there are no diagnostics and feedback here; ibid for even lower level functions like lift surface, rotor health) LS.TRC.2.15 Aircraft configuration different than proc. model for hover flight, leading to mismatch in dynamics and inability to track reference

Table 43. TRC Loss Scenarios (LS.TRC.3)

	Corresponding UCA: UCA.TRC.6, 7	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information

Velocity Not Provided Causes Hazard	LS.TRC.3.1 Tracking Control receives stale automation mode signal LS.TRC.3.2 Tracking Control receives stale flight mode signal; alternatively, flight mode changes too quickly LS.TRC.3.3 Tracking Control receives stale signal from upstream	LS.TRC.3.4 Data fusion algorithm updates at too low of a frequency LS.TRC.3.5 Sensor damage/malfunction results in delayed signal LS.TRC.3.6 Sensor sample rate is too low, and measurements are sent too late
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TRC.3.7 Reference commands are sent too infrequently (FPC updates more frequently than Tracking Control)	LS.TRC.3.8 Actuators or rotors have delayed response to control action

Table 44. Wingborne Tracking Control Loss Scenarios (LS.TC.1)

	Corresponding UCA: UCA.TRC.11, 12, 19, 20, 27	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.TC.1.1 Tracking Control receives stale signal; alternatively, automation mode changes too quickly LS.TC.1.2 Tracking Control receives no signal from upstream	LS.TC.1.6 Data fusion algorithm updates at too low of a frequency LS.TC.1.7 Fusion algorithm mishandles null input from sensor

	LS.TC.1.3 Tracking Control receives stale signal; alternatively, flight mode changes too quickly LS.TC.1.4 Tracking Control receives no signal from upstream LS.TC.1.5 Tracking Control receives no commanded state from upstream	LS.TC.1.8 Sensor damage/malfunction results in no data being sent LS.TC.1.9 Sensor sample rate is too low, and measurements are sent too late
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TC.1.10 Reference commands are sent too infrequently (FPC updates more frequently than Tracking Control)	

Table 45. Wingborne Tracking Control Loss Scenarios (LS.TC.2)

	Corresponding UCA: UCA.TRC.13, 14, 21, 22	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.TC.2.1 TC receives no signal from upstream LS.TC.2.2 TC receives stale signal (e.g. mode logic updates at slower rate than TC).	LS.TC.2.10 State estimates exceed robustness or margins for Tracking Control (e.g. no definition of margin requirements)

	LS.TC.2.3 TC receives erroneous signal (e.g. pilot accidentally bumps inceptors, taking aircraft out of autonomous mode) LS.TC.2.4 TC receives stale signal; alternatively, flight mode changes too quickly (e.g. mode logic updates at slower rate than TC). LS.TC.2.5 TC receives erroneous signal (e.g. sensor damage/malfunction results in incorrect angle-of-attack estimate) LS.TC.2.6 Tracking Control receives no signal from upstream (e.g. logic cannot decipher flight mode) LS.TC.2.7 TC receives no commanded state (e.g. DRP cannot find solution) LS.TC.2.8 TC receives stale signal (e.g. waypoint control updates at slower rate than TC) LS.TC.2.9 TC receives erroneous command (e.g. Path Generator lacks awareness of environment)	LS.TC.2.11 TC receives hover mode feedback variables (e.g. recent mode change to wingborne flight during data fusion) LS.TC.2.12 Sensor damage or malfunction results in incorrect data being sent (e.g. ice covering pitot tube)

	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TC.2.13 Reference commands change too fast for FPC to track (e.g. Path Generator rapidly generates new paths to follow) LS.TC.2.14 No awareness of flight envelope and velocity command gets filtered (e.g. occupant + luggage + fuel + other weight exceeds expected capacity, so waypoint controller generates paths that cannot be achieved)	LS.TC.2.15 Lack of control authority (e.g. hydraulic system failure for control surfaces) LS.TC.2.16 Tracking Control unaware of changes in FPC/I-L control behavior (e.g. could be in a faulted mode and there are no diagnostics and feedback here; ibid for even lower level functions like lift surface, rotor health) LS.TC.2.17 Aircraft configuration different than proc. model for hover flight, leading to mismatch in

		dynamics and inability to track reference (e.g. hover-mode rotors are not completely stowed)

Table 46. Wingborne Tracking Control Loss Scenarios (LS.TC.3)

Corresponding UCA: UCA.TRC.17, 18, 25, 26		
a) Identifying scenarios that lead to Unsafe Control Actions		
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.TC.3.1 Tracking Control receives stale signal LS.TC.3.2 Tracking Control receives stale signal; alternatively, flight mode changes too quickly LS.TC.3.3 Tracking Control receives stale signal from upstream	LS.TC.3.4 Data fusion algorithm updates at too low of a frequency LS.TC.3.5 Sensor damage/malfunction results in delayed signal LS.TC.3.6 Sensor sample rate is too low, and measurements are sent too late
b) Identifying scenarios in which control actions are improperly executed or not executed		
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.TC.3.7 Reference commands are sent too infrequently (FPC updates more frequently than Tracking Control)	LS.TC.3.8 Actuators or rotors have delayed response to control action

Table 47. Pilot Loss Scenarios (LS.PIL.1)

	Corresponding UCA: UCA.PIL.4	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.PIL.1.1 Pilot receives stale automation mode signal, resulting in pilot assuming that the aircraft is in autonomous mode when it is in manual mode LS.PIL.1.2 Pilot receives no flight mode signal from upstream LS.PIL.1.3 Pilot receives stale flight mode signal; alternatively, flight mode changes too quickly LS.PIL.1.4 Pilot receives erroneous flight mode signal LS.PIL.1.5 Pilot does not see terrain, obstacle, or aircraft flying on a conflicting trajectory	LS.PIL.1.6 Displays are cluttered, and key information is difficult to discern LS.PIL.1.7 Displays show wingborne or transition mode feedback variables instead of hover mode variables LS.PIL.1.8 Displays malfunction, and show incorrect data or no data LS.PIL.1.9 Sensor damage or malfunction results in incorrect data being sent
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.PIL.1.10 Inceptor inputs are mapped to wingborne or transition control variables LS.PIL.1.11 No awareness of flight envelope and velocity command gets filtered LS.PIL.1.12 Reference commands change too fast for FPC to track	LS.PIL.1.13 Pilot unaware of changes in FPC/I-L control behavior LS.PIL.1.14 Lack of control authority

Table 48. Waypoint Control Loss Scenarios (LS.WPC.1)

	Corresponding UCA: UCA.WPC.1	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.WPC.1.1 Waypoint Control receives stale signal; alternatively, flight mode changes too quickly	LS.WPC.1.6 Data fusion algorithm updates at too low of a frequency
	LS.WPC.1.2 Waypoint Control receives no signal from upstream	LS.WPC.1.7 Fusion algorithm mishandles null input from sensor
	LS.WPC.1.3 Waypoint Control receives no commanded state from upstream	LS.WPC.1.8 Sensor damage/malfunction results in no data being sent
	LS.WPC.1.4 Aircraft passed all or the last commanded waypoint	LS.WPC.1.9 Sensor sample rate is too low, and measurements are sent too late
	LS.WPC.1.5 Current time has passed the scheduled arrival time of the last waypoint	
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.WPC.1.10 Reference commands are sent too infrequently (Tracking Control updates more frequently than Waypoint Control)	

Table 49. Waypoint Control Loss Scenarios (LS.WPC.2)

	Corresponding UCA: UCA.WPC.2, 3, 4	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.WPC.2.1 Waypoint Control receives erroneous signal LS.WPC.2.2 Waypoint Control receives stale signal; alternatively, flight mode changes too quickly LS.WPC.2.3 Waypoint Control receives no signal from upstream LS.WPC.2.4 Waypoint Control receives erroneous signal from upstream LS.WPC.2.5 Commanded path would cause LOS with other aircraft or terrain/obstacles LS.WPC.2.6 Commanded path is not achievable	LS.WPC.2.7 State estimates exceed robustness or margins for Waypoint Control LS.WPC.2.8 Sensor damage/malfunction results in incorrect data being sent
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.WPC.2.9 No awareness of flight envelope results in an unachievable commanded position LS.WPC.2.10 Reference commands change too fast for TC to track	LS.WPC.2.11 Aircraft deviating too far from commanded path results in the path being unachievable

	LS.WPC.2.12 The WPC’s generated trajectory function is not smooth (there is a discontinuity in the position or its derivative)	

Table 50. Waypoint Control Loss Scenarios (LS.WPC.3)

	Corresponding UCA: UCA.WPC.5, 6	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.WPC.3.1 Waypoint Control receives incorrectly ordered waypoints from upstream LS.WPC.3.2 Waypoint Control receives no time data for waypoints from upstream	LS.WPC.3.3 State estimates exceed robustness or margins for Waypoint Control resulting in the aircraft appearing to pass a waypoint it has not yet reached LS.WPC.3.4 Sensor damage/malfunction results in incorrect data being sent
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.WPC.3.5 Reference commands are sent too infrequently (TC updates more frequently than Waypoint Control)	LS.WPC.3.6 Aircraft deviating too far from the commanded path results in incorrect identification of which position the aircraft should fly to

Table 51. Path Generator Loss Scenarios (LS.PGR.1)

	Corresponding UCA: UCA.PGR.2	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.PGR.1.1 Path Generator receives erroneous waypoint entries from the user LS.PGR.1.2 Waypoints entered by the user do not have adequate separation from obstacles/terrain LS.PGR.1.3 Commanded waypoints are not achievable	LS.PGR.1.4 State estimates exceed robustness or margins for Path Generator LS.PGR.1.5 Sensor damage/malfunction results in incorrect data being sent
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.PGR.1.6 Lack of awareness of other aircraft or obstacles results in LOS LS.PGR.1.7 Path is designed such that it is impossible for the DRP/OFN to avoid LOS LS.PGR.1.8 No awareness of flight envelope results in an unachievable commanded path LS.PGR.1.9 Reference commands change too fast for TC to track LS.PGR.1.10 The generated path has an inadequate spatial resolution (too few waypoints do not sufficiently constrain flight around terrain/obstacles)	

Table 52. Collision Avoidance Loss Scenarios (LS.DRP.1)

	Corresponding UCA: UCA.DRP.8	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard		LS.DRP.1.1 State estimates exceed robustness or margins for Path Generator LS.DRP.1.2 Sensor damage/malfunction results in incorrect data being sent
	b) Identifying scenarios in which control actions are improperly executed or not executed	
Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.DRP.1.3 No awareness of flight envelope results in an unachievable commanded path LS.DRP.1.4 No collision avoidance solution exists within the flight envelope	LS.DRP.1.5 Lack of control authority (e.g. rotor failure)

Table 53. Collision Avoidance Loss Scenarios (LS.DRP.2)

	Corresponding UCA: UCA.DRP.16	
	a) Identifying scenarios that lead to Unsafe Control Actions	

Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.DRP.2.1 The time window for the pilot to override the DRP is too long, and results in late response to potential LOS by the DRP LS.DRP.2.2 Delayed surveillance data for other aircraft positions results in late response to potential LOS by the DRP LS.DRP.2.3 DRP receives waypoints for the aircraft's intended path too late resulting in late identification of a potential collision and unavoidable LOS LS.DRP.2.4 DRP sends late disengage signal to PG resulting in aircraft following PGR into LOS	LS.DRP.2.5 Sensors update at slower rate than DRP resulting in DRP receiving aircraft state information too late LS.DRP.2.6 Sensor malfunction results in aircraft state data being sent too late

b) Identifying scenarios in which control actions are improperly executed or not executed

Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.DRP.2.7 DRP lacks awareness of aircraft dynamics, and underestimates the necessary response time for the aircraft to avoid LOS LS.DRP.2.8 DRP is too slow to calculate a collision avoidance solution	

Appendix E. RTA-Protected Aircraft STPA

Table 54. RTA-Protected TRC Control Loss Scenarios (LS.R-TRC.1)

	Corresponding UCA: UCA.TRC.17, 18, 25, 26	
	a) Identifying scenarios that lead to Unsafe Control Actions	
Hazardous Control Action	1) Unsafe controller behavior	2) Causes of inadequate feedback and information
Velocity Not Provided Causes Hazard	LS.R-TRC.1.1 Tracking Control receives stale signal LS.R-TRC.1.2 Tracking Control receives stale signal; alternatively, flight mode changes too quickly LS.R-TRC.1.3 Tracking Control receives stale signal from upstream LS.R-TRC.1.4 Mode switch is initiated in inappropriate regime LS.R-TRC.1.5 Switch in flight mode causes unsafe step response LS-R-TRC.1.6 Mode is operated in wrong regime (flight mode not changed) LS.R-TRC.1.7 TC receives no signal from upstream LS.R-TRC.1.8 TC receives stale signal (e.g. mode logic updates at slower rate than TC). LS.R-TRC.1.9 TC receives erroneous signal (e.g. pilot accidentally bumps inceptors, taking aircraft out of autonomous mode)	LS.R-TRC.1.17 Data fusion algorithm updates at too low of a frequency LS.R-TRC.1.18 Sensor damage/malfunction results in delayed signal LS.R-TRC.1.19 Sensor sample rate is too low, and measurements are sent too late LS.R-TRC.1.20 Estimate of attitude relative to mode regime is incorrect (e.g. noise causes it to cross barriers) LS.R-TRC.1.21 State estimates exceed robustness or margins for Tracking Control (e.g. no definition of margin requirements) LS.R-TRC.1.22 TC receives hover mode feedback variables (e.g. recent mode change to wingborne flight during data fusion) LS.R-TRC.1.23 Sensor damage or malfunction results in incorrect data being sent (e.g. ice covering pitot tube)

	LS.R-TRC.1.10 TC receives stale signal; alternatively, flight mode changes too quickly (e.g. mode logic updates at slower rate than TC). LS.R-TRC.1.11 TC receives erroneous signal (e.g. sensor damage/malfunction results in incorrect angle-of-attack estimate) LS.R-TRC.1.12 Tracking Control receives no signal from upstream (e.g. logic cannot decipher flight mode) LS.R-TRC.1.13 TC receives no commanded state (e.g. DRP cannot find solution) LS.R-TRC.1.14 TC receives stale signal (e.g. waypoint control updates at slower rate than TC) LS.R-TRC.1.15 TC receives erroneous command (e.g. Path Generator lacks awareness of environment) LS.R-TRC.1.16 Transition from MPC to PID results in inappropriate PID gains (due to gain schedule, etc.)	LS.R-TRC.1.24 No indication provided regarding which controller is active

b) Identifying scenarios in which control actions are improperly executed or not executed

Hazardous Control Action	3) Scenarios involving the control path	4) Scenarios related to the controlled process
Velocity Not Provided Causes Hazard	LS.R-TRC.1.25 Reference commands are sent too infrequently (FPC updates more frequently than Tracking Control) LS.R-TRC.1.26 Reference commands change too fast for FPC to track (e.g. Path Generator rapidly generates new paths to follow) LS.R-TRC.1.27 No awareness of flight envelope and velocity command gets filtered (e.g. occupant +	LS.R-TRC.1.28 Actuators or rotors have delayed response to control action LS.R-TRC.1.29 Lack of control authority (e.g. hydraulic system failure for control surfaces) LS.R-TRC.1.30 Tracking Control unaware of changes in FPC/I-L control behavior (e.g. could be in a faulted mode and there are no diagnostics and feedback here;

	luggage + fuel + other weight exceeds expected capacity, so waypoint controller generates paths that cannot be achieved)	ibid for even lower level functions like lift surface, rotor health) LS.R-TRC.1.31 Aircraft configuration different than proc. model for hover flight, leading to mismatch in dynamics and inability to track reference (e.g. hover-mode rotors are not completely stowed) LS.R-TRC.1.32 Actuators receive to sudden or abrupt change in commanded position due to change in mode LS.R-TRC.1.33 Control mode is switched during change in flight phase (i.e. from hover to wingborne or vice versa) resulting in a misunderstood transient

References

[Abdulkhaleq 2015] Abdulkhaleq, A., & Wagner, S., “A controlled experiment for the empirical evaluation of safety analysis techniques for safety-critical software.” In Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering, 2015. pp. 1-10.

[Abdulkhaleq 2017] Abdulkhaleq, A., Wagner, S., Lammering, D., Boehmert, H., & Blueher, P., “Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles,” Automotive-Safety & Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik, 2017.

[Alves 2018] Alves, E., Bhatt, D., Hall, B., Driscoll, K., Murugesan, A., & Rushby, J., “Considerations in Assuring Safety of Increasingly Autonomous Systems,” NASA, 2018.

[Anderson 2018] Anderson, E., Fannin, T., & Nelson, B., “Levels of Aviation Autonomy,” 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), 2018. pp. 1-8

[ASTM F3061] ASTM F3061 / F3061M-20, “Standard Specification for Systems and Equipment in Small Aircraft”, ASTM International, West Conshohocken, PA, 2020. DOI: 10.1520/F3061_F3061M-20

[ASTM F3230] ASTM F3230-17, “Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft,” ASTM International, West Conshohocken, PA, 2017. DOI: 10.1520/F3230-17

[ASTM F3264] “American Society for Testing and Materials (ASTM), F3264: Standard Specification for Normal Category Aeroplanes Certification,” 2019.

[ASTM F3269] American Society for Testing and Materials (ASTM), “Standard Practice for Methods to Safely Bound Behavior of Aircraft Systems Containing Complex Functions Using Run-Time Assurance,” 2017.

[Boeing 2021] Boeing Commercial Airplanes, “Statistical Summary of Commercial Jet Airplane Accidents–Worldwide Operations| 1959–2020,” Seattle, 2021.

[Cooper 2010] Cooper, J., Schierman, J., & Horn, J., “Robust adaptive disturbance compensation for ship-based rotorcraft,” in AIAA Guidance, Navigation, and Control Conference, AIAA, 2010.

[Cooper 2014] Cooper, J., & Schierman, J., “A Sense and Avoid System for Unmanned Aircraft in Formation Flight,” AIAA Guidance, Navigation, and Control Conference, 2014.

[Enns 1994] Enns, D., Bugajski, D., Hendrick, R., & Stein, G., “Dynamic inversion: an evolving methodology for flight control design,” International Journal of control 59.1, 1994. pp. 71-91

[FAA 2017] Federal Aviation Administration, “A Blueprint for AIR Transformation,” 2017.

[FAA CPI 2017] Federal Aviation Administration, “FAA and Industry Guide to Product Certification (CPI Guide)”, 2017.

[FAA 2020] Federal Aviation Administration, “Concept of Operations (Conops) v1.0 for UAM,” 2020. [Online]. https://www.faa.gov/uas/advanced_operations/urban_air_mobility/

[Feary 2018] Feary, M., “A First Look at the Evolution of Flight Crew Requirements for Emerging Market Aircraft,” NASA, 2018.

[Fernando 2010] Fernando, H., “Fluid dynamics of urban atmospheres in complex terrain,” Annual review of fluid mechanics, Vol. 42, 2010. pp. 365-389.

[Goodrich 2015] Goodrich, K., & Moore, M., “Overview: Simplified Vehicle Operations (SVO),” Tech. rep., NASA, 2015.

[Graydon 2020] Graydon, M., Neogi, N., & Wasson, K., “Guidance for Designing Safety into Urban Air Mobility: Hazard Analysis Techniques,” in Proceedings of the AIAA SciTech Forum, 2020. DOI: 10.2514/6.2020-2099

[Hanna 2006] Hanna, S., Brown, M., Camelli, F., Chan, S., Coirier, W., Hansen, O., Huber, A., Kim, S., & Reynolds, R., “Detailed simulations of atmospheric flow and dispersion in downtown Manhattan: An application of five computational fluid dynamics models,” Bulletin of the American Meteorological Society, Vol. 87, (12), 2006. pp. 1713-1726.

[Harris 2018] Harris, J., “F-35 Flight Control Law Design, Development and Verification,” 2018 Aviation Technology, Integration, and Operations Conference, 2018.

[Horn 2019] Horn, J., “Non-Linear Dynamic Inversion Control Design for Rotorcraft,” Aerospace 6.3, 2019. pp. 38.

[Leveson 2016] Leveson, N., “Engineering a safer world: Systems thinking applied to safety,” The MIT Press, 2016.

[Leveson 2018] Leveson, N., and John P. Thomas, “STPA Handbook,” 2018.

[Lombaerts 2020] Lombaerts, T., Kaneshige, J., & Feary, M., “Control Concepts for Simplified Vehicle Operations of a Quadrotor eVTOL Vehicle,” AIAA AVIATION 2020 FORUM. 2020.

[Leveson 2016] Leveson, N., “Engineering a safer world: Systems thinking applied to safety,” The MIT Press, 2016.

[NASA 2020] NASA, “UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4,” 2020.

[Nguyen 2021] Nguyen, N., “A Physics-Based Spatial Wake Interactional Model of Fixed-Wing Aircraft and Rotorcraft for Urban Air Mobility,” AIAA Scitech 2021 Forum, 2021.

[Peterson 2020] Peterson, E., DeVore, M., Cooper, J., & Carr, G., “Run-Time Assurance as an Alternate Concept to Contemporary Development Assurance Processes,” NASA, 2020.

[Rotach 1999] Rotach, M., “On the Influence of the Urban Roughness Sublayer on Turbulence and Dispersion,” Atmospheric Environment, vol. 33, 1999. pp. 401–408

[RTCA/DO-178C] Radio Technical Commission for Aeronautics (RTCA), “RTCA/DO-178C, Software Considerations in Airborne Systems and Equipment Certification,” 2011.

[RTCA/DO-254] RTCA, Inc., “Design Assurance Guidance for Airborne Electronic Hardware,” (RTCA/DO-254), 2000.

[SAE 1996] SAE, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Aircraft Systems and Equipment,” ARP4761, 1996.

[SAE 2010] SAE, “Aerospace Recommended Practice: Guidelines for Development of Civil Aircraft and Systems,” ARP4754 Rev. A, 2010.

[Schierman 2015] Schierman, J., DeVore, M., Richards, N., Gandhi, N., Cooper, J., Horneman, K., Stoller, S., and Smolka, S., “Runtime assurance framework development for highly adaptive flight control systems,” Air Force Research Laboratory Technical Report AFRL-RQ-WP-TR-2016-0001, 2015.

[Schierman 2020] Schierman, J., DeVore, M., Richards, N., and Clark, M., “Runtime assurance for autonomous aerospace systems,” Journal of Guidance, Control, and Dynamics, 43(12), 2205-2217.

[Slotine 1991] Slotine, J., & Li, W., “Applied nonlinear control,” Vol. 199. No. 1. Englewood Cliffs, NJ: Prentice hall, 1991.

[STAMP-Related Publications] “STAMP-Related Publications,” Massachusetts Institute of Technology (MIT), [Online]. Available: http://sunnyday.mit.edu/STAMP-publications.html.

[Sulaman 2019] Sulaman, S., Beer, A., Felderer, M., & Höst, M., “Comparison of the FMEA and STPA safety analysis methods–a case study,” Software Qual J 27, 2019. 349–387. https://doi.org/10.1007/s11219-017-9396-0

[Takahashi 2017] Takahashi, M., Whalley, M., Mansur, H., Ott, L., Minor, M., & Morford, M., “Autonomous Rotorcraft Flight Control with Multilevel Pilot Interaction in Hover and Forward Flight,” in Journal of the American Helicopter Society, 2017. DOI: 62. 10.4050/JAHS.62.032009

[Uber 2016] Uber Elevate, “Fast-Forwarding to a Future of On-Demand Urban Air Transportation”, White Paper, 2016.

[USAAMC 2000] United States Army Aviation and Missile Command, “Aeronautical design standard performance specification handling qualities requirements for military rotorcraft,” military rotorcraft specification manual, Aviation Engineering Directorate, 2000.

[Walker 2013] Walker, G., Fuller, J., & Wurth, S., “F-35B Integrated Flight-Propulsion Control Development,” AIAA Aviation 2013 International Power Lift Conference, Los Angeles, CA, 2013.

[Wing 2020] Wing, D., Chancey, E., Politowicz, M., & Ballin, M., “Achieving Resilient In-Flight Performance for Advanced Air Mobility through Simplified Vehicle Operations,” In AIAA AVIATION 2020 FORUM, 2020. pp. 2915