Gefördert durch:

Bundesministerium
für Verkehr und
digitale Infrastruktur

aufgrund eines Beschlusses
des Deutschen Bundestages

VOLOCOPTER

DLR Deutsches Zentrum
für Luft- und Raumfahrt
German Aerospace Center

voloCHRIS

Volocopter Contingency Handling with a Runtime Inspection System

mFUND
Das Startkapital für die Mobilität 4.0

Document properties

Title	voloCHRIS Final Project Report
Project Partners	DLR, Institute of Flight Systems, Dept. Unmanned Aircraft Volocopter GmbH
Participants	Volocopter: Florian-Michael Adolf, Markus Ortlieb, Sébastien Bomart DLR: Sebastian Schirmer, Sebastian Benders, Christoph Torens, Simon Schopferer
Date	20 July 2020
Version	1.0

Index of contents

1. Project Overview

New concepts for urban air mobility based on electric vertical take-off and landing (eVTOL) aircraft envision fully autonomous flight operations. Without a pilot onboard, the aircraft must automatically and independently react to events such as system degradations, unexpected air traffic or changing weather conditions. Intelligent algorithms must decide to carry out contingency procedures depending on the situation in a correct, quick, deterministic, and transparent fashion in order to mitigate risks for passengers and people on the ground. The technologies involved for such high levels of autonomy have been developed over the recent years and their functionality has been demonstrated. However, certification of complex systems required for autonomous flight remains a challenge and the applicable regulatory framework is a work in progress. Furthermore, acceptance of the technological solutions by the aviation community, by legislators and by the general public is a key factor that needs to be addressed.

Within the scope of the voloCHRIS project, a system for automated contingency management for an eVTOL passenger aircraft is designed, developed, and demonstrated in flight. The focus of the development is to assess algorithms for decision making in situations relevant to the safety of the passengers. The goal of the project is to gain knowledge about the applicability, performance and verifiability of algorithms and system architectures for contingency management. With the overarching objective of increasing acceptance of confidence in technological solutions, the project aims to contribute towards the development of provably safe decision-making systems for autonomous aircraft.

1.1. Project Goals and Key Activities

The voloCHRIS project persues the following overarching goals:

- Increased awareness for autonomy and certification challenges within the community,
- Increased acceptance of the general public in regard to safe autonomous flight.

To contribute towards these overarching goals, the following project goals are targeted within the voloCHRIS project:

- Demonstration of a prototypical Contingency Management System in simulation and flight test,
- Assessment of applicability and suitability of selected algorithms for automated decision making,
- Identification and discussion of certification aspects and challenges of safe autonomous flight.

The key activities planned to reach these goals are:

- Assessment of the regulatory framework and certification aspects,
- Development and integration of a contingency management system,
- Validation of the developed concepts and algorithms,
- Publication and discussion of the key results and findings.

1.2. Expected Results and Results Utilization

The following key results are expected as an outcome of the voloCHRIS project:

1. Integrated and tested prototypical software for a Contingency Management System of a Volocopter flight test demonstrator,
2. Documentation of the current state of development of the regulatory framework and certification aspects in the context of contingency management for eVTOL aircraft,
3. Documentation of the developed concepts, algorithms, and validation results.

The key findings and results are planned to be published at relevant conferences and discussed within the community. Furthermore, the results are planned to be used to establish a dialogue and support the ongoing cooperation with EASA regarding the topic of autonomous flight for eVTOL aircraft.

1.3. General Approach and Work Packages

The overall project structure is depicted in Figure 1. In a first step, a set of contingency scenarios to be addressed within the scope of the project were defined and requirements regarding the automated decision-making system were derived. Directly contributing towards the goal of increasing and promoting the acceptance of autonomous air taxis, an informative video of the project's vision with visualizations of the contingency scenarios was created in order to reach a broad audience, to raise awareness and to promote further discussions. Aspects of certification were considered to provide further requirements for developing a concept and prototype implementation of a contingency management system. Finally, the concept was demonstrated in simulation and flight test based on a scaled demonstrator platform and an exemplary contingency scenario.

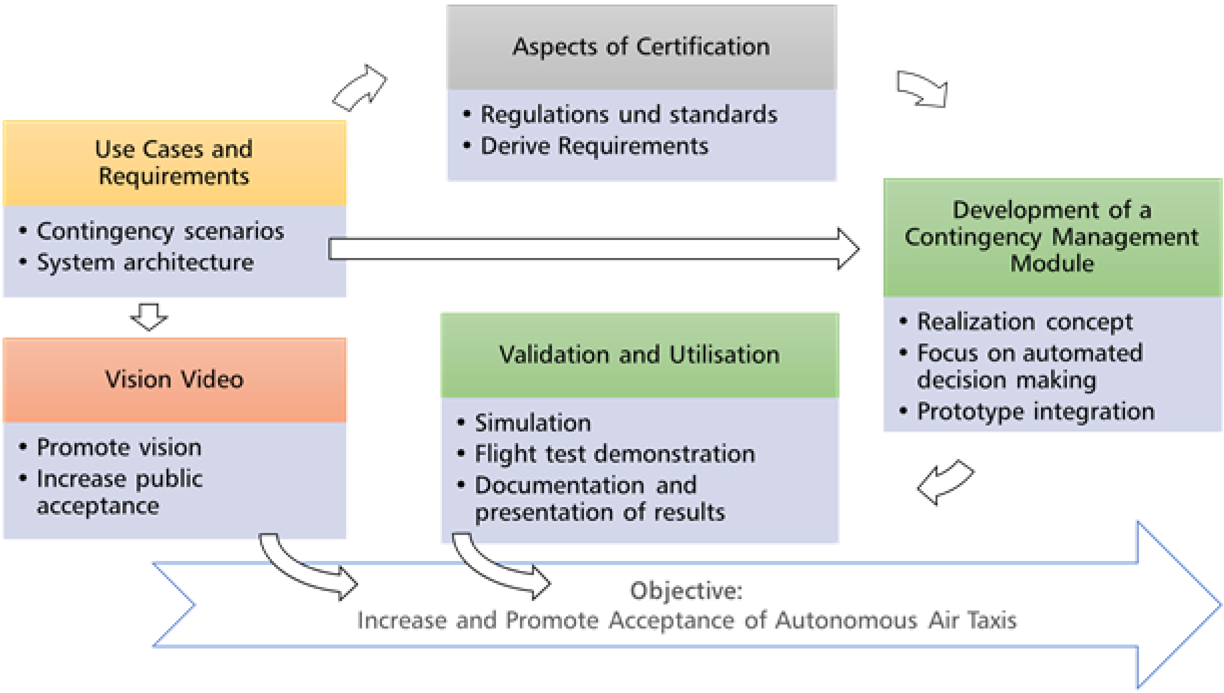


Figure 1: Overall project structure and work packages

The key results of the project include the definition of a set of contingency scenarios, the vision video, an assessment of the regulatory framework and a documented concept and prototypical implementation for a contingency management system. These results were presented to an expert audience on January 30th 2020 in a final project meeting. The valuable questions and feedback received from this event will be the basis for further discussions and future work on the topic of contingency management for autonomous air taxis.

1.4. Project Milestones

The list of milestones and work package scheduling over the project's planned duration of 6 months is depicted in Table 1.

Work Packages	M1	M2	M3	M4	M5	M6
AP1 Vision Video		■	■	■	■	■
AP2 Use-Cases and Requirements	■					
AP3 Aspects of Certification	■	■	■			
AP4 Development of a Contingency Management Module		■	■	■		
AP5 Validation and Utilisation			■	■	■	■

Milestones						
MS1 Use-Cases/Requirements documented	◊					
MS2 Contingency Management Module integrated				◊		
MS3 Flight demonstration					◊	
MS4 Final project meeting						◊

Table 1: Work package scheduling and milestones

2. Vision

At Volocopter we have been setting the standard for Urban Air Mobility since 2011 - with over 1,000 test flights.

Figure 2: Major flights demonstration milestones in 2018 and 2019 of Volocopter's eVTOL fleet

Figure 3: VoloCity flying in a congested area (computer animation).

Our latest generation, the VoloCity, will soon start commercial flight operations, first piloted and later autonomously (Figure 3). Urban Air Mobility is interesting as our VoloCity is designed with inherent safety culture of today's commercial transport aviation in mind. In commercial aviation, the highest safety standards apply to infrastructure, aircraft, and all processes.

Today, autopilots already play an important role in this safety critical environment - however with a human pilot still supervising the automation on board.
We are working on the next stage together with European aviation authorities: we are developing regulations for autonomous VoloCity flights.

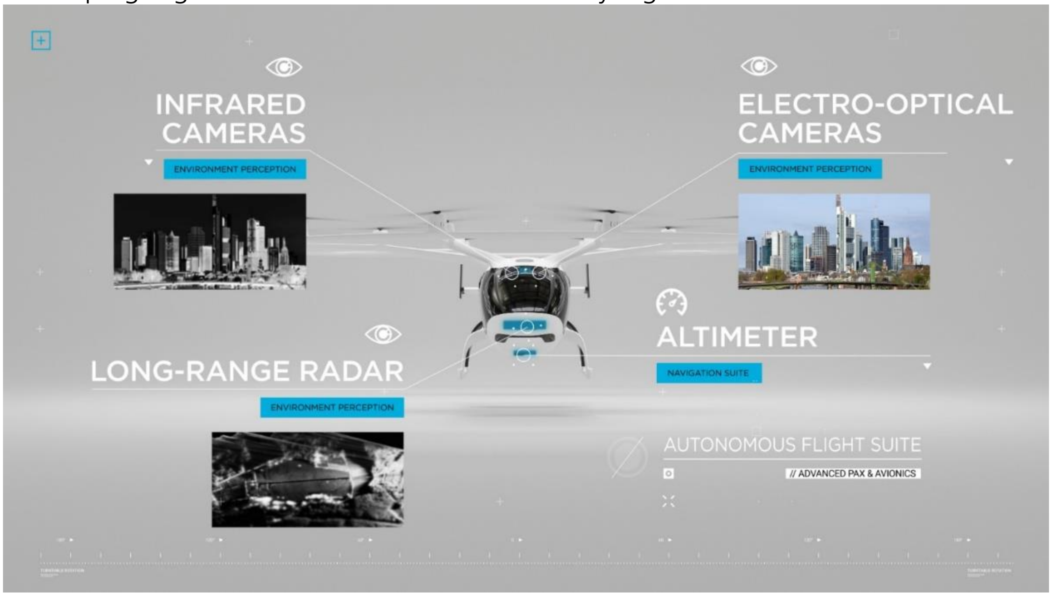


Figure 4: VoloCity sensor suite concept for Unmanned VoloCity flights.

Redundant systems will take over the tasks and duties of the pilot: on the ground and on board. Several sensors ensure a 360° view and detect all objects in the air (Figure 4).

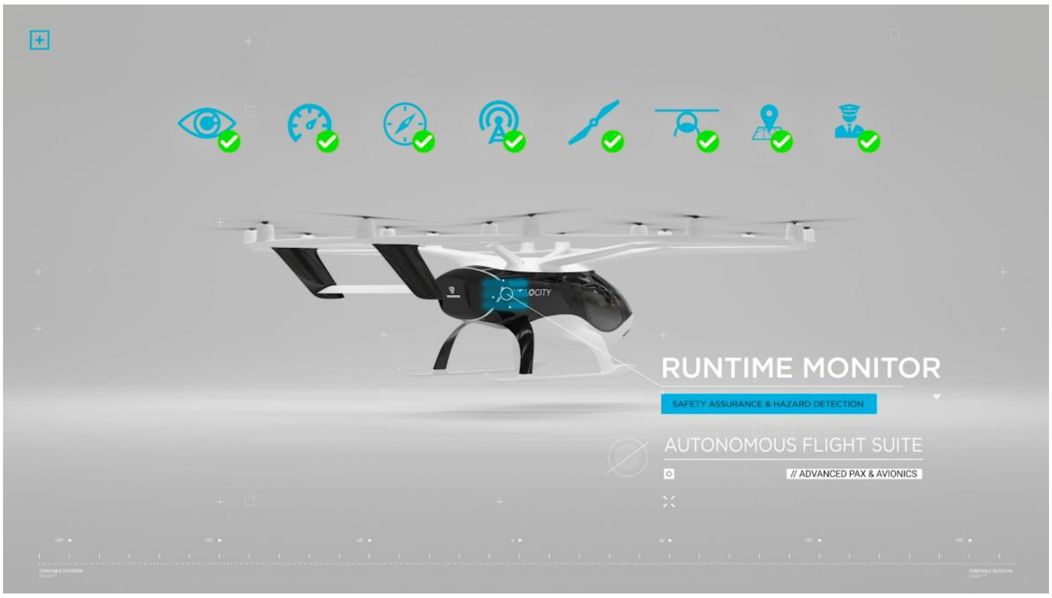


Figure 5: VoloCity advanced monitoring concept for Unmanned VoloCity flights.

An independent monitoring system will keep an eye on all components at any given time (Figure 5). Whether radio communication, propulsion, or flight plan, without the system's approval and permission, no take off without the system's "go".

Figure 6: Flight Management System and onboard databases for safe, real-time decision making.

The Flight Management System (FMS), will make many decisions and automates predefined processes - always on time, correctly and safely.
Before take-off, the FMS will have access to extensive traffic, weather and obstacle data - even without a data connection to the ground (Figure 6).

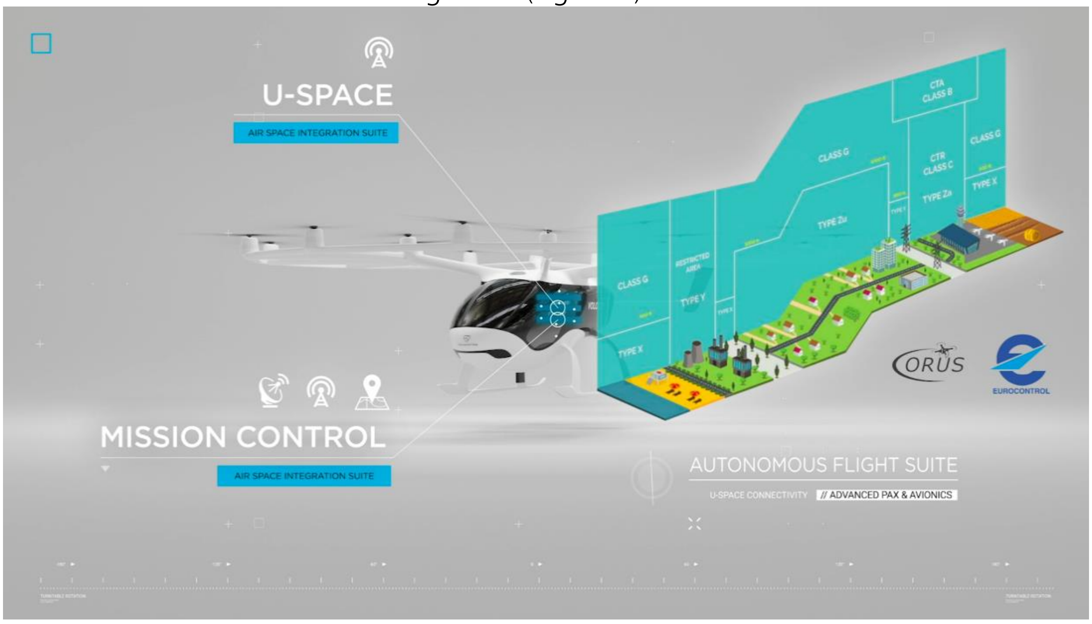


Figure 7: VoloCity ground station & air space integration for Unmanned VoloCity flights.

The VoloCity will be connected to U-Space, Europe's digital airspace management system. This ensures smooth and safe processes with all other airspace participants.
Additionally, it will also have a direct connection to the Mission Control Center. Here, all flights are monitored by specially trained remote pilots - and passengers on board can talk to our staff at any time.

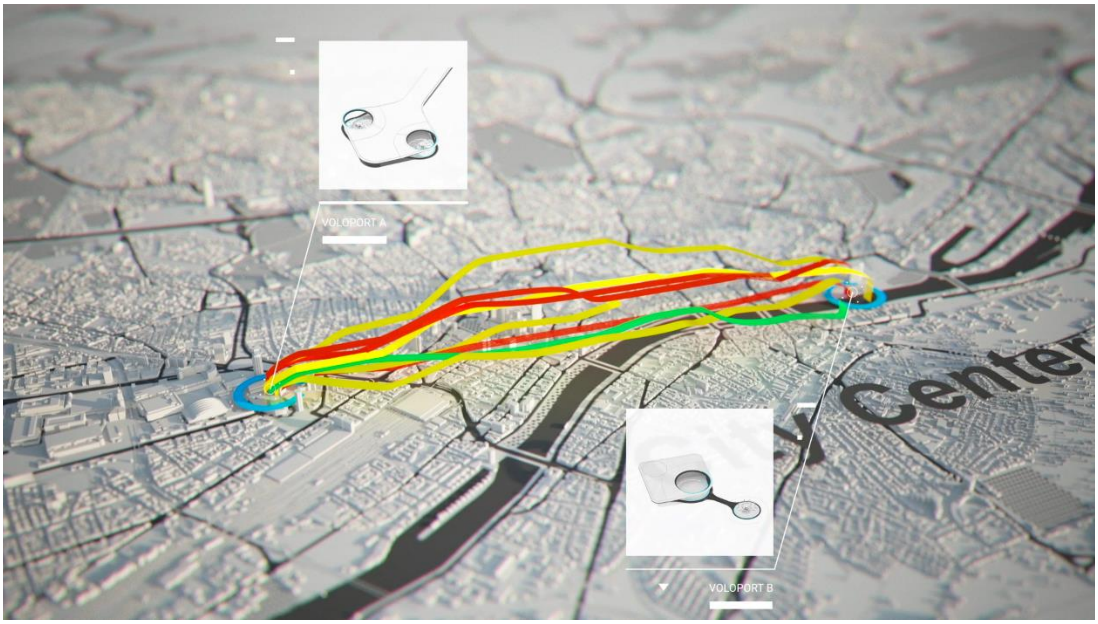


Figure 8: Predefined routes between two vertiports for Unmanned Flights form "A to B".

The VoloCity will operate on defined routes from VoloPort to VoloPort . There are virtually thousands of trajectories in the air to choose from for one route. The best route will be determined before each take-off - based on weather conditions, traffic density, and noise considerations.

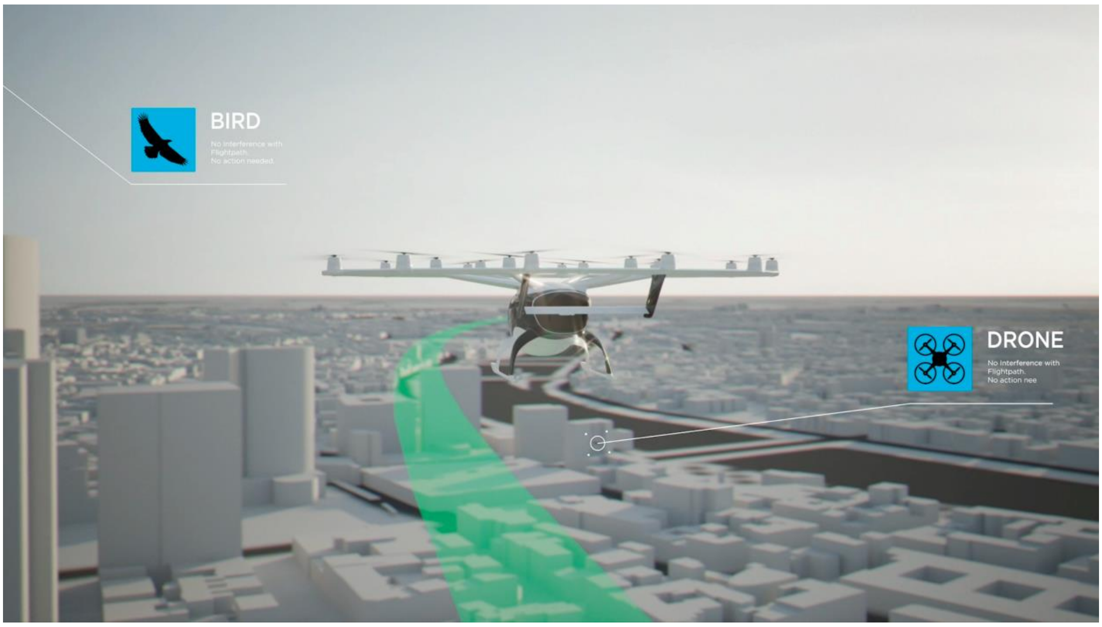


Figure 9: Hazard detection and resolution advisories for the onboard FMS.

The FMS and the independent monitoring system will be permanently active, in order to detect and react to potential hazards (Figure 9). Whether birds or drones - the VoloCity will locate them early. If the flight path is crossed by another airspace participant, the VoloCity will calculate whether a speed reduction or a route change is necessary - a fully automated process, all within milliseconds.

3. Contingency Scenarios

In the frame of the voloCHRIS project the first focus was placed in understanding what type of contingencies will be tackled on a daily basis for urban eVTOL operation. It is thus important to define properly the mission profile of Volocopter vehicle and derive a list of scenarios which could be encountered. The list of derived contingencies is not final of course but the construction of the contingency module will take care of offering a straightforward approach to add identified contingency scenario.

To clearly distinguish between **contingency** vs **emergency** scenarios, both definitions are provided.

i. Contingency is "Plan B" where situation is under control, attempt to maintain level of operation at possible different levels of contingencies
   Example: GNSS impacted by solar storm, runway inspection

ii. Emergency is "Situation out of (safe) control", where triggered after sudden event, or deteriorating event (normal operation -> degraded mode of operation)
   Example: Parachute for emergency landing

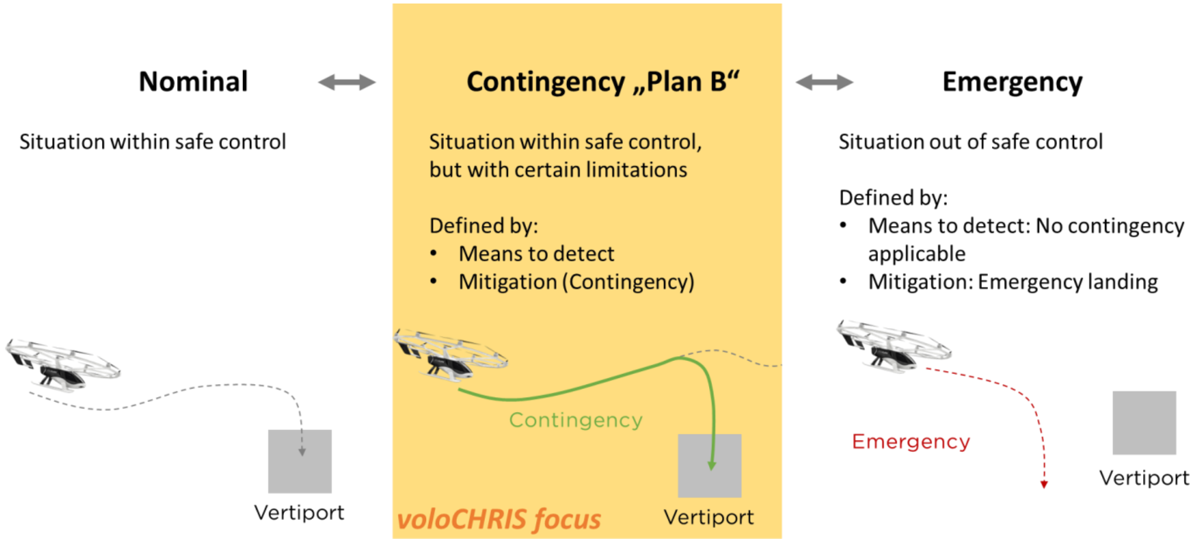


Figure 10: Contingency vs. Emergency

3.1. Mission profile

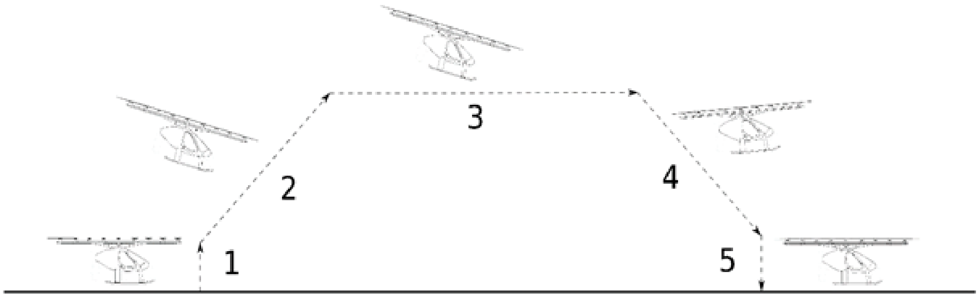


Figure 11: Mission profile of the VC2-1

The Volocopter is designed for the previous nominal flight profile:

1) a vertical take-off to 30 ft altitude AGL at 0.5 m/s
2) a climb path to the cruise altitude of 1000 ft AGL with acceleration to cruise speed
3) cruise flight at cruise speed
4) a descend path to the altitude of 30 ft AGL
5) vertical landing from 30 ft AGL with speed below 0.1 m/s.

Along the mission profile it is important to consider the dynamic limit of the airframe which is bound for safety and comfort to:

- +/- 26° max bank angle
- 50°/s max yaw turn
- 180 meters turn radius (comfort)
- 100 meters turn radius (max bank angle maneuver)
- Max. climb/descent rate of 800 ft/min

These metrics are important to consider the appropriate sensor installation for the current mission profile.
This constrained mission profile of the Volocopter is an important assumption for the development of the different subsystems as it bounds drastically the potential corner cases which could be encountered by the vehicle. Thus, it can be expected that Volocopter will operate on dedicated routes (scheduled/pre-defined route) over a city with a well-known environment (e.g. high-resolution maps could be onboard, landing sites available, availability of required infrastructure for safe flight). The certification process is foreseen to be risk-based and operation centric, thus a strong emphasis will be put in ensuring a priori that the flight is safe to fly. A U-Space provider is expected to be a major entity to support this process. Most of the operation will happen at about 1000 ft in the Very Low Level (VLL) airspace.

Flying in airspaces similar to VLL today is currently not permitted as per SERA.5005 which in turn can provide a preliminary specification of VLL airspaces:

1) over congested areas of cities, towns or settlements or over open-air assembly of people at a height less than 300m above the highest obstacle within a radius of 600 m from the aircraft.
2) elsewhere than as specified in 1, at a height less than 150 meters above the ground or water, or 150 m above the highest obstacle within a radius of 150 m from the aircraft.

Even if this airspace has the advantage to be constrained and potentially well equipped, the biggest challenge in VLL area is to remain well clear from any conflict on the trajectory vs terrain, obstacles (stationary, temporary, wires, mobile obstructions, trees), meteorological and atmospheric phenomena, group of people and flocks of birds.
The following figure gives another representation of the flight profile highlighting the potential take-off and landing location on elevated vertiports with a mapping to the high-level navigation modes.

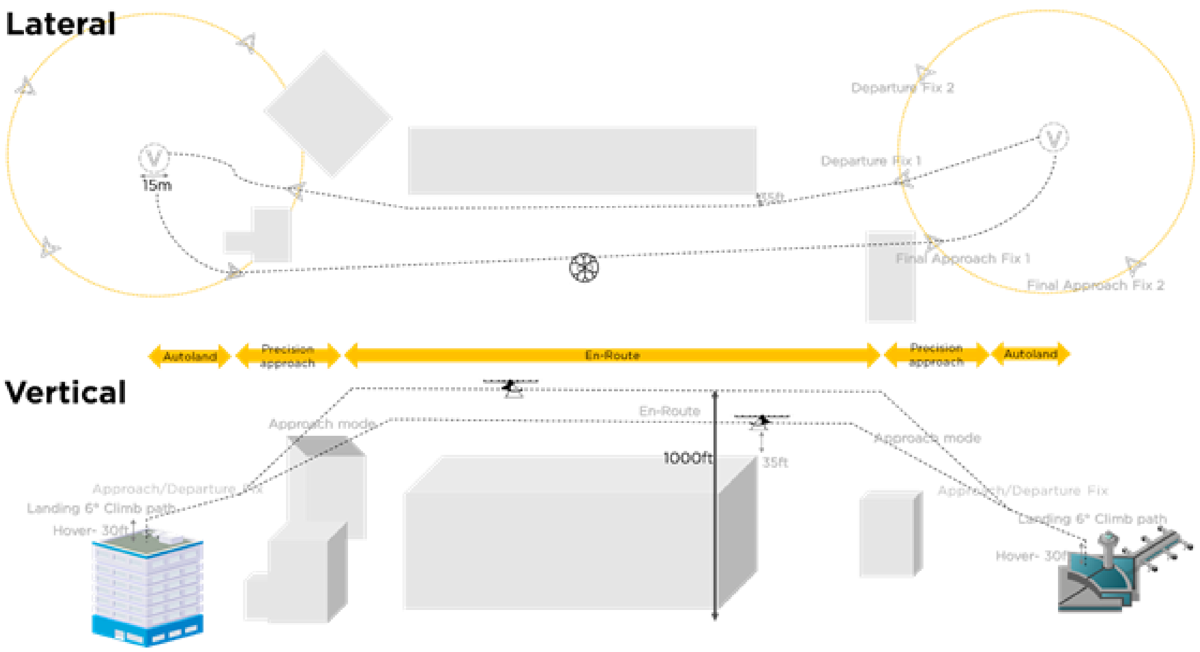


Figure 12: Lateral and vertical mission profile description

On top of this single route description, the target for the early operations is to cover a city with up to 35 minutes flights. Our flight planning process includes several safety features such as considerations regarding the reachability of alternative landing sites, optimal route planning (e.g. wind, range, speed, comfort, efficiency) and deconflicting other airspace users.

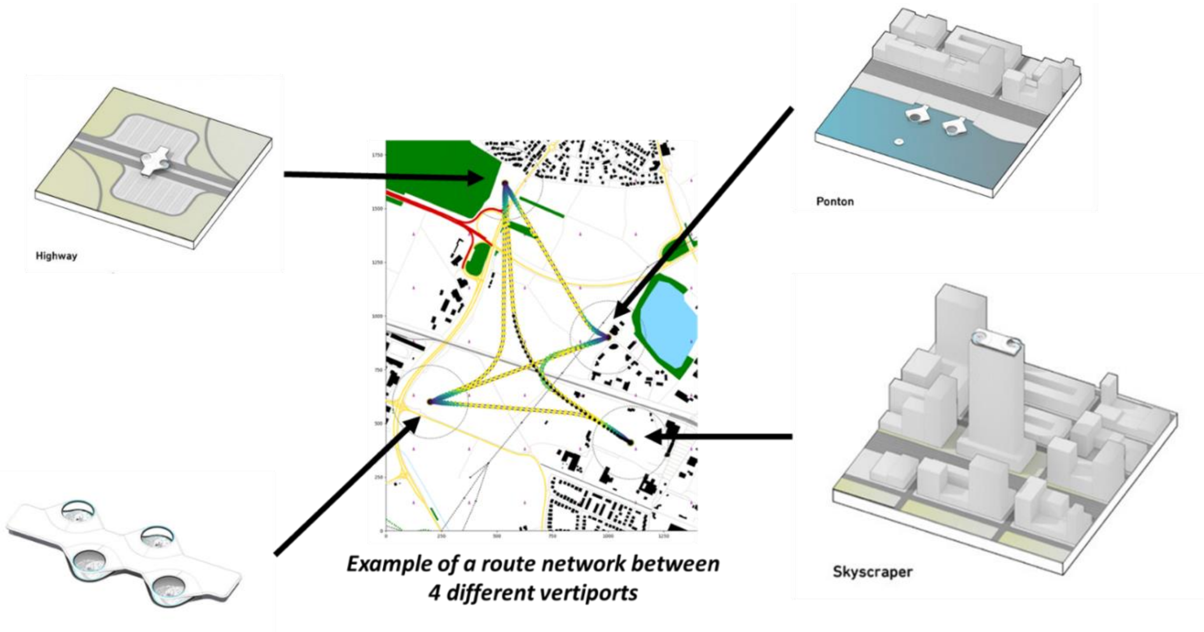
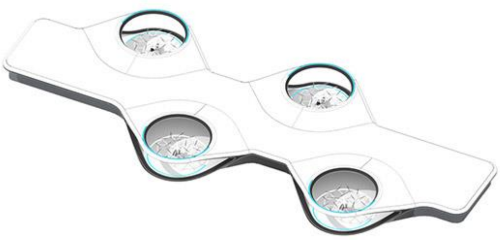


Figure 13: Example network structure with various vertiport implementation

Vertiport location and design influence greatly also the different mission Volocopter will fly. It can be assumed that the operation will be introduced with increasing level of criticality starting from a surface level operation to elevated one and finishing with mixed mode with multiple potential level of landing pad.

a. Surface Level
    i. Ponton (water-to-water over water)
    ii. Highway (critical infrastructure like streets to cross, but open fields)
b. Elevated
    i. Skyscraper (landing on elevated surface, no „open" areas around it, all highest risk)
    ii. Corridor (landing on surface level between building like a combination of highway+skyscraper, confined and no „open" areas around it, all highest risk as well)
c. Surface to Elevated
    i. Tower (landing into different levels depending on designated open slot)



(Left) Multiple vertiport configuration

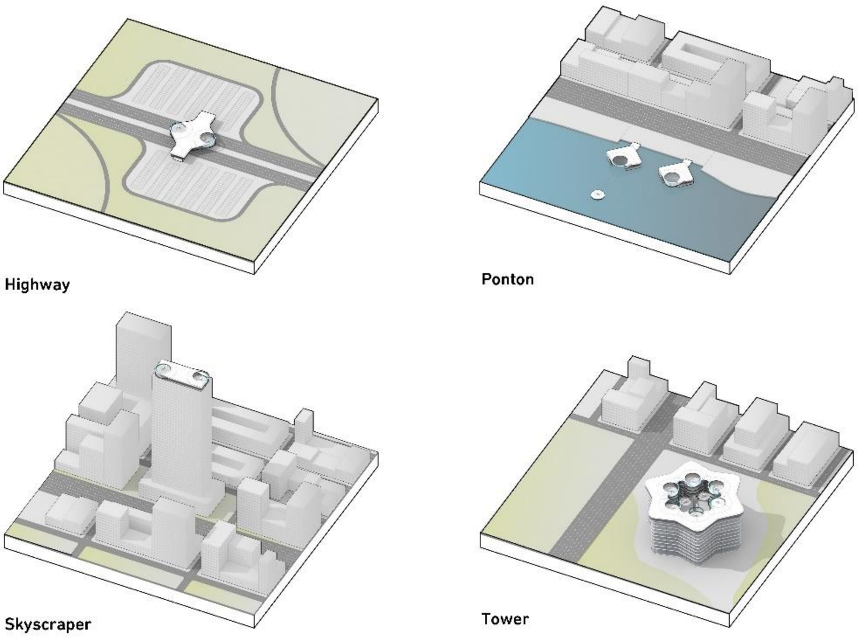


Figure 14: Multiple various vertiport configuration

For the scope of voloCHRIS, we identified two set of *Contingency Cases (CC)*, which are derived below. They are split in mission specific scenarios and GNSS specific cases which can be easily tested at an early stage.

3.2. Contingency cases

All contingency cases are defined first by their respective detection means and their corresponding mitigation action.

3.2.1. (CC 1) Inflight change of destination landing site:

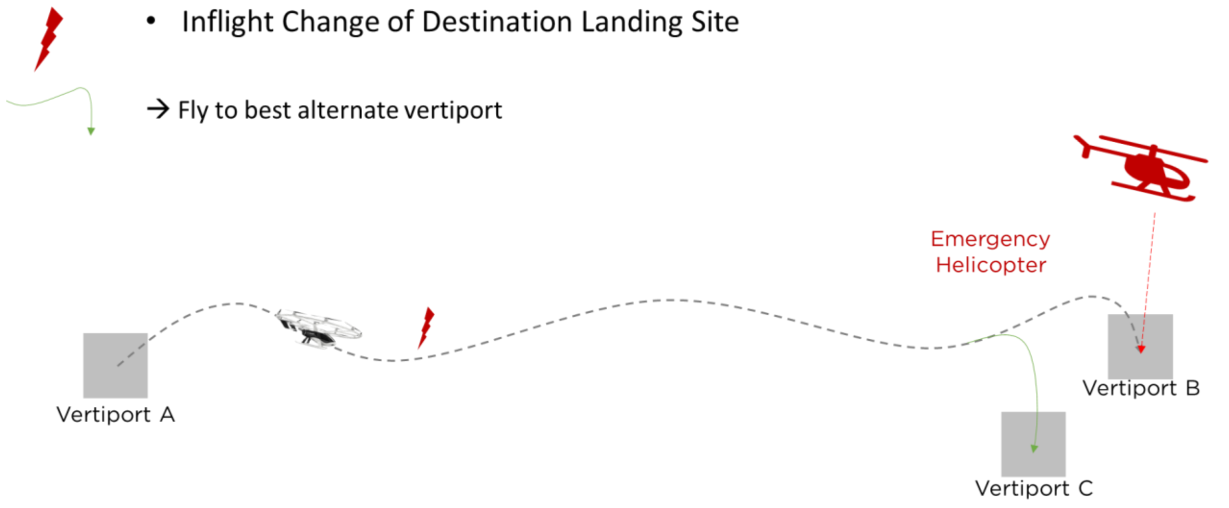


Figure 15: Example contingency trajectories with inflight change of destination landing site

- *Means to detect:*
  - Notification of the inaccessibility of the destination vertiport and potential conflict with priority traffic in the surrounding zone (e.g. from ATC)
  - Thrust reserve limitation
- *Mitigation*:
  - Select alternate/closest landing site
  - Engage contingency maneuver to avoid priority traffic
  - Land at alternate vertiport

3.2.2. (CC 2) Inflight incoming priority traffic encounter:

- *Means to detect:*
  - Notification of potential conflict with priority traffic in the surrounding zone (e.g. from ATC)
- *Mitigation*:
  - Engage contingency maneuver to avoid priority traffic

3.2.3. (CC 3) Loss of Separation:

- *Means to detect:*
  - We monitor the airspace for intruder aircraft with threatening trajectories (e.g. start simple with ADS-B, active sensors to follow)

- *Mitigation*:
  - Select appropriate contingency maneuver to avoid intruder
  - Engage contingency maneuver
  - Closely monitor the intruder's trajectory
  - Continue mission once separation is reestablished.

3.2.4. (CC 4) Loss Link:

- *Means to detect:*
  - On-board C2 & data link equipment signal an interruption in its RX/TX function (Keepalive signal down / time out)
- *Mitigation*:
  - Depending on air space situation and duration of "loss link":
    - Continue as planned for X seconds
    - Prepare "continue mission" of possible (safe)
    - Select closest landing site
  - Inform Airspace user of the unsafe condition (if possible, from air and/or from ground segment)
  - High priority contingency landing at alternate vertiport

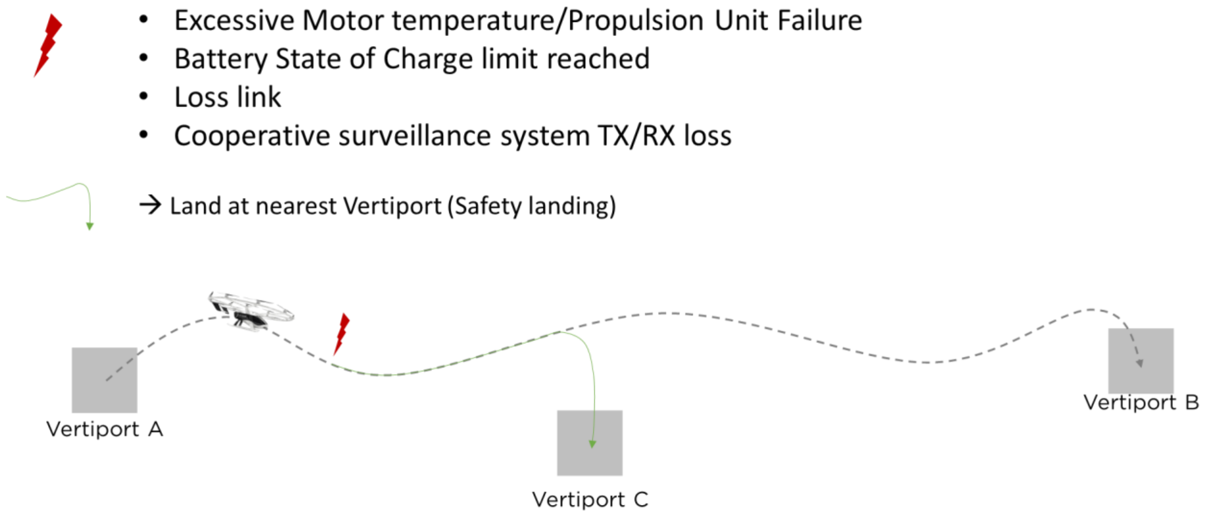


Figure 16: Example contingency trajectories with function degradation

3.2.5. (CC 5) Cooperative surveillance system TX/RX loss:

Broadcast of ownship ID, position and speed is lost

- *Means to detect:*
  - On-board equipment detects a transmission problem
  - Ground segment signals that aircraft track is lost
- *Mitigation*:
  - Airspace user notification of accidentally unregistered aircraft (ground and/or air)
  - Select closest landing site

- Land at alternate vertiport

3.2.6. (CC 6) EPU Excessive Motor temperature

- *Means to detect:*
  - EPU temperature sensor report an excessive temperature
- *Mitigation*:
  - Exit hover flight and limit yaw maneuvers
  - Enter forward flight

3.2.7. (CC 7) Battery State of Charge limit reached

- *Means to detect:*
  - Battery management unit reports a low SoC on one or more of the batteries
- *Mitigation*:
  - Safely switch off the battery pack in low SoC
  - Depending on remaining redundancy:
    - Select closest landing site
    - Land at alternate vertiport

Complete scenarios of these additional systems should be discussed at a preliminary stage already, based on lessons learned from scenarios until CC 7:

3.2.8. (CC-opt 9) Return to home before point of no return

- *Means to detect:*
  - At point of no return, active polling of all necessary infrastructure to continue safe flight
- *Mitigation*:
  - Perform a validation check that all systems are nominal, landing vertiports, ground infrastructure, full redundancy in the overall system

3.2.9. (CC-opt 10) Distinction between different airspace services

- (Non-)Controlled Airspace in general, C vs D-G
- U-Space Operation Type Y (cooperating) vs Z (coordinated)

- *Means to detect:*
  - ATM/U-Space active polling to detect airspace changes

- *Mitigation*:
  - Automatic contingencies rules change depending on flown airspace

4. Aspects of Certification

This chapter discusses the certification considerations for unmanned eVTOL. The challenge of the certification and the integration of such an air taxi into the airspace is that they require a high degree of automation with the vision of unmanned operation, similar to autonomous unmanned aircraft. On the other hand, air taxis need a maximum degree of safety, comparable to the safety of established passenger aircraft (see Figure17 for an illustration).
To give an introduction, first an overview of regulation for established aviation is shown. Afterwards, an overview of the regulation for unmanned aircraft presented. The focus will be on the UAS 'certified' category that is currently in development by EASA. After the overview of regulation, the use of standards will be discussed. From these documents, requirements will be derived that need to be considered for an unmanned eVTOL solution. Finally, there will be an assessment of this analysis.

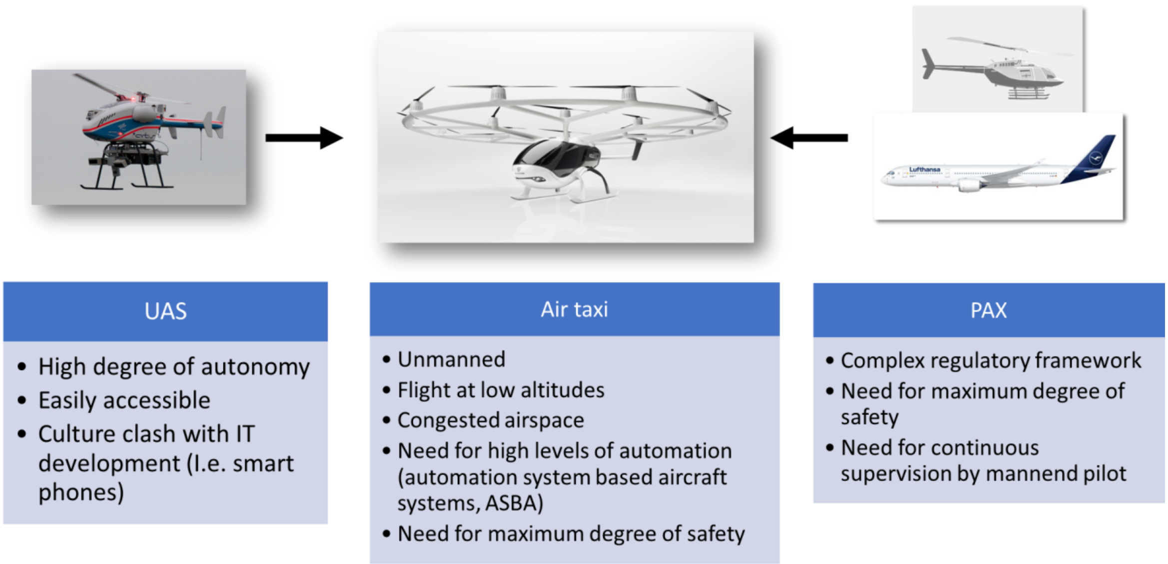


Figure 17: Challenges of air taxi certification

4.1. Regulatory Overview

4.1.1. Regulatory Overview of Unmanned Aircraft

EASA developed 3 categories of UAS operation that can be regulated and certified based on the intrinsic risks involved. The three categories are referred to as open, specific and certified. The open category is reserved for low risk operation under strict restrictions of unmanned aircraft below 25 kg used in visual line of sight (VLOS), requiring no or minimal regulation. The specific category allows a stepwise adaptation of regulation and certification requirements that scales with the actual risks of the operation. The specific category addresses the highest risk class for unmanned operation. The certified category is used for operations that are of an equivalent level of risk comparable to manned aviation, using the same level of rigor and requiring an aircraft type certification, see Figure18.

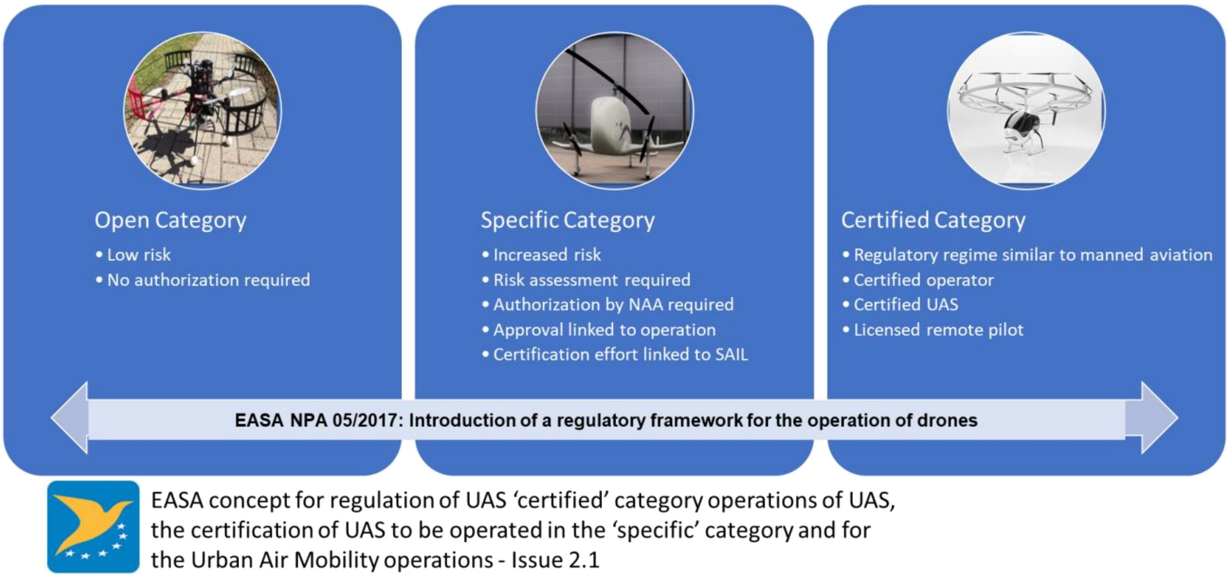


Figure 18: EASA concept for the operation of unmanned aircraft

4.1.1.1. Regulatory Overview of UAS 'certified' category

With the new certified category of unmanned operation, it is necessary to adapt the general existing regulation. Several existing manned aviation regulations are impacted by the new certified category NPA, the scope is shown in Figure 19.

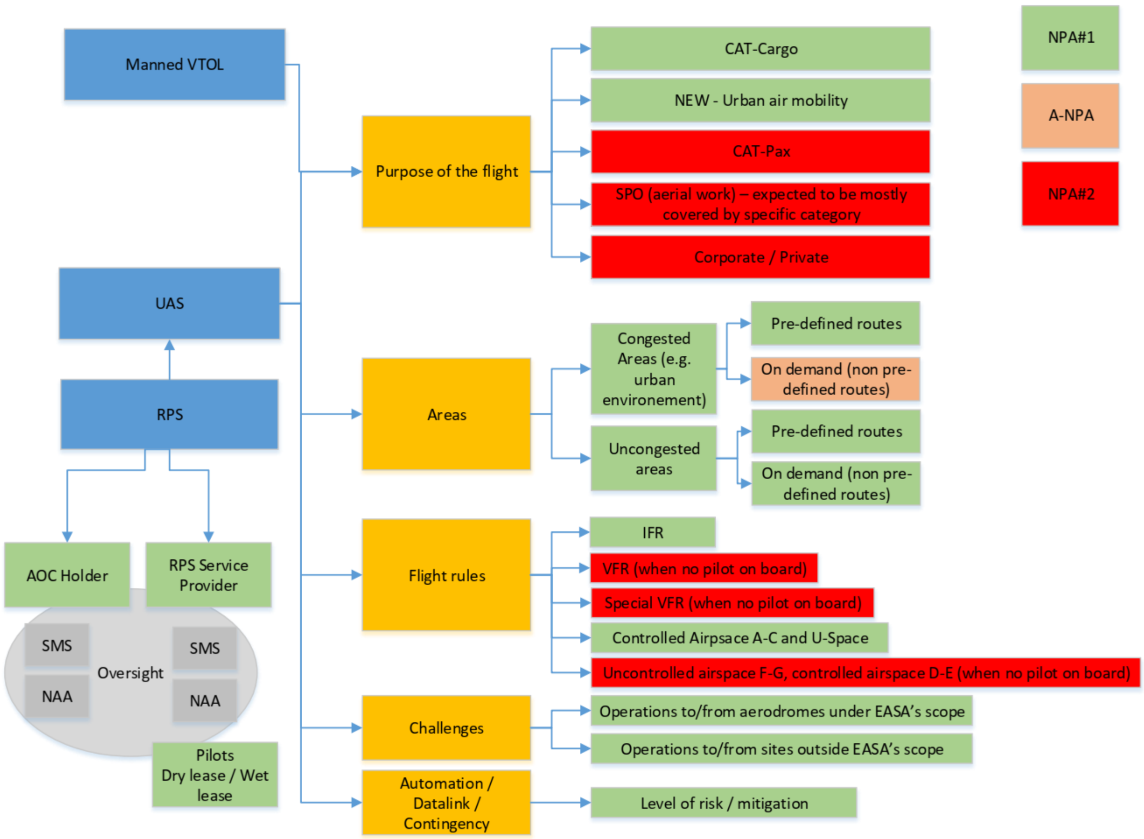


Figure 19: Existing regulation impacted by the certified category NPA[1]

4.1.1.1.1. Airspace Types & U-Space Operation Types

Directly related to the regulation of unmanned aircraft and its operation is the regulation of airspace. A lot of effort is currently put into developing and establishing U-Space. U-Space is a new way of regulating and organizing airspace. Similar to the risk-based approach to regulation of unmanned aircraft with its open, specific and certified categories, U-Space can also be classified by risk, see Figure 20.

[1] Image source: EASA concept for regulation of UAS 'certified' category operations of Unmanned Aircraft Systems (UAS), the certification of UAS to be operated in the 'specific' category and for the Urban Air Mobility operations - Issue 2.1

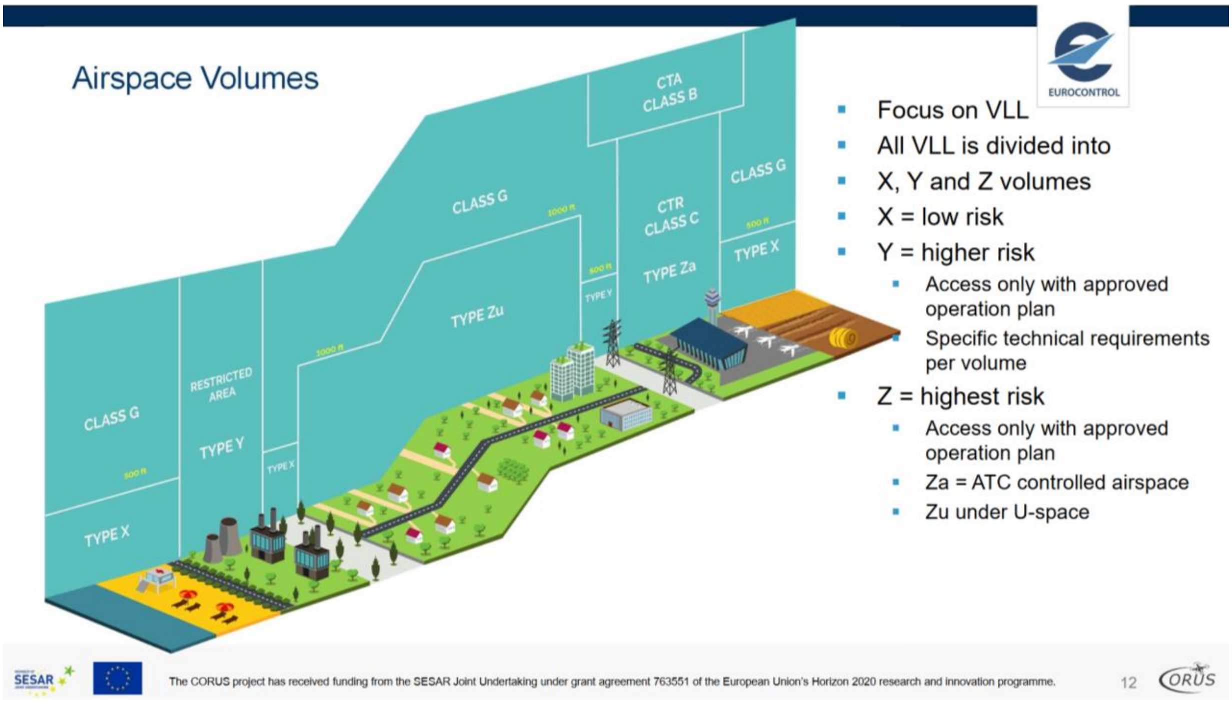


Figure 20: U-Space Airspace volumes[2]

4.1.1.1.2. U-Space Integration for Contingency Management

U-Space provides a number of services/capabilities that will be established in several stages, see Figure 21. More specifically, certain services can interact with the proposed contingency management. U-Space is still in development. However, there is some information on envision services in the different development stages. Services that could be utilized by air taxi contingency management are listed in the following overview by U-Space stage of development.

1. U1
    1. Pre-tactical geofencing
2. U2
    1. Tactical geofencing
    2. Strategic deconfliction
    3. Traffic information
    4. Weather information
3. U3
    1. Dynamic geofencing
    2. Tactical confliction

[2] Image source: https://www.sesarju.eu/sites/default/files/documents/events/U-space%20ConOps%2020190930.pdf

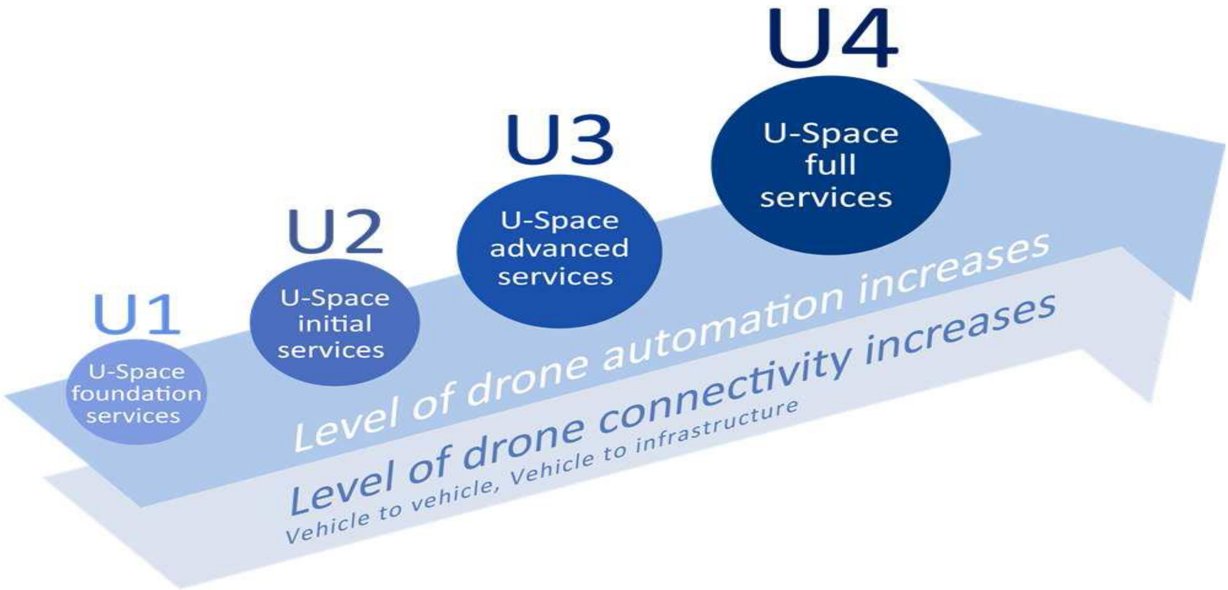


Figure 21: U-Space services roadmap[3]

4.1.1.1.3. ICAO RPS Layer Concept

One important aspect of using unmanned aircraft is the question of remote piloting. The certified category proposes 3 layers of remote pilot stations. The layers are described below and depicted in Figure 22:

- Layer 1 - **RPS Core Layer**: all elements and equipment essential for the crew to operate the RPA
- Layer 2 - **Intermediate Layer**: all assets, equipment and resources required to support the RPS operation, to provide interface between the core and external layers and to provide protection from "undesired inputs" such as hacking, lighting, power failures, EMI etc.
- Layer 3 – **Outer World Layer**; Commercial & Public Infrastructure, External Networks, C2Link Service Provision

[3] CORUS - U-space Concept of Operations (Project Report)

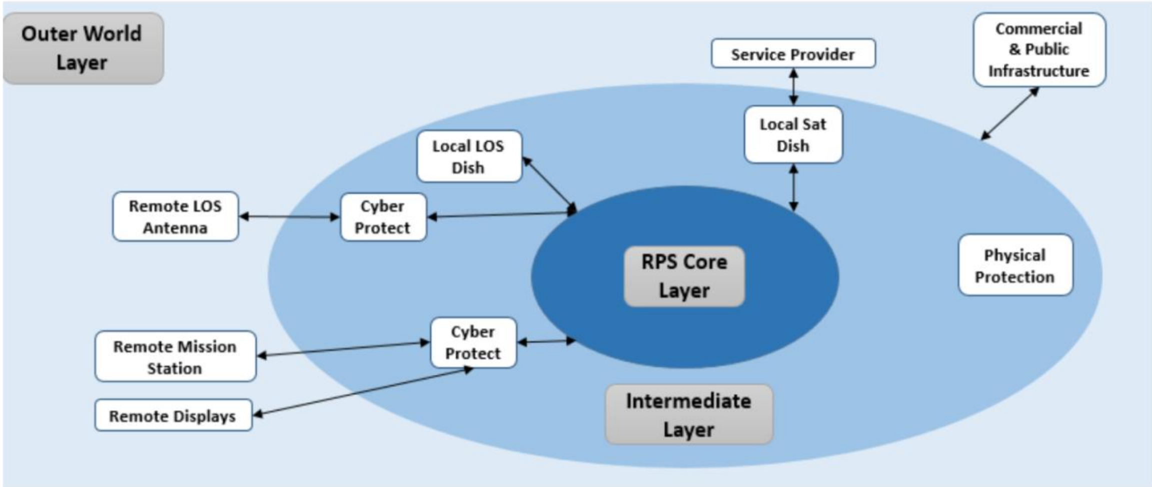


Figure 16: ICAO RPS Layer Concept[4]

4.1.1.1.4. Operation Types (Certified Category)

Within the certified category there are 3 subtypes of operation. The subtypes are defined as follows:

- Operations type #1: IFR operations for the carriage of cargo in airspace classes A-C and taking-off and landing at aerodromes under EASA's scope.

- Operations type #2: Operations of UAS taking off / landing in congested (e.g. urban) environment using pre-defined routes in volume of airspaces where U-space services are provided (…). These include operations of *unmanned automation system – based aircraft (ASBA)*, carrying passengers (e.g. … VTOL air taxis) or cargo (e.g. UAS providing goods delivery services). Take-off and land could be at any aerodrome or any designated landing port, vertiport or landing site.

- Operations type #3: same as Operation type #2 with manned ASBA, including operations in airspace where U-space service is not available.

This distinction gives us additional information. With this project VoloCHRIS, we are targeting unmanned operation of eVTOL air taxis, and thus clearly falling into operations of type 2. However, Volocopter has a roadmap that will first utilize manned operation. With the use of

[4] Image source: EASA concept for regulation of UAS 'certified' category operations of Unmanned Aircraft Systems (UAS), the certification of UAS to be operated in the 'specific' category and for the Urban Air Mobility operations - Issue 2.1

onboard pilots, this falls into the category of operations type 3. The distinction is further depicted in Figure 23.

Figure 23: Certified category types of operations[5]

4.1.1.1.5. Concept for the Certified Category Operation of UAS

The envisioned regulation structure contains vertical and horizontal elements, see figure below. Horizontal elements define for example the aircraft structure, and vertical elements describe specific features across multiple horizontal options.

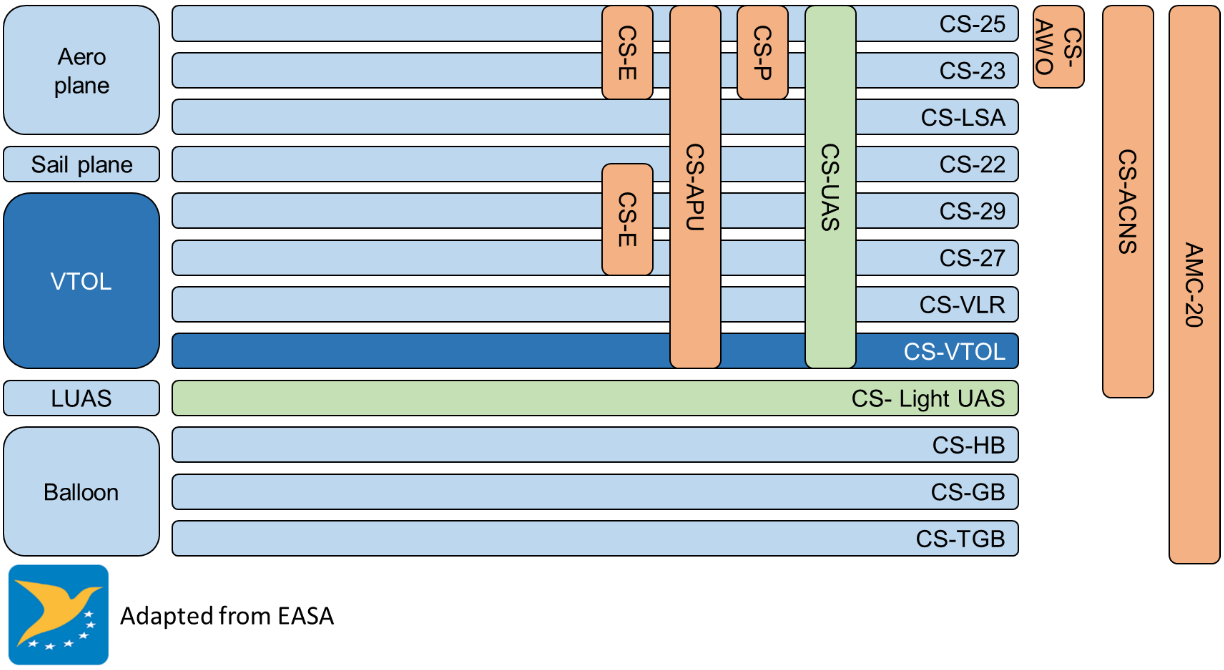


Figure 24: EASA envisioned regulatory structure for aviation[6]

[5] Image source: Wikipedia, https://de.m.wikipedia.org/wiki/Datei:Flugzeug_unten.svg

4.1.1.1.6. SC-VTOL versus CS-VTOL

Although proposed by the certified category NPA, there is no CS-VTOL yet. However, there is a Special Condition for small-category VTOL aircraft, published by EASA in July 2019. The special condition was developed in cooperation with Volocopter. It is based on "CS-23 Normal, Utility, Aerobatic and Commuter Aeroplanes", see also Figure 24: EASA envisioned regulatory structure for aviation4. It describes necessary modifications to the existing CS- 23, due to electrical propulsion and multirotor aspects. Furthermore, the special condition describes 2 subcategories for unmanned aircraft with different requirements for their certification. These categories are

- Category Enhanced
- Category Basic

The major difference for these categories is the resulting failure condition classification, shown in Figure 25: Failure condition classifications by category for the SC-VTOL5. The relevant category for the scope of this project is the category enhanced, because this category is required for operation and urban areas.

		Failure Condition Classifications			
	Maximum Passenger Seating Configuration	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Category Enhanced	-	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
Category Basic	**7 to 9 passengers**	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
	2 to 6 passengers (see note A)	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL C	$\leq 10^{-8}$ FDAL B
	0 to 1 passenger (see note A)	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-6}$ FDAL C	$\leq 10^{-7}$ FDAL C
[Quantitative safety objectives are expressed per flight hour]					

Figure 25: Failure condition classifications by category for the SC-VTOL[7]

[6] Image adapted from: EASA concept for regulation of UAS 'certified' category operations of Unmanned Aircraft Systems (UAS), the certification of UAS to be operated in the 'specific' category and for the Urban Air Mobility operations - Issue 2.1
[7] Image source: EASA concept for regulation of UAS 'certified' category operations of Unmanned Aircraft Systems (UAS), the certification of UAS to be operated in the 'specific' category and for the Urban Air Mobility operations - Issue 2.1

4.2. Standard Overview

While existing regulations adhere to a certain structure, this is not necessarily the case for standards. However, standards describe Industry consensus with a set of best practices. As such, standards are an applicable means of compliance (AMC) to comply with regulations. An ongoing EU project "AW-Drones" is currently gathering the set of standards applicable to UAS, see Figure 26: Logo of the AW-Drones project26. The focus in the first phase is on the specific category, however also standards for the certified category are gathered systematically by partners across the European Union. There are currently more than 600 standards on the topics of Initial airworthiness, Continuing airworthiness, UAS operations, Aerodromes, and others. In the scope of this project, it is not possible to give a complete overview of relevant standards. The focus is on relevant standards for software development and operational safety.

Figure 26: Logo of the AW-Drones project[8]

4.2.1. Software Standards

The applicable software development standards in the context of eVTOL are the following:

- RTCA DO-178C - Software Considerations in Airborne Systems and Equipment Certification
- *RTCA DO-330 - Software Tool Qualification Considerations*
- *RTCA DO-331 - Model-Based Development and Verification Supplement to DO-178C and DO-278A*
- *RTCA DO-332 - Object-Oriented Technology and Related Techniques Supplement to DO-178C/DO-278A*
- *RTCA DO-333 - Formal Methods Supplement to DO-178C and DO-278A*

4.2.2. Operational Safety

There exist standards for operational safety that are applicable to the project use case:

- ASTM F3269–17 Standard Practice for Methods to Safely Bound Flight Behavior of UAS Containing Complex Functions

The standard describes architecture and requirements to ensure safe operation by monitoring the system state and switching to one or more backup systems in case of unsafe behavior. As a result, it is possible to constrain the behavior of untrusted functions. For example, this

[8] Image source: AW-Drones Project

architecture can enable to utilize artificial intelligence safety within an unmanned aircraft. The characteristics of the standard can be summarized as follows; the corresponding architecture is shown in Figure 27: ASTM architecture to safely constrain the flight behavior of UAS containing complex functions27. To utilize the architecture in context of this project, an adaptation is necessary. The adaptations described in the next section.

Characteristics of ASTM standard for operational safety:

- Define safety requirements
- Continuous monitoring of system state
- Triggering of save recovery function

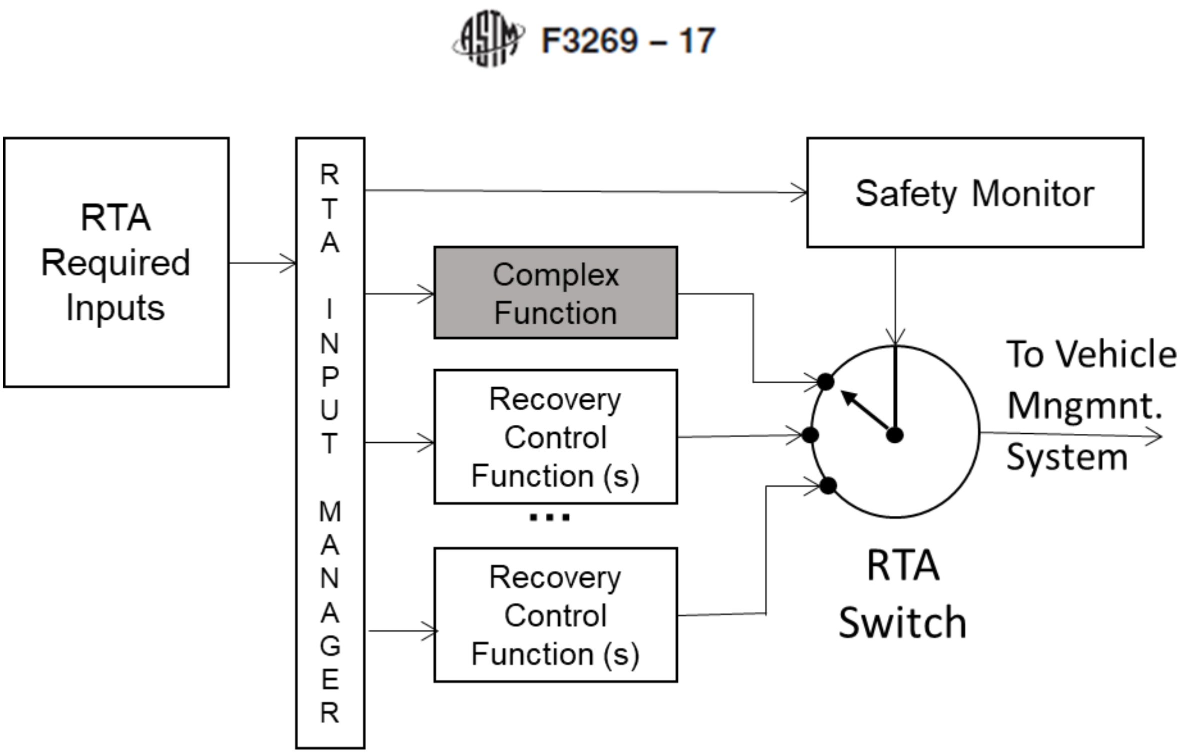


Figure 27: ASTM architecture to safely constrain the flight behavior of UAS containing complex functions[9]

4.3. Derived Requirements

With the analysis done in this chapter, we can derive a number of requirements that a possible solution for the contingency management must comply to. At first the regulatory framework is summarized, before the derived requirements for the software architecture and the run-time assurance architecture are described.

[9] ASTM F3269-17 Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions

The urban air mobility, envisioned with the VoloCHRIS project is unmanned, with no pilot on board. This requires the application of the *EASA regulatory framework for unmanned aircraft operation*. The criticality of the operation falls into the *certified category.* The certified category addresses high-level changes to the European Basic Regulation. This category has subtypes for the allowed types of operation. The project targets to use operations of type 2, requiring predefined routes in airspaces that provides U-space services. Takeoff and landing has to take place at designated vertiports. The unmanned operations are supported by of unmanned automation system – based aircraft (ASBA). The special condition SC-VTOL dictates the use of highest criticality, i.e. FDAL A.

4.3.1. Software Architecture

From software perspective, the following requirements can be derived:

- Use of predefined routes for contingency handling
- Automation is supported using unmanned automation system – based aircraft (ASBA)
- Certification should be performed using the DO-178C family of standards, up to level A
- Use of a robust, verifiable implementation approach
- The use of U-Space services has to be integrated
- Application of an adapted runtime assurance architecture
- Deterministic decision-making

4.3.2. Run-time Assurance Architecture

With the availability of the standard for safe runtime architectures by RTCA, it is possible to develop a safe architecture for the management and execution of contingencies. To do this, the existing architecture from the standard document has to be adapted. This architecture shall allow the vehicle to safely switch from the nominal trajectory to a contingency trajectory. Similarly, a switch from one contingency trajectory to another contingency trajectory should also be possible. A key component of this architecture is the safety monitoring, which uses predefined properties to assess the vehicle as well as the operational state and health. The RTA switch/contingency manager uses this information of system and operational health to switch to the optimal contingency trajectories with known, fixed properties.

5. Development of a Contingency Module

The contingency management module should provide a safe and feasible contingency trajectory in case needed. Figure 28 shows the nominal trajectory from start to destination landing site. In addition, several contingency trajectories to alternate landing sites are shown, which might be used if the destination landing site is blocked or a system failure requires a prompt landing. Furthermore, a circular holding pattern is shown, which might be a feasible contingency trajectory to react on priority traffic or scenarios with loss of separation. Contingencies of maintaining operability of the aircraft's sub-systems (e.g. sensor fusion, actuators, propulsion system) can be found in [3], but are not focus of this work.

Figure 28: Example contingency trajectories with alternate landing sites.

Requirements

Based on the aspects of certification (see chapter 4) the following basic requirements to the contingency management are derived.

- Deterministic decision making
- Hard runtime and memory constraints
- Handle multiple/simultaneous contingency cases
- Provide complete set of feasible contingencies
- Provide best contingency (safety, comfort, timeliness, …)
- Integrate with existing control system
- Extendable for additional contingency cases

System architecture overview

The proposed contingency management module is depicted in Figure 29. Data sources provide information for the monitor module which gathers the information and processes the information for the contingency management module. The contingency management gets the information from the monitor module and decides if a contingency trajectory needs to be executed. Therefore the contingency manager can access a database with pre-planned contingency trajectories. If required, the contingency manager provides the best, feasible contingency trajectory to the mission manager, which executes the contingency trajectory. In the following, the modules are explained in detail.

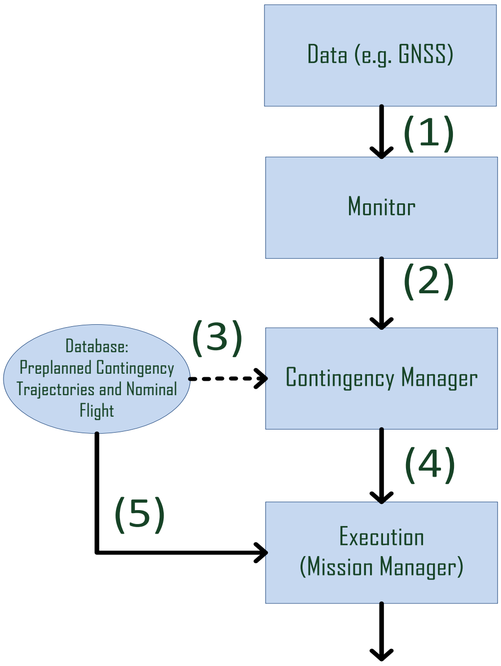


Figure 29: Software architecture and dataflow of the contingency management

5.1. Monitor

The monitor module collects information from various sources and combines, analyses them. The outputs are information which are interpretable by the contingency management module. This architecture with a separate monitor module is widely used [1, 2, 3, 4]. The monitoring for data streams with the LOLA specification language on an unmanned aircraft is described in [9].

The following information may be received by the monitor module according to the contingency scenarios (or contingency cases CC) from Chapter 3.

Information	**Reference Contingency Scenario/Case**	**Notes**	**Datatype**
Interfering aircraft	CC 1, CC 2, CC 3	Potential conflict; CC 3 including positions of intruders	• Set of current positions representing possible intruders (more CA) • List of Booleans representing blocked trajectories (ATC priority)
Status Vertiport	CC 1	i.e. inaccessibility	List of Booleans representing

			Vertiport availability
Rotor information	CC 1	i.e. thrust	Status msg
Datalink degradation	CC 4, CC 5		Current upload and download rates, keep alive signal
Ground information	CC 5		Track deviation
Motor temperature	CC 6		Temperature
Battery status	CC 7		For each battery, boolean representing low state of charge

An overview of various data sources of the monitor module can be found in Figure 30. In Figure 0 sources are categorized in on-board (internal) and off-board (external) data sources. Within the prototype implementation in this project, some modules are implemented as emulators.

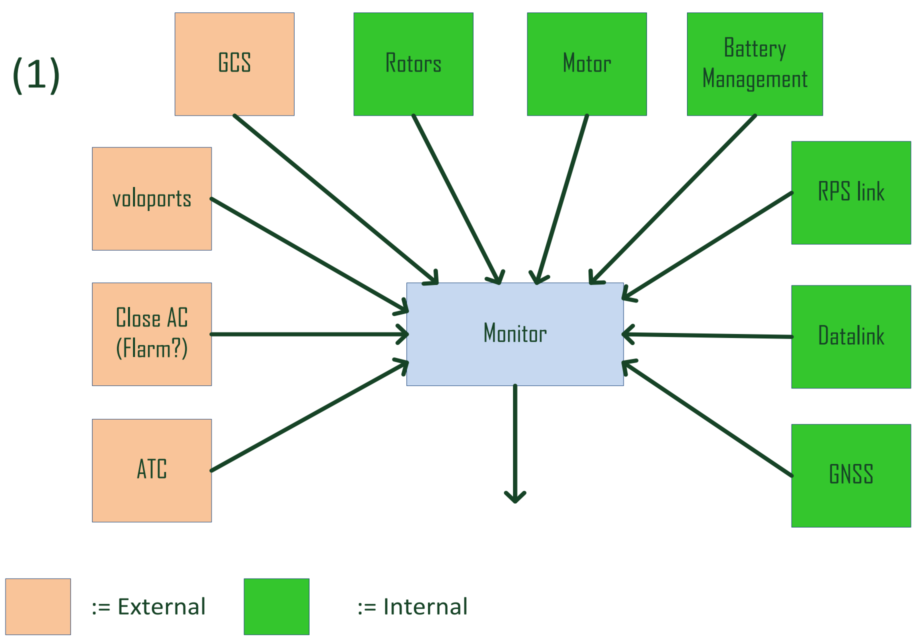


Figure 30: Monitor and data sources

5.2. Contingency Module

The contingency module, or contingency manager, decides based on the information from the monitor, which contingency trajectory is commanded to the mission manager (mission execution module). Finding a feasible contingency trajectory can be understood as a path planning problem. Starting from the state space $\mathbb{X}$ and the configuration space $\mathbb{C} \subset \mathbb{X}$, a feasible contingency trajectory $q: [0, t_f] \rightarrow \mathbb{C}_{free}$ must be found through the collision free space $\mathbb{C}_{free} \subset \mathbb{C}$. Various path planning approaches exist for finding a feasible solution for this problem.
In case of a contingency scenario, the planning space, i.e. state space and configuration space are restricted. As an example, a blocked landing site, or no-fly zones introduce additional obstacles to the configuration space, or in other words limit the free space $\mathbb{C}_{free}$. A damaged propeller might limit the flight envelope of the vehicle or in other words the feasible state space $\mathbb{X}$ of the aircraft. A planning algorithm can then plan a new feasible trajectory given the new requirements. **Fehler! Verweisquelle konnte nicht gefunden werden.**28 shows the changing planning spaces during flight. In case no safe contingency exist, an emergency landing is initiated.

In the proposed approach the path planning is not performed in-flight but limited to a set of a-priori provided contingency trajectories. This solution is a result of the requirements stated above. The main reasons are the bounded runtime and the requirements of pre-defined flight routes coming from SC-VTOL category 2.
The contingency manager gets information about the capabilities of the vehicle and the environment (information about $\mathbb{C}, \mathbb{X}$) from the monitor and selects the best contingency trajectory from the database based on this information.

Obtaining feasible contingency trajectories, predefined routes are definitely a very static solution. Online Planning algorithms provide much more flexible solutions, but are much more difficult to validate in means of correctness and runtime assurance. The approaches in [5, 6] describe configurable and runtime efficient planning algorithms based on cyclic search graphs, where the motion planning problem and combinatorial problem is solved online. In [7] the motion planning problem is solved offline and trajectory segments are stored in a database. The combinatorial problem is still solved online. In contrast to this work, other contingency management approaches assume online planning methods [2, 4]. The choice of the static trajectory library can be found in the ACAS-X framework [8] for example, where static lookup tables are used to provide the best actions to avoid traffic collision. The proposed method could be extended with an online planning module and still use pre-determined routes as a (validated) fallback.

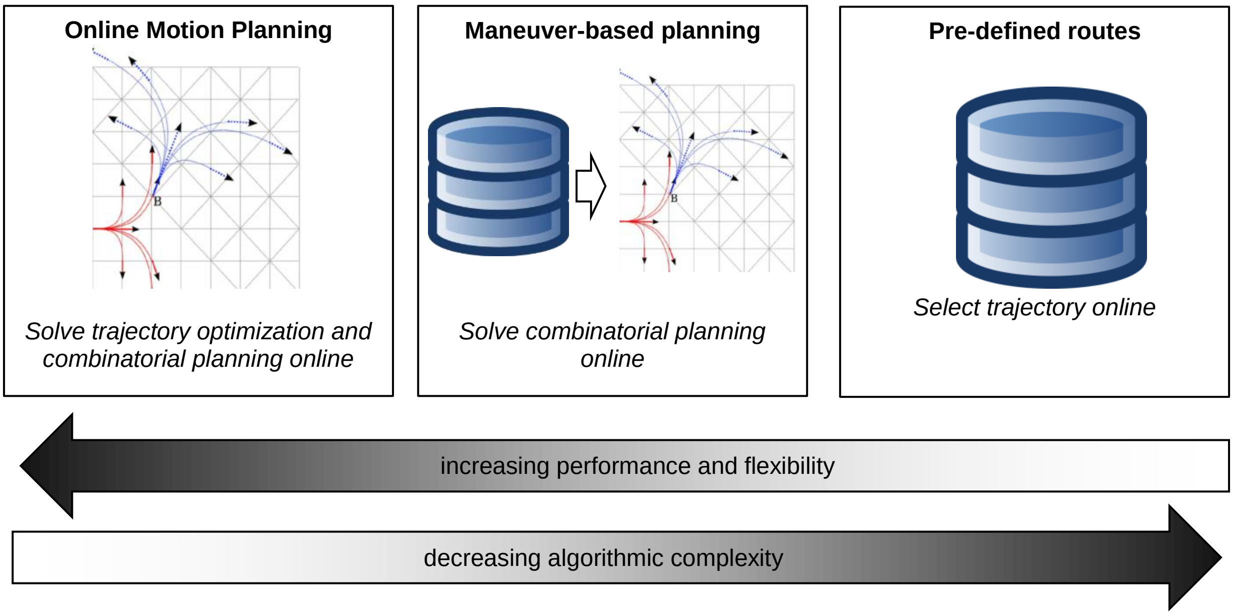


Figure 32: Online versus offline path planning approaches

5.3. Trajectory Database

The trajectory database stores the nominal trajectory and available contingency routes. Within the proposed approach, each trajectory guides the vehicle to a landing site. The aircraft does not return to the nominal trajectory, even if the contingency path is spatially equal to the nominal path in certain segments.

5.4. Contingency Architecture

The system consisting of sensors or other data sources, monitor, contingency manager, and mission manager are integrated as depicted in Figure . As the contingency manager advised the mission manager to switch to a specific contingency trajectory, the system remains modular and a basic system without contingency management requires no changes to the overall system. Figure returns to the initial conceptual design in Figure and guides the reader through the implementation and validation of the system in a real-world application within the next chapter.

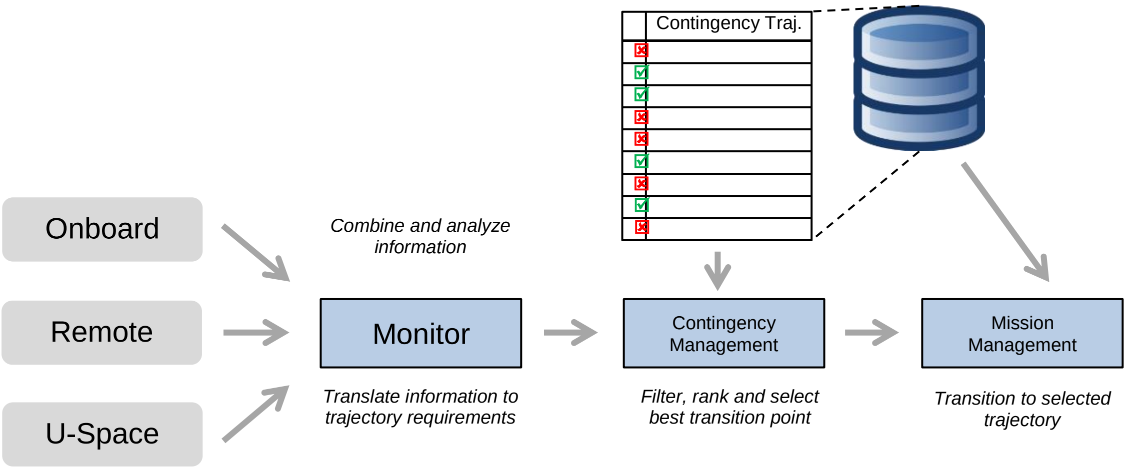


Figure 33: Information flow diagram

Bibliography

[1] [In-Flight Contingency Management for Unmanned Aerial Vehicles, Enric Pastor, Pablo Royo, Eduard Santamaria, Xavier Pratsy, Cristina Barrado, AIAA Aerospace Conference 2009]

[2] [Onboard Decision-Making for Nominal and Contingency sUAS Flight, Joshua Baculi & Corey Ippolito, AIAA SciTech 2019]

[3] [Integrated Vehicle Health and Fault Contingency Management for UAVs - Michael J. Roemer and Liang Tang Handbook of Unmanned Aerial Vehicles, 2015]

[4] [Automated Contingency Management in Unmanned Aircraft Systems, Hector Usach PhdThesis , 2019]

[5] [Reconfigurable Path Planning for Fixed-Wing Umanned Aircraft Using Free-Space Roadmaps, Benders, 2018]

[6] [Minimum-Risk Path Planning for Long-Range and Low-Altitude Flights of Autonomous Unmanned Aircraft, Schopferer, Benders, 2020]

[7] [Benchmarking Unmanned Rotorcraft Trajectories based on Dynamic Fit, Verma, Benders, Dauer, Adolf, 2018]

[8] [Next-generation airborne collision avoidance system, Kochenderfer, Holland, Chryssanthacopoulos, 2012]

[9] [Stream Runtime Monitoring on UAS, Adolf, Faymonville, Finkbeiner, Schirmer, Torens, 2017]

6. Implementation and Validation

Scope of this part is the implementation and integration of the contingency management concept into the existing scaled Volocopter demonstrator. Also, simulation and flight test results are given.

6.1. System Integration

The final system prototype architecture is given in Figure 34. Prior to the project, the applications "Flight Controller", "FC-SDK", "Trajectory Controller", "Mission Management", and "Ground Control Station" already existed. For the internal communication between applications the library ZeroMQ [1] is used.

For the integration of the developed prototype contingency management, new applications had to be written and connected to the internal communication.

A brief explanation of the individual applications follows:

- Flight Controller: Controls the vehicle i.e. the scaled Volocopter demonstrator
- FC_SDK: Interface between the Flight Controller and the onboard autonomy functions
- Trajectory Controller: Executes trajectory and transitions from one trajectory to another
- Mission Manager: Manages the flight phases, e.g. take-off, on-cruise, landing
- Ground Control Station: Umbrella term for the offboard applications
- Monitor: Receives all necessary data and abstracts them into an abstract status notion
- Contingency Management: Receives abstract status information and chooses the "best" contingency trajectory if a contingency is necessary.
- To test failures during simulation and flight testing, emulators were written:
  - Sensor Emulator: Emulates state-of-charge, rotor failures, etc.
  - UTM Emulator: Blocked/freed trajectories and landing sites

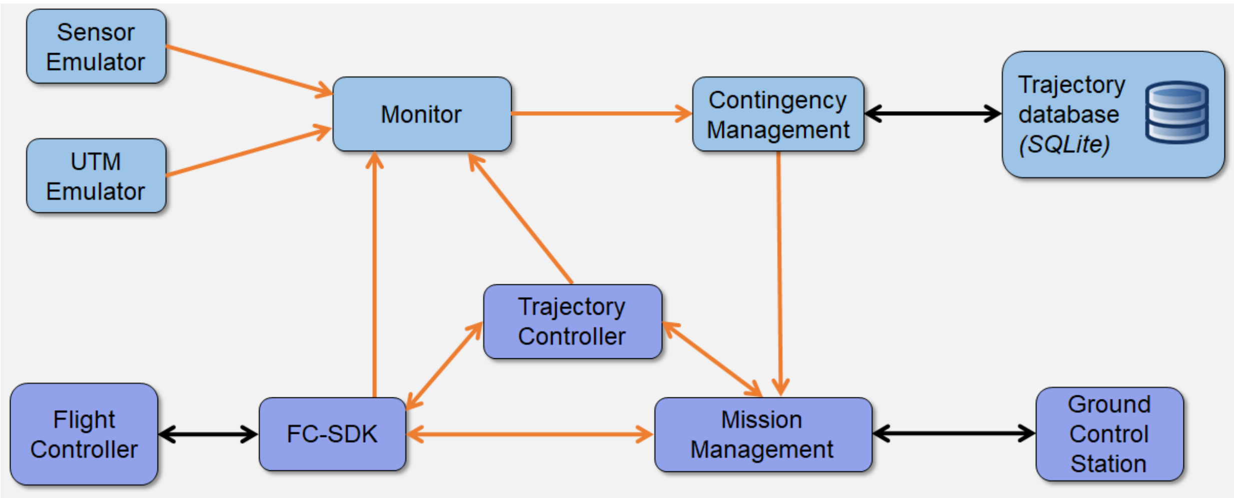


Figure 34: Prototype system architecture

When the contingency management receives status information from the monitor, it prepares a query to receive a set of valid contingencies. Afterwards, the best contingency within the set of valid contingencies is send to the mission management if needed.

6.2. Flight Test Planning

In order to validate the implemented contingency management, we used software in the loop, hardware in the loop, and a final flight test. An overview is given in Figure35.

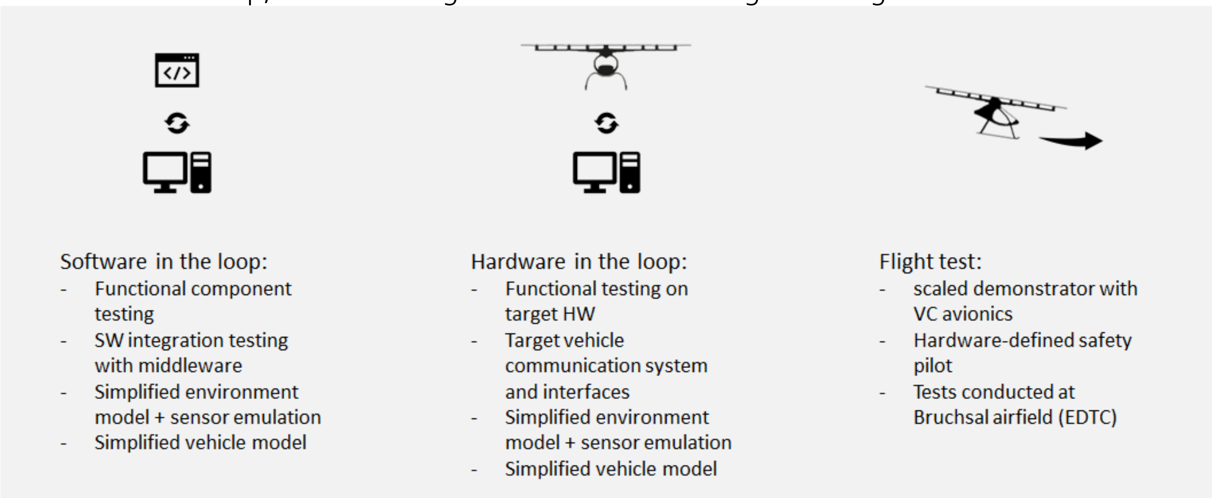


Figure 35: Testing sequence: From simulation to flight test

6.2.1. Prototype

The scalable Volocopter demonstrator which was used for hardware in the loop simulations and flight testing is shown in Figure 36. The demonstrator uses Volocopter specific avionics, e.g. Volocopter Pegasus flight controller and mesh. The maximal take-off weight is approximately 12kg, the gross weight is 5.5kg, and the thrust to weight ratio is 3. As flight guidance computer, the UP^2 maker board with Intel Pentium N4200, 8GB RAM, 64GB memory, running Linux was used. The UP^2 board provides enough resources to run the mentioned applications. Used navigation sensors were: GNSS, barometer, Industrial EO, and radar altimeter. For the software in the loop simulation, as flight controller and fc_SDK, px4 [2] and mavSDK [3] were used, respectively. As multirotor simulator, jMAVSim [4] was used.

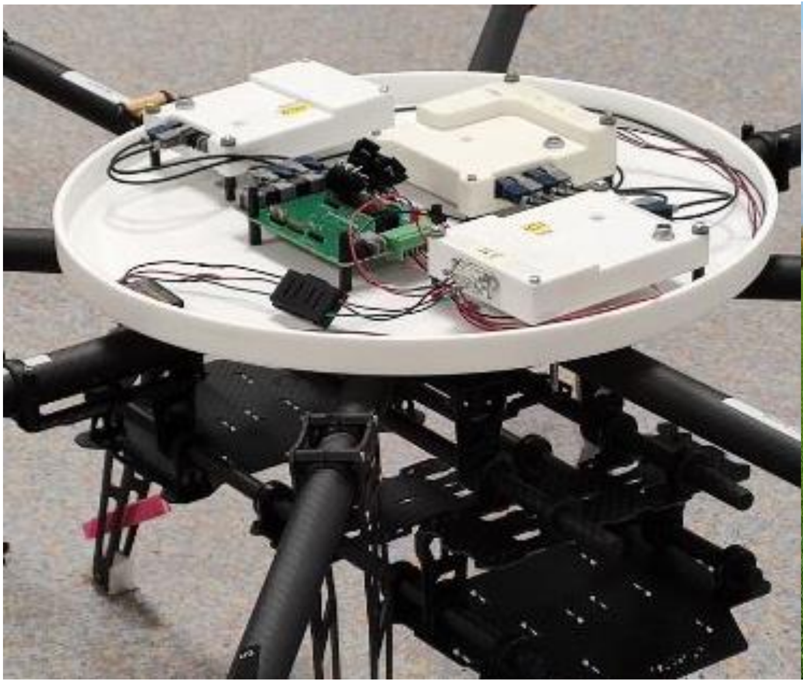



Figure 36: The Volocopter scaled demonstrator used in flight tesing

6.2.2. Mission

For the simulation and the flight test, the same test scenario selection was used. The chosen scenarios were: occupied landing site, priority traffic, and critical state-of-charge.
Figure 37 illustrates the test setup. Starting at Bruchsal airfield VP1, somewhere on the nominal trajectory a contingency event happens upon which the contingency management has to choose a corresponding valid contingency trajectory. Four alternative landing sites were considered and the approximately flight distance was around 300m.

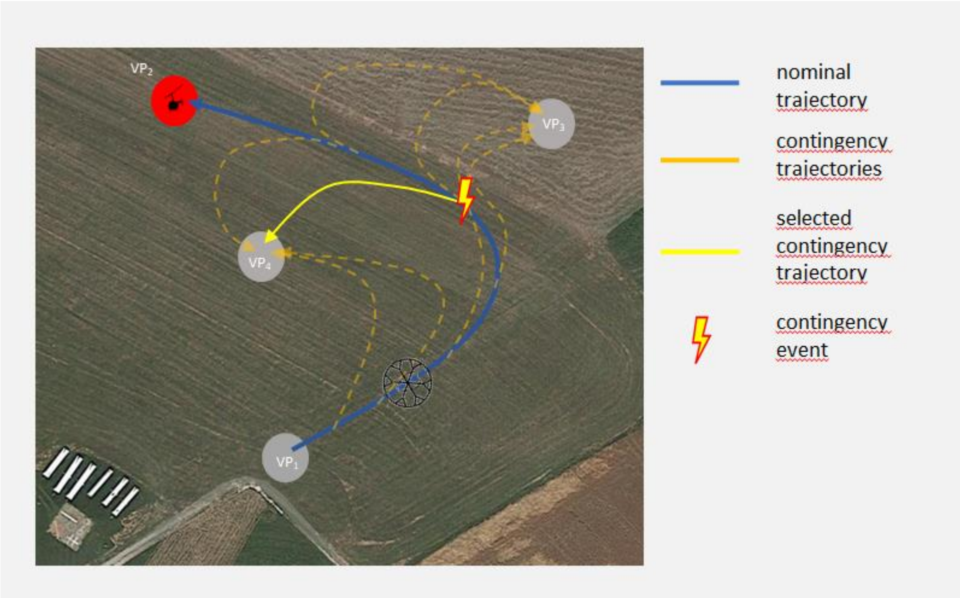


Figure 37: The flight test vehicle reacts to a contingency event. An alternative landing site is selected in flight.

6.3. Professional Discourse

6.3.1. Simulation Results

The described contingency management system and a database of pre-determined contingency trajectories was integrated into a software-in-the-loop (SIL) environment and tested with the scaled vehicle's flight guidance and control software. For demonstration a scenario in which an intruder vehicle lands on the destination landing site, thereby making it inaccessible to the ownship, is selected. The flight distance of the nominal trajectory is about 300m with two additional landing sites located north and south of the nominal flight path, respectively. The vehicle takes off and follows the nominal trajectory. The vehicle receives a notification about the described event at the destination landing site and selects the best contingency trajectory from the set of trajectories following a pre-defined decision logic. In the particular test case we select the shortest trajectory which reaches the landings site closest to the initial destination. The vehicle follows the chosen trajectory to the corresponding alternative landing site.
The observed results show that the described contingency management and database handling modules could be integrated successfully into the existing software environment. The vehicle's behavior following the injection of a contingency event complies with pre-test expectations and validates the presented approach. The herein presented results from SIL tests were reproduced in a hardware-in-the-loop (HIL) setup, paving the way for final validation of the developed contingency management system in a flight test campaign.

6.3.2. Flight Test Results

Following successful testing of the presented approach in SIL and HIL, flight tests were planned as a final validation step in order to demonstrate the developed software modules' maturity level. The flight test should follow the same mission profile as SIL and HIL tests and were intended to be executed at Bruchsal airfield EDTC.
For this purpose the contingency module was ported to the scaled technology demonstrator described in Section 6.2.1. The guidance software and sensor suite installed on this demonstrator enable it to execute automated missions from take-off to landing. In order to test the developed software modules in a realistic context a contingency event simulating an occupied destination landing site should be triggered from a remote test operator during nominal mission execution. The vehicle is expected to repeat the behavior observed in simulation testing and land at an alternative landing site without further intervention from a remote pilot. Due to repeated delays in the flight testing schedule, the planned flight tests could not be executed during the project period. In the following months, the Corona-crisis and related restrictions prevented flight test execution in time to include flight test results in the final project report. However, flight tests are an integral part of ongoing developments and extensions of the voloCHRIS concept and will be continued, once the circumstances allow.

6.3.3. Open Discourse at Final Event

The project research results were presented to an expert audience consisting of representatives from research universities and DLR as well as industry partners. The project results were brought up for discussion with the audience following the presentations. In this discussion, the concepts developed within the project were validated and found plausible by the present domain experts. The operational concept and assumptions towards further development of the voloCHRIS approach could be validated as well. In addition to valuable feedback on the current prototype system, several potential extensions and subjects of future work on contingency management systems could be identified.

The topics most intensively discussed at the final event were (in no particular order):

- Challenges for unmanned flight beyond visual line of sight (BVLOS)
- Equipment required for autonomous flight (e.g. sensors)
- Target level of autonomy and timeline / roadmap for realization
- ATC/UTC/U-space integration for unmanned flight
- Datalink requirements and techonologies
- Detect and avoid requirements and technologies
- Navigation performance, navigation aids and sensors
- Contingency trajectory planning and trajectory databases
- Certification challenges

A detailed summary of the final event can be found in the document "Publikationen".

[1] https://zeromq.org/

[2] https://px4.io/

[3] https://mavsdk.mavlink.io/develop/en/index.html

[4] https://dev.px4.io/v1.9.0/en/simulation/jmavsim.html

7. 1. Conclusions and Outlook

Within the scope of the voloCHRIS project, a system for automated contingency management for an eVTOL passenger aircraft was designed, developed and demonstrated in flight. As a first step, a set of contingency cases were defined in order to derive requirements for the automated decision-making system. The cases include unexpected situations such as high priority traffic encounters, loss of separation or changes of landing site and also cases of system degradation or performance limitation such as link loss, GPS satellite loss or excessive motor temperature.
Also, an analysis of the regulatory framework for autonomous unmanned flight was conducted. The set of currently applicable standards was examined and safety-related requirements regarding the architecture of the contingency management system were derived. Based on this groundwork, a concept for technological realization of an automated contingency management system was developed and documented. Based on a prototypical implementation, the concept was demonstrated in simulation and flight test using a scaled flight demonstrator.

The overarching objective of the voloCHRIS project was to increase acceptance of technologies related to autonomous eVTOL passenger aircraft. The vision of autonomous flight in urban areas was presented to the general public with a video that shows the context and the challenges as well as the currently targeted technological solutions in an easily comprehensible form. The video is expected to be of great value for the near future, to serve as a discussion starter, to educate the general public and to raise awareness for the opportunities associated with the envisioned concepts of urban air mobility. For the expert community, preliminary insights from designing, developing and demonstrating a contingency management system were shared at a project workshop meeting. Furthermore, publications of the developed concepts and findings are planned for the near future. Also, the results of the analysis of the regulatory framework will be shared and discussed with aviation regulators and other stakeholders. Within the scope of the voloCHRIS project, a significant contribution towards increasing acceptance for autonomous urban air mobility has been made and the project's results will be the foundation for future work and collaboration.