|  |
| --- |
| UNCLASSIFIED |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | REFERENCES | ISSUE | DATE |
| logoIRT-StExupery |  |  |  |  |
|  |  |  |  |  |
| logoAirbus |  |  |  |  |
|  |  |  |  |  |
| logoONERA |  |  |  |  |
|  |  |  |  |  |
| logoRR |  |  |  |  |
|  |  |  |  |  |
| DASAVIA |  |  |  |  |
| logoSAFRAN |  |  |  |  |
| logoThales |  |  |  |  |

|  |
| --- |
|  |
| Streamlining Development Assurance  µXAV Specification |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
|  |  | Page : 1 / 46 |

|  |
| --- |
| This document is the intellectual property of RESSAC members It may not be used, reproduced, modified or disclosed without its authorization.  RESSAC members Proprietary Data. |

signatures

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | REFERENCES | APPROVERS |
|  |  | Fonction 1 |
|  |  |  |
|  |  | Name 1 |
|  |  | Fonction 2 |
|  |  |  |
|  |  | Name 2 |
|  |  | Fonction 3 |
|  |  |  |
|  |  | Name 3 |
|  |  | Fonction 4 |
| logoRR |  |  |
|  |  | Name 4 |
|  |  | Fonction 5 |
| DASAVIA |  |  |
|  |  | Name 5 |

Table of contentS

1. Document issues 4

2. Introduction 5

2.1 µXAV: Air Vehicle 5

2.2 Purpose of the document 5

2.3 Method 5

3. INDEX 6

4. µXAV Flight description 7

4.1 Flight phases sequences 7

4.2 Activations 8

5. Foreesable Operating Conditions 9

5.1 Operational Modes 9

5.2 µXAV usage domain 9

5.2.1 Weather conditions: 9

5.2.2 Payload mass 10

5.2.3 Others ? 10

5.3 Foreseeable abnormal inputs and conditions 10

5.4 Assumptions 10

6. Mission Scenarios 12

6.1 Nominal flight in AUTO 12

7. ADDITIONAL REQUIREMENTS and constraints 14

7.1 Expected Operating Performances 14

8. µXAV External interfaces 15

8.1 Mechanical sensors and actuators 15

8.2 Control Panel 15

8.3 Ground Station communication 16

8.3.1 Message from Ground Station to AV 17

8.3.2 Message from AV to Ground Station 17

8.4 USB key data file 18

# Document issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Issue** | **Author(s)** | **Updating purpose** |
| 28/09/2016 | 1 | E. Ledinot/  F.Pothon | Creation of the document based on RESSAC\_CaseStudy\_muXAV\_Specification\_OP\_oriented document |

# Introduction

## µXAV: Air Vehicle

µXAV Air Vehicle is dedicated to 7/7-H24 autonomous or remotely controlled cargo transport. The payloads are of small size (< 10kg).

Flight must be ensured for a large domain of weather conditions, whose definition is simplistically restricted to some wind vector distribution.

Availability, reliability, robustness, energy efficiency are the key performance design drivers of its embedded systems.

## Purpose of the document

This document provides the specification of the drone µXAV at air vehicle level. This specification is mainly organized around 4 elements: Mission Scenario, additional requirements and constraints, foreseeable operating conditions and µXAV external interfaces description.

## Method

Based on knowledge and background of the RESSAC project patterns, the desired behaviour are identified and captured into Mission Scenarios. In parallel the foreseeable conditions in which the µXAV will operate are identified. These conditions define the normal and abnormal inputs and conditions. The development of these data is performed with an incremental approach, in the sense that the number of scenarios is intentionally limited in a first release. Then they are expanded to add new features. The Mission Scenarios address both several mission modes, and possible degraded modes in case of failure, or abnormal environment conditions. These scenarios are supplemented as necessary with additional requirements and constraints such as performances aspects. These additional requirements and constraints do not duplicate the scenarios but express characteristics, conditions that cannot be included in any scenarios.

In parallel of mission scenario development, the µXAV external interfaces are defined. Iterations between the different element of the µXAV specification (Mission Scenarios, additional requirements, external interfaces and foreseeable conditions) are performed to ensure the consistency of the complete specification.

This specification is used as input for each system development. The Mission Scenarios may be directly used as inter-system integration verification cases, while additional requirements will be the purpose of additional validation activities.

# INDEX

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| CP | Control panel |
| RP | Remote Piloting |
| GS | Ground Station |
| µXAV | Multi Function Air Vehicle ? |
| GWC | Good weather conditions |
| AWC | Adverse weather conditions |

# µXAV Flight description

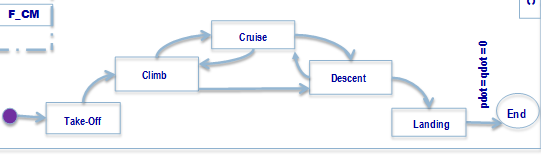
This chapter describes the sequence of phases of a complete flight plan. It will be used to develop the mission scenarios and to identify normal and abnormal foreseeable conditions.

Each flight plan characteristics are a departure time, a distance, a route, an expected arrival time, a maximum speed, and a flight level.

## Flight phases sequences

1. **Preparation of the µXAV**: loading of the payload, uploading the mission parameters, “refuelling” the primary and secondary electrical sources,
   1. **µXAV** **power-up:** Initialization and calibration are setup.
   2. **Payload loading** and the mass of the payload is provided.
   3. **Mission set-up**:
      1. Mode Selection
      2. Transport distance (km),
      3. Cruise speed (m/s),
      4. Flight level (m)
   4. **Minimal resources checks**: Minimum battery capacities …
   5. **Refuelling** ?
   6. **Environment conditions checks**
2. **Mission:** The mission is started.It triggers power-on and initialization of the systems until status ‘Mission Ready’ or ‘Mission Cancelled” is set,

The diagram below identifies possible transition between the mission states (take-off, climb, cruise, descent, landing)



* 1. **Take-off**: Initialization of the systems must have succeeded (READY lighted on).
  2. **Flight**: The µXAV is piloting to keep altitude and speed close to the preset values in spite of the atmospheric disturbances, using thrust or brake pulses, or modulated continuous actions. The cruise is a sequence of “Climb”, “Cruise” and “Descent”.

Once the target range is covered, normal landing is initiated.

* 1. **Landing**: performs simultaneous speed and altitude decrease while trying to maintain q and qdot as close to 0 as possible, until immobility is reached,

1. **Mission termination:** remaining capacities displayed on the control panel and sent to the ground station.
   1. **Payload unloading**
   2. End mission diagnosis and prognosis
   3. End of the mission cycle.
2. **Power-off.**

## Activations

**µXAV** **power-up and power-off:** Pushing the ON/OFF button on the CP.

**Payload loading and unloading** : Activation of the OPEN/CLOSED switch on the CP.

**Mass of the payload**: Three means are available to enter the mass

* Send the NAME Message from the GS
* Rolling the rotactors on the CP
* Information from the USB key plugged in the CP

**Uploading the mission parameters**: Two means are available to enter the mass

* Send the NAME message from the GS
* Information from the USB key plugged in the CP

**The mission is started.**  Two means are available to start the mission

* Send the GO the message from the GS
* Pushing the START button on the CP

# Foreesable Operating Conditions

## Operational Modes

µXAV can be operated in two modes:

* **Mode AUTO** (Autonomous) µXAV operates without any ground station (GS), using the control panel (CP).
* **Mode RP** (Remote Piloting) µXAV operates remotely by a ground station operator. In that mode a two-way communicates between µXAV and the ground station is operative.

The two modes are similar. RP is identical to AUTO when the GS operator sends no command to the µXAV. RP gives the opportunity to modify the mission parameters (altitude, speed, distance) at any moment. This is the only way of remotely ‘guiding’ the µXAV.

Any mix of the two modes is possible: first autonomous, then a ground station operator takes over and modifies the mission modes and parameters (anything else impossible). Other possible mode combination may be to preset and initiates the mission with the ground station, then lets it to complete in fully autonomous mode.

## µXAV usage domain

### Weather conditions:

Wind:

1. *Good Weather Conditions* (GWC) are defined by no icing and *tailwind* (no vertical component) of strength less than 15kt, distributed as uniform law [0,15],
2. *Adverse Weather Conditions* (AWC) are defined by no icing and *headwind* with some vertical component. AWC wind is characterized by:
   * Horizontal headwind:
     + speed fluctuates in [10kt, 25kt] distributed as GL(18,5),
     + direction with respect to heading fluctuates in [-π/4, +π/4] uniformly,
   * Vertical headwind: strength fluctuates in [-10kt, +20kt] as GL(10,5),

Temperature

Altitude

Storm/Rain/Humidity ?

EMI

### Payload mass

### Others ?

## Foreseeable abnormal inputs and conditions

These conditions identify possible *external* and *internal* disturbances that may occur during a mission. They also include any operator error, in the ground station or side of the drone.

* Operating outside the usage domain defined in section [µXAV usage domain](#_µXAV_usage_domain):
* Inconsistency of the mass of the payload when entered by the two or three means.
* A misleading payload mass value may occur even in case of threefold coherency. There is no payload weight sensor aboard the AV. The actual mass has to be estimated by the mission management software,
* In RP mode, arbitrary interleaving of ground station parameter updates and onboard system decisions may occur,
* Breakdowns may occur at any time on electrical, hydraulical, and digital hardware items. Loss of digital communications (internal and/or external) are however possible in case of emitter or receiver failure.
* Cascading effects (e.g electrical -> hydraulical -> mechanical) or thermal effects may lead to many combination of item failures. It may also lead to latent failures before take-off.
* Remote piloting is impossible because of excessive communication latency (+ lack of sensors).

The AV’s behaviour is insensitive to option changes during take-off and landing (too short phases).

1. If still not possible (altitude + distance + weather conditions are incompatible with onboard energy) activate soft landing.

No take-off if onboard energy is incompatible with the mission, under SWC (Standard Wind Condition ) assumption,

1. As soon as rejection of external disturbances (safety envelope) or mission completion is no longer possible, soft landing should be triggered,
2. As soon as rejection of external disturbances (safety envelope) or mission completion is no longer possible and propulsion is no longer available, hard landing (F\_EL) should be triggered,

## Assumptions

This section identifies possible *external* and *internal* disturbances or events that may occur during a mission but not addressed in the scope of this specification. It also includes some assumptions on the behaviour or performances of some system components.

* There is no Cyber-attacks
* There is no failure of the AV’s mechanical body and of the data bus’ cable.
* Communication protocol and the data-link technology ensure no message loss and at most 100ms latency.
* The data-link is not a lossy channel,
* Communication latencies are bounded (2s),
* Transfer preserves integrity of contents (error correcting codes – no security aspects)
* The hardwired links with the mechanical sensors can’t fail

1. Icing can occur only in climb and descent phases (no icing at µXAV’s cruise altitudes),

Because of:

1. systematic contract-based specification (the DIFs),
2. systematic contract-based implementation (system modelling, software and hardware development),
3. an assumption on sufficient effectiveness of development assurance,
4. assumptions A and B,

F\_PT.F\_MM has no mitigation mechanism to tolerate faults that would lead to a wrong perception of µXAV’ state. F\_PT.F\_MM does not try, using estimation algorithms, to reconstruct energy or availability information on its own in order to cross check the data it receives.

In the use case, there is no functional redundancy motivated by possible weakness of development assurance.

If functional redundancy had to be introduced (none in the first version), it would be on request of the safety group, for architectural reasons.

1. *Sensors are ideal*. In later versions the sensors will include fault models (bias, noise, lag) to deal with robustness analysis at AV and system level,
2. *Actuators are ideal*. Similarly in later versions the actuators will be biased and lagging,
3. Some item level components have no failure modes (mechanical parts, wiring, pipes, see Architecting),

# Mission Scenarios

## Nominal flight in AUTO

1. **Preparation of the µXAV**
   1. **µXAV** **power-up:** No error detected

*Initialisation completed in less than 1 minute. Observable property?*

* 1. **Payload loading**. Declared payload mass: 5kg with CP
  2. **Mission set-up**: with USB key
     1. Mode AUTO
     2. Energy efficiency mode ????
     3. Distance: 60 n.m,
     4. Flight level: 1000ft
     5. Speed: 50 kt
  3. **Minimal resources checks**: No error
  4. **Refuelling**: No
  5. **Environment conditions checks:** No error

*READY lights turns on*

1. **Mission:** 
   1. **Take-off**:
   2. **Flight**: Climb, Cruise, Descent
   3. **Landing**
2. **Mission termination:**
   1. **Payload unloading**
   2. End mission diagnosis and prognosis: No error, no need for refuelling *(Observable property?)*
   3. End of the mission cycle.
3. **Power-off.**

Other scenarios to be worked with

* Different values of mission parameters and mass
* Combination of mode AUTO/RP
* Combination of climb/Cruise/Descent
* Mix of mode AUTO/RP
* With/without refuelling
* With change of weather conditions during the flight
* Including possible errors in each phase (Coverage of abnormal inputs/conditions). Definition of expected behaviour for each abnormal conditions and combination

At each phase, to define observable properties, to identify possible abnormal conditions, and to provide performances

To help the definition, a scenario template could be defined.

# ADDITIONAL REQUIREMENTS and constraints

## Expected Operating Performances

The drone flight conditions should meet the ATC (Air Traffic Control) regulatory requirements (flight levels, climb rate etc.)

Mission setup duration should be less than 15 mn when energy “refuelling” is needed, and less than 1 mn otherwise.

Range at Maximum Take-Off Weight (MTOW) should be greater than 100 n.m in good weather conditions, and greater than 50 n.m in bad ones (but still within µXAV’s foreseeable operation conditions – see 6.2.3)).

Maximal cruise speed in favourable wind conditions should be at least 75kt for payload mass lower than 10kg.

When weather conditions are worse than that of operation conditions, a mission abortion logic followed by emergency landing should prevent the loss of the drone and ground damage or casualties. The target failure rates are 10-4 and 10-3 per mission, respectively for catastrophic and hazardous.

Downtime (energy refuelling and maintenance) of the drone should be less than 3 hours per 10.000 flight hours.

# µXAV External interfaces

At AV level there are three groups of exchange with the external environment:

* Mechanical sensors and actuators
* The exchanges through the man machine interface (Control Panel), located on the downside of the drone near the payload bay
* The exchanges with the Ground Station,

## Mechanical sensors and actuators

* Sensors: pitch (p), pitch rate (pdot), roll (q). The roll rate is not measured.
* Actuators: in this first version (no flight mechanics), action of thrust and air brakes are transposed into to two torques

## Control Panel

The payload bay of µXAV is equipped with a Control Panel (CP) featuring (see figure in Architecting section):

* A USB plug for mission parameter upload (in case of no data-link or A mode),
* An ON/OFF general power-on button (two stable positions, lighted when ON),
* An OPEN/CLOSE switch (two stable positions) associated with a two-Rotactor mechanical ‘keyboard’. The button is set by the operator in charge of the payload. He has to enter the mass of the payload by means of the two mechanical cranked Rotactors (0-9, kg),
* An A/RP switch that configures the drone either for Autonomous flight, or for RP mode where communications with the Ground Station (GS) are active.
* A START push button (one unstable position) that launches the mission in A mode.
* A row of four mission indicators (lighted when the label is true), whose status is transmitted to the ground station:
  + READY: the various systems initialized successfully, the mission can be started,
  + COMPLETE: end of the mission in normal situation (landing at the right place in satisfactory conditions),
  + ABORTED: the mission was stopped before landing at the waypoint where the payload had to be delivered. The indicator is lighted after soft and hard landing. Soft landing occurs when enough energy and resources are available and control succeeds (anticipated and mastered situation), hard landing occurs when there is shortage of energy or too many failures. Control operates in a
  + CANCELED: no take-off because of any failure or energy problem
* Two displays: primary source capacity (%), secondary source capacity (%)
* An array of 20 red LEDs signaling the failure modes diagnosed by the maintenance system



*Figure 2: The Control Panel Front-end*

In RP mode the START button of the control panel is inactive.

## Ground Station communication

* µXAV to Ground Station:
  + the state vector, i.e speed, altitude, position, and the 0/1 status of all failure modes handled by the Health Monitoring functions.
  + after mission completion, a message with the remaining electrical capacities of the two sources.
* Ground Station to µXAV:
  + The mode (RP, A) and navigation options (energy efficiency, time efficiency, auto),
  + The navigation parameters: distance, cruise altitude and speed,
  + Possible updates of the mode, parameters or option during the course of the mission.

The perimeter of the project excludes the ground station but includes its communications with the drone.

### Message from Ground Station to AV

The flow is event driven, contrary to the downstream one which has only periodic messages (1 Hz).

|  |  |
| --- | --- |
| **Message Name** | **Content** |
| GS\_MissionSetUp | Structure Type:  [Distance:float;  Speed:float;  Altitude:float] |
| GS\_NavigationMode | Enum Type:  {‘RP’,’A’} |
| GS\_NavigationOption | Enum Type:  {‘SPEED’,’ENERGY’} |
| GS\_GO | None |
| GS\_EmergencyLanding | None |

Message GS\_GO starts the mission from the Ground Station in RP mode.

Message GS\_EmergencyLanding is effective only in RP mode

### Message from AV to Ground Station

A first set of messages downloads the states of the Control Panel, for ground-based mission supervision.

A second set of messages is provisioned to broadcast the sensor values used by the MMS computer, in case of needed in-flight or post-flight technical investigations.

|  |  |
| --- | --- |
| **Message Name** | **Content** |
| AV\_CP\_Switches | Structure Type:  [Power: Boolean;  Mode: {‘RP’,’A’};  Bay:{‘OPEN’,’CLOSED’};  START:Boolean;  Rotactor1:Integer;  Rotactor2:Integer;}  ] |
| AV\_CP\_Displays | Structure Type:  [READY:Boolean;  CANCELLED:Boolean;  COMPLETE:Boolean;  ABORTED:Boolean;  FC\_CAPACITY:Integer;  BAT\_CAPACITY:Integer  ] |
| AV\_CP\_LEDs | Bitfield 3 bytes for 2x10 logical bits  Padding TBDL |
| AV\_Sensors\_Mechanical | Provision |
| AV\_Sensors\_Electrical | Provision |
| AV\_Sensors\_Hydraulical | Provision |
| AV\_MissionCompleted | Structure Type:  [PRIMARY\_SOURCE:Integer;  SECONDARY\_SOURCE:Integer;  ] |

## USB key data file

<to define the file format and parameters .. > to be read