|  |
| --- |
| UNCLASSIFIED |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | REFERENCES | ISSUE | DATE |
| logoIRT-StExupery |  |  |  |  |
|  |  |  |  |  |
| logoAirbus |  |  |  |  |
|  |  |  |  |  |
| logoONERA |  |  |  |  |
|  |  |  |  |  |
| See original image |  |  |  |  |
|  |  |  |  |  |
| DASAVIA |  |  |  |  |
| logoSAFRAN |  |  |  |  |
| logoThales |  |  |  |  |

|  |
| --- |
|  |
| µXAV Operational Specification and Scenarios |

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

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
|  |  | 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 |
|  |  |  |
|  |  | Name 4 |
|  |  | Fonction 5 |
|  |  |  |
|  |  | Name 5 |

Table of contentS

1. Document issues 5

2. REFERENCES 6

3. PURPOSE AND SCOPE OF THE DOCUMENT 7

4. OPERATIONAL CONTEXT 7

5. mAN MACHINE interaction 7

5.1 Control Panel 8

5.2 Ground Station Control 9

6. Operating Procedures 11

7. Expected Performances 12

8. Foreseeable Operating Conditions 13

8.1 Environmental Conditions 13

8.2 Human Errors 13

8.3 Failures 13

8.4 Threats 14

9. mission scenarios 15

9.1 Scenario Pattern 15

9.2 Scenario Coverage 15

9.2.1 Continuous Coverage 15

9.2.2 Discrete Coverage 15

9.2.3 Hybrid Coverage 16

9.3 Scenario 1: Nominal 16

9.3.1 Ground Station 16

9.3.2 Field Operator 16

9.3.3 Environmental Conditions 16

9.3.4 Failure Modes 16

9.3.5 Variants 17

9.4 Scenario 2: Bad Weather Conditions No Failures 17

9.4.1 Ground Station 17

9.4.2 Field Operator 17

9.4.3 Environmental Conditions 17

9.4.4 Failure Modes 17

9.4.5 Variants 17

9.5 Scenario 3: Good Weather Conditions Non Critical Failures 17

9.5.1 Ground Station 17

9.5.2 Field Operator 17

9.5.3 Environmental Conditions 17

9.5.4 Failure Modes 17

9.5.5 Variants 18

9.6 Scenario 4: Bad Weather Conditions Critical Failures 18

9.6.1 Ground Station 18

9.6.2 Field Operator 18

9.6.3 Environmental Conditions 18

9.6.4 Failure Modes 18

9.6.5 Variants 18

10. dependence on increments 19

# Document issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Issue** | **Author(s)** | **Updating purpose** |
| 2017/03/28 |  | E. Ledinot | First version.  Imports from document “Streamlining Development Assurance - µXAV Specification  (Overarching Properties Oriented)”,  with additional scenarios. |
| 2017/05/06 |  | E. Ledinot | Updates in consistency with “µXAV Requirements Allocated to MMS Software (Increment 1)” |

# REFERENCES

[1] “µXAV Systems Process Definition”,

[2] “µXAV Case Study – Development Increments,

[3] “µXAV Layer 0 Functional Specification”,

[4] “µXAV System Requirements Allocated to MMS Software - Increment 1”,

[5] “MMS Functional Scenarios”,

[6] “µXAV regulatory functional safety specifications”.

# PURPOSE AND SCOPE OF THE DOCUMENT

The purpose of this document is to define a set of mission scenarios at air vehicle level (layer 0).

These scenarios are intended:

* to contribute to specification of layer 0 and layer 1 functions,
* to be used for multi-system level verification and validation [1].

This document is common to all increments [2].

Dependence on increment is specified in section 13.

# OPERATIONAL CONTEXT

µXAV is intended to perform 7/7-H24 autonomous or remotely controlled cargo transport missions.

Remote control is ensured by means of a ground station operating a fleet of µXAVs.

The payloads are small size parcels (< 10kg).

Mission range is limited to a few kilometres. Range depends on payload mass, weather conditions and embedded energy capacity.

Flight levels, i.e altitudes, are constrained by regulatory air traffic control considerations.

Flight must be ensured for a large domain of weather conditions, whose definition is simplistically limited to specifying the distribution of some random wind vector. Three classes of wind conditions are defined as “foreseeable operating conditions” in section 6 and used for specification in [3] and [4].

Icing is simplistically addressed as mass perturbation, transient or persistent mass increases/decreases impacting range and flight dynamics.

There are two ways of operating the drone:

* *Without data link*: “**A**utonomous” mode (abbreviated ‘**A**’). The mission parameters are set-up once for all when the payload is attached to the drone by the field operator,
* *With data link*: “**R**emotely **P**iloted” mode (abbreviated ‘**RP**’). The field operator may enter no mission parameters, or enter some that may be updated later by the ground station operator.

A mission is prepared (system boot, payload fixation, and navigation set-up), then launched and performed. It consists in a sequence of phases, possibly disturbed by external conditions (wind and icing) or by internal events (failure modes and energy shortage).

# mAN MACHINE interaction

Two devices:

1. Control Panel (CP), fixed to center of the drone’s upper side (opposite to the payload bay).
2. Ground Station (GS). GS is out of the scope the use case, but the data-link is part of the system to be developed and justified in the use case.

## Control Panel



*Figure 1: Front-end of the Control Panel*

The **initial state** of the drone, common to all scenarios is:

* Drone fielded, payload and field operator by the drone,
* Power-off, the three systems are down,
* Possibly the field operator holds an USB stick storing the mission’s range, altitude and speed parameters,
* On-board energy capacity (from none to maximum).

**CP-based Mission Preparation**

1. ON/OFF button is pushed to power on the systems. If electrical energy is available the systems start booting,
2. The ‘A’/’RP’ switch is positioned. If ‘RP’ mode is selected, the data link becomes active, GS can transmit the navigation parameters,
3. The OPEN/CLOSED switch is positioned to OPEN, the payload bay is opened, the payload is attached to the bay. Then the bay is closed, and the switch is pushed back to CLOSED position,
4. Payload’s mass is dialled on the two rotators,
5. The USB key, if any, is plugged-in,
6. 15s awaiting period for parameter transfer,
7. The USB key, if any, is unplugged
8. The START button is pushed,
9. Time-varying awaiting period until either READY or CANCELLED lights on,
10. In case CANCELLED lights on, end of the mission: payload withdrawal and power switch-off,
11. In case READY is on, the operator must step back a few meters from the drone (safety procedure), which takes-off after a 30s timeout.

After landing, **CP-based Mission Debriefs**:

1. If COMPLETE is lighted-on, the range was met. The primary and secondary displays give the electrical capacities left after mission completion,
2. If ABORTED is lighted-on, the range was not met. Check the payload and µXAV’s integrity, hard landing may have occurred.
3. The 20 LEDs may signal failure modes that were diagnosed in the various systems and necessitate maintenance actions.

## Ground Station Control

Scenarios may entail ground-based interactions. Since GS’ MMI is not in the use case’s perimeter, these interactions are described as message emissions and receptions.

**From GS to AV**

|  |  |
| --- | --- |
| **Message Name** | **Content** |
| GS\_MissionSetUp | [Distance;  Speed;  Altitude] |
| GS\_NavigationMode | {‘RP’,’A’} |
| GS\_NavigationOption | {‘SPEED’,’ALTITUDE’, ’ENERGY’} |
| GS\_GO | n.a |
| GS\_EmergencyLanding | n.a |

Reception of message GS\_GO starts the mission in RP mode. It is equivalent in ‘A’ mode to a START press. In RP mode the START button is inactive.

Message GS\_EmergencyLanding is effective only in RP mode. It triggers an emergency landing, even in absence of safety escapes, energy shortage or excessive failures.

**From AV to GS**

These messages enable the ground operator to monitor mission progress and conditions.

In RP mode they periodically provide the AV’s integrity state. The dynamical state vector (p, pdot, q, qdot) is not transferred. Ground control can only be ensured at navigation and mission management level, communication latencies prevent remote piloting.

|  |  |
| --- | --- |
| **Message Name** | **Content** |
| AV\_CP\_Switches | [Power:true/false;  Mode: {‘RP’,’A’};  Bay:{‘OPEN’,’CLOSED’};  START:true/false;  Rotactor1:Integer;  Rotactor2:Integer;] |
| AV\_CP\_Displays | [READY:true/false;  CANCELLED:true/false;  COMPLETE:true/false;  ABORTED:true/false;  PrimarySourceCapacity:Integer;  SecondarySourceCapacity:Integer] |
| AV\_CP\_LEDs | 2x10 logical bits |

# Operating Procedures

µXAV can be operated in A mode (fully autonomous) without the ground station, using only the control panel.

It can also be operated jointly by a field operator and a ground station operator.

Any mix of the two modes is possible:

* First part of the mission in autonomous flight, then the ground station operator takes over by switching to RP mode and modifies the mission conditions up to landing,
* The field operator takes in charge the payload only, while the GS operator prepares the mission and then starts it. The GS operator can then switch to A mode to let the drone complete its mission autonomously.

A mission scenario consists in:

1. Preparation of the AV:
   1. Loading of the payload,
   2. Uploading the mission parameters by data-link or by mean of a USB stick plugged in the control panel,
   3. Loading of the primary and secondary electrical sources,
   4. Power-on and initialization of the systems until status ‘READY’ or ‘CANCELLED” is got.
2. Start of the mission by means of the data-link, or by START button push on the control panel,
3. Take-off, cruise and landing phases, with possible additional phases in case of mission parameter updates (RP mode only),
4. Mission termination: the remaining electrical capacities are displayed on the control panel and sent to the ground station. Payload release, power-off or start of a new mission.

RP and A modes are identical regarding flight control and performance management.

RP is identical to A when the GS operator sends no command to the AV.

RP mode gives the opportunity to modify the mission parameters (altitude, speed, distance) at any moment. This is the only way of remotely ‘guiding’ the AV.

**Emergency Landing**

It can be triggered:

* Internally (system initiative):
  + In case of lasting dynamical safety escapes,
  + In case of energy shortage.
* Externally (GS initiative):
  + At the operator’s discretion.

# Expected Performances

**Safety**

The hazards and accidents considered in the use case (see the documents of the safety process) are those related to flight control and crashes of the drone.

For every flight phase a flight envelope (also named safety domain or safety constraints) is defined in [4].

The scenarios must check that the safety constraints are met in *any* foreseeable operating conditions (deterministic part of failure condition avoidance).

The probabilistic part of failure condition avoidance is out of the scope of the use case.

**Availability**

Outage of the H24 7/7 drone must not exceed 1hour per 10.000 flight hours.

Using Monte Carlo mission and component reliability simulation this performance may be checked by means of the layer 0 model.

**Mission Performance**

Mission performance has to be checked on every scenario, in ideal and standard environmental conditions.

The performance objectives are met when the range is met while staying at the prescribed speed or altitude (for precision tolerances see [4]).

# Foreseeable Operating Conditions

## Environmental Conditions

Layer 0 scenarios must exercise the whole spectrum of foreseeable operating conditions. They are defined by the external conditions (user interactions and environmental conditions) and the internal conditions (failure modes).

This section defines the spectrum of environmental conditions, i.e. wind and icing conditions.

**Wind conditions**

*Standard Weather Conditions* (SWC) is defined by regulation [6].

*Good Weather Conditions* (GWC) is defined by the AV’s supplier as no icing and tailwind. Tailwind has no vertical component, its maximum strength is lower than 15kt, its intensity is distributed as a uniform law over [0, 15],

*Adverse Weather Conditions* (AWC) is defined by the AV’s supplier as no icing and headwind. Headwind may have some vertical component. AWC wind is characterized by:

* + Horizontal component:
    - * intensity fluctuates in [10kt, 25kt] distributed as the normal law GL(18,5),
      * direction fluctuates in [-π/4, +π/4] uniformly,
  + Vertical component: intensity fluctuates in [-10kt, +20kt] as GL(10,5),

**Icing conditions**

They are modelled as AV’s mass in-flight increase.

They are most likely to occur at take-off and landing.

The mass increase rate is dependent on speed (the higher the speed the higher the rate).

Mass increase is unbounded and may last until the AV stalls.

## Human Errors

The field operator may dial a wrong payload mass on the two CP rotators. µXAV’s flight control laws are designed to adapt and mitigate such errors provided they are limited to some extent.

The mission parameters may be incompatible with on-board energy. Mission management addresses this issue and prevents take-off when mission completion is not ensured.

Multiple and inconsistent versions of the mission parameters may be defined (GS and USB key). µXAV’s software manages these situations and selects the appropriate values.

µXAV is intended to be error proof. The scenarios have to exercise these error passivation capabilities.

## Failures

Breakdowns may occur at any time on electrical, hydraulic, and digital items. It is assumed that there is no failure of the AV’s mechanical body, nor of the data bus’ cable.

Loss of digital communications (internal and/or external) are however possible in case of emitter or receiver failure.

Cascading effects (e.g electrical -> hydraulic -> mechanical) or thermal effects may lead to many combination of item failures. It may also lead to latent failures before take-off.

The scenarios have to exercise the combinatorial aspects of failure modes.

## Threats

Spoofing of the data-link or hacking of the systems by means of the control panel may be considered.

But the use case is at present exclusively safety oriented, security is out of scope.

# mission scenarios

## Scenario Pattern

A scenario results of the *superposition of four concurrent timelines*:

1. **GS**: the time-triggered and event-triggered messages exchanged with the drone,
2. **Field operator**: his interactions with CP at mission’s beginning and end,
3. **Environment**: the wind and icing profiles over the mission’s duration,
4. **Drone**: the physical failures that may randomly occur during the mission (failure modes),

Each scenario is specified by defining these four parallel threads and their possible synchronizations (e.g worst case concomitance of failure modes and wind gusts).

## Scenario Coverage

Testing coverage at layer 0 and layer 1 is an issue of development assurance.

What coverage beyond requirement coverage?

Contrary to software and hardware, system level requirement coverage can’t be supplemented with structural coverage.

This section is intended to help consider *behavioural coverage* based on *input conditions* and combinatorial analysis thereof. The set of scenarios is expected to cover with reasonable confidence the combinatorial space of the input conditions that exercise µXAV’s systems.

### Continuous Coverage

It concerns the continuous physical variables: altitude, attitudes, speed, energy levels, wind and icing profiles.

As there are infinitely many possible joint profiles of these variables, an approach to discretization and coverage may be:

* Reduction of the infinitely many weather conditions to a few regulatory ones (SWC, AWC etc.)
* Reduction of the infinitely many initial energy levels to three cases: best case (maximum capacity), average case (medium capacity), worst case (low or empty capacity).
* Attitudes are not directly controllable at input level. They result from navigation parameters, flight control laws and environmental conditions. They are not concerned by the input coverage analysis.
* Altitude and speed: a grid approach may be applied to the two input parameters (that may be submitted many times to the systems in RP mode).

### Discrete Coverage

It applies to the events, to their relative ordering and to their mapping to physical time.

The events to be considered are:

* Interactions on CP,
* Reception of commands from GS,
* Failures,
* “Zero-crossings” (thresholdings) of continuous dynamics (e.g. the instant at which range is met, the instant at which reference altitude is caught, etc.).

An approach to reduction to finitely many scenarios may be *conservative worst case analysis* regarding:

* The safety objectives,
* The performance objectives,
* Robustness.

Event ordering and time mapping to be selected for the finitely many scenarios ensuring “best coverage”, are those assumed to be the least favourable to mission success.

### Hybrid Coverage

µXAV is an hybrid multi-system. Its dynamics intertwines continuous time dynamics and events (internal and external ones).

Global input conditions coverage analysis has to merge the two preceding coverage analyses.

Worst case oriented merge of the two sets of scenarios may be an approach to come up with a limited number of scenarios closer to max(M,N) than to M\*N, where M and N the numbers of scenarios resulting from the two coverage analyses.

In the sequel we define 4 scenarios in conformance with the pattern approach. No coverage analysis of these 4 scenarios is performed. Definition of supplementary scenarios and analysis of their requirement coverage and input coverage is left to the layer 0 verification and validation activities [1].

## Scenario 1: Nominal

### Ground Station

No role in this scenario, A mode is active from beginning to end of the mission.

### Field Operator

He operates the drone using a USB key to load the navigation options and parameters:

* + Dialled payload mass: 5kg,
  + Distance: 60 n.m,
  + Flight level: 1000ft
  + Speed option: 50 kt

### Environmental Conditions

Ideal or standard, i.e as defined by the regulatory SWC [4], [6].

### Failure Modes

None.

### Variants

Addition of a take-over by the ground station, and modification of the cruise parameters: speed increased by 10kt.

## Scenario 2: Bad Weather Conditions No Failures

### Ground Station

It submits all the mission parameters to the drone.

### Field Operator

He is only in charge of attaching the payload and dialling its mass on the two rotators.

### Environmental Conditions

Wind gusts appear after take-off, conformant to AWC as defined in [4].

The AV makes transient forays in the hazardous flight domain,

### Failure Modes

No component failure, but energy shortage episode.

The energy initial capacity was compatible with mission completion under SWC assumption. As weather conditions evolve into AWC during flight, mission viability may no longer be ensured leading to mission cancellation.

### Variants

Addition of icing conditions to accelerate mission viability loss and occurrence of the consequent emergency landing.

## Scenario 3: Good Weather Conditions Non Critical Failures

### Ground Station

Identical to scenario 1.

### Field Operator

Identical to scenario 1.

### Environmental Conditions

Identical to scenario 1.

### Failure Modes

* 1. Loss of one electrical motor,
  2. Loss of one hydraulic pump,
  3. Loss of one MMS channel
  4. Loss of data bus communications.

### Variants

Addition of some failures no longer tolerated by fail-safe recovery mechanisms, leading to emergency landing.

## Scenario 4: Bad Weather Conditions Critical Failures

### Ground Station

Identical to scenario 2.

### Field Operator

Identical to scenario 2

### Environmental Conditions

Identical to scenario 2.

### Failure Modes

Identical to scenario 3.

### Variants

Mission abortion is decided in RP mode, in conditions compatible with fully controlled landing (soft landing) [4].

Mission abortion is decided in A mode, in conditions where there is no longer propulsion (hard landing).

# dependence on increments

**Increments 1 and 2**

The failure mode events cannot be played.

Timing aspects do not take into account GS-AV transfer latencies.

**Increment 3**

The component failure modes are introduced along with FDIR and signalling logics. They can be activated in the scenarios.

**Increment 4**

All internal and external timing aspects are taken into account.

See [2] for more details.