|  |
| --- |
| UNCLASSIFIED |

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

|  |
| --- |
|  |
| µXAV Operational Specification |

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

|  |
| --- |
|  |

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

|  |
| --- |
|  |

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 4

2. REFERENCES 5

3. PURPOSE AND SCOPE OF THE DOCUMENT 6

4. OPERATIONAL CONTEXT 6

5. mAN MACHINE interaction 7

5.1 Control Panel 8

5.2 Ground Station 9

6. Operating Procedures 11

7. SPECIFIED Performances 12

8. Foreseeable Operating Conditions 13

8.1 Environmental Conditions 13

8.2 Human Errors 14

8.3 Failures 14

8.4 Threats 15

9. mission scenarios 16

9.1 Scenario Pattern 16

9.2 Scenario Coverage 16

9.2.1 Continuous Coverage 16

9.2.2 Discrete Coverage 17

9.2.3 Hybrid Coverage 17

9.3 Scenario Specifications 18

9.3.1 Pre-flight 18

9.3.2 Flight 19

9.3.3 Post-flight 21

10. dependence on increments 22

11. Appendix A – Failure Modes 23

11.1 Mission Management System 23

11.2 Electrical Propulsion System 23

11.3 Hydraulic Braking System 24

# Document issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Issue** | **Author(s)** | **Updating purpose** |
| 2017/03/28 | 1 | E. Ledinot | First version.  Imports from document “Streamlining Development Assurance - µXAV Specification  (Overarching Properties Oriented)”,  with additional scenarios. |
| 2017/05/06 | 2 | E. Ledinot | Updates in consistency with “µXAV Requirements Allocated to MMS Software (Increment 1)” |
| 2018/03/25 | 3 | E. Ledinot | Specification enrichment derived from Simulink modeling and from conformance to the ‘Multi-system Use Case’ (see the ‘Process Definition’ folder).  Compliance of the operational specification with the definition of the input simulation scenarios (MATLAB file InputScenarios.m).  Introduction of the safety regions on the environmental conditions and on the drone’s dynamics as specification material for the safety contracts.  Clarification of mode management (autonomous vs remote control). |

# REFERENCES

[1] Process Definition / Multi-system Use Case,

[2] “µXAV Case Study – Development Increments”,

[3] “µXAV Layer 0 Functional Specification”,

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

[5] “µXAV Certification Specification”.

# 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 the 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 increments is specified in section 10.

# 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 (< 10lb).

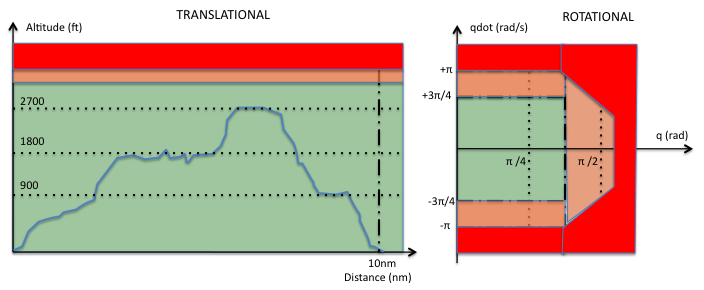
Mission range is limited to a few nautical miles. It depends on payload mass, weather conditions and embedded energy capacity.

Flight levels, i.e altitudes, are constrained by regulation (air traffic control).

Mission kinematics is 2D: altitude and distance.

Speed of the drone’s centre of gravity is measured or estimated wt. the ground.

The 2D kinematics includes some sort of attitude dynamics akin to pitch and pitch rate (the q and qdot state variables of the air vehicle’s mechanical body).



*Figure 1: Mission parameters and their safety regions supporting safety contracts*

Flight must be ensured for a large domain of weather conditions, whose definition is simplistically limited to specifying the probability law of a wind 2D vector (horizontal and vertical components).

Three classes of wind conditions are defined as part of the “foreseeable operating conditions” in section 8. They are used for specification in [3] and [4].

Icing is simplistically addressed as mass perturbation of the AV’s mechanical body: transient or persistent mass increase possibly followed by decrease that impact the range and the flight dynamics (see section 8).

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 by the field operator with a USB key when the payload is installed into the drone’s bay. In case of emergency, the ground station cannot connect to the drone and take over.
* *With data link*: “**R**emotely **P**iloted” mode (abbreviated ‘**RP**’). The field operator may enter no mission parameter at all, or enter some that may be updated later by the ground station operator. During the course of the mission the ground operator may remotely set the drone in Autonomous mode for completion of its mission. As the switch on the control panel stays in ‘RP’ position while the drone returned in ‘A’ mode, the drone keeps listening to messages from the ground station, which has the opportunity to take control back by sending a new ‘RP’ command.

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

# mAN MACHINE interaction

There are two MMI devices:

1. Control Panel (CP): located at the 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 (uplink and downlink message flows) on drone side.

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

* Drone fielded, empty, payload and field operator by the drone,
* On-board electrical energy capacity from low to maximum (scenario-dependent parameter),
* Power-off, the three systems are down,
* Possibly the field operator holds an USB stick storing the mission’s range, altitude and speed parameters,

## Control Panel



*Figure 2: Front-end of the Control Panel*

**CP-based Mission Preparation (Pre-flight phase)**

This sequence is common to the 4 scenarios detailed in section 9, up to some possible permutations of some commands:

1. The ON/OFF button is pushed to power the systems. If electrical energy is available the systems start booting,
2. The ‘A’/’RP’ switch is positioned. If the ‘RP’ mode is selected the data link becomes active on drone side, GS can transmit the navigation parameters and launch the mission,
3. The OPEN/CLOSED switch is positioned to OPEN, the payload bay is opened and the payload is attached to the bay. Then the bay is closed, and the switch is pushed back to CLOSED position,
4. The payload’s mass is dialled on the two rotators,
5. The USB key, if any, is plugged-in,
6. A 5s-waiting time is needed for parameter transfer,
7. The USB key, if any, is unplugged,
8. After parameter transfer from USB-key (or GS) a few seconds are needed until either READY or CANCELLED lights on, depending on mission feasibility conditions (viability analysis – see [4]),
9. If READY is on, the START button may be pushed and the drone takes-off 3s after the button push. The operator must quickly step a few meters back from the drone (safety procedure), especially in bad weather conditions. Flight control limits the drone’s vertical speed at take-off to prevent injuries.
10. In case CANCELLED is on, it is the end of the planned mission: payload withdrawal and power switch-off. Or power is left on, the payload is changed and/or the navigation parameters are modified, and a new mission is attempted,

Some permutation is possible after power-on and mode selection: upload of the navigation parameters and payload installation, including mass dialling, can be permuted and even interleaved without any impact on future behaviour (invariance to permutation of this command group and to permutation with any message from the ground station).

In RP mode the drone waits for the GS messages until 10s have elapsed. The mission is CANCELLED if the messages are not received before this deadline. Message transfer is equivalent to steps #5, 6, 7 of the previous sequence. The other field operator commands (#1 to #4 and #8 to #10) are identical in RP mode.

Post-flight:

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

## Ground Station

Scenarios may include ground-based interactions. Since GS’ MMI is not in the use case’s perimeter, these interactions are described as message emissions and receptions at drone’s RF[[1]](#footnote-1) transceiver level.

**From GS to AV**

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

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, of energy shortage or of any excessive number of component failures in the systems.

**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 interactions with the ground station, i.e. using only the control panel during the pre-flight phase. A field operator and a ground station operator can also operate the drone jointly. The field operator is always needed, at a minimum to install the payload and to configure the control panel so that the drone takes into account the GS’ messages.

A mission scenario consists in:

1. Preparation of the AV:
   1. Installation of the payload,
   2. Mission parameters upload, by means of the data-link or by means of the USB stick plugged in the control panel,
   3. Loading of the primary and secondary electrical sources, if needed,
   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 in ‘RP’ mode, or by push of the START button in ‘A’ mode,
3. Take-off, climb, cruise, descent and landing phases. In ‘RP’ mode, when the navigation parameters are updated by the ground station operator, altitude or speed updates may occur, possibly adding climb or descent phases that are interleaved within the cruise phase. A cruise phase is a stationary phase where the drone’s speed and altitude remain constant up to wind perturbations,
4. Mission termination: the remaining electrical capacities are displayed on the control panel and sent to the ground station. The field operator unloads the shipment and either he switches the systems off, or he refuels the batteries and starts of a new mission.

‘RP’ and ‘A’ modes are identical regarding flight control and mission performances (behavioural invariance to mode switching – stationary states and transients).

‘RP’ mode is identical to ‘A’ mode when the GS operator sends no navigation parameter updates and no emergency landing command to the AV.

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

**Emergency Landing**

It can be triggered:

* Internally (system initiative):
  + In case of lasting safety escapes,
  + In case of energy shortage,
  + In case of non-tolerated configuration of component failures,
* Externally (GS initiative):
  + At the operator’s discretion.

# SPECIFIED Performances

**Safety**

The hazards and accidents considered in the use case are those related to drone crashes (see the documents of the safety process, in particular the Functional Hazard Analyses).

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

The scenarios must explore how far the safety constraints are met in *any[[2]](#footnote-2)* foreseeable operating condition. The scenarios sample and reduce to a finite number of cases the infinitely many possible wind conditions, icing conditions, interleaving of operator commands and failure events.

Part of these disturbed external and internal conditions is tolerated (robustness and fault tolerance mechanisms), and part is not. System design and assurance are in charge of deciding which part is tolerated (amber parts of the safety zones), and which part is not (red parts of the safety zones).

The tolerated/non-tolerated frontiers must comply with the regulatory objectives [5]. See the wind and icing conditions below.

Quantifying the frequency of failure events, i.e. of entries into some failure condition is out of the scope of the use case (safety assessment process / probabilistic analysis). The use case is limited to *qualitative safety* assurance, in other words it is limited to *functional safety* assurance.

**Availability**

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

Using Monte Carlo mission simulation with 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 regulatory environmental conditions.

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Parameter | Payload Mass (lb) | Range (nm) | Speed (kt) | Altitude (ft) |
| Max | 10.0 | 10.0 | 100.0 | 3000.0 |
| Min | 0.0 | 0.1 | 0.0 | 300.0 |

# Foreseeable Operating Conditions

## Environmental Conditions

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

**Wind conditions**

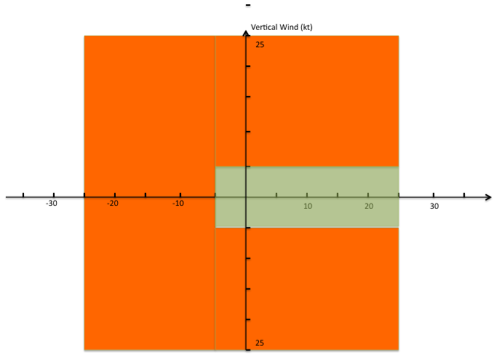
*Standard Weather Conditions* (SWC) is defined by regulation [5]. Design assumes SWC encompasses the nominal conditions (the green part of the behavioural space) and the *to-be-tolerated* abnormal conditions (the amber part of the behavioural space). Following CS25.237 and CS25.341 crosswind specifications, a symmetrical wind distribution and two upper bounds, respectively 20kt, 25kt, are assumed.

Robustness at system and item levels is the verification objective that needs these amber zones on environmental conditions. The statement ‘to-be-tolerated’ means that safety has to be preserved whereas performances may be degraded.

*Good Weather Conditions* (GWC) is defined by the AV’s supplier for *best-case analysis* in functional safety verification and in mission performance verification.It specifies that there is no icing and that wind helps improving the performances (tailwind favourable to the range). Tailwind has nearly no vertical component ([-5kt, +5kt]). The horizontal component is upper-bounded by 25kt when wind orientation is favourable. Its intensity is distributed as a uniform law over [0, 25kt].

*Adverse Weather Conditions* (AWC) is defined by the AV’s supplier for *worst-case analysis* in functional safety verification and in mission performance verification. (AWC) comprises presence of icing conditions simultaneously with strong headwind, including strong vertical components that are dangerous at take-off and landing. (AWC) is more severe than (SWC). Robustness and fault-tolerance do not ensure safety on the whole span of (AWC). AWC wind is characterized by:

* + *Horizontal component*: intensity fluctuates in [-35kt, -25kt] distributed as GL(-30,10)[[3]](#footnote-3). Positive wind (tailwind) pushes the drone towards its waypoint.
  + *Vertical component*: intensity fluctuates in [-10kt, +20kt] as GL(5,15). Positive vertical wind lifts the drone.



*Figure 3: Safety region view of wind conditions*

**Icing conditions**

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

They are most likely to occur at take-off and landing (cloud traversals).

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

Mass increase is unbounded and may last until the AV stalls because of excessive extra weight.

## 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. On-board mission management software addresses this issue and prevents take-off when mission completion is not ensured.

Multiple and inconsistent versions of the mission parameters may be uploaded (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 logics.

## Failures

Breakdowns may occur at any time on electrical, hydraulic, and digital components. It is assumed that there is no failure of the AV’s mechanical body or of the data-bus’ cables.

Loss of digital communications (internal and/or external) are however possible in case of RF-transceiver failure.

Cascading effects (e.g electrical -> hydraulic -> mechanical), thermal effects, vibrational effects may lead to many combination of simultaneous component failures (see CCA[[4]](#footnote-4)s on the safety process side). 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 USB-key may be considered.

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 the CP at mission’s beginning and end,
3. **Environment**: the wind and icing mission profiles,
4. **Drone**: the component physical failures that may randomly occur during the mission (failure modes),

Every scenario is defined by specifying these four parallel threads. They are interleaved into a single mission timeline.

The first scenario is a representative of *best-case* conditions: no perturbation, mission success. This group of conditions constitutes the most frequent cases.

The last scenario is a representative of *worst-case* conditions: accumulation of perturbations beyond system mitigation capabilities, leading to mission abort. It belongs to a group of cases that should be very remote (quantification is out of scope of the use case).

These two extreme-case scenarios are in ‘A’ mode. They exercise autonomy on one hand to test routine optimal efficiency and the other hand test the limits of the robustness and fault-tolerance domains.

Scenarios 2 and 3 are intermediate cases managed in ‘RP’ mode: the operator copes with the unexpected events by changing the speed (energy saving), the altitude (icing avoidance) or the distance (decrease for reduction of exposure to additional failure modes).

## Scenario Coverage

Testing coverage at layer 0 and layer 1 is a major issue of system development assurance.

What coverage beyond requirement coverage?

This section is intended to help consider *behavioural coverage* based on combinatorial analysis. The set of 4 scenario patterns is expected to help cover 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. Since there are infinitely many possible joint profiles of these variables, an approach to finite-case reduction may be:

* Reduction of the infinitely many weather conditions to a few equivalence classes (SWC, GWC, AWC),
* Reduction of the infinitely many initial energy levels to three cases: best-case (maximum capacity), average-case (medium capacity), worst-case (low 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 input coverage analysis.
* Altitude and speed: a uniform grid may be defined over the range of the two input parameters.

### Discrete Coverage

It applies to the relative ordering of events and to their mapping to the physical timeline.

The events to be considered are:

* Interactions on CP (power, mode, bay, USB-stick, rotators, start),
* Reception of commands from GS,
* System failure modes,
* “Zero-crossings” of continuous dynamics (e.g. the instant at which range is met, the instants at which reference altitude or reference speed is caught, alarm thresholds, etc.).

An approach to reduction to finitely many scenarios may be *adversarial* *conservative abstraction* with respect to:

* The safety objectives,
* The performance objectives,

The finitely many chosen scenarios have to define the event orderings and time mappings that are provably the least favourable to mission success.

### Hybrid Coverage

µXAV is a 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 are the numbers of scenarios resulting from the two previous coverage analyses.

In the sequel we define 4 scenarios in conformance with the pattern approach. To save space the field operator’s and the GS operator’s timelines are merged into a single “Operators’ ” timeline. The four scenarios are presented in alignment tables to facilitate identification of their respective differences. The first table aligns the two missions in autonomous mode (scenarios 1 and 4). The second one compares scenarios 2 and 3.

These four scenarios are implemented in MATLAB file InputScenarios.m

Definition of supplementary scenarios and analysis of their requirement coverage is left to layer 0 verification and validation activities [1].

## Scenario Specifications

### Pre-flight

In pre-flight phase the environment plays no role and failure modes are unlikely.

Some latent failures may manifest themselves at power-on on worst-cases.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario 1** | | | **Scénario 4** | | |
| **Operators** | **Environment** | **Failure Modes** | **Operators** | **Environment** | **Failure Modes** |
| ON/OFF Push |  |  | ON/OFF Push |  |  |
| Switch on ‘A’ |  |  | Switch on ‘A’ |  |  |
| Switch on ‘OPEN’ |  |  | ‘1’ dialled on rotator 1 |  |  |
| Payload Installed |  |  | ‘0’ dialled on rotator 2 |  |  |
| Switch on ‘CLOSED’ |  |  | USB-key plugged-in  (10nm, 3000ft, 100kt) |  |  |
| ‘0’ dialled on rotator 1 |  |  | Await 4s |  |  |
| ‘5’ dialled on rotator 2 |  |  | Switch on ‘OPEN’ |  |  |
| USB-key plugged-in  (5nm, 1500ft, 50kt) |  |  | Payload Installed |  |  |
| Await 10s |  |  | Switch on ‘CLOSED’ |  | Electrical Pump Fail |
| If ‘READY’ push START |  |  | If ‘READY’ push START |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario 2** | | | **Scénario 3** | | |
| **Operators** | **Environment** | **Failure Modes** | **Operators** | **Environment** | **Failure Modes** |
| Push ON/OFF |  |  | Push ON/OFF |  |  |
| Switch on ‘OPEN’ |  |  | Switch on ‘RP’ |  |  |
| Payload Installed |  |  | Await 8s |  |  |
| Switch on ‘CLOSED’ |  |  | ‘1’ dialled on rotator 1 |  |  |
| Switch on ‘RP’ |  |  | Message received  GS\_NavigationParameters  (10nm, 3000ft, 100kt) |  |  |
| ‘0’ dialled on rotator 1 |  |  | ‘0’ dialled on rotator 2 |  |  |
| ‘5’ dialled on rotator 2 |  |  | USB-key plugged-in  (6nm, 2500ft, 75kt)  Operator error |  |  |
| Message received  GS\_NavigationParameters  (5nm, 2250ft, 100kt) |  |  | Switch on ‘OPEN’ |  |  |
| Message received  GS\_NavigationMode ‘RP’ |  |  | Messages received  GS\_NavigationMode ‘RP’  GS\_NavigationOption ‘ALTITUDE’ |  |  |
| Message received  GS\_NavigationOption ‘SPEED’ |  |  | Payload Installed |  |  |
| Await 15s |  |  | Switch on ‘CLOSED’ |  |  |
| If ‘READY’ push START |  |  | If ‘READY’ push START |  |  |

### Flight

Operators play no role is scenarios 1 and 4 (autonomous cases).

Many variants of failure mode sequences may be played in scenarios 3 and 4 (see appendix A for a comprehensive list of the failure modes).

The conditions of scenario 4 are so adverse that emergency landing is triggered in autonomous mode. A variant in ‘RP’ mode could monitor the drone’s degradation and trigger emergency landing manually.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario 1** | | | **Scénario 4** | | |
| **Operators** | **Environment** | **Failure Modes** | **Operators** | **Environment** | **Failure Modes** |
| n.a. | (GWC) | none | n.a. | (AWC) |  |
|  | Take-Off  5kt Tailwind |  |  | Take-Off  20kt Headwind | T=20s  Engine 1 Failed |
|  | Cruise  5kt Tailwind |  |  | Icing  From t=25s to t=45s | T=30s  MMS.CH2.CPU Failed |
|  | Descent  5kt Headwind |  |  | Cruise  30kt Headwind  25kt Vertical Wind Bursts | T=40s  EPS.Modulator Failed |
|  | Landing  5kt Headwind  No Vertical WInd |  |  | Landing  30kt Headwind  Wind Shear  20kt Vertical | T=55s  MMS.CH1 Bus Failed |

Scenario 2 illustrates avoidance of bad conditions:

1. The first one because of strong adverse headwind at 2250ft: a command to descend to 1000ft is sent in hope for weaker wind,
2. But icing is suspected at this lower altitude (detected by the joint trends of electrical over-consumption and spurious losses of altitude). A climb order to reach 1500ft is sent: an attempt to fly still at low altitude but above the icing conditions,

Scenario 3 illustrates exposure time reduction: shortening of the distance and lowering of the cruise altitude to minimize impact in case of hard emergency landing. After two breakdowns, occurrence of third non-tolerated failure mode may most likely trigger emergency landing.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scénario 2** | | | **Scénario 3** | | |
| **Operators** | **Environment** | **Failure Modes** | **Operators** | **Environment** | **Failure Modes** |
|  | (SWC)  Compliance with Airwothiness Regulation | No component failure |  | (SWC)  Compliance with Airwothiness Regulation |  |
|  | Take-Off  10kt Headwind |  |  | Take-Off  No Wind |  |
|  | Cruise altitude 2250ft  30kt Headwind |  |  |  | Loss of Engine 2  during climb |
| The GS Operator modifies the navigation parameters :  Option=’ALTITUDE’  Altitude=1000ft | Decrease of the adverse wind with altitude decrease 18kt at 1000ft |  |  |  | Loss of MMS Channel 1  The drone becomes vulnerable in case of additional failure |
|  | Icing Condtions  50g/s at drone speed [50kt,75kt] and altitude [800ft,1300ft] |  |  | The GS Operator modifies the navigation parameters :  Option=’ALTITUDE’  Altitude=300ft  Distance = 7nm instead of 10 nm |  |
| The GS Operator modifies again the navigation parameters :  Option=’ALTITUDE’  Altitude=1500ft |  | Energy shortage pending  Energy initial capacity was compatible with (SWC) but weather conditions near (AWC ) |  |  | Loss of Bus Transfer |
|  | Icing stays constant on [1000ft, 1300ft] and stops on [1300ft, 1500 ft] |  |  |  |  |

### Post-flight

For all scenarios :

1. The field operator awaits 30s while reading the displays and LEDs of the control panel
2. He pushes the ON/OFF switch to OFF.

# 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**

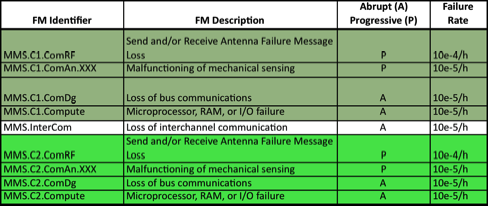
All internal and external timing aspects are taken into account.

See [2] for more details.

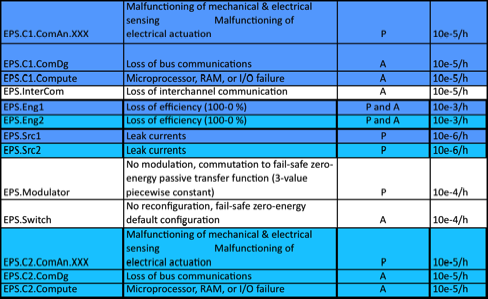
# Appendix A – Failure Modes

Part of the failure modes listed in the following tables has no observable effect for the operators (sensor, actuator, and communication failures). Observable failures are to be preferred for simulations. The first two failure modes of scenario 3 and scenario 4 are observable in GS messages and CP displays.

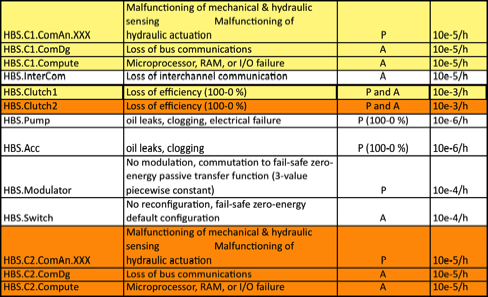
## Mission Management System



## Electrical Propulsion System



## Hydraulic Braking System



1. Radio Frequency [↑](#footnote-ref-1)
2. CS 25.1309. Regulation requires *exhaustive* analysis, not best-effort, state-of-the-art, or comprehensive analysis. [↑](#footnote-ref-2)
3. **G**aussian **L**aw [↑](#footnote-ref-3)
4. Common Cause Analysis [↑](#footnote-ref-4)