|  |
| --- |
| UNCLASSIFIED |

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

|  |
| --- |
|  |
| RESSAC Case Study  µXAV Air Vehicle Functional Hazard Analysis |

|  |  |
| --- | --- |
|  | SCOPE |
|  |  |
|  |  |
|  |  |

|  |
| --- |
|  |

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

|  |
| --- |
| 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 |
| See original image |  |  |
|  |  | Name 4 |
|  |  | Fonction 5 |
| DASAVIA |  |  |
|  |  | Name 5 |

Table of contentS

1. PREAMBLE 5

1.1 Document Issues 5

1.2 Executive Summary 5

2. Purpose of the document 6

3. references 7

4. conformance to ARP 4761 rev. A 8

5. AFHA Inputs 10

6. review of aircraft level functions 11

7. failure conditions of aircraft LEVEL functions 12

7.1 Hazard Analysis 13

7.1.1 Energy 13

7.1.2 Environmental Conditions 13

7.1.3 Computation 13

7.1.4 Component Reliability 13

7.1.5 Human Factor 13

7.2 Payload Transport Function (F\_PT) 14

7.2.1 Single Failure Conditions 14

7.2.2 Combined Failure Conditions 15

7.3 Emergency Landing Function (F\_EL) 15

7.4 Health Monitoring Function (F\_HM) 15

7.5 Functional Interaction Failures 16

8. efFects of failure conditions 17

8.1 Payload Transport 18

8.1.1 Communication 18

8.1.2 Energy 20

8.1.3 Flight Control 20

8.1.4 Mission 21

8.1.5 Combinations of Failure Conditions 22

8.2 Emergency Landing 22

8.2.1 Flight Envelope Monitoring 22

8.2.2 Hard Landing Command 23

8.3 Health Monitoring 23

8.3.1 Detection and notification of component failure modes 23

9. classification of effects’ severities 25

9.1 Payload Transport 26

9.1.1 Communication 26

9.1.2 Energy 27

9.1.3 Flight Control 27

9.1.4 Mission 28

9.1.5 Combinations of Failure Conditions 28

9.2 Emergency Landing 28

9.3 Health Monitoring 29

9.3.1 Detection and notification of component failure modes (FC\_HM) 29

10. Afha assumptions 30

11. AFHA OUTPUTS 31

12. AFHA substantiation 33

# PREAMBLE

## Document Issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Issue** | **Author(s)** | **Updating purpose** |
| 03/06/2017 | 1 | E. Ledinot | Creation of the document, limited release by email |
| 13/06/2017 | 2 | E. Ledinot | Severities supplemented, first version uploaded on Github. |
| 30/12/2017 | 3 | E. Ledinot | Editorial changes when performing the PASA |

## Executive Summary

Air Vehicle level Functional Hazard Analysis conformant to ARP 4761 revision A.

Identifies the hazards using the µXAV operational specification, the level 0 functional specification, and the level 0 organic architecture.

Identifies the failure conditions for each level 0 function and identifies their severity.

# Purpose of the document

This document is the output artefact of the Air-vehicle level Functional Hazard Analysis (AFHA). AFHA is the first activity of the safety assessment process.

It is used as input of the Preliminary Air-vehicle level Safety Assessment (PASA), and it is necessary:

* to the development process (see the life-cycle document),
* to the assurance process (baseline or based on the Overarching Properties).

# references

[1] µXAV Air Vehicle Operational Specification.

[2] µXAV Air Vehicle Functional Specification.

[3] µXAV Process Definition.

[4] µXAV MMS System Functional Specification.

# conformance to ARP 4761 rev. A

As of June 2017, revision A has not been released.

However, the new document is nearly finalized (industrial comments phase). Many enhancements have been added at aircraft level to address ever tighter integration between systems (e.g Cascading Effect Analysis, Failure Condition Functional Mapping, MBSA, etc.).

As the RESSAC case study was designed to address the safety-critical aspects related to multi-system multi-physics that arise in cross-system control functions, it makes sense to seek conformance of the use case with the forthcoming version of ARP 4761.

For self-contentedness of this document, in particular for readers external to the aeronautic community, the essentials of the standard are reminded at the beginning of every section. This informative material is mentioned in italic for clear separation from the true content of the document. Traceability of the excerpts to the sections of ARP 4761-A is ensured with the following notation: [letterOfAppendix.u.v.w].

Conformance of µXAV’s AFHA is partial because some aspects are meaningless for a drone-like air vehicle very different from Part 25 aeroplanes (e.g impact for crew and occupants). The structure of the document is conformant with APPENDIX A, AIRCRAFT FUNCTIONAL HAZARD ASSESSMENT (AFHA) Déc. 2016.

*The AFHA process is a top down method for identifying failure conditions and assessing the severity of failure condition effects as shown in Figure A-1.*

**

*Figure A-1 AFHA Activites*

*The assessment process consists of the following activities:*

1. *Gather AFHA inputs,*
2. *Review and confirm that the aircraft level functions and the functional breakdown are complete and at the appropriate level of detail,*
3. *Determine the failure conditions associated with the aircraft functions,*
4. *Determine the effects of each failure condition considering flight phases, operational and environmental conditions and events,*
5. *Assess and classify the severity of each failure condition’s effects,*
6. *Capture AFHA assumptions.*

*The Aircraft Functional Hazard Assessment (AFHA) is a process that allows the identification and evaluation of potential hazards related to an aircraft* ***regardless of the details of its design****. It is performed early in the development process and is used to* ***establish the safety objectives for the functions*** *of the aircraft to achieve a safe design.*

*An AFHA is* ***independent of system function allocation****. Typically the AFHA may require change only if assumptions are found to be incorrect during the development process, not as a result of system design.*

# AFHA Inputs

*The inputs to the AFHA are the aircraft level functions, derived from the aircraft design objectives and the fundamental necessities of flight due to the laws of physics, and the operational and environmental conditions the aircraft is designed to encounter [A.2.1].*

The required inputs for the development of µXAV are provided by [1] and [2].

The AV-level functions, i.e that are mapped on more than one system, defined in [2] are:

* Payload Transport (F\_PT)
* Communication (F\_CM)
* Energy Management (F\_EM)
* Health Monitoring (F\_HM)
* Fault Tolerance (F\_FT)
* Emergency Landing (F\_EL)

The environmental conditions defined in [1] are:

**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**

Their effect is the 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.

# review of aircraft level functions

*The AFHA does not define aircraft functions; however, it requires a clear, explicit and complete list of aircraft functions as an input*. *For the AFHA, the aircraft functions should be described in terms of* ***what*** *the function is to accomplish,* ***rather than the means envisioned to implement*** *the function. The* ***completeness of the function list is essential*** *to AFHA. There should be consistency between the functions analyzed in the AFHA and the aircraft functional requirements.*

*Aircraft functions are broadly stated and intended to be inclusive of all possible implementations, as no functional decomposition or design decisions may have yet been considered. The list of aircraft functions used as an input to the AFHA should include all functions performed by the aircraft as a whole.*

*The aircraft functions may be broken down into sub-functions, resulting in a hierarchical structure with two or more levels. Failure conditions are derived from the lowest level of the function decomposition. Functional decomposition does not imply a particular allocation of functions to systems, but allows more specific failure conditions to be derived and assessed in the AFHA.* [A.2.2].

For self-contentedness of the document, here is the list of the air vehicle level functions, with their sub-functions, if any, and a brief description of their behavior. See [1], [2], [4] for further details:

* **Payload Transport (F\_PT)**

It ensures transport of a payload while meeting various navigation constraints. It decomposes into four sub-functions:

* + *Communication Management (F\_CM),* digital communication with the ground station and between the systems (EPS, HBS, MMS), analog links with the physical devices (sensors and actuators),
  + *Energy Management (F\_EM),* monitors the electrical capacity stored in the two electrical sources,
  + *Mission Management (F\_MM)*ensures supervision: it schedules the phases of a mission (take-off, climb, cruise, landing) depending on all events that may occur (communication, energy, external conditions, failure modes etc.). F\_MM also performs navigation, i.e defines the target operating point for flight control,
  + *Flight Control (F\_FC),*analyzes the sensors and computes the commands to actuate the drone. It ensures stability despite disturbances (wind, icing), and meets the cruise operating point submitted by F\_MM.
  + *Fault Tolerance (F\_FT),* reconfigures the functions and resources to cope with the failures that occur during the mission.
* **Emergency Landing (F\_EL),** monitors the drone’s dynamics, checks the phase-dependent flight domain envelope, and aborts the mission in case of long lasting safety escapes.
* **Health Monitoring (F\_HM)** monitors the health status of all the equipments, and notifies the detected failures to supervision (F\_MM).

# failure conditions of aircraft LEVEL functions

*A failure condition is a descriptive statement that characterizes the nature of the failure or impairment of a function. The failure conditions describe the failed state of the aircraft function including the amount or type of impairment.*

*Failure conditions vary in detail with the level of function from which they are derived, from extremely broad descriptions for aircraft level functions, such as “total loss of thrust” to very specific cases at the system level function evaluation, such as “loss of altitude indication barometric correction”.*

*Failure conditions can be broadly categorized as the* ***loss*** *of a function or as a* ***malfunction****. In general each aircraft function will have one loss of function and one malfunction of interest.* *Loss of function may be total or partial. Malfunction is a condition where the function is performed outside its specified limits (e.g. erroneous, uncommanded, misleading).*

*Failure conditions may have* ***vastly different effects depending on*** *whether the crew are notified and are able to perform timely* ***mitigating actions****. Separate failure conditions may be created considering whether the crew is aware or unaware of the condition.*

*A failure condition identification matrix may be used to assist the analyst in considering all types of failure conditions for every function. This is one method of summarizing failure condition identification.*

| ***ID #*** | ***Aircraft Function*** | ***Total loss*** | ***Partial loss*** | ***Malfunction*** |
| --- | --- | --- | --- | --- |
| *3* | *Control aircraft energy* | | | |
| *3.1* | *Maintain or increase aircraft energy* | | | |
| *3.1.1* | *Provide thrust* | *3.1.1.L1 Insufficient thrust to maintain positive climb rate* | *3.1.1.L2 Insufficient thrust to meet required climb gradient* | *3.1.1.M1 Uncommanded high thrust* |
| *3.2* | *Reduce aircraft energy* | | | |
| *3.2.1* | *Provide controlled aerodynamic drag* | *3.2.1.L1 Total loss of controlled aerodynamic drag* | *3.2.1.L2 Reduced controlled aerodynamic drag* | *3.2.1.M1 Uncommanded aerodynamic drag device deployment* |
| *3.2.2* | *Provide high lift capability* | *3.2.2.L1 Total loss of high lift capability* | *3.2.2.L2 Reduced high lift capability* | *3.2.2.M1 Uncommanded high lift activation without crew awareness*  *3.2.2.M2 Uncommanded high lift activation with crew awareness* |

*Failure conditions in the AFHA are broadly stated in order to* ***provide a scope which encompasses all detailed failure scenarios*** *that can lead to the top level functional effect.*

*If the* ***functional decomposition*** *is performed in such a way that the sub- functions identified are required to achieve a necessary aircraft function,* ***combined failure conditions*** *of these functions should be identified. Functional dependency should be evaluated for all functions from which failure conditions are derived.*

*If the function list developed for the assessment includes* ***related functions****, the AFHA should consider* ***combined failures*** *of the related functions*

*All quotes originate from [A.2.3].*

## Hazard Analysis

Seeking systematic identification of the potential failure conditions of any given function, the hazard sources that are relevant for µXAV have been reviewed hereafter.

### Energy

Speed, altitude and kinetic energy are hazard sources, since any uncontrolled flight into terrain may damage goods and hurt people.

There are no hazards related to air separation (flight collision avoidance) in the case study. Navigation is limited to 2D motion of the drone (Distance, Altitude) in an empty sky.

Electrical energy is the only power source. Voltage and currents aboard the drone are not dangerous, but wrong energy management during flight may lead to crash.

### Environmental Conditions

Wind gusts are the main hazard. The flight control laws can only compensate bounded wind disturbances.

Icing leads to mass increase, energy over consumption, and possibly stall followed by crash.

### Computation

Specification faults and implementation faults at any level (system, software, and hardware), if not mitigated by fault tolerance mechanisms, may lead to flight control failures and consequent unintended harmful behaviours of the drone.

### Component Reliability

The physical devices (pumps, electrical motors, electronic components, etc.) may fail. These failure events are the only ones amenable to probabilistic quantification by the safety assessment process.

### Human Factor

The field operator may enter wrong mission data.

The ground station operator may also enter wrong mission data and send inappropriate navigation commands.

## Payload Transport Function (F\_PT)

### Single Failure Conditions

| **ID #** | **Aircraft Function** | | **Total Loss** | | **Partial Loss** | **Malfunction** |
| --- | --- | --- | --- | --- | --- | --- |
| F\_PT | Payload Transport | | | | | |
| F\_PT.  F\_CM | Manages internal and external communications | | | | | |
| CM1 | External communication | CM1.TL: No interaction with the ground station | | CM1.PL: One-way communication, or lossy two-way channel | | CM1.Ma: Content failures  CM1.Mb:Timing failures |
| CM2 | Digital internal communications | CM2.TL: Isolated systems, except for the analog links | | CM2.PL: Some senders off, some receivers off | | CM2.Ma: Content failures  CM2.Mb : Timing failures |
| CM3 | Analog internal communications | CM3.TL: All analog sensing and actuation links are off | | CM3.PL: Some peer-to-peer links are off, | | CM3.M: Content failures (noise) |
| F\_PT.  F\_EM | Energy Management | | | | | |
| EM | Estimation of energy storage | EM.TL: No estimate | | EM.PLa: No estimate on the primary source  EM.PLb: No estimate on the secondary source | | EM.M: non detected wrong estimate (misleading) |
| F\_PT.  F\_FC | Flight Control | | | | | |
| FC1 | Attitude  Control | FC1.TL: permanent safety escape (stall, swirl, etc.) | | FC1.PL: transient safety escapes | | FC1.M: unstable control |
| FC2 | Speed & Altitude  Control | FC2.TL: permanent violation of avigation constraints | | FCL2.PLa:transient violation of preset altitude  FCL2.PLb: transient violation of preset speed | | FCL2.M: unstable regulation (oscillatory, overshoots in dampening perturbations etc.) |
| F\_PT.  F\_MM | Mission Management | | | | | |
| MM | Navigation settings | MM.TL: freeze of parameters and modes | | MM.PLa: modes frozen  MM.PLb: parameters frozen | | MM.M: the mode or some parameter has a non detected erroneous value |

Analog and digital communications are distinguished because they have significantly different reliability characteristics. Analog communications are assumed to be more reliable and robust than bus-based communications.

Topology of communications, and consequently of cascading failure effects, are also different between digital and analog links: 1-to-n with buses, 1-to-1 with analog links.

Note: The failure conditions of F\_FT are missing.

### Combined Failure Conditions

This section is similar to §7.5, but it addresses combinations of failures internal to F\_PT (§7.5 addresses the external ones).

Regarding the physical initiators, i.e the analog link failure modes or the physical causes to inaccurate energy estimation, architectural analysis is needed, in particular on the electrical powering of analog links, sensors and actuators. This dependency analysis, made in PASA or CCA[[1]](#footnote-1), has to determine which of the above listed failure conditions can be regarded as independent and which ones are subject to potential dependences (cascading effects).

Regarding the potential residual development faults in F\_CM, F\_EM, F\_FC and F\_MM (systematic failures), a conservative approach would be to consider any combination of the listed failure conditions[[2]](#footnote-2), because they are many data-flow dependencies between these sub-functions.

A more advanced and exploratory approach would be to use static analysis on the source code of the integrated sub-functions to compute the influence cone[[3]](#footnote-3) of each ‘contract-failure’. Depending on the results, some software-induced cascading effects could be proved impossible, and the FC combination analysis may be reduced accordingly.

## Emergency Landing Function (F\_EL)

| **ID #** | **Aircraft Function** | **Total Loss** | **Partial Loss** | **Malfunction** |
| --- | --- | --- | --- | --- |
| F\_EL | Emergency Landing | | | |
| EL1 | Flight envelope monitoring | EL1.TL: permanently undetected safety escapes | EL1.PL: transient unavailability of safety escape detection | EL1.M: unpredictable false positives and false negatives on safety escapes |
| EL2 | Hard landing command | EL2.TL: crash prevention by fast descent and landing unavailable | EL2.PL: possibly poorly controlled landing (high energy at impact) | EL2.M: possibly uncontrolled landing (crash or severe damage) |

## Health Monitoring Function (F\_HM)

| **ID #** | **Aircraft Function** | **Total Loss** | **Partial Loss** | **Malfunction** |
| --- | --- | --- | --- | --- |
| F\_HM | Health Monitoring | | | |
| HM | Detection and notification of component failure modes | HM.TL: No detection, no alarms | HM.PL: detection and alarm available for some components, or some failure modes only | HM.M: arbitrary errors in signaling component losses or failure modes |

## Functional Interaction Failures

F\_PT, F\_EL and F\_HM do exchange information at AV level. Interaction failures between these top level functions are not addressed by the function per function analysis of sections 7.2, 7.3, 7.4.

Failures at AV level induced by interaction between the top level functions after one or several function-failures, have to be considered.

Examples of such post-failure interactions are:

* Wrong or unavailable component health statuses delivered by F\_HM propagate in F\_PT and impact mission supervision (e.g viability decision making),
* F\_PT and F\_EL control each other: F\_PT activates F\_EL in case of emergency (soft and hard landing), F\_EL monitors F\_PT and aborts it in case of persistent non-diagnosed safety escapes. So ‘correctness-failures’ (activation of a residual fault) may propagate between these two functions.

The analysis should also consider if “failure-less failure conditions” are possible. In other words the analysis should envision the case where a failure at AV level would result from the interaction of functions that are correct individually, but not collectively.

# efFects of failure conditions

*The AFHA next examines each failure condition and determines the effects on the* ***aircraft****,* ***crew*** *and* ***occupants***.

*Failure condition effects may vary depending upon the* ***flight phase*** *at the time of failure condition occurrence. The failure condition effects may also be affected by* ***operating or environmental conditions****. The failure condition effects assessment considers* ***the most severe plausible effects*** *of failure conditions during each flight phase or condition.*

*The effects are described by a* ***narrative*** *and characterized with* ***brief statements*** *regarding the effect in aircraft, crew and occupant categories.* *The effects of each failure condition are determined by constructing a scenario narrating its expected outcome.*

***Worst case environmental conditions*** *within the approved aircraft operating envelope should be considered to be present where relevant when evaluating the effects of failure conditions. [A3.4]. These conditions are implicitly assumed and need not be specifically stated for every failure condition, though their influence should be described in the failure effects narrative when relevant.*

*In some cases the approved envelope for an* ***environmental condition*** *includes* ***extremes*** *that are infrequent. In these cases it may be acceptable to define a range of normally encountered conditions, with conditions outside this range considered to be environmental extremes.* *It may be acceptable to add the environmental extreme explicitly to the failure condition. In most cases, the original failure condition should be retained and a combined failure condition (original failure condition and environmental extreme) added to the AFHA [A3.4]*

*The* ***combined failure condition*** *should be assessed for* ***all*** *identified* ***flight phases*** *[A3.4].*

*Certain* ***environmental occurrences*** *outside the approved operating envelope may be considered environmental events. Examples of environmental events include:*

*• Windshear or microburst,*

*• Iced runway,*

*• Icing conditions, for aircraft not approved for flight in known icing conditions.*

*In most cases, the original failure condition should be retained and a combined failure condition (original failure condition and environmental event) added to the AFHA. The combined failure condition should be assessed for all identified flight phases.[A3.5]*

*Each of the failure condition’s effects is* ***qualitatively******assessed****. Usage of* ***standard******assessment******terms*** *facilitates consistency between failure condition descriptions. [A2.4]*

*A* ***matrix or table*** *may be used to capture the evaluation of each failure condition, applicable flight phases, failure effects descriptions and relevant environmental or operational conditions.. The specific evaluation format for describing the effects is not critical, provided it is thorough {A2.4].*

***Assumptions*** *may need to be established in order to predict some failure condition effects. Any such assumptions should be* ***documented*** *and subsequently* ***confirmed****. [A2.4]*

## Payload Transport

### Communication

#### CM1 External Communications

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | GS operator prevented from commanding and/or monitoring | none | none |
| Climb | Total or partial freeze of navigation parameters | none | none |
| Cruise | Total or partial freeze of navigation parameters | Mitigation no longer possible in RP mode | Mitigation no longer possible in RP mode |
| Descent | Freeze on transient descents. No effect on the final descent | Mitigation no longer possible in RP mode | Mitigation no longer possible in RP mode |

**Environmental conditions:** windy conditions worsen impact of communication loss with GS.

#### CM2 Digital internal communications

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | Mission cancellation | None on payload  Supervision partially isolated from the energy management systems | none |
| Climb | None on field operator  GS operator may lose control in RP mode | Supervision (MMS) partially isolated from the energy management systems (EPS, HBS) | Dependent on success of EPS hardware- only flight control |
| Cruise | None on field operator  GS operator may lose control in RP mode | Supervision (MMS) partially isolated from the energy management systems (EPS, HBS) | Dependent on success of EPS hardware- only flight control |
| Descent | None on field operator  GS operator may lose control in RP mode | Supervision (MMS) partially isolated from the energy management systems (EPS, HBS) | Dependent on success of hardware- only flight control |

**Environmental conditions:** windy conditions worsen impact of bus communication loss between systems.

#### CM3 Analog internal communications

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | Mission cancellation in any mode (A or RP) | None on payload  Impact on sensing and actuating | none |
| Climb | None on field operator  Put stress on GS operator as sneaky physical behaviors may be observable | Impact on flight control | Dependent on F\_FC’s ability to mitigate the effects of the perturbed signals |
| Cruise | None on field operator  Put stress on GS operator as sneaky physical behaviors may be observable | Impact on flight control | Dependent on F\_FC’s ability to mitigate the effects of the perturbed signals |
| Descent | None on field operator  Put stress on GS operator as sneaky physical behaviors may be observable | Impact on flight control | Excessive speed, wrong attitude, or wrong location at landing |

**Environmental conditions:** windy conditions worsen impact of disturbed signals or sensor/actuator losses.

### Energy

#### EM Estimation of Energy Storage

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | Fooled decision making on mission viability | None on payload | none |
| Climb | None on field operator  GS op: Fooled decision making on mission viability | Supervision may be fooled by erroneous viability estimates | Dependent on loss of flight control and emergency landing |
| Cruise | None on field operator  GS op: Fooled decision making on mission viability | Supervision may be fooled by erroneous viability estimates | Dependent on loss of flight control and emergency landing |
| Descent | None on field operator  GS op: Limited when at end of mission | Potential loss of control in case of unanticipated energy exhaustion at landing | Crash in case of under actuation |

**Environmental conditions:** windy conditions and icing worsen sensitiveness to erroneous energetic management and energy shortage.

### Flight Control

#### FC1 Attitude Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | none | none | none |
| Climb | Field operator exposed to injury at take-off  Stress on GS operator | AV may stall and crash | Limited if crash occurs early in climb phase |
| Cruise | None on field operator  Stress on GS operator | AV may stall and crash | Greater with altitude and speed |
| Descent | None on field operator  Stress on GS operator | AV may crash, even in “controlled flight” | Uncontrolled landing with injuries or fatalities |

**Environmental conditions:**

* Windy conditions and icing worsen sensitiveness to erroneous flight control,
* Bad weather conditions may cause transient attitude-related safety escapes even by correct control (perturbations beyond specified limits).

#### FC2 Speed and Altitude Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | none. | none | none |
| Climb | Field/GS operator(s) may detect trajectory is inconsistent with settings | Navigation constraints violation exposes the drone to air separation risks | In case of air collision |
| Cruise | GS operator may detect trajectory is inconsistent with settings | Navigation constraints violation exposes the drone to air separation risks | In case of air collision |
| Descent | GS operator may detect trajectory is inconsistent with settings | Possible mission failure (landing at a wrong place) | In case of landing at a wrong place |

**Environmental conditions:** windy conditions and icing worsen sensitiveness to erroneous flight control. Bad weather conditions may cause transient navigation-related safety escapes, even with correct flight control (perturbations beyond specified domain).

### Mission

#### MM Navigation parameters settings

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | Fooled operators. Unavailability of remote mitigation actions | none | none |
| Climb | Fooled operators. Unavailability of remote mitigation actions | AV exposed to air collision | Only in case of air collision because of erroneous altitude |
| Cruise | Fooled operators. Unavailability of remote mitigation actions | AV exposed to air collision | Only in case of air collision because of erroneous altitude |
| Descent | Fooled operators. Unavailability of remote mitigation actions | AV exposed to incorrect landing location | Incorrect payload delivery place |

**Environmental conditions:** unanticipated or inaccurate estimation of windy/icing conditions worsen the listed effects.

### Combinations of Failure Conditions

A cumulative approach, without snow ball or cascading effects, may be used to define the effects of multiple failure conditions, as defined by 7.2.2.

## Emergency Landing

### Flight Envelope Monitoring

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | none | none | none |
| Climb | In bad weather condition GS operator may notice undetected safety escapes and need for manual activation of emergency landing | Controlled Flight into Terrain (CFT) accidents | In case of CFT accidents |
| Cruise | In bad weather condition GS operator may notice undetected safety escapes and need for manual activation of emergency landing | Controlled Flight into Terrain (CFT) accidents | In case of CFT accidents |
| Descent | In bad weather condition GS operator may notice undetected safety escapes and need for manual activation of emergency landing | Controlled Flight into Terrain (CFT) accidents | In case of CFT accidents |

**Environmental conditions:** windy and icy conditions make detection of flight safety escapes all the more necessary and likely to happen.

### Hard Landing Command

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | none | none | none |
| Climb | none | none | none |
| Cruise | none | none | none |
| Descent | Stress in case of awareness | Crash inevitable in case of mission abortion | Crash energy dependent on speed and altitude when mission is aborted |

**Environmental conditions:** windy and icy conditions make emergency landing more sensitive to crash.

## Health Monitoring

### Detection and notification of component failure modes

|  |  |  |  |
| --- | --- | --- | --- |
| **Flight Phase** | **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** |
| Mission Preparation | Fooled perception of airworthiness | Inaccurate viability decision making | none |
| Climb | Fooled decision making by GS operator (RP mode) | Supervision fooled by inaccurate AV health perception | Cascading effect on flight control leading to crash |
| Cruise | Fooled decision making by GS operator (RP mode) | Inaccurate viability decision making | Cascading effect on flight control leading to crash |
| Descent | Fooled decision making by GS operator (RP mode) | Supervision fooled by inaccurate AV health perception | Cascading effect on flight control leading to crash |

**Environmental conditions:** no significant sensitiveness of component reliability to wind and icing conditions. Turbulence may generate mechanical vibrations and shocks, that in turn may lead to failure modes in electrical wiring or electronic components.

# classification of effects’ severities

*When the identification and summary of all failure condition effects is complete, the failure condition classification activity can begin. The severity classification is determined by using* ***the most severe*** *effect associated with a failure condition.*

*A single classification for the failure condition may be derived from the worst case effect in any flight phase or separate classifications may be obtained for each flight phase, by selecting the worst case classification from the aircraft, crew and occupants effect categories for each flight phase.*

*It is important to* ***avoid assuming a severity classification during the identification of failure effects****, as the assessment process can be incomplete if there is excessive focus on preconceived outcomes for common failure conditions.*

*The summary statements of effects from the previous section are used to determine the classification of each failure condition by comparison to the appropriate regulatory guidance*.

| ***Effect on Aircraft*** | ***Effect on Crew*** | ***Effect on Occupants*** | ***Classification*** |
| --- | --- | --- | --- |
| *Complete loss of aircraft*  *Prevents continued safe flight and landing* | *Crew unable to accomplish required tasks, or*  *Required crew strength or skill in excess of crew capability, or*  *Crew incapacitation* | *Multiple occupant fatalities* | *Catastrophic* |
| *Large reduction in aircraft functional capability or safety margin* | *Excessive crew workload increase, crew unable to fully accomplish required tasks, or*  *Crew physical distress* | *Small number of occupant fatalities or severe injuries not including flight crew* | *Hazardous* |
| *Significantly reduced aircraft functional capability or safety margin* | *Significant crew workload increase, or*  *Conditions impairing crew efficiency* | *Occupant physical distress or non-fatal injuries* | *Major* |

[A2.5]

## Payload Transport

### Communication

#### External Communications (FC\_CM1)

Long cruise with occurrence of unanticipated events defines the worst case conditions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Loss of flexibility for the field operator. For long range missions with unanticipated events, loss of remote mitigation capability | Safety margin reduction (loss of remote mitigation capability) | Higher risk of crash in bad conditions | Major |

#### Digital internal communications (FC\_CM2)

All phases posterior to take-off are worst case conditions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Loss of mitigation cruise parameter change. | Safety margin reduction because viability decision is no longer transmitted to secondary control laws in EPS. | More risk of crash, especially on bad weather conditions. Loss of mission (no payload delivery) | Hazardous |

#### Analog internal communications (FC\_CM3)

All phases posterior to take-off are worst case conditions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Injury at take-off.  Workload of GS operator | May lead to loss of control if occurrence on key sensors or actuators | Crash | Catastrophic |

### Energy

#### Estimation of Energy Storage (FC\_EM)

Worst case conditions are defined by long range missions with overestimation of energy left.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Unexpected mission losses (underestimates case) or crashes (overestimates case) | Mislead mission management with potential crash or undue mission cancellations | In case of crash, dependent on altitude, speed, payload mass | Catastrophic |

### Flight Control

#### Attitude Control (FC\_FC1)

All phases posterior to take-off are critical.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| At take-off, the field operator is exposed to injuries | Destruction of the drone and payload | Damage on estate. High speed, high mass crashes may lead to severe injuries or fatalities. | Catastrophic |

#### Speed and Altitude Control (FC\_FC2)

Cruise and landing are the most critical phases.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Increased GS workload | Destruction in case of air collision, loss in case of landing at a wrong location | Severe in case of air collision or crash over urban areas | Hazardous |

### Mission

#### Navigation parameters settings(FC\_MM)

Cruise (with parameter updates, i.e transient climb/descent phases) is the worst case condition.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| GS operator loses NAV control (mitigation means) | No direct impact on payload.  Possible energy over consumption, with safety margin reduction | If crash occurs as ultimate consequence of wrong navigation | Major |

### Combinations of Failure Conditions

Communication failures have electrical or electronic initiators, i.e physical and random. Layer 0 and layer 1 architectural analysis is in charge of establishing the dependence and independence conditions between these initiators.

The other initiators are activation of development faults. Any combination has to be considered since location and effect of these potential residual faults are unknown.

## Emergency Landing

#### Flight Envelope Monitoring (FC\_FEM)

All flight phases are worst case, especially in bad weather conditions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Workload on GS operator in case of mitigation actions | Severe in case of bad weather conditions (crash risk) | Severe in case of crash | Catastrophic |

#### Hard Landing Command (FC\_HLC)

Descent is worst case.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| none | Destruction | Damages, injuries, fatalities | Catastrophic |

## Health Monitoring

### Detection and notification of component failure modes (FC\_HM)

Worst case is underestimation of resource losses.

All phases are equally concerned since at any time non-anticipated need for emergency landing leads to crash.

|  |  |  |  |
| --- | --- | --- | --- |
| **Effect on field and/or GS operator(s)** | **Effect on AV & Payload** | **Effect on ground people and goods** | **Classification** |
| Misleads, wrong mission management decisions in RP mode | No degradation | Higher risk of crash | Hazardous |

# Afha assumptions

*There are instances where details necessary to perform the AFHA are not yet available. In these cases, the safety analyst must make assumptions regarding operating or environmental conditions, airframe capabilities or other factors. Assumptions may be made for as-yet-unspecified development information. These are inputs to the AFHA process which are necessary, but were not yet available in the functional information provided to the AFHA process.*

***Any consideration*** *made during the assessment that was* ***not based on validated functional information*** *should be documented as an assumption.*

*Assumptions should be captured and* ***formally communicated*** *to the appropriate development information sources. The assumption may* ***then*** *be* ***confirmed, or corrected*** *based on new development information. In the latter case, a design change or a revision of the AFHA may be required. [A2.5]*

This section should contain a recap of the assumptions made when establishing the list of functions, identifying their associated failure conditions, and filling-in the effects/severity tables.

At this stage of development, there is no identified assumption used when establishing this first edition of AFHA.

# AFHA OUTPUTS

*The output of the AFHA process is a document or set of documents containing:*

• *The list of aircraft level functions and functional decomposition; including supporting discussions needed to aid the understanding of the function scope and purpose and the relationship between top level functions and lower level functions,*

*• The detailed AFHA worksheet, containing all the identified failure conditions, their effects during each flight phase and their resulting severity classifications,*

*• The list of assumptions used in identifying functions, performing the function decomposition, identifying failure conditions, determining failure condition effects or determining severity classifications.*

*The AFHA document is not expected to significantly change as the development process proceeds. Since the aircraft level functions and decomposition do not depend on system architecture; only assumptions found to be incorrect, changes to basic airframe definitions or high level operating parameters have the potential to invoke a revision of the AFHA.*

*AFHA results are an input to the PASA. If the PASA identifies deficiencies in the analysis, or design deficiencies that cause aircraft functional information to be changed, this may result in an iteration of the AFHA.*

|  |  |
| --- | --- |
| ***Table Entry*** | ***Entry Definition*** |
| *Aircraft Function*  *Sub Function* | *The hierarchy of the aircraft function and sub-functions being analyzed. The number of levels in the aircraft level functional decomposition is at the analyst’s discretion; however, the decomposition of aircraft level functions should not presume a particular allocation of functions to systems.*  *See section A.2.2* |
| *ID No* | *Unique numbering system for organization, tracking and traceability* |
| *Failure Condition* | *Description of the failure or impairment of the function.*  *See section A.2.3* |
| *Flight Phase* | *List the applicable aircraft operational phases for this failure condition. See section A.2.4* |
| *Effect of Failure Condition on Aircraft, Crew, Occupants* | *Description of the Failure Condition effects on the aircraft, crew and occupants. Sufficient detail should be provided to understand the failure scenario and conclude the severity classification based on the captured effects. Separate effects statements and classifications may be provided for each flight phase or a single generalized effect and worst case classification provided for the failure condition.*  *See section A.2.4* |
| *Severity Classification* | *Catastrophic, Hazardous, Major, Minor, or No Safety Effect as defined in applicable certification guidance material.*  *See section A.2.5* |
| *Assumptions, Comments, Rationale or Reference to Supporting Material* | *Data supporting the determination of effects and classification of the failure condition, including any applicable guideline material.*  *See section A.4* |

This document is the output of µXAV’s AFHA.

There is no separate spreadsheet.

# AFHA substantiation

*Substantiation of AFHA failure conditions, failure effects and failure effects classifications is encompassed in the aircraft and system development process objectives described in ARP4754B/ED79B.[A4]*

To be clarified: to what extent does the development process review AFHA’s outputs in the use case? To be addressed when discussing safety in the criteria.

1. Common Cause Analysis, including Common Mode Analysis, Zonal Analysis and Particular Risk Analysis [↑](#footnote-ref-1)
2. The failure conditions are assumptions on the external effect of activation of the unknown residual faults [↑](#footnote-ref-2)
3. With sound tools the influence cones are over approximated, so independence inference is conservative [↑](#footnote-ref-3)