29th Congress of the International Council of the Aeronautical Sciences
St. Petersburg, Russia; September 7-12, 2014

AUTONOMOUS TAKE-OFF AND LANDING FOR UNMANNED AIRCRAFT SYSTEM: RISK AND SAFETY ANALYSIS

Sergio Chiesa*, Sara Cresto Aleina*, Giovanni Antonio Di Meo*, Roberta Fusaro*, Nicole Viola*
***Politecnico di Torino**

Keywords: *UAV, ATOL, Risk and Safety Analysis, Avionic System*

Abstract

The aim of this paper is to conceive the possibility of applying the Required Navigation Performance (RNP) requirements where Global Navigation Satellite System (GNSS) augmentations are considered for the Automatic Take-Off and Landing (ATOL). An aircraft, belonging to the Medium Altitude Long Endurance (MALE) category of Unmanned Aerial System (UAS) has been considered as case-study. Once the avionic architecture has been designed, the Safety and risk analysis was carried out with a particular focus on Functional Hazard Analysis and Fault Tree Analysis techniques. The proposed methodology allows the researchers to evaluate the reliability of each avionic equipment and the safety level of the whole avionic system. Furthermore, the results pointed out the main criticalities of the architecture and some future in-depth studies are proposed.

1 General Introduction

The Risk and Safety Analysis is one of the most important evaluations that should be performed since from the beginning of the design phase. Moreover, it is also an activity proposed by the most important System Engineering methodologies reported in literature [1] [2]. Its increasing relevance is mainly due to the fact that this type of analysis allows to prevent design errors and to choose the safer configurations among a group of possible architectures. Like all the other analyses that are performed during the whole Product Life Cycle, the Safety and Risk Analysis is inserted in an iterative process and it can be performed at different levels of detail.

In this article, typical tools of Risk and Safety Analysis are applied to an aircraft belonging to a MALE UAS category to conceive the possibility of applying the Required Navigation Performance (RPN) requirements where Global Navigation Satellite System (GNSS) augmentations are considered for the Automatic Take-Off and Landing (ATOL). This study has been performed within the SMAT (Sistema di Monitoraggio Avanzato del Territorio – Advanced Territory Monitoring System) research program, a project funded by Regione Piemonte e Fondo Europeo di Sviluppo Regionale, now at its second phase. In particular, SMAT F2 proposes to study and demonstrate an advanced monitoring system to accomplish planned tasks and to prevent and monitor different types of emergency, using a fleet of Unmanned Aerial Vehicles (UAVs). This field of studies is in-line with the market trends. In particular, as far as our particular case-study is concerned, it has been noticed that the steady increase in the Air Traffic (AT) together with the more stringent constraints for fuel consumption and emissions reduction produced the need of improving some navigation performances, especially for the civil aviation aircraft. The basic idea here proposed is to use the GNSS (Global Navigation Satellite System) Signal in Space (SIS) performances [3]. Three are the main fields of interest for the improvement of the Air Traffic Management (ATM) functionalities: Communication,

Navigation and Surveillance, in accordance with [4]. As far as communication and surveillance fields are concerned, the adoption of new data links, able to elaborate greater data flows, can allow improvements for the performances. Conversely, navigation is the main field of interest in which a big amount of new technology improvements are focused in order to obtain more accurate estimation of the aircraft position. The augmentation systems of GPS-SIS are the basic element of these new avionic technologies presented and discussed in the following sections. Firstly, the paper deals with the analysis of the state of the art of avionic navigation systems (certified Area Navigation (RNAV) and/or Required Navigation Performance (RNP)) today implemented, or under-development, in the civil aviation. In this context, a particular attention is paid to the new techniques and relative technologies requested for precision approaches with vertical guidance (i.e. APV). The paper also includes a detailed analysis of the international normative listed through ICAO and FAA documents focusing on the new augmentation systems (SBAS – Satellite Based Augmentation System, GBAS – Ground Based Augmentation System, ABAS – Aircraft Based Augmentation System) and its relative Technical Standard Operations (TSO) requirements. In the second part of the article the integration of these systems has been supposed into an UAS avionic architecture in order to perform autonomous landing. Then, a Functional Hazard Analysis (FHA) focused on the ATOL function is performed. After Risk considerations, Safety analysis has been applied to the designed avionic system, for verifying that important redundancies considered in avionic design could ensure safety levels requested for operations. To this purpose, Fault Tree Analysis (FTA) is proposed. Finally, the most promising design alternatives are described and some design improvements are suggested in order to design an ATOL system able to comply with the safety requirements.

2 Background and generalities about Navigation systems

In order to understand the functionalities implemented in the avionic system configuration that will be proposed in a following section, it is necessary to provide an overview of the state-of-art technologies and the International Rules requirements.

2.1 Background and ICAO Road Map

Through the Assembly Resolution A37-11 contained in [5], the International Civil Aviation Organization (ICAO) indicated to all the members the implementation of the new airworthiness set of requirements called Performance Based Navigation (PBN), listed in ICAO document 9613 [6]. PBN is defined as the international regulatory framework to standardise the implementation of Area Navigation (i.e. RNAV) worldwide [6], with a focus on the performances requested for the aircraft approach operations with vertical guidance (Approach with vertical guidance, APV). RNAV is the main operating standard navigation for the civil aviation. Today, almost all the civil aircraft have adequate area navigation performances, but only the modern jet-aircraft implement Required Navigation Performances (RNP) which represent the new standard requirements for modern civil avionic systems layout, reported in [6]. The APV procedures are based on the GNSS and Barometric Vertical Navigation (Baro-VNAV) functionalities, allowing accurate and continuous capacities of lateral and vertical guidance without any support from the common terrestrial radio navigation systems such as Instrumental Landing System (ILS). It is convenient to notice that the integration between vertical guidance and lateral guidance would greatly reduce the risk of fatal accidents during approach and landing operations.

ICAO identified the Baro-VNAV and the augmented GNSS systems as the suitable technologies to ensure vertical guidance performances. Between these two systems, the augmented GNSS has been selected for our purposes, because it is also suitable for older and smaller aircraft.

From the ICAO Air Navigation Conference (ANC-11) all the members

confirmed their intentions to perform and improve satellite navigation performances through the implementation of the PBN. Finally, in the above-mentioned AC-36-23, ICAO suggests to all members the implementation of the APV methodology as the new approach and landing procedure. Moreover, this technology can also be exploited in order to guarantee "back-up mode" for Precision Approach (PA). Furthermore, ICAO established a timeline for implementation of the PBN and RNP navigation performances on each national territory of State members and it is reported in [6].

2.1 PBN and RNP: General Guideline and Navigation System

PBN enables the transition from the classical *sensor-based navigation* to the modern *performance-based navigation*. The first one is the navigation strategy adopted by the majority of the civil aircraft for over 40 years. As far as this navigation strategy is concerned, each flight track is based on direct signals issued from ground-based radio navigation aids. This method reveals that the routes are completely dependent by the terrestrial location of the navigation beacons resulting in longer and less efficiency routes. Conversely, through the PBN navigation requirements, RNAV defines a navigation method that allows the aircraft operations along any desired flight route within the coverage of the terrestrial-reference navigation aids. This type of navigation completely removes all the restriction imposed by the sensor-based navigation. In particular, the PBN concept defines the RNAV navigation systems performances in terms of integrity, accuracy, availability, continuity and functionality levels requested for each specific aircraft operations. Today, the Basic GNSS equipment, introduced after the ANC-10, are under development through the implementation of the augmentation systems such as SBAS and GBAS, while the performances of the GNSS systems will be further improved by the introduction of Galileo and a more efficient GLONASS system.

The RNP specifications [6] [7] include all the requirements for the on-board self-contained performance monitoring and alerting systems and procedures. These specifications should be considered as the primary way to verify the requested safety levels of the navigation systems, relating both to longitudinal and lateral navigation performances. Indeed, they allow the crew to immediately detect whether the navigation system achieves the navigation performances requested for the operation.

The use of navigation systems RNP-certified offers sensible safety, operational and efficiency benefits during the entire mission. Indeed, the implementation of the vertical guidance performances provides the progress of navigation applications from 2D (along the track and lateral control) to 3D. In this contest it is important to underline that navigation systems certified PBN/RNAV are not automatically certified RNP, and vice-versa. In particular, through the implementation of the PBN specifications, it is possible to ensure RNAV capabilities. The determination of aircraft position can be performed by every navigation systems that respect the RNP or RNAV specification imposed by the airspace of operation. The *ICAO document number 9613* [6] reports the entire navigation specifications structure here shortly described with the RNP specifications. Examples of civil aircraft with RNP capabilities are: Airbus A320, Airbus A380, Boeing B-737 NG and Boeing B787.

As far as RNAV navigation systems are concerned, they are designed to ensure proper accuracy levels with repeatable and predictable flight trajectories through the integration of input information from different kinds of avionic equipment. Among them, the most important to be considered are the air data sensors, the inertial reference system and the radio and satellite navigation coupled with the internal navigation databases. The basic functions that can be ensured by a general RNAV system are: navigation, flight plan management, guidance and system control. Typically, the RNAV navigation systems are multiple-sensor based including GNSS, DME, VOR and IRS and navigation databases, which contain all the pre-stored information about the navigation aid locations, route and procedures.

2 Approach and Landing Procedures

As it is outlined in the previous sections, this article deals with the Risk and Safety Analysis of an avionic system able to permit the UAV to perform automatic take-off and landing. For this reason, in the following subsections, at first traditional procedures are examined and then, new augmentation systems are introduced.

3.1 State of Art technologies

Commonly, the approach procedures are exclusively based on the ground navigation aids, such as ILS, VOR and Non Directional Beacon (NDB). It is important to underline that the PBN requirements do not include any RNAV approach specifications for approach and landing operations. Consequently, the RNAV (GNSS) approaches have been reclassified as RNP Approach with Lateral guidance (RNP APCH-LNAV). These types of approach procedure are only referred to the RNP APCH specifications which include desired accuracy values of lateral guidance (LNAV) for all phases of flight of instrument approach manoeuvres: initial, intermediate, final and, eventually, missed approach segment, as shown in the following Figure.

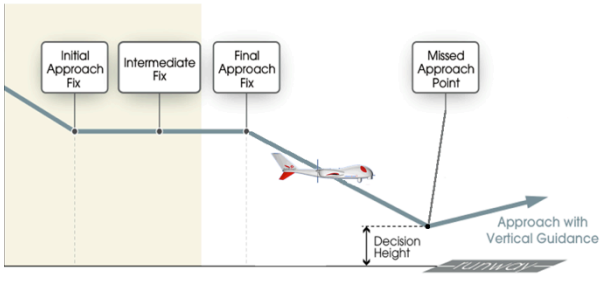

Fig. 1. Typical UAS approach maneuvers.

Two classes of RNP approach operations have been defined: the RNP APCH and RNP AR APC. The first one is characterised by a RNP value for final approach segment fixed at 0.3 nm for RNP APCH, varying from 0.3 nm to 0.1 nm for RNP AR APCH. Another important difference between them is that RNP APCH may include vertical guidance, while RNP AR APCH always includes vertical guidance and requires specific crew training and operational approval. The categories of RNP APCH procedures that today can be performed are essentially four:

- RNP APCH - LNAV: where lateral guidance is provided by the GNSS Signal In Space (SIS).
- RNP APCH - LNAV/VNAV: where the GNSS SIS ensures lateral and vertical guidance provided also by barometric vertical navigation (Baro - VNAV).
- RNP APCH - LP (Localiser Performance): where lateral guidance performances, equivalent to localiser approach, is provided by augmented GNSS SIS.
- RNP APCH - LPV (Localiser Performance with Vertical guidance): where lateral and vertical guidance is provided by augmented GNSS SIS, such as SBAS. This approach technique is similar to the GNSS-ILS approach procedure.

It has also important to remind that, before the advent of the vertical guidance, the approach classification was divided in only two types of approach strategies: Non-Precision Approach (NPA) and Precision Approach (PA). Once the ICAO resolution A36-23 has been released, a third classification of Approach with vertical Guidance (APV), was defined by ICAO as

"*An instrument approach procedure which utilises lateral and vertical guidance but does not meet the requirements established for precision approach and landing operations*".

The table below clearly summarizes the actual situation for approach and landing procedures.

3.2 Augmentation systems

All the required specifications, regulating the implementation of the satellite systems such as GNSS and GLONASS for air navigation, are summarised in the ICAO document "*Annex 10 Aeronautical Telecommunications*" [10].

Considered augmentation systems for the GNSS SIS are: the *Aircraft-Based Augmentation System* (ABAS), the *Satellite-*

Based Augmentation System (SBAS) and the *Ground-Based Augmentation System* (GBAS). Annex 10 reports all the basic technical requirements for each augmentation system mentioned. As far as ABAS systems are considered, the most important element is the GNSS receiver that is integrated with the sensors inside the navigation sub-system. Conversely, the main feature of the SBAS system is represented by its ability to correct the navigation errors introduced by the ionosphere. The high levels of integrity and accuracy ensured by the SBAS systems allow matching the requirements for APV approach procedures. There are four different performance levels, or Classes, that can be reached through SBAS systems, depending on the needed corrections and then on the integrity and accuracy level requested for the navigation sub-system. They are:

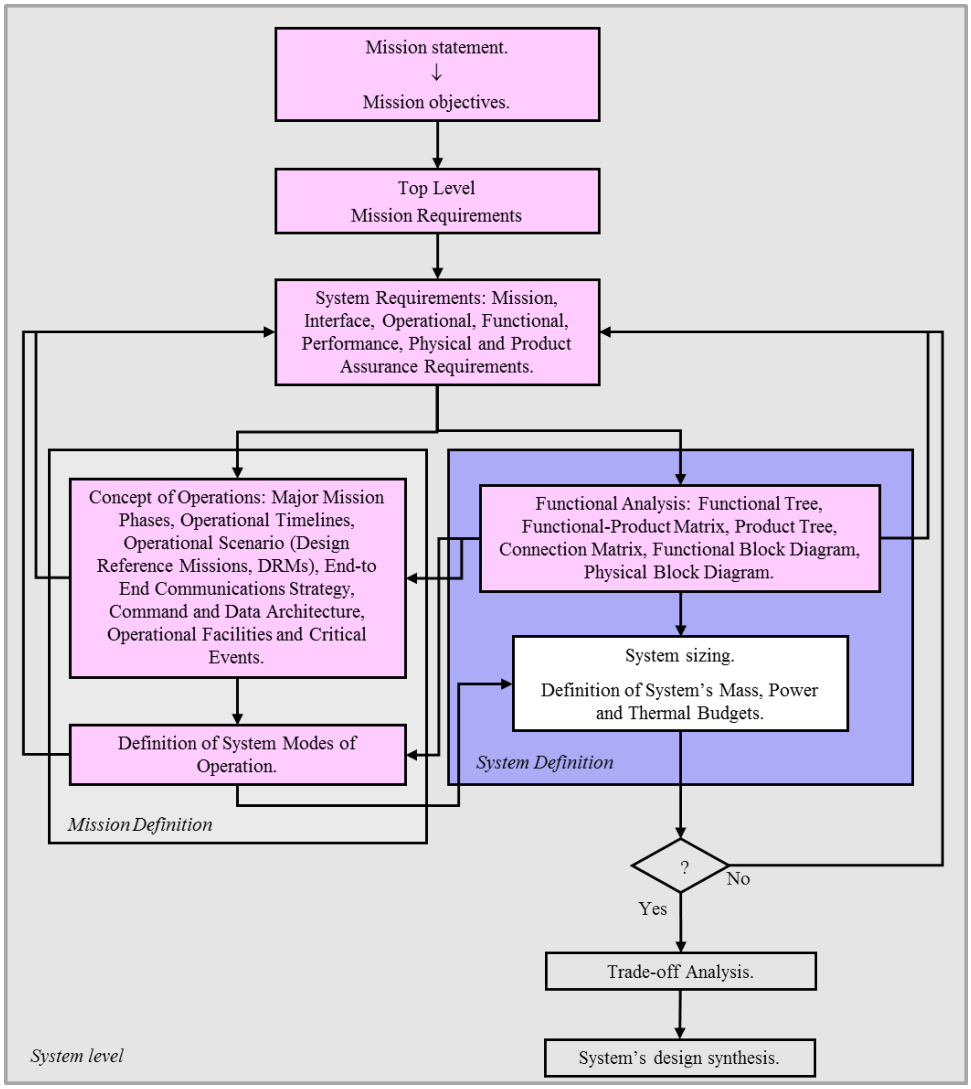

Fig. 2. System Engineering iterative approach

- Class I: SBAS systems supported the en-route, terminal and LNAV approach procedures)
- Class II: SBAS systems supported the en-route thorough LNAV/VNAV approach procedures
- Class III and IV: SBAS systems supported the en-route and terminal with

LPV, LP, LNAV and LNAV/VNAV approach procedures

Considering GBAS system, the requirements are regulated through standard RTCA/DO-253A and by FAA TSO-C161a and TSO-C162a but indications are also present in the ICAO document Annex 10 in which it is clearly defined the GBAS systems as "able to manage more than 49 approaches at the same time" support PA CAT-I procedures.

Inside the "*Annex 10 Standard and Recommended Practises*" (SARPs) is also indicated that GBAS augmentation systems will be considered Precision Approaches CAT-II and CAT-III certified, but this is still under development and test. The FAA AC 20-138c, coupled with the ICAO documents, has to be considered like the most powerful reference for all TSO necessary for implementation of augmented GNSS systems.

4 Avionic System proposed for ATOL functionalities

Once the main topics and navigation requirements have been introduced, this paragraph proposes an avionic architecture suitable for an Unmanned Aerial platform able to ensure Automatic Landing capabilities. The configuration that will be used has been proposed by Alenia Aermacchi, one the major partner in SMAT F2 project and it is the results of an iterative design process in which Functional Analysis had a relevant role. The scheme reported in Figure 2 shows the logical and chronological sequence of activities that has to be performed as suggested by System Engineering Methodologies [8], [9], [10].

The selected avionic architecture is a "Duplex type architecture" composed by two main Data Buses connecting all systems for exchanging data information. On the right and the left side of the scheme proposed all the augmentation systems earlier described are reported, without the presence of ILS, VOR, DME and NBD system: the commonly terrestrial navigation aids.

The presented avionic architecture is designed to perform APV approach procedures. Each single augmentation system primary sends its output to the CMU, directly connected with one of the main data buses. A "switch box" (yellow box in the Figure) allows the control station to switch from automatic to manual control of the UAS platform.

5 Safety and Risk Analysis

Once the avionic architecture has been defined, the safety and risk analysis has been carried out. The primary goal of the safety process is to ensure the detection, and then the evaluation, of safety critical conditions that might affect the UAS operations. The steps followed for the Safety Analysis are:

- Avionic system description,
- Functional Hazard Analysis
- System Safety Assessment (SSA).

The aim of the SSA is to assess the risk related with the applicable hazards. In particular, in our case the main focus is on UAS Landing operations. The SSA performed is based on Fault Tree Analysis (FTA) and uses the values obtained from FMECA analysis here not reported.

It is to be noticed that UAS is equipped with a Flight Termination System (FTS), which is a parachute useful to prevent the flight outside the segregated airspace or in order to limit damages in the case of the UAS results completely out of control.

Typically, this system can be activated by ground station or by UAS on-board systems in the case of detected loss of control.

5.2 Methodology overview

The Risk Assessment is composed by two main phases: the first one deals with the detection of hazardous events, assigning to them a severity or probability category belonging to 5 levels: Catastrophic, Critical, Major, Minor and No Safety [11] [12].

Failure Rate values (FR) of the considered avionic equipment are reported below. The presented data derive directly from Equipment Supplier/Manufacturer when possible, or are In-service data coming from Jane's Avionics [6]. In the case where it has not been possible to

obtain reliability data from Equipment Supplier/Manufacturer datasheets or literature, NPRD-11 library (Non Electronic Parts Reliability Data) has been used for deriving them. Furthermore, the following tables show each avionic item with its relative FR value.

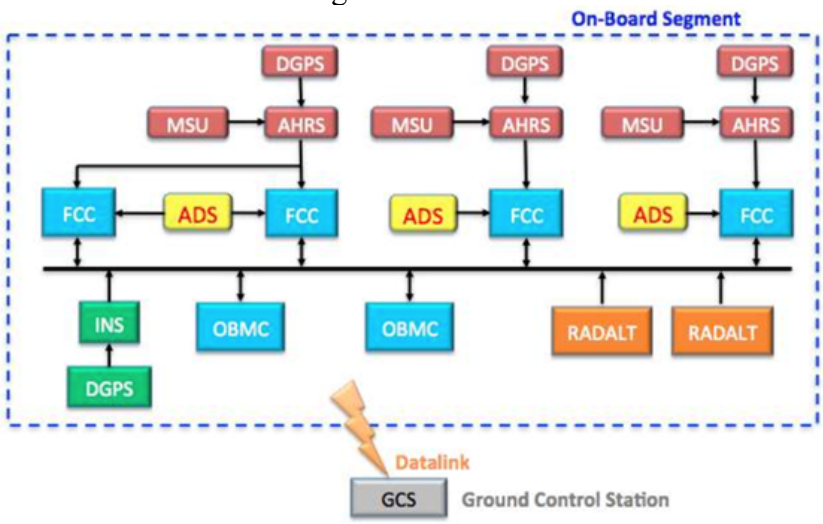

Fig. 3. Avionic system architecture.

Failure Severity	Failure Condition	Safety Objective
Catastrophic (CAT)	Failure Conditions that could result in flight collision or impact on ground population. This kind of Failure Condition could be determined by total loss of guidance control of the aircraft when the FTS is lost or not effective.	$Q<10^{-6}$
Critical (CRT)	Failure Conditions that would reduce the capability of the airplane, the ability of the crew to cope with adverse operating conditions to the extent that there would be the following: large reduction in safety margins or functional capabilities; total loss of guidance control with FTS fully effective or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely. The event could lead to a limited risk of causing injuries to third parties, possibly fatal. Typical event would be crash in the open country (OC - a ground zone covering the test area except dedicated crash sites and runway).	$Q<10^{-5}$
Major (MJ)	Failure Conditions that would reduce the capability of the airplane, the ability of the crew to cope with adverse operating conditions to the extent that there would be, a significant reduction in safety margins or functional capabilities; a significant increase in crew workload or in conditions impairing crew efficiency. The event could cause crash of the vehicle on dedicated crash site (DCS - areas without any population), or on the active runway environment when it is cleared to use it.	$Q<10^{-4}$
Minor (MN)	Failure Conditions that would not significantly reduce airplane safety and involve crew actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in crew workload (such as routine flight plan changes).	$Q<10^{-3}$
No safety effect	Failure conditions that would have no effect on safety.	

Tab. 1. Safety requirements.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]	FR [10^{-6}] DGPS	MTBF [hrs] DGPS
Navigation: Differential GPS	GPS Antenna	20	50000	114.8085	8710.156
	GPS Receiver	20	50000		
	GPS Converter	23,3623	42804		
	Receiving Antenna (UHF)	20	50000		
	Power Supply	31,4462	31800,3		

Tab. 2. Differential GPS RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]	FR [10^{-6}] AHRS	MTBF [hrs] AHRS
Navigation: AHRS	Gyroscope/Accelerometer (x)	64	15625	192	5208,33
	Gyroscope/Accelerometer (y)	64	15625		
	Gyroscope/Accelerometer (z)	64	15625		

Tab. 3. AHRS RAMS estimations.

	Avionic Subsystems	FR [10^{-6}] MSU	MTBF [hrs] MSU
Navigation: MSU	Magnetic Sensor Assembly (Magnetic and Temperature sensors)	17,4	57471
	Microcontroller		
	Accelerometer sensor		
	Power Supply		

Tab. 4. MSU RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]
Flight Control Computer	FCC	175	5714.28

Tab. 5. Flight Control Computer RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]	FR [10^{-6}] AHRS	MTBF [hrs] AHRS
Air Data System	Air Data Probe	20	50000	188,23	5312,65
	Electrical Connector	0.0163	$61.35*10^6$		
	Pneumatic Tube - 1	0.1104	$9,05*10^6$		
	Pneumatic Tube - 2	0.1104	$9,05*10^6$		
	Air Data Computer	130	7692,30		
	AOA Sensor	18	55555		
	TAT Sensor	20	50000		

Tab. 6. Air Data System RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]	FR [10^{-6}] AHRS	MTBF [hrs] AHRS
Inertial Navigation System	IMU	246.429	4057,96	576,42	1734, 85
	NCU	130	7692,30		
	Gyroscope/Accelerometer (x)	64	15625		
	Gyroscope/Accelerometer (y)	64	15625		
	Gyroscope/Accelerometer (z)	64	15625		
	Power Supply	8.42	118764,84		

Tab. 7. Inertial Navigation System RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]
On Board Mission Computer	OBMC	175	5714.28

Tab. 8. On Board Mission Computer RAMS estimations.

	Avionic Subsystems	FR [10^{-6}]	MTBF [hrs]	FR [10^{-6}] AHRS	MTBF [hrs] AHRS
RADALT	RADALT Antenna	20	50000	133,2462	7504,91
	RADALT Electronic Unit	81.8	12224,94		
	Power Supply	31,4462	31800,34		

Tab. 9. RADALT RAMS estimations.

5.3 Fault Hazard Analysis

The Fault Hazard Analysis (FHA) is a systematic and in-depth analysis performed in order to detect and classify all the possible fault conditions [13] [14] [15]. The input data of the FHA are: safety requirements, critical categories, functional and system analysis. As it has been previously noticed, this type of analysis can be done since the very beginning of the design phase until the last verification phases. Moreover, it can be applied both at system level (e.g. aircraft) and sub-system level (e.g. avionic sub-system).

The output of the FHA typically consists of a list of hazardous events classified according to each single critical level assigned and characterised by their probability value. Table 10 reports the FHA analysis performed at aircraft level.

Failure Hazards Analysis		
Hardards	**Code**	**Severity**
Automatic Landing		
Loss of control during landing before DH	01-LLT	MJ
Loss of control during landing after DH	02-LLT	CRT
Loss of ATOL function before DH	03-ATOL	MIN
Loss of ATOL function after DH	03-ATOL	MJ
Loss of control during landing before DH with controlled crash in DCS	03-LLT_CC_DCS	CRT
Loss of control during landing before DH with uncontrolled crash in DCS	04-LLT_ UC_DCS	CAT
Loss of control during landing before DH with controlled crash in OC	05-LLT_ CC_OC	CAT
Loss of control during landing before DH with uncontrolled crash in OC	06-LLT_ UC_OC	CAT
Loss of control during landing after DH with controlled crash in DCS	07-LLT_BDE_ CC_DCS	CRT
Loss of control during landing after DH with uncontrolled crash in DCS	08-LLT_BDE_ UC_DCS	CAT
Loss of control during landing after DH with controlled crash in OC	09-LLT_BDE_ CC_OC	CAT
Loss of control during landing after DH with uncontrolled crash in OC	10-LLT_BDE_ UC_OC	CAT

Tab. 10. FHA analysis.

For the aim of this work, the safety analysis has been conducted for the following hazardous events only, because they have been considered the most relevant:

- Loss of control during landing before DH with uncontrolled crash in OC
- Loss of ATOL function before DH
- Loss of ATOL function after DH

5.4 Fault Tree Analysis

The Fault Tree Analysis (FTA) is a deductive failure analysis focused on one particular undesired event providing a method for determining all causes that produce this event [13] [15]. The analysis starts from the identification of a particular Top Level hazard event selected between the FHA results in the table above. Then, the Top Event is analysed until all failures (called Basic Events) causing this Top Event are systematically identified following the typical "Top-down" approach. The top event causes are themselves examined to determine their immediate causes. This process is repeated, identifying the sources of system events at varying level of complexity, down to the lowest level of decomposition: the basic events. A Fault Tree diagram is a graphical representation of the logical interconnection between the failures and the conditional events based on the Reliability Block Diagram analysis of the avionic architecture, here not reported. The Top events proposed, as it has been already said, are the UAS catastrophic event "*Loss of control during landing after DH with uncontrolled crash in OC*" together with the *"Loss of ATOL function"*. The last is analysed both in the case it happens before or after the Decision Height point; in the first case it is possible to suppose Minor Effects while in the second case Major Effects can be hypothesized.

The main output produced by a quantitative FTA Evaluation is the numerical probability of the under-investigation Top Event.

In order to perform the quantitative FTA Evaluation process, the FR of each Basic Event and the "Exposure Risk Time" of the Basic Events should be set. As far as the Exposure Risk Time is concerned, it is convenient to notice that it should be associated with losses and/or malfunctions of a function/item used during the entire ATOL flight procedures. In this case the Exposure Risk Time is the estimated time of a long duration standard flight requested for the UAS platform and it has been set equal to 36 hours. In the FTA Evaluation each considered avionic item has been assumed

as "not reparable".

In addition to these considerations, it could be convenient to report some definitions.

- Q(t) is the calculated value for the unavailability (i.e. the probability of failure at a given time point).
- Q(H) is the ratio Q(t) to the mission time, which as already said is supposed to be 36 hours.

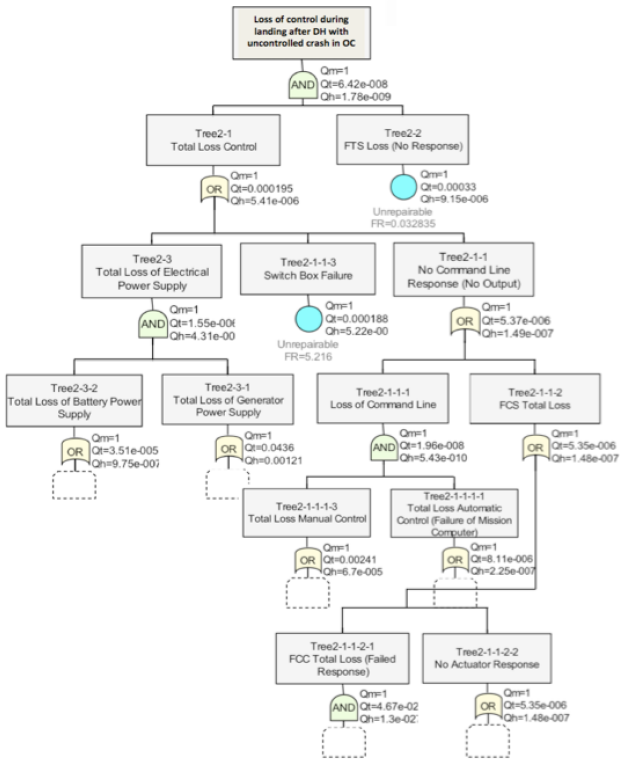

Fig. 4. FTA diagram for loss of control during landing after DH with uncontrolled crash in OC function.

Using the FR above reported, the Fault Tree diagrams have been drawn. To this purpose, a Reliability software, called Ram Commander® has been selected. Figures 4 and 5 shows the FTA diagrams obtained for the two top selected top events.

The numerical results of the performed FTA are summarized in Table 11 and 12.

Top Event	Severity	Q(t)	Q(H)	Objective
Loss of control during landing after DH with uncontrolled crash in OC	CAT	6.42e-008	1.78e-009	$Q(t)<10^{-6}$

Tab. 11. FTA results for loss of control during landing after DH with uncontrolled crash in OC function.

Top Event	Severity	Q(t)	Q(H)	Objective
Loss of ATOL function before DH	MIN	3.29e-003	9.15e-005	$Q(t)<10^{-3}$
Loss of ATOL function after DH	MJ	3.29e-003	9.15e-005	$Q(t)<10^{-4}$

Tab. 12. FTA results for loss of ATOL functionalities.

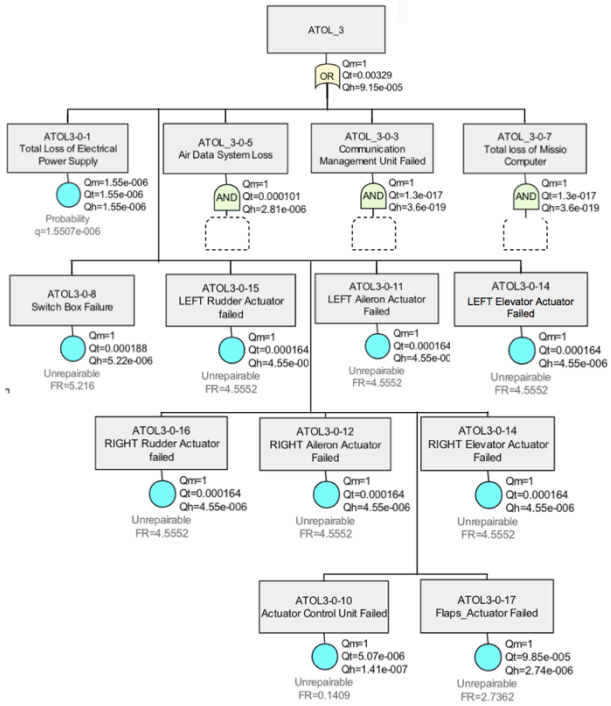

Fig. 5. FTA diagram for loss of ATOL functionalities.

5.5 Results

Once the FHA and the FTA have been performed, it is possible to associate to each failure condition, the results of these analyses and verify if the safety requirements, specified at the beginning of the process, are satisfied. In case the safety analysis underlines that the system is not compliant with the requirements, corrective actions should be hypothesized and an enhanced version of the avionic system provided. As it has already been outlined, this is a typical iterative process that ends when the designed configuration matches the safety requirements imposed by the Certification Entities.

Considering the case that has been proposed in this work, Table 11 reports the results of the analyses, the level of severity associated with the relative failure condition considered and the safety requirement that has to be satisfied (Objective).

Moreover, Table 11 reveals that the

Avionic Architecture proposed in Figure 3, provided by Alenia Aermacchi, results compliant with the above-mentioned EASA CS-25 Safety Objectives. It is also important to highlight that the case of *Total Loss of ATOL functions* during landing is equal to the probability of *Total Loss of Deviation Estimation* for the same flight phase, for this reason the associated Reliability Block Diagrams and Fault Tree result to be the equivalent. In the same way, RBD and FTA associated to the *Total loss of Deviation Estimation during T/O* are equivalent to the ones for the *Total Loss of ATOL functionalities during T/O*.

Code	Failure Conditions	Results	Severity	Objective
01-TLAPOS	Total loss of augmented position	$4{,}36*10^{-10}$	MJ	$< 10^{-5}$
02-EUAPOS	Erroneous and undetected augmented position	TBD[1]	HAZ	$< 10^{-7}$
03T/O-TLDEST	Total loss of deviation estimation in Take-Off	$3.12*10^{-8}$	MIN	$< 10^{-3}$
04T/O-EUDEST	Erroneous and undetected deviation estimation in Take-Off	TBD[1]	MJ	$< 10^{-5}$
05T/O-TLATOL	Total Loss of ATOL functions in Take-Off	$3.12*10^{-8}$	MIN	$< 10^{-3}$
06T/O-EUATOL	Erroneous and undetected ATOL functions in Take-Off	TBD[1]	MJ	$< 10^{-5}$
07LND-TLDEST	Total loss of deviation estimation in Landing	$4.84*10^{-8}$	MJ	$< 10^{-5}$
08LND-EUDEST	Erroneous and undetected deviation estimation in Landing	TBD[1]	HAZ	$< 10^{-7}$
09LND-TLATOL	Total Loss of ATOL functions in Landing	$4.84*10^{-8}$	MAJ	$< 10^{-5}$
10LND-EUATOL	Erroneous and undetected ATOL functions in Landing	TBD[1]	HAZ	$< 10^{-7}$

Tab. 11. Safety analysis results

6 Conclusions

The risk and safety analysis methodology described in this paper reveals that the avionic architecture hypothesized to perform an autonomous take off and landing it is compliant with the safety requirements. Thus, in future, further in-depth studies could be performed at component level, following the iterative process typical of the system engineering.

References

[1] INCOSE, *System Engineering Handbook,* June 2006

[2] NASA, *System Engineering Handbook,* 2013

[3] ICAO, Global Navigation Satellite System (GNSS) Manual Doc 9849, (2012)

[4] ICAO, Procedures for Air Navigation Services — Air Traffic Management Doc 4444, (2001).

[5] ICAO, *Assembly Resolution in Force Doc 9958*, (2010).

[6] ICAO, *Performance-Based Navigation (PBN) Manual Doc 9613*, (2008).

[7] ICAO, *Quality Assurance Manual for Flight Procedure Design Doc 9906*, Volume V, (2009).

[8] N. Viola, S. Corpino, M. Fioriti and F. Stesina, *Functional Analysis in Systems Engineering: methodology and applications* in Prof. Dr. Boris Cogan . Systems Engineering - Practice and Theory. p. 71-96, RIJEKA, InTech, ISBN: 9789535103226, doi: 10.5772/34556 (2012).

[9] R. Ian Faulconbridge, Michael J. Ryan, *Managing Complex Technical Projects: A Systems Engineering Approach*

[10] S. Chiesa, M. Fioriti, N. Viola. *Methodology for an integrated definition of a System and its Subsystems: the case-study of an Airplane and its Subsystems* in "Systems Engineering - Practice and Theory, ISBN: 978-953-51-0322-6", INTECH (2012)

[11] H. E. Roland, B. Moriarty *System Safety Engineering and Management,* 2nd Edition, Wiley (1990)

[12] D. Ozuncer, L. Speijker, J. Stoop, R. Curran, *Development of a Safety Assessment Methodology for the Risk of Collision of an Unmanned Aircraft System with the Ground* (2011)

[13] S. Chiesa, *Affidabilità, sicurezza e manutenzione nel progetto dei sistemi,* CLUT (2008)

[14] D. O. Anderson, *Hazard Analysis in Engineering Design,* 2001

[15] M. Waßmuth, S. C. Stilkerich, E. Lübbers, *Distributed Safety Assessment for Airborne Systems.*

Copyright Statement