Failure Modes and Effects and Criticality Analysis and Fault Tree Analysis methodologies applied to civil RPAS systems

Failure Modes and Effects and Criticality Analysis and Fault Tree Analysis methodologies applied to civil RPAS systems

Federica Bonfante[1], *Matteo* Dalla Vedova[1*] , and *Paolo* Maggiore[1]

[1]Politecnico di Torino, Department of Mechanical and Aerospace Engineering, Corso Duca degli Abruzzi no. 24, 10129, Turin, Italy

Abstract. This paper is on the Failure Modes and Effects and Criticality Analysis and Fault Tree Analysis methodologies applied to the equipment and functional subsystems of Remotely Piloted Aircraft Systems (RPAS). Such aerial vehicles have been used almost exclusively for military purposes until the first decade of the 2000s. The debate then was focused both on technical and regulatory issues and research activities. Thanks to this renewed interest on unmanned systems and thanks to relatively recent improvements in information science, telecommunication, electronics and material science a strong awareness on the potential extension of unmanned technologies to civil applications arose up. A variety of economic benefits has been recognized by the aviation community from the civil use of RPAS, but, due to the absence of the pilot on board both military and civilian RPAS have always been relegated to fly into segregated airspaces. Technical potentialities of RPAS will be fully exploited integrating them into controlled airspaces in a reliable and safe way. This paper shows an example of application of FMECA and FTA to RPAS and discusses the adequacy and utility of these methodologies to study RPAS reliability as well as the possible future developments of this work.

1 Remotely Piloted Aircraft Systems (RPAS): the origin and the expected future developments

Since 1944 the International Civil Aviation Organization (ICAO) officially acknowledged the existence of unmanned aircraft systems (UAS) in the Chicago Convention. The technical development of RPAS started in the 1950s and is still on going. RPAS were born for military purposes with the advantage to relieve the pilot from risks deriving from aerial attacks close to the enemy area. More recently thanks to the last improvements in computer science, electronics, telecommunications and material science, UAS technology has been redirected to civilian applications opening new ways and possibilities for this aeronautical new distruptive technology [1]. Expected economic benefits deriving from civilian use of RPAS will be achievd accomplishing the full and safe integration of RPAS into controlled airspaces.

* Corresponding author: matteo.dallavedova@polito.it

Physically, RPAS is composed of the aerial segment (a rotor or fixed wing RPAS or a hybrid RPAS fed by hydrogne fuel cell to ehance flight range and endurance), the ground segment (represented by a portable radiocontroller or a complete ground control station as for the moment it happens for miliatry RPAS), and the Communication, Command and Control (C3) radiolink to exchange in uplink/downlink with the aircraft [2].

This paper is organized as follows: Section 1 introduces RPAS; Section 2 describes the FMECA and FTA methodologies applied, the considered RPAS architecture used as basis for the analysis and the most significative obtained results; Section 3 sums up the conclusions and suggests possible future developments of the present work.

2 The methodology (FMECA and FTA), the RPAS architecture and the results

The reliability of a system is the probability that it performs its mission for the intended period of time under given operating conditions. An unmanned system will be considered reliable if it will remain fully operative from the preflight tests/engine start-up phase to the duration of the whole mission until landing and engine shutdown [3].

In this paper an example of application of classical aeronautical reliability analysis techniques, FMECA and FTA, is described and discussed with regards to the most critical issues.

The Failure Modes and Effect and Criticality Analysis (FMECA) [4] is an extended version of FMEA (Failure Modes and Effects Analysis which ranks each potential failure mode according to its combination of severity and probability of occurrence [4]. The criticality analysis is completed with the evaluation of the most proper solutions/actions applicable to reduce the probability of occurrence of the considered failure mode [4]. The FMEA/FMECA allows the analyst to find out single point of failures and collects them in a final report draft as per [4] at task 103. The classical FMECA has been applied to an RPAS architecture to identify single technical failures; a sort of FMECA process has been applied focusing on human factor related to RPAS. Following the Human Factor Analysis and Classification System (HFACS) model issued by Prof. James Reason [5], possible errors and violations have been identified.

The Fault Tree Analysis (FTA) has been applied to RPAS single subsystems/functionalities to find out RPAS combinations of faults capable to lead to the loss of a RPAS subsystem/functionality.

Both FMECA and FTA, that can be executed both in a quantitative and qualitative way, have been performed at qualitative level. This approach has been chosen due to the assumption that the purpose of the considered work was not to evaluate the punctual reliability of an RPAS, but the adequacy and utility of the proposed methodologies to find out critical issues in terms of single and multiple RPAS points of failure to successively derive from these data useful indications to identify technical hazards typical of RPAS.

The FMECA has been performed following the Military Standard 1629 Revision A [4]; the FTA has been performed according to the Military Handbook 338 Revision B [6].

The RPAS architecture used for the analyses and composed from the top to the bottom of the aerial segment, the radio link and the ground segment, is represented in Figure 1.

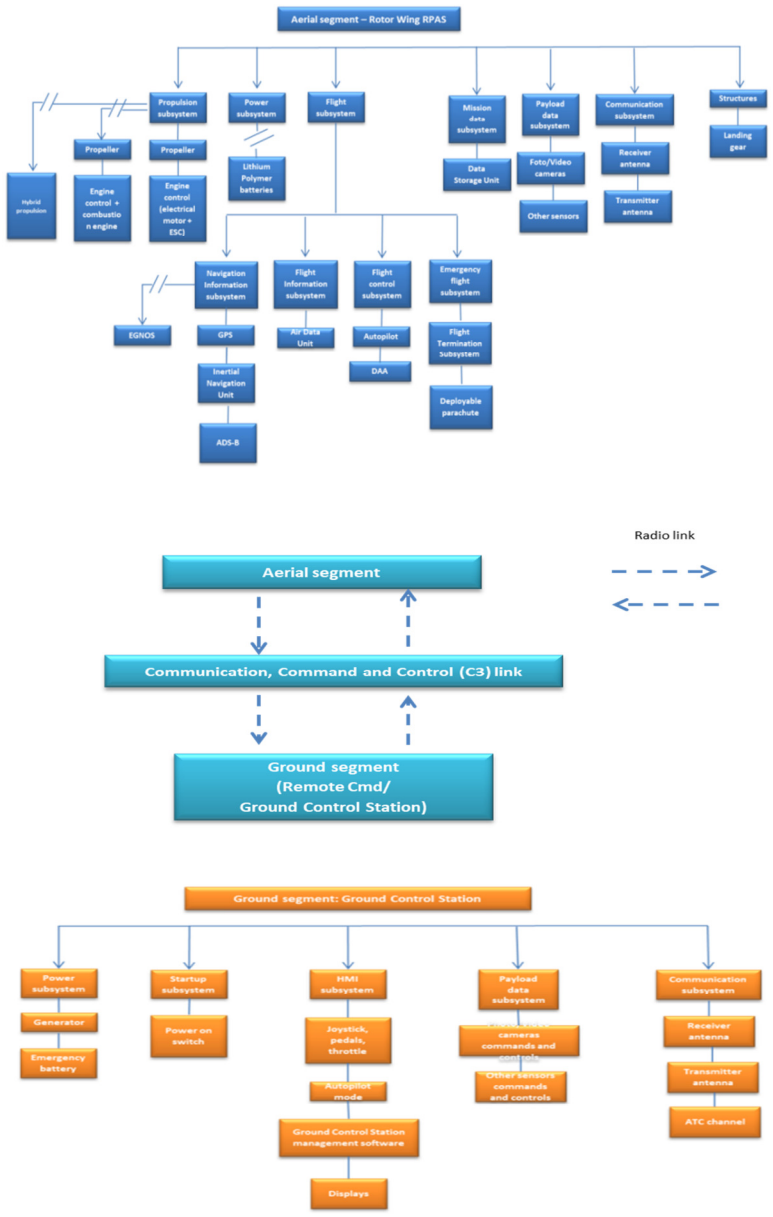

Fig. 1. RPAS architecture [3]

The RPAS subsystems and functionalities have been allocated according to RPAS mission phases as shown in Figure 2 [3] and Table 1 [3].

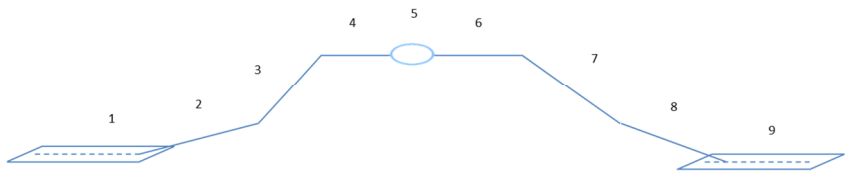

Fig. 4. RPAS flight mission phases [3]

Table 1. RPAS functionalities and mission phases [3]

RPAS Subsystems	**Mission phases (Rotor wing RPAS)**						
Start-up Subsystem	1, 2	3	4	5	6	7	8, 9
Structures	X	X	X	X	X	X	X
Propulsion Subsystem	X	X	X	X	X	X	X
Power Subsystem	X	X	X	X	X	X	X
Flight Navigation Subsystem	-	X	X	X	X	X	-
Flight Information Subsystem	-	X	X	X	X	X	-
Flight Control Subsystem	-	X	X	X	X	X	-
Emergency Flight Subsystem	-	X	X	X	X	X	-
Mission Data Subsystem	X	X	X	X	X	X	X
Payload Data Subsystem	-	-	-	X	-	-	-
Communication Command and Control subsystem	X	X	X	X	X	X	X
Ground Control Station subsystem	X	X	X	X	X	X	X

The FMECA analysis has been performed considering for every RPAS equipment the possible single failure modes. Each failure mode has been coded and described in terms of effects (local, higher and next level), mission phase affected (Figure 4 and Table 1), severity of consequences ([4] para. 4.4.3), probability of occurrence ([4], Task 102, Para. 3.1), detectability level ([4], Task 101, Para. 5.1), criticality ranking ([4], Task 102, Figure 102.2) and possible compensation or mitigation actions ([4], Task 101, Para 5.7).

The FMECA process analysis on human figures involved into RPAS operations (the remote pilot, the pilot on board manned aircraft and the Air Traffic Controller (ATC)) mentioned above has been implemented according to the same criteria.

Among all the RPAS equipment and functionalities studied, FMECA results about Automatic Surveillance Dependant – Broadcast (ADS-B) equipment and FTA results on Detect and Avoid (DAA) functionality (under Flight Control subsystem) related to ADS-B reliability and performance are reported as examples of the performed work. The reason of for this choice is that these items play a crucial role for safety in the incoming integration of RPAS into controlled airspace besides manned aircraft ([7], [8]).

Eighteen ADS-B single failures have been identified and considered performing FMECA as the most significative ones for RPAS operations.

Hereinafter some of them are reported as example to succesively focus on the discussion of the obtained results.

Results: ADS-B loss of position accuracy (Probability of occurence: E, Failure consequence level ‘Catastrophic’, Detection method: ‘None’); GPS receiver unit fault (Probability of occurrence: E, Failure consequence level ‘Catastrophic’, Detection method: ‘None’); ADS-B out antenna deterioration (Probability of occurrence: D, Failure consequence level ‘Catastrophic’, Detection method: ‘None’); ADS-B emitter transponder fault (Probability of occurence: E, Failure consequence level ‘Catastrophic’, Detection method: ‘None’); erroneous altitude data (Probability of occurence: C, Failure consequence level ‘Catastrophic’, Detection method: ‘None); abrupt interruption of ADS-B service (Probability of occurence: B, Failure consequence level ‘Catastrophic’, Detection method:

'Visual or audible warning devices'); loss of satellite integrity signal (Probability of occurence: E; Failure consequence level 'Catastrophic', Detection method: 'Visual or audible warning devices'); sudden delayed aircraft position updates without any notification (Probability of occurence: C, failure consequence level 'Catastrophic', Detection method: 'Visual or audible warning devices'); sudden loss of ADS-B data to ATC controllers (Probability of occurence: D, failure consequence level 'Catastrophic', Detection method: 'Visual or audible warning devices'); ADS-B ground station failure (Probability of occurence: D, failure consequence level 'Catastrophic', Detection method: 'Visual or audible warning devices'); human error (Probability of occurence: D, failure consequence level 'Catastrophic', Detection method: 'None').

Table 2 shows the final ADS-B resulting criticality matrix. The severity of the considered ADS-B occurrence has always been classified by the Authors as 'Catastrophic (Level I) because unavoidably an ADS-B failure impacts the safety of operation of RPAS increasing the risk for mid air collision with other aircraft (manned or unmanned).

Table 2. ADS-B criticality matrix

				CRITICALITY
LEVEL A – FREQUENT				
LEVEL B – REASONABLY PROBABLE				Abrupt interruption of ADS-B service (NISSA10)
LEVEL C - OCCASIONAL				Erroneous altitude Data (NISSA7) Degradation of data accuracy sent by the satellite to the ADS-B (NISSA12) Sudden delayed aircraft position updates without any notification (NISSA14) Degradation/loss of ADS-B signal (NISSA16) Human error (nissa18)
LEVEL D - REMOTE				ADS-B OUT antenna deterioration(NISSA3) Broadcast of distorted data (NISSA5) Sudden loss of ADS-B data to ATC controllers without notification (NISSA15) ADS-B ground station failure (NISSA17)
LEVEL E – EXTREMELY UNLIKELY				ADS-B loss of position accuracy (NISSA1) GPS receiver unit fault (NISSA2) Broadcast of incorrect data (NISSA4) Emitter transponder failure (NISSA6) Data encoding error (NISSA8) Loss of position data to be sent to the emitter (NISSA9) Abrupt lack of GPS data(NISSA11) Loss of satellite signal integrity (NISSA13)
	CATEGORY IV - MINOR	**CATEGORY III - MARGINAL**	**CATEGORY II – CRITICAL**	**CATEGORY I - CATASTROPHIC**

According to [7], the most of failure modes are undetectable from the remote pilot; in the other cases visual or audible warning devices can be foreseen for his situational awareness.

Examples of preventive measures are design solutions (redundant equipment) or operator actions like regular maintenance and testing of ADS-B avionic equipment.

On the basis of the performed analysis, redundancy can be suggested for GPS receiver using EGNOS (also more reliable than GPS thanks to Receiver Autonomous Integrity Monitoring (RAIM) or Fault Detection and Exclusion (FDE) functions) or inertial navigation equipment, in particular to compensate in case of abrupt interruption/lack of ADS-B service [7].

Avionics maintenance actions can be suggested to prevent failures due to euipment aging like ADS-B out antenna deterioration or altimeter failure,

As said, the ADS-B failure affects the 'Detect and Avoid' functionality ([9], [10]) due to the loss of RPAS/aircraft position information. Without the provision of this datum, the autoplot autopilot will not receive the input from the DAA to command the RPAS to perform the proper evasive manouvers in order to avoid collisions. The combinations of events that lead to DAA loss, that is GPS failure, altimeter failure and ADS-B failure have been formally addressed implementing a simple DAA fault tree and solving the related truth table with three variables. The loss of DAA functionality suggests the potential occurrence of hazards like 'Loss of separation' and 'Mid-air collision'.

3 Discussion and conclusions

This paper shows an example of application of reliability analysis tecniques to RPAS. The obtained results confirm that FMECA and FTA are valuable decisional tools for RPAS too while RPAS are now object of great interest and attention from the international aviation community.

This work shows an example of an extended FMECA/FTA evaluation performed on a complete RPAS architecture to find out more technical failures. Then these data have been evaluated in terms of risk assessment to implement a more comprehensive risk matrix including environmental and weather hazards.

As discussed in Section 2, useful design indications can derive from reasoning about reliability of systems both against single and combined failures. Suggestions about when and how implementing equipment redundancy or using proper maintenance actions can arise from study like the one reported in this paper.

Another possible extension of the present study, is performing systematic analyses to identify the most critical items and issues to focus on when it will be necessary to define technical critera for future RPAS airworthiness certification.

References

1. European Commission Staff Working Document, *Impact assessment* (Brussel, 2015)
2. International Civil Aviation Organization (ICAO), *Circular no. 328/AN 190 Unmanned Aircraft Systems* (ICAO, 2011)
3. B. J. de Oliveira Martins Franco, L. C. Sandoval Góes, *Failure analysis methods in Unmanned Aerial Vehicles*, (Proceedings of COBEM 2007, 19th International Congress of Mechanical Engineering, © 2007 by ABCM)
4. *Military Standard 1629 Rev. A*, (United States of America, Department of Defence, 1980)
5. J. Reason, *Human Error* (Cambridge University Press, 1990)
6. *Military Handbook 338 Rev. B* (United States of America, Department of Defence 1998)
7. B. Syd Ali, W. Ochieng, A. Majumdar, W. Schuster, T. K. Chiew, *ADS-B failure mode and models* (The Journal of Navigation, 67, 995–1017. © The Royal Institute of Navigation, 2014)
8. B. Syd Ali, W. Ochieng, A. Majumdar, *ADS-B probabilistic safety assessment* (The Journal of Navigation, pages 1, 20. © The Royal Institute of Navigation, 2017)
9. Single European Sky ATM Research Joint Undertaking (SESAR JU). *Demonstrating RPAS Integration in the European Aviation System A Summary of SESAR Drone Demonstration Projects Results* (SESAR Joint Undertaking, Bruxelles, Belgium, 2016; pp. 1–28)
10. Centro Italiano Ricerche Aerospaziali (CIRA). *SESAR Joint Undertaking RPAS 0.3 RAID Demonstration Report* (1st ed., SESAR Joint Undertaking, Bruxelles, Belgium, 2016, pp. 1–156)