Risk Analysis of the Future Implementation of a
Safety Management System for Multiple RPAS Based

electronics

MDPI

Article

Risk Analysis of the Future Implementation of a Safety Management System for Multiple RPAS Based on First Demonstration Flights

Francesco Grimaccia [1,2,*], Federica Bonfante [3,*], Manuela Battipede [3], Paolo Maggiore [3] and Edoardo Filippone [4]

1 Energy Department, Politecnico di Milano, Via La Masa 24, 20156 Milan, Italy
2 Nimbus Srl, Via Bertola Poligono 19, 10040 Turin, Italy
3 Department of Mechanical and Aerospace Engineering, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Turin, Italy; manuela.battipede@polito.it (M.B.); paolo.maggiore@polito.it (P.M.)
4 Centro Italiano Ricerche Aerospaziali (CIRA), Via Maiorise 1, 81043 Capua, Italy; E.Filippone@cira.it (E.F.)
* Correspondence: francesco.grimaccia@polimi.it (F.G.); federica.bonfante@polito.it (F.B.)

Academic Editor: Sergio Montenegro
Received: 12 May 2017; Accepted: 21 June 2017; Published: 5 July 2017

Abstract: The modern aeronautical scenario has welcomed the massive diffusion of new key elements, including the Remote Piloted Aircraft Systems (RPAS), initially used for military purposes only. The current decade has seen RPAS ready to become a new airspace user in a large variety of civilian applications. Although RPAS can currently only be flown into segregated airspaces, due to national and international Flight Aviation Authorities' (FAAs) constraints, they represent a remarkable potential growth in terms of development and economic investments for aviation. Full RPAS development will only happen when flight into non-segregated airspaces is authorized, as for manned civil and military aircraft. The preliminary requirement for disclosing the airspace to RPAS is the implementation of an ad hoc Safety Management System (SMS), as prescribed by ICAO, for every aeronautical operator. This issue arises in the context of the ongoing restructuring of airspaces management, according to SESAR-JU in Europe and NextGen in the USA (SESAR-JU has defined how RPAS research should be conducted in SESAR 2020, all in accordance with the 2015 European ATM Master Plan). This paper provides the basis to implement a risk model and general procedures/methodologies to investigate RPAS safety, according to the operational scenarios defined by EASA (European Aviation Safety Agency). The study is based on results achieved by multiple-RPAS experimental flights, performed within the RAID (RPAS-ATM Integration Demonstration) project.

Keywords: RPAS; non-segregated airspaces; UAV integration; SMS

1. Introduction

According to Circular number 328 issued by the International Civil Aviation Organization (ICAO) [1], an Unmanned Aircraft System, or UAS, sometimes called also "drone", is an aircraft without a human being (pilot) on board.

A UAS can be fully autonomous or remotely piloted by a human being operating it from a ground station, using a HMI to command and control the aircraft and a ground or satellite radio datalink (up/downlink) to convey the control signals and download the flight data: this last category of UAS, defined as Remotely Piloted Aircraft Systems (RPAS) by the aforementioned ICAO Circular, is the main object of this paper, according to Article number 8 of the Chicago Convention. Fully autonomous UAS are not subject to ICAO documentation and so will not be considered in this paper.

Among the military pioneers of RPAS, the United States Air Force and the Israeli Air Force have been the leading actors. Nowadays most Western air forces are equipped with RPAS. Military groups

have acknowledged the flexibility and effectiveness of the RPAS in accomplishing the following duties [2]:

- Surveillance over land and sea with extended endurance (fly time up to 24 hours);
- Accurate reconnaissance on selected targets even if located deep in hostile areas;
- Real-time acquisition and transfer of images and videos to the ground station and/or to the analysis post (data exploitation);
- Employment even within crisis/conflict scenarios;
- Deployment for surveillance and recognition tasks during crisis events not requiring the same level of resources needed for deploying traditional manned aircraft;
- Because of aircrew absence, easier governmental authorization to perform risky operations preventing any crew from being captured in the operational theatre;
- Overall high flexibility due to the simple architecture of ground segment of the RPAS, including the modularity and scalability of mission sensors (payload);
- Low cost profile, given the absence of crew.

Besides ISR (Intelligence Surveillance Reconnaissance) purposes, RPAS clearly ensures flexible employment as it could help with crisis management such as immigration monitoring, antipiracy efforts, or civil protection during earthquakes, floods, landslides, and large forest and vegetal fires. In fact, RPAS are usually intended to be used in case of "Dull, Dangerous and Dirty" (3D) missions [3].

For civil applications, RPAS activities are strongly supported by the European Aviation Safety Agency (EASA), which is encouraging the development of civil unmanned systems in order to promote a new growing market in Europe and to better safeguard the human operators involved in aerial work. In particular, according to [3], the expectations are significant: from 2006 to 2014, 146 fatalities occurred in aerial work, involving both fixed and rotary wing aircraft. Fatalities are expected to decrease proportional to the replacement of conventional manned aircraft with unmanned aircraft, per single aerial operation.

For RPAS civil applications in Europe, regulations are currently under the EASA responsibility for unmanned aircraft with a maximum take-off weight over 150 kg, and it is left to the National Civil Aviation Authorities (for example, ENAC in Italy [4]) for RPAS with maximum take-off weight under 150 kg. According to these regulations, UAS could be employed within two main aerial domains: scientific research and development purposes, or specialized commercial operations. Specialized operations include all the activities of "aerial surveys", such as video and photo shooting, aerial examination of buildings and infrastructure (bridges, railways, and motorways), surveillance as well as search and rescue operations. In both cases, safety issues are inherent to the operation of a single RPAS [4] or, on a larger scale, to the integration of RPAS into civil airspaces [5–11]. Meanwhile, the current manned aviation scenario is envisaging a change in the airspace management, to increase capacity while preserving the safety of operations.

This study aims at describing the new hazards introduced by RPAS entering the current manned aviation scenario. In this paper, this issue is firstly described from the ICAO perspective, then from the SESAR JU Program point of view, which focuses on the European situation. Within the SESAR JU research demo projects, aimed at investigating issues related to RPAS integration into non-segregated airspaces, attention is focused in particular on the RAID (RPAS-ATM Integration Demonstration [12]) program, developed in Italy under the leadership of CIRA, the National R&D aeronautical research center. During RAID experimental activities (composed of both computer simulations and real flight tests), in fact, several concerns emerged about the integration of RPAS into non-segregated airspaces. The risk analysis presented in this paper, thus, was developed by processing the RAID results, to foster future implementation of a Safety Management System for multiple RPAS.

As far as the Safety Management System is concerned, the international situation is not yet uniform: worldwide, recent ICAO recommendations encourage the adoption of the Safety Management System even for RPAS operators, to deal with a totally new concept of airspaces

operations and traffic management. In Europe, the European Aviation Safety Agency (EASA) is working to develop "operation-centric" requirements to merge RPAS aerial operations into future non-segregated skies. Such requirements will be scaled to low, medium or high levels of safety risk, according to the considered RPAS operational flight scenario. This twofold vision on how to address the safety problem, namely the adoption of a Safety Management System even for RPAS operators and the RPAS operation-centric safety risk requirement, suggested the basic ideas described in this paper: to implement a risk model, as well as a general procedure/methodology to investigate RPAS safety aspects, prior to operating in manned airspaces in the future. The definition of an ad hoc taxonomy for RPAS casualties, already existing for manned aviation, represents the ideal follow-up content for the study described in this paper, starting from the first experimental flights.

This paper is structured as follows: Section 2 initially focuses on ICAO (Section 2.1) as well as European SESAR JU and EASA (Section 2.2) directives for future civil airspaces; then it describes safety issues that emerged from the performed experimental activities for the SESAR JU RAID demo project (Section 2.3); finally, it introduces the concept of a Safety Management System in aviation (Section 2.4), in accordance with recent new ICAO recommendations for all aeronautical operators (RPAS ones included). Section 3 describes the concept of the risk model and procedures/methodologies to evaluate RPAS safety in non-segregated airspaces. Section 4 contains a discussion of the possible future development of the present study. Finally, Section 5 sums up the conclusions related to the topics presented in this article.

2. Air Traffic System Management: The New ICAO Concept of Operations and the Integration of RPAS into Non-Segregated Airspaces. The Safety Management System.

2.1. ICAO New Concept of Airspaces and Traffic Management

The International Civil Aviation Administration (ICAO) is the body of the United Nations that, since 1944, has supported the growth of civil aviation, focusing on the safe operation of aircraft in the airspace. Worldwide, all the aviation organization/authorities, primarily ICAO, together with research centers and industries, are trying to identify the new difficulties involved in the integration of RPAS into the airspace with manned traffic. The general requirement is that the introduction of RPAS among traditional aircraft shall not affect the flight safety, performance, and security achieved by manned aviation. Assuming that ICAO considers RPAS as aircraft, their behavior must be compliant with the General Air rules [13,14]: Operatively, for example, RPAS must be able to fly under VFR or IFR conditions, respecting the rules foreseen in every airspace class where RPASs are flying, as well as interacting with Air Traffic Control (ATC) entities, without requiring sudden changes in the current procedures. Nevertheless, RPASs differ from manned aircraft in at least two peculiarities: the pilot is not on board, because s/he remotely controls the vehicle operating from a ground station; and the remote pilot uses a Command and Control (C2) Data Link to perform his/her tasks, sending commands to the aircraft in uplink and receiving and monitoring data telemetry in downlink. The abovementioned differences between RPAS and manned aircraft are major challenges for the safe integration of unmanned platforms into non-segregated airspaces. The regulation framework written for manned aircraft needs to be reviewed and adapted to RPAS, bearing in mind the aforementioned peculiarities. Certification rules and assessments, ground and flight test programs, a new airworthiness concept, certificates of airworthiness, types certificates, and maintenance programs to maintain the airworthiness and flight logs managed by the national aviation authorities are examples of formal aspects that need to be re-defined for RPAS.

There is one more element to be considered: RPAS are entering current airspaces, which are changing in terms of new concepts of operations as per [13], planned to be effective as of 2025. In fact, due to the increase in volume of actual manned traffic, current ATM limitations lead to an inefficient usage of airspaces and related ATM resources. The new ATM layout will be designed to be more efficient, global, cost-effective, and flexible. Moreover, it will be fully integrated and cooperative. The so-called Global Airspace Traffic Management (GATM) will act as the provider of centralized services under a common sky arranged and managed in such a way as to use the available airspace more

intensively and increase flight safety awareness. For example, in Europe the airspace will no longer be divided into blocks according to national boundaries, but according to the effective volumes of traffic instead. Operatively, the ATM will monitor the flight trajectory of each aircraft throughout all of the flight phases. ATM service will consist of supervising the interactions between each single trajectory, as well as the hazards, in order to achieve the optimum system outcome, with minimal deviation from the user-requested flight trajectory, whenever possible, aiming at enhancing flight safety as well. The new global concept of ATM will be scalable and adaptable to the specific needs of each state, balancing demand and capacity. Each flight will be seen as a form of efficient handling of traffic from gate to gate. Hazards like other aircraft, terrain, weather, wake turbulence, incompatible airspace activity, up-to-date aeronautical data (NOTAMs), and ground vehicles will be faced by making use of conflict management techniques in order to avoid collisions and maintain safe and orderly traffic from the flight planning phase onwards. ATM will be requested to satisfy the following issues: safe separation minima, on-time ATM services delivery, traffic capacity balancing and synchronization, information management, quality and meteorological data provision, services in the air and on the ground, the flexibility of the system, coordination capacity, human performance, automated functions, and navigational services compliant with environmental requirements.

In this scenario of progressive optimization within airspace management, duplication of ATM functions between air and ground operations will be removed; accurate planning at the global, national, and regional level will allow for risk prevention (for instance, pilots not aware about valid NOTAMS).

Migration from legacy to new technologies will ensure an unchanged level of safety as minimum requirements will be either maintained or enhanced: the use of airspace within a full self-separation and automatic collision avoidance context will be encouraged, prescribing the integration of Automatic Dependent Surveillance–Broadcast (ADS–B) devices providing geopositioning based on satellite assistance rather than traditional ground RADAR assistance (Identification Friend or Foe-IFF).

The resulting airspace organization and management will be more flexible and increasingly tactical in application: users of the airspace will be pragmatically identified by means of their specific requirements. Use of dynamic 4D trajectory systems will be common.

Uncontrollable and unpredictable events against ATM like weather and natural phenomena, including lines of thunderstorms, standing waves and clear air turbulence, snow on runways, volcanic ash, and so on, will continue to have significant consequences for user operations, but they will be considered as a deviation of the aircraft compared to the predicted trajectory and properly managed as hazards.

In this new environment, ATM will also be able to accommodate new users in the airspace such as RPAS and space transiting vehicles, this last not being the object of this paper.

2.2. Single European Sky Air Traffic Management Research Program (SESAR1/SESAR2020)

Worldwide, two important ATM research programs are in progress: The Single European Sky Air Traffic Management Research Program (SESAR2020—SESAR1 was the first program of SESAR and it was run from 2008 to 2016. SESAR 2020 will be in progress for the next six years), in Europe, under the sponsorship of the European Union (EU) and Eurocontrol, and the NextGen Research Program, in the United States of America, led by the Federal Aviation Administration (FAA). SESAR was launched in 2004 to define, develop, and implement, from a technological perspective, what was needed in order to increase the Air Traffic Management (ATM) performance, with the final purpose of building a new European intelligent air transport system, able to increase the airspace capacity while reducing costs for users (It was calculated that the average cost for transporting U.S. passengers was almost half of the average cost for Europe.).

In 2007, with an official endorsement of the European Council, the SESAR Joint Undertaking (SESAR JU) was established as a public–private partnership. SESAR JU has been working, since 2007, at modernizing the European Air Traffic Management system by coordinating and concentrating all ATM-relevant research and innovation efforts in the European Union (EU). Operatively, SESAR JU

is actively working to safely integrate RPAS into non-segregated airspaces [15,16] to foster their development and diffusion in Europe.

With reference to RPAS regulations, the European aviation community, through SESAR JU and EASA initiatives, is pushing to write a common regulation for RPAS to ensure uniformity of procedures among nations in terms of flexibility and safety for future daily commercial operations with manned and unmanned operators flying together in the common airspace. Standardized regulations will also be the key for the solid development of the RPAS market, especially in Europe [3]. From this perspective, SESAR1 has been working to set these new regulations in Europe. Related research activity has been ongoing since 2012 throughout different RPAS demonstration projects [17]: AIRICA, ARIADNA, CLAIRE, DEMORPAS, INSuRE, MedALE, ODREA, RAID, and TEMPAREIS.

Some important general indications coming from the abovementioned experiments can be summarized as follows:

- A solid regulation and certification framework shall be implemented by European and national aviation authorities;
- New appropriate policies and procedures shall be defined to create an RPAS systems interface with ATC, maintaining/enhancing the current level of safety in daily flight operations;
- Reliable and safe Detect and Avoid capabilities shall be embedded on RPAS systems (on board the air segment or inside the ground station);
- A reliable and safe C2 (Command and Control) datalink shall be implemented together with spectrum protection techniques/devices;
- Specific training plans and certification procedures shall be defined for accrediting remote pilots.

The present work relies extensively on data collected through the large experimental activity, consisting of 50 flight simulations and 12 flight tests, conducted within the RAID [12,18] program, a project co-financed by the SESAR JU and started in 2013.

2.3. The RAID Demonstration Project: Test Design, Experimental Results, and Recommendations

Perfectly fulfilling the general intents of SESAR Program, the RAID [12,18] demonstration project aimed at testing the limits of the current air traffic system concept of operations and practices when introducing, into non-segregated airspaces, RPAS equipped with Automatic Dependent Surveillance–Broadcast (ADS-B) devices. ADS-B was one of the main foci of RAID. By 2020, in fact, all aircraft will have to be equipped with ADS-B devices, which will replace the traditional airborne transponder (IFF), as requested by the ICAO Asia/Pacific Air Navigation Planning and Implementation Regional Work Group in 2003 [19,20]. During the 11th ICAO Navigation Conference [19], it was recognized that ADS-B, as future ATM equipment [13], could be the enabler of a new concept of operations for traffic volume optimization. Potentially, ADS-B can be used in any kind of environment or operation because of its own embedded features; it can also easily support surveillance of airspaces where other sensors (e.g. RADAR) are unavailable or cannot be used. ADS-B devices have the capability of enabling the Air Traffic Controller to monitor aircraft position in real time, which is a great improvement compared to the current situation, for which, in some areas, only voice position reports are available. Indeed, in a future scenario, featuring the massive employment of ADS-B, voice communication will continue to be used in support of ADS-B position reports. Current ATM ground sensors with their coverage limitations (RADAR) and practices will be replaced by satellite surveillance procedures and ADS-B devices. The latter have reached a technology readiness level and maturity that perfectly fit with the new concept of operations foreseen in [13,21]. This future operational scenario, with a growing number of civil RPAS being integrated, will allow us to reach the expected commercial forecasts.

The SESAR solution, from a technical perspective, consists of the ADS-B ground station and the Surveillance Data Processing and Distribution (SDPD) functionalities [21]. It has to be noted, that ADS-B implementation assures proper mitigation against deliberate spoofing of the ground system by external agents.

The RAID demonstration program is described to explain the operational criticalities that shall be solved to integrate RPAS into non-segregated airspaces.

The main aim of RAID was to evaluate what kind of issues could arise when integrating RPAS with manned aircraft sharing the same airspace and to explore limitations of current ATM infrastructures and management. From this operational point of view, human performance, safety, and security were evaluated and experimentally assessed/measured, generating results and recommendations for further testing activities.

All experimental activities were managed, conducted, and coordinated by the CIRA center located in Capua (Naples, Italy), with the flight test area located between two airports: the Grazzanise Airport and Capua Airport.

Figure 1 [18] shows the whole experimental system.

The integration of RPAS with manned aircraft was tested using the flying objects as follows. A FLARE Optionally Piloted Vehicle (OPV), namely a TECNAM P92 VLA aircraft completely set up by CIRA, was used under RPAS configuration (remotely piloted); FLARE OPV was authorized by ENAC to operate through a temporary Permit to Fly (PtF) for experimental purposes. At the same time a hexa-rotor mini-RPAS PPL 612, provided by the Italian Nimbus srl, was used as an unmanned intruder. PPL 612 was authorized by ENAC to operate through a temporary Permit to Fly (PtF) for experimental purposes. Finally, a storm RG CS Very Light Aircraft (VLA), provided by a third party, was used as a cooperative manned traffic/intruder in the airspace; RG CS VLA was authorized by ENAC to operate through a certificate of airworthiness.

The OPV is defined in accordance with Federal Aviation Administration (FAA) Order 8130.34A as an aircraft equipped with a flight control system that allows modifications to flight controls that enable the aircraft to be remotely piloted (outside the cockpit), either by a remote flight operator or by the on-board flight control system itself; OPV also includes an onboard safety pilot who can override the flight control system in the case of malfunction or any other hazardous situation. The FLARE OPV system consisted of two manual piloting modes: direct or augmented, by mean of a stability control and augmentation module; in both cases the autopilot was available to provide indications to the pilot by input of the flight director or by direct feeding of the mobile surface actuator. Each of the above aircraft was equipped with an ADS-B OUT device. FLARE OPV was also equipped with an ADS-B IN device for the management of the Detect and Avoid functions to be tested. The DAA concept of operation is, in fact, based on the interaction between the RPAS equipped with an ADS-B IN and surrounding air traffic, equipped with ADS-B OUT devices.

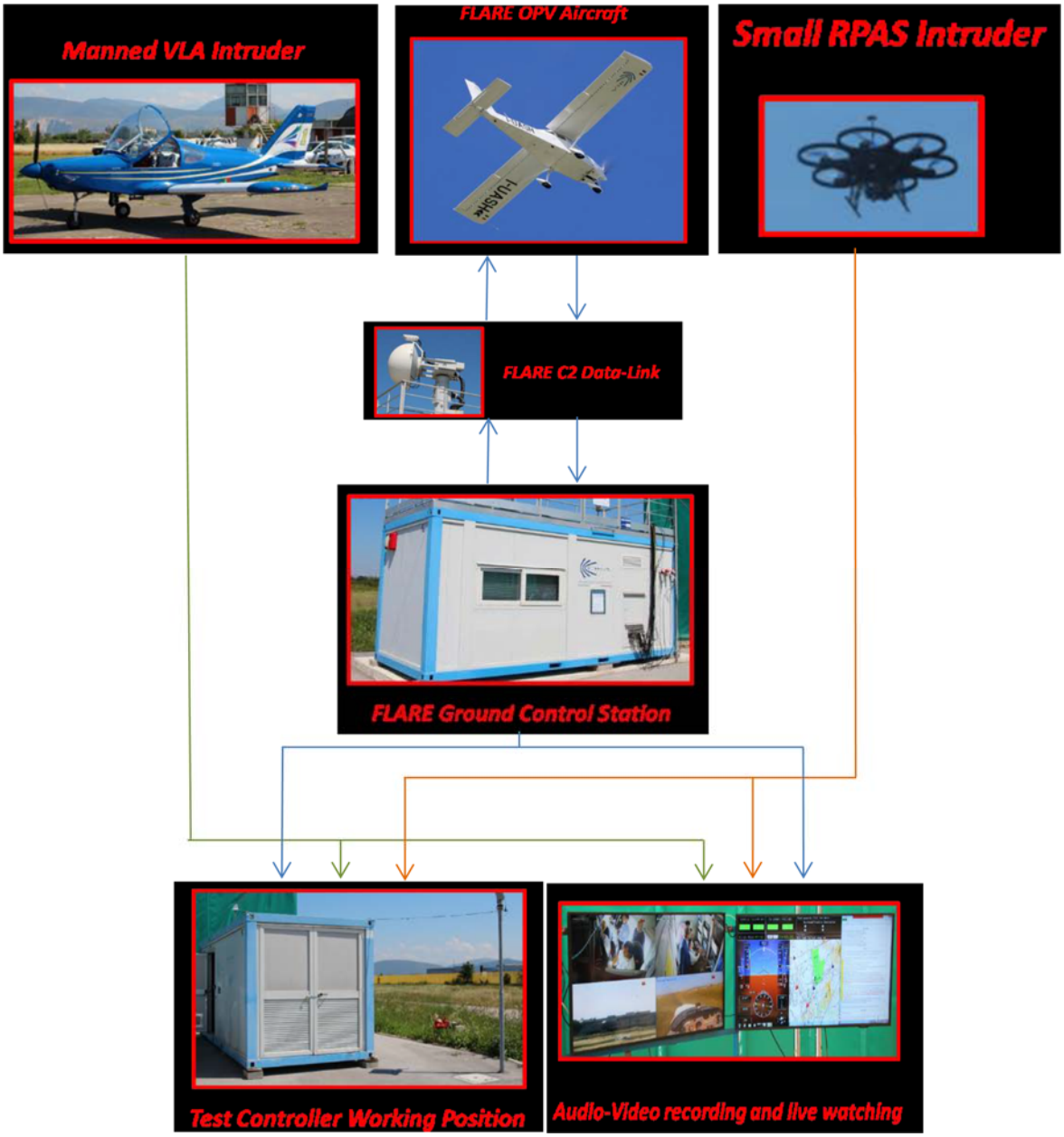


Figure 1. RAID test bed architecture (from [18]); Contains public sector information licensed under the Open Government Licence v3.0, see [22].

Additionally, the RAID flight facilities architecture consisted of:

- A FLARE C2 Datalink (a full duplex communication link in S-band piloted by a directive antenna ranging up to 20 km);
- A FLARE Ground Control Station, able to replay the datalink and the ground segment subsystems architectures of an RPAS when the OPV was used as Remotely Piloted Aircraft System;
- An audio/video recording and live watching facility;
- A test controller working position.

RAID testing activities were mainly focused on evaluating:

- The impact of new concept of operations on the existing framework and feasibility about consequent changes; this aspect was assessed considering remote pilots' and air traffic controllers' (ATC) acceptability on this item;

- The impact of a new concept of operations and consequent changes on remote pilots, ATCOs, and their level of acceptability; this aspect was assessed evaluating situational awareness, error propensity, workload, and timeliness of undertaken actions;
- The impact of the usage of automated systems on existing context: this aspect was assessed by evaluating the consistency of automation, the human workload, the situational awareness, the trustiness of the automated system, and the timeliness of actions;
- Performance of Detect and Avoid (DAA) system: this aspect was assessed evaluating its accuracy, effectiveness, and timeliness based on the data/information provided;
- Performance of ATC Controllers operating with unmanned intruders: This aspect was assessed taking into account the communication load, effectiveness, timeliness, general situational awareness, and general framework acceptability.

The new technology under examination, the Detect and Avoid (DAA) system (Figure 2) [18], was tested during both real-time simulations and flight tests. DAA is considered crucial for the integration of RPAS into the manned airspace as it is the only means of providing the aircraft with an acceptable degree of situation awareness in the absence of a pilot on board.

A DAA system is designed to:

- Provide situational awareness to the remote pilot by showing an integrated overall traffic picture based on the elaboration of signals received from ADS-B equipment that is installed on the other aircraft;
- Provide self-separation to the RPAS in case of a missed separation related to a specified horizon; it indicates the suggested maneuver to restore the separation minima among the involved assets. A remote pilot can either accept the proposed maneuver by implementing it in manual mode or by letting the autopilot to automatically implement it;
- Provide collision avoidance functionalities in order to identify the preliminary conditions triggering a collision over a given time horizon, then provide the proper maneuver to avoid it.

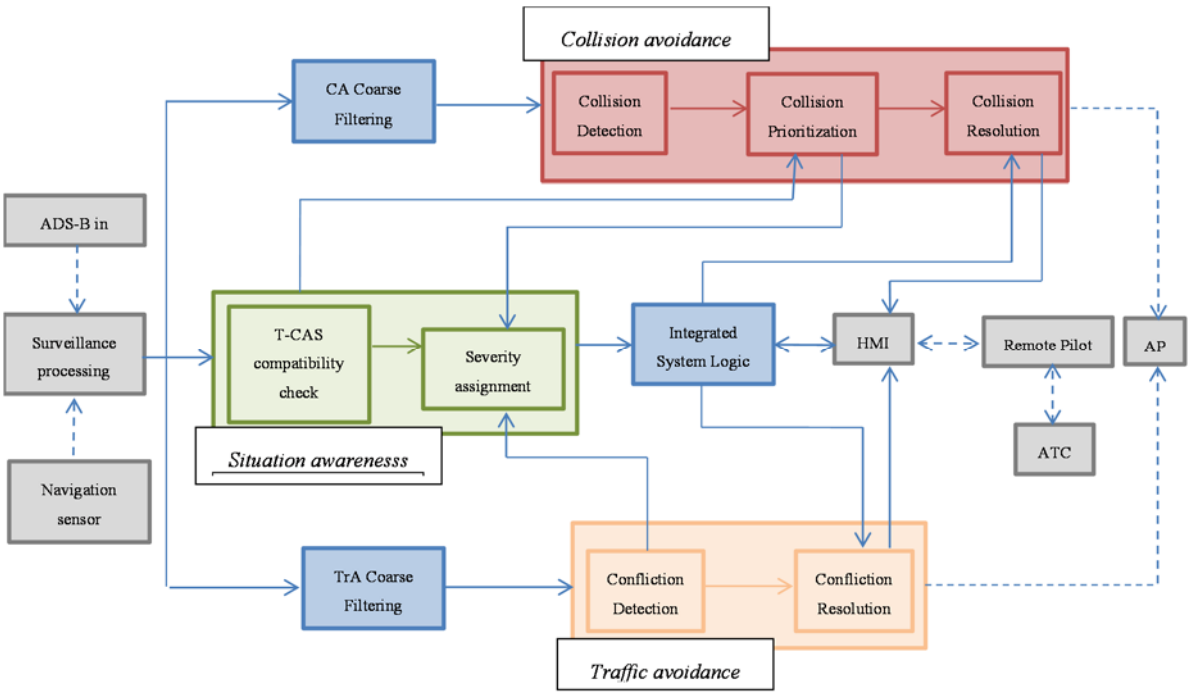


Figure 2. Overall DAA system functional architecture tested during RAID flight sorties (from [18]); it contains public sector information licensed under the Open Government Licence v3.0, see [22].

As shown in Figure 2 [18], the ADS-B interface with the remote pilot cockpit feeds the related data/symbol to the displays; the remote pilot can interact with the DAA system by implementing the abovementioned actions through a proper Human–Machine Interface (HMI) located in the remote station. The DAA equipment is able to predict a loss of separation or a collision according to pre-programmed conditions; moreover, the DAA filters indications to pre-select traffic, suggesting the best separation recovery maneuver for both the aircraft. This concept of operation represents the minimum requirement to be implemented on air platforms to operate in future optimized and shared airspaces, as described by ICAO in [6]. For this reason, ICAO requires that all manned and unmanned aircraft operating in the integrated airspaces shall be ADS-B capable as of 1 January 2020.

RAID experimental exercises were arranged purposely to simulate and test this navigation requirement in flight. Furthermore, the robustness of unmanned platforms against GPS spoofing was also tested and verified. GPS spoofing is an intentional contamination of GPS signals with false navigation data. In RAID tests, the spoofing attack was simulated through an eastwards effect that alters the heading: Information about a false deviation is sent to the autopilot and displayed to the remote pilot (who is not alerted of the attack), while the real aircraft heading remains unchanged.

With reference to the Air Traffic Controllers (ATC), during operational activity they communicated with remote pilots on the ground (and with onboard pilots only for safety reasons) using VHF radios. All experimental activities, both computer simulations and flight tests, were coordinated via radio by the Flight Conductor/Flight Director from the Controller Working Position (CWP) located in the FLARE Ground Control Station. The flight scenario was the Grazzanise CTR (Control Zone) around the Capua Civil Airport (Naples, Italy), (ICAO indicator: "LIAU"; ICAO code: "2A"). The mentioned CTR airspace was Class G, which means "Not Controlled Airspace," but RAID sorties simulated IFR flights, namely flights operated in classes of airspaces where separation is under ATC responsibility only (Figure 3, [18]).

Figure 3. Flight test area with effective operative area (inside) (from [18]); it contains public sector information licensed under the Open Government Licence v3.0, see [22].

All experimental activities were only executed with positive Visual Meteorological Conditions (VMCs) due to safety reasons. Minimum altitude was established at 1500 ft above medium sea level (AMSL), while the top altitude was set at 8200 ft AMSL.

All the experimental activities were executed in the timeframe from 27 April to 6 May 2016. Each flight was dedicated to verify specific aspects related to the concept of operation under testing. With reference to safety items, RAID flights can be arranged as in Table 1.

Table 1. RAID flight sorties: Hazards (data from [18]); it contains public sector information licensed under the Open Government Licence v3.0, see [22].

Light	Traffic	FLARE in RPAS mode (ime window)	Hazards				
			DAA/ADS-B system failure	2 link system failure	Limitation in human performances	Weather and terrain on DAA and C2 link systems	Loss of GNSS, DAA and C2 Link systems
1	FLARE A/C only	41′	-	-	x	-	-
2	FLARE A/C only	22′	-	-	x	-	-
3	FLARE A/C only	33′	-	-	x	x	x
4	FLARE A/C & Mini RPAS	24′	-	-	x	-	-
5	FLARE A/C & manned VLA	7′	-	-	x	-	-
6	FLARE A/C & manned VLA	20′	-	-	x	-	-
7	FLARE A/C only	27′	-	-	x	x	x
8	FLARE A/C & manned VLA	25′	-	-	x	x	x
9	FLARE A/C & manned VLA	29′	x	x	x	x	x
10	FLARE A/C & manned VLA	31′	x	x	x	x	x
11	FLARE A/C & manned VLA	6′	x	x	x	x	x
12	FLARE A/C only	20′	x	x	x	x	x

Test results were collected in terms of direct observations, post-flight questionnaires, debriefing sessions, flight test reports, and recorded data. RAID experimental activity has been described in this article as a solid basis to show some typologies of hazards that shall be taken into account when investigating the integration of multiple RPAS into unsegregated manned airspaces:

- RPAS DAA/ADS-B system failure: Risk of collision (such as mid-air collisions with other aircraft or site crashing);
- C2 Link system failure: Likely loss of control of RPAS units; risk of collision (such as mid-air collisions with other aircraft or site crashing);
- Human performance referred to ATC controller with high workload situations: Risk of error, risk of collisions;
- Human performance referred to remote pilots with high workload case: Risk of error, risk of collisions;
- External factors: Emergency/contingency procedures; effects of DAA recovery maneuvers;

- Jamming and spoofing (not simultaneously performed): Effects on safety, especially in the case of DAA equipment failure.

It is important to notice that adverse weather conditions and profile terrain usually represent possible hazards for RPAS integration into non-segregated airspaces, but, as already mentioned, RAID flight activity has been executed under VMC conditions and at remarkable altitude for safety reasons. With regards to the DAA systems, two elements/cases should be considered as relevant within the flight safety domain: On the one hand, although maneuvers are automatically suggested by DAA, they might not be implemented/executed in a timely manner by the remote pilot; on the other hand, it might be that the remote pilot has initiated an avoidance maneuver without receiving the proper ATC clearance. In both cases, these facts can create disappointment among ATC personnel, leaving the sensation of a lack of situational awareness.

Finally, in specific airspace classes, VFR flights also have to follow ATC instructions; VFR flight rules were developed years ago, when VMC parameters were referred to the visual eye of pilots, whereas RPAS platforms might be equipped with visuals/optics more advanced than human eyes in terms of longer distance and wider field of view. This aspect, again, could generate ATC personnel disappointment in terms of a lack of situational awareness.

Results of RAID exercises shall be globally considered successful, despite the following constraints. Just a few participants were involved in the experimental activity: the FLARE and one or two intruders; the ATM environment consists of a number of flying assets/platforms managed by ATC controllers. This limitation required the use of a qualitative approach to human machine performance evaluation. Each critical combination of events, put to the test during the flight activity, was executed by informing the pilots/remote pilots and ATC controllers in advance. Although this measure safeguarded the flight safety of the experimental activity, it has minimized the workload of ATC and pilots, making the test results indicative of achievement. Finally, no physiological data have been collected with remote pilot and ATC controllers; the results derive just from self-reported post-flight evaluations.

The following considerations support the importance of collecting and validating each result that is expected to be used as a solid basis for further investigations on hazard analysis, related to RPAS operations into non-segregated manned airspaces:

- Human machine performance was evaluated according to Eurocontrol Human Factor Case Guidance specifications;
- Pilots, remote pilots, and ATC controllers were professional and highly skilled/trained;
- The remote pilot, flight director, safety pilot, and most of the relevant stakeholders participated in the post-flight debriefings in order to capture/consider all of the data/results from each point of view (lessons learned);
- The Controller Working Position (CWP), used during the experimental activity, was implemented according to the inputs received from the ATC controllers, being compliant with the design requirements and adherent to real ATC controllers' working positions;
- ATC controllers were in direct communication with the FLARE remote pilot and the other flying platforms via VHF radio; however, the CWP could also supervise the air traffic equipped with ADS-B equipment, flying near the flight test area;
- New technologies such as ADS-B devices were tested within a step approach to achieve realistic scenarios.

2.4. The Concept of Safety Management System in Aviation and the New ICAO Prescriptions for All Worldwide Aeronautical Operators

In Southern Afghanistan, on 2 September 2006, a NIMROD (tail number XV230), a Maritime Reconnaissance aircraft of the British Royal Air Force (RAF) (see Figure 4), after performing an Air-To-Air Refueling during a routine mission, suffered an in-flight fire that led to the aircraft's loss and consequent crew deaths.

Figure 4. RAF NIMROD XV230 aircraft (from [23]).

A dedicated Board of Investigation was established in order to identify the cause of this catastrophic incident. A detailed report was issued in 2009 [24]. The following items were identified as the root causes of the incident: A fuel escape occurred during the air-to-air refueling phase; there was an overflow from the blow-off valve towards the fuel tank that caused fuel to track back along the fuselage. Consequently, a fuel leak from the fuel system (fuel coupling or pipe) caused an accumulation of fuel within the fuel tank dry bay No. 7. Although probable, the fuel leak might have been caused by a hot air leakage that damaged the fuel system seals; the ignition of that fuel was probably initiated at contact with an exposed element of the aircraft: The Cross-Feed/Supplementary Cooling Pack (SCP) duct.

Followup investigations identified mistakes and carelessness in performing the safety analysis; further organizational problems and gaps were discovered. Focusing on safety analysis, the following items were recognized: The company committed to executing such a study, BAE Systems, had labeled 40% of the hazards as "Open" and 30% of them as "Unclassified." Globally, safety documentation review, error analysis, and risk categorizations were accomplished. However, they issued vague recommendations such as "further work is required" in most cases, failing to provide useful recommendations, lessons learned, or procedures. The aforementioned catastrophic fire, corresponding in the safety analysis to Hazard H73, was caused by the Cross-Feed/Supplementary Cooling Pack duct; that issue was one of those assessed by BAE as "Open" or "Unclassified." Many concerns were raised about BAE and its ethical principles during the investigation. With reference to organizational problems or gaps, many concerns arose around the Ministry of Defense (MoD)'s in-service support and airworthiness bureau for defense equipment and RAF aircraft during the years prior to the loss of NIMROD XV230. New efforts towards a safety culture arose from this baleful event. This event helps us to understand some basic elements of modern aviation and the related safety culture: The hazard/risk analysis and organizational issues.

These key points represent the fundamentals of the Safety Management System (SMS) as it is implemented in aviation. Flight safety is paramount in the aeronautical context; without a doubt, it is the primary requirement for aviation. Although human activities lead to risk, which cannot be completely removed, it can at least be properly mitigated. This concept is fully applicable in the aviation context. Risk mitigation is a seamless activity: From an operational perspective, risk mitigation is a daily activity in aviation, both in civil [25] and military applications [26,27]. So, risk mitigation can be intended as a dynamic process and effectively an open matter. Safety is the condition when probabilities of harming people, or damaging property, is reduced and maintained at or below an acceptable level; it is ensured through a continuous process of hazard identification and safety risk management. Safety is a property of the system, not of its single components. In the case of aviation, the system (composed of the aircraft, the aircrew, the ATC personnel and infrastructure, etc.) can be classified as a complex system [28]. This definition influences the methodology that must be used to approach aviation safety, distinguishing between traditional and more up-to-date approaches to risk analysis, risk management, and risk mitigation [29].

The literature identifies three main eras in aviation safety evolution, as reported in Figure 5 [30]:

1. A technical era, from the early 1900s to the late 1960s, when aviation developed as a form of mass transportation. In this period, deficiencies in safety were related to technical factors and a lack of technical knowledge;
2. A human factor era, from the late 1960s to the mid-1990s: Improved technology and a wider technical knowledge allowed people to focus on safety issues related to human performance, which still remains a recurrent root cause of incidents: Human–machine interfaces were optimized; electronic systems and onboard computer systems changed the aircraft into a "system of subsystems" and helped the human operator to better perform his tasks. The aforementioned enhancements allowed for a decrease in the crew workload and the associated occurrence of human mistakes;
3. An organizational era, from the mid-1990s to today, when safety is seen from a systematic perspective. Organizational factors are encompassed in the system together with technological and human factors; it is recognized that an organization's culture and policies can have a great impact on safety and risk mitigation. Usually, a safety analysis resulting from data collected about occurred incidents is augmented by a new proactive approach to safety. Proactive and reactive methodologies have been developed to identify precursors of incidents before the incidents have the chance to occur. This new approach has led to the concept of a Safety Management System.

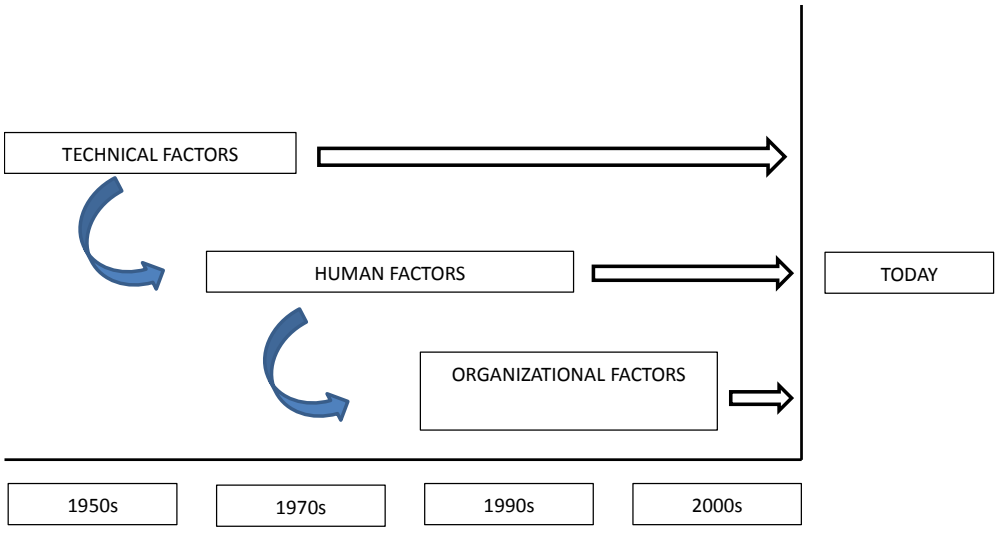


Figure 5. Safety evolution in aviation (from [30]).

Traditional methodologies, based on Newton's and Descartes' approaches, attribute the functioning or nom-functioning of a system to the functioning or non-functioning of its components (the technical era). The failure of a complex system is explained in terms of the failure/breakage of individual components identified as physical or human components [29].

Instead, safety is an emergent property of the system that cannot be foreseen by examining its single components. In fact, an accident can occur even if all components are nominally working [28].

More updated methodologies identify an accident of a technological system as the result of a combination of human and organizational factors that generates a "chain of events" [29] (human factor area and organizational area). It must be noted that human error influences the aviation system both from inside, as aviation systems are built and flown by human beings (from aboard or from the ground, as in the case of RPAS) and from outside, as aviation systems, like any complex technological system, are immersed in an environment made up of human beings whose decisions and actions can condition the system itself.

The aforementioned "chain of events" is what is able to infiltrate through a system's defenses (or controls or mitigation factors [31]), leading to an accident (Figure 6) [30].

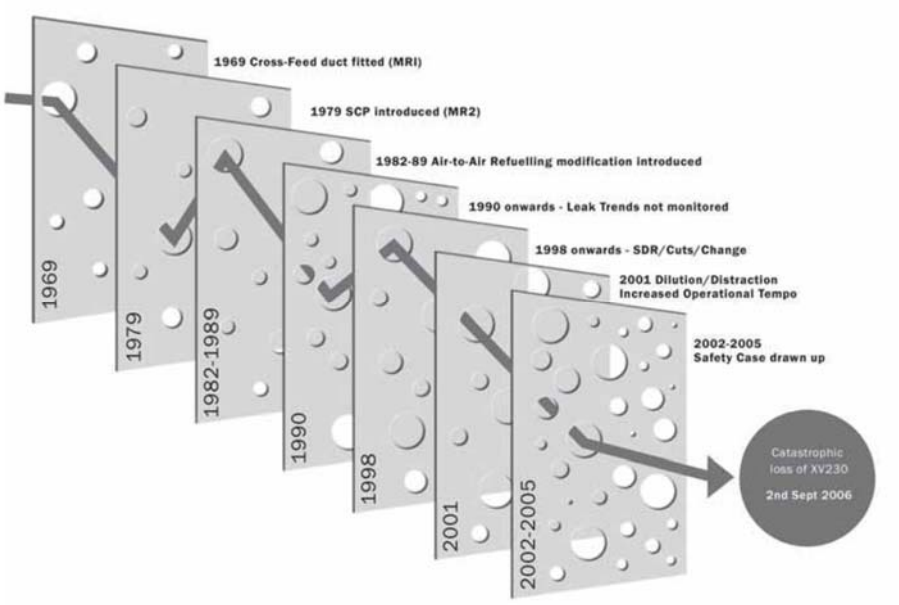


Figure 6. Safety "Swiss Cheese Model" applied to a specific event (from [30]).

Figure 6 [29], applied to the NIMROD aircraft case, represents the "Swiss Cheese Model," a metaphor chosen by Professor James T. Reason (another similar scheme is the "Bow Tie" model) to visualize the delicate plot made of active accident-enabling factors like failure of equipment, human error or violations (a detailed classification of these issues is reported, for example, in [31]), or organizational enabling factors and system defenses.

Organizational safety is the best compromise between financial and safety management (refer to the concept of safety space as stated in [30] (Figure 7).

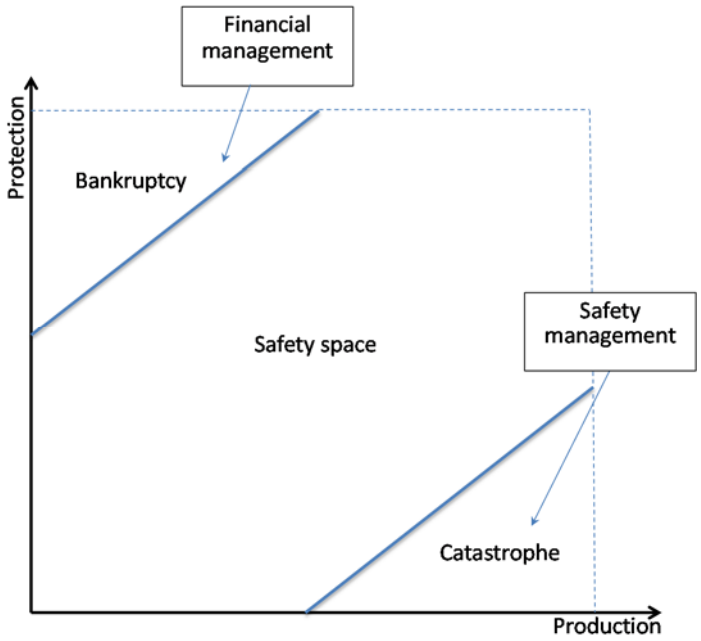


Figure 7. Safety space (from [30]).

Often, changes in an organization might cause problems or incidents. Therefore, in a complex and hazardous sector such as aviation [30], changes must be adequately managed/monitored.

After occurrences such as discussed in [25] or other catastrophic events, the technical community understood and started to implement a real safety culture, consisting of several aspects, the most important one being the so-called "reporting culture" or "just culture" ([32] or even [26,27]). Each safety-related event must be recorded in a database, implemented, for example, by a commercial airline; such data are often sensitive and, in fact, ICAO [30] recommends adopting measures to protect them as such data must be used for safety analysis purposes only. The collected data are filtered according to quality and analyzed in order to identify breaches in the organization. Usually, suitable data for the safety database come from mandatory incident/accident investigation reports, voluntary reporting data, continuing airworthiness reports, operational performance monitoring data, safety risks analyses, audits or safety studies, as well as data from other nations or regional or international investigation organizations [30]. Such data are systematically analyzed to deliver proper safety recommendations to face future incidents [30]).

Focusing now on RPAS, ICAO Annex 19 [33] introduces a conceptual revolution in aviation safety management and responsibility because it places the responsibility for safety at a state level that requires the implementation of an SMS by both service providers and general aviation operators as part of the State Safety Program. Annex 19 prescribes that all of the aforementioned operators/users must implement an SMS, properly tailored to the size and complexity of their organization and the kind of operations usually performed. This recommendation is valid also for RPAS manufactures and operators, as stated in ICAO Document 10019 Manual on Remotely Piloted Aircraft Systems (RPAS) [5], where the SMS is acknowledged to be part of the implementation of a State Safety Program (SSP) for these new users into the aeronautical scenario.

More details are given in Section 7.3.2 of [5], which formally recommends that the RPAS operator has implemented an effective SMS and fully validates our initial statement.

3. Elements of Risk Analysis to Implement a Novel Safety Management System for RPAS

The previous sections described the general context in which RPAS are spreading for civilian applications, in terms of modern airspace's evolving scenario and complex systems' safety issues.

With reference to this challenging context, the present research focuses on the implementation of a Safety Management System tailored to Remotely Piloted Aircraft Systems, with particular attention to the light segment, which is traditionally removed from this kind of tool and analysis.

Considering a real existing and operative light RPAS, issues related to the safety management for these platforms should be considered from multiple points of view, including impacts on national aviation regulation, as interesting outcomes of the research as well.

Beyond the four pillars (safety policy and commitment; safety risks; safety assurance; safety promotion and just culture) supporting the SMS approach for the organizations working with RPAS, the core of this research is focused on safety and risk analysis and a management model, based on the integration of RPAS into non-segregated airspaces.

EASA has proposed a new paradigm (referring to [3,34]), which is based on the operational-centric approach to the integration of RPAS into non-segregated airspaces. The rationale behind this choice is that the natural consequence of RPAS being remotely piloted is that neither a human pilot nor other human beings are on board. Therefore, the seriousness of an accident (even if not catastrophic) is given from the operational scenario only. Basic indications for potential operational scenarios are given by EASA in [3,31]: The level of risk will be considered to build a regulatory framework rather than defining maximum take-off weight or other similar parameters.

Three levels of risks for RPAS operations shall be considered and consequently the related flight authorizations will be defined; EASA is investigating the following issues:

1. "Open" category: Safety will be assured by compliance with operational limitations, and the associated level of risk will be classified as low;
2. "Specific category": The operator is asked to provide a risk assessment together with a list of mitigation initiatives. Flight authorization is released by the proper National Aviation Authority, which can be supported by a qualified entity. The associated level of risk will be classified as medium;
3. "Certified category": Requirements become comparable to those related to manned aviation, overseen by the National Aviation Authorities (NAA) and EASA regulating areas such as licenses, airworthiness, maintenance programs, etc. The associated level of risk will be classified as high.

Although the Safety Management System will be fully implemented on RPAS classified under "Certified category," SMS integration will be even more critical for RPAS categorized as "Specific," because the related operations will occur within non-segregated airspaces. The new concept introduced with the above definitions is that, according to EASA, the RPAS operations categorized as "specific" will undergo certification rather than the RPAS used to perform them. In particular, flight authorization shall be supported by a proper risk assessment for every RPAS operation, executed within a non-segregated airspace. The correspondent risk mitigation will depend on the characteristics/specifications of the involved RPAS. "Specific category" operations include VLL (Very Low Level) operations below 150 m (500 ft) and operations conducted at altitudes between 150 m (500 ft) and Flight Level 600 (effective integration into non-segregated airspace), which are exactly the scenarios of major interest to the growing RPAS business in Europe and abroad.

The EASA agency, in accordance with [34], is providing a set of standard scenarios for the "Specific" category regarding typical RPAS operations.

RPAS risk models and procedures/methodologies, made to investigate the level of safety of RPAS operational scenarios, can be developed as the final result of the RAID research, which takes into account the key aspects and elements (including natural elements) that really impact RPAS real flights and operations. Real safety issues arising from RAID are the starting point to implement a more comprehensive RPAS safety model, which includes human and organizational components of risk analysis.

According to the authors, according to the data gathered from the RAID demo activity, as reported in Table 1 and applying following ICAO suggestions (refer to Tables 2, 3, 4, 5 and 6 [30]), the following final safety risks (Table 7) can be identified.

Thus, the logical process of safety analysis is composed of the following fundamental steps that can be easily mapped to the case of multiple RPAS flying in the same airspace:

- Hazard analysis: A hazard is a condition or an object potentially able to cause injury/death or damage/failure to equipment and systems with consequent partial or total loss of their functionality; the resulting hazard analysis leads us to identify and prioritize the hazards;
- Safety risk identification and prioritization: This phase foresees (from [30]):
    1. The safety risks definition
    2. The calculation of the safety risk probability of occurrence (Table 2)
    3. The definition of safety risk severity (Table 3)
    4. The safety risk assessment (Table 4)
    5. The definition of a safety risk tolerability matrix (Tables 5 and 6)
    6. The definition of safety risk management (Table 7)

Table 2. Safety risk probability [30].

Likelihood	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

Table 3. Safety risk severity adaptable to RPAS [30].

Severity	Meaning	Value
Catastrophic	Equipment destroyed Multiple deaths	5
Hazardous	A large reduction in safety margins, physical distress or a workload such that the operators cannot be relied upon to perform their tasks accurately or completely Serious injury Major equipment damage	4
Major	A significant reduction in safety margins, a reduction in the ability of the operators to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency Serious incident Injury to persons	3
Minor	Nuisance Operating limitations Use of emergency procedures	2
Negligible	Minor incident Few consequences	1

Table 4. Safety risk assessment [30].

Risk probability	Risk severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	1A	1B	1C	1D	1E

Table 5. Safety tolerability risk matrix [30].

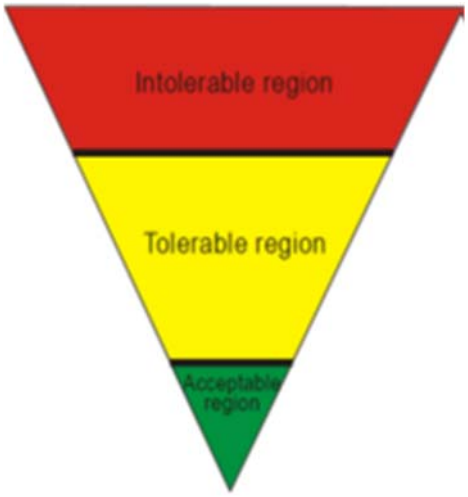
Tolerability description	**Assessed risk index**	**Suggested criteria**
	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Acceptable based on risk mitigation. It may require management decision
	3E, 2E, 1E, 2D, 1D, 1B, 1C,	Acceptable

Table 6. Safety tolerability risk matrix [30].

Risk index range	**Description**	**Recommended action**
5A, 5B, 5C, 4A, 4B, 3A	High risk	Cease or cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional or enhanced preventive controls are put in place to bring down the risk index to the moderate or low range.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable.
3E, 2E, 1E, 2D, 1D, 1B, 1C,	Low risk	Acceptable as is. No further risk mitigation required.

Table 7. RAID demo project flight test activity results: A safety risk identification and prioritization.

Hazard	Risk assessment					
	Safety risk probability	**Safety risk severity**	**Safety risk assessment**	**Tolerability**	**Risk range description**	**Recommended action**
DAA/ADS-B failure	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
C2 link failure	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
Human factor: ATC high workload	Occasional (4)	Hazardous (4 or B)	4B	Unacceptable	High risk	Cease or cut back operation promptly
Human factor: Remote pilot high workload	Occasional (4)	Hazardous (4 or B)	4B	Unacceptable	High risk	Cease or cut back operation promptly
Meteorological conditions	N/A[7]	-	-	-	-	
Impact against terrain	Occasional (4)	Catastrophic (5 or A)	4A	Unacceptable	High risk	Cease or cut back operation promptly
Jamming/spoofing with DAA/ADS-B in failure	Improbable (2)	Hazardous (4 or B)	2B	Acceptable based on risk mitigation	Moderate risk	Schedule performance of a safety assessment to bring down the risk index to the low range if viable

During the investigations, internal and external factors related to RPAS systems should be considered to develop the aforementioned final items of this research. According to [5], the internal elements for the RPAS can be divided as follows:

- Different RPAS propulsion systems:
    1. Rotor RPAS;
    2. Fixed wing RPAS;
    3. Hybrid propulsion RPAS.
- Different RPAS functional system architectures:
    1. Autopilots type, configuration and redundancy;
    2. Number of motors and related electronic management system;
    3. Types of Flight Termination Systems (FTSs) and functional link to the autopilot.

In this context, the authors want to underline that only a real RPAS flight, as the RAID demonstration clearly showed, can perform a critical analysis in order to properly investigate the above list of technical items. Additionally, as required by SMS manuals, FMECA/FMEA reliability analyses should be developed on the identified real RPAS to concretely investigate all the possible failure modes and their effects in a comprehensive scheme.

Concisely, the external or boundary elements that must be considered during analyses and evaluations can be grouped as follows:

- In-flight hazards:
    1. Risk of mid-air collision with conflicting traffic or risk of terrain impact [32];
    2. Influence of meteorological conditions;

3. Thunderstorms;
4. Turbulence;
5. Temperatures;
6. Wind gusting.

- Other airborne hazards:
    1. Wake Turbulence;
    2. Wind shear;
    3. Potential impact with birds;
    4. Volcanic ash.
- On-ground hazards:
    1. Other surrounding aircraft on ground in the aerodrome area of operations;
    2. Other vehicles on ground in the aerodrome area of operations;
    3. Typical aerodrome infrastructures;
    4. People in the aerodrome operational areas.
- Hazards related to human factors:
    1. The absence of the pilot on board;
    2. The performance of the remote pilot;
    3. The performance of ATC personnel.
- Hazards related to the Ground Control Station (GCS)
- Hazards related to the Command and Control (C2) datalink:
    1. Functional aspects;
    2. The case of a loss of the datalink;
    3. The case of malicious jamming;
    4. The case of malicious spoofing.

The above list of internal and external RPAS hazards should always be analyzed with reference to the aforementioned standard scenario to ensure compliant with EASA recommendations. Risks' probability of occurrence and severity must be calculated for each typical operation or flight expected in the standard scenario for any RPAS category. Safety assessment and risk matrices should be implemented accordingly.

As had been done for manned aviation, the definition of a proper taxonomy, that is a classification of possible causes of incidents for RPAS, can be considered as the proper way ahead for future studies.

4. Discussion

This article introduces the idea of building an ad hoc, tailored SMS to promote the future integration of RPAS into non-segregated airspaces, starting by modeling a comprehensive risk analysis. This is the initial step, in order to develop the growth potential of RPAS, from an economic point of view, in line with the new ICAO recommendations, for every aeronautical operator. In fact, after their initial deployment for military purposes only, RPAS are demonstrating their versatility and economic advantage when used to accomplish different civilian applications. However, like any other kind of aviation actor, they shall be compliant with the recent indications, issued by ICAO, on safety management matters. Nevertheless, RPAS are going to access non-segregated airspaces, which are undergoing a general reorganization to improve efficiency against the increasing volume of traffic, while maintaining the highest level of flight safety. International regulators encourage the affirmation of RPAS as new actors in the aviation scenario; however, safety shall not be compromised by their operation.

In this context, following the first experimental results of research projects involving multiple drones, Europe is proposing an "operation-centric" flying scenario. This scenario requires RPAS

operators to demonstrate proper safety implementation measures by means of safety risk analysis and evaluation. In this context, the SMS represents the key tool for implementing all the required flight safety measures. Starting from the experimental results achieved by multiple-RPAS experimental flights in the project RAID, a solid basis was provided to further implement a risk model and general procedures to investigate RPAS safety.

The following points shall be taken into account to form the basis of a proper implementation of the risk model. As foreseen by SMS requirements [32], boundaries and system constraints shall be defined a priori (before starting the analysis). The system is intended to be composed of at least RPAS and remote pilots, manned aircraft and pilots, ATC operators, airspaces with their own rules like, for example, right of way, horizontal and vertical separations, collision avoidance with respect to other manned or unmanned aircraft, generic obstacles, terrain (see [35] for an interesting approach to the possible use of low cost-sensors to accomplish these detect and avoid functions) and aviation infrastructure. With reference to possible airspace configurations, suggestions come from the last RPAS Eurocontrol workshop held at NATO Headquarters, Brussels in April 2017 [36], where many examples of operative scenarios below 500 ft were showed and discussed.

With regard to the implementation of a FMECA/FMEA analysis of a real light RPAS, proper attention has to be paid to the estimation of the correct probability of occurrence of the considered failures. As is well known, this parameter must be calculated with great accuracy to properly support the decision-making process [37]. Furthermore, an additional delicate issue will be data gathering concerning the risk of mid-air or on-ground collisions for each phase of a RPAS flight. The major criticality is given by the fact that RPAS, especially for civilian use, is still a recent technology and the flight accident database is not consistently populated yet.

The definition of a new taxonomy for RPAS incidents has been identified as a possible development of the study.

Final considerations at the system level suggest that the high complexity and criticality [38] of aviation systems can increase further with the forthcoming integration of RPAS into non-segregated airspaces. These elements suggest that new approaches should be explored to study and categorize the system safety beyond the traditional consolidated SMS methodologies [29,39,40]. These new methodologies are recognized to be particularly suitable for quickly changing technologies like modern ones [40], aviation and RPAS systems related to the systems theory [40], and upgraded techniques to evaluate safety like the System-Theoretic Accident Model and Processes (STAMP) methodology [40]. The idea is that accidents occur not simply as a consequence of chain of events; rather, they happen as a result of a combination of system components' interactions and indirect or systemic causal mechanisms. In systems theory, safety is defined as an emergent, controlled property, which imposes opportune constraints on system behavior and interactions among its components. Safety becomes a form of control in the system, where the aim of control is to enforce safety constraints. Accidents are interpreted as occurrences stemming from inadequate control or enforcement of constraints on design, development, or system operation. According to STAMP safety methodology, every system can be modeled and studied according to three main steps: A safety constraint definition, a hierarchical model structure definition (where each level imposes constraints on the system level beneath it), and control processes definition and execution. As stated in the literature [40], the potential advantages of this methodologies and tool, based on STAMP, are such that, after having applied them in practice on very complex real systems, they were much easier and more effective to use than the traditional ones.

5. Conclusions

This article deals with a preliminary risk analysis on the basis of the RPAS flight test activity performed within the RAID demo project. A more comprehensive risk model and general procedures will be the immediate development of this study, to investigate RPAS safety according to the recent ICAO recommendations, on the adoption of a Safety Management System and operational scenarios defined by EASA. Definition of a new taxonomy for RPAS incidents will be a possible development of this study. Systems theory and related tools and methodology will be explored as well, to better

understand the occurrence of possible accidents into operative scenarios, with RPAS flying with manned aircraft into non-segregated airspaces.

List of abbreviations

3D Missions	Dull, Dirty and Dangerous Missions
ADS-B	Automatic Dependent Surveillance Broadcast
AIRICA	ATM Innovative RPAS Integration for Coastguard Applications
AP	Autopilot
AMSL	Above Medium Sea Level
ARIADNA	Activities on RPAS Integration Assistance and Demonstration for operations in Non-Segregated Airspace
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
C2	Command and Control
CIRA	Centro Italiano Ricerche Aerospaziali
CLAIRE	CiviL Airspace Integration of RPAS in Europe
CTR	Control Zone
C WP	Controller Working Position
DAA	Detect and Avoid
DEMORPAS	Demonstration Activities for Integration of RPAS in SESAR
EASA	European Aviation Safety Agency
ENAC	Ente Nazionale Aviazione Civile
EU	European Union
FAA	Federal Aviation Administration
FLARE	Flying Laboratory for Aeronautical Research
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects ad Criticality Analysis
GATM	Global Air Traffic Management
GCS	Ground Control Station
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
IFF	Identification Friend or Foe
INSuRE	Integration into non-segregated ATM
ISR	Intelligence Surveillance Reconnaissance
MedALE	Mediterranean ATM Live Exercise
MoD	Minister of Defense
NOTAM	Notice to Airmen
ODREA	Operational Demonstration of RPAS in European Airspace
OPV	Optionally Piloted Vehicle
PtF	Permit to Fly
RADAR	Radio Detection and Ranging
RAF	Royal Air Force
RAID	RPAS-ATM Integration Demonstration
R&D	Research and Development
RPAS	Remotely Piloted Aircraft System
SCP	Supplementary Cooling Pack
SDPD	Surveillance Data Processing and Distribution
SESAR-JU	Single European Sky ATM Research – Joint Undertaking
SMS	Safety Management System
SSP	State Safety Program
STAMP	System-Theoretic Accident Model and Processes
TCAS	Traffic Alert and Collision Avoidance System
TEMPAREIS	Testing Emergency Procedures in Approach and En Route Integration Simulation
UAS	Unmanned Aerial System

UAV	Unmanned Aerial Vehicle
VLA	Very Light Aircraft

Acknowledgments: The activities have been carried out in the frame of the project RAID, co-financed by the SESAR Joint Undertaking as part of RPAS Demo projects of the SESAR Program (2013 SESAR SJU/LC/0087-CFP). Opinions expressed in this work reflect the authors' views only and the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

Author Contributions: Authors' contributions were equal in this research based on flight experimental data gathered after the conclusion of the project RAID, co-financed by the SESAR Joint Undertaking.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Civil Aviation Organization. Circular 328 AN/190 Unmanned Aircraft Systems, 1st ed.; ICAO: Montréal, QC, Canada, 2011; pp. 1–54.
2. De Rosa, A. Gli aeromobili militari a pilotaggio remoto: evoluzione normativa e prospettive. Intervento svolto nel corso del Seminario di studi: Cyber warfare ed operazioni con aeromobili a pilotaggio remoto: Problematiche giuridiche. Centro Alti Studi per la Difesa Gruppo Italiano dell'International Society for Military Law and the Law of War: Roma, Italy, 2013; pp. 1–14.
3. European Aviation Safety Agency. Technical Opinion Introduction of a regulatory framework for the operation of unmanned aircraft Related A-NPA: 2015-10-RMT.0230; EASA: Köln, Germany, 2015; pp. 1–44.
4. Ente Nazionale Aviazione Civile. Remotely Piloted Aerial Vehicles (RPAS), Courtesy English translation, 2nd ed.; ENAC: Rome, Italy, 2016; pp. 1–38.
5. International Civil Aviation Organization. Document: 10019 AN/507: Manual on Remotely Piloted Aircraft Systems (RPAS) 1st ed.; ICAO: Montréal, QC, Canada, 2015; pp. 1–54.
6. Martin T.L.; Campbell, D.A. RPAS Integration Within an Australian ATM System: What equipment and which airspace. In 2014 International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, 27–30 May 2014; pp. 656–668.
7. Cappello, F.; Ramasamy, S.; Sabatini, R. A low-cost and high-performance navigation system for small RPAS applications. *Aerosp. Sci. Techn.* **2016**, *58*, 529–545.
8. Ramasamy, S.; Sabatini, R.; Gardi, A. Novel flight management system for improved safety and sustainability in the CNS+A context. In 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS) Herdon, VA, USA. 21–23 April 2015; pp: G3-1–G3-11, doi:10.1109/ICNSURV.2015.7121225
9. Barrado C.; Pérez-Batlle M.; Lopez M.; Pastor E. Paired T-test analysis to measure the efficiency impact of a flying RPAS in the non-segregated airspace. In 35th IEEE/AIAA Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 25–29 September 2016; pp. 1–7. doi:10.1109/DASC.2016.7778008
10. Thomas E.; Bleeker O. Options for insertion of RPAS into the air traffic system. In 34th IEEE/AIAA Digital Avionics Systems Conference (DASC), Prague, Czech Republic, 13–18 September 2015. doi:10.1109/DASC.2015.7311429
11. Cunliffe, AM; Anderson, K.; DeBell, L.; Duffy, J.P. A UK Civil Aviation Authority (CAA)-approved operations manual for safe deployment of lightweight drones in research. *IJRS* **2017**. doi:10.1080/01431161.2017.1286059
12. Filippone E., Grimaccia F., Monteleone A., Real-Time Simulations Results: Test scenarios DAA system. In Workshop of RAID project, Rome, Italy, 10 December 2015.
13. International Civil Aviation Organization. Annex 2 to the Convention on International Civil Aviation, 10th ed.; ICAO: Montréal, QC, Canada, 2005; pp. 1–74.
14. International Civil Aviation Organization. Amendment 43 to the International Standards Rules of the Air (Annex 2) ICAO: Montréal, QC, Canada, 2012; pp. 1–24.
15. International Civil Aviation Organization. Document 9854 AN/458 Global Air Traffic Management Operational Concept; 1st ed.; ICAO: Montréal, QC, Canada, 2005; pp. 1–82.
16. Cordón, R.R.; Sáez Nieto, F.J.; Cuerno Rejado, C. RPAS integration in non-segregated airspace: The SESAR approach System interfaces needed for integration SESAR WPE. In Fourth SESAR Innovation Days, 25–27 November 2014; pp. 1–8.

17. 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.
18. Centro Italiano Ricerche Aerospaziali. SESAR Joint Undertaking RPAS 0.3 RAID Demonstration report, 1st ed.; SESAR Joint Undertaking: Bruxelles, Belgium, 2016; pp. 1–156.
19. International Civil Aviation Organization. Eleventh ICAO Air Navigation Conference CARE/ASAS Action information from ANC/11 related to ADS-B, ASAS and ACAS 1st ed.; ICAO: Montréal, QC, Canada, 2004; pp. 1–54.
20. International Civil Aviation Organization. ADS-B implementation and operations guidance document 7th ed.; ICAO: Montréal, QC, Canada, 2014; pp. 1–85.
21. Single European Sky ATM Joint Undertaking. Available on line: http://www.sesarju.eu/sesar-solutions/enabling-aviation-infrastructure/ads-b-ground-surveillance-system (accessed on 27 February 2017).
22. Available online: https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (accessed on 28 June 2017).
23. Available online: http://www.airforcesmonthly.com/2009/10/28/nimrod-report-blasts-mod/ (accessed on 28 June 2017).
24. Haddon-Cave, C. The NIMROD Review, Report, ISBN: 9780102962659, Crown Copyright: London, UK, 2009; pp. 1–587.
25. Comitato 8 Ottobre 2001. Available on line: http://www.comitato8ottobre.com/ (accessed on 27 February 2017).
26. Vicinanza, E.; Col, T. Anatomia di un incidente Predator RQ-1C. *Sicurezza Aeronautica Militare* **2014**, *305*.
27. Magg. Matteo Zuliani, Anatomia di un incidente C130J. *Sicurezza Aeronautica Militare* **2014**, *306*.
28. Dekker, S.; Cilliers, P.; Hofmeyr, J.H. The complexity of failure: Implications of complexity theory for safety investigations. *Saf. Sci*. **2011**, *49*, 939–945.
29. Leveson, N.G. Applying system thinking to analyze and learn from events, *Saf. Sci*. **2011**, *49*, 55–64.
30. International Civil Aviation Organization. Document 9859 AN/474 Safety Management Manual (SMM), 3rd ed.; ICAO: Montréal, QC, Canada, 2013; pp. 1–54.
31. U.S. Department of Energy. Human Performance Improvement Handbook, vol. 1, DOE Standard: Washington, DC, USA, 2009. Available online: http://energy.gov/sites/prod/files/2013/06/f1/doe-hdbk-1028-2009_volume1.pdf (accessed on June 2017).
32. Federal Aviation Administration. Safety Management System Manual: Air Traffic Organization, 4th ed.; Federal Aviation Administration: Washington, DC, USA, 2014, pp. 1–128.
33. International Civil Aviation Organization. Annex 19 to the Convention on International Civil Aviation Safety Management, 1st ed.; ICAO: Montréal, QC, Canada, 2013; pp. 1–44.
34. European Aviation Safety Agency. Explanatory note "Prototype" commission regulation on Unmanned Aircraft Operations. EASA: Köln, Germany, 2016.
35. Gageik, N., Benz, P., Montenegro, S. Obstacle detection and collision avoidance for a UAV with complementary low-cost sensors. *IEEE Access* **2015**, *3*, 599–609. doi:10.1109/ACCESS.2015.2432455
36. EUROCONTROL: Bird's eye view of present drone integration below 500ft. Available online: http://www.eurocontrol.int/events/rpas-atm-integration-workshop (accessed on 11 April 2017).
37. Banghart, M., Fuller, K. Utilizing confidence bounds in Failure Modes Effects Analysis (FMEA) Hazard Risk Assessment. In 2014 IEEE Aerospace Conference, Big Sky, MT, USA, 1–8 March 2014.
38. Zio, E. Challenges in the vulnerability and risk analysis of critical infrastructures, *Rel. Eng. Syst. Safety* **2016**, *152*, 137–150.
39. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res*. **2016**, *253*, 1–13.
40. Leveson, N.G. Engineering a Safer World: Systems Thinking Applied to Safety; The MIT Press: Cambridge MA, USA, 2011. Available online: http://mitpress.mit.edu/books/engineering-safer-world (accessed on 24 June 2017).