Sanz, D., Valente, J., del Cerro, J., Colorado, J. & Barrientos, A. (2015). Safe operation of mini UAVs: a review of regulation and best practices, *Advanced Robotics*, 29 (19), pp. 1221-1233.

DOI: 10.1080/01691864.2015.1051111

Safe operation of mini UAVs: a review of regulation and best practices

D. Sanz[a*], J. Valente[b], J. del Cerro[a], J. Colorado[c] and A. Barrientos[a]

[a]*DISAM, Center for Automation and Robotics – CAR UPM-CSIC, Jose Gutierrez Abascal 2, Madrid, Spain;* [b]*Departamento de Ingenieria de Sistemas y Automatica, Universidad Carlos III de Madrid, Av. Universidad, 30 – Leganes, Madrid, Spain;* [c]*Department of Electronics, Pontificia Universidad Javeriana, Calle 40 No. 5-50, Bogota, Colombia*

This paper is focused on the safety of mini UAV (mUAV) systems. It presents the great efforts that are being done in air legislation, including the present and future normative. Nevertheless, considering that the work is not finished yet, a low-level risk analysis concept is introduced. Based on the international regulations, a specific three-step structure for mUAV hazard analysis is presented: identification, assessment, and reduction in a recursive loop that provides a solid architecture for facing the wide range of possible risks.

Keywords: safety; unmanned aerial units; risk assessment; normative; risk management

1. Introduction

In the last few years, the Robotic Community has assisted to an amazing increment of the mini unmanned aerial vehicles (mUAVs) employment. They are being used for different purposes and tasks, from agriculture to surveillance or rescue, both individually and in a cooperative way. Many steps forward have been given up so far and there is a predictable growing of this trend. Nevertheless, the daily work with those physical platforms inevitably implies some risks (such us platform or property damages, human injuries.) that are disregarded most of the times.

Safety can be defined as 'the a state in which the system is not in danger or at risk, free of injuries or losses'. This state should be the first requirement and target in every application or design, and its legislation a priority for the air authorities. However, there is a lack of safety policy issuing aerial mobile units yet. In this way, it is important to enhance the state of art of these policies and discuss about the future policies that could augment the safety usage of mUAVs. This paper highlights the present and estimates the future of the legislation in this area (Section 2). Besides, summarizes the international approach for risk analysis, including hazard identification (Section 3.1) and evaluation (Section 3.2), as well as a group of techniques for risk reduction and avoidance in mUAV systems (Section 3.3).

On the other hand, the current efforts have specific targets, deepening in the airworthiness certification or in the limitations established for the scenario and the pilots. In general, global approaches are not considered. Nevertheless, they are really useful since allow to correlate more than one cause with several effects, as well as to tackling the safety guarantee from a comprehensive point of view. In this sense, Section 3 bases on ISO 31000:2009 normative to specify a three-step integral rationale method to perform this process: Firstly, possible hazards should be identified (Section 3.1), accordingly with their nature and the characteristics of the system. After that, their potential damage has to be estimated and assessed in the specific context – both individually or together with other events. In this regard, Section 3.2 specifies the method used to perform the evaluation. As Section 3.3 details, this is considered the best way to afford an adequate response to the potential problems, providing specific solutions depending on the origin and the magnitude of the menace.

2. Legal framework

The first point to be considered when evaluating the safeness of a system is the legal framework that applies to the system. It contains a previous analysis of the problem, so the applications of its guideline helps to avoid or minimize the main part of the risk that may arise. Nevertheless, legislation analysis and study require a hard work in the sense of discriminating the applying directives for each individual case. This study deepens not only on the common normative –generalist, referred to machinery or electronic equipment –, but also on the drones specifically. Furthermore, as the air legislation for mUAVs is quite uncertain and diffuse, the current work has been also presented in form of proposals and on-going normative.

*Corresponding author. Email: d.sanz@upm.es

2.1. *Common applying normative*

As previously stated, even before analyzing the air-related aspects of the UAVs, it is important to analyze their constrains from a higher point of view: firstly, considering their nature as vehicles or mobile machines. Secondly, even more abstract, attending to their definition as complex systems that interact among them (both internally and externally). In this sense, the present regulations referring to machinery and engineering systems are the following ones:

- ISO 12100:2010: 'Safety of machinery. General principles for design'.[1]
- ISO 14121-1:2007: 'Safety of machinery. Risk assessment'.[2]
- ISO 31000:2009: 'Risk management. Principles and guidelines'.[3]
- ISO 13849-1:2006: 'Safety of machinery. Safety related parts of control systems'.[4]
- IEC 31010:2009: 'Risk management. Risk assessment techniques'.[5]

Besides, from the systemic point of view, the UAV has also to be considered as a collection of electronic devices. In this regard, the regulations regarding to electromagnetic compatibility, EMC (IEC/TR 61000-3-2 [6]), radio frequency and communications (ISO/IEC 18000-1:2008 [7]), or those referring to tracking, location, navigation, and geographic information in general (ISO 19133:2005 [8]) must be observed.

2.2. *General UAV normative: the international picture*

Since the emergence of Unmanned Aerial Vehicles is a relatively new phenomenon, the regulation and legislation in its regarding is mostly under development yet.[9] Besides, due to the military origin of the UAVs, global standardization has been postponed many times, turning out lately to be a difficult issue: each country has its own regulation, being in many cases being inherited from the military policies.

However, the authorities and regulatory institutions have recently realized about the relevance of UAVs in civil applications. So, a major global effort has been taken in order to give shape to a common regulation that may allow UAVs to fly globally: it started in 2005 with the Cross Atlantic cooperation among the US Federal Aviation Authority (FAA), the European Aviation Safety Agency (EASA), and Eurocontrol. During the process, two main topics were settled: firstly, a common classification for the UAVs (see Table 1 [10]). Secondly, a set of metric and procedures that have defined the main lines for the common policy.[12] In this sense, basing only on six characteristics (i) mass, (ii) maximum fight ranges, (iii) relative altitudes, (iv) flight endurance, (v) wing-type[1], and (vi) flight control scheme [2]), two different scopes were defined:

- Operational approval: Applies to drones class I. It consists of a proof demonstrating safe flight capabilities, licensing, training, and limitations of the system.
- Full regulations: Applies to drones class II. It requires a certification of airworthiness, vehicles registration, design certification, etc.

Basing on this, FAA imposed in the US a two-step certification process before allowing any vehicle to operate within the National Air Space (NAS): firstly, an airworthiness certification is required. Then, a waiver (Certificate of Authorization, COA) regarding the operability of the system and its collision avoidance capabilities have obtained.[13,14]

In the same line, European legislation has defined a similar procedure. Nevertheless, as far as the cooperation only focused on big–medium UAVs, EASA's scopes have been focused on addressing UAVs with a take-off weight (MTOW) over 330 lb/150 kg [15]: small UAVs (also called Light UAVs, LUAS) regulation has been diverted to the corresponding EU's Air Authorities. In this regard, the most advanced civil frameworks for regulating the safe operation of UAVs (either civil or military) are located in the UK, France, and Austria. On the other hand, from the military point of view, regulations in Germany, Croatia, Czech Republic, and Sweden should be highlighted [16]: They regulate common aspects, mainly centered in the dynamics of the vehicle and the safety of the environment. In the first aspect, common rules are defined, such as the maximum velocity (90 kts $\simeq$ 46 m/s), the maximum kinetic energy on impact (95KJ), or the maximum height above the surface (400 ft $\simeq$ 122 m). Other regulations are not standard, and differ depending on the country air authorities: (i) the maximum distance to the operator (e.g. 500 m, 1 km or Visual Line-of-Sight, VSL), and (ii) position lights requirement.

These data agree with other countries regulations:

- Australia (CASA): Civil Aviation Safety Regulations, CASR. Part 101.[17,18]
- France (DGA): UAV Systems Airworthiness Requirements (USAR) [19]
- Israel (CAII): UAV Syst. Airworthiness Regulations.[20]
- Japan (JUAV): Safety standard for commercial use, unmanned, rotary-wing aircraft in uninhabited areas.[21]
- UK (CAA): Light UAV Systems Policy (LUAS).[22]
- USA (FAA): AC91-57,AFS-400 UAS Policy 05-01 [23]

However, despite the operational/environmental restrictions have a common base, they have been specified differently on each country: for example, the maximum distance to populated areas (between 150 and 500 m), the distance to outsider (between 50 and 200 m), the maximum distance to airports/military zones (between 2 and 5 Km), or the

Table 1. Light UAV classification according to [10,11].

Initials	Name	Mass	Range	Altitude	Endurance
u	**Micro**	< 5 kg	< 10 km	250 m	< 1 h
m	**Mini**	5–15 Kg	< 10 km	150 m	< 2 h
CR	**Close Range**	25–150 kg	10–30 km	3000 m	< 4h
SR	**Short Range**	50–250 kg	30–70 km	3000 m	< 6h
MR	**Medium Range**	150–500 kg	70–200 km	5000 m	< 10 h

Table 2. Comparison of the current UAV proposals/legislation.

NOC[a]	ORG.	NORMATIVE													[b]
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
AUS (N)	CASA		X		X						X				
ESP (P)	MDE	X	X	X	X	X	X	X		X	X	X			X
FRA (N)	DGA	X	X	X	X	X	X	X		X	X	X			
GBR (P)	CAA	X	X	X	X	X				X	X				
GER (N)	BWB-WTD	X	X	X	X					X	X	X			X
ITA (P)	ENAC	X	X	X	X	X	X	X	X	X	X	X	X	X	
ISR (N)	CAAI				X		X					X	X	X	
JPN (P)	JUAV	X	X	X	X	X				X					
SWE (P)	FMV	X	X	X	X	X	X	X		X	X	X			
USA (N)	FAA	X			X		X	X	X	X		X			

[a]NOC corresponds to the international acronym of the country. The actual status of the normative is presented between parenthesis: P stands for proposal, N for established normative.

[b]In the normative, 1 corresponds to the classification of the drone according to its weight ($\simeq$ 150 kg); 2 maximum flight speed under 36 m/s; 3 maximum distance to the pilot under 500 m; 4 maximum relative height under 122 m (400 feet); 5 maximum kinetic energy on impact under 95 KJ; 6 minimum distance to populated areas under 150m; 7 minimum distance to any individual person under 100 m; 8 airplane modeling license required; 9 drone required to fly under visual line of sight (VLOS); 10 not allowed to carry people or animals; 11 ATM civil certification for flying in a non-segregated airspace required; 12 airworthiness official certification required; 13 Flight Guidance System (FGS) and lighting systems required; 14 official flight authorization required in private areas/fields.

suitable areas for taking-off/landing [24] have quite different values. Furthermore, beyond the minimums established by the FAA–EASA cooperation, the some of the issues considered by each regulation are really diverse. Table 2 presents the comparison that has been done regarding those considerations:

2.3. Ongoing normative and proposals. Working groups and organism involved

As it has been presented in Section 2.2, the international picture regarding to the mUAVs regulation is fragmented and divided. However, efforts are being done in this direction: despite a common normative does not seem to be achieved in a short/medium period,[25] many organisms and organizations are involved in the mUAV regulation. In this sense, apart from the national air authorities, there are many groups gathering manufacturers, users, designers, and researchers attempting to establish a common frame to regulate safety on UAV operation. They all establish guidelines and/or provide with recommendations. Nevertheless, it is necessary to highlight the work done by EUROCAE (Specifically the Working Group 73), USICO, JARUS (Joint Authorities for Rulemaking on Unmanned Systems), ICAO (International Civil Aviation Organization), and UVS International: although their documents have no official validity, they are taken into account when defining the official regulation. Even more, they are usually used as common guidelines until the legislation releases.

Besides, both the official organisms Joint Aviation Authority (JAA) and Eurocontrol have assembled a joint group named UAV Task Force. It has aimed to issue a proposal report – regarding safety requirements – according to the suggestions of the aforementioned partners.[26] As a result of this, it has been established a common criteria for determining the direction of the future common regulatory policy: 'UAVs must comply with an equivalent level of safety (ELOS) compared to conventionally manned aircraft'.[27] So, considering the air traffic standards, this delineation has established the minimums required for the development of the future policy.

3. Risk analysis

Even fulfilling all the applying normative and observing every aspect of the legislation, there is always a potential risk involved in any process: risks are inherent to action, and it is impossible to completely avoid them.

Control, mitigate, and/or reduce them is the best possible thing to do. In this sense, RMas – also known as Risk Analysis architectures (RAas) – focus on this target, trying to identify, classify, and evaluate the hazards in order to delimit their effects and coverage.[28,29] Besides, since RMas are generic evaluative frameworks, they have been employed in multitude of fields and areas. Economists, engineers, consultants, or merchants have adapted similar structures to their workspace and requirements.[30] For example, Chapman's PRAM (Project Risk Analysis and Management) methodology – which integrates RA as a subtask within each project –, has been considered in diverse fields: construction.[31] project management [32], and even aviation.[3][33]

Focusing on the engineering processes and systems, most of the RMa adaptations understand risk as a bond between event and undesirable consequences (that should be avoided or minimized). According to how these bonds are considered, two different approaches have emerged: on the one hand, methods that analyze the nature of those links, focusing on their temporal behavior; on the other, architectures trying to find the causes originating the events in order to control their repercussions from the beginning.

Among the first ones – those focusing on the frequency and effects of the incidents – event-driven feedback methods are the most popular ones due to their flexibility. For example, Kuchard proposed a structure based on events, where faults are modeled in terms of occurrences (that have been caused by anomalies, malfunctions, human errors, etc).[34] Its top-down architecture is a particularization of the common Fault Tree Analysis (FTA),[35] that was afterwards used by Murtha to propose a standard design for reliable UAVs.[36] Likewise, Apthorpe combines both Probabilistic Risk Assessment (PRA) [37] and the Event Tree Analysis (ETA) [38] decomposition into basic events to estimate the system reliability.[39] Used in the EUROCONTROL's Safety Assessment Methodology, his approach combines logic models (of the ways systems can fail) with statistical failure rates in order to associate failure probabilities with consequences.

Contrarily, the second branch of Risk Analysis architectures analyze the origins of the thread, focusing on the source–consequence relationship. For example, both the Failure Modes and Effects Analysis (FMEA) and the Fault Hazard Analysis (FHA) methodologies determine potential causes and probabilities of these risks.[40,41] Then, they both – with different depth levels – associate the models created with resultant effects to the subsystem and its operation.[33] Likewise, Hazard Operability Study (HAZOP) [42] and Statistical Process Control (SPC) [43] identify and monitor potential problems to statistically determine relationships and bonds. Even the methodologies that consider the system as a whole – those focusing on the general behaviur, instead on the specific events – try to establish relationships among circumstances and errors: for example, Celik's Common Cause Analysis (CCA) and Root cause analysis (RCA) allow to identify and associate common errors (events) in order to eliminate redundancies by [44,45].

The previously commented ISO 31000:2009 standard emerged as an attempt to combine both approaches.[3] Depicted in Figure 1,[4] it combines most of the strengths proposed by the rest of architectures in a modular approach: it provides with a flexible and adaptive linear-but-feedback RA scheme that analyzes the system reliability in terms of effect-to-cause. It considers both bottom-up and top-down manners (deductive or inductive, respectively), defining the system's specifications within the first stage of the RA process. Besides, it combines both 'event management' and '*a priori* information' approaches in the event-based methods, providing with a higher adaptability. Finally, ISO 31000:2009 also includes the reduction procedures within the analysis process, guaranteeing a higher robustness and suitability degree.

This behavior is achieved by implementing a three-step architecture that allows to make independent evaluations but maintaining a global view: as it is possible to appreciate in the figure, problems from one stage can find their solution (i.e. avoidance/reduction) in the following phases. Likewise, problems can be back-propagated in order to discover potential sources/origins in previous stages.

In this regard, first step in the process – after defining the requirements and specifications of the system – is the statement of the boundaries. They limit not only the system but also the operating framework (Section 3.1). Once enclosed the dangers, the possible risks (i.e. failures, malfunctions, etc.) should be found. The search is narrowed according to the nature of the danger and the origin of the hazards. Finally, the risks found are evaluated according to ISO 13.849-1:2006 methodology and classified depending on their severity.

The information extracted during the analysis is managed in order to minimize or avoid the risk. This Risk Reduction Procedure (RRP) is presented in Section 3.3, but it is important to anticipate that this structure is not linear, since the introduction of new measures or techniques for minimizing or avoiding the risks may introduce new hazards. From this point, a recursive evaluation of the risk is necessary, not only for assess the performance of the solution but also their effects in the system behavior. Nevertheless, this architecture might go into an endless loop. Due to this, the loop has a limited number of iterations that force a redefinition of the system's specifications if it is not possible to equate the risk level to the one required.

For all these reasons, this procedure has been considered the most suitable one to implement a RAa for a drone. Thus, following subsections present how the standard has been customized in order to adapt these structures to analyze the risk of outdoor UAV missions.

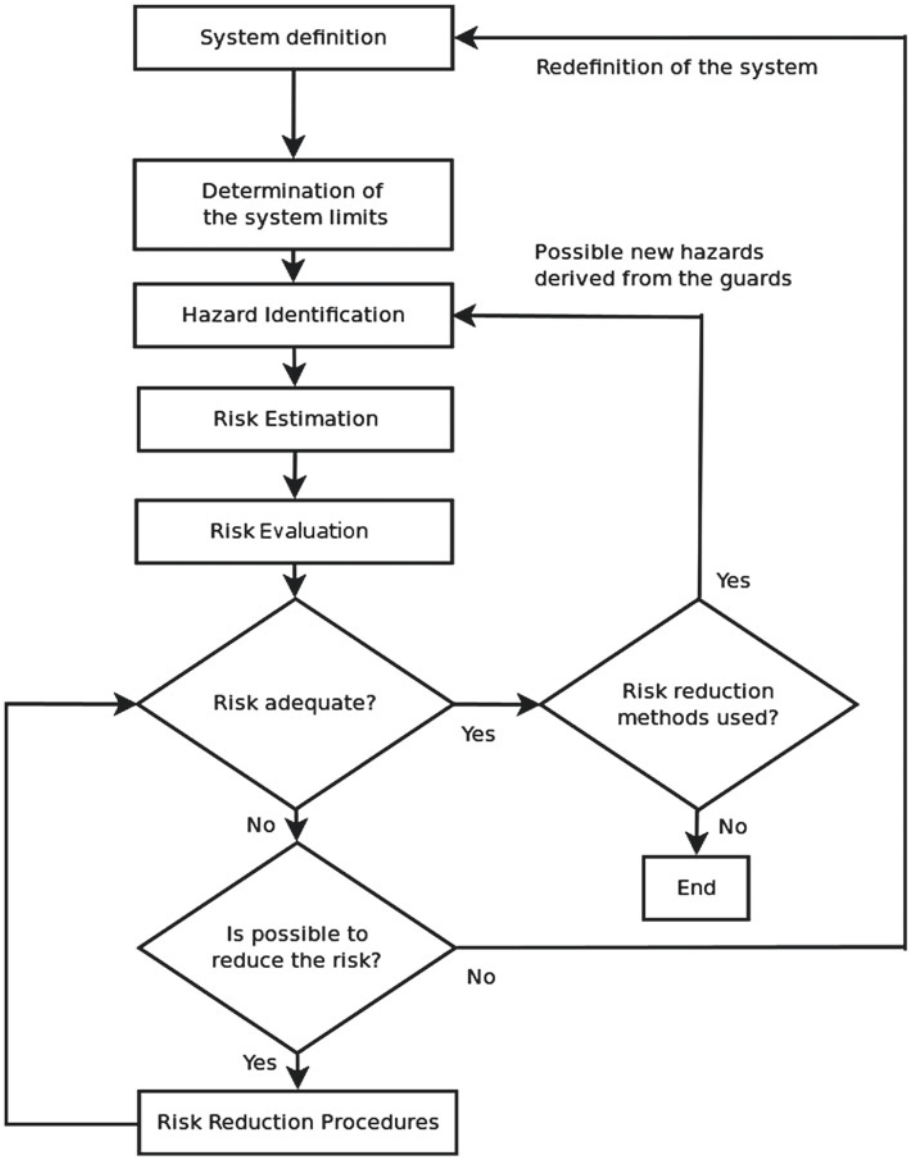


Figure 1. Simplified architecture of the risk assessment and risk reduction.

3.1. Risk identification

As previously stated, before analyzing the potential hazards of the system, it is necessary to state the limits of the operation so as to enclose the possible consequences of an accident or failure.[46] So, focusing on mUAV outdoor missions, physical/temporal requirements are derived from the normative and applying regulations and the manufacturer's specifications, logic and previous experiences.[47] Thus, restrictions are not only imposed to the equipment, but also to the environment and to the flight procedures. It is possible to divide the limits according to their nature:

(1) Physical limits (Unit and components):. They refers to the kinematic and dynamic restrictions imposed by/to the mUAV. Their origin (self or imposed) may derive from the physical restrictions of the machine itself or from the dispositions of the legal framework. For example, maximum payload (or the equivalent Maximum Take-Off Weight, MTOW) or maximum speed is clearly defined by the drone's characteristics, but other restrictions have not so well defined their origin. In these cases (e.g. maximum/minimum height or the Maximum kinetic Energy on Impact), limits are defined by the most restrictive source.

(2) Temporal limits (Life time):. Temporal restrictions are derived from the degradation or efficiency-loss of the drone's components. In this sense, short time (e.g. maximum time of flight, time of response of the commands or acquisition time of the sensors) or long time (e.g. engines and battery degradation) restrictions should be

considered, establishing a safety margin in order to guarantee their behavior.

(3) Environmental limits (Flight location and conditions):. As in the physical restrictions, limits are imposed by the own drones or/and by the legislation, although the scope is more clear. Weather conditions such us wind speed, ambient light, or dust/rain presence should be taken into account from the platform side. On the other hand, the minimum distance from populated areas or from airports/military installations, the inclusion of the drone in the non-segregated airspace, or the GPS coverage must be also considered.

(4) Behavioral limits (Operation and procedures):. Finally, flight constrains are applied in the operation, affecting to the procedures and actions of the pilot (both autonomous and manual). Could be included in this topic the minimum distance to the operator or the algorithmic and sensing capacities of the vehicle (environmental known).

The lack of respect for these restrictions unquestionably supposes a potential hazardous situation. Nevertheless, as previously said, since the regulations are fixed and static they do not cover all the possible risky situations of the evolving UAVs and their circumstances. Therefore, it is possible to limit the hazards constraining the characteristics of the flight, but to avoid them completely is impossible.

So, even assuming the operation conditions satisfy the applying normative and that the operation is framed according to the previously explained, it is required to analyze which are the potential hazards to be found. In this sense, the drone's potential risks can be classified attending to their sources, dividing them between intrinsic system's problems and outside sources:

(1) External sources are those whose behavior and/or presence is not related or connected with the mUAV itself. Since they are not manageable, their presence supposes an extra risk that should be considered. The interference of third-party agents (e.g. animals, humans, other equips, EMC emitters, etc.), the environmental conditions (e.g. wind, temperature, GPS signal quality.) or the presence of dynamic elements – where both relative movement and interaction should be considered – is the main sources of external hazards.[48,49]

(2) Internal sources are those related with the drone's operation/performance, derived from one of more procedures associated to the application. The analysis performed is depicted in the Table 3. It presents the activities related with the flight that may provoke a breakdown or a risky situation.

External risks can be evaded using avoidance techniques and mechanisms. Nevertheless, internal-sources hazard are completely unavoidable. Their rate can be decreased and their effects minimized or enclosed, but it is not possible to eliminate them. So, it is mandatory to analyze which are their sources and which are the possible consequences in order to evaluate their possible effects later. Considering breakdowns as the main internal hazard source for UAVs, their nature has been analyzed. In this sense, they can be classified attending to their origin and taking into account the magnitude affected by its effect [50]: Table 4 presents a relation of hazardous events, established in this work according to their physical type. It provides, as well, with some examples of the possible consequences of the hazards action.[51] It should be noted that the risks are interrelated, so a hazard could be classified in several different groups. As well, the consequences or problems caused could also be originated by different hazards. So, classification in this table has been done according to their occurrence probability and their deep composition or characteristics, but considering the problems of hazard combination.[52]

3.2. Risk assessment

Once identified the candidate risks sources and their nature, the second step implies estimating the seriousness and severity of their effects (i.e. to appraise the consequences of a potential breakdown or accident during the UAV mission). In this sense, according with ISO 14121 – as well as in most of the risk evaluation methods,[53,54] hazard assessment is a function of two factors: the first one refers to the severity of the damage that evaluates in a fuzzy way the harm resultant from an hypothetical incident. On the other hand, the second factor defines the probability of occurrence, determining the frequency of exposition to the risks. The relation between these factors determines the risk level of the component. The summation of the risk estimation for every component and procedure in the system outputs the global risk figure.

(1) Seriousness of damage: As previously said, the seriousness of the damage evaluates the harm that could be provoked in an accident. Potential damage is key factor to estimate the risk associate to a component, defining in this sense the importance of the processes where the damage has his origins. Seriousness rate is composed of two factors: Firstly, the severity of the injuries or the damage to health (both for the drone and for the element it crashed into). This aspect is assessed in a fuzzy way, and generates a scaled output according not to the percentage of destruction but with the evaluation of the impact/importance in the system. According with the international normative, only reversible and irreversible damages are considered in the scale, although we propose an intermediate (light / serious / death or destruction) would be positive in order to improve the characterization of the damages.[55]

Second factor – which it is not considered in the actual legislation but that has been proposed in many

Table 3. Analysis of hazards internal sources.

Stage	Activity
Preparation	Manufacture, Load, Transport, Assembly,Handle,Packaging
Startup	Setup, Assemble, Adjustment, Connections, Test, Installation, Integration (e.g. payload mount/unmount)
Operation	Piloting, Human intervention, Setup, Supervision, Human manipulation, Violations of safety procedures, Verification, OS hung up
Maintenance	Settings, Cleaning, Conservation, Lubrication, Periodicity, Suitability, Cleaning, Charging process of batteries
Design	Materials, Components, Physical stability, Resistance, Compliance, Software
Control	Algorithmic stability, Time of response, Refresh rate, Accuracy, Error handling, Hysteresis, Software Virus

Table 4. Analysis of the hazards according to their nature.

Type	Sources	Consequences
Mechanical hazards	Impacts, Emissions, Give-offs, Collisions, Breaks, Friction, Pressure, Inadequate balance/stability, Mobile parts	Run over, Crush, Cut or section, Drag or entrapment, Hook, Friction or abrasion, Impact, Injection, Puncture, piercing
Power supply breakdowns	Violation of maximum absolute ratings, No energy, Perform variation, Short circuit, Polarization	Decelerations, Accelerations, Burn, Overheating, Falls, Motor stop, Saturation
Thermal hazards	Overheat, Flames, Freeze, Abrasion, Explosions	Burn, Freeze, Battery problems, CPU auto switch-off, Injuries from radiation heat, Dehydration
Electronic hazards	Saturation, Overflows, Derives, Isolating inappropriate, Synchronization, I/O errors, Disconnection	Overheating, Sensors confusion, Radiations, Control loose, Short circuiting
Electromagnetic & Radiation Hazards	Electrostatic phenomena, Interferences, Ionizing radiations, Spectrum saturation	Disorientation, Failures in active components, Overheating, Erroneous reception/send, Interferences in the communications, Drone out of control, Sensors inconsistency
Algorithmic hazards	Infinite loops, Inadequate values, Values out of range, Delayed process, Sequencing, Overflows, Synchronization	Drone out of control, Reception/send wrong parameters, Synchronization failures

scales, corresponds to the number and affiliation of the agents involved in the event. It should be distinguished among critical and non-critical components, as well as if people or third-party elements affected. In this sense, the classification proposed: components of the mUAV, the drone itself, the payload (in case of exist), external infrastructures or objects, the operator (the pilot or anyone involved in the UAV operation), one person or several people.

(2) Probability of damage: This figure estimates the frequency of occurrence of a hazardous event. The incident rate, as a function of the system use, is the value resultant from the composition of three factors [55,56]:

- Exposition to the danger: These data evaluate the quantity of risk the drone has been exposed to. In order to evaluate it, it should be taken into account the exposition time (mean period T of exposition every time it is exposed), the number of agents exposed (in case of being a fleet), the kind of exposition (e.g. manual or not, normal operation or emergency mode) and the frequency of exposition, meaning the time exposed to the risk over the total time of operation (e.g. to the collisions risk, total time when the drone is close to another object, over the total flight time).
- Probability of occurrence of a hazardous event: The frequency of incidents can be determined experimentally or/and provided by the manufacturers. The event rate derived from the human intervention or not specifically detailed (because the component has not been verified or because its verification is not conclusive) is determined by means of statistics and history: Statistical reliability, accident history, and similarities with other systems [57]
- Ability to prevent the risk or limit damage: The aptitude to avoid a hazardous situation or limit harm in case of accident influences the probability of occurrence of such damage. In this sense, both aptitudes mitigate the global risk, so should be taken into account as an active factor. The issues related with this capacities are

the people/operator skills (e.g. reflexes, agility, ability to escape), the speed of the events, the perception of risk (general information, direct observation, warning signs), the operator qualification and experience, and the suitability of the guards and safety systems (risk identification, agents involved, usability, possible interferences, etc.)

According to all these factors, a general evaluation of the selected risk is performed. As depicted in the Figure 2, the factors described above are combined using the Kinney method in order to obtain the Performance Level (PL) metric.[58,59] PL is employed to manage the assessed hazard and refers to the general reliability required by the component/system in order to operate under safety conditions (probability of a dangerous failure per hour). This metric considers both quantity (e.g. measurements of reliability, ability to resist failures, etc.) and quality aspects (i.e. system's performance upon failure conditions, failure monitoring, and safety related to software implementations).

3.3. Risk reduction

Once determined the possible hazards, their sources as well as possible effects, the last stage is to analyze and establish possible methods for avoiding or limiting the possible harm. The reliability level required, robustness needed, and performance requirements are defined in the chart presented in the Figure 3: it establishes a relationship among four different parameters, related to the confidence on the drone's capabilities. Apart from the PL determined before (see Section 3.2), a fuzzy figure for the MTTF (Mean Time To Failure) is defined. It expresses the mean time until a design's or component's first failure and determines the quality required to the components. As well, the Diagnostic coverage (DC) figure is also defined, quantifying the proportion between the number dangerous failures detected and the occasions when the failure mode has been activated. Finally, the last feature refers to the category (Cat.): It determines – in case of existing a controller – the control architecture specified for guarantying an adequate safety level (Being B not especial requirements and the numbers different control configurations). In this sense, for example, if both the MTTF and DC of a mUAV are low, an architecture of type 2 (Cat. 2) will be required for obtaining an a/b performance level – what is the minimum one required by the regulation.

According this regulation (ISO 12100-1:2003), there are three possible stages of where is possible to interact for achieve these figures. First level tries to eliminate the hazard by means of an inherent safe design (Chapter 4, of the ISO normative). When it is not possible, second level performs risk reduction by implementing protective and preventive measures. They are complementary methods for the intended use and reasonably foreseeable misuse (Chapter 5); Finally, if no one of the previous methodologies is enough reduce the risk adequately, the imposition of safety procedures is required. In this sense (Section 5.5 of ISO normative):

(1) Design process: As described in Section 3, first stage in any design is the definition of the requirements and the characteristics specification. It is a critical phase, and its inappropriate accomplishment makes possible the presence of risk and problems in the following stages. Thus, the appropriate materials, components and procedures election, as well as the careful definition of the specifications is a crucial issue.[47]

Simulation is a significant tool to determine the behavior and time response of the component simulated. It allows identifying execution problems impossible to determine in other ways – and estimate the probability of occurrence of a hazardous event. As well, simulations are really useful in order to adjust the probability level introduced to the risk estimator when trying to locate the recurrent errors source. Thus, it should be defined and developed a test bed. Prototyping and verification allow the manufacturers and operators to evaluate the correct performance and the correct system's status of every hazardous component or element of the system. Both auto-check and visual inspection should be considered, in order to corroborate system's condition and identify possible problems before executing the mission.

Finally, halfway between Design and Protection Measures is situated the Control issue: In order to help the designer, ISO 13849-1:2006 provides a methodology based on the categorization of structures according to specific design criteria and specified behaviors in case of default. These categories are depicted in the Figure 4 and correspond with the four categories extracted during the risk assessment process (Section 3.2).

As it is possible to appreciate in the image, the complexity of the control structure is defined according with the safety requirements (or, in other words, with the hazard level): The higher the estimation hazard is, the most sophisticated the scheme must be.

Category B does not imply any special requirements. Moving forward, Cat. I requires from an close-loop controller (L). It balances the measures acquired from the environment and provides with an answer according to it. This scheme is complemented with a supervisor (S) in Category II, allowing to auto-detect errors or failures in the own control system. Besides, it also adds a direct feedback information from the output to the control (L). Nevertheless, it could be not enough in really dangerous situations. They requires architectures with different levels of redundancy, like the ones described in Categories III and IV. This kind of scheme it is not only able to detect the problem, but also avoid it and continue working.

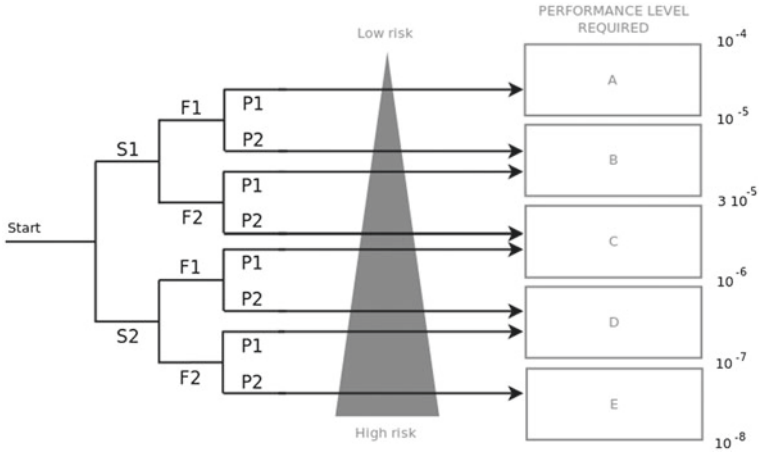


Figure 2. Evaluation of the hazard according to ISO 13849. Required Performance Level analysis[1]. S stands for Severity of Damage, F for Frequency of Exposure to the hazard, and P for the capacity to avoid or limit the risk. In all the factors, suffix 1 refers to the lower level of the corresponding magnitude (e.g. S1 implies low potential damage) and 2 to the higher level (e.g. F2 depicts high exposure). On the other hand, the performance levels (PL) range from A to E, as a representation of the failures/hour rate (presented in the upper right corners.

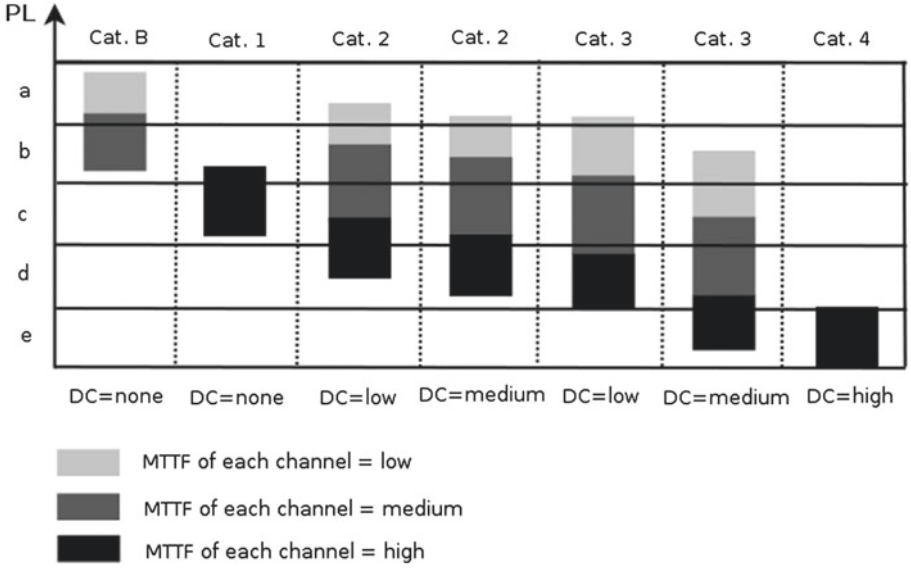


Figure 3. Evaluation chart form MTTF, DC, and Control Category definition after the PL analysis and set up.

These structures should be applied when considering protective devices (e.g. control devices, sensing systems, locking devices, etc.), control units (e.g. a logic block, data processing units, etc.), and other control elements (e.g. relays, safety switches, valves, etc.). Nevertheless, as previously said, the inclusion of these schemes should/must be not the unique measure included: Redundancy structures, hardware supervisors, and watchdogs, or ruggedization methods clearly improve the fail tolerance of the system.

(2) Prevention/Protection: Guards are elements not included in the core of the system, but added in order to provide a protection service. It is in charge of limit the damage not only to the drone's elements but also to third- party agents. They are conceived as physical – both passive and active – sentinels, capable to absorb kinematic energy or limit the movement of the air vehicles or the people around it. Examples of these kinds of elements are propeller protections, landing legs, parachute, airbags, or protection nets.

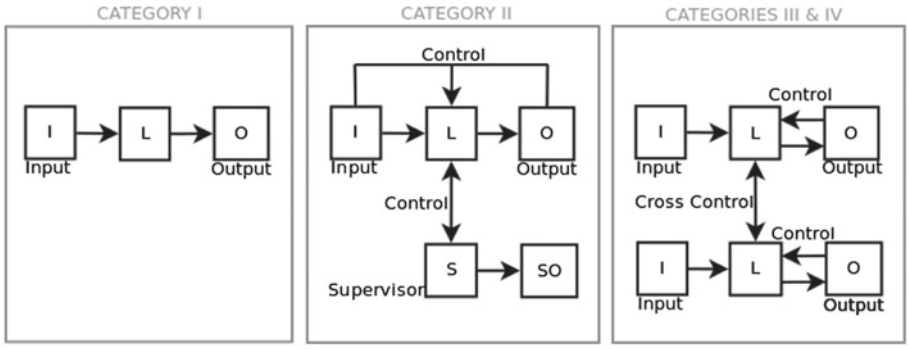


Figure 4. Control architectures derived from the risk analysis. Categories I, II and III/IV, respectively.

At all events, it is important to note that even if the guards are not able provide a full safeness range, the capacity of decreasing the exposition to the danger or reduce its effects is equally valid. That is why warning systems like horns or lighting are considered preventive elements, since they allow to increase the reaction time and the risk perception.

(3) Safety procedures: Procedures are required when it is not possible to adequately avoid neither to minimize the risks. They refer to all these activities related with every stage of the system, necessaries to guarantee a minimum safety level during the flight. Operating procedures affect both before, during, and after the mission.

First of all, verification (e.g. check batteries, scan frequencies in order to avoid interferences, measure wind speed, etc.) and signaling (e.g. notification to the authorities or people involved directly or indirectly, indications in the flight area, etc.) are mandatory before start the flight. During the mission development, it is also important to monitor the level, the data link performance, etc. in order to detect possible problems. Finally, a flight report should be filled out, in order to have a temporal register. It will help the maintenance process, since it will be possible to get, for example, real data about the motor or batteries use. Despite of being not deeply treated in the normative or in the safety procedures rules, maintenance plays a fundamental role on the global safeness. Its correct execution limits the probability of occurrence of a hazardous event. The activities that maintenance involves are cleanliness, reparations, replacement, adjustment, calibration, and verification.

Finally, not include in the maintenance process itself, but also perform before the mission, there are some activities or issues related with the specific education of the operators that increase the safety of the system. These procedures increase the expertise with the system and provide a good knowledge to avoid or manage hazardous situations: qualification, experience (e.g. simulators), and update.

4. Conclusions

Worldwide normative in the mUAV field is being improved quickly, spending a great effort on increase the safeness on these systems. Nevertheless, the work is not already finished, and the existing legislation are uncertain and loose. Safeness should be the first requirement in every system, and even more in those that can provoke a great damage.

Considering that plenty of systems are being develop regarding external risk avoidance (sense & avoidance), the main challenge is pointed in the internal ones. Risk Analysis Architectures have been studied, since they are the structures intended to reduce the risk levels. Among all of them, ISO 31000:2009 has been found as the most reliable and complete one, due to its feedback scheme and its combination of both deductive and inductive structures. Complemented by other regulations (ISO 14121-1:2007 and ISO/IEC 27005:2011), it has been focused and customized in order to be applied into mUAV outdoor missions. Drones' general features and scenario characteristics have been considered – basing on the international regulations – in order to provide with a guide for hazard analysis.

The three-step method (identification, evaluation, and reduction) provides iterative way for assessing and managing the actual hazards. Each one of the stages has been also adjusted to the mUAV scenario: drone's typical breakdowns have been studied and identified. They have been assessed according to their relevance and nature, using the methodology proposed in the standard. Nevertheless, the methodology has been refined and completed. Firstly, including intermediate categories that match better the mUAV reality (i.e. light/serious/destroyed instead reversible/irreversible). Secondly, proposing new metrics (i.e. number and affiliation of the agents involved) to evaluate the potential risk.

Finally, considering the drones capabilities, risk reduction alternatives have been studied. ISO 12100-1 has been followed, defining a multilevel architecture based on the evaluation done. Control systems and guards have been specifically adapted to mUAV.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

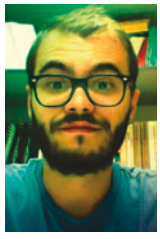
This work has been supported by the Robotics and Cybernetics Research Group at Technique University of Madrid (Spain), and funded under the projects 'ROTOS: Multi-Robot system for outdoor infrastructures protection', sponsored by Spain Ministry of Education and Science (DPI2010-17998), and 'Robot Fleets for Highly Effective Agriculture and Forestry Management', (RHEA) sponsored by the European Commission's Seventh Framework Programme (NMP-CP-IP 245986-2 RHEA). The authors want to thank all the project partners: Agencia Estatal Consejo Superior de Investigaciones Científicas - CSIC (Centro de Automática y Robótica, Instituto de Ciencias Agrarias, Instituto de Agricultura Sostenible), CogVis GmbH, Forschungszentrum Telekommunikation Wien Ltd., Cyberbotics Ltd, Università di Pisa, Universidad Complutense de Madrid, Tropical, Soluciones Agrícolas de Precisión S.L., Universidad Politécnica de Madrid – UPM (ETS Ingenieros Agrónomos, ETS Ingenieros Industriales), AirRobot GmbH & Co. KG, Università degli Studi di Firenze, Centre National du Machinisme Agricole, du Génie Rural, des Eaux et des Forèts - CEMAGREF, CNH Belgium NV, CNH France SA, Bluebotics S.A. y CM Srl.

Notes

1. Rotatory of fixed wing.
2. Autonomous adaptive/non-adaptive, monitored, supervised, and direct.
3. PRAM is the current RA standard used by the FAA's System Safety Handbook.
4. The scheme presented is a combination of the references described in ISO 14121-1:2007, ISO 31000:2009, ISO/IEC 27005:2011 and ISO/IEC 31010:2009. Nevertheless, the main core is included in ISO 31000:2009.

Notes on contributors

D. Sanz is currently a PhD candidate at the Universidad Politécnica de Madrid (Spain). He received both his BSc in Telecommunication Engineering and his MSc in Automation and Robotics from the Universidad Politécnica de Madrid (Spain). His main research interests are: Cognitive robotics, UAVs, Risk perception and avoidance and Wireless Sensor Networks.



J. Valente is a visiting professor at Universidad Carlos III in Madrid (Spain). He studied Computer and Electronics Engineering at Universidade Nova de Lisboa (Portugal) and received his PhD from the Universidad Politécnica de Madrid (Spain) in 2014. His main research interests are: Field robotics, Aerial robots, Path Planning, Navigation, and Control.

J. del Cerro is an associated professor at Universidad Politécnica de Madrid (Spain). He studied Industrial Engineering at Universidad Pontificia Comillas (Spain) and received his PhD from the Universidad Politécnica de Madrid (Spain). His main research interests are: Service Robots, Aerial Robots, GNC, and Multi Robot systems.

J. Colorado is an assistant professor in the Department of Electronics Engineering at Pontificia Universidad Javeriana in Bogota (Colombia). He studied Electronics Engineering at Pontificia Universidad Javeriana in Bogota (Colombia) and received both MSc and PhD degree from the Universidad Politécnica de Madrid (Spain) in 2010 and 2012, respectively. His main research interests are: Field Robotics, Bio-inspired Robotics, Micro Aerial Vehicles, and Control & Dynamics Modelling.

A. Barrientos is a full professor at the Universidad Politécnica de Madrid (Spain). He studied Electronics Engineering and received his PhD in Industrial Engineering (1986), both from the Universidad Politécnica de Madrid (Spain). Besides, he received MSc in Biomedical Technology (2002) from the Universidad Nacional de Educación a Distancia (Spain). His main research interests are: Service Robots, Aerial Robots, Biomedical engineering, and telerobotics.

References

[1] ISO. Iso 12100–1: safety of machinery – general principles for design. International Organization for Standardization. Technical Report; 2010.

[2] ISO. Iso 14121–1: safety of machinery – risk assessment. International Organization for Standardization. Technical Report; 2007.

[3] ISO. Iso 31000: risk management – principles and guidelines. International Organization for Standardization. Technical Report; 2009.

[4] ISO. Iso 13849–1: safety of machinery safety-related parts of control systems – part 1: general principles for design. International Organization for Standardization. Technical Report; 2006.

[5] IEC. IEC/ISO 31010: 2009. International Electrotechnical Commission. Technical Report. Switzerland; 2009.

[6] IEC. Iec 61000-3-2: limits for harmonic current emissions. International Electrotechnical Commission. Technical Report; 2004.

[7] ISO/IEC. Iso 18000: information technology – radio frequency identification for item management: International Organization for Standardization. Technical Report; 2008.

[8] ISO. Iso 19133: geographic information – location-based services. tracking and navigation. International Organization for Standardization. Technical Report; 2005.

[9] Hayhurst K, Maddalon J, Miner P. Unmanned aircraft hazards and their implications for regulation. In: 25th digital avionics systems conference, 2006 IEEE/AIAA; October; Portland, OR; 2006. p. 1–12.
[10] van Blyenburgh P. Unmanned aircraft systems: the current situation. In: Easa UAS workshop; February. Paris, France; 2008.
[11] Arjomandi M. Classification of unmanned aerial vehicles. Technical Report. Australia: The University of Adelaide; 2007.
[12] UAVM. What is the current regulatory status for civil uav commercial flight?; August; 2010. Available from: http://www.uavm.com/uavregulatory.html.
[13] Loh R, Bian Y, Roe T. Uavs in civil airspace: Safety requirements. Aerospace and Electronic Systems Magazine, IEEE. 2009;24:5–17.
[14] Scheneider W. Unmanned aerial vehicles roadmap 2002–2027. Office of the Secretary of Defense. Department of Defense of the United States of America. Technical Report; February; 2004.
[15] EASA/EC. Regulation 1592/2002 – annex 1 essential airworthiness requirements. EASA. Technical Report; 2002.
[16] FLYGI. Rules of military aviation (rml). Military Flight Safety Inspectorate – Swedish Armed Forces. Technical Report; September. Sweden; 2000.
[17] CASA. Ac 101–3: unmanned aircraft and rockets model aircraft. Civil Aviation Safety Authority. Technical Report. July. Australia; 2002. Available from: http://www.casa.gov.au.
[18] CASA. Civil aviation safety regulations (casr), part 101. Civil Aviation Safety Authority. Technical Report. Australia; January; 2004.
[19] DGA. Uav systems airworthiness requirements (usar). Delegue General pour l Armement, Ministre de la défense. Technical Report. France; January; 2005.
[20] CAAI. Uav systems airworthiness regulations. Civil Aviation Administration of Israel. Technical Report. Israel; 2006. Available from: www.caa.gov.il.
[21] JUAV. Safety standard for comercial-use, unmanned, rotary-wing aircraft in uninhabited areas. Japan UAV Association. Technical Report; January; 2005. Available from: www.juav.org.
[22] Haddon D, Whittaker C. Uk-caa policy for light uav systems (luas). Civil Aviation Authority. Technical Report. UK; May; 2004. Available from: www.caa.co.uk.
[23] FAA. Afs-400 UAS policy 05–01. Federal Aviation Authority. Technical Report. :USA; September 2005.
[24] Fitzgerald D, Walker R, Campbell D. Classification of candidate landing sites for UAV forced landings. Aiaa guidance, navigation, and control conference and exhibit; San Francisco, CA; 2005.
[25] Maneschijn A. A framework and criteria for the operability of unmanned aircraft systems [PhD thesis]. Stellenbosch, South Africa: Stellenbosch University; 2010.
[26] JAA/EUROCONTROL. Uav task-force final report. A concept for the european regulations for civil unmanned aerial vehicles (UAVS). JAA/EUROCONTROL. Technical Report; May 2004.
[27] Clothier R, Walker R, Fulton N, Campbell D. A casualty risk analysis for unmanned aerial system (UAS) operations over inhabited areas. In: Aiac12 – twelfth Australian international aerospace congress, 2nd Australasian unmanned air vehicles conference; Melbourne; 2007. Available from: http://eprints.qut.edu.au/6822/.
[28] Hokstad P, Steiro T. Overall strategy for risk evaluation and priority setting of risk regulations. Rel. Eng. Syst. Safety. 2006;91:100–111. Available from: http://www.sciencedirect.com/science/article/pii/S095183200400290X.
[29] Lough K, Stone R, Tumer I. The risk in early design method. J. Eng. Design. 2009;20:155–173.
[30] Stephens R, Talso W. System safety analysis handbook: a source book for safety practitioners. 2nd ed. System Safety Society; 1999.
[31] Rezakhani P. Classifying key risk factors in construction projects. Institutul Politehnic din Iasi. Buletinul. Sectia Constructii. Arhitectura. Technical Report 2; 2012.
[32] Saleem S, Abideen Z. Do effective risk management affect organizational performance. European J. Bus. Manage. 2011;3:258–267.
[33] FAA. FAA system safety handbook. chapter 9: analysis techniques. Federal Aviation Administration. Technical Report. USA; December 2000.
[34] Kuchar J. Safety analysis methodology for unmanned aerial vehicle (UAV) collision avoidance systems. In: USA/Europe air traffic management R&D seminars; Baltimore, MD; 2005.
[35] Ericson C, Li C. Fault tree analysis. Hazard Anal. Tech. Syst. In: System Safety Conference. Orlando, Fl; 1999. p. 1–9. Safety. 2000:183–221.
[36] Murtha J. An evidence theoretic approach to design of reliable low-cost uavs [Master's thesis]. Blacksburg, Virginia, USA: Virginia Polytechnic Institute and State University; 2009.
[37] Vesely W. Probabilistic risk assessment. In: Johnson SB, Gormley TJ, Kessler CD et al., Syst. Health Manage.: Aerospace Appl. Chichester: Wiley; 2011:253–263.
[38] Clemens P. 2002. Event tree analysis. JE Jacobs Sverdrup.
[39] Apthorpe R. A probabilistic approach to estimating computer system reliability. In: Proceedings of the fifteenth systems administration conference (lisa xv) San Diego, CA; 2001. p. 31.
[40] Mohr R. Failure modes and effects analysis. JE Jacobs Sverdrup; 2002.
[41] Roland H, Moriarty B. Fault hazard analysis. System safety engineering and management. 2nd ed. 2009. p. 223–225.
[42] Knowlton R. Introduction to hazard and operability studies: the guide word approach. Chemetics International Company; 1981.
[43] Oakland J. Statistical process control. Routledge; 2008.
[44] Celik S. Safety process implementation for unmanned aerial systems. In: Dale C, Anderson T, editors. Achieving systems safety. Springer: London; 2012. p. 43–53.
[45] Wilson P. Root cause analysis: a tool for total quality management. ASQ Quality Press; 1993.
[46] Casarosa C, Galatolo R, Mengali G, Quarta A. Impact of safety requirements on the weight of civil unmanned aerial vehicles. Aircraft Eng. Aerospace Tech. Int. J. 2004;76:600–606.
[47] Raspotnig C, Opdahl A. Comparing risk identification techniques for safety and security requirements. J. Syst. Softw. 2013;86:1124–1151.
[48] Clothier R, Walker R. The safety risk management of unmanned aircraft systems. In: Handbook of Unmanned Aerial Vehicles; Springer; 2014.
[49] Johnson C. The hidden human factors in unmanned aerial vehicles. In: International systems safety society conference; Baltimore, MD, USA; 2007.
[50] Cork L, Walker R, Dunn S. Fault detection, identification and accommodation techniques for unmanned airborne vehicles. In: Australian international aerospace congress; Melbourne:

Australian International Aerospace Congress (AIAC); 2005; Melbourne.
[51] Hayhurst K, Maddalon J, Miner P, et al. Preliminary considerations for classifying hazards of unmanned aircraft systems. NASA TM-2007-214539, National Aeronautics and Space Administration. Technical Report. Hampton, Virginia: Langley Research Center; 2007.
[52] Dermentzoudis M. Establishment of models and data tracking for small UAV reliability [Master's thesis]. Monterey, California, USA: Naval Postgraduate School; 2004.
[53] FAA. Faa system safety handbook. appendix b: comparative risk assessment (CRA) form. Federal Aviation Administration. Technical Report. USA; December 2000.
[54] Dalamagkidis K, Valavanis K, Piegl L. Evaluating the risk of unmanned aircraft ground impacts. In: 2008 16th mediterranean conference on control and automation; June; 2008. p. 709–716.
[55] Van der Cruyssen C. Risk assessment guidelines. FPS Economy – Quality and Safety Deparment. Technical Report. The Netherlands; December 2007.
[56] Jaeger C, Renn O, Rosa E, et al. Risk, uncertainty, and rational action. Earthscan/James & James; 2001.
[57] Lough K, Stone R, Tumer I. Failure prevention in design through effective catalogue utilization of historical failure events. J. Failure Anal. Prev. 2008;8:469–481.
[58] Babut G, Moraru R, Cioca L. Kinney-type methods: usefull or harmful tools in the risk assessment and management process? In: International conference on manufacturing science and education; October; Sibiu, Romania; 2011.
[59] Kinney G, Wiruth A. Practical risk analysis for safety management. DTIC Document. Technical Report; June; 1976.