Preprints.org

Article

Not peer-reviewed version

A Hierarchical Quantitative Risk Assessment Framework for Evaluating Performance and Resilience in Drone-Assisted Systems

Nektarios Fotiou *, Konstantinos Katzis, Stavros Katsaronas, Hamed Ahmadi

Posted Date: 31 March 2026

doi: 10.20944/preprints202603.2408.v1

Keywords: aerial systems; analytic hierarchy process; assets; drone-based systems; impact; risk analysis; threats; unmanned aerial systems (UAV); vulnerabilities

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

A Hierarchical Quantitative Risk Assessment Framework for Evaluating Performance and Resilience in Drone-Assisted Systems

Nektarios Fotiou [1,*], Konstantinos Katzis [1], Stavros Katsaronas [1] and Hamed Ahmadi [2]

[1] Department of Computer Science and Engineering, European University Cyprus, Nicosia, 2404, Cyprus

[2] School of Physics Engineering and Technology, University of York, YO10 5DD, United Kingdom

* Correspondence: nf172496@students.euc.ac.cy

Highlights

What are the main findings?

- A novel quantitative risk analysis methodology directed towards drone-assisted services integrates established risk assessment frameworks with a multi-level hierarchy structure to model dependencies among the defined risk parameters of assets, vulnerabilities, and threats.
- The model incorporates risk parameters and interdependencies between systems' components, environmental factors, and operational constraints to quantify and prioritise dynamically changing failure scenarios.

What are the implications of the main findings?

- The study presents a risk assessment model, and a use case of a drone-assisted delivery system demonstrates its efficiency in systematically evaluating and prioritizing the most critical risk contributors to system performance degradation.
- Findings support improved awareness of technical, environmental, safety, and security risks, empowering proactive measures and mitigation strategies during the planning phase for resilient drone-assisted operations.

Abstract

Rapid integration of UAVs into multiple sectors involving military, commercial, and civilian applications introduces new operational capabilities but also raises critical safety, reliability and resilience challenges. This paper presents a quantitative risk assessment approach for evaluating the performance and resilience of drone-assisted systems. The methodology is based on existing assessment frameworks and combines established standards with the principles of the multi-criteria hierarchy concept. The proposed approach models the interactions between systems' components, environmental factors, structural limitations and operational uncertainties to identify potential failure scenarios and quantify their impact. A qualitative analysis is performed to identify and register the required risk elements of assets, vulnerabilities, threats, likelihood, and impact. Following this, a hierarchical model is developed to define the dependencies among them and enable their quantification. To demonstrate the applicability and feasibility of the proposed methodology, a drone-assisted delivery system is examined, showcasing its effectiveness in identifying hazards, evaluating critical risk elements and quantifying risk events. The results indicate the significance of the methodology in ranking the verified risk elements and identifying those that made the greatest contribution to system failure. Also, it highlights that weather-driven and power-related elements are among the most significant contributors to performance deterioration.

Keywords: aerial systems; analytic hierarchy process; assets; drone-based systems; impact; risk analysis; threats; unmanned aerial systems (UAV); vulnerabilities

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

1. Introduction

Unmanned Aerial Systems (UAS) have become a highly popular technology, revolutionizing applications across the military, civilian, and commercial sectors [1]. These flying robots have promoted the development of several applications owing to their ease of deployment, low maintenance costs, high mobility, and ability to hover [2]. Such systems have been utilized as platforms for delivering multiple emerging technologies, such as Internet connectivity [3], mobile communications delivery [1,4], surveillance for border or essential side monitoring [1], emergency broadband services for disaster relief [5,6], navigation augmentation [7], atmospheric research [8], border control [9], and delivery of goods [10,11]. The advent of UAS has brought significant benefits; however, their widespread use has introduced serious challenges that hinder deployment. Specifically, when operating in an open environment under conditions of uncertainty, aerial systems are exposed to numerous natural, man-made, and structural threats, impeding the accomplishment of their objectives and degrading their performance. According to [12] and [13], UAS can be vulnerable to hardware attacks (adversarial direct access to the drone's components), wireless attacks (violation of the communication link to capture data or gain full control of the vehicle), and sensor spoofing (jamming or GPS spoofing). Furthermore, the deployment of aerial systems might indicate a significant number of other safety hazards and risks. System loss or failure, loss of control, loss of transmission, collision with terrestrial or aerial objects, failure or loss of navigation system, rotor failure or malfunction, take-off and landing incidents, damage caused by harsh weather and environmental conditions and power failure are some examples of hazards stated in [14–16]. With this in mind, aerial systems should be considered as dynamic cyber-physical systems of systems containing multiple components: sensors, communications, computation and control modules that communicate using wireless communication channels [1,17–19]. The multi-variety and complex factors implemented in their utilisation make aerial systems more prone to safety and security risks that might jeopardize their performance and resilience. Thus, assessing performance, reliability and resilience should be considered as a core requirement. Without a clear understanding of the potential risks, the use of aerial systems, especially for commercial and civilian applications, will not be possible at an acceptable level.

1.1. Problem Statement

Risk management is one of the main steps in nearly all projects and organizational processes. In the UAS field, it is necessary to employ a comprehensive risk analysis methodology, based on the objective of their utilisation [20]. Such analysis should be an ongoing process of assessing risks that exist to regulate safe application and ensure the system's effective functioning under uncertain and hazardous conditions. Over the years, various methodologies and frameworks have been proposed to assess and to show how risk assessment concepts have been conceptualised. Among the generic and well-regarded risk assessment frameworks are: NIST SP800-30 [21], ISO/IEC 27005 [22], EBIOS [23,24], ENISA [23], OCTAVE [25], CRAMM [26], FAIR [27,28] and SORA [29,30] (the reader may refer to the related guidebooks regarding their methodology, principals, and main objectives of the frameworks). The literature reviewed revealed that a variety of risk-analysis frameworks and standards are aimed at helping organisations assess risks. Some of them are considered enterprise-wide approaches, such as OCTAVE and FAIR, while others are countered as institutional standards such as ISO and NIST. In addition, among the reported frameworks, SORA is the only methodology targeting drone flights; however, it is a qualitative approach that cover the safety-related aspects of drone flights such as ground risk (harm to people on the ground if the drone crashes) and risk of collision with other aircraft in the airspace. Moreover, it was shown that some frameworks could be implemented independently (ISO, NIST and CRAMM). It has also been pointed out that some of the identified frameworks could serve as guidelines (ENISA) or supplementary tools compliant with other approaches (EBIOS and FAIR). In addition, the presented risk assessment methodologies refer to several different applications, complex critical infrastructures or interdependent systems. The

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

"one-size-fits-all" approach of existing frameworks may fail to accommodate the processes and requirements of aerial systems. In addition, while the established frameworks have their benefits, they need to be better suited to the unique requirements, peculiarities, and complexities of advanced aerial systems to serve the objective of the study, that is: evaluating the performance of a drone-assisted system. Consequently, the complexity and increasing interdependencies specific to modern aerial systems render the existing assessment methods very difficult to evaluate. None of these is suitable in its current form for the risk assessment of complex drone-based systems. Many researchers have proposed methodologies, particularly for quantitative risk assessments of systems or critical infrastructures and processes. Reviewing several references that address the issue, different approaches have been proposed: the probability theory [31], stochastic theory (Markov processes, semi-Markov processes, branching processes), Petri nets theory, Bayesian Networks [32], the theory of fuzzy set [31] (pp. 19-27), [33,34], Analytic Hierarchy Process (AHP) – Fuzzy Analytic Hierarchy Process (FAHP) and Fuzzy Comprehensive Evaluation (FCE) [35].

Many studies have explored the risk assessment of aerial systems. For instance, the authors in [1], discussed Federal Aviation Administration (FAA) pre-flight assessment process in which a Safety Management System (SMS) is implemented for the identification of risks and the adoption of a risk mitigation strategy to ensure the safe flight of a UAS [36]. Additionally, researchers in [37], introduced a safety assessment process framework for UAVs using Petri nets. Moreover, the authors of [15] aimed to develop a qualitative scheme for risk assessment of UAVs based on specific services and communication infrastructure. Their aim was to provide a preliminary assessment framework to describe and formalise a UAV's risk assessment. Similarly, [38] presented a four-phase qualitative risk assessment model for an aerial system. The proposed model was implemented to assess the safety of a quadcopter drone [39]. Additionally, researchers in [40] deals with the complex human-machine environment aiming to identify, classify and mitigate the errors of human factors involved in aerial system accidents. Also, the authors of [41] proposed a computational framework for decision-making under uncertainty, to facilitate the autonomous and safe operation of small drone-like unmanned aerial systems. The framework is based on the identification of risk factors, such as dynamic obstacles and battery drains, the estimation of the likelihood of occurrence, and the classification of feasible trajectories, according to the level of safety. Furthermore, [16] it presents a preliminary safety risk assessment, through the application of a qualitative safety risk management process followed by a Bayesian Network-based probabilistic risk estimation methodology. In addition, [42] deals with a qualitative assessment of risks, vulnerabilities and safety countermeasures of aerial systems deployed to support the transportation industry. Additionally, [1] proposed a framework for the safety assurance of drones over the Internet. More precisely, it provided a functional safety methodology for drone crashes based on a qualitative safety analysis followed by a quantitative approach using Bayesian Networks (BN). Reference [43] introduced a framework named Unmanned aircraft system Traffic Management (UTM) Risk Assessment Framework (URAF) developed to provide real-time safety evaluation and tracking capability by utilising Bayesian Belief Networks (BBNs). In addition, the authors in [44] provided a cyber security threat analysis and modelling of an aerial system. By following a goal – oriented approach for security analysis, they constructed a threat model based on threat – related concepts to describe potential attacks on the system and possible paths pertaining to these threats. Finally, using network simulation analysis, they attempted to estimate the likelihood of each attack and how different attacks would affect the system. Furthermore, references [45,46] presented a quantitative and qualitative risk analysis of UAV flights for construction job sites. Initially, a qualitative risk assessment was presented by combining a theoretical approach (reviewing aviation regulations and safety specifications of UAV flights on a construction job site) and Monte-Carlo simulation to evaluate fatality risks. Apart from that references [47,48] are dealing with the application of AHP as a component of a mixed hazard analysis methodology related to aerial-based systems. The authors of [47], proposed a methodology that integrates hazard identification and expert judgment. On the other hand, [48] proposed a mixed-methods approach that relied on a comprehensive literature review and multicriteria decision-

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

making to evaluate the safety of drone-assisted projects. Finally, the authors in [13] presented a security assessment methodology for UAV services, based on generic risk assessment standard of NIST 800-30 complement with a penetration testing technique.

Therefore, even though there is literature available describing risk assessment frameworks and models, there is limited work done towards developing a modelled framework taking into consideration the factors consisting of the concept of 'Risk': assets, vulnerabilities, threat sources, probabilities and impact. This paper builds on the previous work presented in this section and proposes a practical model to evaluate and improve the effective deployment of drone-assisted systems, targeting a variety of UAS, and assisting in quantitatively assessing the system's performance. Specifically, the study follows a combination of approaches: (i) a qualitative analysis of risk factors, followed by a (ii) quantitative assessment. By applying qualitative analysis, it produces the basis to gain all the necessary information (hazards and risk elements identification, dependencies among them, etc.) to conceptualize the quantitative component and determine the input data required to initialise the risk assessment. Subsequently, the quantitative approach is achieved by the implementation of a methodology that is identified as suitable and appropriate for application to specific UAV-type scenario and capable of providing numerical values for each identified risk element and potential failure scenarios. The proposed framework facilitates risk quantification using an identifiable set of factors based on a predefined set of requirements within the scope of the executed scenario.

1.2. Contribution

Motivated by the gap identified in the literature, that none of the commonly used risk assessment techniques is strictly targeting aerial systems within the context of risk elements of assets, vulnerabilities, threats, likelihood and impact, this paper expects to contribute to the body of knowledge and be significant in a number of ways. The main contribution of this study is to provide a straightforward and effective framework, demonstrating how qualitative risk analysis and a multi-criteria hierarchy approach combined with the fundamentals of pairwise comparisons, could be applied and integrated to systematically identify, and evaluate failure scenarios and related risk factors in UAV-assisted applications. In summary, this study contributes to the field of UAV performance and resilience as below:

- *Provides fundamental knowledge on UAV-based technologies, applications, and related risks*. This is beneficial for future research as it comprehensively serves as a resource for UAV-related hazards, weaknesses and challenges, which is an essential prerequisite for identifying and assessing risks of aerial platforms;
- *Gives an insight into the association of the components of a drone-assisted system and the identified vulnerabilities and threat sources*. This perspective allows practitioners to better understand interactions between systems' components, environmental factors, structural limitations and operational uncertainties. It also empowers experts to identify and quantify dynamically changing failure scenarios;
- *Illustrates a feasible risk assessment approach directed towards and tailored for drone-assisted services, by integrating established risk assessment standards and a multi-criteria hierarchy approach following the principals of pairwise comparisons*. The goal is to decompose the identified hazards into risk elements, establish the dependencies among them, assign numerical values and quantify them;
- *Verifies and classifies risk elements leading to the identified risks along with the relationships and dependencies between them*. The aim is to empower evaluators to verify and evaluate those risk elements that made the greatest contribution to system's operation, and quantify possible failure scenarios;
- *Presents a use case considering a drone-assisted delivery system as a testbed to verify the applicability and suitability of the proposed methodology.* The goal is to provide a useful tool for practitioners and operators, during the planning phase, to identify possible risks, evaluate their impact according

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

to the mission's parameters (e.g., services, type of aerial platform, area of operation, weather, regulations and operator's skills) and proactively take measures to mitigate them.

The remainder of this paper is organized as follows: Section 2 provides a summary of the concept of risk assessment and the terminology surrounding risk. In addition, it provides a brief overview of the frameworks selected for conducting the risk assessment. The proposed risk assessment methodology is described in detail in Section 3. Section 4 presents an illustrative use case to demonstrate the applicability and feasibility of the proposed method. Section 5 evaluates the most important findings of the research while Section 6 discusses the broader application of the proposal. Finally, Section 7 summarizes the main points of the study and provides concluding remarks and prospects for future work.

2. Literature Review and Background

2.1. Concept of Risk Assessment – Definition of Risk

Risk is considered as function of the adverse impacts that would arise if a circumstance or event occurs and the likelihood of occurrence [21]. In a similar way, the authors in [49] consider risk as the combination of what can happen, the probability of happening and the consequence (impact) if it does happen. Additionally, authors in [50], integrate the terms of 'Asset' and 'Vulnerability' to the explanation of risk, in order to express the entity upon which impact could be assessed to deal with and also to highlight that the term 'threat' by itself is insignificant in the absence of underlying vulnerabilities. Consequently, risk (R) should be expressed as a function of Likelihood (L) of a threat event (T), exploiting the vulnerability (V) and its severity, measured as its outcome impact (I), on an asset (A).

Equation (1) below expresses the definition of risk as stated in [50]. The subscript (i) is employed to distinguish between the different potential threat events (i=1, 2, 3, 4, …., N).

$$R = \{ < ((V(Ti,) Li, A(Ii)) > \} (1), \quad (1)$$

Below is a summary of the elements consisting of the concept of risk:

- *Risk*, as defined above and stated in [21,50] bullet;
- *Asset* is any tangible or intangible valuable unit of a system including hardware, software, interfaces, data and information, system mission, processes, person support, image or reputation, system and data criticality and sensitivity [51]. Also, environment/environmental conditions that the system resides in and the dependencies among the other assets should be considered as assets, as well bullet;
- *Vulnerability* is a weakness of an asset, due to the lack of or ineffectiveness of controls that could be exploited by a threat source [22]. A vulnerability could also emerge naturally as systems functions evolve, environment of operation changes, new technologies emerge, or new threats arise [21];
- *Likelihood of occurrence* is the probability that a given threat can exploit a given vulnerability [21,22];
- *Impact* from a threat event defines the magnitude of harm that can be expected to result from the consequences [21]. Such impact is assessed in terms of the system's performance and resilience.

2.2. Selecting the Most Appropriate Risk Assessment Approach

The aim of this paper is to suggest a hybrid methodology for the risk analysis of drone-based services. To conduct the qualitative analysis, we apply an asset-based approach that could serve the main objective of the study of constructing a risk assessment methodology based on the risk elements of assets, threats, vulnerabilities and impact [22]. Such an approach empowers the identification and classification of the risk elements with an emphasis on critical assets and highlights the dependencies and interactions among them. Consequently, if all valid combinations of assets, threats and vulnerabilities can be enumerated within the scope of the assessment, then, all the risks events can

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

be identified and evaluated. A combination of NIST 800 – 30 [21] and ISO 27005 [22] frameworks is selected to identify those factors that are affecting the utilisation of an aerial system. As stated in [23,52,53] both frameworks complement each other. As pointed out in [50], NIST 800 – 30 is developed to target federal information systems. Moreover, it is a flexible, explanatory and repetitive approach aim at identifying the risk elements. Regarding ISO 27005, it supports the general concepts of risk assessment and is designed to assist in the proper implementation of information security based on a risk management approach. Moreover, compared to the NIST approach, the ISO framework provides flexible guidelines for technology, people, and processes. Integrating both frameworks into a single analysis should create a robust framework, that allows the construction of a comprehensive qualitative analysis that meets the objectives of this study. In addition, implementing the explanatory recommendations, lists, and tables, outlined in both documents should be useful for collecting the qualitative information needed.

To fulfil the quantitative part of the proposed framework, the Analytic Hierarchy Process (AHP) is implemented [54–56]. AHP combines qualitative analysis with quantitative investigation [57]. The main idea is the abstraction of a system into several levels and the decomposition of the objective to a set of elements [58–60]. In a typical hierarchy the top level reflects the focus of the problem. The elements at each level are of the same order of magnitude and must be capable of being related to some or all the elements in the next higher level [61,62]. The pair-wise comparisons between the elements in each layer are conducted from starting at the top of the hierarchy and working down. The preferences between two elements are initially expressed verbally, then translated into an absolute numerical scale from 1 to 9 [56]. Finally, the relative weight of each element and the composite weights are calculated by aggregating the weights through the hierarchy. Within the context of this paper, AHP should serve as an appropriate method for decomposing risk into elements, arranging them into an hierarchy and evaluate them [61,63,64]. Each layer should consist of elements of the same order (assets, vulnerabilities, threats and impact) Also, the hierarchical structure should serve as the basis for demonstrating the dependencies and connections among the different risk elements. Therefore, from a risk assessment perspective, AHP should facilitate the grouping of the risk elements and their establishment into layers. Furthermore, the ability of AHP to serve as an effective method combining qualitative investigation with quantitative analysis could assist their comparison and evaluation based on their criticality, importance and on the level of risk they pose to the successful deployment of an aerial-assisted system [48,65]. Ultimately, the evaluation of the composite weights should assist in establishing and quantifying the failure scenarios threatening the performance of the system.

2.3. NIST – ISO Standards for Risk Assessment

The implementation of the NIST 800-30 and ISO 27005:2022 frameworks lead to the identification and registration of the elements required for the risk assessment process. References [21] and [22] provide an excessive presentation and implementation of these standards. However, application of these standards, exclusively for risk analysis of aerial platforms, either in combination or individually, has not been identified in the literature. In this paper a combination of the two frameworks should support the intension of the qualitative stage for the implementation of an asset-based approach and the enumeration of the combinations among system's assets, threats and vulnerabilities within the scope of the risk assessment. The following steps should be implemented: Risk Identification, Asset Identification, Threats Identification, Vulnerability Identification, Likelihood Determination, Impact Assessment and Risk Determination. In how these steps should serve the objectives of the paper are presented in Section 3.1.

2.4. Analytic Hierarchy Process for Risk Assessment

According to the reviewed literature, AHP is applicable and suitable for conducting quantitative risk assessment. Authors in [61] proposed multi-layer, AHP-based assessment to evaluate and prioritise risk factors influencing project management through pairwise comparisons. Similarly,

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

authors in [64] aimed in evaluating uncertain factors such as weather changes, aircraft failures, and employee status, all contribute to the occurrence of aviation accidents through the implementation of an AHP-risk assessment model. Likewise, authors in [66] sited in [64], implemented a mixed-method approach to identify and evaluate risks of productivity management in construction projects. Apart from that in authors in [67] established a 2-layer hierarchy to evaluate Confidentiality, Integrity and Availability (CIA triad) of information systems. Also, a probability distributions approach was applied to identify vulnerabilities and threats and to calculate the associated risk levels. A different approach is followed by authors in [68,69]: by employing a 3-layer AHP scheme followed by the application of Fuzzy Comprehensive Evaluation (FCE) aimed to assess the risks of an information system. In the same way, Fu and Zhou in [70] and Lee in [35] combined AHP with FCE for information security risk evaluation, through the formation of a 3-layer hierarchy consisting Assets, Threats, Vulnerabilities and Safety Measures. Beyond the literature mentioned above, some other references at which authors were proposing AHP as a risk assessment approach are listed below: Mustafa and Al-Bahar [62] investigated the subject of risk assessment in construction projects by presenting a AHP scheme for classifying various sources of risk and introducing a layer consisting of different levels of risk. Moreover, Tsai and Huang [71] presented a risk assessment method for wireless networks through the design of a 4-layer analytical hierarchy from the perspectives of the risk, security requirements, attacks and controls and the dependencies among them. Furthermore, Zhao et. al [72] developed a synthetical risk assessment model based on AHP theory to evaluate hazards. Practically, their model determined the impact weights of probability and severity by using pair-wise comparison matrices and calculates risk by evaluating them. In addition, Siddayao, Valdez and Fernandez [60] proposed a model for flood risk analysis based on Fuzzy AHP to calculate the relative weights of different flood risk factors. In [55], Aminbakhsh, Gunduz, and Sonmez, proposed a framework to assist in safety risk assessment and accident/injury prevention by adopting AHP conjointly with the Cost of Safety (COS) model. Fundamentally, a safety risk management framework was presented, for effective administration of safety risks by using a multi-criteria comparison technique. The proposed approach used the AHP method to decompose the decision problem into a hierarchy of more easily comprehended sub-problems, to compare the risk factors and to assign weights allowing their reliable prioritisation. Apart from that references [47] and [48] were dealing with the application of AHP as a component of a mixed hazard analysis methodology related to aerial-based systems. Authors in [47], were proposing a systematic methodology, which integrated hazard identification, expert judgment and risk assessment for preliminary hazard analysis in a drone-assisted inspection system. Authors in [48], proposed a mixed-methods approach that relied on a comprehensive literature review and multicriteria decision-making to compare and evaluate the identified risk causal factors, based on the level of risk posed to the successful application of the drone-assisted system.

3. Proposed Risk Assessment Methodology

The purpose of the paper is to conduct a risk assessment methodology for a drone-based system, mainly focusing on civilian drone-assisted operations. At first the potential risk factors need to be identified and then risks are ranked based on their magnitude. A core requirement is the identification and registration of the risk elements, which the drone-based system might encounter during an operation. To formulate the combined risk factors' sets, each of the potential factors that affect the system's utilisation need to be determined. That being so, a drone-assisted system is considered to be an integrated system with operators, equipment, and environment. According to [48], resilience and performance of a system are affected by a set of parameters related to the behavior of the different components of the system. Consequently, considering the integration of a drone-assisted system, the performance of the system is affected by various factors that are part of this system. According to this, the risk factors associated with drone application are classified into five categories, based on their sources: (1) drone-related, (2) environment-related, (3) operators'-related, (4) mission-related, and (5) operating area-related. Our methodology consists of two main

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

components: the qualitative component, implemented by the application of the basic guidelines of NIST and ISO standards and the quantitative component, employed by the execution of the basic principles of the AHP. The first approach involves assessing various conditions that can affect the system's performance. We conduct an analysis based on NIST [21] and ISO [22] standards, to identify the hazardous conditions, along with their possible causes and their consequences that affect the effective operation of the system. In addition, employed assets are listed, associated vulnerabilities are documented, potential threats are recognized, and possible impact effects are associated with those threats, in terms of resilience and performance requirements. The second approach is a quantitative estimation method based on AHP, which is used to model the risks factors related to drone-assisted system operation and to evaluate the risk scenarios threatening the system's performance and resilience. A multi-layer hierarchy is designed based on the outputs of the qualitative analysis. The implemented AHP is used to estimate the level of importance of each risk element. It also enables the formation of relations between them. This model defines the relationship between the elements of one layer with elements of a nearby layer and most importantly enables the employment of the importance of each layer's elements with all other related elements. In other words, the importance for each risk factor is calculated using the AHP approach and is correlated and affected by the importance of all the associated hierarchy elements. Given these considerations provided, the proposed framework empowers the final ranking of the verified failure scenarios and their impact considering defined connections and relationships. Also, the quantitative approach enables us to identify high risk pathways, detect and classify the most influential factors. In what follows, we will present the mixed-method framework, by first describing the qualitative component of the proposed methodology, followed by the AHP-based component. Workflow is illustrated in Figure 1.

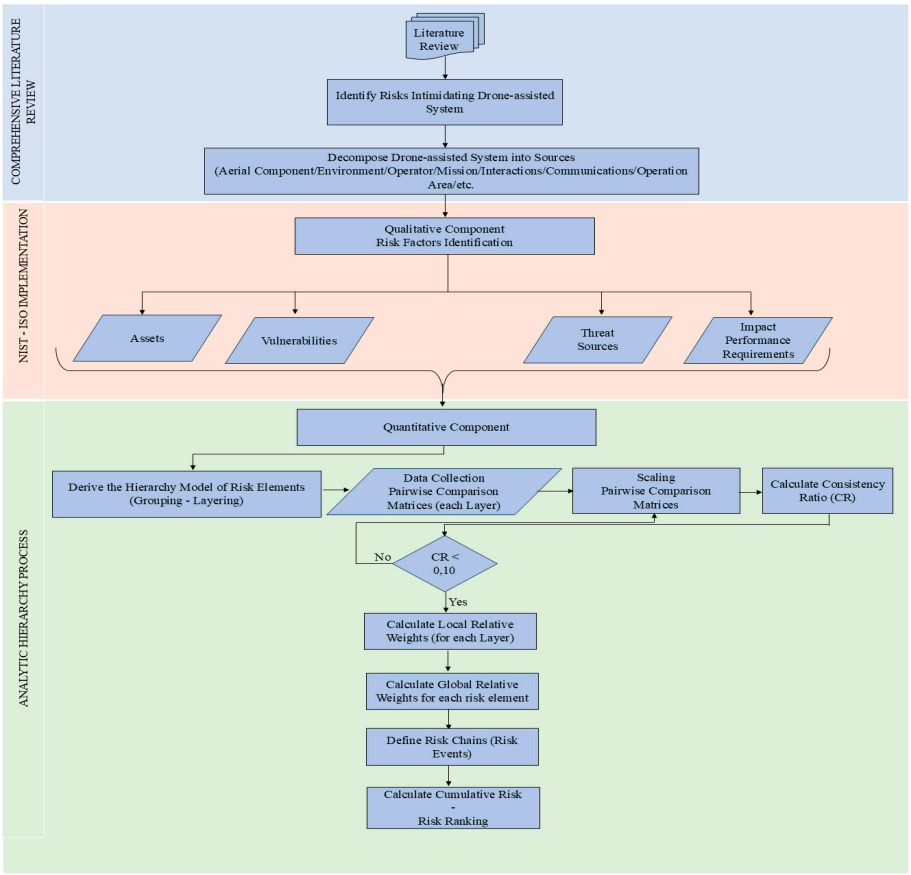

Figure 1. Proposed Framework Workflow.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

3.1. Qualitative Component

Prior to the application of NIST-ISO assessment, the potential hazards intimidating system's performance as well as the causal factors are identified through a comprehensive review of relevant scientific publications. Such references were identified and studied by mostly using scholarly databases named Google Scholar, IEEE Explore, MDPI and ScienceDirect. The selection of the available references was made among the most recently published articles in journals and conferences that discuss the risks associated with the use of drone-based systems. As revealed from the literature, the diverse application of aerial systems poses different types of risk:

1. *Aerial Component-related risks*: These are the risks associated with the aircraft and sensors mounted on it [48]. Inappropriate pre-flight inspection is a reason leading to a system's failure [73]. Furthermore, deterioration in the performance of the aircraft due to sensors malfunction should be considered as an aircraft-related risk [17]. Other risk sources related to the aerial component include, errors in navigation system [1], flying close to buildings or at a low altitude [16,47,74], lack of necessary and high-performing technical features [48] and rotor failures [74,75];
2. *Power efficiency-related risks*: Ineffective power source is an issue under investigation. Current types of drones carry batteries for short-time flights [76]. So, energy consumption is an important challenge facing drone-assisted systems [77]. Also, since aerial systems are battery powered, limited energy or unreliable power management poses risks such as power loss, limited fight range, limited processing capabilities and restrictions in flight time [2,78];
3. *Environment-related risks*: Environmental conditions pose a challenge to aerial systems and have become a tough and cardinal challenge (wind, temperature, icing, precipitation, hurricanes, etc.) [1,2,74,75]. The environment can negatively impact system's performance by creating situations that can lead to disruptions and mission failures [2,79]. Harsh weather conditions significantly increase the possibility of failure [12,14,15]. Rain, snow and extreme temperatures can threaten components such as sensors, frame and propellers causing malfunctions, failure or navigation problems [47]. Also, high illumination could disrupt the vision of both the operator and the system's sensors leading to accidents [48];
4. *Human operator-related risks*: Proper utilisation and safe operation during a system's deployment is highly dependent on the skills of the operator [74,75] Despite that operator's role can be limited to commanding and monitoring the system's activities, this does not make the system immune from human-triggered disruptions [79]. Lack of experience could make operators nervous, potentially leading to unsuccessful navigation. In addition, insufficient training might cause improper utilization and navigation of the system [73]. Moreover, lack of awareness, fatigue and stress are factors that lead to accidents [1,74];
5. *Area of operation-related risks*: Airspace density is an important factor that might lead to hazardous events. Flying objects could strike the aircraft and cause damage or even worse lead to crashes [48]. Additionally, deploying an aerial system over unknown zones or diverse environments poses risks such as physical attacks, usurp control by malicious entities or cyber-attacks from hackers to gather data or steal the equipment [2]. Furthermore, operating a drone-assisted system over non-segregated airspace increases the risk of mid-air collisions resulting in fatal accidents [80];
6. *Mission-related risks*: These are harmful incidents that might arise from specific type of operation. For instance, operating to accomplish sensitive missions such as border patrolling or intelligence, surveillance and reconnaissance require the implementation of additional countermeasures to safeguard sensitive information; violation of such measures could lead to mission failure. Additionally, faulty operation leading to aerial systems falling from higher altitudes or flying very close to people could have a greater adverse effect on people or structures on the ground. Similarly, the absence of predefined operating procedures could cause misunderstanding and concerns to the operators [48];

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

7. *Communication-related risks*: Aerial systems are extremely dependent on wireless transmissions for navigation and information exchange [81]. Wireless communication is a primary target for cyberattacks [13]. These attacks aim at intercepting information or to gain access to the system. [82,83]. Lack of efficient security mechanisms, inadequate protection measures or authentication techniques carry risks such as inappropriate control, breaking the encryption of the communication to capture data [1,82,84];
8. *Regulation-related risks*: In protecting safety, security and privacy, specific regulations should be put in place. Safeguarding citizens' lives, drones' free circulation within specific boundaries should be the primary target of regulations [78]. Non-compliance with existing regulations such as unauthorised trespassing or flying below the minimum altitude or even carrying a payload heavier than the required are essential risk factors that should increase the probability of lethal consequences [47,48,73,74]. Moreover, unregulated drone traffic densities entail high risk of collision with other flying objects [85].

The qualitative analysis concludes with the risk elements establishment. Considering the definition of risk defined by Equation (1), the steps stated in Section 2.3 are as follows:

- *Asset identification*: Asset analysis is performed by counting the entire system. Relationships between assets and importance on the mission accomplishment are also defined. Comprehensive illustration and justification should be presented in a forthcoming section;
- *Vulnerability Identification*: Assets are examined separately and a list of vulnerabilities that could be exploited is defined. The product of this phase should be applied to the evaluation of the importance and criticality of each vulnerability. Lists provided by [22] could be used as supportive material and guideline;
- *Threat's identification*: Identified risk hazards are decomposed, and relevant threats are documented. Threats are classified into the categories listed in Table 1. This allows experts to correlate threats and vulnerabilities and to establish the required relationships and dependencies. The lists of typical threats provided by [21,22] help with the identification and documentation of the drone-related threats;
- *Impact Determination*: The adverse impact of threat events on a specific asset is determined. According to [21,86] impact on an information system is characterized by a set of security requirements. However, visiting the issues surrounding aerial platforms' performance an extensive set of requirements is defined: Confidentiality, Integrity, Availability, Reliability, Safety, Survivability and Maintainability.

The analysis is presented in a forthcoming section. The workflow risk analysis is conducted in a qualitative manner. A quantitative analysis in the form of a hierarchical multi-layer technic is implemented to enhance the qualitative analysis

Table 1. Threat Classification.

Threats' Category	Description
Accidental	Erroneous actions taken by individuals in the course of executing their responsibilities, e.g. erroneous operation, unsuccessful navigation/landing and loss of control.
Structural	Failures of equipment, environmental controls or software due to ageing, resource depletion or other circumstances, which exceed expected operating parameters.
Adversarial	Malicious individuals or groups that seek to exploit the system's components such as system reconnaissance and surveillance through physical observation, hardware interception and modification, spoofing, jamming, theft, unauthorised access to the equipment, eavesdropping, etc.
Environmental	Natural disasters and failures of critical assets, processes and links on which the system depends on, outside of the control of the system's users or administrators.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

3.2. Quantitative Component

In this part, we propose the quantitative element of the methodology which is based on a multi-layer hierarchy approach. In using the AHP to model the risk events, a hierarchical structure to represent their quantification problem is needed. To model the interactions between systems' components, environmental factors, structural limitations and operational uncertainties a multi-level structure of the risk elements is established. The qualitative outputs of the previous process are used as inputs at this phase. Also, essential pairwise comparisons are performed. AHP is implemented as below. The reader may refer to references [56,58,60] for background information.

3.2.1. Qualitative Outputs are Organized in a Hierarchical Manner

The elements of the hierarchy to reach the objective of the assessment are specified. The selected qualitative outputs are *assets, vulnerabilities, threats and requirements* [49,50]. These elements are classified and organised into a 5-layer hierarchy. Figure 2 illustrates a generalised form of hierarchy.

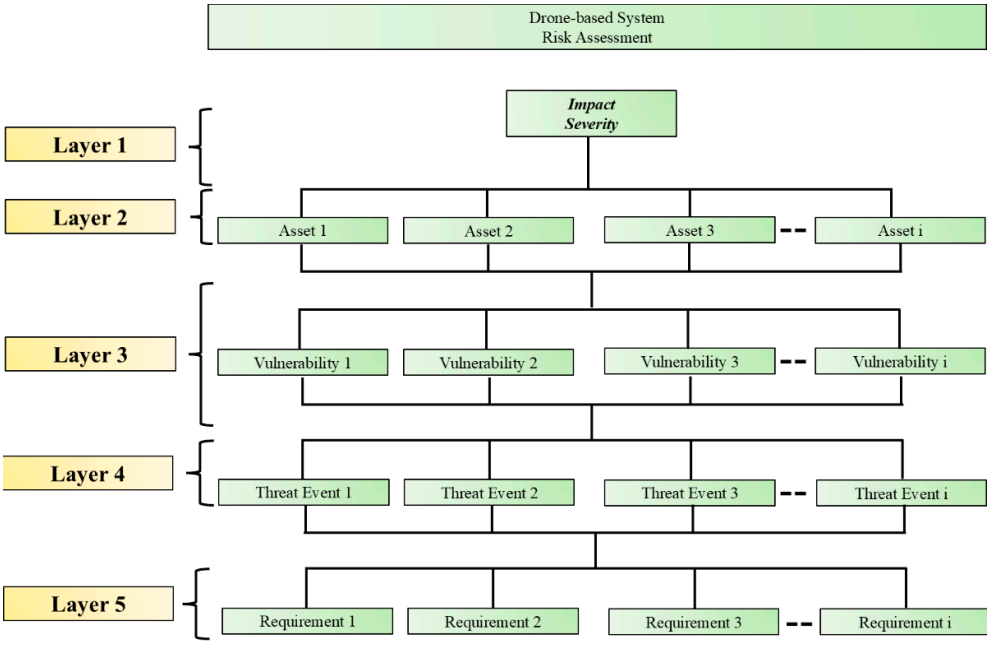

Figure 2. Multi-layer Hierarchy (Generalized form).

3.2.2. Schematic Representation of the Decision Hierarchy

A multi-layer hierarchy is formed based on the risk elements identified and classified through the qualitative processes. As stated above, the elements of assets, vulnerabilities, threats and performance requirements are organized and presented as different layers of the hierarchy. Among them multiple connections and relationships are detected and demonstrated. As illustrated in Figure 2, the top layer of the model represents the overall goal of the hierarchy: impact severity which threatens system's performance and resilience. The 2nd layer represents the assets that contribute to the system's function, thus used to evaluate assets. The 3rd layer represents the vulnerabilities identified by asset; each vulnerability inherits context from its parent asset. The 4t layer is constructed to introduce threat sources intimidating the entire system; in the diagram, they are linked across multiple vulnerabilities, forming a many-to-many relationship. Finally, the 5th layer is constructed to introduce the requirements denoting system's performance and resilience. Their placement at the bottom of the hierarchy reflects a goal-decomposition approach, i.e. these requirements must be met to maintain system functionality despite threats. This cross-layering association of elements is realistic and reflects the true nature of hazards, i.e. hierarchy effectively captures how vulnerabilities,

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

threat sources, and performance requirements relate to each asset under the common goal of impact severity. In addition, it follows the logic of the references cited above, which use AHP as a component of mixed hazard analysis methodology for the quantitative analysis of risks and the evaluation of the related risk factors.

3.2.3. Establishment of Relationships

Among the different layers, the proposed structure reflects the dependencies and relationships between the risk factors of each layer and addresses the dynamics of a critical drone-assisted system, as presented below:

- Assets have vulnerabilities. Vulnerabilities are exploited by threats, which in turn have an adverse impact thus affecting systems' requirements;
- A single vulnerability could be exploited by more than one threats [21];
- Risk materializes because of a series of threat events, each of which might take advantage of one or more vulnerabilities [21];
- Each threat event, according to its associated vulnerabilities, affects one or more of the system's assets;
- A threat source could have an adverse impact and affect the system in multiple ways, regarding the specified requirements. Similarly, every requirement can be affected by more than one adversarial threat source (many-to-many relationship;

A detailed analysis of the application of the constructed relationships and dependencies is presented in Section 4.

3.2.4. Pair-wise Comparison Matrices

Analytic hierarchy process is used to compare the importance between two elements and establish a judgment matrix where the dimensions of the matrix depend on the number of factors. In this paper, it is implied to establish 4 matrices: one for each layer. In each hierarchical level, the weights of the elements are calculated by performing the pairwise comparison process between the elements of each layer, according to their contribution to reaching the main objective of the hierarchy [67]. Equation (2) below, is a general form of the comparison matrix:

$$A = [a_{ij}]\ \text{n-by-n} \begin{bmatrix} 1 & a_{12} & \cdots & a_{1j} \\ \frac{1}{a_{12}} & 1 & \cdots & a_{2j} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1j}} & \frac{1}{a_{2j}} & \cdots & 1 \end{bmatrix}, \quad (2)$$

where: A is the pairwise comparison matrix, n is the number of compared elements and a_{ij} is the comparison weight between the elements a_i and a_j. In addition, reciprocal element a_{ji} is equal to $1/a_{ij}$.

3.2.5. Scaling Pair-wise Comparison Matrices

To derive priority matrices, comparisons need to be converted into integers. The values within the matrix are ratios between the elements and are determined based on the importance of each element in reaching the objective of the hierarchy. In creating the pairwise comparison matrix in this study, fundamental AHP comparison scales from 1 to 9 is employed to indicate how much one element is more important than another. Table 2 presents the numerical scale values and their equivalent intensities (verbal statements). Finally, a square matrix where each element value ranges from 1/9 to 9 is derived. The diagonal elements of the matrix are always equal to 1 whereas the non-diagonal elements capture the perceived relative importance of the corresponding elements [60]. To establish the importance of a risk element in the same layer, the following approaches are used as guidelines:

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

- The importance of every asset is evaluated based on its criticality, the way it contributes to mission accomplishment and the level of its susceptibility to threats (the more susceptible it is to multiple threat sources, the greater the possibility of failure; thus, it is considered more critical;
- A vulnerability is considered to be greater importance than another based on the ease of its exposure and exploitation, and on the level of its possible impact. Hence, its importance, over the other vulnerabilities, is weighted based on the number and criticality of the affected assets and also on the related threat sources; the more threat events are exposing a specific vulnerability, the higher is the level of concern;
- Every threat event is characterized by a level of effectiveness and capability [21], which is used to evaluate the threat's criticality. Therefore, is brought about that the more assets are affected by the initiation of a threat event the higher is the level of criticality of this specific threat source (higher criticality, more importance);
- According to [21], the likelihood of a threat event is not defined as a function in the statistical sense. Instead, assessors assign a score based on available evidence, experience and expert judgment. Consequently, in this study the likelihood of a threat event is embedded and evaluated through pair-wise comparisons of the elements of Layers 3 and 4;
- Impact is categorised by performance and resilience objectives and assessed based on the level of adverse effect [21,86]. Following the dynamic flow of information through the different layers of the hierarchy the level of impact is power-driven by the number of vulnerabilities exploited, the number of threat events intimidating the mission, and the quantity of requirements that are exposed.

Table 2. Fundamental Scale for Pairwise Comparison.

Intensity of importance	Definition	Explanation
1	Equal Importance	Two activities contribute equally to the objective.
3	Moderate importance of one over another	Experience and judgment favor one activity over another.
5	Essential or strong importance	Experience and judgment strongly favor one activity over another.
7	Very strong importance	An activity is strongly favored and its dominance demonstrated in practice.
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation.
2, 4, 6, 8	Intermediate values between the two adjacent judgments	When compromise is needed.
Reciprocals	If activity i has one of the above numbers assigned to it when compared with activity j, then j has the reciprocal value when compared to i.	
Rationals	Ratios arising from the scale	If consistency were to be forced by obtaining n numerical values to span the matrix
For the elements being closer together than indicated by the scale, judgments can use values such as 1.1, 1.2, …., or any other appropriate even finer value, for their pair-wise comparison.		

3.2.6. Calculating Priority Vector and Consistency Ratio

The Consistency Ratio (CR) is used to measure the consistency in the pair-wise comparison and also to evaluate the quality of expert judgments [35,60]. According to [35,58,60], for different matrices' sizes, the acceptable CR values has been set as: 0.05 for a 3-by-3 matrix; 0.08 for a 4-by-4 matrix; 0.1 for larger matrices. However, supposing that all knowledge has to be consistent contradicts the parameter of experience which requires continued adjustment in understanding. In the AHP, it is unrealistic to expect the assessors to provide consistent pair-wise comparisons. The reason is that inconsistency itself is substantial because without it, novel knowledge which might possibly lead judgments to change preference order, cannot be admitted. Thus, the objective of developing a wide-ranging consistent framework depends on admitting some inconsistency but not exceeding the threshold of 0.10 by very much. However, as discussed in [87], there are several other consistency

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

checks that are not associated with this threshold. It is also criticised that in the case of a large number of elements, the CR values defined by Saaty falls above 0.10, because of the application of the 9-point scale. According to Saaty [56], the CR can be estimated as follows:

$$CR=\frac{CI}{RI}\ , \tag{3}$$

CI is the consistency indicator, and RI is a random index, that is dependent on the sample size n, as shown in Table 3.

Table 3. Random Consistency Index (RI).

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41
n	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
RI	1.45	1.49	1.52	1.54	1.56	1.58	1.59	

Using the same approach, for the constructed matrices, CI is computed according to the following formula [56]:

$$CI=\frac{\lambda_{max}-n}{n-1}\ , \tag{4}$$

λ_{max} is the maximum eigen value and n is the number of elements of each matrix. λ_{max} is obtained as follow:

$$\lambda_{max}=\sum_{i=1}^{n}\frac{(AW)_i}{nW_i}\ , \tag{5}$$

and,

$$A\ X\times W=\lambda\ max\ \ X\times W, \tag{6}$$

$$A\ X=\lambda\ max\ \ X\rightarrow|A-\lambda I|=0\ , \tag{7}$$

In Equations (6) and (7) above, A is the comparison matrix resulting from (2), W is the stemmed vector of relative weights, I is the identity matrix, and X is a matrix obtained from the sum of the values of each column of matrix A. To obtain the eigenvector of the comparison judgment matrix W, we: divide the elements of each column of matrix A by the sum of that column. Then, to obtain the vector of relative weights (eigen vector) we add the elements in each resulting row (to obtain a 'row sum') and divide this sum by the number of the elements in the row. For a greater understanding, the next Section will follow a practical application of the formulas and present the above procedure with numerical examples.

3.2.7. Calculating Local Weights

The resulting vector W comprises the relative weights of the elements in each layer. The relative weight of an element indicates its local weight and represents the importance of this element compared with the other elements that meet at the same level. Nevertheless, this does not mean that an element that is ranked as of higher importance compared to the other elements in its layer will not necessarily have the highest priority in the risk assessment of the entire system. Considering the proposed many-to-many relationships and connections between elements, the local weights at each layer should be propagated across the hierarchy. For example, assume the local weight of vulnerability in layer 3. According to the number of assets linked to this vulnerability, the outcome importance should be changed, either decreased or increased. Bearing in mind what is mentioned above and considering the proposals referring to layering and the dependencies among the elements of the hierarchy, it is necessary to implement the calculation of global weights. According to [56], weighting the locally derived scales by the priority of the elements of the upper layer (parent layer) results in global derived scale.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

3.2.8. Calculating Global Weights

As Saaty mentioned in [56], when relative measurements are used in AHP and when the priorities of the elements of the different layers are set in advance, the final ranking at each layer depends on the number of elements of the nearby layers. To evaluate the final ranking of all elements of the hierarchy global weight is implemented. According to [47,56] global weight is the total importance of each element. The global weight is calculated by a typical AHP based on the hierarchy relationship of an element with its parent element (upper layer's relationship) and the cascading local weights [88]. Global weight is equal to the product of the local weight of this element and the local weight of its parent element [48,55,89]. Additionally, when an element is related to more than one element in its upper layer, the global weight results from the summation of the contributions of these multiple elements. As depicted in Figure 2, the first layer represents the objective of the hierarchy. The global weights of the assets (GWA) are calculated by multiplying the local weights of Layer 2 (Asset Layer) by the weights of its upper layer. Considering that Layer 1 represents the objective of the hierarchy, its derived local scale is considered to be the unit. Therefore, according to previous paragraph, GWA is equal to the assets' local weights (LWA). Regarding the calculation of the global weights of the vulnerabilities (GWV), the following equations are applied. In Equation (8), a vulnerability is associated with one asset; thus, its global weight (GWV) is calculated by multiplying its local weight (LWV) by with the local weight of the connected asset (LWA). In Equation (9), it is assumed that an identified vulnerability is related to two assets. In this case, the global weight of this specific vulnerability (GWV) results from the summation of the products of the local weights of the vulnerability (LWV) and the local weights of these two assets (LWA_i, …, LWA_j):

$$GWVi = LWVi \times LWAi, \quad (8)$$

$$GWVi = LWVi \times (LWAi + \ldots. + LWAj), \quad (9)$$

Similarly, Equations (8) and (9) are adapted to calculate the global weights for threat sources and requirements. Equations (10) and (11) illustrate the general form of the equations for estimating the threat sources' (GWT) and requirements' (GWR) global weights, respectively:

$$GWTi = LWTi \times (GWVi + \ldots.+ GWVj), \quad (10)$$

$$GWRi = LWRi \times (GWTi + \ldots + GWTj), \quad (11)$$

Calculating global weights is important because with relative measurement the calculated importance of any element and its priority, as well, might change when new elements are added or old ones deleted from any layer [56]. For example, assume that a new threat is identified. Based on the proposed framework, and the dependencies and relationships between the elements across the different layers, it is obvious that not only the ranking of the threat sources within the same layer would be altered but also the final ranking of the risk requirements should be affected as well. In conclusion, the proposed framework implements two different types of variables: local weights that reflect the relative importance among the elements within the same layer and introduces the concept of global weights. This function allows the propagation of relative importance across layers and enables the comparison of all elements compared to the goal of the hierarchy.

3.3. Define Risk Chains

At this stage, the identified risk hazards can be described as a chain of elements. According to [49,50], every recognized risk event is a function of an asset threatened by a threat, which in turn exploits a known vulnerability and has an adverse effect on the asset in terms of resilience and performance. Therefore, considering the general form of the proposed hierarchy (see Figure 2) every risk event is described by an *Asset - Vulnerability - Threat - Requirement* chain. Each chain starts with the objective of the framework, follows a route through every layer, and ends at a requirement by connecting one element per layer. Each chain denotes a risk chain and represents a specific risk

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

scenario that threatens system performance. For example, assuming the possible risk hazard of *'Low temperature might decrease the battery life of drones'*, mentioned in [47]. Following the procedure of qualitative analysis, it is concluded that the affected asset is the airborne component (drone/UAV). In addition, the possible threat source that might affect the asset is extreme weather conditions (low temperature) [21]. Additionally, the potential vulnerability that might be exploited is the ineffective power source. This is justified by the literature review. Temperature is considered to be the most influential indicator affecting the capacity of lithium-ion batteries' in cold weather which can cause the battery to drain faster [90], while extreme heat can lead to overheating issues [91]. Finally, the impact of the outcome on the system's performance should be either on the system's maintainability or survivability. In addition, it could be mentioned that extreme weather conditions could not only exploit ineffective power source, but also another vulnerability, that is defective components. In these cases, multiple risk paths can be identified and classified. Therefore, different vulnerabilities and threat sources can be defined and assigned to each resulting chain, substantially strengthening what is documented in [21], that the development of threat scenarios should exploit one or more vulnerabilities and that a set of vulnerabilities can be exploited by one or more threats. A detailed analysis of the possible risk hazards, risk chains and implemented risk elements is provided in Section 4 through the use case scenario.

3.4. Cumulative Risk Contribution – Risk Ranking

There is a need for a more defensible overview of the risk elements and how they drive total risk and can elucidate how a system's performance and resilience are affected. For this study, cumulative risk is employed. Specifically, cumulative risk evaluates the combined effects of multiple risk elements on the performance and the resources of a system [92]. As mentioned in [93] the term 'cumulative risk' refers to the combined risks from aggregate exposures to multiple agents or stressors. In this paper, the following features are considered: identified risk elements are treated as agents; risk elements act together rather than individually, thus exposing the system to numerous risk events; and the aggregation of the risk elements results in the evaluation of risks. The resulting outcome refers to the combined risk factors of exposure via all relevant pathways through multiple layers. It is applied to evaluate the portion of influence that each risk element has on the top-level layer of the hierarchy and is attributable to that factor, after the propagation of relative weights. The cumulative risk estimation is directed as follows:

- Compute local weights, following the steps of in Section 3.2.6 and 3.2.7;
- Estimate Global Weights, through the application of Equations (8) to (10);
- The desired risk chain is selected from the outcomes of the previous procedure conducted for the risk chain definition;
- The amount of influence of each element is defined which is attributable to its connected elements. To obtain a common numeric range/scale, and to allow aggregation into a final score, linear data normalization is selected [94]; each risk element influences and is influenced equally by its connected elements, thus in case of multiple parent nodes linear data normalization is applied [95]. Equation (12) expresses a general form of the function of the influence of a risk element on the elements of a lower layer. The influence of each factor is related to its importance (local or global weight). GW stands for global weight and $\sum \mathrm{GW}$ stands for the summation of the global weights, in the case of multiple elements of a higher layer connected to a single element of a lower layer:

$$\text{Proportion}\left(\text{parent} \rightarrow \text{child}\right) = \frac{\text{GW (parent)}}{\sum \text{GW (parents)}}, \tag{12}$$

- Multiply all proportional influences across a single pathway, starting from the assets layer and concluding to requirements layer. To better understand the above process numerical examples are provided in the following section of the study, based on the illustrative use case scenario.

  Numerical examples are provided in Section IV for a better understanding of the above process.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

4. Proposed Methodology Application – Illustrative Use Case

To demonstrate the proposed approach, a drone-based delivery use case is used to validate its effectiveness and applicability, as the drone delivery service is becoming an emerging topic for different companies and purposes [96]. This case is merely illustrative. The proposed framework may serve as the basis for other drone-assisted system applications across different types of drones. Specifically, it is assumed that a multi-rotor drone is deployed to serve a single customer in an urban area [13,97–99]. The system is deployed during daylight hours. The package to be delivered should not weigh more than 30kg. In addition, special consideration should be given to avoid damaging the parcel or degrading its contents. Therefore, rainy and windy weather, as well as extreme temperatures, pose considerable risk. During dispatch through a stationery warehouse, the parcel is loaded [98,100]. Additionally, the GPS coordinates of the destination are set, and a reliable communication channel is established [2]. Finally, the route of the drone is planned considering the flight distance, speed, weight of the payload, and external factors, such as wind speed and temperature [21,22]. The drone flies to the destination-customer throughout the shipment phase. The flight altitude is not considered higher than 200 m. Drone can fly over people, highways, and streets. When possible, the path of the drone will be planned above non-populated zones, and it might also fly over people to use the shortest path [1]. This is the most critical phase because the drone is exposed to significant risk sources such as weather conditions, barriers interfering with its route, undesirable obstacles, bad control, equipment malfunctions, unpredictable failures and malicious attacks [98]. Finally, the drone reaches its destination and landings occur. This process poses several risks, including malicious attacks, unintentional package drops, accidental damage to the package and human injuries. The DJI FlyCart 30 Package Delivery Drone is considered to have a reference system to implement the framework [101]. This drone was chosen based on its distinctive features: it is capable of delivering packages to homes, though built for more challenging and demanding scenarios, such as transporting cargo across challenging terrain [102]. As shown in Figure 1, in order to initialise the process, the first component of the methodology is the systematic use of all available information from journal articles, conference papers, surveys, and reports, and the analysis of the examined drone-based system. The goal is to identify and classify potential hazardous events and to decompose the system into sources: (i) equipment, (ii) area of operation, (iii) mission, (iv) environmental conditions, (v) communication means, (vi) humans' involvement, and (vii) relationships. To avoid repetition, the elements of the scenario are described at the beginning of this section, and potential hazards are presented in Section 3.1.

4.1. Use-Case Qualitative Component

In what follows, the qualitative component is implemented. Following the systematic process described in Section 3.1 and by employing the information revealed from the relevant literature and publicly available reports we choose the required risk parameters: (i) system's assets, (ii) vulnerabilities, (iii) possible threats and (iv) associated impacts. These parameters are used in the next step of the methodology to build up the hierarchical structure.

- *Assets' Identification*: This is the primary and most important step in an asset-based approach [21,22]. An aerial system is an interconnected system of systems, composed of a ground control system, airborne unit (including embedded sensors and subsystems) and a communication link [13,19,103,104]. In addition, human administration is considered a component of this system [17,77]. In addition, environmental conditions (weather), area of operation, and regulations are external elements outside the boundaries of the system but are capable of influencing its state. These should be considered as significant elements in governing the utilisation of an aerial system and potential sources of hazardous event. Consequently, for this study, the system's assets are: *Airborne Component (Drone), Ground Control Station* (Controller), *Communication Links (Wireless medium)*, *Regulations/Policies*, *Environmental Conditions*, *Operator* and *Area of Operation*;

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

- *Vulnerabilities' Identification*: The outlined vulnerabilities denote the system's limitations and susceptibilities due to the lack of or ineffectiveness of controls. Through the analysis, the potential vulnerabilities are as follows: *Ineffective Power Source*, *Power Consumption*, *Defective Components*, *Wrong Handling*, *Susceptibility to Wireless Attacks*, *Susceptibility to Weather Conditions*, *Lack or Violation of policies/regulations*, *Faulty Operation*, *Lack of Operators' Skills*, and *Susceptibility to Adversarial Actions*. The identified vulnerabilities associated with the system's assets are presented in Table 4 (see also Supplementary Material S1, for reference). As shown, several vulnerabilities are linked to multiple assets. Weaknesses are expected to be exploited sequentially or simultaneously; therefore, it is important to record multiple interconnections;

Table 4. Vulnerabilities (in association with the assets).

Assets	Vulnerabilities
Airborne Component (Drone)	Ineffective Power Source, High Power Consumption, Defective Components, Wrong Handling
Controller (Ground Control Station)	Defective Components, Wrong Handling
Communication Links	Susceptibility to Wireless Attacks, Defective Components, Susceptibility to Weather Conditions
Regulations/Policies	Lack or Violation policies/regulations
Environmental Conditions	High power consumption, Susceptibility to Weather Conditions
Operators	Wrong Handling, Faulty Operation, Lack of Expertise/Training/Skills
Area of Operation	Lack or Violation policies/regulations, Susceptibility to Adversarial actions

- *Threats' Identification*: Possible attacks, failures, man-made and natural events that compromise the system's functioning are defined along with their association with the identified vulnerabilities. Table 5 presents the threats intimidating system's performance along with the exploited vulnerabilities (see also Supplementary Material S1, for reference) [22]. Each threat is classified into one of the categories listed in Table 1. The identified threats are not limited to those that have been highlighted. For simplicity, the most frequently mentioned in the literature have been selected: *Power Failure, Equipment Failure, Control Loss, Wireless Attacks, Extreme Weather Conditions, Collision with Objects, Unsuccessful Navigation,* and *Physical Attacks (Unauthorised Access);*
- *Likelihood Determination*: Likelihood is treated as a score based on judgment; therefore, its estimation is embedded in the pair-wise comparisons of vulnerability and threat importance. Comparisons are analysed at the next step of the framework, through the utilisation of the quantitative component;
- *Impact Determination*: Impact of a threat event is the magnitude of harm expected to occur in the system after the exploitation of vulnerability. According to [21] the adverse impact of a threat might be capable of harming anyone of the system's sources: for the system's mission, a possible impact could be the inability to perform a specific function, for an asset could be a damage to it or the loss of the asset, for a human admin could be the damage of image or reputation due to lack of proper education or policies' violation, to the relationships could be any relational harm. The association between the identified threats and their potential impact on the related requirements of *Confidentiality, Integrity, Availability, Reliability, Safety, Survivability and Maintainability* is demonstrated in Table 5. Additionally, Supplementary Material S1 (Tables S3 and S4) provides information and a comprehensive explanation of the established requirements.

In summary, each threat source affects one or more assets, a single threat might exploit more than one vulnerability and a single vulnerability could be exploited by more than one threat; the more assets are affected, the higher the probability for the threat event to have an adverse impact; the more vulnerabilities are exploited, the higher the risk for the system to not accomplish its mission.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Table 5. Threats (in association with the vulnerabilities and potential impact).

Threats	Vulnerabilities	Impact on
Power Failure **(Structural Threat Event)**	Ineffective power source, Susceptibility to Weather Conditions, High power consumption, Susceptibility to wireless Attacks	Availability, Reliability, Survivability
Equipment Failure **(Structural Threat Event)**	Ineffective power source, Defective Components	Availability, Maintainability, Survivability
Control Loss **(Accidental Threat Event)**	High power consumption, Wrong Handling, Susceptibility to wireless Attacks, Susceptibility to Weather Conditions, Lack or Violation policies/regulations, Faulty Operation, Lack of Expertise/Training/Skills,	Availability, Safety
Wireless Attacks **(Adversarial Threat Event)**	High power consumption, Susceptibility to wireless Attacks, Wrong Handling	Confidentiality, Integrity, Availability, Maintainability
Extreme Weather Conditions **Environmental Threat Event)**	Ineffective power source, High power consumption, Susceptibility to Weather Conditions	Reliability, Maintainability, Survivability
Collision w/Objects **(Accidental Threat Event)**	Susceptibility to wireless Attacks, Lack or Violation policies/regulations, Faulty Operation, Lack of Expertise/Training/Skills, Adversarial actions	Availability, Safety, Maintainability
Unsuccessful Navigation **(Accidental Threat Event)**	High power consumption, Wrong Handling, Susceptibility to wireless Attacks, Susceptibility to Weather Conditions, Faulty Operation, Lack of Expertise/Training/Skills, Adversarial actions	Availability, Safety, Reliability
Physical Attacks (Unauthorised Access) **(Adversarial Threat Event)**	Lack or Violation policies/regulations, Susceptibility to Adversarial actions	Confidentiality, Integrity, Availability, Maintainability

4.2. Use-Case Quantitave Component

The quantitative component is focused on the defined risk elements and through hierarchical methodology attempts to quantify the classified hazardous events. By applying AHP the subjective preferences are transformed into quantifiable weight values in order to serve the objective in quantifying an aerial system's performance [61].

4.2.1. Hierarchy Construction

The identified risk factors are organised in the 5-layer hierarchy model already presented and comprehensively described in Section 3.2.2, following the generalised hierarchy of Figure 2.

4.2.2. Dependencies Definition

The use-case hierarchy model is presented in Figure 3. It considers the definition of Risk and reflects the dependencies and relationships between the risk factors of each layer as presented in Table 4 and Table 5. Moreover, it addresses the dynamics of a critical drone-assisted system, following the proposed approaches and guidelines presented above in Sections 3.2.3 and 3.2.5.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

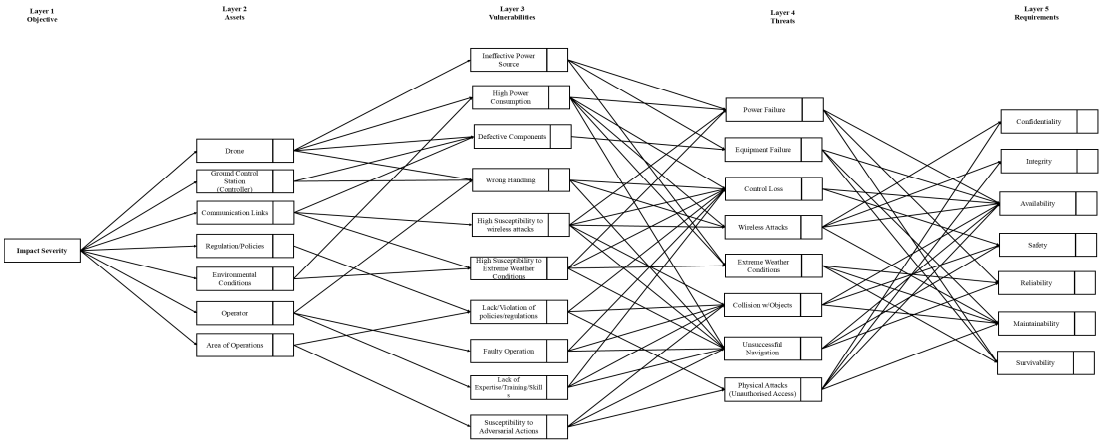

Figure 3. Drone-assisted System's Hierarchy Model.

4.2.3. Pair-Wise Comparison

After all the elements are identified and categorized, pairwise comparisons are performed. For this study's purposes, all pair-wise comparisons are verified based on the reviewed literature and requirements analysis of the illustrated use case. Explanations and statistical data are provided in-text in the following paragraphs. Comparison scales are described in Step 4.2.4.

Layer 1: Framework's Objective

The first layer of the hierarchy represents the main goal or objective of the framework. Specifically, it defines the primary aim of the structure which is the impact of severity of the identified risks on the performance of the drone-assisted delivery system. Starting by clearly stating this top-level goal, the frame of the decision problem is set up. Subsequent layers break down the hierarchy into different risk elements and extend it to the lower layers.

Layer 2: Assets Layer

- *Drone (Airborne Component)*: It refers to the aircraft and the flying element of the system [78]. It consists of various subsystems such as the frame, motors, propellers, flight controller, battery, flight controller and sensors [77,78]. It is the central component and enabling technology; therefore, it is likely to be perceived as the most important asset [98]. Regarding its comparison with the communication medium, it can be said that the drone itself is the actual asset performing the operation; thus, it is considered of moderate importance over the medium. Similarly, compared to the environment, despite the fact that it heavily influences the drone's performance, the drone slightly favors it, owing to the mechanisms that allow the operation of the system under extreme weather conditions.
- *Ground Control Stations*: It is a land-based system equipped with specialized software and hardware [13]. It is the primary interface to communicate with, remotely control, and exchange data with the airborne component [78]. It plays a critical role either the aircraft is controlled automatically or manually by the human operator [11,98,100]. Therefore, compared with the communication medium, both are considered to be of equal importance. Additionally, compared to operators, the controller is the primary interface between the human and drone therefore, it is considered to be of equal importance. However, one can assess the operator as more important than the controller, if unskilled and untrained personnel can result in mission failure. In addition, compared to the environment, the latter is generally considered to be more crucial for drone performance.
- C*ommunication Link*: As mentioned in Section 4.1 the communication medium is an asset of the aerial system, enabling bidirectional data exchange between the airborne component and controller [105]. However, environmental conditions (rain, temperature and wind) can affect the connection between the aerial component and controller consequently, between them, environment favors over communications. Additionally, different wireless attacks can violate

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

communication links, [2,15,84]. Regarding a possible drone crash, reference [106] states a percentage of 11% while [1] mentioning a considerable failure rate of up to 14%, owing to degraded communication quality.

- *Regulations/Policies*: Relevant policies have been developed to ensure that drone operators, whether recreational or professional, have a clear understanding of what is allowed under certain conditions [2,107,108]. The examination of regulations and policies as independent components is critical because violation of these rules might lead to the loss of the drone's management, unauthorised access to the equipment or a probable crash. Regulations govern the way the drone operates; thus, the operator slightly favors them because he is the admin, ensuring that the drone functions within regulations. Under specific scenario assumptions, regulations are not considered a significant factor compared with other assets.
- *Environmental Conditions*: Several studies have revealed that weather robustness is an essential gap and of high priority that may affect the ambitions to expand drone operations. [109]. High wind speeds, rain, snow, and changeable weather might have adverse impact on the drone's frame, and disturb its electronic circuits, sensors, and communication channels [14–16]. It is well noted that bad weather conditions mean that there are no flies for the system. Also, the capability to resist certain weather conditions is determined by the specifications of the drone [2]. Therefore, compared to other assets, environmental conditions favor them, expect for the aerial component.
- *Operators*: These people perform activities related to the drone's mission [78]. As a system asset, the human operator involves skills, expertise, mental - physical health and training [47]. Unskilled and untrained operators, who are unable to adapt to area limitations might result in mishandling and mission failure. Therefore, the operator is typically considered as equally important as the area of operation. However, the operator should adapt to and work within the constraints of the area of operation; hence the operator's importance is assessed slightly higher.
- *Area of Operation*: Area of operation is an external element that can influence the system's performance**.** Areas of operation should be urban or suburban, mountainous or lowland, friendly or hostile. Different characteristics result in an assessment of hazardous events in another way. However, according to [106], changes in the operating environment have a minimal effect on the system operation (5%). Regarding the tested scenario, for a drone-based system utilised under relatively controlled conditions the area of deployment has little to no effect on the pairwise-comparison. However, regarding unknown zones or diverse environments, the area of operation should have been considered a vital factor for successful deployment; therefore, its importance should be evaluated accordingly.

Layer 3: Vulnerabilities Layer

- *Ineffective Power Source*: The power source of drones is a key challenge under investigation [77]. According to several professionals [110], battery efficiency varies based on the battery chemistry, manufacturer specifications and operational conditions (discharge rates, environment, airflow, etc.). Temperature is the most influential indicator for lithium-ion batteries [90,91]. As [111] revealed, the optimal operating temperature of lithium-ion battery is 20–50 °C. However, outside this range, the capacity should decrease by 50% faster in some cases [112]. Considering that the current limitations on batteries constrict system autonomy, a power source is considered to be a vulnerability of high concern, which is more essential than almost all other possible vulnerabilities. It is no coincidence that the authors of [1,81] attributed possible drone crashes to the loss of electrical power and power propulsion at a percentage of up to 38%.
- *Power Consumption*: Related to the power source of the system. When an aerial system is utilised to accomplish a mission, the energy consumed by the system depends on the aircraft's aerodynamics, weather conditions, altitude/air density, parcel weight, flying route (take-off consumes the most energy), and speed [113,114]. Testing these factors into physics-based models mentioned in [115–117], it is discovered that power consumption and its alteration during flight time must be considered to ensure that the drone successfully reaches its destination and

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

accomplishes its delivery mission. For this reason, power consumption is considered to be of high importance except when compared to weather conditions, and wireless attacks.

- *Defective Components*: This study considers aircraft (including sensors, batteries and circuits), ground controller and communication medium as the most critical components with defects [13,79]. These components play a crucial role in the drone's performance. Each of these may increase the attack surface, thus posing potential sources of hazardous situations. Consequently, the defective components should be weighted as unpredictable factors of major importance. References [1] and [75] provide a high percentage of failures. Reference [1] mentions a range of failure from 6% to 63% while a study in [75] indicates that the accident probability due to malfunctions or technical deficiencies related to the power source lies between 55% and 63%. In a similar way reference [107] indicates that the highest causal factor leading to loss of control is equipment failure and manufacturing failures at a rate of 34%.
- *Wrong Handing*: This refers to improper human intervention. In this study, it is a vulnerability associated with operators training and expertise [21,22], therefore, its importance is assessed according to the way the system is controlled. As mentioned in [2], the percentage of a possible crash due to autopilot controller failure is approximately 23%. Otherwise, in the case of manual flight control, the evaluation of wrong handling should vary from low (14% according to [106]) to medium (22% according to [81] and 35.3% according to [74]), to very high importance due to the high mishap rate of up to 65%, due to pilot error. Moreover, as mentioned by [118] human contribution to drone accidents is evaluated at 40% in case of erroneous control during 'on task' phase (i.e. conducting its mission) and at 55% in case that the operator aims to contribute to failure recovery. For this scenario, it is assumed that the aerial component accomplishes its mission automatically; hence, the importance of this potential vulnerability is weighted accordingly, depending on the factor that is compared with.
- *Susceptibility to wireless attacks*: Wireless attacks can violate communication links and sensors [12,84]. Attacks, such as GPS Spoofing or Signal Jamming, can cause deviations, erratic movements or even unexpected behaviors [119,120]. Moreover, inadequate authentication mechanisms and weak encryption protocols can cause man-in-the-middle attacks, eavesdropping attacks, denial-of-service attacks or malware attacks, thus threatening communication links [13]. Considering that countless attacks of different sophistication are threatening communication links, it should be concluded that susceptibility to wireless attacks is of essential importance. Similarly, in comparing this vulnerability with the statistical data from the two relevant studies [1,81], it is stated that at a rate of 9% and 14%, respectively, there is a possibility of a system crash due to security attacks.
- *Susceptibility to weather conditions*: Temperature affects the battery, wind speed can cause trajectory deviation, and rain might affect drone's circuits [47]. According to [109], global drone flyability is the highest in warm and dry continental regions. Also, it is noted that the most limiting weather factor is precipitation and that common drones have an operational temperature range of 0 to 40 ℃, maximum wind speed resistance of 10 m/s. Furthermore, the sensors and circuits are sensitive to moisture, rain and precipitation [48]. In addition, ice and snow accretion may cause problems to propellers. The analysis in [1], indicates that the possibility for a drone to crash owing to the weather effect lies within the range of 5% to 18%. In a similar way reference [106] reveals that environmental factors have a contribution of 14%, leading to loss of control. Having said that and also that weather affects power efficiency, weather conditions are examined, at least, of moderate importance, and are consequently, capable of actively affecting successful deployment.
- *Lack or violation of policies and regulations*: The existence of regulations should be considered an important part of a drone-based delivery system in and around cities [121]. The violation of these rules may lead to a loss of drone management. In addition, inadequate traffic management or ineffective estimation of drone's density in low-altitude airspaces increases the probability of lethal consequences [73]. According to [1], the percentage of possible drone crashes caused by

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

air traffic management failure is low, ranging from 2% to 8%, or up to 9% due to inadequate regulations or violations [118]. In addition, the violation of security controls empowering physical attacks depends on the area of operation and the type of mission. For this study, it is assumed that there is no violation of any aviation or security controls, thus this vulnerability is considered to be of minimal importance.

- *Faulty Operation and Lack of Operator's Expertise:* This type of weakness indicates the system's inability to operate properly owing to external factors, such as adversarial attacks, weather conditions, or erroneous control [12,84,119,120]. Operator's experience is a significant factor contributing to accidents. According to [106] the highest number of accidents for total flying experience within 20 – 99 hours is rated at 35% while the lowest number of accidents for total flying experience of 1,000+ hours is assessed at 3%. However, as was mentioned above about '*Wrong Handling'*, the mission of a drone-based delivery system should be achieved, through manual operation or automatically. Therefore, the possibilities of these kinds of vulnerabilities to be exploited are significantly reduced and their importance is weighted accordingly, because the examined system operates automatically.
- *Susceptibility to adversarial actions*: These types of attacks target hardware components and intend to compromise the system's functionalities (i.e. bombing, gunshots, mission surveillance or reconnaissance, equipment interference or physical attacks [13,21]. The lack of control and security restrictions makes a system prone to such attacks [78]. However, in this scenario, adversarial attacks should not be considered as an important factor compared to vulnerabilities such as weather conditions, defective equipment and power consumption. Nevertheless, it could be compared with lack of expertise and policy violations and being of moderate importance in terms of the level of its impact in case of exploitation.

Layer 4: Threats Layer

- *Power Failure*: Battery provides the necessary power for extended flight durations [13,77,105]. Any technical or structural failure is considered a threat. [22] Therefore, possible power failure is classified as a threat that, if it occurs, should directly exploit vulnerabilities such as ineffective power source or high-power consumption. In addition, power failure is indirectly associated with vulnerabilities such as susceptibility to wireless attacks and weather conditions (due to increased power consumption from deviations or erratic movements). The percentage of 38% for a possible drone crash owing to power failure should not be considered negligible [1]. The proportion of 14% stated in [106], for power loss should not be considered insignificant. Given that the limited capacity of drone batteries is considered a challenge [77] and that the effects of such a threat might involve the entire system, it is concluded that power failure is of essential or strong importance.
- *Equipment Failure:* It occurs depending on the durability of the system. Vulnerabilities, including defective components (battery, circuits, structure), susceptibility to weather conditions (rain, snow, temperature, or even high wind might harm the circuits, battery or structure of the drone) and adversarial actions (equipment destruction or damage) might be exploited. Consequently, a possible failure, especially a breakdown of the aerial component, might threaten the successful completion of the mission and its effects should be extensive. Therefore, '*Equipment Failure'* should be considered as essential or strong importance, if the crash rate reported in [1] ranges from 6% to 63%.
- *Control Loss*: Loss control of the system is an erroneous action taken by the operator and might take advantage of vulnerabilities such as wrong handling, faulty operations and lack of expertise. In addition, high power consumption, weather conditions, susceptibility to wireless attacks and violation of aviation regulations are vulnerabilities associated with control loss. Under different circumstances, it might be of essential or strong importance, although, based on the assumptions that have been set, most of these factors are controllable. Hence, compared with other threats, control loss might be considered to be as of minor importance.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

- *Wireless Attacks*: They might threaten communication means, controller and sensors leading to severe consequences [13,84]. Their importance is assessed in consideration of the essentiality of communication means and the fact that susceptibility to wireless attacks is evaluated as of high concern. Considering the possibility of up to 14%, for a system to crash due to security attacks, it should be concluded that susceptibility to wireless attacks is judged accordingly [119,120,122].
- *Extreme Weather Conditions*: Weather conditions, as a hazard threatening a system [21], should always be carefully considered. For the tested scenario, it is assumed that the weather conditions are ideal for a drone to accomplish flight. Having in mind what is already mentioned above for the susceptibility to environmental conditions, weather is evaluated at least of moderate importance, and consequently, capable of affecting the successful completion of a package to be delivered.
- *Collision with objects*: This is a considerable threat, particularly when deploying a system above urban area. The probability of a mid-air collision varies from 2% to 38% [1]. Also, the likelihood of a drone crashing due to its inability to avoid a collision is low up to 5%. Similarly, the probability of other aerial components approaching a drone-assisted system and leading to an accident was approximately 30% [74]. Moreover, regarding a possible accident due to a collision, reference [106] states a percentage of 8%. As shown, the estimation varies and depends on factors such as object density, embedded collision avoidance sensor, and drone's trajectory. Therefore, for our study, collision is considered of some importance, because the impact will have severe consequences, such as equipment damage, loss of lives and injuries to unsuspecting bystanders or package destruction.
- *Unsuccessful Navigation*: Linked directly to 'Wrong Handling', it is assumed that the aerial component accomplishes its mission automatically, hence its importance is reviewed as of minor concern. However, unsuccessful navigation of a drone-based system is indirectly associated with other vulnerabilities such as 'Susceptibility to Weather Conditions', 'Susceptibility to Wireless Attacks' or 'High Power Consumption' thus its importance is weighted accordingly [48,76,77].
- *Physical Attacks (Unauthorised Access)*: These types of attacks target hardware components [13]. In addition, they aim to cause physical damage, usurp control, steal the cargo, disrupt the mission, or interfere with sensitive equipment on the system. For the examined scenario, the system is utilised under relatively controlled conditions, thus, the importance of physical attacks is lessened. It favors only over control loss and unsuccessful navigation, because the level of its impact should affect the entire mission. Under other circumstances where the system could operate for a different mission or in a diverse environment (transportation of valuable materials or for critical surveillance missions), physical attacks should have been considered an important factor for the successful accomplishment of the mission.

Layer 5: Requirements Layer

For the evaluation of the requirements the linked threats and the impact of each requirement are considered (see Tables 4 and 5 and Supplementary Material S1, for reference). For instance, about '*Confidentiality*', the qualitative analysis revealed that it is violated by '*Wireless Attacks*' and '*Physical Attacks*'. Similarly, '*Availability*' is shown to be endangered if the system is spoofed, penetrated, suspended, disrupted, or physically tampered and cannot operate as expected. Following the hierarchy in Figure 3, '*Availability*' is violated by almost all the identified threats. Therefore, when '*Availability*' is compared to '*Confidentiality*', it is considered as of essential or very strong importance. Apart from that, *Confidentiality* and *Availability* are two pillars representing a critical balance where excessive security (high confidentiality) can hinder user access (low availability). However, when it comes to critical aerial systems strict access rules might improve secrecy yet can block urgent needs, such as emergency system utilisation. In addition, the importance of safety relies on the fact that in the event of an accidental or adversarial threat, the system itself is going to be in a difficult situation, as well as human lives [123]. Therefore, when it comes to human loses or injuries 'Safety's'

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

importance favors over all the studied requirements as of the highest possible order. According to this approach, the requirements are weighted as follows:

- *Confidentiality*: Unauthorised access to system's equipment and communication links' disclosure (due to wireless attacks [13,84]) are the identified threats capable of intimidating confidentiality. Considering the importance of these threats and the examined scenario, confidentiality does not seem to be very important in affecting the resilience and performance of the system.
- *Integrity*: With reference to the hardware, integrity denotes tampering with the equipment, for instance malicious or accidental destruction of components [124]. Therefore, *Wireless Attacks*, *Unauthorized Access* and *Weather Conditions*, are possible threats that can violate system's integrity. Comparing the importance of confidentiality and integrity, it seems that they lag behind other requirements, by a similar level. Nevertheless, when it comes to the comparison between them, integrity favors slightly over confidentiality owing to its connection to the important factor of *Weather Conditions*.
- *Availability*: As qualitative analysis reveals, availability is an extremely important parameter for a drone-based system to be 'ready to operate' [125,126]. Hence, when is compared to *Confidentiality* and *Integrity*, it is considered as of essential or very strong importance. In addition, compared to *Safety*, when it comes to human loses or injuries 'Safety's' importance favors over all the studied requirements. Also, regarding the comparison of *Availability* with *Survivability* and *Maintainability*, both favor over *Availability*, for the reasons will be explained below.
- *Safety*: The importance of *safety* relies on the fact that in the case of an accidental or adversarial threat, not only is the system itself going to be in a difficult situation but possible also human lives [123]. Therefore, the possibility of causing fatalities upgrades its importance over other requirements and makes *Safety* favored as of the highest possible order of affirmation.
- *Reliability*: This is closely related to *Availability* [124–126]. Additionally, it is a key factor that determines the operational efficiency of drones [127,128]. Based on the facts and assumptions made for the specific case study, *Reliability* favors over *Confidentiality* and *Integrity*, is equal to *Availability* and finally, it is characterized as subservient to the remaining requirements.
- *Maintainability*: Restored easily to normal operating conditions after a hazardous event, increases the probability of the system being available and reliable [129,130]. Considering that the hazards that are threatening the system's normal operation are of the most highly rated ones (*Equipment Failure*, *Wireless Attacks*, *Collision with Objects*, *Weather Conditions*), it is concluded that the comparison favors maintainability over almost all the other requirements.
- *Survivability*: This is a subset of resilience, and indicates the capability of the system to fulfil its mission, even in the presence of any threat [131,132]. For a drone-based system, that operates in an open environment, ensuring *Survivability* with robust and consistent controls is considered the most important. Therefore, when it comes to compare *Survivability* to the other requirements, it favors all of them, thus increasing the likelihood of a successful mission accomplishment.

4.2.4. Scaling Matrices

According to the analysis provided in Sections 3.2.4 and 3.2.5, matrices are established. The elements of each level of the hierarchy, were rated using the fundamental comparison scales [56] (see Table 2). Additionally, comparison numerical values are assigned based on statistical models retrieved from different sources provided by articles published in well-established journals and conferences. Table 4 presents the comparison matrix formulated for the Assets' Layer. In a similar way, pair-wise comparisons were conducted for Layers 3, 4 and 5, and associated matrices were formulated based on the explanation thoughts described above (Matrices formulated for layers 3, 4 and 5 are presented in Supplementary Material S2 – Tables S5 to S8).

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

4.2.5. Calculating Priority Vectors and Consistency Ratio

After establishing the pair-wise comparison matrices, priority vectors are calculated. This is performed by following the procedure described in Section 3.2.6. For illustration purposes an explanation is given in calculating the priority vector of Assets' layer: for value normalization, values of Table 6 are divided by the sum of the elements of the column they belong to. Then, the sum of the elements in each resulting row (to obtain a 'row sum') is divided by the number of elements in the row, thus resulting in the relative importance of this element. Assumimg the risk element of *Drone (Airborne Component*) (see shaded row of Table 7): 0.30 + 0.3103 + 0.2222 + 0.1818 + 0.4615 + 0.2338 + 0.1579)/7, gives 0.2668, which is the relative importance of *Drone (Airborne Component)*. Similarely, relative importance of all assets is calculated. Table 7 presents the normalised values of the pair-wise comparisons of Layer 2. In addition, last column illustrates the calculated priority vector.

Table 6. 2nd Layer Pair-wise Comparison Matrix.

ASSETS	Drone (Airborne Component)	Ground Control Station	Communication Links	Regulations/ Policies	Environmental Conditions	Operator	Area of Operations
Drone (Airborne Component)	1,00	3,00	2,00	3,00	2,00	3,00	3,00
Ground Control Station	0,33	1,00	1,00	3,00	0,33	1,00	3,00
Communication Links	0,50	1,00	1,00	3,00	0,25	3,00	3,00
Regulations/Policies	0,33	0,33	0,33	1,00	0,25	0,50	2,00
Environmental Conditions	0,50	3,00	4,00	4,00	1,00	4,00	4,00
Operator	0,33	1,00	0,33	2,00	0,25	1,00	3,00
Area of Operations	0,33	0,33	0,33	0,50	0,25	0,33	1,00
Column Sum*	**3,3333**	**9,6667**	**9,0000**	**16,5000**	**4,3333**	**12,8333**	**19,0000**

* Column Sum - obtained from the summation of the elements of each column.

Table 7. 2nd Layer - Normalised Pair-wise comparison matrix.

ASSETS	Drone (Airborne Comp.)	Ground Control Station	Commun. Links	Regulations/ Policies	Environm. Conditions	Operator	Area of Operations	Priority Vector
Drone (Airborne Component)	0,3000	0,3103	0,2222	0,1818	0,4615	0,2338	0,1579	**0.2668**
Ground Control Station	0,1000	0,1034	0,1111	0,1818	0,0769	0,0779	0,1579	**0.1156**
Communication Links	0,1500	0,1034	0,1111	0,1818	0,0577	0,2338	0,1579	**0.1422**
Regulations/Policies	0,1000	0,0345	0,0370	0,0606	0,0577	0,0390	0,1053	**0.0620**
Environmental Conditions	0,1500	0,3103	0,4444	0,2424	0,2308	0,3117	0,2105	**0.2715**
Operator	0,1000	0,1034	0,0370	0,1212	0,0577	0,0779	0,1579	**0.0936**
Area of Operations	0,1000	0,0345	0,0370	0,0303	0,0577	0,0260	0,0526	**0.0483**

To ensure the consistency of comparisons, CRs are calculated using Equations (3), (4) and (5). The resulting λ_{max}, n, CI and CR values are listed in Table 8. From the valus analysis, it is deduced that the CR is less than the acceptable values (CR<0.1); hence, the judgment is consistent.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Table 8. Consistency Check.

LAYERS	λ_{max}	n	CI	CR
2nd (Assets)	7.4825	7	0.0804	0,0609
3rd (Vulnerabilities)	10.7025	10	0.0781	0.0524
4th (Threat Sources)	8.5162	8	0.0737	0.0523
5th (Requirements)	7.6419	7	0.1070	0.0810

4.2.6. Calculating Local Weights

In AHP, the calculated relative priorities (estimation is conducted through the previous step) within the same layer of the hierarchy consist of the local weights [89]. Table 10 summarises the calculated local weights for all risk elements.

4.2.7. Calculating Global Weights

As explained in Section 3.2.8, it is necessary to calculate the global weights of each element. According to [89], global importance quantifies the overall importance within the entire hierarchy of elements. In addition, the global importance of an element is distributed among its connected child nodes (elements of the immediately below layer). Similarly, the global weight of any element is calculated from the product of its local weight and the global weight of its parent element (element of the immediately above layer) [89]. Starting with Layer 1 (hierarchy's objective – root of the hierarchy), both the global and local weights sum up to 100%; thus, both the global and local weights of its child layer coincide [89]. Therefore, regarding the assets' weight, which is the child layer of the objective, the calculated relative weights of assets are also considered global. In regard to the global weights of vulnerabilities, threats and requirements, these are estimated by applying Equations (8), (9), (10) and (11). Table 9 presents the sample calculations for estimating a vulnerability's ,a threat's and a requirement's global weight based on the propagation of weights across the hierarchy (see Supplementary Material S3 for mathematical analysis and calculations for all elements).Table 10 summarizes the computed global weights.

Table 9. Global Weights (Sample Calculations).

	Local Weight	**Parent Nodes (Pn G W)**	**Parent Nodes Global Weight**	**Global Weight (L) x (∑ Pn G W)**
Defective components **(Vulnerability)**	0.1410	Drone	0.2668	0.0740
		Ground Control Station	0.1156	
		Communication Links	0.1422	
Power Failure **(Threat)**	0.2152	Ineffective power source	0,0415	0,0440
		High power consumption	0,0513	
		Susceptibility to wireless attacks	0,0167	
		Susceptibility to Weather Conditions	0,0948	
Safety **(Requirement)**	0,3545	Control Loss	0,0112	0,0093
		Collision w/ Objects	0,0040	
		Unsuccessful Navigation	0,0110	

Table 10. Local and Global Weights.

ELEMENT	LOCAL WEIGHT	GLOBAL WEIGHT
ASSETS LAYER		
Environmental Conditions	0.2715	0.2715
Drone (Airborne Component)	0.2668	0.2668
Communication Links	0.1422	0.1422
Drone Controller	0.1156	0.1156
Operator	0.0936	0.0936
Regulations/Policies	0.0620	0.0620
Area of Operations	0.0483	0.0483
VULNERABILITIES LAYER		
High Susceptibility to Extreme Weather Conditions	0.2292	0.0948
Defective components	0.1410	0.0740
High power consumption	0.0953	0.0513
Ineffective power source	0.1557	0.0415

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Wrong Handling	0.0576	0.0274
High Susceptibility to wireless attacks	0.1173	0.0167
Lack of Expertise/Training/Skills	0.0523	0.0049
Faulty Operation	0.0512	0.0048
Adversarial Actions	0.0657	0.0031
Lack or Violation policies/regulations	0.0347	0.0021
THREATS LAYER		
Power Failure	0.2152	0.0440
Extreme Weather Conditions	0.2028	0.0381
Wireless Attack	0.1580	0.0151
Equipment Failure	0.1133	0.0130
Control Loss	0.0552	0.0112
Unsuccessful Navigation	0.0542	0.0110
Collision w/ Objects	0.1273	0.0040
Unauthorised Access	0.0740	0.0004
REQUIREMENTS LAYER		
Survivability	0.1883	0.0179
Maintainability	0.1682	0.0119
Availability	0.1004	0.0099
Safety	0.3545	0.0093
Reliability	0.1004	0.0093
Integrity	0.0519	0.0008
Confidentiality	0.0362	0.0006

4.3. Define Risk Chains

Following the process described in Section 3.3 specific risk events are reported. Every risk event is described by a chain of *Asset* → *Vulnerability* → *Threat* → *Requirement*, which starts from the objective of the hierarchy, follows a pathway through every layer and ends at a requirement. By analyzing the connections between the risk elements in the hierarchy, as these are formed and presented in Figure 3, *147 pathways* are established. Table 11 summarises the total risk chains in which each risk element is involved. As shown by counting the risk chains per layer, their sum is 147. (Supplementary Material S4 illustrates all the registered pathways). From the analysis of data shown in Table 11, it is observed that the leading nodes through which the majority of the chains are passing from are as below: the '*Drone*' (36 paths) followed by '*Communication Links*' (29 paths) and '*Environmental Conditions*' (26 paths), in assets' layer. As for the 3rd Layer, the vulnerability of '*High Power Consumption*' (30 paths) and '*Wrong Handling*' (27 paths) are the leading nodes. Regarding the threats' layer '*Unsuccessful Navigation*' (33 paths) and '*Wireless Attacks*' (24 paths) gather most of the pathways. Regarding the 5th layer of requirements, it is noted that most of the risk chains lead to the requirement of '*Availability*' (45 paths), followed by the 27 paths which end at the requirement of '*Safety*'. The requirements with the least number of routes terminating in these are '*Confidentiality*' and '*Integrity*' (8 paths, respectively). Nonetheless, the number of risk chains is not necessarily the determining factor for the risk level. One risk element might influence many risk paths of little importance, whereas another element there might contribute to fewer risk chains but of greater importance. Each element of the hierarchy contributes an amount of risk to each of its associated chains, based on its global importance. Thus, the combination of element contributions leads to cumulative risk in the risk chain. In addition, the aggregation of the cumulative risk that passes through a specific element allows for the evaluation of the total contribution of each node to the overall severity impact.

Table 11. Risk Chain Sum Total and Associated Aggregated Risk.

Asset	Risk chains (Aggreg. Risk)	Vulnerability	Risk chains (Aggreg. Risk)	Threat Source	Risk chains (Aggreg. Risk)	Requirement	Risk chains (Aggreg. Risk)
Drone (Airborne Component)	36 **(0.02046)**	High Power Consumption	30 **(0.01477)**	Unsuccessful Navigation	33 **(0.00611)**	Availability	45 **(0.00991)**
Communication Links	29 **(0.01317)**	Wrong Handling	27 **(0.00306)**	Wireless Attacks	24 **(0.00538)**	Safety	27 **(0.00929)**
Environmental Conditions	26 **(0.02186)**	High Susceptibility to Extreme Weather	22 **(0.02196)**	Control Loss	22 **(0.00507)**	Reliability	22 **(0.00934)**

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

		Conditions					
Operator	25 **(0.00190)**	High Susceptibility to Wireless Attacks	15 **(0.00458)**	Power Failure	18 **(0.01711)**	Maintainability	22 **(0.01188)**
Ground Control Station	12 **(0.00159)**	Susceptibility to Adversarial Actions	10 **(0.00043)**	Extreme Weather Conditions	15 **(0.01739)**	Survivability	15 **(0.01791)**
Area of Operation	10 **(0.00043)**	Defective Components	9 **(0.00383)**	Collision w/Objects	15 **(0.00251)**	Confidentiality	8 **(0.00056)**
Regulations/Policies	9 **(0.00028)**	Ineffective Power Source	9 **(0.00948)**	Equipment Failure	12 **(0.00598)**	Integrity	8 **(0.00080)**
		Lack or Violation of Policies/Regulations	9 **(0.00028)**	Physical Attacks	8 **(0.00014)**		
		Faulty Operation	8 **(0.00064)**				
		Lack of Expertise/ Training/Skills	8 **(0.00066)**				

4.4. Cumulative Risk Contribution – Risk Ranking

Based on the procedure described in Section 3.4, the contribution of each element to its associated risk chains is computed by applying Equation (12) and taking into account the results of the methodology stated in Table 10. In addition, the Cumulative Risk for every chain was assessed, allowing the ranking of the identified risk events. Finally, the impact of severity of every of each risk element was evaluated by aggregating the risk chains involved. Here is an illustrative example: From the hierarchy of Figure 3, assume the pathway of *Environmental Conditions - High Susceptibility to Extreme Weather Conditions - Unsuccessful Navigation – Safety.* Starting from the node of *Safety*, it is linked to the threats of '*Control Loss*', '*Unsuccessful Navigation*' and '*Collision with Objects*'. According to Equation (12) the proportion of influence of '*Unsuccessful Navigation*' on '*Safety*', is calculated at *0.42* as below:

$$\text{Proportion}\left(\text{parent} \rightarrow \text{child}\right) = \frac{\text{GW (parent)}}{\sum \text{GW (parents)}},$$

$$\frac{0.0110}{0.0112+0.0110+0.0040} = 0.42,$$

Similarly, we estimate the proportion of influence of *High Susceptibility to Extreme Weather Conditions* on the examined chain. To do this we examine the vulnerabilities involved in *Unsuccessful Navigation*; *High Susceptibility to Extreme Weather Conditions, High Power Consumption, Wrong Handling, High Susceptibility to Wireless Attacks, Faulty Operation, Lack of Expertise/Training/Skills and Physical Attacks.* Considering their global weights (see Table 10), the sum was *0.203*. Hence, the share of affection for *High Susceptibility to Extreme Weather Conditions* which corresponds to *Unsuccessful Navigation* was *0.0948/0.203 = 0.47*. Finally, we estimate the influence of the asset of *Environmental Conditions* that feeds the examined pathway. The assets involved are *Environmental Conditions* and *Communication Links*. The sum of their global weights was *0.2715 + 0.1422 = 0.4137*; thus, the volume of affection linked to *Environmental Conditions* was *0.2715/0.4137 = 0.656*. Finally, the cumulative risk of path *Environmental Conditions - High Susceptibility to Extreme Weather Conditions - Unsuccessful Navigation – Safety* was *0.656 × 0.47 × 0.42 × 0.0093 = 0.0012*. This value indicates the proportion of risk owing to this specific sequence of elements. The same process was applied to calculate the Cumulative Risk contribution for all pathways (see the last column of Table S14 on Supplementary Material S4, for reference). In addition, Figure 4 depicts the 40 most significant risk chains with the highest cumulative risk contribution. For the study's simplicity, these chains have been selected and investigated

Apart from that, the total contribution of each element to the overall severity impact is evaluated by aggregating the cumulative risk of the chains passing through this element. That is Table 11 illustrates the aggregated risk contribution per element in parenthesis. Analyzing the Cumulative

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Risk contribution and aggregated values per element empowers experts to identify high-risk pathways and also to detect the most influential elements of the hierarchy.

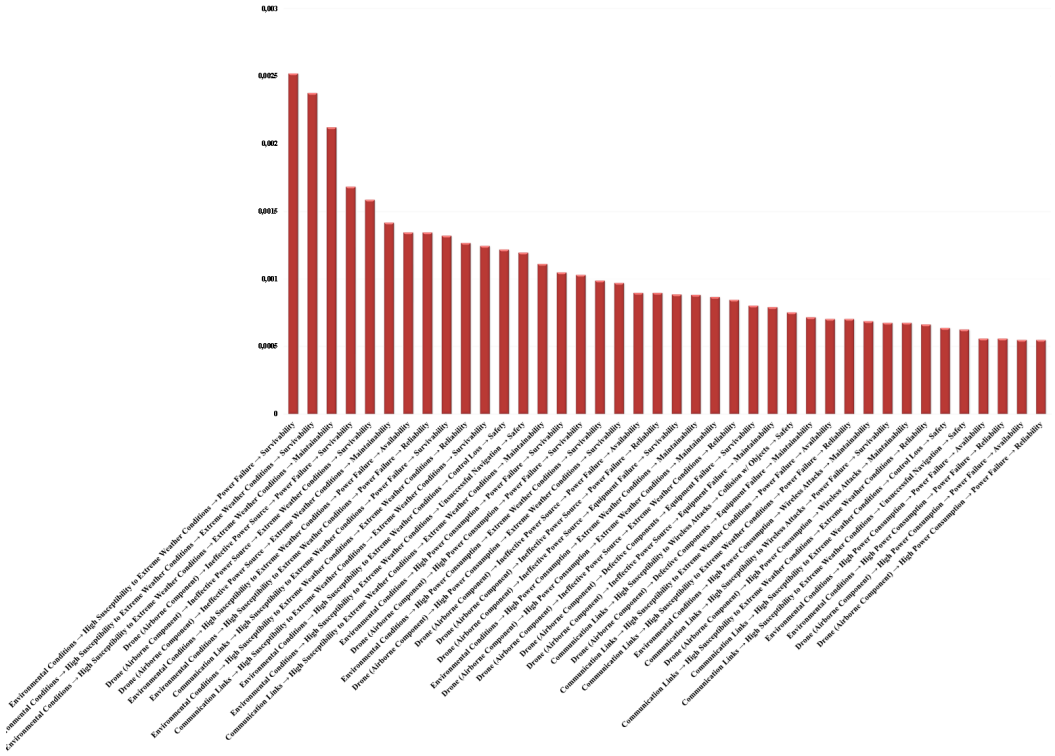

Figure 4. Overall Ranking of the 40 most Hazardous Risk Chains (based in Cumulative Risk).

5. Analysis of Results

By applying the pair-wise comparison for estimating the relative weight, it was revealed that *Environmental Conditions* are perceived as the most significant asset at 0.2715 followed closely by the *Airborne Component* at 0.2668. *Communication Links*, *Ground Control Station*, *Operator*, *Regulations/Policies* and *Area of Operations* complete the order of importance with scores of 0.1422, 0.1156, 0.0936, 0.0620 and 0.0483, respectively. These findings confirmed the significant role of weather conditions in deployment of a drone-based system and their impact on its performance [109]. Additionally, the ranking of the airborne component as the second most important factor, strengthens the literature reviewed, regarding its prominent position as an enabling technology, especially for systems providing delivery services [98]. For the 3rd layer, *High Susceptibility to Extreme Weather Conditions* was shown to be of the highest importance at 0.2292. This is justified because weather is a poorly resolved factor that affects the ambitions to expand drone operations by the adverse effect on drone endurance, performance, avionics, sensors and aerodynamics [109]. *Ineffective power source* is the next most important vulnerability followed closely by *Defective components*, *High susceptibility to wireless attacks* and *High-power consumption*. *Susceptibility to Adversarial actions*, *Wrong handling*, *Lack of expertise/training/skills*, *Faulty operation*, and *Lack or Violation policies/regulations* are rated with the lowest score. Regarding the threat sources' layer, *Power Failure* identified to bear more impact than the other elements with a score of 0.2152. This goes off well because given the limited capacity of drone batteries, the power source is considered as a challenge still under investigation [77,106]. In addition, *Extreme weather conditions*, *Wireless attacks*, *Collision with objects* and *Equipment Failure* were similar with scores of 0.2028, 0.1580, 0.1273 and 0.1133, respectively. These findings verify what was already reviewed in the literature and reported above: (i) countless wireless attacks threaten the communication links of a drone-based system [2,12,13,84], and (ii) weather conditions as a hazard

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

threatening a system, are always unpredictable, well-thought-out and most importantly capable of disturbing almost all components of the system [109]. Finally, *Physical Attacks*, *Control Loss* and *Unsuccessful Navigation* are ranked as less important because for the purposes of this study are assumed to be within manageable levels. However, in a different scenario, the contribution of these factors should be assessed differently, thus, their contribution to the performance of the system should be evaluated accordingly. Finally, in the requirements layer, the elements were ranked from the most significant to the least important as *Safety*, *Survivability*, *Maintainability*, *Availability*, *Reliability*, *Integrity* and *Confidentiality*. As shown, the requirement of *Safety* was perceived as the weightiest element with a score of 0.3545 because it is considered a factor that relies on the fact that in the case of an accidental or adversarial threat event, not only is the system itself going to be under difficult situation but also possible human lives as well [2,123]. Next, the model processes the derived local weights to estimate the global weights (to quantify the overall importance within the entire hierarchy [89,133]. By checking the weights presented in Table 6, there were elements whose importance had been altered. As already said in Section 4.2.7, the local importance of assets (Layer 2) corresponds to global importance [89]. Therefore, the asset ranking remains as follows: *Environmental Condition*, *Airborne Component*, *Communication Links*, *Ground Control Station*, *Operator*, *Regulations/Policies* and *Area of Operations.* Regarding 3rd layer's elements, *High Susceptibility to Extreme Weather Conditions* was still perceived as a vulnerability with the highest global weight. This is supported by considering the dependencies and relationships depicted in Figure 3, given that *Susceptibility to weather conditions* is linked to *Environmental Conditions* which is scored as the most important asset. *Defective components*, *High power consumption* and *Ineffective power source* were the next most important vulnerabilities. Contrary to what was calculated, the propagation of relative weights, from layer 2 to the vulnerability layer, causes an upgrade to the importance of *Defective Components* and *High-power consumption*, whereas at the same time the priority of *High Susceptibility to Wireless attacks* and *Ineffective Power Source,* is reduced. The explanation given regarding the degradation of the *Susceptibility to wireless attacks* is that the latter is associated with the asset of *communication links* (rank 3rd among assets), whereas the promotion of *Defective Components and High-Power Consumption* importance, depends on their association with *Environmental Conditions* and *Aerial Component*. Regarding the threat Sources, *Power Failure*, E*xtreme Weather Conditions* and *Wireless Attacks* remain as of the highest priority. Additionally, it is noteworthy that although *Collision with Objects* is a threat source related to equipment damage, loss of lives or injuries to unsuspecting bystanders, its global significance was downgraded and finally placed in the penultimate position. This can be justified when considering the vulnerabilities associated with *Collision with objects* given that they are evaluated in the last positions of the ranking. Similarly, the threat of *Control Loss* was evaluated as being of higher importance. This can be explained by the increased dependence on multiple vulnerabilities. Ultimately, referring to performance requirements, as marked, '*Survivability*' is scored as the most substantial requirement, unlike 'Safety' which was originally ranked as the most important requirement. This can be explained by reviewing the established dependencies. As shown, *Survivability*: (i) is impacted by the highest scored threats of *Power Failure* and *Extreme Weather Conditions*, (ii) which in turn expose the top-rated vulnerabilities of *High Susceptibility to Extreme Weather Conditions*, *Defective components, and Ineffective power source* and (iii) the affected assets are the *Drone* and the *Environmental Conditions*. Furthermore, the reduction in *Safety's* ranking could be explained by the fact that the risk elements that are linked to it and joined under the arrows representing its dependencies have been defined by the lowest rank elements of *Control Loss* and *Unsuccessful Navigation.*

As for aggregated risk, the total number of risk chains is not necessarily the determining factor. The global importance of each element and the corresponding cumulative risk contribution of each chain define the level of risk. As listed in Table 11, the aerial component, communication links, and environmental conditions direct the most risk chains. However, as revealed by the aggregated risk, the asset with the greatest influence is *Environmental Conditions* (0.02186). Similarly, checking out the vulnerability layer indicates that *High Power Consumption*, *Wrong Handling* and *High Susceptibility to*

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

Extreme Weather Conditions are directing most of the risk chains. The three most dominant vulnerabilities are *High Susceptibility to Extreme Weather Conditions* (0.02196), *High Power Consumption* (0.01477) and *Ineffective Power Source* (0.009). Likewise, the three leading threat sources are *Unsuccessful Navigation*, *Wireless Attacks* and *Control Loss*, while in terms of influence, *Extreme Weather Conditions* (0.01739), *Power Failure* (0.01711) and *Unsuccessful Navigation* (0.00611) seem to be the most significant. Finally, regarding the requirements of performance *Availability*, *Safety* and *Reliability* have the highest appearance in risk paths, whereas *Survivability* (0.01791), *Maintainability* (0.01188) and *Availability* (0.00991) are the most influential elements. From the analysis of the Cumulative Risk Contribution (for simplicity of analysis, we select the 40 most weighty risk chains) it is deduced that *Environmental Conditions* followed by the *Drone (Airborne Component)* are the leading assets of the chains depicted in Figure 4 (see Supplementary Material S4 for reference). Specifically, the chains that include *Environmental Conditions - High Susceptibility to Extreme Weather Conditions – Power Failure* and *Environmental Conditions - High Susceptibility to Extreme Weather Conditions - Extreme Weather Conditions* are evaluated as the weightiest risk chains. Moreover, the chains that are involved in *Environmental Conditions*, vulnerability of *Susceptibility to weather conditions* and threat sources of *Extreme weather conditions* and *Power Failure* have a significant effect on the system's *survivability* (complications in fulfilling the mission, even under hazardous conditions), *maintainability* (inability to be restored to normal operating conditions after a failure) and *reliability* (failure to accomplish a specific mission under the determined objective tasks). Additionally, when coming to the asset of *Drone (Aerial Component)* it is revealed that the chains *Drone (Airborne Component) - Ineffective Power Source - Power Failure* and *Drone (Airborne Component) - Ineffective Power Source - Extreme Weather Conditions* are evaluated as the next most significant hazardous chains that affect the system. Specifically, when threat sources such as *Power Failure* and *Extreme Weather Conditions* expose the vulnerabilities of drones, the requirements of *survivability* and *maintainability* are affected. Lastly, regarding the *Communications Links*, it seems that their involvement with the system's risk is limited only through wireless attacks and weather conditions, and consequently with a smaller overall input than the assets of *Environmental Conditions* and *Aerial Component*. Furthermore, regarding the reported weaknesses of these systems, it seems that *High Susceptibility to Extreme Weather Conditions* is the most frequent and impactful vulnerability. Checking out the hierarchy, it can be said that *High Susceptibility to Extreme Weather Conditions* is only connected to *Environmental Conditions* and *Communication Links* on the left. However, its association with numerous risk chains is due to its connection with many dominant threat sources such as *Power Failure*, *Control Loss*, *Extreme Weather Conditions* and *Unsuccessful Navigation*. Similarly, vulnerabilities such as *High Power Consumption*, *Ineffective Power Source*, and *Defective Components* are also the elements most involved in risk chains. Additionally, concerning the risk elements of the threat sources' layer, it appears that *Extreme Weather Conditions* and *Power Failure* are typically the most substantial contributors, followed by *Equipment Failure* and *Wireless Attacks*. *Control Loss* and *Unsuccessful Navigation* were the least involved elements, concentrated only on safety-oriented paths. Closing, the requirements of *Survivability* and *Maintainability* seem to be prominent, as expected, and are powered by influential threats such as *Power Failure* and *Weather Conditions*. In addition, *Safety* appeared within the most hazardous chains but influence the risk chains only via *Unsuccessful Navigation* and *Control Loss*. Regarding the requirements of *Availability* and *Reliability* the outcomes revealed that they are mainly shown through *Power Failure* and *Equipment Failure*. *Integrity* and *Confidentiality* appear in fewer pathways (related to *communication links* and data disruption through *wireless attacks*) and have a low-risk contribution.

6. Discussion of Results

The mixed-method approach and hierarchical arrangement of risk elements enable us to conduct systematic identification and evaluation of potential hazardous events. The hazards were investigated through comprehensive literature review and qualitative risk analysis. They were also decomposed into essential risk elements stemming from the broader environment in which aerial systems evolve, such as assets, weather conditions, human involvement, and executed processes and

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

services. Then, a multi-criteria hierarchy model was used to incorporate the relative weights and relationships between the identified risk elements. It also drove their propagation across the different layers of the hierarchy, estimated their global importance, and enabled the identification of the most significant factors contributing to the system's failure. The identification of high risk chains and the detection of the most influential elements can empower specialists to decide on the required actions: (i) invest in hardening, redundancy, and maintenance of the most influential assets; (ii) design or develop appropriate controls for the most significant weaknesses; (iii) prioritize detection, prevention, and response for the most powerful threat sources; (iv) strengthen the controls mapped to the most heavily impacted requirements. For the use case of this study, weather-related elements are identified as one of the most significant risk contributors. Therefore, weather-hardening strategies should be among the top levers for improving the system's resilience and performance; focusing on weather forecasting, following weather-avoidance guidelines, or implementing a go/no-go logic to help practitioners ensure the successful completion of the mission. In addition, power robustness appears to be the second most important axis for ensuring the sustainability of the system and successful mission accomplishment. Taking measures to ensure the battery's health and quality; careful planning of the route by considering all those parameters that affecting power consumption; adjusting drone's speed and altitude while flying, in case of an unexpected hazardous incident to achieve system's performance degradation; and defining the acceptable margins of power consumption (or remaining battery energy) per planned route, are some of the best practices to safeguard system's performance. Apart from that, as illustrated by the constructed hierarchy, threat sources such as *Unsuccessful Navigation*, *Control Loss* and *Collision with Objects* influence the requirement of *Safety*. Although *Safety* was assessed locally as highly important, its global importance was downgraded because its contributors were evaluated as insignificant threats. Nevertheless, targeted safety controls should be implemented, even if the system performs automatically and its route is predefined. Thus, accurate and reliable positioning systems are required. Also, points with a high concentration of people should be avoided. Operators must be carefully selected so that they are fully trained and able to respond immediately to a hazardous situation that is developing negatively. However, detailed route planning is required to avoid known obstacles. Finally, measures should be taken to protect the system from wireless attacks. Despite this, the analysis of the illustrative case scenario has shown that wireless attacks and susceptibility to such threats were not among the most important factors, compared to weather conditions and battery efficiency. Literature reviews have shown that cyber-attacks remain a challenge [2,13,44,77]. Countermeasures such as strong authentication algorithms and effective encryption keys should be implemented to protect the communication link between the controller and airborne component. Most importantly, protection from GPS spoofing or signal jamming should also be applied. Such attacks are likely to occur. According to [12,84,119] wireless attacks, in the form of GPS spoofing or signal jamming can disrupt the drone's communication or control systems and sensors, leading to deviations, crashes, unexpected behaviors and erratic movements. Therefore, measures to counter jamming and spoofing threats are suggested for implementation: anti-jamming add-on devices, embedded software on board the UAV, and resilient positioning, navigation, and timing systems are available on the market for detecting signal navigation threats [134]. Summing up, in this study, the risk elements associated with the utilisation of a drone-assisted system were identified by implementing a hybrid risk assessment approach. Regarding the applicability of the developed risk assessment framework, the established model can be used as an evaluation tool to assess the risk level of integrating a drone-assisted system into different workflows, such as package delivery, surveillance and the provision of communication services. Utilising a drone-assisted system poses several risks related to the area of operation, environmental conditions, type of mission, and the technical specifications of the system. These parameters were correlated in different ways. To this end, the proposed model could be suitable as a guide for understanding and mitigating risks. The risk elements, identified and verified during the application of the proposed framework, could provide personnel (practitioners, technicians, controllers, etc.) with a better understanding of the root causes of risks and how they are

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

interconnected and interrelated. Accordingly, this can promote awareness of the technical, environmental, safety, and security risks that might arise in the utilisation of aerial systems.

7. Conclusions and Future Work

This study took a step toward presenting a systematic risk assessment approach for drone-assisted services. It applied a hybrid methodology including steps covering the qualitative analysis (NIST-ISO integration) and quantitative evaluation (a multi-layer hierarchical process based on AHP's fundamentals) of risks associated with drone services. First, fundamental information on risk assessment and risk was presented. In addition, different approaches employed for risk assessment of aerial systems are reviewed. This background knowledge was utilized to define a simple, functional, easily understandable and applicable model, suitable for drone-oriented applications, while considering the risk elements of assets, vulnerabilities, threat sources, and impact. The applicability and feasibility of the proposed method were demonstrated by applying it to a drone-assisted package-delivery system, explaining its effectiveness in identifying hazards, evaluating risk elements and assessing risk events. The use of a multi-criteria hierarchy model defined the propagation of the relative importance of each element across the hierarchy and estimated its global importance. It also empowered the final ranking of the verified risk elements and enabled the identification of the factors that made the greatest contribution to the occurrence of system failure. Additionally, the framework visualized different risk chains, each assessed as a separate entity, constituting a separate risk event. In this study, it was validated and deduced that weather-related factors were the greatest contributors to risk. *Environmental Conditions, Susceptibility to Weather Conditions, and Extreme Weather Conditions* were the leading elements of the aggregated risk. In addition, they influence the majority of the 40 most significant risk chains. Moreover, the *Airborne Component* was another risk factor contributing to the increase in exposure to hazardous situations. Filtering the most significant risk chains revealed that drone influenced 16 of them. Furthermore, power-related elements appear to be the second most important factor to consider. Most chains involving *High Power Consumption*, *Ineffective Power Source* and *Power Failure* were listed among the weightiest risk chains. Therefore, considering the manufacturers' technical recommendations, adjusting the drone's speed and altitude while flying, defining the acceptable margins of power consumption, and maintaining a safe energy threshold are the best practices for safeguarding the system's performance. Regarding the environmental conditions, temperatures above 40°C, rainy and windy conditions are parameters decreasing battery efficiency, thus should be considered before deploying an aerial system. Moreover, regarding the *Communications Links*, it seemed that their involvement with the system's risk is limited only through wireless attacks and weather conditions, since they influence only 10 out of 20 of the most important risk chains. Nonetheless, communication channels are outlined as a critical component, especially in cases of manual control, and are vulnerable to sophisticated attacks. Therefore, effective authentication and security mechanisms must be implemented. Closing, regarding the requirements of *Survivability*, seemed to be prominent, (influencing 13 out of the 40 most considerable risk chains) and powered by influential threats such as *power failure* and *weather conditions*. Consequently, taking power- and weather-related controls should increase the system's resilience and decrease the impact on the system's performance in the case of a hazardous event. Although the proposed risk assessment approach may have the potential to strengthen both the conceptual and functional skills of experts, future work will extend its applicability to different drone-based applications. The factors involved in the risk assessment of drone-assisted systems vary. Owing to their dynamic nature, it is suggested that practitioners involve the proposed framework by adjusting the relative weights and evaluating the resulting risk contributions, according to the planned applications and use cases. In addition, future work will implement an experimental evaluation of the framework, including simulation tests to support the findings summarized above. Therefore, to obtain more effective results, in our future work we intend to evaluate the weightiest risk contributors under and different scenarios by assessing the effect of temperature, atmospheric conditions, characteristics of the area of operation, characteristics and type

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

of the mission, technical characteristics of the drone, battery and energy consumption. The proposed framework along with the simulations tests is expected to serve as a useful, complementary tool that can be easily modified and adjusted to different applications and various types of aerial systems.

Supplementary Materials: The following supporting information can be downloaded at the website of this paper posted on Preprints.org. Supplementary Material S1: Qualitative Analysis, Supplementary Material S2: Pair-wise Comparison Matrices, Supplementary Material S3: Global Weights and Supplementary Material S4: Risk Chains – Risk Contribution. References [2,13,21,71,84,86,123–126,128,129,131,132], are cited in Supplementary Material S1.

Author Contributions: "Conceptualization, N.F.; methodology and validation, N.F.; writing, N.F.; review, editing and supervision, K.K, S.K. and H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article/supplementary material. Further inquiries can be directed to the corresponding author.

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

References

1. Allouch, A.; Koubâa, A.; Khalgui, M.; Abbes, T. Qualitative and Quantitative Risk Analysis and Safety Assessment of Unmanned Aerial Vehicles Missions Over the Internet. *IEEE Access* **2019**, *7*, 53392–53410.
2. Shakhatreh, H.; Sawalmeh, A. H.; Al-Fuqaha, A.; Dou, Z.; Almaita, E.; Khalil, I.; Othman, N. S.; Khreishah, A.; Guizani, M. Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. *IEEE Access* **2019**, *7*, 48572–48634.
3. Katzis, K.; Ahmadi, H.; Shakir, M. Z. A Novel Airborne Self-Organising Architecture for 5G+ Networks. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*; IEEE, 2017. https://doi.org/10.1109/VTCFall.2017.8288095.
4. Join the airborne revolution. Day and night. Whatever the weather. ALLSOPP HELIKITES LTD. https://www.helikites.com/. (accessed 2025-12-07).
5. Katzis, K.; Grondoudis, A. Disaster Monitoring and Disaster Relief Using High Altitude Platforms. In *1st International Conference in Safety Crisis Management*; Nicosia, Cyprus, 2011.
6. Reynaud, L.; Rasheed, T. Deployable Aerial Communication Networks: Challenges for Futuristic Applications. In *9th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*; Paphos, Cyprus, 2012. https://doi.org/10.1145/2387027.2387030.
7. Saeed, A.; Younes, A. B.; Cai, C.; Cai, G. A Survey of Hybrid Unmanned Aerial Vehicles. *Progress in Aerospace Sciences* **2018**, *98*, 91–105. https://doi.org/10.1016/j.paerosci.2018.03.007.
8. Katzis, K.; Grondoudis, A.; Boustras, G.; Papazoglou, P. Forest Fires: Proactive and Reactive Surveillance Employing in-Situ, Aerial, and Space Technology. In *International Conference on Remote Sensing and Geoinformation of Environment*; Paphos, Cyprus, 2013. https://doi.org/10.1117/12.2027599.
9. Helikite Airborne Surveillance Systems. Allsopp Helikites Ltd. https://www.helikites.com/aerial-surveillance-aerostats. (accessed 2025-11-21).
10. Borghetti, F.; Caballini, C.; Carboni, A.; Grossato, G.; Maja, R.; Barabino, B. The Use of Drones for Last-Mile Delivery: A Numerical Case Study in Milan, Italy. *Sustainability* **2022**, *14* (3), 1766. https://doi.org/10.3390/su14031766.
11. Zubin, I.; Wiegmans, B.; Arem, B.; Duin, R. Using Drones in the Last-Mile Logistics Processes of Medical Product Delivery: A Feasibility Case Study in Rotterdam. In *The 99th Annual Meeting Transportation Research Board*; Washington DC, (USA), 2020.
12. Kim, A.; Wampler, B.; Goppert, J.; Hwang, I.; Aldridge, H. Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. In *Infotech@Aerospace 2012*; 2012. https://doi.org/10.2514/6.2012-2438.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

13. Anagnostis, I.; Kotzanikolaou, P.; Douligeris, C. Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services. *IEEE Access* **2025**, *13*, 47955-47995. https://doi.org/10.1109/ACCESS.2025.3549861.
14. Kardasz, P.; Doskocz, J.; Hejduk, M.; Wiejkut, P.; Zarzycki, H. Drones and Possibilities of Their Using. *Journal of Civil and Environmental Engineering* **2016**, *6* (3). https://doi.org/10.4172/2165-784X.1000233.
15. Hartmann, K.; Steup, C. The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. In *5th International Conference on Cyber Conflict (CyCon), Tallin*; IEEE: Talin, Estonia, 2013; pp 1–23.
16. Barr, L. C.; Newman, R.; Ancel, E.; Belcastro, C. M.; Foster, J. V.; Evans, J.; Klyde, D. H. Preliminary Risk Assessment for Small Unmanned Aircraft Systems. In *17th AIAA Aviation Technology, Integration, and Operations Conference*; AIAA: Denver, Colorado, 2017. https://doi.org/10.2514/6.2017-3272.
17. Rong-xiao, G.; Ji-wei, T.; Bu-hong, W.; Fu-te, S. Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective. In *2020 International Conference on Computer Engineering and Application (ICCEA)*; IEEE: Guangzhou, China, 2020; pp 259–263. https://doi.org/10.1109/ICCEA50009.2020.00063.
18. Shakeri, R.; Al-Garadi, M. A.; Badawy, A.; Mohamed, A.; Khattab, T.; Al-Ali, A.; Harras, K. A.; Guizani, M. Design Challenges of Multi-UAV Systems in Cyber-Physical Applications: A Comprehensive Survey and Future Directions. *IEEE Communications Surveys & Tutorials* **2019**, *21* (4), 3340–3385. https://doi.org/10.1109/COMST.2019.2924143.
19. Gomes, R.; Straub, J.; Jones, A.; Morgan, J.; Tipparach, S.; Sletten, A.; Kim, K. W.; Loegering, D.; Feikema, N.; Dayananda, K.; Miryala, G.; Gass, A.; Setterstrom, K.; Mischel, J.; Shipman, D. An Interconnected Network of UAS as a System-of-Systems. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St*; IEEE: Petersburg, FL, USA, 2017; pp 1–7. https://doi.org/10.1109/DASC.2017.8102148.
20. Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39); National Institute of Standards and Technology NIST: Gaithersburg, MD 20899-8930, 2011.
21. Guide for Conducting Risk Assessments (NIST Special Publication 800-30); Gaithersburg, MD 20899-8930, 2012.
22. ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks; Geneva, 2022.
23. Eckmaier, R.; Fumy, W.; Mouille, S.; Quemard, J.-P.; Polemi, N.; Rumpel, R. *ENISA Risk Management Standards*; ENISA, 2022.
24. *EBIOS - Risk Manager*; National Cybersecurity Agency of France (ANSSI), 2019.
25. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. *Introduction to OCTAVE Approach*; PA 15213-3890: Pittsburgh, 2003.
26. *CRAMM*. Wikipedia. https://en.wikipedia.org/wiki/CRAMM.
27. *Risk Taxonomy*; The Open Group, Berkshire, 2009.
28. Talabis, M. R. M.; Martin, J. L.; Wheeler, E. *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis*; Elsevier Inc: Waltham, MA 02451, USA, 2013. https://doi.org/10.1016/C2010-0-69579-4.
29. *SPECIFIC OPERATIONS RISK ASSESSMENT*. https://drones.gov.cy/gr/sora-risk-assessment/. (accessed 2025-10-13).
30. *Specific Operations Risk Assessment (SORA)*. https://www.easa.europa.eu/en/domains/drones-air-mobility/operating-drone/specific-category-civil-drones/specific-operations-risk-assessment-sora#group-easa-downloads. (accessed 2025-10-14).
31. Shang, K.; Hossen, Z. *Applying Fuzzy Logic to Risk Assessment and Decision-Making*; Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries, 2013.
32. Wang, J.; Fan, K.; Mo, W.; Xu, D. A Method for Information Security Risk Assessment Based on the Dynamic Bayesian Network. In *International Conference on Networking and Network Applications (NaNA)*; Hakodate, Japan, 2016; pp 279–283. https://doi.org/10.1109/NaNA.2016.50.
33. Shapiro, A. F.; Marie-Claire, K. *Risk Assessment Applications of Fuzzy Logic*; Canadian Institute of Actuaries, Society of Actuaries, Casualty Actuarial Society, 2015.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

34. Sallam, H. Cyber Security Risk Assessment Using Multi Fuzzy Inference System. *International Journal of Engineering and Innovative Technology (IJEIT)* **2015**, *4* (8), 13–19.
35. Lee, M.-C. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. *International Journal of Computer Science & Information Technology (IJCSIT)* **2014**, *6* (1), 29–45. https://doi.org/10.5121/ijcsit.2014.6103.
36. *Safety Management Systems (SMS) for Airports and Airport Projects*. https://www.faa.gov/airports/airport_safety. (accessed 2025-10-24).
37. Gonçalves, P.; Sobral, J.; Ferreira, L. Unmanned Aerial Vehicle Safety Assessment Modelling through Petri Nets. *Reliability Engineering and System Safety* **2017**, *167*, 383–393. https://doi.org/10.1016/j.ress.2017.06.021.
38. Ferrigan, J. *Safety Risk Assessment for UAV Operation*; AeroTract Geospatial, 2022.
39. *DJI Agras T30," DJI Sciences and Technologies Ltd*. Available online: https://www.dji.com/global/t30. (accessed 2025-12-22).
40. Neff, P.; Garman, K. Identifying and Mitigating Human Factors Errors in Unmanned Aircraft Systems. In *16th AIAA Aviation Technology, Integration, and Operations Conference*; 2016. https://doi.org/10.2514/6.2016-3593.
41. Sankararaman, Shankar.; Krishnakumar, K. Towards A Computational Framework for Autonomous Decision-Making in Unmanned Aerial Vehicles. In *AIAA Information Systems-AIAA Infotech at Aerospace*; Texas, 2017. https://doi.org/10.2514/6.2017-0446.
42. Johnsen, S.; Evjemo, T. E. State of the Art of Unmanned Aircraft Transport Systems in Industry Related to Risks, Vulnerabilities and Improvement of Safety. In *29th International European Safety and Reliability Conference*; Hannover, Germany, 2019. https://doi.org/10.3850/978-981-11-2724-3_0151-cd.
43. Ancel, E.; Capristan, F. M.; Foster, J. V. Real-Time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM). In *17th AIAA Aviation Technology, Integration, and Operations Conference*; Denver, Colorado, 2017. https://doi.org/10.2514/6.2017-3273.
44. Javaid, A. Y.; Sun, W.; Devabhaktuni, V. K.; Alam, M. Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In *IEEE Conference on Technologies for Homeland Security (HST)*; IEEE: Waltham, MA, USA, 2012; pp 584–590. https://doi.org/10.1109/THS.2012.6459914.
45. Moud, H. I.; Shojaei, A.; Flood, I.; X. Zhang. Monte Carlo Based Risk Analysis of Unmanned Aerial Vehicle Flights over Construction Job Sites. In *9th International Conference on Simulation and Modeling Methodologies, Technologies and Applications*; Porto, Portugal, 2018. https://doi.org/10.5220/0006868804510458.
46. Izadi, H. M.; Shojaei, A.; Flood, I.; Zhang, X.; Hatami, M. Qualitative and Quantitative Risk Analysis of Unmanned Aerial Vehicle Flights over Construction Job Sites. In *The Eighth International Conference on Advanced Communications and Computation (INFOCOMP) 2018*; Barcelona, Spain, 2018.
47. Aliyari, M.; Ashrafi, B.; Ayele, Y. Z. Hazards Identification and Risk Assessment for UAV–Assisted Bridge Inspections. *Structure and Infrastructure Engineering* **2021**, *18* (5), 421–428. https://doi.org/10.1080/15732479.2020.1858878.
48. Xu, Y.; Turkan, Y. The Development of a Safety Assessment Model for Using Unmanned Aerial Systems (UAS) in Construction. *Safety Science* **2022**, *155*, 105893. https://doi.org/10.1016/j.ssci.2022.105893.
49. Kaplan, S.; Garrick, J. B. On the Quantitative Definition of Risk. *Risk Analysis* **1981**, *1* (1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.
50. Tweneboah-Koduah, S.; Buchanan, W. J. Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *The Computer Journal* **2018**, *61* (9), 1389–1406. https://doi.org/10.1093/comjnl/bxy002.
51. *Glossary, National Institute of Standards and Technology*. Available online: https://csrc.nist.gov/glossary/term/asset. (accessed 2025-10-28).
52. Fikri, A. M.; Putra, F. A.; Suryanto, Y.; Ramli, Kallamullah. Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science* **2019**, *61*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234.
53. Putra, A.; Soewito, B. Integrated Methodology for Information Security Risk Management Using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications* **2023**, *14* (4). https://doi.org/10.14569/IJACSA.2023.0140468.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

54. Saaty, T. L. *The Analytic Hierarchy Process*; McGraw-Hill: New York, 1980.
55. Aminbakhsh, S.; Gunduz, M. G.; Sonmez, R. Safety Risk Assessment Using Analytic Hierarchy Process (AHP) during Planning and Budgeting of Construction Projects. *Journal of Safety Research* **2013**, *46*, 99–105.
56. Saaty, R. W. The Analytic Hierarchy Process - What It Is and How It Is Used. *Mathematical Modelling* **1987**, *9* (3–5), 161–176.
57. Vaidya, O. S.; Kumar, S. Analytic Hierarchy Process: An Overview of Applications. *European Journal of Operational Research* **2006**, *169* (1), 1–29. https://doi.org/10.1016/j.ejor.2004.04.028.
58. Cheng, E. W.; Li, H. Analytic Hierarchy Process: An Approach to Determine Measures for Business Performance. *Measuring Business Excellence* **2001**, *5* (3), 30–37. https://doi.org/10.1108/EUM0000000005864.
59. Shin, D. Woong.; Shin, Yoonseok.; Kim, G. H. Comparison of Risk Assessment for a Nuclear Power Plant Construction Project Based on Analytic Hierarchy Process and Fuzzy Analytic Hierarchy Process. *Journal of Building Construction and Planning Research* **2016**, *4* (3), 157–171. https://doi.org/10.4236/jbcpr.2016.43010.
60. Siddayao, G.; Valdez, S. E.; Fernandez, P. L. Analytic Hierarchy Process (AHP) in Spatial Modeling for Floodplain Risk Assessment. *International Journal of Machine Learning and Computing* **2014**, *4* (5), 450–457. https://doi.org/10.7763/IJMLC.2014.V4.453.
61. Hsiao, L.-S.; Huang, C.-Jan.; Liu, H.-T.; Lin, I.-L. An AHP-Based Assessment of the Relative Importance of Risk Factors in Project Management: Designing a Bid Preparation Checklist. *Systems* **2025**, *13* (5), 328. https://doi.org/10.3390/systems13050328.
62. Mustafa, M. A.; Al-Bahar, J. Project Risk Assessment Using the Analytic Hierarchy Process. *IEEE Transactions on Engineering Management* **1991**, *38* (01), 46–52.
63. Canco, I.; Kruja, D.; Iancu, T. AHP, a Reliable Method for Quality Decision Making: A Case Study in Business. *Sustainability* **2021**, *13* (24), 13932. https://doi.org/10.3390/su132413932.
64. Yang, H.; Chen, P.; Huang, Y.; Ma, J.; Guo, F.; Yu, H.; Xu, W.; Han, L.; Cao, H. Research on Real Time Risk Monitoring System of Airline Operation Based on AHP. In *IEEE International Conference on Computer Science and Educational Informatization (CSEI)*; IEEE: Kunming, China, 2019. https://doi.org/10.1109/CSEI47661.2019.8938848.
65. Peng, G.; Han, L.; Liu, Z.; Guo, Y.; Yan, J.; Jia, X. Application of Fuzzy Analytic Hierarchy Process in Risk Evaluation Model. *Frontiers in Psychology* **2021**, *12*. https://doi.org/10.3389/fpsyg.2021.715003.
66. Calik, I.; Kerim, K.; Onur, Ş. Life Cycle Risk Management for Improving Labor Productivity in Construction Projects in Türkiye. *Buildings* **2025**, *15* (3), 484. https://doi.org/10.3390/buildings15030484.
67. Bamakan, S. M. H.; Dehghanimohammadabadi, M. A Weighted Monte Carlo Simulation Approach to Risk Assessment of Information Security Management System. *International Journal of Enterprise Information Systems* **2016**, *11* (4), 63–78. https://doi.org/10.4018/IJEIS.2015100103.
68. Xiao, L.; Qi, Y.; Li, Q. Information Security Risk Assessment Based on Analytic Hierarchy Process and Fuzzy Comprehensive. In *International Conference on Risk Management & Engineering Management*; IEEE: Beijing, China, 2008; pp 404–409. https://doi.org/10.1109/ICRMEM.2008.71.
69. Thompson, A.; Alese, B.; Folasade, A.; Ayeni, O. Information Security Risk Analysis Using Analytic Hierarchy Process and Fuzzy Comprehensive Evaluation. *International Journal of Computer Science and Information Security (IJCSIS)* **2020**, *18* (6), 36–45.
70. Fu, S.; Zhou, H. The Information Security Risk Assessment Based on AHP and Fuzzy Comprehensive Evaluation. In *IEEE 3rd International Conference on Communication Software and Networks*; Xi'an, China, 2011; pp 124–128. https://doi.org/10.1109/ICCSN.2011.6014018.
71. Tsai, H.-Y.; Huang, Y.-L. An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks. *IEEE Transactions on Reliability* **2011**, *60* (4), 801–816. https://doi.org/10.1109/TR.2011.2170117.
72. Zhao, Y.; Jiao, J.; Zhao, T. A Synthetic Risk Assessment Model Based on AHP. In *Reliability and Maintainability Symposium*; IEEE: Colorado Springs, CO, USA, 2014; pp 1–6. https://doi.org/10.1109/RAMS.2014.6798469.
73. Kobaszyńska-Twardowska, A.; Łukasiewicz, J.; Sielicki, P. W. Risk Management Model for Unmanned Aerial Vehicles during Flight Operations. *Materials* **2022**, *15* (7), 2448. https://doi.org/10.3390/ma15072448.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

74. Li, X.; Sun, X.; Fang, M. Risk Assessment of Unmanned Aerial Vehicle (UAV) Operations Based on Bayesian Network. In *2022 2nd International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR)*; Xi'an, China, 2022; pp 189–193. https://doi.org/10.1109/ICBAR58199.2022.00043.
75. Du, S.; Zhong, G.; Wang, F.; Pang, B.; Zhang, H.; Jiao, Q. Safety Risk Modelling and Assessment of Civil Unmanned Aircraft System Operations: A Comprehensive Review. *Drones* **2024**, *8* (8), 354. https://doi.org/10.3390/drones8080354.
76. Benarbia, T.; Kyamakya, K. A Literature Review of Drone-Based Package Delivery Logistics Systems and Their Implementation Feasibility. *Sustainability* **2022**, *14* (1), 360. https://doi.org/10.3390/su14010360.
77. Mohsan, S. A. H.; Khan, M. A.; Noor, F.; Ullah, I.; Alsharif, M. H. Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review. *Drones* **2022**, *6* (6), 147. https://doi.org/10.3390/drones6060147.
78. Derhab, A.; Cheikhrouhou, O.; Allouch, A.; Koubaa, A.; Qureshi, B.; Ferrag, M. A.; Maglaras, L.; Khan, F. Internet of Drones Security: Taxonomies, Open Issues, and Future Directions. *Vehicular Communications* **2023**, *39*. https://doi.org/10.1016/j.vehcom.2022.100552.
79. Ordoukhanian, E.; Madni, A. Resilient Multi-UAV Operation: Key Concepts and Challenges. In *AIAA Science and Technology Conference and Expo*; AIAA, 2016. https://doi.org/10.2514/6.2016-0475.
80. Fitrikananda, B. P.; Jenie, Y. I.; Sasongko, R. A.; Muhammad, H. Risk Assessment Method for UAV's Sense and Avoid System Based on Multi-Parameter Quantification and Monte Carlo Simulation. *Aerospace* **2023**, *10* (9), 781. https://doi.org/10.3390/aerospace10090781.
81. Susini, A. A Technocritical Review of Drones Crash Risk Probabilistic Consequences and Its Societal Acceptance. In *Risk Information Management, Risk Models and Applications (RIMMA)*; Berlin, 2015; Vol. 7, pp 27–38.
82. Ficco, M.; Granata, D.; Palmieri, F.; Rak, M. A Systematic Approach for Threat and Vulnerability Analysis of Unmanned Aerial Vehicles. *Internet of Things* **2024**, *26*.
83. Kumar, S.; Tiwari, A.; Ahirwar, Y.; Kumar, G.; Arafat, M. Y. The Rise of UAV-Based Smart Surveillance: A Systematic Review of Trends and Technologies. *IEEE Access* **2025**, *13*, 181553–181575. https://doi.org/10.1109/ACCESS.2025.3621736.
84. Tsao, K.-Y.; Gilder, T.; Vassilakis, V. G. A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-Hoc Networks. *Ad Hoc Networks* **2022**, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894.
85. Chitta, S.; Jain, R. Last Mile Delivery Using Drones. In *Technology Convergence, innovation & Decision Sciences*; Seoul, South Korea, 2017.
86. Saripalli, P.; Walters, B. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In *IEEE 3rd International Conference on Cloud Computing*; IEEE: Miami, FL, USA, 2010; pp 280–288. https://doi.org/10.1109/CLOUD.2010.22.
87. Pant, S.; Kumar, A.; Ram, M.; Klochkov, Y.; Sharma, H. K. Consistency Indices in Analytic Hierarchy Process: A Review. *Mathematics* **2022**, *10* (8), 1206. https://doi.org/10.3390/math10081206.
88. Koulinas, G.; Marhavilas, Panagiotis. K.; Demesouka, O.; Vavatsikos, A. Risk Analysis and Assessment in the Worksites Using the Fuzzy-Analytical Hierarchy Process and a Quantitative Technique – A Case Study for the Greek Construction Sector. *Safety Science* **2019**, No. 112, 96–104. https://doi.org/10.1016/j.ssci.2018.10.017.
89. Szabo, Z. K.; Szádoczki, Z.; Bozóki, S.; Stănciulescu, G. C.; Szabo, D. An Analytic Hierarchy Process Approach for Prioritisation of Strategic Objectives of Sustainable Development. *Sustainability* **2021**, *13* (4), 2254. https://doi.org/10.3390/su13042254.
90. Li, N.; Liu, X.; Yu, B.; Li, L.; Xu, J.; Tan, Q. Study on the Environmental Adaptability of Lithium-Ion Battery Powered UAV under Extreme Temperature Conditions. *Energy* **2021**, *219*, 119481. https://doi.org/10.1016/j.energy.2020.119481.
91. *4 Factors That Impact Drone Flight Times*. Agri Spray Drones. Available Online: https://agrispraydrones.com/blogs/news/4-factors-that-impact-drone-flight-times. (accessed 2026-01-14).
92. Callahan, M. A.; Sexton, K. If Cumulative Risk Assessment Is the Answer, What Is the Question? *Environ Health Perspect* **2007**, *115* (5), 799–806. https://doi.org/10.1289/ehp.9330.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

93. Callahan, M. A. *Framework for Cumulative Risk Assessment*; U.S. Environmental Protection Agency (EPA): Washington, DC, 2003.
94. Vafaei, N.; Ribeiro, R.; Camarinha-Matos, L. M. Normalization Techniques for Multi-Criteria Decision Making: Analytical Hierarchy Process Case Study. In *IFIP Advances in Information and Communication Technology*; Costa de Caparica, Portugal, 2016. https://doi.org/10.1007/978-3-319-31165-4_26.
95. Trung, D. D. Development of Data Normalization Methods for Multi-Criteria Decision Making: Applying for MARCOS Method. *Manufacturing Review* **2022**, *9* (22). https://doi.org/10.1051/mfreview/2022019.
96. *Delivery Drones Market Report 2026*. Available Online: https://www.thebusinessresearchcompany.com/report/delivery-drones-global-market-report. (accessed 2026-01-22).
97. Yang, H.; Lee, Y.; Jeon, S.-Y.; Lee, D. Multi-Rotor Drone Tutorial: Systems, Mechanics, Control and State Estimation. *Intelligent Service Robotics* **2017**, *10* (3), 79–93. https://doi.org/10.1007/s11370-017-0224-y.
98. Alkouz, B.; Shahzaad, B.; Bouguettaya, A. Service-Based Drone Delivery. In *IEEE 7th International Conference on Collaboration and Internet Computing (CIC)*; Atlanta, GA, USA, 2021; pp 68–76. https://doi.org/10.1109/CIC52973.2021.00019.
99. Ghamari, M.; Rangel, P.; Mehrubeoglu, M.; Tewolde, G. S.; Sherratt, R. S. Unmanned Aerial Vehicle Communications for Civil Applications: A Review. *IEEE Access* **2022**, *10*, 102492–102531. https://doi.org/10.1109/ACCESS.2022.3208571.
100. Anbaroglu, B. Parcel Delivery In An Urban Environment Using Unmanned Aerial Systems: A Vision Paper. In *ISPRS Annals of Photogrammetry, Remote Sensing and Spatial Information Sciences*; 2017; pp 73–79. https://doi.org/10.5194/isprs-annals-IV-4-W4-73-2017.
101. *DJI FlyCart 30: Dynamic Aerial Delivery*. Available Online: https://www.dji.com/global/flycart-30. (accessed 2024-12-16).
102. *30 Things to Know About DJI FlyCart 30*. Available Online: https://enterprise-insights.dji.com/blog/30-things-to-know-about-dji-flycart30. (accessed 2024-12-13).
103. Hossain, N. U. I.; Lutfi, M.; Ahmed, I.; Akundi, A.; Cobb, D. Modeling and Analysis of Unmanned Aerial Vehicle System Leveraging Systems Modeling Language (SysML). *Systems* **2022**, *10* (6), 264. https://doi.org/10.3390/systems10060264.
104. Barros, J.; Henriques, J.; Reis, J.; Rosado, D. P.; Melao, N. Unmanned Aerial Systems: A Systematic Literature Review. In *Information Technology and Systems*; Springer: Temuco, Chile, 2024; pp 82–93. https://doi.org/10.1007/978-3-031-54235-0_8.
105. Osmani, K.; Schulz, D. Comprehensive Investigation of Unmanned Aerial Vehicles (UAVs): An In-Depth Analysis of Avionics Systems. *Sensors* **2024**, *24* (10). https://doi.org/10.3390/s24103064.
106. El Safany, R.; Bromfield, M. A Human Factors Accident Analysis Framework for UAV Loss of Control in Flight. *The Aeronautical Journal* **2025**, *129*, 1–27. https://doi.org/10.1017/aer.2025.24.
107. *UAS Regulations: Common European rules for UAS*. Available Online: https://drones.gov.cy/regulations/. (accessed 2026-01-26).
108. Xu, C.; Liao, X.; Tan, J.; Ye, H.; Lu, H. Recent Research Progress of Unmanned Aerial Vehicle Regulation Policies and Technologies in Urban Low Altitude. *IEEE Access* **2020**, *8*, 74175–74194. https://doi.org/10.1109/ACCESS.2020.2987622.
109. Gao, M.; Hugenholtz, C.; Fox, T.; Kucharczyk, Maya.; Barchyn, T.; Nesbit, P. Weather Constraints on Global Drone Flyability. *Scientific Reports* **2021**, *11* (1), 12092. https://doi.org/10.1038/s41598-021-91325-w.
110. *Why Your Drone Battery Life Is Getting Shorter (And How to Fix It)*. Available Online: https://www.ctechigroup.com/why-your-drone-battery-life-is-getting-shorter-and-how-to-fix-it.html. (accessed 2025-01-13).
111. Lv, S.; Wang, X.; Lu, W.; Zhang, J. Z.; Ni, H. The Influence of Temperature on the Capacity of Lithium Ion. *Energies* **2022**, *15* (1), 60. https://doi.org/10.3390/en15010060.
112. Wawrzyn, D. *Some Helpful Tips for Maximizing Your Drone's Battery Life*. Available Online: https://www.propelleraero.com/blog/some-helpful-tips-for-maximizing-your-drones-battery-life/. (accessed 2025-01-13).

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

113. Zhang, J.; Campbell, J. F.; Sweeney, D. C.; Hupman, A. C. Energy Consumption Models for Delivery Drones: A Comparison and Assessment. *Transportation Research Part D: Transport and Environment* **2021**, *90*, 102668. https://doi.org/10.1016/j.trd.2020.102668.
114. Akram, N.; Khoshrangbaf, M.; Challenger, M.; Dagdeviren, O. Energy Consumption Modeling and Flight Time Analysis of Micro Drones. *IEEE Access* **2025**, *13*, 109854-109866,]. https://doi.org/10.1109/ACCESS.2025.3581944.
115. Benson, T. *Aerodynamics Index*. Available Online: https://www.grc.nasa.gov/www/k-12/VirtualAero/BottleRocket/airplane/drageq.html (accessed 2026-03-21).
116. Susi, J.; Unt, K.-E.; Heering, S. Determining the Efficiency of Small-Scale Propellers via Slipstream Monitoring. *Drones* **2022**, *7* (6), 381. https://doi.org/10.3390/drones7060381.
117. *Aerodynamics for Students*. Available Online: https://aerospace101.com/aircraft-performance/rotor-momentum-analysis.html. (accessed 2026-01-16).
118. Grindley, B.; Phillips, K.; Parnell, K. J.; Cherrett, T.; Scanlan, J.; Plant, K. L. Over a decade of UAV incidents: A human factors analysis of causal factors. *Applied Ergonomics* **2024**, *121*, 104355. https://doi.org/10.1016/j.apergo.2024.104355.
119. Kumar, S. M.; Kasbekar, G. S.; Maity, A. Identification of GPS Spoofing as a Drone Cyber-Vulnerability and Evaluation of Efficacy of Asynchronous GPS Spoofing. In *22nd IFAC Symposium on Automatic Control in Aerospace (ACA 2022)*; Mumbai, India, 2022; Vol. 55, pp 394–399. https://doi.org/10.1016/j.ifacol.2023.03.066.
120. *Drone Spoofing and Countermeasure*. Available Online: https://www.nqdefense.com/anti-drone-drone-spoofing-and-countermeasure/. (accessed 2026-01-10).
121. *Drone Laws in Cyprus*. Available Online: https://uavcoach.com/drone-laws-in-cyprus/. (accessed 2025-05-08).
122. *What is drone jamming and how can it be countered?* Available Online: https://doodlelabs.com/what-is-drone-jamming/. (accessed 2026-01-31).
123. Zhang, X.; Liu, Y.; Zhang, Y.; Guan, X.; Delahaye, D.; Tang, L. Safety Assessment and Risk Estimation for Unmanned Aerial Vehicles Operating in National Airspace System. *Journal of Advanced Transportation* **2018**, *2*, 1–11. https://doi.org/10.1155/2018/4731585.
124. Petritoli, E.; Leccese, F.; Ciani, L. Reliability Assessment of UAV Systems. In *IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace*; IEEE: Padua, Italy, 2017; pp 266–270. https://doi.org/10.1109/MetroAeroSpace.2017.7999577.
125. Waliullah, M.; Gan, D. Wireless LAN Security Threats and Vulnerabilities. *International Journal of Advanced Computer Science and Applications* **2014**, *5* (1), 176–183. https://doi.org/10.14569/IJACSA.2014.050125.
126. Petritoli, E.; Leccese, F.; Ciani, L. Reliability and Maintenance Analysis of Unmanned Aerial Vehicles. *Sensors* **2018**, *18* (9), 3171. https://doi.org/10.3390/s18093171.
127. Selvamuthu, D.; Singla, I.; Agarwal, D. Reliability and Maintainability Analysis of UAV Systems: An Analytical Approach. In *IEEE Space, Aerospace and Defence Conference (SPACE)*; IEEE: Bangalore, India, 2025; pp 1–6. https://doi.org/10.1109/SPACE65882.2025.11171267.
128. Fusaro, R.; Chiesa, S.; Cresto Aleina, S.; Fioriti, M. Ontribution To R.A.M.S Estimation in Early Design Phases of Unmanned Aerial Vehicles - UAVs. **2015**, *16*, 73–83.
129. *Maintainability*. Available Online: https://www.sciencedirect.com/topics/engineering/maintainability#:~:text=Maintainability%20is%20defined%20as%20the,in%20accordance%20with%20prescribed%20procedures.. (accessed 2026-01-04).
130. Gudmundsson, S. Chapter 1 - The Aircraft Design Process. In *General Aviation Aircraft Design*; Elsevier, 2013; pp 1–32. https://doi.org/10.1016/B978-0-12-818465-3.00001-X.
131. Mohammad, A. J.; Hutchison, D.; Sterbenz, J. P. G. Towards Quantifying Metrics for Resilient and Survivable Networks. In *14th IEEE International Conference on Network Protocols (ICNP 2006)*; Santa Barbara, California, USA, 2006.
132. Ellison, R. J.; Fisher, D.; Linger, R.; Lipson, H.; Longstaff, T.; Mead, N. *Survivable Network Systems: An Emerging Discipline*; 1999.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 March 2026 doi:10.20944/preprints202603.2408.v1

133. Vaezi, A.; Jones, S.; Asgary, A. Integrating Resilience into Risk Matrices: A Practical Approach to Risk Assessment with Empirical Analysis. *Journal of Risk Analysis and Crisis Response* **2023**, *13* (4), 252–272. https://doi.org/10.54560/jracr.v13i4.411.
134. *Jamming and Spoofing Protection for UAVs Using GNSS Signals*. Available Online: https://safran-navigation-timing.com/jamming-and-spoofing-protection-for-uavs-using-gnss-signals/. (accessed 2025-12-01).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.