Supplementary Material S1

Qualitative Analysis

Tables S1 to S4 below illustrate the final outcomes of the qualitative element resulted from the application of the proposed risk methodology on the use-case scenario.

Table S1. Association of Assets - Vulnerabilities

Assets	**Vulnerabilities**
Aircraft (Airborne Component)	Ineffective Power Source High Power Consumption Defective Components Wrong Handling
Controller (Ground Control Station)	Defective Components Wrong Handling
Communication Links (Wireless Medium)	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

Table S2. Association of Vulnerabilities – Threats

Vulnerabilities	Threats
Ineffective Power Source	Power Failure Equipment Failure Extreme Weather Conditions
High Power Consumption	Power Failure Control Loss Wireless Attacks Extreme Weather Conditions Unsuccessful Navigation
Defective Components	Equipment Failure
Wrong Handling	Control Loss Wireless Attacks Unsuccessful Navigation
Susceptibility to Wireless Attacks	Power Failure Control Loss Wireless Attacks Collision w/objects Unsuccessful Navigation
Susceptibility to Weather Conditions	Power Failure Control Loss Extreme Weather Conditions Unsuccessful Navigation
Lack or Violation Policies/Regulations	Control Loss Collision w/objects Physical Attacks (Unauthorised Access)
Faulty Operation	Control Loss Collision w/objects Unsuccessful Navigation
Lack of Expertise/Training/Skills	Control Loss Collision w/objects Unsuccessful Navigation
Susceptibility to Adversarial Actions	Collision w/objects Unsuccessful Navigation Physical Attacks (Unauthorised Access)

Table S3. Association of Threats – Impact Requirements

Threats	**Impact Requirements**
Power Failure ***(Structural Threat Event)***	Availability Reliability Survivability
Equipment Failure ***(Structural Threat Event)***	Availability Maintainability Survivability
Control Loss ***(Accidental Threat Event)***	Availability Safety
Wireless Attacks ***(Adversarial Threat Event)***	Confidentiality Integrity Availability Maintainability
Extreme Weather Conditions ***(Environmental Threat Event)***	Reliability Maintainability Survivability
Collision w/objects ***(Accidental Threat Event)***	Availability Safety Maintainability
Unsuccessful Navigation ***(Accidental Threat Event)***	Availability Safety Reliability
Physical Attacks (Unauthorized Access) ***(Adversarial Threat Event)***	Confidentiality Integrity Availability Maintainability

Table S4. Impact Requirements – Explanation and Examples

Requirement	Description Impact Examples
Confidentiality	The property of restricting unauthorised personnel from accessing system's components, mission-critical or sensitive information [13]. Essentially, keeping components or data confidential means keeping them secret [21], [86]. Unauthorised access to system's equipment and communication medium disclosure (eavesdropping or man-in-the-middle attacks, jamming, active interfering [84]) are some examples of threats intimidating system's confidentiality.
Integrity	Represents the control of information and equipment from improper modification or destruction, including ensuring information non-reputation and authenticity [125]. Damaging integrity means tampering with equipment and that data or messages exchanged between system's components are executed, modified, suspended, copied, replayed or deleted by an illicit entity [71]. Backdoor malware, data tampering (data being altered during transmission), impersonation (unauthorised or malicious drone being connected to the system), insider (sensitive data leakage leading to privacy issues), Man-in-the-Middle, modification (equipment, data or message manipulation), sybil, injection attacks and wormhole are examples of attacks threatening a drone-based system's integrity [13], [84].
Availability	To be 'ready to operate' [126]. It is the ability of the system to be in state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided [124]. In this study 'Availability' is endangered if any of the system's assets, is spoofed, penetrated, suspended, disrupted, physically tampered and cannot operate as expected thus becoming temporarily or indefinitely accessible or available in an adequate manner [13], [71]. Control loss or unsuccessful navigation could lead to a considerable condition of system's unavailability. Even the theft of a package to be delivered could be considered as a violation of system's availability [2], leading to its inability to accomplish to its main task. Moreover, GPS spoofing, Wi-Fi jamming or network disruptions can have potential cause loss of connectivity, impacting the availability of communication and data exchange [13].
Reliability	Closely related to availability, Reliability is defined as 'The probability that a system, subsystem or component is able to perform specific function in a pre-established time under pre-established conditions' [124], [126]. Thus, since drone-based systems deployed for critical operations, are called to operate in environmentally uncontrolled areas which cannot be inhabited during flight and being exposed to environmental extremes of pressure, temperature and shock, reliability is proposed to be considered and evaluated through the step of impact determination [128]. Inability for an asset to perform a task under unexpected situation, unreliable battery capacity or the failure of the operator to navigate the system properly due to improper training or expertise, consist conditions of violating a system's reliability [2].
Safety	The condition of being protected from harm or other non-desirable outcomes. Safety can also refer to the control of hazards to achieve an acceptable level of risk. It is considered as an additional requirement to be used for the measurement of existing controls and mechanisms for the prevention of threat attacks [126]. Relies on the fact that in case of an accidental or adversarial threat event not only the system itself is going to be under difficult situation but also human lives. Loss of lives or injuries due to control loss, unsuccessful navigation or collision with objects a[123]re some examples of possible impact on system's safety. Injury from a dropped package is a safety's compromise [2]/
Survivability	The capability of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures, or accidents [131], [132]. It is considered as the most important objective to be assessed and evaluated due to the nature of the threats and the type of the missions that aerial systems are called to accomplish. For this study, impact on system's survivability is mostly related to threats such as extreme weather conditions and failures

	that are affecting the asset of aerial component, such as inability to perform a task, damage or loss of component or damage or loss of equipment.
Maintainability	The ability with which maintenance activities can be performed on an asset or equipment. It refers to the ease and efficiency that a piece of equipment in a failed state can be restored to normal operating conditions after undergoing maintenance in accordance with prescribed procedures [129]. In combination with Reliability, Availability and Safety (RAMS Analysis), it is beneficial for someone to increase resilience of a drone, to reduce repair and maintenance costs and also decrease the failure rate [124], [126] and [128]. For this study impact on maintainability is related to the sources that, based on the existing controls, could possibly recover or not after an adverse impact, such as the aerial component after a failure, the communication links after a wireless attack, the controller after a physical attack or even the operator after the violation of any existing policies or regulations