ORIGINAL RESEARCH **Open access**

Preventive Organizational and Technical Measures for Drone Malfunction and User Negligence: A Stakeholder-Centric Approach

Ravi Kumar[1*], Neha Sharma[1], Aniket Deshmukh[2], Sanjay Kulkarni[3], Arjun Nair[4]

Abstract

Drones are now being incorporated into a growing range of operations across multiple fields, including military, commercial, and personal applications. The current legal framework falls short in adequately addressing accountability and proactive safeguards when vulnerabilities are exploited or negligence occurs during drone operations. The industry can effectively address these gaps by embedding solutions into technological development and standardization initiatives. These factors are particularly significant because improper drone use can have substantial consequences for people, assets, and structures located in the operational airspace. This study seeks to explore how these matters are addressed under current laws and how they are perceived by people, while accounting for the technical features and the full network of participants involved in drone activities. For this purpose, we conducted an extensive survey completed by 233 participants from organizations focused on IT, legal matters, and cybersecurity. The collected data were examined both qualitatively and quantitatively. The outcomes point out specific gaps in today's standards and indicate that: (1) participants throughout the drone network are seen as jointly accountable in particular scenarios, (2) responsibility for putting preventive actions in place needs to be spread among all relevant drone stakeholders, and (3) automated preventive systems are regarded as more beneficial than direct human involvement when dealing with drone failures or improper use. We also suggest adjustments to policy frameworks to better address the highlighted scenarios. These research findings can guide policymakers toward strengthening the existing standardization system and related technologies for drone operations. They also support stakeholders in fostering greater confidence among drone users. In addition, the paper offers valuable guidance for manufacturers of drone software and hardware to fine-tune their designs and build user confidence. Overall, confidence in the use of drones for both commercial and individual use grows when robust standardization is combined with well-designed incident response plans that address potential harm to drones or to external parties.

Keywords Vulnerability management, User-centric security, Security by design, Digital responsibility

*Correspondence:
Ravi Kumar
ravi.kumar@iari.res.in
[1] Department of AI for Mango and Coconut Yield Prediction, Faculty of Agriculture, Indian Agricultural Research Institute, New Delhi, India
[2] Department of Machine Learning for Monsoon Onset and Crop Sowing Dates, Faculty of Agriculture, IIT Bombay, Mumbai, India
[3] Department of Smart Soil Moisture Monitoring, Faculty of Agriculture, Savitribai Phule Pune University, Pune, India
[4] Department of Precision Disease Forecasting, Faculty of Agriculture, IIT Kharagpur, Kharagpur, India

Introduction

Over the past few years, drone applications have expanded considerably for military, commercial, and personal needs. Overall, increased digital integration generally increases exposure to risks [1]. These risks cover situations that fall into

This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits non-commercial use, distribution, reproduction, and adaptation in any medium or format, provided that appropriate credit is given to the original author(s) and source, a link to the license is provided, and any changes made are indicated. Adapted material must be distributed under the same license.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

three broad groups: user actions that result in financial losses, effective cyber intrusions, and mistakes or technical failures in the drone system (affecting either software or hardware). The sections that follow analyze each of these three groups, providing examples of possible situations and technical explanations of the related cyber risks. In this regard, potential causes of financial losses can be divided into two groups: internal and external [2]. Internal causes mostly involve mistakes, incorrect setups, or defects in the drone's software or hardware. External causes primarily involve deliberate interventions by individuals or organizations intended to cause financial harm. Such external influences can originate from the operator or from outside actors intentionally seeking to trigger losses.

The adoption of these advanced technologies has put pressure on current laws governing accountability and risk prevention, prompting fresh interpretations of established rules and underscoring the need for updated regulations tailored to modern technological realities. Broad tort law principles, along with targeted product liability regulations, have proven inadequate for fully managing every scenario that arises in the drone environment [3, 4].

Within this environment, conversations have arisen about specific accountability questions related to careless drone handling and breakdowns stemming from unaddressed weaknesses within the systems [5]. Most of these studies concentrate mainly on the legal dimensions. On the operational side, however, industry-wide standardization, combined with structured internal procedures, is crucial for developing consistent guidelines for the duties and roles of all parties involved across the entire drone lifecycle.

This paper centers on these key liability questions to clarify how they ought to be managed in light of current laws and industry norms, to understand the perspectives of actual drone users, and to recommend updated industry standards that properly assign roles and duties to all involved parties. Beyond that, the paper offers concrete technical safeguards that responsible parties should apply in different situations.

To explore these points, we conducted a detailed qualitative assessment of applicable regulations, taking into account the unique technical aspects of drone operations and the broader set of involved parties.

We also employed a quantitative strategy to cross-check the insights by administering a targeted questionnaire to professionals in the IT, legal, and cybersecurity sectors. The survey focused on views about liability allocation and prevention strategies to gather opinions on preferred methods for handling these issues.

The research yields three core findings:

Civil accountability for careless conduct or failure to act is generally understood as a collective duty shared by several parties in the drone network. This perception arises because each party contributes to the development, configuration, and preparation of the drone for active service.

This observation connects closely to the second finding, which concerns risk prevention. Preventive actions are similarly viewed as a joint responsibility distributed across the drone network, with each participant playing a vital role in executing specific protective measures.

The third finding builds upon the earlier ones. Survey participants expect the drone's software to deliver automatic responses during technical failures and to stop unsafe or careless actions initiated by the drone operator.

These three findings have the potential to enhance ongoing draft standards for Internet of Things technologies, notably NIST SP 800-82 r3 and the proposed EU Cyber Resilience Act, as discussed in greater depth later in the document.

In a novel way, this research connects specific technical situations that can lead to harm through negligence and transforms them into practical standardization actions the industry can adopt to prevent and resolve them, while carefully weighing the contributions each participant in the drone network can make.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Consequently, the study introduces an original approach that reviews both targeted and general legal structures, offers solutions for the identified negligence scenarios, and confirms those solutions using numerical data.

The paper examines the topics mentioned from the perspective of technological workflows and the importance of establishing uniform technical and procedural guidelines within the defined research boundaries, with an emphasis on prevention.

Moreover, the scope is limited to civilian drones, deliberately excluding military and governmental ones, and draws upon existing civil regulations within the European Union as well as fundamental civil law concepts from comparable jurisdictions.

The remaining parts of the paper follow this sequence: Section 2 provides a review of the existing literature on drones, focusing on standardization and cybersecurity. Section 3 then outlines the research hypotheses and goals. Section 4 details the data sources and methods applied. Sections 5 and 6 provide a deeper analysis of the findings and recommend updating standards in line with the results. The final section summarizes the key outcomes, acknowledges study constraints, and suggests avenues for subsequent investigation.

Literature Review

We focused on prior work and further developed a keyword correlation map tied to the main topic **(Figure 1)** to underscore the value of the associated scholarly contributions.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

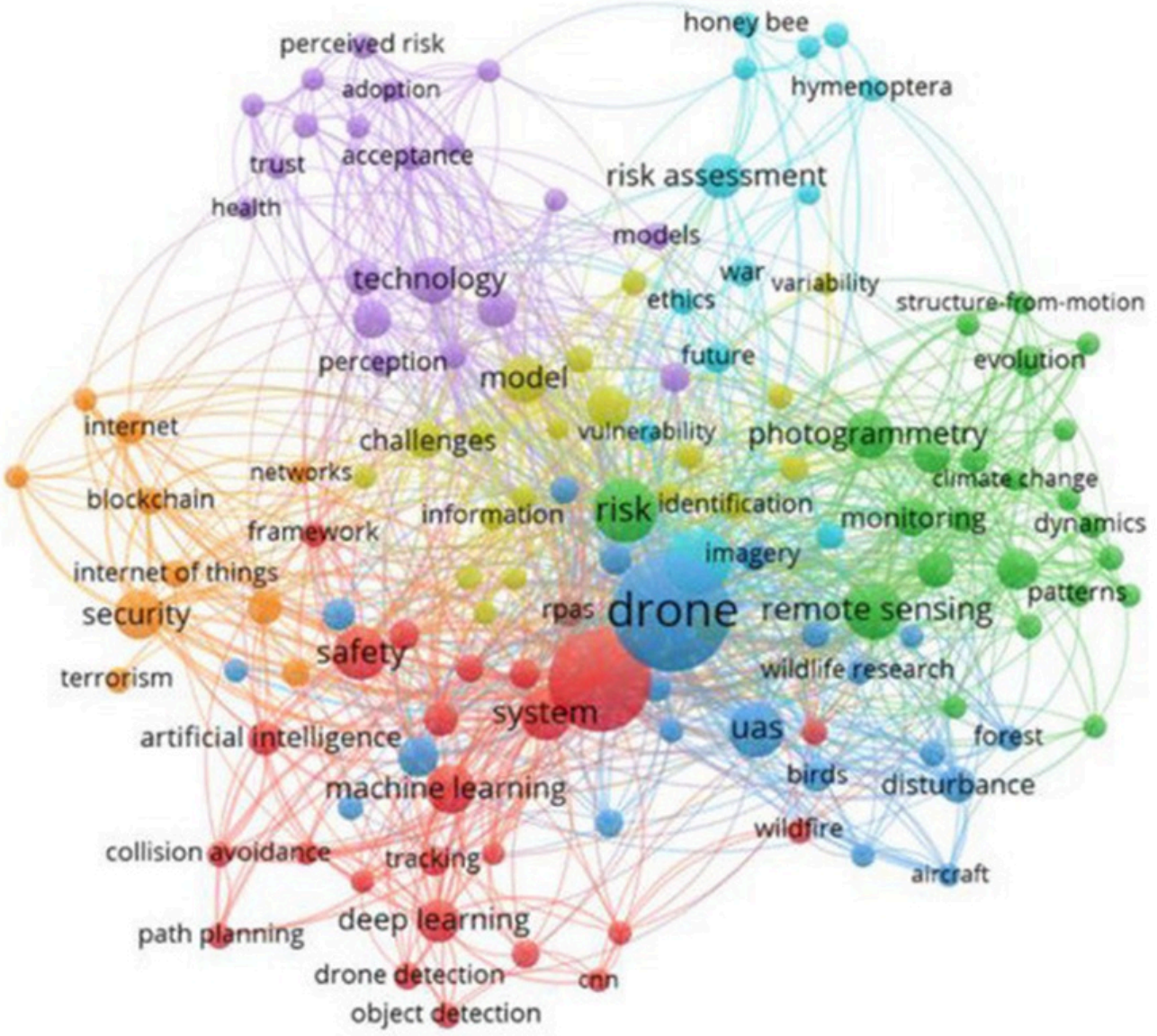

Figure 1. Map of articles relevant to the keywords using the Web of Science database.

The entries in this map demonstrate the two primary research pathways in the area: one covering organizational and standardization topics (such as frameworks, risk assessment, perception, acceptance, and monitoring), and the other focusing on practical technical applications (such as vulnerability, path planning, and collision avoidance).

A large portion of current drone-related publications focus on how these devices function [6] or on their benefits across multiple industries [7]. Naturally, such works have enhanced comprehension of device management and offered a comprehensive picture of the wide array of potential uses. Yet writings on damages and civil liability arising from drone activities remain quite scarce.

Looking through the lens of standardization, materials on legal challenges with drones generally review approval procedures and their alignment in defined regions (for example, the European Union). This covers cross-field analyses, such as the one by Konert and Balcerzak [8]. Attention to this has persisted for roughly ten years since drone adoption was still in its early stages.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Nevertheless, several investigations appear in common law settings, mainly from American sources [9], in contrast to civil law regions where coverage on the issue is more limited [10]. Further pieces position drone oversight as an effective model for managing innovative technologies. There are also reviews of legal proceedings involving drone operators, including content from Skytango, which supports enterprise clients overseeing fleets of drone pilots in diverse operational areas [11].

Table 1 offers a concise overview of the five leading cases in this domain to provide context on the outcomes of violating national drone rules. Drawing from recent occurrences, these instances involved the most severe penalties or jail terms. Frequent issues include flying drones in forbidden locations or without required registration.

Table 1. Top 5 cases of drone operators' prosecution.

Country	Fee amount	Cause	Conclusion
United States of America	USD 200,000	The incident was evaluated in October 2015. Initially, a penalty of USD 1.9 million was proposed for 43 unauthorized drone flights over New York and Chicago between 2012 and 2014. SkyPan was also accused of operating 65 drones without proper registration, licensing, or communication equipment. After an agreement with the FAA in January 2017, the penalty was reduced to USD 200,000, with an additional USD 150,000 applicable if regulations were violated again.	The FAA stated that SkyPan operated aircraft outside recommended procedures, creating potential risks to people and property.
United Kingdom	GBP 1,800	Nigel Wilson, a drone hobbyist, conducted nine illegal flights over football stadiums in England and landmarks in central London (including Big Ben and Buckingham Palace), flying as close as approximately 50 m. He uploaded footage of these activities to YouTube. He was fined under the Air Navigation Order (2009).	Wilson's drone use posed a risk to public safety in crowded urban and stadium areas.
United Kingdom	GBP 1,125	Richard Brunner carried out an unauthorized drone flight over a promotional shoot above Hyde Park, flying at a distance of around 10 m.	The location was a restricted area, and flying there required prior authorization.
Netherlands	EUR 8,000	André Rieu, the well-known violinist and conductor, used a drone during a performance at the Vrijthof in Maastricht, where about 12,000 people were present. The area is centrally located, where drone use is prohibited. Although the exact fine was not officially published, press reports estimated it at EUR 8,000, making it the highest fine issued by Dutch authorities.	Drone use over inner-city public events in the Netherlands is prohibited and considered improper.
China	18 months in jail	In 2015, an employee of Beijing UAV Sci-Tech Co was sentenced to 18 months in prison for operating a company drone that interfered with commercial flight operations.	The individual's actions were deemed a serious threat to public aviation safety.

Source: Author's processing, based on a Skytango article.

Some academic works investigate accountability based on overarching tort law concepts but lack an in-depth review of concrete examples. Broad tort law, applicable in both common law and civil law systems, necessitates an act (or failure to act), actual harm to a person or organization, and a clear connection linking them. Under civil law, someone can be held

© 2025 The Author(s). | Published by Agro Intelligence Research Press

responsible for their direct conduct or for issues arising from assets they possess or supervise. Given the multifaceted drone network — involving hardware creators, software developers, system integrators, distributors, regulatory bodies, certifiers, and service maintainers — determining which party's conduct satisfies the tort law requirements for act, cause, and outcome can be complex [12, 13].

Additional publications discuss particular rules, including those from the EU on product accountability. Yet this approach often sidelines contributions from other parties in the drone network [14]. It further emphasizes aftermath scenarios rather than forward-looking prevention. Some research considers UAV applications within global legal frameworks but restricts its scope to individual nations, such as the Netherlands. More works stay narrowly legal without extending to interdisciplinary assessments of operational scenarios [15]. Some also explore moral questions alongside standardization topics [16].

Technically speaking, multiple papers examine strategies to prevent damage or control losses caused by drone operator carelessness [17], as well as ways to spot and fix in-flight failures [18]. Additional technical analyses evaluate the hazards of unmanned aircraft striking the ground [19] and risk-focused methods for addressing them [20]. Other contributions cover airborne platforms (services or applications) that utilize aerial systems, their weaknesses, and approaches to refine configurations and UAV performance to reduce the likelihood of surprises. There exist classifications of cyber risks for drones and corresponding defenses, though there is limited guidance on embedding them into workflows among those designing, maintaining, and operating drones [2, 21]. At present, these elements remain unconnected to matching legal requirements or broader industry rules and standards.

In September 2020, Australia's Civil Aviation Safety Authority issued guidance for micro. It excluded remotely piloted aircraft to support users in understanding and implementing rules and safety protocols before initial and subsequent flights, as well as while airborne, noting restricted zones [22]. This marks an advancement in organizing preventive procedures at a standardized level. Even so, more procedural development is required to fully advance this standardization.

Per details shared in the Dedrone Airspace Security Insight Report 2022, the Federal Aviation Administration in America launched its Airport Unmanned Aircraft Systems Detection and Mitigation Research Program in 2021 [23]. The effort evaluated anti-drone solutions at five key international airports in the US to enhance protection for passengers and piloted aircraft from drone-related threats. In the same year, INTERPOL ran multi-day tests assessing drone defense capabilities in protected airspace via spotting, following, and recognizing both devices and their controllers. These technologies are growing vital for safeguarding airports, airspace, and prohibited zones near populated areas, detention centers, and key facilities. Such advances point to valuable technical features for review and deployment. That said, civilian applications require strong process standardization and organizational frameworks to ensure smooth, successful use.

In June 2022, the Department of Defense Responsible AI Working Council released its strategy document on responsible artificial intelligence practices and rollout paths. It highlights top industry methods for building AI and for employing tools to detect and reduce associated risks throughout an AI system's lifecycle [24]. This offers applicable workflow ideas for drones, especially for mitigating certain failures or operator behavior.

In light of the available scholarship, our paper seeks to connect the determination of liability with the corresponding preventive systems within technological workflows and standardization settings. The present study is part of a larger initiative on proactive cybersecurity for drone operations, which also includes [25, 26].

Hypothesis and Objectives

Prior analyses in the preceding part review the dangers and accountability associated with drone activities from a single legal perspective, failing to investigate cross-dimensional interactions. Creating and operating drones introduces specific cyber weaknesses that can be addressed through technical fixes and avoidance, as well as through standardization or

© 2025 The Author(s). | Published by Agro Intelligence Research Press

process-oriented frameworks. Unfortunately, current writings fall short in assessing technical factors and their implications under standardization and process-based approaches.

Our paper extends the foundation laid by existing sources by probing more deeply into the links between technical and legal aspects. The goal is to reduce the exploitation of weaknesses and raise confidence among users from varied business fields and private individuals alike.

With this in mind, the article aims to identify deficiencies in standardization and technological process setups and propose solutions (specifically regarding negligence, protective measures, and accountability). In seeking appropriate technical solutions for these shortcomings, best practices for prevention were reviewed.

Respondent perspectives on harm from breakdowns and careless actions, plus recommended safeguards, are captured in these goals:

Objective 1 (O1): Gauging views on who bears accountability when events stem from operator carelessness or system failures.

Objective 2 (O2): Gauging which approaches appear effective at stopping harm due to operator carelessness or system failures.

Hypothesis 1 (H1) (regarding O1): Operators of drones are seen as accountable when incidents result from careless flying.

Hypothesis 2 (H2) (regarding O2): Ongoing instruction for drone operators is beneficial for reducing careless incidents.

Hypothesis 3 (H3) (regarding O1): When hardware problems occur, the majority point to the party combining hardware and software components as accountable.

Hypothesis 4 (H4) (regarding O2): Early participants in the drone development cycle are tasked with installing suitable protective systems to mitigate failures and/or operator behavior.

Hypothesis 5 (H5) (regarding O1): Preference leans toward automatic systems instead of human-directed steps when applying protective measures.

Hypothesis 6 (H6) (regarding O1): Creators of drone software carry responsibility for weaknesses in their programs, whether spotted early or later after deployment.

Hypothesis 7 (H7) (regarding O2): Merging instant protective security features for drones with routine checks delivers the strongest protection.

Materials and Methods

In examining this study, we designed and deployed a survey instrument via QuestionPro. This tool helps pinpoint accountability and protective strategies related to drone operations. The survey was prepared in Romanian and English versions and shared with experts online via email and social platforms such as LinkedIn, Twitter, and Facebook. Participation came from specialists in the field during the period from May to July 2021. It included 17 questions total, two of which served to profile the participant group. This paper emphasizes particular questions that align directly with the issues under review.

We applied a screening procedure to exclude invalid entries and unfinished submissions. Once filtering concluded, 233 fully completed responses were obtained in both English and Romanian from individuals working at specialized firms in

© 2025 The Author(s). | Published by Agro Intelligence Research Press

IT, legal, and cybersecurity sectors across Europe and North America. The geographical breakdown for the English-language version appears in **Figure 2**. Variations in language used for distribution may lead to minor differences in how answers are understood. A large share of participants originated from Romania (44.12%).

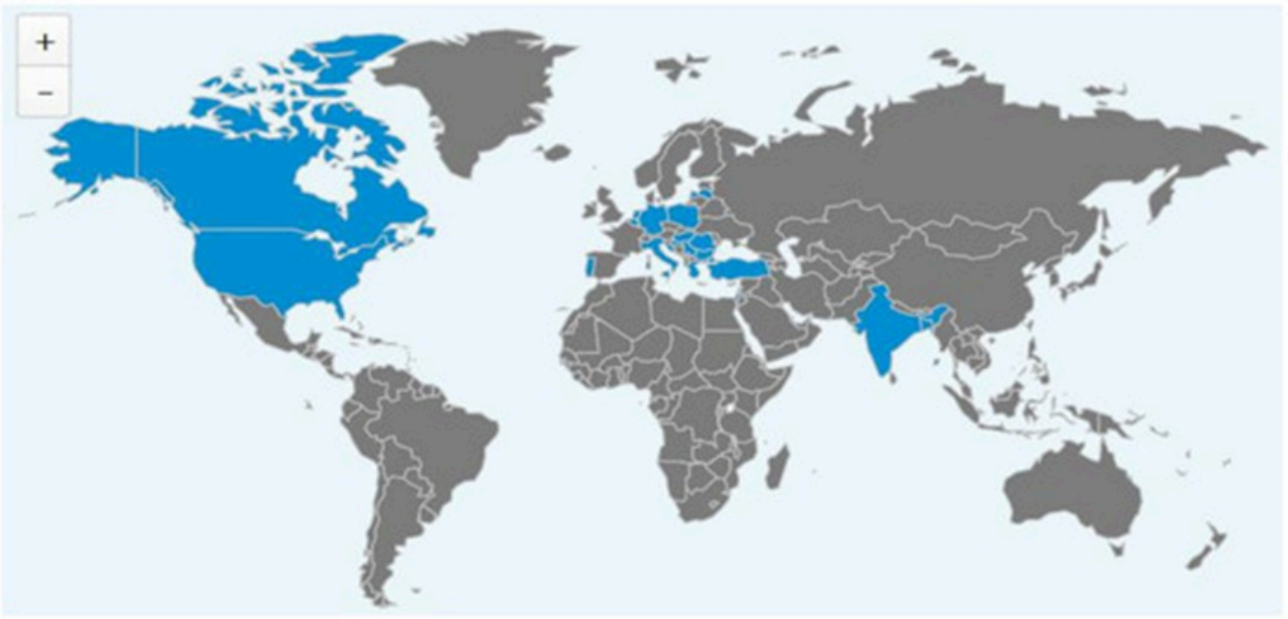

Figure 2. Distribution of respondents from a geographical perspective (blue represents the countries of the responders) (Source: QuestionPro; analytics derived from the questionnaire and provided by the authors).

This study examined two main scenarios: careless behavior by drone operators and technical failures in the drone itself. Each scenario is considered from dual viewpoints — accountability when harm occurs and protective actions that one or more involved parties can adopt.

Answers from the survey receive review through their spread, looking at how often specific replies appear and the overall pattern of those frequencies.

We further assessed key replies by using the middle value in the data sets (the median) to understand the typical position within the response ranges.

Moreover, paired questions were crafted to explore identical subjects from complementary perspectives: who should bear the costs of harm and which parties should apply safeguards against it. Therefore, the evaluation links accountability- and protection-related responses for each matching pair, aiming to reveal alignment in the assignment of responsibilities to appropriate parties.

The combined qualitative and quantitative review is supported by suggestions for updates to standardization and operational workflows. Emphasis was placed on aligning the numerical findings with ongoing proposed guidelines, specifically NIST SP 800-82 r3 Guide to Operational Technology (OT) Security and the draft EU Cyber Resilience Act (Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements).

Items addressing accountability aim to capture participants' perspectives on who should be held responsible across the relevant situations covered in the study. From a financial standpoint, this also indicates opinions on how to handle compensation for losses.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Items focused on protective actions examine participants' support for various proposed policies to prevent cyber-related events.

Results and Discussion

This section presents the survey results. The two perspectives covered here carry significant financial importance for both drone operators and manufacturers, and rely heavily on established standards and clear definitions of operational workflows. These represent common situations arising during a drone's operational lifespan. Therefore, the primary issues involving harm from careless behavior — including user conduct or omissions that unintentionally cause losses, as well as improper drone handling — and breakdowns stemming from various weaknesses or incorrect configurations in the drone's software or hardware are addressed.

User actions resulting in economic damages

The initial risk category concerns drone operators. Operators may engage in deliberate misconduct (often termed insider threats in cybersecurity) or through carelessness.

One notable drone incident in the commercial sector that caused financial harm and disrupted operations occurred in December 2018 at Gatwick, the UK's second-largest airport by passenger volume. It led to a 36 h closure to prevent two drones from colliding with planes. The disruption resulted in costs of at least GBP 15 M (USD 19.8 M) for the airport, impacting 140,000 passengers and 1,000 flights. The event was caused by a pair of drone hobbyists living close to the site, who faced arrest for compromising operational safety or endangering people by flying within 1 km of the airport perimeter. Following the occurrence, Gatwick put in place a fixed drone detection setup to maintain ongoing protection and robustness.

The two categories of conduct described produce varying determinations of accountability under standard civil liability rules and can be addressed through distinct standardization and procedural approaches. This scenario connects to H1, in which drone pilots are held accountable for events resulting from careless flying, and to H2, where regular training for drone operators can reduce such incidents of negligence-related harm.

A specific survey item asked: "Who is responsible when damage occurs due to the negligent flying of drones?" Responses appear in the key of **Figure 3**.

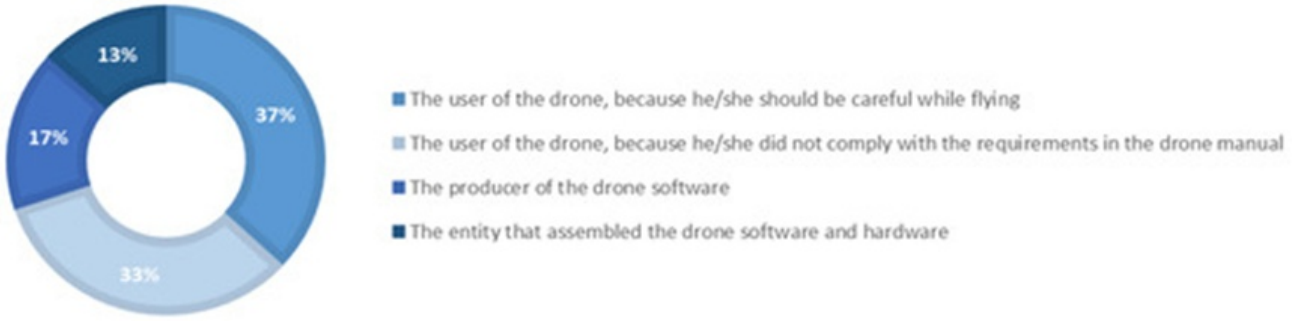

Figure 3. Question responses—responsible for damages (Source: Author's processing).

Based on the shares shown in **Figure 3**, participants identify the drone operator as at fault in these instances. Primary causes include carelessness while flying and failure to follow device guidelines. Here, it follows that the drone supplier bears no accountability for these events, having supplied all required components for correct functioning, while the operator acted irresponsibly and ignored them.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

The survey reviewed two hypotheses. First, the user's general duty of caution when operating the drone (similar to driving a vehicle). Roughly 37% of participants saw this as a core user duty, with most of those from Europe. Second, the requirement for users to adhere to the drone maker's usage conditions. This received support from 33% as vital, again mainly from European participants. Hence, most viewed carelessness as exclusively an operator mistake. Notably, 30% indicated that the drone manufacturer (or assembly entity) is liable. This suggests participants see manufacturers as capable of protecting users from their own errors by foreseeing potential improper applications (e.g., not matching intended use, specs, or guidelines) and incorporating technical features to prevent adverse outcomes in foreseeable situations.

As a result, H1 receives confirmation at 70% based on participant opinions, with nearly balanced justifications for operator accountability: attentiveness during flight and solid understanding of drone operation (including handling emergencies).

This aligns with the noted shortage of adequate protective actions by operators outlined here. Accordingly, three key elements for avoiding negligence-based accidents include: (i) drone hardware and software creators providing clear information on operational methods, (ii) establishing systems for initial and ongoing user qualification through practical drone handling in varied conditions, and (iii) informing users of emerging weaknesses and routine checks on drone condition. These elements raise total expenses for drone manufacturing (and upkeep), plus extra burdens and work for operators. For effectiveness, strong education on flight hazards is crucial, paired with suitable technical and procedural guidelines to support the elements above.

From a pure tort law standpoint, one might contend the operator bears no blame for harm to others due to the absence of deliberate intent [27]. This assessment varies according to the specific conduct or omission. In some instances, even careless acts or failures qualify as grounds for civil liability (for example, detecting malware on the control device yet proceeding with drone use). In reality, evaluation occurs individually per situation. Still, greater accountability can be achieved through more explicit standardization rules for operators and required actions throughout the drone's lifespan, covering maintenance and pre-flight preparations [28].

Additionally, this situation links closely to the one in Section 5.1. Considering the major effects a drone event might have on private or public property, or even on people, it becomes vital to integrate protective technical and procedural safeguards against potential threats, such as drone self-diagnostics (including checks of the control software running on the operator's device) before takeoff. This pairs well with expanded operator instruction.

In technical terms, additional automated features for detecting irregular behavior or verifying operator commands are sound choices. Such features are examined in existing studies through a purely technical lens, lacking broader supply chain or full-lifecycle framing [29, 30]. Naturally, multiple dimensions apply here, and considerations must encompass all aspects of drone operation, ranging from data links and collision-prevention sensors to positioning and beyond.

Entities need anti-drone tools to safeguard individuals, assets, and data from aerial risks. When operating a drone through a tablet, PC, or smartphone, ensuring a clean environment free of harmful software is critical. Two helpful protections for the control unit include live antivirus scanning and device recovery features, along with VPN services for network safeguarding. Using a VPN encrypts the operator's link and hides online activity. An additional defense against unauthorized takeover involves modifying personal habits. Predictable routes can allow attackers to anticipate drone positions for targeting. Maintaining visual contact helps operators detect issues promptly.

Technology for tracking drones supports spotting (via radar), sorting (distinguishing from other items), recognizing (specific drone type), positioning, following, and notifying about presence. Four categories exist: Radio Frequency (RF) Analyzers for capturing signals between drone and controller, sound detectors (microphones) to pick up noise and determine direction, visual tools and cameras offering sight of drones and loads while capturing proof for legal actions, and radar systems that emit signals, receive bounces, and calculate object bearing and place.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Equipment for countering drones includes:

• Systems that physically eliminate the drone, though existing rules prohibit such neutralization methods.

• Radio frequency jammers are sending strong signals to block control links.

• Powerful microwave tools create pulses that interfere with electronics.

• Intense laser systems that damage the drone's build or components.

Therefore, from a procedural standpoint, industry standards and operational workflows need greater emphasis on the duties of the listed parties [31, 32]. This should extend across the entire drone supply network.

Another survey item inquired: "In case of negligent flying, what are the relevant measures for preventing damages? (one to five scale, one meaning total disagreement and five meaning total agreement)".

Table 2 reveals the number of answers for each existing option, on a one-to-five scale. The last column shows the average score, calculated similarly to the one from the previous question. The highest average score belongs to drone automatic responses to prevent certain types of crashes/incidents. This predominant response from respondents obliges drone builders to consider enabling the device to respond as a measure to prevent unpleasant events during negligent flight.

Table 2. The number of answers for each existing option, on a one-to-five scale.

Measure	Average score	5	4	3	2	1
Automatic drone safety actions designed to prevent incidents or crashes	4.37	181	54	23	11	11
Regular refresher training is required for drone operators	4.13	157	47	44	17	14
Requirement to obtain a drone "driving license" after completing substantial training	4.03	152	50	32	22	23

Source: Author's processing.

Hence, the bulk of participants believe that technology ought to play a leading role in preventing user carelessness. This requires further investment and development from manufacturers. At the same time, it shows participants hold manufacturers accountable for accident avoidance even here. This aligns with the systems noted earlier and in Section 5.

Next, the second choice favored by participants involves ongoing operator instruction. It scored above the basic level of initial practical training. This confirms that the participant's opinions align with the suggestions in this paper regarding sustained, hands-on preparation and education for operators. It represents the best way to update users on current risks and prevention methods, such as configuring altitude limits for RTH (return-to-home) activation and installing the latest operating system updates for secure, reliable operation. Technically, various methods support risk-prioritized handling given the broad external influences and operator commands. Sensor information in this setup requires dedicated validation against standard levels.

This aligns with the discussion, emphasizing the ongoing nature of harm avoidance.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Moreover, this contradicts H2, since regular operator instruction earns a score of 4.13 as useful; yet the top approach is seen as built-in automatic reactions in the drone software to counter user carelessness (scoring 4.37). Participants thus see periodic training as beneficial but insufficient on its own and as needing integration with software-embedded automations (for instance, an RTH command proves highly effective against signal loss between the operator and the drone).

These findings further illuminate H2. Participants recognize the value of the technical and procedural steps taken by every party in drone manufacturing, distribution, and operation (including operators) to prevent careless incidents and resulting harm. This indicates acceptance of extra expenses and time investments as worthwhile for achieving safer drone activities.

H5 gains support, since operators favor automated systems over manual steps. This highlights the importance of dependable, robust automation to build customer confidence in products.

A fundamental concept in stopping cyber threats involves raising awareness and providing instruction. Accordingly, both the draft NIST SP 800-82 and the draft Cyber Resilience Act highlight the need for training and user information. While this can reduce some attack types, survey responses suggest developing additional automated safety features for drones to mitigate harm from operator carelessness during flights.

In this scenario, the recommendation is to require parties to examine and implement safety mechanisms to address user carelessness. Such details can connect to weakness handling covered in both NIST SP 800-82 and the Cyber Resilience Act across the drone's entire lifespan.

Malfunctioning of Software or Hardware

Malfunctioning involves the absence of an effective algorithm (for instance, one that has not been tested thoroughly or contains undetected bugs from the quality assurance stage) or flawed hardware component development and integration, occurring independently of any threat actor involvement [33].

A questionnaire item inquired: "Who bears responsibility in the event of a hardware malfunction?" The possible answers appear in the legend accompanying **Figure 4**.

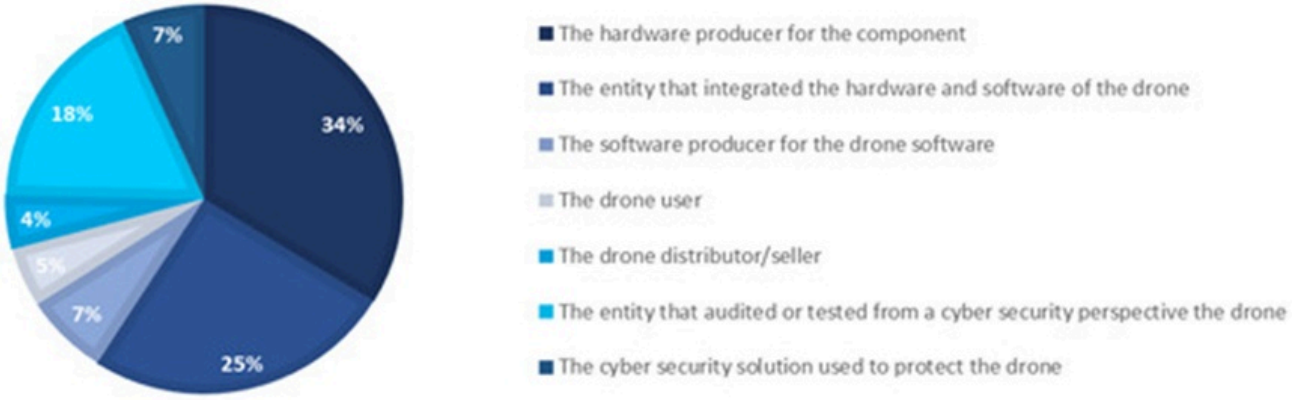

Figure 4. Question responses—malfunctioning of hardware components (Source: Author's processing).

As illustrated in **Figure 4**, 34% of participants hold the hardware producer accountable for issues with malfunctioning drone hardware components. Meanwhile, 25% point to those responsible for integrating software and hardware elements into drones. Instances attributing blame to distributors, sellers, or users remain rare.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Consequently, opinions on hardware-related problems are divided primarily between the hardware producer (34%) and the integrator (25%), with the largest share of these views coming from European respondents. This mirrors the pattern observed for software vulnerabilities, which respondents expect the producer (or integrator) to detect. Notably, the distributor/seller category received just 4%, a marked decrease compared to the software vulnerabilities query.

H3 is invalidated. Only 25% of answers named the integrator, while the hardware producer obtained the largest share at 34%. As previously indicated, this assessment is technically open to debate, as some vulnerabilities may be identified by the hardware producer. In contrast, others emerge during the integrator's evaluation of hardware-software interactions.

H4 is validated, since responses center on the hardware producer—the party that assembled the drone components and conducted pre-market audits. Interestingly, the software producer alone accounted for just 7% of responses, compared with 34% for the hardware producer and 25% for the integrator.

These outcomes align with the stipulations in the draft NIST SP 800-82 (Section 5.2.5, Layer 5—Software security) and the draft EU Cyber Resilience Act (e.g., article 10), which highlight the roles of producers, importers, and distributors. For this scenario, it is particularly relevant that stakeholders beyond producers may require a stronger role in vulnerability management than what the current drafts of the EU Cyber Resilience Act and NIST SP 800-82 propose.

An additional noteworthy question regarding vulnerability handling and prevention asked: "Who is responsible if vulnerabilities are found in the drone software from the beginning and these allow an attacker to take over the drone?" Responses are displayed in **Figure 5** below.

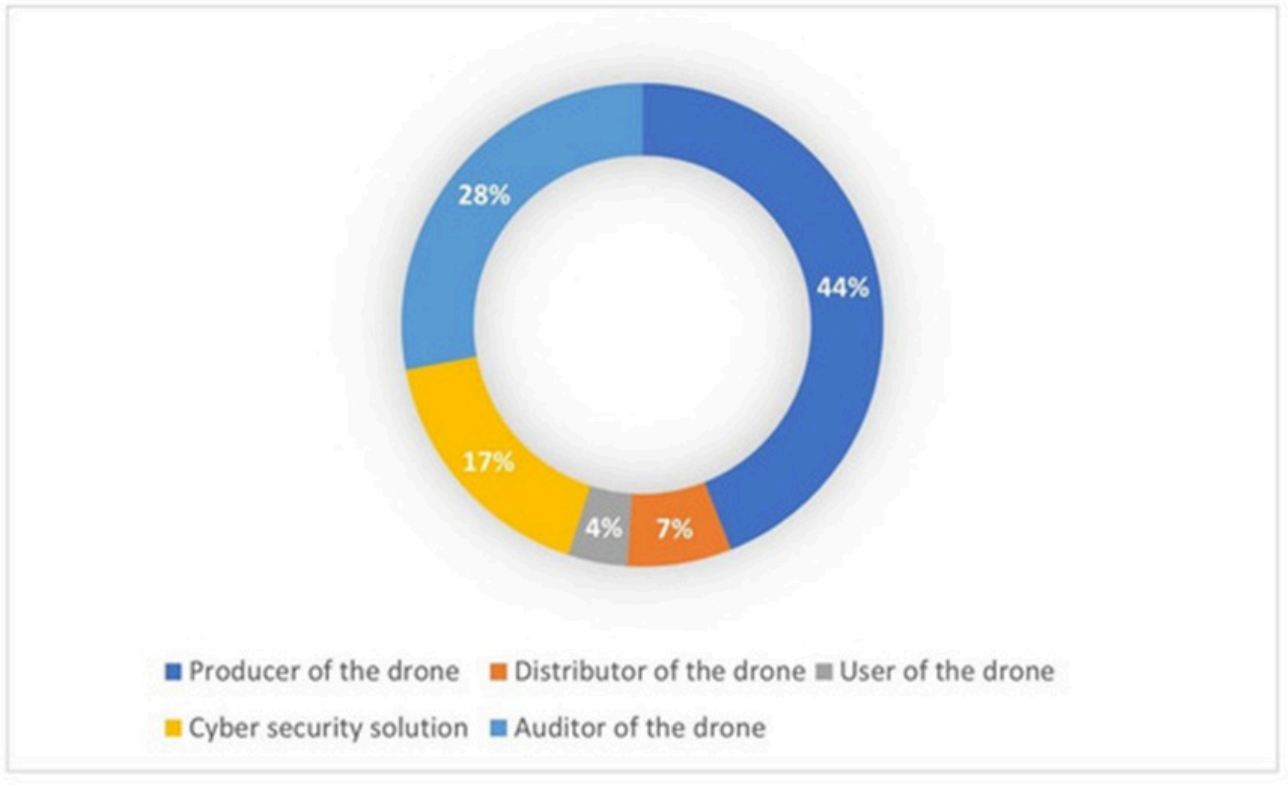

Figure 5. Question—liability in case of outset vulnerabilities (Source: Author's processing).

This item offers a deeper understanding of participants' opinions on which stakeholder is ideally positioned to implement preventive or corrective actions to address vulnerabilities. It further elaborates on how respondents perceive the drone lifecycle and the need for certain parties to engage at several stages.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

Respondents notably identify the drone software producer as the party best positioned to detect vulnerabilities early (before market distribution) and to continue doing so throughout the device's usable period, including by supplying updates across the drone's operational life.

H6 has been validated because the drone software producer is considered the most capable of identifying and resolving vulnerabilities, given its deep knowledge of the proprietary source code and its ability to run repeated tests throughout the drone's lifespan. That said, the cybersecurity solution provider and the auditor are also considered key overseers in this process, serving as neutral entities that certify the drone's safety and security. Combined, these two received 45%, with most supporters based in Europe.

One question addressed preventive strategies: "What option is the most relevant preventive measure when vulnerabilities are found in the initial software of the drone? (one to five scale, one meaning total disagreement and five meaning total agreement)," with results outlined in **Table 3**.

Table 3. Question–preventive measures for initial vulnerabilities.

Measure	Average score	5	4	3	2	1
Cybersecurity audits are conducted before drones are released to the market	4.38	165	41	31	9	7
Ongoing cybersecurity inspections are performed regularly on drones	3.57	96	45	52	26	34
Built-in failsafe systems that allow a safe landing if a drone is taken over by attackers	4.25	152	48	30	9	14
Onboard cybersecurity software designed for threat detection and prevention	4.47	177	37	25	8	6

Source: Author's processing.

This query directly connects to the prior one, as the chosen preventive actions also indicate which parties are most appropriate to carry them out.

Three alternatives scored quite similarly. This reveals two key insights: first, that multiple layers of protection are deemed necessary for effective vulnerability management; second, that various stakeholders can play meaningful roles at different phases of the drone lifecycle. For instance, market-entry auditing scored highly at 4.38, whereas ongoing periodic audits were rated lower at 3.57.

Additionally, respondents emphasized the importance of cybersecurity automation, awarding the top score to cybersecurity software and a strong rating to automatic failsafe mechanisms.

This outcome partially invalidated H7, because the automated cybersecurity solution—not periodic auditing—achieved the highest rating.

Therefore, when elaborating on vulnerability management requirements, standards like the draft NIST SP 800-82 and the draft EU Cyber Resilience Act should take this perspective into account. Experts do not consider minimal disclosure or availability of vulnerability information adequate. Accordingly, these points could be integrated into Sections 5.2.5, 6.4.3, and 6.2.4.5 of the draft NIST SP 800-82 and Article 10 of the draft Cyber Resilience Act.

Furthermore, this implies that the conformity assessment outlined in the draft Cyber Resilience Act is considered insufficient to prevent damage and cyber incidents. Greater automation from producers and other participants in the drone ecosystem is necessary to deliver real-time protection against malfunctions and the exploitation of vulnerabilities.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

This section explores the findings within the broader context of standardization, technical process frameworks, and technical considerations. It also provides further background on possible prevention strategies from both standardization and organizational technological-process perspectives.

User actions resulting in economic damages

For specific drone flight categories, users must implement appropriate security protocols. These protocols may apply to elements such as flight paths or comparable features [34].

Economic harm to people or ground-based third-party property (stemming from user negligence or deliberate actions during drone operation), encompassing privacy breaches affecting individuals on the ground or physical damage from drone crashes [35].

Damage to other drones is also possible, such as collisions in flight or with other airborne items (arising from user negligence or intent).

In these scenarios, the user typically bears liability for both the conduct and any resulting harm, given the deliberate or careless nature of the activity [36]. Cases of user negligence resulting in damage raise questions about whether the drone software included adequate safeguards (e.g., preventing acceleration toward detected obstacles) or whether the provided training and user manual offered clear guidance on command consequences and proper execution procedures.

While liability may be more straightforward under current legal frameworks, existing regulations lack specific clauses to prevent such damages [13].

Suggestions for this scenario center on prevention strategies. One involves certification training that combines hands-on flying experience with education on the legal repercussions of harmful actions, thereby fostering greater awareness. Another focuses on built-in technical safety features for particular maneuvers, such as automatic obstacle avoidance to reduce collision risks.

Implementing these measures demands time and financial investment from drone producers, distributors, users, and other certification participants. However, given the field's relative newness and the absence of uniform specifications among manufacturers or consistent requirements across nations, such preventive measures could significantly reduce user-generated damage, whether intentional or accidental.

From a standardization viewpoint, elevating the maturity of both standardization efforts and technological process frameworks in the drone domain requires tackling real-world issues already observed and prioritizing prevention to safeguard public and individual safety. This approach would enhance the relevant sections of both the draft NIST SP 800-82 and the draft EU Cyber Resilience Act.

As a result, this use case relates to user carelessness that inadvertently permits attackers to seize control of the drone. This can happen through multiple channels, most commonly via malware introduced into a connected IT system or device, which then propagates to the drone.

Malfunctioning of software or hardware

From a technical standpoint, bugs can still emerge even after software undergoes comprehensive testing in accordance with prevailing best practices. To reduce the risks of malfunctioning as much as possible, ongoing analysis must be conducted (such as vulnerability assessments and bug hunting) to detect any such issues.

These elements relate to the drone's safety, as referenced earlier in the product safety legislation. However, they can also carry consequences under civil tort law, assuming all required conditions are met (inaction resulting in a malfunction and

© 2025 The Author(s). | Published by Agro Intelligence Research Press

damage, presence of damages, and a direct link to the entity's inaction) [37].

Similar to the other use cases discussed previously, this typically places the burden of proof on users, prolongs legal proceedings, and erodes user and public confidence in drone safety. Therefore, from an economic viewpoint, boosting commercial drone adoption requires targeted preventive measures alongside more precise liability rules for parties involved in developing the drone's software/hardware and in its ongoing maintenance. Additionally, clarifications regarding entities (producers, distributors, maintenance providers) located inside or outside the EU should be provided to build confidence in the drone supply chain for distribution and operation [38].

Regarding existing legislation, a clear separation is needed between producers of drone components and entities that introduce complete drones to the market. Liability should primarily fall on the latter, with options to seek compensation from the former if necessary, either within the same legal action or through separate proceedings [39].

Since certain malfunctions may only surface years after drones enter the market (comparable to automobiles), lawmakers could introduce obligations for continuous monitoring of drone conditions.

Moreover, in some instances, drone users may be allowed to modify the existing software or install custom software directly on the drone or the ground control system. Such modifications can generate vulnerabilities, stemming from faulty software implementation that introduces backdoors or enables specific exploits, or from contaminated software that grants attackers access to the UAV. Restrictions on modification capabilities and mandatory pre-use verification of changes could serve as effective preventive security measures [40].

One approach to addressing these risks involves preventive actions, such as initial certification of drones before market release and regular follow-up verifications focused on vulnerability detection through targeted testing [2]. The interval could be set as a standard (e.g., once a year) with provisions for urgent checks when new bug or malfunction types arise. Certification and recertification testing should go beyond the existing technological checklist reviews required under current drone distribution rules. As noted in earlier sections, present regulations refer to best practices and state-of-the-art methods without specifying exact tests or key performance indicators. The certification framework appears in the draft Cyber Resilience Act under Article 10. Still, its detailed scope should be broadened to encompass the vulnerability management and automation aspects for cyber-attack prevention outlined above. Since the draft NIST SP 800-82 lacks such a certification process, it could be incorporated into the document.

Given that a significant portion of drones (particularly consumer models) depend on external devices, such as mobile phones or tablets, serving as ground control stations, this introduces a broader range of threats to aircraft operations. Vulnerabilities in these control devices can be exploited by attackers to gain partial or complete control of drones. Consequently, another method to verify normal drone operation could involve installing antivirus software on the ground control station. This would identify typical malicious activities and notify the user, potentially stopping drone launch if risks are present.

In addition, the data link layer in the UAV architecture could be subject to attacks such as GPS jamming or DoS. Implementing a protected communication channel between the aircraft and ground control system (for example, via TLS) or relying on inertial navigation systems that operate without external signals could help counter these threats [41].

For particularly critical and hazardous bugs or errors that could cause substantial economic losses, producers could issue public notices urging customers to return affected drone models [42]. Additionally, over-the-air mechanisms to immobilize the drone until the newest update packages are applied could prove valuable in averting major incidents.

As with automobiles, effectiveness depends on consumer/user responsiveness, and it may fall short if information fails to reach them. For this reason, direct and prompt communication channels should be established between drone

© 2025 The Author(s). | Published by Agro Intelligence Research Press

hardware/software producers and users (with or without authorities' involvement). Insurance options for such malfunctions could also be explored as a partial risk transfer mechanism [43].

These suggestions aim to incorporate the questionnaire findings and can be adapted to existing supply chain structures and industry standards, depending on target markets. From a technological perspective, stakeholders can develop a risk-based strategy tailored to their specific roles in the drone lifecycle. Technically, this could draw on approaches such as threat modeling or assessing attack likelihood through red teaming exercises, as described in Refs. [44] and [45]. Illustrations of such risk-based evaluations appear in Ref. [46]. However, these examples require further customization based on the stakeholder's specific technical environment.

Risk management elements feature in the draft NIST SP 800-82, along with supply chain review (Sections 4.2.1, 6.1.3, 6.1.4, and 6.1.5). Yet these primarily adopt a purchaser-focused lens rather than addressing all stakeholders in the drone ecosystem. The value of the proposed measures lies in enabling continuous or periodic risk assessment and management by all relevant participants in the drone ecosystem.

Under Article 10(5) of the draft EU Cyber Resilience Act, producers must conduct and refresh risk assessments for their products, including those arising from third-party components integrated into drone software. Even so, an additional requirement for implementing mitigation steps to address identified risks and reduce their probability or severity should be added [47]. Furthermore, in some situations, the producer may not be the optimal party for conducting the risk assessment [48]. Therefore, additional duties should apply to other stakeholders involved in adapting or altering the drone.

The two measures described could result in additional expenses for drone hardware or software producers, ultimately affecting drone users. Implementation must be customized to keep costs low while delivering strong security to users promptly. In evaluating this, the damages prevented by these measures should be weighed against the time and expenses of litigation. This leads to a cost-benefit evaluation of preventive actions, consistent with other European legislative trends, such as those for medical devices (Regulation (EU) 2017/745) and essential services (NIS Directive and draft NIS Directive 2.0) [49, 50].

Summary of proposals

Clear rules on liability for negligence are necessary, taking into account both objective and subjective factors. These include the actions or inactions expected of the drone user, the specific flight context, the drone's characteristics, and the training the user has completed. Such clarity could be achieved in various ways, for instance, through industry-wide standardization or collaborative efforts among drone stakeholders. The purpose of this paper is to determine which stakeholders are best positioned to put in place or oversee prevention mechanisms for cases of negligence and malfunction.

Prevention mechanisms that standardization, technological process frameworks, or producers might mandate include automatic failsafe systems and regular training sessions. Failsafe systems mean that in specific scenarios (such as a rapid loss of altitude or unsuitable user commands for the flight zone or user profile), the drone switches to an autonomous mode and performs a safe landing. Periodic training keeps drone users informed about current safe flying practices. These elements could be incorporated into the draft NIST SP 800-82 and the draft EU Cyber Resilience Act, as they have not been addressed to date.

To avoid drone malfunctions, pre-market evaluations combined with regular follow-up evaluations could be beneficial. Additionally, sensors and key performance indicators could help inform drone users about emerging problems or trigger built-in automatic prevention features in the drone software. This corresponds to the organizational processes across the drone lifecycle, which have technical consequences for drone evaluation and for the development or modification of drone software and hardware. Such elements could be defined at the industry level among market participants through

© 2025 The Author(s). | Published by Agro Intelligence Research Press

standardization to ensure product safety upon market introduction. In relation to the draft NIST SP 800-82 and draft EU Cyber Resilience Act, these elements could strengthen the draft provisions.

The responsibility of each component producer needs to be established individually for both initial and ongoing assessments to track potential malfunction risks and to integrate automatic prevention features where feasible.

Therefore, regarding negligence and from a prevention perspective, respondents considered automatic systems the most effective option, rather than relying on pilot training as the main safeguard. This places greater demands on the parties developing the drone's software and hardware, including those providing maintenance services.

Moreover, stakeholders positioned earlier in the drone lifecycle are considered best suited to ensure appropriate organizational and technical safeguards. This could be captured in relevant standards and frameworks, including codes of conduct.

Additionally, automatic preventive actions are favored over manual approaches or regular reviews and audits. This heightens demand for automation and rapid updates among stakeholders in the drone lifecycle and could be challenging to implement in practice without suitable standardization and frameworks. In relation to the draft NIST SP 800-82 and draft EU Cyber Resilience Act, these elements could enhance the draft provisions, particularly concerning proactive steps and the involvement of various stakeholders across the drone ecosystem, beyond just the producer.

Limitations and future directions of the research

As explained earlier, this research paper examines the perspectives of professionals who regularly work with drones across different settings and from various viewpoints (IT, legal, and others) on current standardization to prevent damage and other adverse outcomes linked to user negligence and malfunction.

With respect to legislative rules, EU-level drone legislation has primarily addressed flight restrictions (permitted zones and altitudes) and required training for drone operators. Issues such as liability and preventive organizational or technical measures are largely managed at the national level, using general civil law principles. Furthermore, industry-level standards or frameworks on these matters remain scarce.

For these reasons, incorporating the opinions of relevant experts on how standardization and frameworks should tackle these issues is crucial for future work in the area. This provides the article's novel contribution by compiling current gaps in standardization and suggesting remediation and prevention strategies.

Accordingly, this research paper does not seek to recommend legislative modifications and is not aimed at markets beyond the EU. Moreover, the objective is not to define liability for specific scenarios, but instead to capture respondents' views on which stakeholder in the drone ecosystem is best equipped to handle preventive measures for the discussed use cases involving user negligence and malfunctioning.

In upcoming articles on drones, the intention is to expand on the topics covered here and, as far as possible, to compare variations in legislation and drone operations across global regions relative to European rules. Such research could support harmonizing implementation rules and measures. It could ultimately form a collection of proposals for review, assessment, and adoption by specialized bodies within the International Telecommunication Union and other qualified international organizations.

Conclusion

This research paper has concentrated on two primary sources of damage that occur without deliberate intent and has outlined how liability for such incidents might be understood within the drone ecosystem, while also highlighting available

© 2025 The Author(s). | Published by Agro Intelligence Research Press

prevention mechanisms. The goal concerning liability is to review how customers perceive the responsibilities of different stakeholders across the drone lifecycle. This perspective supports the subsequent phase of the research, which involves aligning liability insights with the identification of entities responsible for preventive actions against malfunctioning and user negligence. The preventive measures examined here operate at technical and organizational levels, potentially involving specific processes at the industry or standardization level, followed by targeted technical implementations.

As technology continues to evolve, so does the approach to shaping and evaluating liability, taking into account all stakeholders involved throughout the product or service lifecycle. In the drone context, the questionnaire yielded notable insights from respondents about liability and which stakeholders are best suited to prevent certain unintentional damages.

Regarding user negligence leading to adverse outcomes, 70% of respondents identified the user as the accountable party (validating H1), while 30% pointed to the drone's producer (or integrator). This aligns with respondents' emphasis on preventive measures (the highest score of 4.37), invalidating H2, which focused on periodic training, indicating that certain security capabilities should be built into the drone from the outset (e.g., automatic responses to prevent crashes or incidents). These help mitigate cases where users behave negligently, such as disregarding operating instructions or failing to meet their duty of care.

In the area of hardware security, H3 was invalidated because respondents primarily assigned responsibility to the hardware producer (34%) rather than the integrator (25%). In addition, H4 was validated, as stakeholders positioned early in the drone lifecycle were held accountable for establishing appropriate preventive measures against malfunctions and user actions, ranging from component producers to the entity that audits the drone before market release. This also underscores the value of independent parties in checking the security and safety aspects of products. From a technical and organizational standpoint, this highlights the necessity of standardized verification processes carried out by neutral third parties, which may involve black-box, grey-box, or even white-box analysis. A grey or white box approach can, from a technical viewpoint, deliver a more thorough evaluation and outcomes that accurately reflect the drone's condition at that stage.

Furthermore, it indicates that customers primarily focus on the production phase and pay less attention to maintenance requirements throughout the drone's lifecycle. This could represent an area worth investigating further to understand customer reasoning. Their answers might stem from the importance of properly regulating market entry, while maintenance is seen as routine. Alternatively, it could reflect an assumption that new vulnerabilities or prevention needs do not arise during the drone's operational life, despite this being quite likely given technological developments and patterns of vulnerability discovery. From a technical perspective, this process is vital throughout the drone lifecycle, not just at the initial market launch stage. Therefore, from a technical and organizational perspective, it is highly questionable to emphasize the moment of market entry over the drone's full lifecycle.

Concerning H5, respondents regarded automation as critical for damage prevention, with the user's role less central and a ready-made solution preferred for preventive measures that require no particular setup or user input. This means producers of drone software and hardware are expected to collaborate to anticipate negligent user behavior and incorporate technical mitigation features accordingly. Additionally, the industry is expected to, through collaboration and standardization, establish technical and organizational methods to prevent malfunctions in a constantly evolving vulnerability landscape.

The research article has reviewed elements related to technological processes and the necessity of standardizing technical and organizational issues within its scope, from a prevention standpoint. It has also suggested targeted modifications to draft standards in the domain to better address prevention mechanisms in a forward-looking, ongoing way, engaging all pertinent stakeholders rather than limiting the focus to the producer.

Future studies building on this article's scope could delve deeper into the suggestions presented and develop a comprehensive set of recommendations within organizational and technical process frameworks, including a taxonomy

© 2025 The Author(s). | Published by Agro Intelligence Research Press

for these frameworks.

The research in this article is restricted to civil drones and excludes military or institutional ones. It bases its analysis on the existing civil legislation at the European Union level and on civil law principles in relevant countries.

Acknowledgements

None

Conflict of interest

None

Financial support

This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III. This paper was co-financed by the Bucharest University of Economic Studies during the PhD program.

Ethics statement

None

Received: 25 Nov 2023 Revised: 30 Jan 2024 Accepted: 15 Feb 2024
Published online: 25 May 2025

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at https://creativecommons.org/licenses/by-nc-sa/4.0/.

References

1. European Aviation Safety Agency. Concept of Operations for Drones—A Risk Based Approach to Regulation of Unmanned Aircraft; European Aviation Safety Agency: Cologne, Germany, 2015.

2. Yaacoub J-P, Noura H, Chehab A. Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things. 2020;11:100218.

3. Comandé G. Product liability in Italy. In: European product liability: an analysis of the state of the art in the era of new technologies; Machnikowski P, editor. Cambridge, UK: Intersentia; 2016.

4. Accompanying the document communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, artificial intelligence for Europe,

{COM(2018) 237 final}. 2018. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137 (accessed on 10 January 2023).

5. Konert A, Kotliński M. U-space–civil liability for damages caused by unmanned aircraft. Transp Res Procedia. 2020;51:304–12.

6. Kardasz P, Doskocz J, Hejduk M, Wiejkut P, Zarzycki H. Drones and possibilities of their using. J Civ Environ Eng. 2016;6:1–7. https://doi.org/10.4172/2165-784X.1000233.

7. Zain M, Hussin AK, Ganraj D. An ultralight helicopter for rice farmers. Universiti Teknologi MARA: Masai, Malaysia; 2001.

8. Konert FAA, Balcerzak BT. Legal and ethical aspects of rules for the operation of autonomous unmanned aircraft with artificial intelligence. In: Proceedings of the 2021 International Conference on Unmanned Aircraft Systems (ICUAS), Athènes, Greece, 19 July 2021; p. 602–9. https://doi.org/10.1109/ICUAS51884.2021.9476822.

9. Sehrawat, V. Liability Issue of Domestic Drones. Santa Clara High Technol. Law J. 2018, 35, 110. https://digitalcommons.law.scu.edu/chtlj/vol35/iss1/3 (accessed on 10 January 2023).

10. Okuboyejo S. Drone law 2.0: the evolving legal typology for commercial drones in European private law. SSRN; University of Amsterdam: Amsterdam, The Netherlands; 2022. https://doi.org/10.2139/ssrn.4048640.

11. Skytango.com. https://skytango.com/15-drone-fines-from-around-the-world/ (accessed on 10 January 2023).

12. Bassi, E. European Drones Regulation: Today's Legal Challenges. In Proceedings of the 2019 International Conference on Unmanned Aircraft Systems (ICUAS), Atlanta, GA, USA; 2019.p. 443–50.

13. De Schrijver S. Commercial use of drones: commercial drones facing legal turbulence: towards a new legal framework in the EU. US-China Law Rev. 2019;16:338.

14. Altawy R, Youssef AM. Security, privacy, and safety aspects of civilian drones: a survey. ACM Trans Cyber-Phys Syst. 2017;1:1–25. https://doi.org/10.1145/3001836.

15. Bassi E. From here to 2023: civil drones operations and the setting of new legal rules for the European single sky. J Intell Robot Syst. 2020;100:493–503. https://doi.org/10.1007/s10846-020-01185-1.

16. Molina M, Campos VS. Ethics and civil drones: European policies and proposals for the industry. Springer: Berlin/Heidelberg, Germany; 2018. https://doi.org/10.1007/978-3-319-71087-7.

17. TNO. Final Report: Technical Aspects Concerning the Safe and Secure Use of Drones. 2016. https://www.thehaguesecuritydelta.com/uavs-drones (accessed on 10 January 2023).

18. McNeely J, Hatfield M, Hasan A, Jahan N. Detection of UAV hijacking and malfunctions via variations in flight data statistics. In: Proceedings of the 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, USA; 2016; p. 1–8.

19. Dalamagkidis K, Valavanis K, Piegl LA. Evaluating the risk of unmanned aircraft ground impacts. 16th Mediterranean Conference on Control and Automation, Congress Centre, Ajaccio, France. 2008. https://mediatum.ub.tum.de/doc/1289295/347096.pdf (accessed on 10 January 2023).

20. Choudhary G, Sharma V, Gupta T, Kim J, You U. Internet of drones (IoD): threats, vulnerability, and security perspectives. In: Proceedings of the 3rd International Symposium on Mobile Internet Security (MobiSec'18), Cebu, Philippines; 2018.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

21. Yahuza M, Idris MYI, Ahmedy IB, Wahab AWA, Nandy T, Noor NM, et al. Internet of drones security and privacy issues: taxonomy and open challenges. IEEE Access. 2021;9:57243–70.

22. Australian Government Civil Aviation Safety Authority—CASR. Part 101 Micro and Excluded Remotely Piloted Aircraft Operations Guide. 2020. https://www.casa.gov.au/sites/default/files/2021-08/part-101-micro-excluded-rpa-operations-plain-english-guide.pdf (accessed on 10 January 2023).

23. Dedrone. Airspace Security Insight Report 2022. 2022. https://www.dedrone.com/white-papers/airspace-security-insights-report-2022 (accessed on 10 January 2023).

24. Department of Defense Responsible AI Working Council Has Published the US Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway Paper. 2022. https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF (accessed on 10 January 2023).

25. Șcheau MC, Găbudeanu L, Brici I, Vîlcea AL. Preventive cybersecurity steps to enhance drone usage. In: Proceedings of the 23rd RSEP International Economics, Finance and Business Conference, Virtual/Online; 2021; ISBN 978-605-70583-5-5.

26. Șcheau MC, Achim MV, Găbudeanu L, Brici I, Vîlcea AL. Legal, economic and cyber security framework considerations for drone usage. Appl Sci. 2022;12:4663.

27. Vacek JJ. The next frontier in drone law: liability for cybersecurity negligence and data breaches for UAS operators. Campbell L Rev. 2017;39:135.

28. de Sio FS, Di Nucci E. Drones and responsibility, mapping the field. Routledge: London, UK; 2016.

29. Raja G, Anbalagan S, Narayanan VS, Jayaram S, Ganapathisubramaniyan A. Inter-UAV collision avoidance using deep-Q-learning in flocking environment. In: Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2019; IEEE: Piscatvie, NJ, USA; 2019. p. 1089–95.

30. Raja G. Authorized arming and safeguarded landing mechanism for drones. In Proceedings of the 2020 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan; 2020.

31. Akram RN, Markantonakis K, Mayes K, Habachi O, Sauveron D, Steyven A, et al. Security, privacy and safety evaluation of dynamic and static fleets of drones. In: Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA; 2017; p. 1–12.

32. Salamh FE, Karabiyik U, Rogers M. A constructive DIREST security threat modeling for drone as a service. J Digit Forensics Secur Law. 2021;16.

33. Choi CH. A study on IoT (Internet of Things)-based disaster detection and prevention system. Adv Sci Lett. 2016;22:3446–8.

34. Commission Implementing Regulation (EU) 2019/947 of June 2019. https://www.easa.europa.eu/document-library/regulations/commission-implementing-regulation-eu-2019947 (accessed on 10 January 2023).

35. Bertolini A, Episcopo F. The expert group's report on liability for artificial intelligence and other emerging digital technologies: a critical assessment. Eur J Risk Regul. 2021;12:644–59.

36. Ntovas A, Tsimplis M, Veal R, Quinn S. Liability for operations in unmanned maritime vehicles with differing levels of autonomy. Institute of Maritime Law: Southampton, UK; 2016. p. 212.

37. European Parliament. Artificial intelligence and civil law: liability rules for drones. The European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: Strasbourg, France; 2018.

© 2025 The Author(s). | Published by Agro Intelligence Research Press

38. Harris KK. Drones: proposed standards of liability. Santa Clara High Tech LJ. 2018;35:65.

39. Pustahelji R. Reflections on civil liability for damages caused by unmanned aircrafts. Zb Rad Pravnog Fak. 2019;53:311–26.

40. Huttunen M. Civil unmanned aircraft systems and security: the European approach. J Transp Secur. 2019;12:83–101.

41. Bryson M, Sukkarieh S. UAV localization using inertial sensors and satellite positioning systems. In: Handbook of unmanned aerial vehicles; Valavanis K, Vachtsevanos G, editors. Springer: Dordrecht, The Netherlands; 2015.

42. Alwateer M, Loke SW. Emerging drone services: challenges and societal issues. IEEE Technol Soc Mag. 2020;39:47–51.

43. European Union. Study on third-party liability and insurance requirements of remotely piloted aircraft systems. European Union: Maastricht, The Netherlands; 2014.

44. Odarchenko R, Usik P, Volkov O, Simakhin V, Gospodarchuk O, Burmak Y. 5G networks cyberincidents monitoring system for drone communications. In: Proceedings of the 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), Kyiv ; 2019; p. 165–9.

45. Salamh FE, Karabiyik U, Rogers MK, Matson ET. Unmanned aerial vehicle kill chain: purple teaming tactics. In: Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA; 2021; p. 1081–7.

46. Fiondella L. The Application of Unmanned Aerial Systems in Surface Transportation—Volume II-F: Drone Cyber Security: Assurance Methods and Standards; Report No. 19-010; University of Massachusetts Dartmouth: North Dartmouth, MA, USA; Massachusetts Department of Transportation Office of Transportation Planning: Boston, MA, USA, 2019.

47. Heliguy Installs Drone Defense at Gatwick Airport. https://www.heliguy.com/blogs/posts/heliguy-installs-drone-defence-at-gatwick-airport (accessed on 10 January 2023).

48. Interpol. Drone Incident Framework. 2021. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-carries-out-full-scale-drone-countermeasure-exercise (accessed on 10 January 2023).

49. Official Journal of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. European Commission: Brussels, Belgium; 2016.

50. European Parliament. The NIS2 Directive—A high common level of cybersecurity in the EU. Briefing, 2022. Airport Security Economic Impacts of Drone Incidents to Airports. https://www.911security.com/blog/airport-security-economic-impacts-of-drone-incidents-to-airports (accessed on 10 January 2023).

© 2025 The Author(s). | Published by Agro Intelligence Research Press