A Review of the Legal, Regulatory and Practical Aspects Needed to Unlock Autonomous Beyond Visual Line of Sight Unmanned Aircraft Systems Operations

Hartmann, Jacques; White, Samuel; Matalonga, Santiago; Riordan, James

DOI:
10.1007/s10846-022-01682-5

Publication date:
2022

Journal of Intelligent & Robotic Systems (2022) 106:10
https://doi.org/10.1007/s10846-022-01682-5

SURVEY PAPER

A Review of the Legal, Regulatory and Practical Aspects Needed to Unlock Autonomous Beyond Visual Line of Sight Unmanned Aircraft Systems Operations

Santiago Matalonga[1] · Samuel White[2] · Jacques Hartmann[2] · James Riordan[1]

Received: 12 March 2022 / Accepted: 28 June 2022

Abstract
Services that exploit Unmanned Aircraft Systems (UAS) are poised to revolutionise the service industry with a projected value of 71 BUSD by the end of the decade. A key enabler of this technology is the unlocking of autonomous Beyond Visual Line of Sight (BVLOS) operations. BVLOS operations will depend on a robust Detect and Avoid (D&A) capability. Yet, currently in the UK and EU, BVLOS operations are only allowed in specific cases and scenarios. As a result, the technological landscape for the development of robust D&A faces limitations, and there is little market incentive for development. Furthermore, while automated BVLOS is a future technology, a strong D&A capability is of importance now for all types of UAS operations. As the remote pilot has to deal with information overload from the controller device and the environment. These high-risk UAS operations are becoming more common. In this paper, we discuss the current legal framework in the UK making comparisons to EU countries. We make the case that even when an operation abides by the current framework the remote pilot is exposed to several legal liabilities. We review the roadmaps for UAS adoption (including certification processes for UAS-based products) and highlight that for software-intensive systems, key steps are missing to assure the quality of the product. Finally, we build on these findings to set forwards a path to complement future certification processes to enable autonomous based UAS operations to share the airspace with remotely piloted operations.

Keywords UAS · Detect and Avoid · Laws and Regulations · Standards

1 Introduction

Services that exploit (UAS) are poised to revolutionise several aspects of our lives. From last-mile deliveries to the survey of critical infrastructure (like power lines, wind farms, and bridges). The value of the UAS services industry is expected to grow three-fold in the next decade to 71 Billion USD [1]. The societal benefits arising from unlocking the UAS service industry include a reduction of the carbon footprint, improving supply-chain efficiency by leveraging last-mile delivery [2] and have been identified as key enablers of UN sustainable development goals [3, 4].

UAS missions can be classified according to the distance between the remote pilot and the UAS (see Fig. 1). Visual Line of Sight (VLOS), Extended Visual Line of Sight (EVLOS) and Beyond Visual Line of Sight (BVLOS) operations require a direct connection between the UAS and the remote pilot. The remote pilot is responsible for the safety of the operations. Current commercial of the shelf UAS, and manufacturers are incorporating D&A capabilities to assist the remote pilot when flying the UAS and detecting potential hazards. Yet, even the most advanced UAS does not have full D&A capabilities [5]. In the UK, remote pilots performing commercial operations must undertake training. The regulatory framework in the UK is tethered to manned aviation concepts, assuming a pilot is present (either in the cockpit or on the ground – hence the term remote pilot). Currently,

✉ Santiago Matalonga
santiago.matalonga@uws.ac.uk

Samuel White
s.f.s.white@dundee.ac.uk

Jacques Hartmann
j.hartmann@dundee.ac.uk

James Riordan
james.riordan@uws.ac.uk

[1] ALMADA Research Centre, School of Computing, Engineering and Physical Science, University of the West of Scotland, Glasgow, UK

[2] School of Social Sciences, University of Dundee, Dundee, UK

Published online: 22 August 2022

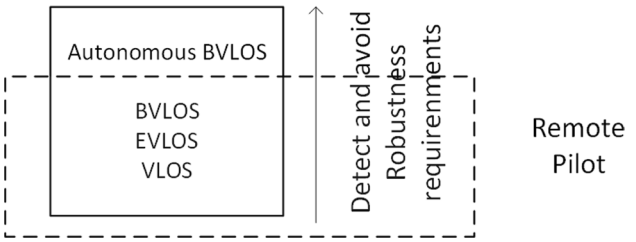

Fig. 1 Concept of Detect and avoid requirements for UAS operations

the law does not recognise the capability of sensors, and supporting systems, to perform hazard detection.

BVLOS operations are not allowed in the UK and EU, except under specific clearance from national aviation authorities and within clear, geofenced areas, see e.g. [6]. The landscape for legal and regulation for UAS operations is complex and dependent on international, regional, and national law. While UAS operations have been standardised in the UK and EU, liability is dealt with at the national level according to individual states' legal systems. Autonomous BVLOS operations will not require a remote pilot to operate the UAS and will rely on Artificial Intelligence to complete their missions.

To unlock the potential of autonomous UAS operations, robust D&A is important to enable autonomy. Robust D&A can enable the UAS to foresee and avoid potentially hazardous situations. In the UK and Europe, as we will show in this paper, human remote pilots of UAS operate under the umbrella of the European Union Aviation Safety Agency (EASA) regulation. These remote pilots must demonstrate their professional capabilities being demonstrated through professional certifications. In the UK, this professional certification is called the General Visual Line of Sight Certificate [7], other EU countries name it differently, but the requirement for UAS pilots to being certified when operating in the specific category is defined in EU Regulation 2019/947 [8]. Good practice dictates that these pilots operate under a "just culture" [9], meaning that as long as best practice and risk avoidance are followed, then the operation is conducted under the guidance of the regulations. Furthermore, even when abiding by operational regulations, remote pilots are potentially liable under civil or criminal law.

When looking at autonomous BVLOS operations, there is no set of regulations or requirements for determining the capabilities or shared understanding of the targets and capacities needed for robust D&A [10]. Current regulation foresees the upcoming myriad of operations that can benefit from autonomous UAS operations, but the development of robust D&A technology will need clear requirements are target that have not yet been defined. Current Commercial of the Shelf Solutions (COTS) – sometimes marketed as autonomous – are assistive (L2), not autonomous (L3 and beyond) [11], (see Sect. 6).

In this paper, we draw from the first results of the RAPID project, an EU funded project that aims to save lives by automating the maintenance/inspection survey of critical infrastructure (see Sect. 2). Our team is composed of interdisciplinary researchers in computing, standards and regulation auditors, policy and law. The main goal of this paper is to draw attention to the current state of the law in the UK (and comparing with some EU regions), to show how the current legal framework curtails innovation. We also highlight that the roadmaps for the adoption of UAS operation are missing steps. Finally, we draw from our results in DAA UAS research to convey our vision of the needed quality assurance for software-intensive systems that support UAS operations and show how future certification frameworks can be developed so that autonomous UAS can safely share the airspace with piloted UAS.

This paper presents a review of the legal landscape (Sect. 2) that supports the UAS operations in the UK, which despite Brexit is still shaped by EU law, drawing a comparison with EU countries that although subject to the same overarching basic regulation on design ('Delegated Regulation' (2019/945) and rules and procedures for the use of UAS ('Implementing Regulation' (2019/947) (Sect. 4) have different legal rules on civil and criminal liability. Current rules for product certification are not defined for software-intensive systems (Sect. 5). Therefore, we present the technical challenges for devising a certification framework that can be used to show that an autonomous UAS can be "as safe as" a remote piloted UAS (Sect. 6). Others have identified this lack of a standardised framework as a deterrent for the development of autonomous UAS operations (for instance see [12]). We outline how such a framework would behave in the current legal landscape and demonstrate the consequences with indicative requirements (Sect. 7).

Solving the technological problem of how to design and deliver robust D&A capability is critical for autonomous UAS operations, but it is also important for remotely piloted operations. Robust D&A capability will minimize risk in cluttered environments where global positioning satellite signals can be lost (like in and around critical infrastructure) – with or without the presence of a remote pilot, in VLOS and BVLOS operations. However, to fully exploit this technology, the legal framework must facilitate a path for this technology to go from the lab to the real world.

2 The RAPID Project as an Example Use Case for Autonomous BVLOS Operations

The RAPID project is a Horizon Europe funded project [13]. The consortium members are based in several European countries (Belgium, France, Germany, Ireland, Norway

and UK). Our interdisciplinary team is comprised of experts and researchers in artificial intelligence, software engineering, computer science and law, who have worked in several industries including safety–critical embedded software, maritime and aviation.

RAPID's main use case is to demonstrate the capacity for a swarm of autonomous UAS to survey critical infrastructure (a bridge in a busy inland port). Currently, bridge inspection is a costly, human-intensive, and hazardous endeavour. Existing practice requires the surveyors to close the bridge to traffic, deploy cranes and put human engineers in hazardous situations (e.g. hanging off the side of the bridge). Autonomous UAS can reduce risk to human engineers when surveying the bridge, but incorporating autonomous UAS in a cluttered urban environment must be done with a view towards safety. The autonomous survey UAS must become aware of hazards that might be unforeseen during mission planning. In particular, small uncooperative flying objects (like birds, other UAS, low-flying manned aircraft, and service helicopters). If autonomous UASs are to de-risk human operations, then it is of the utmost importance that they do not introduce additional risks.

To achieve the successful demonstration of the aforementioned use case, several technologies must be developed and integrated – among them – the development and deployment of robust D&A software systems that can detect small uncooperative flying objects that can threaten the safety of the use case [14].

3 The Legal Landscape Underpinning UAS Operations

This section summarises the legal aspects that a remote pilot must be aware of when performing UAS operations.

EASA is the legal regulator for civil aviation in Europe. European rules for UAV operations are partly harmonized, but legal liability for accidental harm to people vary greatly and are fragmented under national law. Although the UK has left the EU, the rules in place still largely mirror those prior to Brexit and thus EU standards remains important to understanding how the UK regulates the use of UAV. It remains to be seen how the relationship between the UK and the EU will develop in the future.

Since 2009 EASA has issued a set of regulations that address UAS operating requirements (EASA, 2009; EASA, 2010; EASA, 2015; EASA, 2017; EASA, 2019/945 and 947), see [5]. Under this framework, an unmanned aircraft is defined as an "aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board" [8]. While the concepts for operation, production and maintenance of unmanned aircraft are defined at the domestic level (see [15]), there are no common rules on several legal issues, among them civil liability and criminal law, which are not within the competence of the EU or EASA. Currently, there are no drone specific privacy or data protection legislative instruments at national or European levels. At the European level, the right to respect for private life is regulated mainly by the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union and the right to data protection is regulated by the General Data Protection Regulation.

Most UAS operators would assume that by abiding by regulation they are conduction their missions under solid legal foundations, however, the laws around UAS operation have not evolved to tackle the complexities of current technologies. In this paper, with the intent of simplifying the intricacies of the different countries, we base the discussion in terms of the UK legal system, and we compare it with other European legal systems within the RAPID project (see Sect. 2).

3.1 Civil Liability of UAS Operations

The use of UAS raises a range of issues where the rules of civil liability may come into play. In many civil law countries, such issues are mainly dealt with in property or in some cases criminal law. Whereas in common law countries, such as the UK, it is mainly dealt with under the law of tort, which also has close links with issues of privacy.

Tort law protects varies types of rights by providing a remedy for the harm caused to those rights [16]. As such, tort law "can be employed to protect whatever interests are deemed worthy of protection in any particular society" [17]. The development of protected rights is closely connected to developments in human rights law [17]. Much of the discussion of tort law in this paper is based on English law, Ireland is the only other common law country which is part of the RAPID consortium but its tort law has developed with a high degree of similarity to English law, see e.g. [18] and [19], and the law of both nations has been influencd also by membership of both the EU and ECHR.

Rights protected by tort law include the right to physical integrity or personality rights, such as reputation and privacy [20]. Thus personal injury or loss of human life that results from a falling aircraft or UAS may lead to claims for damages. In the UK in such a situation, the UAS' owner will bear legal responsibility as a matter of strict liability (ie regardless of fault) because of the Civil Aviation Act 1982.

Similarly, invasion of privacy or loss of reputation may lead also to a claim for damages, some of which are dealt with under tort law others under law that regulates the right to privacy. In addition, tort law also includes other acts, such as trespass, which refers to the unjustifiable interference with the possession of land [20]. Unlike the other forms of tort,

trespass is actionable in the courts whether or not the claimant has suffered any damage.

A classic example of trespass is walking on another person's land without their permission. But trespass can also be committed by entering another person's airspace. A leading case concerned the erection of an advertising sign which extended a mere eight inches over the neighbour's land. This was trespass [21]. Even the arm of a crane swinging over someone's property can be a trespass [22]. But the law is uncertain in relation to UAS. Thus, in another leading case, it was held not to be trespass if an aircraft flies above the level of the ordinary use of land, in this case, more than 30 m above the property [23]. The decision was influenced by the Civil Aviation Act 1982, s76(1) of which specifically states that a trespass is not committed if an aircraft flies above property at a "reasonable height" having regard to the prevailing conditions. This raises questions as to how far up in the airspace above someone's property trespass can occur and how the current law applies to UAS? But if anything falls onto the land it is a trespass even if the aircraft was flying at a reasonable height [16, 24].

In addition to the above, applying traditional tort rules to autonomous UAS is fraught with difficulties, especially applying notions of foreseeable harm [25]. Autonomous systems, per definition, perform tasks without direct human control or supervision. Self-learning capabilities, as explained below, moreover mean that they are capable of using new data to alter initial programming. The choice of such data, and the degree of impact it has on the outcome, is constantly adjusted by the evolving algorithms themselves, making it impossible for the programmer or operator to foresee all harm. This raises the very real question of what a programmer or operator of autonomous UAS needs to do to show reasonable care? In essence, the current legal framework is anthropocentric. Humans are the primary subject and object of norms that are created, interpreted, and enforced by humans. But as machines get smarter and more autonomous, lawmakers and courts will face increasingly complex dilemmas regulating their conduct, for discussion see [49]. As noted in a 2019 report by the Expert Group on Liability and New Technologies, established by the EU Commission [26]:

> "The more complex these ecosystems become with emerging digital technologies, the more increasingly difficult it becomes to apply liability frameworks."

The current uncertainty poses many concerns for those seeking to develop UAS, particularly in BVLOS settings where the usual tests for liability in tort may not be sufficiently developed or nuanced enough to offer adequate guidance. As it stands, the legal uncertainty hampers cross border cooperation and provides no incentives for the development of the current technology.

3.2 Privacy and Data Protection Concerns of UAS Operations

Existing UAS capabilities and applications raise several issues in respect of privacy, data protection, and general ethical concerns [27]. Although closely related, the right to respect for private life and the right to personal data protection are distinct rights [28]. Currently, there are no UAS specific privacy or data protection legislative instruments at either the national or European level [26]. Instead, at the European level, the right to respect for private life is regulated mainly by the ECHR and the Charter of Fundamental Rights of the European Union (CFR), and the right to data protection is regulated by the General Data Protection Regulation (GDPR). Each of these instruments works differently and the UK is no longer subject to the CFR or GDPR. The current law in the UK is governed by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit)) Regulations 2019 which amended the UK Data Protection Act 2018 and merged it with the requirements of the EU GDPR to form a new, UK-specific data protection regime.

The right to respect for private life exists in Article 8 of the ECHR, and Article 7 of the CFR. Neither instrument, however, contains any detailed provision UAS, nor is there any case law that directly addresses UAS. There is, in contrast, a rich case law on surveillance, albeit this mostly concerns arbitrary interference with the right to respect to privacy by public authorities. But this case law is insufficient to provide real clarity for those operating UAS, particularly in new and novel use cases.

Specific rules on UAS are also found in domestic law. Among others, the German Air Traffic Ordinance (LuftVO), which regulates UAS in Germany, stipulates that there is a ban on UAS operations over residential property if the take-off mass of the device is more than 0.25 kg or the device or its equipment is capable of receiving, transmitting or recording optical, acoustic or radio signals unless the owner or other authorised user has expressly consented to the overflight [29]. Similarly, Article 6211–3 of the French Transport Code states that the right of an aircraft to fly over private property cannot be conditions that would interfere with the exercise of the owner's rights.

At the European and national level, data protection is regulated by the GDPR. Unlike the previous two instruments, the GDPR does not mainly address States or the Institutions of the EU. Instead, it addresses both Member States and as well as all-natural and legal persons within the EU's jurisdiction. In this way, it resembles domestic law, and like domestic law, it is also far more detailed in its provisions. The GDPR forms part of the UK's retained law, post-Brexit (see Sect. 3). GDPR does not apply to the processing of personal data by a natural person in the course of a "purely

personal or household activity" as Recital 18 notes. However, commercial UAS operations over a residential property where the aircraft is equipped with a camera requires specific permission.

Article 4 of the GDPR provides a broad definition of "personal data". The right to personal data protection comes into play whenever such data are processed. This includes any data that may enable identification, such as photographic images that are clear enough to recognise a person. Consequently, any use of UAS for visual or other surveillance that captures members of the public and records them must comply with the GDPR. This is not limited to images. The form in which personal data is stored or used is irrelevant. Thus, audio recordings, for example, spoken communications, may also contain personal data [30, 31].

As in other areas of the law, the case law will eventually develop to provide more certainty, for instance, relating to the capture of digital images for autonomous UAS D&A capabilities. But as it stands, legal uncertainty creates little incentives for the development of these technologies.

3.3 Criminal Law of UAS Operations

The operation of UAS may also violate criminal law. In 2014, for example, Robert Knowles became the first person in the UK to be successfully prosecuted for the dangerous and illegal operation of a UAS. He was convicted for having flown in restricted airspace, as well as allowing the device to fly too close to a vehicle bridge. Both offences breached the UK's 2009 Air Navigation Order and Mr Knowles was fined £800 and order to pay costs [32]. Other countries likewise have specific operational conditions UAS in geographical zones [8]. French law, for example, provides six months imprisonment or a fine of up to €15,000 for unintentionally operating a UAS over a prohibited area. The fine increases to €45,000 and imprisonment may increase to a year if this is done intentionally, as outlined in Article L6232-2. It is, however, unclear how these provisions would apply to an autonomous UAS.

A 2019 German decision illustrates another possible interaction between criminal law and the operation of UAS. A German district court ruled that a homeowner was justified in shooting down a UAS which was flying over his property. The court found that the defendant's actions were justified according to Sect. 228 of the German Civil Code because he defended himself against an infringement of his property and private life [33]. He was thus acquitted of a charge of damage to property. In addition to recognising the defendant's right under the Civil Code to take action to prevent the infringement of the defendant's rights, the court also stated that is was likely that the UAS operator had violated the German Criminal Code, and for this reason criminal proceedings could have been brought against the operator.

The uncertain application of criminal law, which like civil law is anthropocentric, highlights the difficulty of applying the law to autonomous UAS operations, BVLOS or otherwise. Not only is the application of criminal law to autonomous UAS uncertain, but criminal law varies significantly from one country to another. Complicating cross-border cooperation and again providing little incentive for development.

4 Regulations for UAS Operations

This section describes the issues surrounding autonomous software-intensive systems under current roadmaps.

Regulatory bodies have foreseen the challenges and complications that will arise when UAS are allowed to perform autonomous missions BVLOS. EASA regulations require direct connection to and from the remote pilot and line of sight [15]. These regulations segment the operations according to risk:

- **Open operations** do not require authorisation by an Aviation Authority for the flight but must stay within defined boundaries for the operation (e.g. distance from aerodromes, from people, etc.). The UAS must be flown: (I) under direct visual line of sight (VLOS): 500 m, (II) at an altitude that does not exceed 150 m above the ground or water, (III) outside specified reserved areas (airport, environmental, security), and (IV) to avoid flying over crowds, which is prohibited.
- **Specific operations** require a risk assessment that will lead to an "Operations Authorisation" with specific limitations adapted to the operation. To operate under this category, the drone operator needs authorization from the relevant national aviation authority. The regulation defines two standards scenarios for operations within this category. When the operation cannot be classified within these two standards scenario, specific authorization is needed and should be applied based on the Specific Operation Risk Assessment methodology (see below) [8].
- **Certified operations** aim at future operations of UAS, and envisions unmanned taxis or unmanned deliveries. These are foreseen as operations with higher risk and thus will always require certification. Regulations for the certified operations are currently under development [15] and the first draft is expected in 2021 [8].

Other interest groups have looked at UAS operations and their safety. Unlike EASA, these organizations have not legal mandate to make legal rules. Their recommendations can influence future rules. We review them in this section as they complement the complexity of the landscape that UAS operations face.

JARUS is a group of experts from the National Aviation Authorities and regional aviation safety organizations. It has developed a Specific Operation Risk Assessment (SORA) [34] which is considered the leading framework of UAS operations, according to a recent NATO report [5]. The purpose of the JARUS SORA is to define a methodology for the risk assessment which will be required to support an application for authorization to operate a UAS within the specific category. The risk assessment allows the operation to be classified under one of the five possible Specific Assurance and Integrity Levels (SAIL). The methodology also requires that mitigation actions are aligned with the relevant threat level.

Finally, Air Traffic Management Services, like U-Space, will enable the integration of airspace for both manned and unmanned aircraft [35]. One of the key goals of U-Space is to "enable high-density operations with multiple automated drones under the supervision of fleet operators" (from [35]). Again, the capability for "robust detect and avoid operations" is seen as a key enabler for the "significant increase of UAS operations" [35].

In short, the regulatory landscape envisages the development of unmanned BVLOS UAS operations and takes a cautious approach towards it, i.e. recognising that whilst it is not allowed at the moment, progress towards it seems inevitable. To address the challenges of unmanned BVLOS several developments must come into play (from technology and standards to the accompanying regulations).

5 Software Product Certification for UAS Systems

This section aims to convey that there are currently no standard or certification processes for software-intensive systems that can be used to demonstrate the capabilities of a software system deployed for commercial UAS operations.

Regarding aviation-specific standards, in 2021, EASA has published the guidelines for the certification of UAS-based products operating in the specific category [36]. The first certification issued under this provision was awarded in June 2021 [36]. These are risk-based guidelines, with operators advise to submit their designs (and supporting evidence) for EASA certification. Yet, these guidelines are biased towards manufacturing solutions, indeed there are no software-based examples in [36], and like the ISO ISO/IEC 250xx family of standards (see below), the scope is defined and provided by the interested party. Alternatively, the EASA's AMC 20-115D established requirements of quality assurance of software aspects of airborne systems [37], yet in this case, the regulation is based on larger, manned aircraft.

For the certification of software-intensive solutions (like D&A artificial intelligence-based solutions) the International Standards Organization offers two alternatives, the ISO 9001:2018 and the I the ISO/IEC 250xx family of standards. The ISO 9001 series of standards is arguably the most widespread standard. Its process-based, meaning that it focuses on formalizing, and improving the process as a means to improve the quality of the products.

ISO 9001:2018 does not deliver the needed depth and the attention must be placed on *product-oriented certifications*. Historically, the ISO 9001 series evolved from being scoped to manufacturing environments to product and services environments (after 2001). Yet for certifying the capabilities of software-intensive products, the ISO/IEC 250xx family of standards is more suitable. First, the ISO 9001:2018 audit guideline established a provision for a stakeholder to deem clauses 8.5 (Product provision) and 7.1 (Measurement and Calibration) outside of the scope of the certification [38]. These are two key areas to consider for D&A capabilities. Furthermore, while the ISO 9001:2018 standard a process-based. Process-based standards operate on the assumption that improving the process will lead to a better product, but they do not guarantee that the quality of a specific product resulting from a certified quality managed process. In contrast, product-based standards govern the capabilities of a specific product.

The ISO/IEC 250xx:2013 is specifically targeted at software based-products [39] (as opposed to process), meaning that a specific version is under the scope of an evaluation. It is much more complex to navigate than ISO/IEC 9001:2018 and is comprised of 12 different standards addressing aspects of software quality model, measurement, requirements, and evaluation. The ISO/IEC 25,010:2011 defines the quality attributes that can be measured in a software product. The quality attributes are grouped into eight quality characteristics (functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability and portability). However, for the purposes of certifying fit-for-purpose D&A systems, the ISO/IEC 25,040:2011 [40], falls short as it only establishes evaluation procedures (not certification procedures). We stress that product certification is not the same as product evaluation. Product certification requires that an audit is performed by an independent and objective third party [38], and is not covered by the ISO/IEC 250xxx family of standards [39].

Table 1 summarizes the key comparison points of the standards mentioned in this section.

6 Understanding Requirements for Autonomy in UAS Quality Assurance and the Challenges to Attain Them

An autonomous system seeks to achieve a goal and operates without interferences from a human actor and can exhibit unpredictability and non-deterministic behaviours (adapted

from [41]). In a scenario involving remote unmanned BVLOs operations, a fully autonomous robust *D&A capability* is to be expected to ensure these operations are as safe as manned operations. However, we highlight that none of the reviewed standards or regulations has defined D&A capability. For instance in terms of the size and type of objects that must be detected by an autonomous D&A system. Nor have these defined the standard manoeuvres and separation that the UAS must maintain with the intruder object been outlined.

EASA has set the roadmaps for the application of AI in airborne operations [42]. The two core concepts of this roadmap are the levels of automation as well as the trustworthiness and explainability of AI (XAI). XAI is aimed at making the decisions of AI systems understandable to humans [43]. The taxonomy of autonomy for surface vehicles [11] (developed by an international automotive manufactures interest group with no mandate to establish regulations) establishes a five-category taxonomy to describe the level of human involvement in the task. The taxonomy ranges from no automation to fully autonomous. In this taxonomy, human intervention is expected at higher levels (levels 3 and 4), and fully autonomous driving is not achievable until the human can be completely taken out of the loop. In Fig. 2 we map the EASA roadmap against the 5-level autonomy taxonomy. We also incorporate the capabilities for robust D&A and show how they map to this taxonomy.

The EASA airborne operation roadmaps foresee that XAI will be a key enabler technology for the adoption and public acceptance of autonomy in airborne systems. However, we note that the roadmap targets only level 3 autonomy by 2029. Furthermore, it is worth noting that the scope of EASA reports is very broad, applying to aviation in general and not specifically to UAS. The envisioned use cases in [44] do not address UAS operations, let alone D&A requirements. Additionally, neither the EASA roadmap documents nor the literature on XAI delves into the requirements imposed on the development process to achieve the quality levels expected in the roadmaps. The quality assurance of these types of systems is not only challenging [45, 46], but pushes the limits of current engineering technologies [47]. Our experience in assuring the quality of these types of systems suggests that the following main strategies must be put in place to guarantee its quality:

Table 1 Summary of reviewed standards

Characteristic	ISO 9001:2018	ISO/IEC 250xx:2013	EASA Guidelines
Standpoint	Process Based	Product based	Product Based
Origin	Manufacturing	Software	Manufacturing
Technical Requirements	Provided by the interested party		
Scope provisions in the standard	Clauses 8.5 and 7.1 can be left out of the scope	The scope is defined during evaluation preparation	Product requirements define the certification scope
Output	Certification	Evaluation	Certification

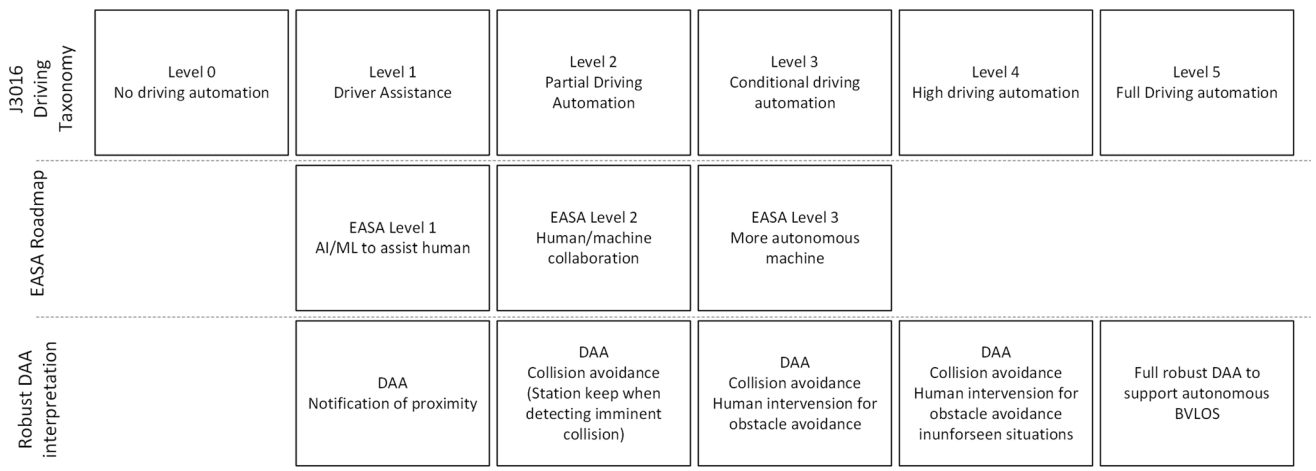

Fig. 2 Autonomy levels taxonomy, mapping between J3016[11], EASA Roadmap [42] and DAA capabilities

- **Consider software quality in the development process**: XAI is concerned with the AI model, the post-hoc explainability of the model and the management of the data used during the development and training of the model. This requires careful consideration of the development process and in particular of the versioning and configuration management of the software assets. Dataops and model-ops lifecycle management processes must assure reproducibility of the lab results in the operational environment [48].
- **Exploit computational platforms for testing**: Verification of these software systems require investment in testing infrastructure that can reproduce the operational environment [49].
- **Exploit Digital Twins**: Exploit advanced compute-intensive techniques (digital twins) that impose no restrictions in the context and its variation for verifying self-adaptive autonomous CPS [50].

As we discuss in Sect. 7, we are arguing that regulators and lawmakers must understand these technical aspects for the development of the standards and a future certification ecosystem that fosters innovation whilst maintaining the safety and security of the airspace. These definitions will become the key enabler to allow the certification of unmanned BVLOS operations and to provide reasonable levels of assurance for the safety of current and future UAS operations.

7 Envisioning an Ecosystem to Support Innovation in Regulated Unmanned UAS Operations

This section conveys that other domains have faced similar challenges for deploying software-intensive solutions and draws their lessons learned in the D&A UAS domain.

We draw from two seemingly different domains that have tackled similar certification needs. First in the maritime industry when container ships are approaching inland ports, it is the port authority that is responsible for having updated maritime charts. Therefore, the requirements for deploying maritime charts technology are well established. The second domain is related to secure credit card online transactions. In 2019 there was over 440 billion online credit card transaction [51], that massive volume of transaction requires quality levels and reliability to assure the smooth operation of the system. Therefore, credit card operators conceived the Payment Card Institute to develop standards that would assure the secure and reliable operation of the system. Whist we are using these scenarios as a reference, we note that in contrast to D&A scenarios, there is no obvious risk to life when the software fails. Nonetheless, we name these common drivers as:

CD1. A key stakeholder with financial interests in the events of failures.
CD2. An independent body that can provide objective audits.
CD3. Specific quantitative quality targets must be achieved to deploy new technology in the domain.
CD4. Market pull to design and deploy new technologies.

A key difference of the DThis section envisions how a regulated environment that fosters innovation in unmanned BVLOS operations can be developed. A key enabler is that the legal framework should be able to recognise the complexity of the technologies involved when assessing liability. And only technologies that have been certified can be legally allowed to be deployed.

Identifying Key Stockholders with Financial Interests (C1) In the unmanned BVLOS domain, regulation and legal framework become major factors in ensuring the success of operations. As mentioned in Sect. 2 the legal framework is risk-averse as loss of life caused by unmanned autonomous accidents is not tolerated by the general public.

Current regulations establish probability formulas for life-critical missions in manned UAS operations (for instance [5]), and these formulas can be ported to unmanned UAS operations. The legal framework should enable unmanned operations once the flight capabilities can be demonstrated (though the compliance with a standard) to be at least equal to the capabilities of a human pilot.

Identifying and Developing an Ecosystem of Independent Auditors (CD2) A pool of independent auditors must be trained and become available for certifying the capacity of the autonomous UAS against a standard. As mentioned in Sect. 4, we believe that the ISO/IEC 250XX family of standards provides the best-known model for the type of standard that will be needed to demonstrate human-like capabilities from autonomous UAS. The challenges involved in developing the technologies that support autonomous UAS will require that these auditors are trained and proficient in the involved technologies. Furthermore, the standard must be product-based (not process-based), as the auditor must certify the compliance of each software system deployed to the UAS. This minimises the risk that faulty versions of the systems are deployed to the operational environment.

Finally, we stress that it is the key stakeholder who must define the scope of the product audit through the definition of a standard with clear measurement targets (**CD3**) (see Table 1). As such, regulators (like EASA) must develop these standards that consider the software-intensive nature of BVLOS technical solutions (see Sect. 6) to incorporate

clear and SMART targets into the standard (see Table 2). This standard must also consider the requirements for the human resource that will become the auditors. As described in ISO/IEC 19,011:2011 all audits must be planned and tailored to the specific organization. This is carried out by the trained auditor in cooperation with the organization. Upon completion of the audit, a report must then be submitted to the regulator. For AI-intensive systems, this report will need to include not only versioning information of the software and hardware components but also dataset to assure explainability and uniqueness of the version deployed to the operational environment.

Specific Quantitative Quality Targets that Must be Achieved to Deploy New Technology in the Domain (CD3) As mentioned, the standard must establish SMART target against which the capability of the system will be measured. We exemplify with the D&A scenario but are mindful that requirements must include other areas of the autonomous BVLOS missions.

Requirements for D&A are loosely defined in the literature and observed reports. For instance, in [52], only broad lines of interest are mentioned, these are fly by sensors to avoid interruptions to communications, or fly-by-wire, which means to prepare flightpath (and variations) to and from the mission target to accommodate for unexpected events in the operational environment. In [5] Safety is defined as the potential of the system to cause either mid-air collision with manned aircraft and harm to people. And, as mentioned before, specific formulas to calculate the probability of these events are provided. Scenarios for loss of hardware and communication capability can be inferred from the EASA Concept of Operation for UASs [15], but mostly deal with foreseen issues related to physical services (like loss of GNSS, Communication with the pilot, etc.). Detect and avoid requirements and scenarios are deemed key for the successful delivery of UAS operations, but have since not yet been defined [53].

In Table 2 a few examples of indicative requirements that can be included in an autonomous Detect and Avoid standard are presented.

Requirements in column "Derived requirement" from Table 2 express generic compliance requirements written in a generic standard language. To demonstrate compliance the developers of autonomous BVLOS technologies must interpret these requirements to their operational scenarios. For example, for Req1, three representative validation scenarios have been described in [5] given a loss of communication between the UAS and the Command and Control Centre:

Verify that navigation mode switches to a relative.
Station keep for a specified period until communication is restored.
Return to home – following the inbound flight path if communication is not restored after a pre-determined period.

For autonomous BVLOS operations, the service provider must interpret these and document them into appropriate test cases (Req5) so an auditor can access compliance. For instance, a critical test case could involve the artificial loss of communication for a period greater than the autonomy of the UAS, so that the autonomous BVLOS UAS can demonstrate its capacity to safely return to home without running out of battery.

7.1 Initial Results When Dealing with Req3 and Req4

In the context of the use case presented in Sect. 7.1, we exemplify compliance with our indicative requirements (see Table 2) for a future standard. In this section, we draw the example of detecting a small non-cooperative flying object entering the vicinity

Table 2 Indicative requirements for robust autonomous Detect and Avoid standard requirements

ID	ISO 25010 Quality attribute	Derived requirement
Req1	Availability	Establish a two-way communication between the UAS and the Command and Control Centre (taken from [15, 53])
Req2	Adaptability	Demonstrated capability for vertical and lateral manoeuvres that can be autonomously taken to react to unforeseen static objects in the operational environment (adapted from [15])
Req3	Operability	Detect small intrusions in vicinity airspace and monitor their flightpath to determine if they are at risk to the autonomous UAS operation (adapted from [54])
Req4	Functional correctness	For potentially hazardous small intrusions navigate to achieve separation based on a 50 ft. horizontal and ± 15 ft. vertical volume (adapted from [54])
Req5	Testability	Establish and maintain a Test Suit to demonstrate all previous requirements

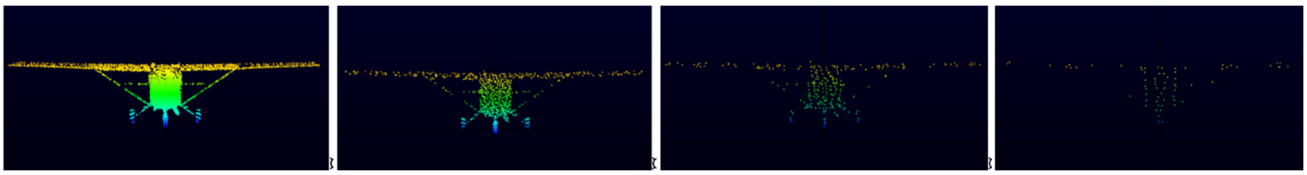

Fig. 3 Elevation front profile of a small aircraft imaged at 15 m, 45 m, 75 m, and 150 m (bottom row, left to right) (from [14])

of the unmanned BVLOS UAS (related to Req3 in Table 2). We describe our development process in terms of the recommendations in Sect. 6 and present our initial results (evolved from [14]).

Consider Software Quality in the Development Process We have devised an incremental life cycle process with feedback loops from the product to the development process. Software is verified in small increments through unit test cases and deployed to the field at regular intervals.

Exploit Computational Platforms We rely on real-world LiDAR simulators to complement the limitations of the Unity Game engine for the Digital Twin. This simulation is executed in a massive parallel distributed GPU to assure real-time performance. The capabilities of the simulated Lidar is compared at regular intervals with the capabilities of the real world LiDAR to assure consistency between the real and the virtual world.

Exploit Digital Twins A digital twin of the operational environment (the port of Hamburg) has been created and is used to set up use cases that feed the detect computer vision algorithm with trainable data sets.

Warrantee Data Quality and Versioning Foreach version of the Detect CNN, the codebase and the data set is labelled together. So that it is possible to revert to the previous version and to compare the capability of the different versions. This information is critical for establishing the version of the product that can potentially undergo a certification.

Figure 3 presents our indicative results towards Req3, showing the simulation results of the LiDAR capabilities to detect an incoming small flying manned aircraft at different ranges.

7.2 A Discussion of Possible Breaches of Law from Autonomous UAS Operations

Notwithstanding the envisioned ecosystem described in Sect. 7, in this section, we discuss how we a UAS operation like the bridge inspection of critical infrastructure (like the RAPID use case from Sect. 2).

Perspective from the Regulatory Framework The unmanned UAS would have had its software and hardware components certified under the proposed certification process. This would assure that the cyber-physical system behaves.

Perspective from Civil and Criminal Liability We would suggest that to enable innovation, an unmanned UAS should be treated as a human pilot. Yet as mentioned, the law is anthropogenic, therefore the assignment of liability in case of accidents is not straightforward, and it is a hurdle to innovation. In the scenario that the UAS is used as a service by a third party (not the organization that developed the UAS or the D&A capabilities), and it is involved in an accident. In this case, the chain of causality is not straight forwards. As the thirds party can claim the liability in the software/hardware and the manufacturer can claim it lies in the use. This is a similar conundrum as self-driving cars should have, but currently -as self-driving car manufactures have not claimed full autonomy, the burden is on the driving using "assistive driving technology".

8 Conclusions

In this paper, we have taken a multi-disciplinary approach to study the legal and technological aspects of the large-scale deployment of autonomous BVLOS operations of UAS. We presented a summarised account of the legal and regulatory issues that must be considered when performing UAS operations. We showed how a remote pilot is exposed to legal consequences, even when the operation abides by all laws and regulations.

Furthermore, we reviewed the current certification process for deploying UAS technologies. We identify how the current certification process draws mainly from the hardware-based certification process, and fail to recognise the characteristic of software-intensive products. We exemplify these observations with the development of DAA software onboard COTS UAS. These software systems rely on machine learning algorithms that must be trained with massive amounts of data. The certification process must contemplate the characteristics of these software systems to assure that technologies deployed to the operational environment are safe.

We summarised current state-of-the-art regarding quality assurance of safety–critical software-intensive systems and provided a blueprint for a future framework that facilitates the certification and deployment of secure software-intensive solutions that can be proven to operate at a capability that is comparable to an experienced remote pilot. For instance, for D&A technologies, a key enabler for achieving autonomous BVLOS operations is the development of robust D&A technologies that can detect potential hazards and take appropriate actions. In operations involving remote pilots, the burden of detecting and avoid lies with the pilot and their capacity to safely and responsibly operate the aircraft. However, we have shown that there is no equivalent requirement for autonomous UAS to demonstrate similar capabilities. We have shown that this capability can be incorporated into a standard. This has been achieved in other domains, in particular maritime and online payments. The capacity to develop such a standard, supported by the right infrastructure (CD1 and CD2), can be used to demonstrate the competency (airworthiness) of autonomous UAS. As a result, we presented indicative requirements for the D&A system that this type of standards should define. And draw from our research lines to convey how a service provider should demonstrate the capabilities of its software-intensive product, and discuss the implication of similar technologies in terms of the potential civil, criminal and privacy laws.

Looking forward, we are engaging with regulators with a view to providing input to influence ongoing law and policy regarding UAS. On the technology side, we are characterising the detection capabilities of different sensors (optical, thermal, radar and LiDAR) and will continue to build upon the results in [14].

9 Code or data availability

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Author Contributions All authors contributed to the study conception and design. The first draft of the manuscript was written by Santiago Matalonga and all authors (Santiago Matalonga, *Samuel White, Jacques Hartmann and James Riordan)* commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Authors are partially financed by the RAPID Project (www.rapid.eu), H2020-EU.3.4. Grant Agreement number 861211.

Declarations

Competing Interest The authors have no relevant financial or non-financial interests to disclose.

Ethics Appoval Not applicable to the research described in this manuscript.

Consent to participate Not applicable to the research described in this manuscript. No human participantes were involved in the the research described in this manuscript.

Consent to publish Not applicable to the research described in this manuscript. No human participantes were involved in the the research described in this manuscript.

References

1. BIS Research: Global UAV market value in 2018 and 2029 (in billion U.S. dollars) [Graph]. (2019)
2. Zubin, I., van Arem, B., Wiegmans B., van Duin R.: Using drones in the last-mile logistics processes of medical product delivery. A feasibility case study in Rotterdam. In: 99th Annual Meeting Transportation Research Board. (2020)
3. Kitonsa, H., Kruglikov, S.V.: Significance of drone technology for achievement of the United Nations sustainable development goals. R-economy **4**(3), 115–120 (2018)
4. SDG Knowledge Hub: "Drones for SDGs: Fast, Low-cost Delivery of Health Care Supplies for Remote Populations in Malawi," 2019. [Online]. Available: https://sdg.iisd.org/commentary/guest-articles/drones-for-sdgs-fast-low-cost-delivery-of-health-care-supplies-for-remote-populations-in-malawi/. [Accessed: 16-Jun-2021]
5. NATO - Applied Vehicle Technology panel: "considerations for the harmonisation of UAS regulations for common nato operations," (2020)
6. UK CAA: Step forward for the drone industry as Civil Aviation Authority authorises trial of a concept for routine BVLOS operations. (2021). [Online]. Available: https://www.caa.co.uk/news/drone-trial-of-routine-bvlos-operations-concept-authorised/. [Accessed: 07-Mar-2022].
7. UK CAA: Flying in the specific category. (2020) [Online]. Available: https://www.caa.co.uk/Commercial-industry/Aircraft/Unmanned-aircraft/Small-drones/Flying-in-the-specific-category/. [Accessed: 06-May-2021]
8. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.). 2019, p. C/2019/3824.
9. UK CAA: Regulatory Article 1200 - Air Safety Management.
10. Stewarts law: Getting the Deal Through's guide to Drone Regulation 2020. 202AD. [Online]. Available: https://www.stewartslaw.com/news/guide-to-drone-regulation-2020-lexologys-getting-the-deal-through/. [Accessed: 30-Aug-2021]

11. SAE: J3016_202104. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. (2021)
12. Jiménez López, J.: RPAS certification. Where the challenges lie. Military Airworthiness Conference. Rome 2014 (2014)
13. Revolve Media: RAPID Website. (2022). [Online]. Available: https://rapid2020.eu/. [Accessed: 07-Mar-2022]
14. Riordan, J., Manduhu, M., Black, J., Dow, A., Dooly, G., Matalonga, S.: LiDAR simulation for performance evaluation of UAS detect and avoid. 2021 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1355–1363. (2021). https://doi.org/10.1109/ICUAS51884.2021.9476817
15. EASA.: EASA concept of operations for drones. (2015)
16. van Dam, C.: European tort law. Oxford University Press, Oxford (2013)
17. Oliphant, K.: The law of tort. LexisNexis, London (2013)
18. O'Neill A.: Rescuing the Law of Tort? The Decision of the Supreme Court in O'neill v Dunnes Stores. Irish Jurist (1966-). **45**, 240–245 (2010)
19. Binchy, W.: Tort Law in Ireland: A Half-Century Review. Irish Jurist **56**, 199–218 (2016)
20. Clerk, J.F.: Clerk & Lindsell on torts, 23rd edn. Sweet & Maxwell, London (2020)
21. Kelsen v Imperial Tobacco Co. 2 QB 334, 2 All ER 343. (1957)
22. Anchor Brewhouse Developments Ltd v Berkley House (Docklands Developments) Ltd 38 BLR 82. (1987)
23. Bernstein of Leigh v Skyviews & General Ltd QB 479. (1978)
24. Horsey, K.: Tort law. Oxford University Press: Oxford, United Kingdom New York, NY, (2019)
25. Barfield, W.: Advanced introduction to law and artificial intelligence. Edward Elgar Publishing, Cheltenham, UK Northampton, Massachusetts (2020)
26. Matalonga, S., Rodrigues, F., Travassos, G.H.:. Characterizing testing methods for context-aware software systems: Results from a quasi-systematic literature review. J. Syst. Softw. **131**, 1–21 (2017). https://doi.org/10.1016/j.jss.2017.05.048
27. Finn, R. de H. P. J. L. Wright David: "Study on privacy, data protection and ethical risks in civil remotely piloted aircraft final report," Directorate-General for Enterprise and Industry (European Commission), Luxembourg, (2014)
28. European Union: Charter of Fundamental Rights of the European Union. (2012)
29. LuftVO [German Air Traffic Regulations]
30. Peck v the United Kingdom, No. 44647/98. (2003)
31. Köpke v Germany, No. 420/07. (2010)
32. UK CAA: CAA successful prosecutions: 1 April 2014 TO 31 March 2015. (2015)
33. Giesa A.: Judgment of April 24, 2019 - 9 Cs 926 Js 3044/19. (2019)
34. JARUS WG 6: "JARUS guidelines on Specific Operations Risk Assessment (SORA). (2017)
35. SESAR Joint Undertaking: U-Space Blueprint Brochure. (2017)
36. EASA: Design verification of UAS operated in the 'specific' category and classified in SAIL III and IV. (2021)
37. EASA: AMC 20–115D Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178. (2017)
38. ISO 19011:2012 - Quality Management System Auditing
39. Rodríguez M., Piattini M.: Experiencias en la industria del software: Certificación del producto con ISO/IEC 25000. In: CIBSE 2015 - XVIII Ibero-American Conference on Software Engineering. (2015)
40. ISO/IEC 25040:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process
41. Wang, Y.K.N, Plataniotis, S., Kwong, H., Leung, S., Yanushkevich, F., Karray, M., Hou, et al.: On autonomous systems: From reflexive, imperative and adaptive intelligence to autonomous and cognitive intelligence. En 2019 IEEE 18th International Conference on Cognitive Informatics Cognitive Computing (ICCI*CC), 7-12, (2019). https://doi.org/10.1109/ICCICC46617.2019.9146038
42. EASA: Artificial Intelligence roadmap: A human-centric approach to AI in aviation. 202AD
43. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S. et al.: Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI, 22 de octubre de 2019. http://arxiv.org/abs/1910.10045
44. EASA: EASA Concept Paper: First usable guidance for Level 1 machine learning applications: A deliverable of the EASA AI Roadmap. (2021)
45. Fredericks, E.M., DeVries, B., Cheng, B.H.C.: Towards run-time adaptation of test cases for self-adaptive systems in the face of uncertainty. Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems - SEAMS 2014, 2014, 17–26. https://doi.org/10.1145/2593929.2593937
46. Matalonga, S., Rodrigues, F., Travassos, G.H.: Challenges in testing context aware software systems. En Systematic and Automated Software Testing, Ed. SBQS. BelloHorizonte (2015)
47. Matalonga S., Amalfitano D., Doreste A., Fasolino, A.R., Travassos G.H.: Alternatives for Testing of Context-Aware Contemporary Software Systems in industrial settings: Results from a Rapid review. (2021)
48. Munappy, A.R., Mattos, D.I., Bosch, J., Olsson, H.H., Dakkak, A.: From Ad-Hoc Data Analytics to DataOps. In: Proceedings of the International Conference on Software and System Processes, pp. 165–174. (2020)
49. Matalonga, S., Rodrigues, F., Travassos, G.H.: Characterizing testing methods for context-aware software systems: Results from a quasi-systematic literature review. J. Syst. Softw. **131**, 1–21 (2017)
50. Matalonga, S., Travassos G.H.: Testing Context-aware Software Systems: Unchain the Context, Set It Free!. In: Proceedings of the 31st Brazilian Symposium on Software Engineering, pp. 250–254. (2017)
51. The Nilson Report.: Number of purchase transactions on payment cards worldwide in 2019, by brand (in billions). (2020)
52. Protti, M., Barzan, R.:UAV Autonomy-Which level is desirable?-which level is acceptable? Alenia Aeronautica Viewpoint. (2007)
53. NATO Standard: AEP-4671. Unmanned Aircraft Systems Airworthiness requirements. (2019)
54. Walter, B., Suchy N.: Concept of Use for the Airborne Collision Avoidance System Xu for Smaller UAS (ACAS sXu). (2020)

Dr. Santiago Matalonga is a Lecturer at the University of the West of Scotland. He has a Phd in software and systems from the Universidad Politécnica de Madrid, and did post-doctoral studies at Unviersidad Federal do Rio de Janheiro PESC/COPPE. Since 2010 he is a graded researcher in the Uruguayan research agency and since 2012 in the National Program for the development of basic sciences. Since 2019 he is a fellow of the Higher Education Academy (UK). He has over 60 publications in international journals and conferences in software engineering. Dr Matalonga is currently working on improving the quality of Contemporary Software Systems (IoT; Ubiquitous; Distributed and Systems of systems; AI and Blockchain applications in B2B software systems) and enhancing the productivity of the development teams. To achieve this, he pursues a holistic approach by tackling the problem from both fronts: technical-oriented (architecture, development and testing) and process-oriented (Lean/Agile, or Dev-ops and continuous engineering).

Dr Samuel White is a Lecturer in Law in the School of Business and Creative Industries at the University of the West of Scotland (UWS). He was previously a postdoctoral researcher working on the Risk Aware Port Inspection Drone (RAPID) project and a tutor in law at the University of Dundee. He completed his LLB (Hons) at the University of Dundee before working in risk and compliance in the financial services sector. In 2017, he returned to the University of Dundee to complete a PhD funded by the Carnegie Trust for the Universities of Scotland. Dr White has a particular interest in human rights, constitutional law, and the interaction between domestic and international law. He regularly submits evidence to inquiries on these issues and has presented and published research in these areas around the world. Since 2015, Dr White has been a director of the Scottish Legal Action Group, an access to justice charity.

Dr Jacques Hartmann is a Professor of International Law at the University of Dundee, UK, and Visiting Professor at Universidad de la Sabana, Colombia. He is a generalist international lawyer, and his published works reflect the breadth of the discipline, encompassing diverse areas such as human rights and drone regulation. He has published widely in leading legal journals; his most recent publication is The Achievements of International Law, Hart 2021. Professor Hartmann holds a PhD from Cambridge University, where also he worked as a Research Associate at the Lauterpacht Centre for International Law. He has taught international and human rights law at numerous universities in the UK, including Durham, Glasgow and Edinburgh and overseas, while regularly appearing as an invited speaker for international legal affairs. Prior to joining Dundee University, Professor Hartmann worked as Legal Officer at the Danish Ministry of Foreign Affairs, representing Denmark before the International Court of Justice as well as at various diplomatic conferences. He has submitted evidence to several governmental enquiries and has vast experience assisting governmental, intergovernmental and non-governmental organisations.

Dr. James Riordan specialises in robotics and sensing and is an expert in autonomous vehicles applied to land, air, and sea domains. He is a Reader at University of the West of Scotland where he leads an €8 million portfolio of research projects as Principal Investigator and founding Director of the ALMADA Research Centre. He is PI of the European Commission H2020 project RAPID (risk aware port inspection drones) and is an independent external expert to the European Union Aviation Safety Agency. Dr. Riordan has a PhD in underwater sonar modelling and simulation from University of Limerick, Ireland. He has established and successfully commercialised several strands of patented research and has been recipient of 3 national awards for research and innovation. He is currently supervising 5 PhD students and he publishes extensively in international journals and conferences.