UNMANNED AIRCRAFT SYSTEMS AND STRICT PRODUCT LIABILITY IN THE UK: TIME FOR REFORM

George LELOUDAS* & Furkan BULUT**

Digitalisation and advanced communication technologies are poised to enable the deployment of Unmanned Aircraft Systems (UAS) in non-segregated airspace through Beyond Visual Line of Sight (BVLOS), including those that are autonomous. This transition shifts the primary source of accident risk from human error to product defect. . As such, it is critical to assess the adequacy of the relevant compensation mechanisms. The Consumer Protection Act 1987 (CPA 1987) is the primary tool that imposes strict liability on producers for defective products in the UK; however, it was drafted before the widespread deployment of interconnected cyber-physical systems and self-learning algorithms. This article evaluates the application of the CPA 1987 to UAS, arguing it is unable to cater for digital technologies, including (but not limited) to defining the "product", establishing post-supply liability, and addressing the burden of proof for AI applications. Furthermore, it argues that reliance on the operator-focused s 76 (2) – (4) of the Civil Aviation Act 1982 transfers the burden of product defects onto UAS operators. Building upon the new EU Product Liability Directive, this article concludes that the existing product liability framework of the UK is inadequate and requires reform.

Keywords: unmanned aircraft systems (UAS), product liability, strict liability, Consumer Protection Act 1987, Civil Aviation Act 1982, digitalisation, artificial intelligence, legislative reform

1. INTRODUCTION

1.1 Automation and digitalisation in transport

Nikola Tesla's 19th-century radio-controlled vessel, called "Teleautomatics", introduced the idea of remotely steering transport via wireless technologies.[1] Progress in computer science during the 20th century and Industry 4.0, a revolutionary shift towards digital products, have sped up this development, building on major advancements in communication systems, computerised control systems, preprogrammed automation, the growth of networked systems, and the Internet of Things.[2] The world is now entering an era of human-machine collaboration, where tasks are not only performed remotely but are increasingly delegated to intelligent machines thanks to significant advances in artificial intelligence and machine learning. In this setting, the integration of autonomous systems has opened the door to reducing human oversight in vehicle operation, enabling unmanned vehicles.

Primarily, automation in the transport sector aims to shift certain risks, often called the "Three Ds - dangerous, dirty, and dull", from humans to machines.[3] This encompasses dangerous tasks that jeopardise human lives, such as inspecting ship hulls; dirty tasks that expose humans to

* *Professor, Institute of International Shipping and Trade Law, HRC School of Law, Swansea University, Wales, United Kingdom. Email: g.leloudas@swansea.ac.uk*
** *PhD Candidate, Tutor in Law, HRC School of Law, Swansea University, Wales, United Kingdom. Email: furkan.bulut@swansea.ac.uk* and *furkanbulut4@gmail.com*.

[1] *See,* George V Sosic, *TESLA – The Father of RC* published by the Academy of Model Aeronautics in *The AMA History Project Presents: Biography of Nikola Tesla* (2010), https://www.modelaircraft.org/sites/default/files/TeslaNikola.pdf (accessed 20 Oct 2025).

[2] S O Johnsen et al *Experiences of main risks and mitigation in autonomous transport systems* 2019 J. Phys.: Conf. Ser. 1357 012012.

[3] Douglas M Marshall, *Dull, Dirty, and Dangerous: The FAA's Regulatory Authority over Unmanned Aircraft Operations,* [2004-2008 Transfer Binder] Issues Aviation L. & Pol'y 1,0085ff (2007).

harmful environments, like monitoring air quality; and dull tasks, such as performing repetitive and monotonous activities like handling cargo. Remotely controlled and autonomous vehicles are recognised not only for their ability to minimise these risks but also for their potential to improve global commercial and environmental sustainability. This entails speeding up operations in the transport sector, supporting the circular economy by increasing supply chain efficiency, and aiding the fight against climate change through the use of alternative energy sources to lower carbon emissions.[4]

The autonomous car market, encompassing driving assistance technologies to high automation levels that do not require human supervision, is experiencing rapid growth and is expected to reach USD 2,752.80 billion by 2033.[5] Highly automated vehicles are projected to account for a significant percentage of new car sales in Europe (7%), the United States (9%), and especially in China (36%) by 2035.[6] The shipping industry follows a similar path with the market for vessel autonomy reaching USD 2.3 billion in 2023.[7] Also, as of 2023, 215 companies are estimated to be actively developing autonomous solutions for vessels, and projects involving autonomous container ships and ferries have already commenced operations.[8] Rolls-Royce anticipates that autonomous ships will be fully operational by 2035.[9] The technological and economic momentum demonstrated by the motor vehicle and maritime industries is mirrored in the aviation sector, to which we now turn our attention.

1.2 Growth in Unmanned Aircraft Systems (UAS)

The aviation sector has long experienced similar technological advancements, including the use of autopilot systems and fly-by-wire technology, which have replaced mechanical controls.[10] This digitalisation is made possible by the rapid miniaturisation of microprocessors, which allowed complex computational power onto small airframes, and the integration of reliable satellite navigation systems (such as GPS), which provide accurate, all-weather positioning data essential for non-visual and autonomous flights.[11] Progress in communication systems has further assisted, as command and control (C2) data links enabled low-latency,

---

[4] *See,* George Leloudas & Michael Chatzipanagiotis, *Use of Unmanned Aircraft Systems in a Maritime Context* in B Soyer and Andrew Tettenborn (eds) *Disruptive Technologies, Climate Change and Shipping* (Informa Law from Routledge 2022) 55ff (Leloudas & Chatzipanagiotis).

[5] Precedence Research, *Autonomous Vehicle Market Size, Share, and Trends 2025 to 2034* https://www.precedenceresearch.com/autonomous-vehicle-market?utm_source=chatgpt.com (accessed 20 October 2025).

[6] PWC, *Digital Auto Report 2023 (volume 2)*, https://www.strategyand.pwc.com/de/en/industries/automotive/digital-auto-report/volume2.html?utm_source=chatgpt.com (accessed 20 Oct 2025).

[7] Hazel Sivori, and Lauren Brunton, *Out of the Box. Implementing autonomy and assuring artificial intelligence in the maritime industry* (Thetius LR 2023) https://www.lr.org/en/knowledge/research-reports/2023/ai-and-autonomy/ (accessed 20 Oct 2025).

[8] *Ibid.* See also Yara, *Yara Birkeland, two years on* https://www.yara.com/knowledge-grows/yara-birkeland-two-years-on/ and Finferries, *Finferries' Falco world's first fully autonomous ferry* https://www.finferries.fi/en/news/press-releases/finferries-falco-worlds-first-fully-autonomous-ferry.html (accessed 20 Oct 2025).

[9] *See*, Rolls-Royce, *Autonomous Ships – The Next Step* https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/%20customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf (accessed 20 Oct 2025).

[10] *See*, Atul Garg, Rezawana Islam Linda and Tonoy Chowdhury, *Evolution of aircraft flight control system and fly-by-light flight control system,*3 International Journal of Emerging Technology and Advanced Engineering (2013) 60.

[11] *See*, Kenzo Nonami, Farid Kendoul, Satoshi Suzuki, Wei Wang, & Daisuke Nakazawa, *Autonomous Flying Robots: Unmanned Aerial Vehicles and Micro Aerial Vehicles* (Springer 2010).

high-bandwidth communication between the remote pilot, air traffic controllers and the aircraft, bridging the gap left by eliminating the human pilot on board.[12] This convergence of technologies allowed the development of what is now known as Unmanned Aircraft Systems (UAS), commonly referred to as drones.

Their deployment is already underway across various fields. UAS are expected to contribute up to £45 billion to the UK economy by 2030.[13] For instance, in agriculture, they are used for field mapping and nutrient assessment;[14] in construction, they improve safety management;[15]and in fire and rescue operations, they are increasingly common for filming, thermal reconnaissance and dropping fire retardant, enjoying high public support due to their life-saving potential.[16] The maritime industry also utilises them extensively for the inspection and maintenance of complex structures, such as offshore installations and ship hulls, often reducing human risk.[17]

Although large cargo loads and passenger transport via unmanned vehicles are not yet routinely performed, they are within reach as technological barriers continue to diminish, and regulators become more confident in the reliability of new technologies. UAS are also set to become a fundamental part of society, as evidenced by a policy paper of the British Government in 2022, where it was indicated that they are poised to fulfil their potential, starting with small cargo deliveries and eventually transporting humans.[18]

This ambition was part of the reason behind the establishment of the UK Airspace Modernisation Strategy (AMS), which addresses the future of all UK airspace users (manned commercial, general aviation, military, UAS, and new vehicles like electric Vertical Take-off and Landing (eVTOL)). Crucially, it will provide the regulatory framework to facilitate routine BVLOS and autonomous operations for UAS in non-segregated airspace.[19] BVLOS is an operational mode that allows UAS to be flown without the remote pilot maintaining direct visual contact, paving the way for autonomous UAS operation.[20]

---

[12] *See*, Ibid., and International Civil Aviation Organisation (ICAO), *Manual on Remotely Piloted Aircraft Systems (RPAS)* (Doc 10019 2015).
[13] PWC UK, *Skies Without Limits v2.0* (July 2022) https://www.pwc.co.uk/intelligent-digital/drones/skies-without-limits-2022.pdf (accessed 20 Oct 2025)(PwC UK Report).
[14] *See*, Samuel Hassler & Fulya Baysal Gurel, *Unmanned Aircraft System (UAS) Technology and Applications in Agriculture* (9) Agronomy 2-3 (2019).
[15] *See*, Mark C. Tatum & Junshan Liu, *Unmanned Aircraft System Applications in Construction* (196) Procedia Engineering 167, at 170 (2017).
[16] *See*, George Leloudas, *The Insurability of Third-Party Liability Risks Arising from the Use of Civilian Uncrewed Aircraft Systems (UAS) in the UK* in Baris Soyer and Ozlem Gurses, Insurability of Emerging Risks (Bloomsbury Publishing 2025) 277ff (Leloudas Insurability).
[17] *See*, Leloudas & Chatzipanagiotis, *supra* n. 4.
[18] *See,* HM Government, *Advancing airborne autonomy: Commercial drones saving money and saving lives in the UK*, https://assets.publishing.service.gov.uk/media/62d52e158fa8f50c08c53382/drone-ambition-statement.pdf (accessed 20 Oct 2025)
[19] *See*, UK CAA, *Airspace Modernisation Strategy 2023–2040: Part 1 Strategic objectives and enablers* (CAP 1711 2023) https://www.caa.co.uk/our-work/publications/documents/content/cap1711/ (accessed 20 Oct 2025). It is important to note that AMS is a multi-decade program addressing all airspace users (crewed commercial, general aviation, UAS, eVTOL etc).
[20] *See,* Leloudas Insurability, *supra* n. 4, at 285ff and George Leloudas, *Civil Liability of Drones in the UK* in Jacques Hartmann, Benjamyn I. Scott, Steven Truxal, Andrea Bertolini, & Anna Masutti (eds), *Civil Regulation of Autonomous Drones in Europe* (Elgar Publishing 2024) 274, at 283ff.

The attributes of UAS also align with the British Government's Jet Zero Strategy to reach net-zero emissions by 2050.[21] Most UAS are powered by electric batteries, hybrid systems, solar energy, or alternative sources, such as hydrogen fuel cells, offering zero-tailpipe-emissions operation in contrast to traditional kerosene-based aviation.[22] This aligns with the Government's recently confirmed targets to promote a transition to sustainable fuels,[23] as UAS promise to reduce carbon emissions by 2.4 million tonnes by 2030, mainly by reducing the need for fossil-fuel-intensive crewed flights.[24]

This ambition to transition UAS from "Visual Line of Sight" (VLOS) operations to BVLOS and autonomous operations transfers the primary source of accident risk from operational failure to product defect.[25] As such, it requires a commensurate update to the legal system, which currently struggles to assign responsibility when a technically sophisticated product fails.

This article argues that failures in UAS technology—intended for widespread, day-to-day deployment—raise concerns about losses and damages suffered by consumers. However, the UK's strict product liability framework, found in the Consumer Protection Act 1987 (CPA 1987), is incapable of accommodating the cyber-physical nature, software complexity, and self-learning algorithms of autonomous UAS. Despite the existence of a separate strict liability regime for ground damage under s. 76(2) – (4) of the Civil Aviation Act 1982 (CAA 1982), the CPA 1987 is the primary mechanism that forces legal scrutiny upon the product itself. The subsequent chapters establish the urgency of this legal challenge.

Chapter 2 begins by detailing the technological imperative, examining how UASs' cyber-physical complexity, their drive toward BVLOS and autonomy, and the reliance on Artificial Intelligence (AI) fundamentally shift the locus of control—and thus, liability—from the human pilot to the product itself. Chapter 3 then analyses the liability regime of s 76(2) – (4) CAA 1982 to highlight why sole reliance on the operator-focused CAA 1982 undermines product safety, confirming the necessity of reforming the CPA 1987. Finally, Chapters 4 and 5 provide the core analysis of the CPA 1987, explaining its inability to handle the digital products, the timing of a defect in self-learning systems, and the claimant's impractical burden of proof, before concluding that the UK must consider a new product liability regime.

2. UAS TECHNOLOGY, BVLOS AND AUTONOMY

---

[21] *See,* UK Department for Transport, *Jet Zero Strategy. Delivering Net Zero Aviation by 2050* https://assets.publishing.service.gov.uk/media/62e931d48fa8f5033896888a/jet-zero-strategy.pdf (accessed 20 Oct 2025).

[22] See Benjamyn Scott & Öykü Kurtpinar, *High Hopes and Higher Hurdles: Unpacking Six Regulatory Challenges Facing Advanced Air Mobility*, Chapter 5 (Leiden University Research Series, Issue 2025/03) for a discussion on the contested nature of "zero-emission" claims when considering the life cycle of Advanced Air Mobility (AAM) aircraft.

[23] *See*, Renewable Transport Fuel Obligations (Sustainable Aviation Fuel) Order 2024 SI 2024/1187 and the Sustainable Aviation Fuel Bill that, at the time of writing (October 2025), was going through the Parliament of the United Kingdom.

[24] PwC UK Report, *supra* n. 13.

[25] For an analysis of the regulatory framework governing operations of UAS in the UK, including VLOS operations and the rules of the Open, Specific and Certified Category, *see*, Leloudas Insurability, *supra* n. 16, at 281ff and George Leloudas, David McClean, Michael Gill, Daniel Wand, Auguste Hocking, Andreas Ruehmkorf, Ingrid Koning, Katherine Posner, Philip Chrystal, *Shawcross and Beaumont on Air Law*, (Lexis Nexis, Issue 194, 2025), Division V, Ch. 26.

While the commercial and environmental benefits of UAS are clear, their path to full integration is complicated by a mismatch between modern technology and existing liability frameworks. This mismatch is the result of a shift from reliable, hardware-based systems to cyber-physical and non-deterministic systems, to which we now turn our attention before analysing the suitability of the current product and third-party liability laws.

2.1 Evolution from hardware to cyber-physical systems

Today's UAS increasingly incorporate cyber-physical elements to deploy them safely in high-risk environments and achieve long endurance and high payload capacity. This design approach is reinforced by class marking requirements that mandate designing all UAS classes to minimise injury risks.[26] At the same time, this evolution from hardware to cyber-physical systems complicates the regulatory framework, because these elements may not reflect the notion of product under product liability laws, require constant modification, and have the potential to exceed the producer's control.

For example, the UK CAA requires specific category UAS to interact with all airspace users, ensuring transparency to aircraft and air traffic controllers.[27] UAS integrated into the broader aviation system must be compatible with all surveillance systems, without imposing any undue additional workload on air traffic controllers or pilots. Thus, operational information can be transmitted back to UAS operators during flight through data communication relays.[28]

To further illustrate our example, we can look into sensor technology. Remote sensing capabilities of UAS encompass a variety of sensors, ranging from visual range cameras that collect data for diverse surveillance purposes, enhanced by stabilisation software to mitigate distortions , to those designed for the electromagnetic spectrum, gamma rays, biological elements, and chemical compounds.[29] Moreover, RADAR and Synthetic Aperture Radar (SAR) achieve fine azimuth resolutions, maintain consistent resolutions regardless of distance, and adapt to different operational needs through signal processing.[30]

These examples demonstrate that UAS operate through a complex combination of hardware and software that reduce the reliance on remote pilots by facilitating communication with other users and aircrafts, very quick data processing, and adaptation to air navigation. However, it increases the necessity of modifications to the system, namely updates and upgrades, to enhance the software's capabilities and adapt to changing operational circumstances.

Moreover, the operation of UAS is expected to leverage emerging connection and storage technologies, such as the Internet of Things (IoT) and cloud computing, and also to perform

---

[26] Assimilated Regulation 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems Parts 1-6, 16, and 17 of the Annex (UK Regulation 2019/945).
[27] UK CAA, *CAP 722: Unmanned Aircraft System Operations in UK Airspace – Guidance* (16 April 2024), 2.3.1 https://www.caa.co.uk/our-work/publications/documents/content/cap-722/ (accessed 20 Oct 2025) (CAP 722).
[28] Paul G Fahlstrom, Thomas J Gleason & Mohammad H Sadraey, *Introduction to UAV systems* (John Wiley & Sons 2022) 10.
[29] Chris A. Wargo, Gary C. Church, Jason Glaneueski & Mark Strout, *Unmanned Aircraft Systems (UAS) research and future analysis,* IEEE Aerospace conference, 1, at 5 – 6 (2014).
[30] *Ibid*., at 28.

complex tasks by utilising scalable data storage.[31] This integrated approach also generates and uses big data, the complexity of which presents challenges for conventional processing methods.[32] Thus, it is inevitable that UAS will become an integral part of a more interconnected environment, reflecting the broader evolution of the aviation sector, driven by the delegation of core safety functions to the product itself.. This cyber-physical integration lays the technological foundation for the next stage of regulatory ambition, which is to enable routine operations of UAS in BVLOS and autonomous modes.

2.2 BVLOS operations, UAS autonomy and the control shift

The operational and economic benefits of UAS are critically dependent on moving beyond VLOS to routine BVLOS and eventually autonomous operations. The challenge for the regulator is managing the risk transfer that accompanies this operational shift. When the pilot is removed from the cockpit, or their sightline is disconnected from the aircraft, the burden of ensuring safety is transferred from the human's real-time judgment to the product's technical integrity.

The UK CAA manages this challenge through distinct classifications of automation and control.[33] Autonomous UAS systems, corresponding to the UK CAA's Level 4 (High Automation) and Level 5 (Full Automation), delegate control entirely to the system, which becomes responsible for the operations, monitoring, and safety of the flight.

Critically, autonomy must be distinguished from the broader concept of BVLOS which can accommodate both remotely piloted and autonomous flights. A remote pilot operating a UAS from a control centre (BVLOS) may still be fully in charge (non-autonomous), or the system may be managing the flight with the pilot supervising (semi-autonomous, Levels 2 or 3).

However, even in semi-autonomous operations designed to keep the human "in the loop", the regulatory framework prioritises product safety for BVLOS flights. The UK CAA's strategy links any permission for complex BVLOS flights to the system's demonstrated ability to manage critical risk independently.[34] The regulator requires assurances that, should connectivity be lost (Loss of Control or C2 Link Loss), the UAS itself can execute a safe, emergency procedure to avoid collision, set a new flight path, or land safely.

This core safety principle is formally codified in the CAA's strategic roadmap, CAP 3038: Delivering Scalable UAS BVLOS in the Specific Category,[35] which outlines the gradual pathway to integrate routine BVLOS operations into UK airspace, relying on the following two developments:

---

[31] Ibrahim Abaker Targio Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, & Samee Ullah Khan, *The rise of "big data" on cloud computing: Review and open research issues* 47 Information systems 98ff (2015).

[32] Robbi Rahim, Rizwan Patan, R. Manikandan, & S. Rakesh Kumar, *Introduction to blockchain and big data* 1in Neeraj Kumar, N. Gayathri, Md. Arafatur Rahman, & B. Balamurugan Blockchain, *Big Data and Machine Learning* (CRC Press 2020) 1.

[33] For the classifications, see CAP 722, *supra* n. 27, at Chapter 4.5, and for a more detailed analysis of them see Leloudas Insurability, *supra* n 17, at 285ff.

[34] *Ibid.*

[35] UK CAA,*CAP3038: Delivering Scalable UAS BVLOS in the Specific Category - The UK CAA Technical Strategy Delivery Model* (24 September 2024) https://www.caa.co.uk/our-work/publications/documents/content/cap3038/ (accessed 20 Oct 2025).

a) The establishment of "Atypical Air Environments" (AAE) by utilising segregated or semi-segregated airspace where other traffic is absent, often due to physical obstacles or proximity to ground infrastructure. With this development, volumes of airspace where the mid-air collision risk with crewed aviation is inherently minimised become available.
b) For integration into standard airspace, the CAA requires Transponder Mandatory Zones (TMZ) to create a "known traffic environment" within which "within which an accurate position and intentions of all aircraft is established and shared by an ANSP to all integrated users".[36] This environment requires the UAS to possess a technical capability—a combination of Electronic Conspicuity (EC) and Detect and Avoid (DAA) systems—to ensure that collision avoidance is handled by the product, thereby substituting for the pilot's traditional visual separation role.

In all these scenarios, the regulatory transition from VLOS to BVLOS—whether autonomous or supervised—solidifies the shift of the primary safety burden onto the integrity of the UAS product. The core question becomes "why did the product (the DAA system, the flight algorithm, the software) fail to protect the public as it was designed and certified to do?". This transfers the primary safety burden—and thus the liability—onto the integrity of the UAS product itself. This inevitable reliance on self-learning and complex non-deterministic algorithms, particularly AI, forms the most profound challenge to product liability law.

2.3 Artificial Intelligence and autonomous operations

The UK CAA has recently noted that autonomous UAS need to be able to "follow the planned route, communicate with Aircraft Controllers and other airspace users, detect, diagnose and recover from faults and operate at least as safely as a system with continuous human involvement".[37] Achieving this requires AI tools for situational awareness (SA), such as deep neural networks or machine learning models, as they enable UAS to recognise potentially hazardous situations.[38]

It is important to note at this stage that AI and autonomy are not synonyms. Autonomy refers to the ability of the system to fulfil goals independently, while AI refers to the ability of the software to perceive, learn, and make decisions. While a UAS may use pre-programmed algorithms to perform certain functions without operational independence, achieving Levels 4 and 5 of autonomy is critically dependent on the said advanced AI tools for functions such as situational awareness, detection, and real-time fault diagnosis.

Implementing AI-driven systems requires aligning product safety requirements with the characteristics of self-learning. This context primarily emphasises non-deterministic algorithms, denoting the potential for various unknown states of execution.[39] This uncertainty arises because the system, even when given the same set of instructions, may produce different outcomes or make decisions that were not encountered during its testing. This non-

[36] *Ibid.*
[37] CAP 722, *supra* n. 27, at 4.5.1.
[38] Arslan Munir, Alexander Aved & Erik Blasch, *Situational Awareness: Techniques, Challenges, and Prospects* 3 AI 55, at 66-67 (2022).
[39] Jacques Cohen, *Non-Deterministic Algorithms* (11) ACM Comput Surv 79 (1979) and C. W. Johnson, *The Increasing Risks of Risk Assessment : On the Rise of Artificial Intelligence and Non-Determinism in Safety-Critical Systems* presented in the 26th Safety-Critical Systems Club Symposium, (Vol. 15) Safety-Critical Systems Club York, at 8, (2017).

deterministic trait conflicts with the fundamental safety principles of aviation which require that systems are predictable and verifiable to achieve airworthiness certification.

In any case, the transfer of safety authority from the human pilot to the autonomous system means that accidents resulting from DAA failures, C2 link loss, or flawed self-learning algorithms are automatically channelled into product defect claims. When the system is operating at UK CAA Levels 4 or 5, the legal inquiry ceases to be what the human did wrong and becomes why the product failed to perform the task it was designed and certified to execute.

3. QUANTIFYING PRODUCT FAILURE AND THE ROLE OF SECTION 76 OF THE CIVIL AVIATION ACT 1982

The shift described in Chapter 2—where control is transferred from the human pilot to the autonomous system—converts accidents from primarily operational failures into product defects, necessitating an examination of the compensation mechanisms available to victims, particularly those based on strict liability. This chapter first reviews the statistical evidence underscoring the dominance of technical failure as a cause of UAS incidents, before analysing the first of the two co-existing strict liability regimes, namely the operator-focused s. 76(2) – (4) CAA 1982.

In 2021, statistics from the UK Aircraft Accident Investigation Branch (AAIB) revealed that UAS incidents accounted for over a quarter of notifications, namely 191 out of 746,[40] and in 2022, the UK AAIB reported 138 UAS-related incidents.[41] While AAIB figures are lower in 2024, with 54 incidents,[42] police records show higher figures, with over 6,000 incidents involving UAS reported in 2023, around 11% of which involve criminal offences.[43] This discrepancy is flagged by insurers, that note a tendency for UAS-related incidents to be underreported.[44]

One suggestion is that this underreporting might stem from the reporting requirements of the relevant regulations. The UK AAIB-led accident investigations require the reporting of UAS incidents[45] that result in a fatal or serious injury to a person and in major structural damage.[46] They also cover incidents which indicate a high probability of an accident ("serious incident", such as a near-collision).[47] Yet, assimilated Regulation 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation, which requires the UK CAA, among other things,

---

[40] UK AAIB, *Annual Safety Review 2021* (April 2021) 28 https://assets.publishing.service.gov.uk/media/62a1c1b1e90e070396c9f75d/Annual_Safety_Review_2021.pdf (accessed 20 Oct 2025) (UK AAIB 2021).
[41] UK AAIB, *Annual Safety Review 2022* (April 2022) 22 https://assets.publishing.service.gov.uk/media/64492a1ef12683000cca68b6/AAIB_Annual_Safety_Review_2022.pdf (accessed 20 Oct 2025) (UK AAIB 2022).
[42] UK AAIB, *Annual Safety Review 2024* (June 2025), 10 https://assets.publishing.service.gov.uk/media/68629e291c735341c2111b0c/AAIB_Annual_Safety_Review_2024.pdf (accessed 20 Oct 2025) (UK AAIB 2024).
[43] *See,* ProtectUK, *Threat from Drones in the UK* https://www.protectuk.police.uk/threat-risk/threat-analysis/threat-drones-uk (accessed 20 Oct 2025).
[44] See, Leloudas Insurability, *supra* n 17, at 280 referring to M Thompson , A Tarr , J Tarr and S Ritterband, *Unmanned Aerial Vehicles Liability and Insurance* in D Wilkinson , A Tarr , J Tarr and M Thompson (eds), *The Global Insurance Market and Change* (Taylor & Francis 2023) 213, at 217.
[45] Under assimilated Regulation 996/2010 on the investigation and prevention of accidents and incidents in civil aviation.
[46] Article 2(1).
[47] Article 2(16).

to proactively collect and analyse safety information, and is triggered by the broader threshold of "any safety-related event which endangers or which, if not corrected or addressed, could endanger an aircraft, its occupants or any other"[48] exempts UAS for which a certificate or declaration is not required pursuant to Article 56(1) and (5) of assimilated Regulation 2018/1139 on common rules in the field of civil aviation from the requirement to report occurrences to the UK CAA-led mandatory occurrence reporting scheme (MOR),[49] unless the incident results in a fatal/serious injury or involves a manned aircraft. This exemption means that non-injurious failures of such UAS do not have to be reported to the UK CAA, potentially fuelling the said underreporting.

While there has been no fatal injury reported in the UK so far, the potential for catastrophic injury by UAS, particularly in workplace environments or urban centres, is confirmed by risk modelling. As estimated by the UK AAIB, a UAS of "1.4 kg falling from 8 m could cause a fatal injury".[50] Furthermore, models show that a blunt object with a mass of 4.97 kg falling from a height of more than about 3 m could result in a fatal injury, even to someone wearing a hard hat, underscoring the risk of UAS operations in workplaces.[51] The risk is amplified if one considers the potential for mid-air collisions, landings into motorway traffic, or falling pieces causing property damage and injury to third parties.[52] Moreover, their potential to operate close to nuclear plants, ports, and other critical infrastructure, increases their catastrophic potential, particularly if used by terrorists keen to bypass geofencing restrictions and no-fly zones.[53]

The evidence from the UK AAIB suggests that product-related failures are the primary cause of incidents, which highlights the importance of focusing on product liability regimes. According to the 2024 UK AAIB Annual Safety Review, Loss of Control in Flight (LOC-I) remains the largest category, accounting for 24 events (44.4%) of UAS incidents.[54] We recognise that LOC-I is a broad category that includes both technical faults and operational errors. However, other causes are clearly product-driven: System or Component Failures (SCF-PP/NP) caused 14 events (25.9%), and Loss of Data Link (U-LINK) caused 12 events (22.2%).[55]

When SCF and U-LINK failures are combined, they make up 48.1% of UAS incidents in 2024, slightly surpassing the total for LOC-I failures. Additionally, the high number of incidents caused by losing the data link between the remote pilot and the unmanned aircraft (UA) is particularly worrying, especially in urban UAS and VTOL operations, particularly "if similar communication technologies are to be used with larger UAS"[56] as such failures are likely to

[48] Article 2(7).
[49] Article 3(2).
[50] UK AAIB 2021, *supra* n. 40, at 8.
[51] *Ibid.*
[52] *See* Julie-Anne Tarr, Nick Sharpe and Patrick Slomski, *Technology challenges inherent in safety regulation*, Drone Law and Policy (Routledge 2021) 376.
[53] Leloudas Insurability, *supra* n. 17, at 292. See, also, Benjamyn Scott, *The First UK Conviction for the Illegal Use of an Unmanned Aircraft and how it Can Help Improve Regulations within the EU* (2015) 14 The Aviation & Space Journal 11 for an analysis of the first UK conviction in the case of *CAA v Robert Knowles* for breaching restricted airspace around critical infrastructure (UAS flown over a nuclear installation),
[54] UK AAIB 2024, *supra* n. 42, at 11.
[55] *Ibid.*
[56] *Ibid*.

cause lethal injuries based on the risk modelling referred to earlier. As a result, claims against producers may become more common than they are today.

Third parties injured by a UAS that has experienced a technical failure have two potential recourse avenues, both of which are based on strict liability. They have a claim against the UAS producer (and/or component part producer) under the CPA 1987 for product defect and because the CPA 1987 route is non-exclusive,[57] a separate claim against the UAS owner under s 76(2) – (4) CAA 1982 for ground damage.

While third-party victims might pursue claims under common law negligence or contract law,[58] the CPA 1987 offers the most effective recourse. The Act eliminates the claimant's need to prove fault—a requirement that is often impossible to meet against opaque AI systems—and, crucially, targets compensation for consumer-based losses, which define the majority of UAS victims in public spaces. Furthermore, the CPA 1987 fills (or at least should fill) gaps in the UAS insurance coverage, particularly given the novelty and uncertain risk profile of autonomous features.[59]

The UK's s 76(2) – (4) CAA 1982, establishes a system of strict and unlimited liability for third-party damage caused by aircraft (including UAS) and was designed to provide a straightforward, "no-frills" recovery regime for third parties, bypassing the need to prove fault.[60] The owner of the UAS is held liable solely upon proof that damage was caused by the aircraft or an object falling from it (e.g., a falling camera, sensor, or propeller). The Act offers virtually no special defences to the owner/operator, even in cases of terrorism, hijacking, or cyber interference. The only defence is the victim's contributory negligence, making the liability almost absolute. Victims can recover for "material loss or damage", which explicitly includes stand-alone psychiatric injuries,[61] distinguishing it from more restrictive international conventions governing the liability of air carriers to passengers, such as the Montreal Convention 1999,[62] that limits recovery to bodily injury.

Liability attaches to the registered owner, which creates a discrepancy with the mandatory registration requirement that is imposed on the operator of the UAS, namely, the entity that manages the UAS and is responsible for its maintenance, operation, and ensuring that the remote pilot has the necessary permissions to fly it. While current "wet leases" (where the owner supplies the pilot) simplify the matter, the growing trend toward "dry leases" (where the owner supplies the UAS; the lessee supplies the pilot/operator) unfairly allocates liability risk to the owner, who lacks operational control. Section 76 (4) partly mitigates this unfairness by making the lessee liable for dry leases exceeding 14 days, yet the owner remains primarily liable for the first 14 days of any dry lease.[63]

---

[57] CPA 1987, s 2(6).
[58] *See*, Duncan Fairgrieve and Richard S Goldberg, *Product liability* (Oxford University Press 2020) 27ff and 535ff (Fairgrieve & Goldberg) and Reynold M. Sachs, *Negligence or Strict Product Liability: Is There Really a Difference in Law or Economics* 8 Ga. J. Int'l & Comp. L. 8 259, 278 (1978).
[59] For a detailed analysis of the insurance regime governing UAS operators and UAS operators' insurance policies, see Leloudas Insurability, *supra* n. 17, at 289ff.
[60] For a detailed analysis of the regime see Leloudas Insurability, *supra* n. 17, at 308ff.
[61] *Glen v Korean Airlines* [2003] EWHC 643 (QB).
[62] Convention for the Unification of Certain Rules Relating to International Carriage by Air, agreed at Montreal on 28 May 1999 (Montreal Convention 1999).
[63] This provision derives from the 1952 Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface, Signed at Rome, on 7 October 1952 (1952 Rome Convention).

While the simplicity of s.76(2) CAA 1982 offers victims a compelling and immediate path to recovery against the UAS owner/operator, and we acknowledge that a producer's deeper pockets are often a practical motivation for litigation against it, relying solely on the CAA 1982 regime undermines the current liability debate. The CAA 1982 was designed to manage operational failure, imposing liability regardless of the accident's cause, but it demands no legal scrutiny over the product itself. In a world of autonomous systems, this lack of scrutiny runs the risk of allowing the creator of the dominant risk (the producer of the defective product) to be potentially liable only under secondary, indemnity actions by the owner/operator or its insurers that are not subject to the strict product liability regime and are further hindered by contractual limitation of liability clauses and disclaimers of implied warranties (such as fitness for purpose etc), especially if the owner/operator is a commercial entity. This way the financial consequences of product failure are transferred to the owner/operator who often lacks control or knowledge of the technical defect. This inevitably tilts the scale in favour of producers as the owner/operator, that is strictly liable under the CAA 1982 did not create the risk of product failure, and yet becomes the only source of recovery. In contrast, the CPA 1987 is the only strict liability tool that should force scrutiny upon the design and software of the UAS itself. As the dominant source of accidents in the statistical analysis is product defect, the necessity of examining the suitability of the CPA 1987 is heightened.

Part 1 of the CPA 1987 implemented the EU Product Liability Directive 85/374 (PLD)[64] into UK law, and following Brexit, Part 1 of the CPA 1987 was retained (as assimilated law). Since then, the European Union, reflecting the challenges of new digital technologies, has enacted a new Product Liability Directive 2024/2853 (PLD 2024/2853),[65] that came into force on 9 December 2024, with EU States having until 9 December 2026 to transpose its provisions into their domestic legal system, at which point the new Directive will replace the original PLD and will apply to products placed on the market from 9 December 2026 onwards. The UK has not taken such a step and, as such, the following Chapter will critically evaluate whether the CPA 1987 is structurally capable of meeting this challenge, analysing its failures to define a digital product, establish liability for post-supply defects, and provide a workable burden of proof against opaque cyber-physical systems.

4. DIGITAL INCOMPATIBILITY OF PART I OF THE CPA 1987

4.1 Scope and applicability of Part I of the CPA 1987 in the context of cyber-physical systems

By implementing the provisions of the PLD in the UK, Part I of the CPA 1987 establishes a no-fault liability regime. The core function of the Act is to provide victims with strict liability recourse against producers of defective products for death, personal injury, or property damage caused by them in the UK. The basis for imposing strict liability was to eliminate divergences between EU member states, providing equal protection for consumers and a fair apportionment

[64] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7 August 1985, 29.
[65] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC OJ L, 2024/2853, 18 November 2024 (Directive 2024/2853). For the failed Proposal for a Directive of the European Parliament and the Council on adapting non-contractual civil liability rules to artificial intelligence, see below note 72.

of risk.[66] It was noted in *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland,*[67] that foreseeable risks should be borne by the producers based on their ability to know the technical aspects better than consumers, take precautions through their experiments and research or measures to protect themselves through insurance against any damage. Thus, victims were relieved from having to prove the producer's fault, based on the principle that producers were in an advantageous position in terms of technical knowledge.

Strict liability applies to "death or personal injury or any loss of or damage to any property (including land)".[68] Property damages cover properties that, at the time they are lost or damaged, are ordinarily intended for private use, occupation or consumption; and are intended by the person suffering the loss or damage mainly for their own private use, occupation or consumption, and do not cover the defective product itself.[69] Thus, UAS operators (in their private capacity) and third parties, such as innocent bystanders or owners of properties the UAS crashes into, can seek compensation for death or personal injury, as well as loss of or property damage used privately. Any damage to property used for business purposes and damages to or losses of the UAS itself cannot be recovered under the Act. Also, economic losses are not coverable unless they are incurred as a direct consequence of property damage.[70]

However, the Act was drafted when cyber-physical systems were beyond the consideration of regulators, and it is questionable whether it can address their characteristics. The main technological developments in the context of UAS that challenge the Act include:

a. Intangible items (e.g. software, data) which may be embedded in the hardware during manufacturing or supplied later by different service providers, via bespoke or mass-produced types. This may not be covered by the definition of "product" in the CPA 1987.

b. The producer's control, which remains ongoing after the deployment of the UAS through software updates and upgrades (which can be carried out by a different producer). Therefore, the ongoing control by the producer will serve as a decisive factor, especially in interpreting the notion of defect.

c. Autonomous algorithms improve through self-learning and decision-making, leading to uncertainty and opacity for stakeholders, including producers. As their experience increases with more frequent operations—such as when autonomous UASs are routinely used in non-segregated airspace—their decision-making capabilities will be enhanced, which may challenge the producers' control over safety.

d. Interconnectivity, as UAS are part of cyber-physical environments and interconnected with different sources and products via, among others, cloud technologies and IoT. This will prompt the need to redefine fundamental terms such as "product" and "defect".

---

[66] Opinion of the Economic and Social Committee on the n the Proposal for a Council Directive concerning liability for defective products [1979] OJ C114/15, 1.1.3 as cited in Fairgrieve & Goldberg, *supra* n 58, fns 101-103.
[67] Case C-300/95, *Commission of the European Communities v United Kingdom of Great Britain and Northern Ireland* [1997] ECR I-2649, ECLI:EU:C:1997:255 (*Commission v UK*).
[68] CPA 1987, s 5 (1).
[69] CPA 1987, s.5(2),(3).
[70] Fairgrieve & Goldberg, *supra* n 58, at 639.

Given that BVLOS and autonomous UAS technologies rely on complex systems and intangible elements, the scope and interpretation of the Act are challenged. By and large, liability under the Act is confined to defects existing at the time a product is "supplied by its producer to another",[71] preventing victims from invoking this strict liability regime for subsequent malfunctions, such as defects in updates, upgrades, cybersecurity vulnerabilities or self-learning errors. This framework also makes it harder to establish a "causal link" between the defect and the resulting damage, placing the burden of proof on the claimant and potentially denying victims compensation.

While the European Union has introduced the new PLD to address the characteristics of these products,[72] the UK did not follow suit: it was previously suggested that the current product safety framework remains reasonably comprehensive for liability issues not involving advanced AI; however, it was acknowledged that new and complex risks are presented by more advanced uses of AI in consumer products.[73] However, we support a different perspective, to which we now turn.[74] To assist our analysis, we have devised the following UAS-related scenarios:

1. The components for remote sensing attached to two UAS showed no defects initially; however, a collision occurred between them during a BVLOS operation due to:

   Scenario A: The producer of the UAS and a software developer under the control of the UAS producer introduced two new stabilisation software updates to one of the UAS to mitigate the effects of atmospheric turbulence better. Are these stand-alone software updates a "product" within the meaning of CPA 1987?

   Scenario B: The malfunction occurred due to data supplied by the commercial satellite service provider (or potentially through an IoT platform) to the second UAS, which caused a software upgrade to malfunction due to incompatibility with that data. Is data provided at a later stage considered as "product"?

2. Scenario C: An autonomous UAS that is deployed by a construction company to monitor its projects encounters a mapping issue. This arises from the incorrect guidance given by algorithms, which rely on information received from the onboard cameras of the UAS. Consequently, the vehicle crashes into a high-end yacht moored in the marina, resulting in a significant explosion, which leads to a claim by the yacht's owner. The inquiry reveals that the algorithm incorrectly determines its course during the data processing stage.

[71] CPA 1987, s 3(2)(c).

[72] The EU has also, unsuccessfully, introduced an AI liability directive in 2022 in the form of a Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final. The proposal was formally withdrawn in October 2025 (see Withdrawal of Commission Proposals OJ C, C/2025/5423, 6.10.2025) as several EU States believed that national laws could address this issue, and also, there was a perception among businesses that an additional layer of liability would hinder innovation and investment.

[73] Office for Products, Safety and Standards, *Study on the Impact of Artificial Intelligence on Product Safety*, (December 2021) 60.

[74] For an excellent assessment of the regulatory conflict between the EU's operation-centric UAS rules and its new technology-centric AI legal framework, see Benjamyn I. Scott, Bart Custers & Henning Lahmann, *Drone Regulation and AI Law: Assessing the Intersection of the EU Legal Frameworks for Unmanned Aircraft and Artificial Intelligence* 49 ASL 565 (2024).

4.2 The Notion of Product

Since UAS include specific intangible components integrated into their physical medium, such as software, or elements that are not present at the time of circulation, like data or open-source software added later, this raises the question of whether the definition of a product covers these elements. Section 1(2)(c) CPA 1987 defines product as "any goods or electricity and …includes a product which is comprised in another product, whether by virtue of being a component part or raw material or otherwise…".There is no doubt that a UAS embedding intangibles, such as software, falls within the scope of the definition. A study carried out for the European Commission also asserted that the PLD allows for a concept in which digital products integrated into a physical medium can be classified as a product within its meaning.[75]

However, it is not clear whether purely defective software is covered when the device itself is not defective (such as stabilisation software updates provided later in Scenario A) or when data is provided by an external source (commercial satellite services or IoT data in Scenario B).[76] In that respect, it is debatable whether other intangible components inherent in the operational functionality of UAS, such as non-embedded software, the source code of software, or data shared by service providers or through multiple IoT platforms, are covered. This issue holds particular significance when examining the liability associated with intangibles whose producers are different from those of the UAS.

English courts have not yet addressed whether intangibles, such as those in both scenarios, constitute a product under the CPA 1987. Nonetheless, there are a few cases arising from other legal instruments that can shed light on our discussion. In *St Albans City & District Council v International Computer Ltd*,[77] it was held that a computer disk qualifies as "goods" under the Sale of Goods Act 1979 and the Supply of Goods and Services Act 1982. In contrast, a computer programme, being downloadable information without physical transfer (i.e., standalone software or an application downloaded from the internet without being embedded in specific hardware), was not. Later on, in *Beta Computer (Europe) Ltd v Adobe Systems (Europe) Ltd*,[78] this view was criticised because, considering the features of complex products and "the true nature and effect of the contract", there is no difference when a computer program is used "as effectively as if the medium were a disk or CD or magnetic tape". This view gained support from the CJEU in the case of *Software Incubator Ltd v Computer Associates (UK) Ltd*,[79] which followed a preliminary ruling request from the UK Supreme Court. The discussion concerned whether a copy of computer software supplied electronically constitutes a sale of goods under the Commercial Agents (Council Directive) Regulations 1993/3053 (SI 1993/3053). It was held that "…the concept of sale of goods referred to in Article 1(2) of Directive 86/653 must be interpreted as meaning that it can cover the supply, in return for

[75] Deloitte, *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability* (2018) 119 https://op.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en (accessed 20 Oct 2025).
[76] *Ibid*.
[77] [1996] 4 All ER 481, 493.
[78] 1996 SLT 604.
[79] Case C-410/19, *Software Incubator Ltd. v Computer Associates (UK) Ltd* ECLI:EU:C:2021:742 (16 September 2021).

payment of a fee, of computer software to a customer by electronic means where that supply is accompanied by the grant of a perpetual licence to use that software."[80]

Some academics support the idea that mass-produced software should be considered a product because it resembles physically marketed items, rather than being purely informational or a service.[81] This approach aligns with the aim of strict product liability to protect the public from defects in mass-produced items and distinguishes between products and services, which fall outside the scope of the CPA 1987. For example, in *The Salvage Association v CAP Financial Services Ltd*,[82] the court distinguished bespoke software (explicitly encoded for a client) as a supply of services. Bespoke software does not fit the strict liability rationale because the supplier typically is not in a clearly superior position to manage risks compared to the user, thus it shouldn't be subject to the strict liability regime. However, some have argued that including electricity in the definition is a deliberate choice of the drafters against recognising other intangible items.[83] One could also argue that the Medical Devices Directive, which explicitly lists software among the devices within its scope, provides a clear example of this approach.[84]

The expert groups of the European Commission, when discussing new technologies and liability, argued that the supply of intangibles, or the communication and interconnection of digital products, can be considered as "necessary" for complex products.[85] They adopted this approach of "necessity" to distinguish between a product and a service, similar to the method used in the construction of the United Nations Convention on Contracts for the International Sale of Goods (CISG).[86] Taking the same approach, if an intangible item is deemed necessary for the product it is incorporated into, it can also be considered a product. Nonetheless, the increasing volume of intangible assets, such as big data provided through IoT or cloud computing, makes the definition of what is "necessary" open to debate, as data can sometimes be crucial to a product's function and at other times merely enhances performance.

While this debate is ongoing in the context of the CPA 1987, the European Union has chosen to explicitly broaden the scope of its new product liability scheme. The new PLD defines product as "all movables, even if integrated into, or interconnected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials and

---

[80] *Ibid*., para 51.
[81] Felix Collin, *Maritime Product Liability at the Dawn of Unmanned Ships – the Finnish Perspective (2018) University of Turku , Faculty of Law Research Paper Series 2 / 2018*, 4-5. https://www.utu.fi/sites/default/files/public:/media/file/RPR_2_2018.pdf (accessed 20 Oct 2025) and Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?* 67 Md. L. Rev. 425, 273 (2008).
[82] [1995] FSR 654.
[83] See, for example, Karin Albeit, *The applicability of the EU product liability directive to software* 34 CILSA 188, 200 (2001).
[84] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices OJ L 169, 12 July 1993, 1 (as amended), Art 1(2).
[85] European Commission, *Liability for Artificial Intelligence and other emerging digital technologies: Report from the Expert Group on Liability and New Technologies – New Technologies Formation*. (2019) 33 https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf (accessed 20 Oct 2025)
[86] United Nations Convention on Contracts for the International Sale of Goods 1489 U.N.T.S. 3, *see*, also UNCITRAL Secretariat, *Explanatory Note on the United Nations Convention on Contracts for the International Sale of Goods* (A/CN.9/SER.D/1).

software".[87] This includes standalone software, irrespective of whether it is stored on a device, retrieved through a communication network, or accessed via cloud computing.[88] Thus, software updates are products, and their developers are the manufacturer of the new PLD.[89] Thus, the modifications to UAS, such as the software updates referenced in Scenario A, are products, and their developers are manufacturers.

Data is considered as a product insofar as it constitutes a "digital manufacturing file", defined as "digital version of, or digital template for, a movable which contains the functional information necessary to produce a tangible item by enabling the automated control of machinery or tools".[90] However, pure information, i.e., media files or non-commercial tools, such as the source code of software, free and accessible open-source software circulated outside the course of a commercial activity, is not considered a product.[91] In addition, "related services", being defined as "a digital service that is integrated into, or inter-connected with, a product in such a way that its absence would prevent the product from performing one or more of its functions", are also included.[92] Thus, data provided by a satellite service provider or through an IoT platform, if necessary for a UAS to perform its task, as in our Scenario B, is regarded as a product. In cases where the provider of the data differs from the manufacturer of the UAS, whether it is "within the control of the manufacturer" becomes relevant for holding the first producer liable, as discussed in the next section.

This approach is more fitting, given that cyber-physical systems, such as UAS, rely on continuous digital involvement through software updates and communication links to maintain functionality.

4.3 The Notion of Defect

The strict liability regime places significant emphasis on the concept of "defect" which is defined in the CPA 1987 as the safety of a product"…not such as persons generally are entitled to expect; and for those purposes "safety", in relation to a product, shall include safety with respect to products comprised in that product and safety in the context of risks of damage to property, as well as in the context of risks of death or personal injury". [93]

This definition of safety leaves a lot to be desired, as the determination of safety levels hinges on the interpretation of reasonable expectations, and establishing a product's inferior quality does not indicate it is defective unless it genuinely poses a risk of damage or injury.[94] The

[87] Directive 2024/2853, *supra* n 65, Art. 4(1).
[88] *Ibid*., recitals nos 13 and 14.
[89] *Ibid*. The original PLD and the CPA 1987 use the term "producer" encompassing the actual manufacturer, component part suppliers, and importers (PLD, art. 3). The new PLD uses the term "manufacturer" instead (art. 4(5)) to achieve consistency with the EU product safety framework; however, the scope of liability remains similarly broad, covering any party that places or substantially modifies the product for commercial purposes. This article uses "manufacturer" when referring to the new PLD to maintain consistency with the updated legal text.
[90] *Ibid*., Art. 4(2).
[91] I*bid*., recitals nos 13 and 14.
[92] *Ibid*., Art. 4(3).
[93] CPA 1987, s. 3.
[94] Department of Trade and Industry, *Implementation of the EC Directive on product liability: An explanatory and consultative note* (1985), para 55.

phrase "persons generally are entitled to expect'' was said to be a reference to the intention to consider general expectations rather than general persons.[95]

Section 3(2) CPA 1987 provides a list of circumstances that must be considered when determining the "entitled expectations" of persons generally. While the Act provides that "all circumstances" shall be considered, certain factors are explicitly enumerated, including "marketing, presentation, instructions, and warnings", "reasonably expected use", and "time of supply of the product by the producer to another".[96] However, these are non-exhaustive. Other circumstances include the presence of apparent or hidden dangers; whether the product complies with relevant safety regulations and similar standards; the balance between the product's risks and benefits, as well as the costs and feasibility of implementing safer measures design.[97] The last two tests are the most frequently discussed ones; therefore, we will focus on them in Chapter 4.4.

Defects are typically categorised as design defects, manufacturing defects, and warning defects. A design defect occurs when a product is manufactured with a fundamental design deficiency that renders it unsafe for its intended or contemplated purpose.[98] Even if a product adheres to the criteria for a safe design, manufacturing processes may still result in the production of defective items. In manufacturing defects, not all items deviate from the design specifications; instead, certain copies fail to meet these requirements, resulting in unsafe products.[99] In warning defects, a defect arises when users are not adequately informed about the potential risks that should be disclosed, thereby preventing consumers from making informed decisions.[100] Manufacturing and warning defects are relatively easier to identify, as the former can be checked by comparing the product to other safely manufactured copies, and the latter can be determined by checking if the potential risks were previously recognised and consumers are informed. Considering the nature of autonomous UAS that self-learn, act, and may deviate from their intended purposes by design (see Scenario C), design defects will be the focus of our scrutiny.

4.4 Design defects: the AI challenge

The definition of "defect" in the CPA 1987 is reminiscent of the US consumer expectation test, which examines whether the product is "dangerous to an extent beyond that which would be contemplated by the ordinary consumer who purchases it, with the ordinary knowledge common to the community as to its characteristics".[101] Due to the broad wording of the definition, the test is applied in diverse ways. In the *Boston Scientific* case, the Court of Justice of the European Union (CJEU) interpreted it as "specific requirements of the group of the users for whom the product is intended".[102] According to this ruling, a product is not safe when "an abnormal potential for damage'' exists.[103] Nonetheless, in *Colin Gee v Depuy International*

[95] Fairgrieve & Goldberg, *supra* n 58, 362.
[96] CPA 1987, s.3(2).
[97] Fairgrieve & Goldberg, *supra* n 58, 358-359.
[98] I*bid*., at 384.
[99] *Ibid.*
[100] *Ibid.*
[101] Restatement (Second) of Torts § 402A cmt. I (Am Law Inst 1965).
[102] Joined Cases C-502/13 and C-504/13, *Boston Scientific Medizintechnik GmbD v AOK Sachsen-Anhalt-Die Gesundheitskasse and Betriebskrankenkasse RWE* para 38 ECLI:EU:C:2015:148 (5 March 2015).
[103] *Ibid*., paras 40 and 54.

Limited,[104] an English court addressed whether a product's inherent design risks—such as its intrinsic tendency to cause adverse effects—could automatically be designated as a defect. The court decisively held that the consumer expectations test requires an assessment of what the public is entitled to expect, rather than simply labelling all customary or irreducible risks of a product's intended function as a defect.

The risk-utility test—which later became the predominant standard in most U.S. jurisdictions, particularly for design defects—requires balancing a product's risks against its utility, feasibility, and cost.[105] A product is deemed defective when the court determines that a reasonable alternative design was available, meaning the foreseeable reduction in harm that would have been achieved by implementing the alternative design outweighed the increased cost and reduced utility of that alternative.

If we apply the consumer expectation test to our Scenario C, we need to determine whether the UAS fails to meet the safety expectations of the general public and surrounding property owners, rather than focus on the commercial user. Despite the UAS's exclusive use for construction monitoring, the inherent tendency of flying objects, especially UAS, to diverge from their intended operating areas means the risk of damage remains a critical concern.

Applying the risk-utility test, the main question becomes whether a reasonable alternative design – especially a design that will provide greater situational awareness via AI, would have been justified. Of greater significance is the benchmark for the alternative design. As noted by Borghetti, comparing an algorithm against the actions of a human is flawed, primarily because algorithms must promise a better standard of safety than the human actions they replace, and because many autonomous tasks are fundamentally beyond human capabilities. The comparison should be against the potential outcomes of a different algorithm.[106]

However, this comparison is flawed because of the nature of non-deterministic algorithms, which may yield different outputs even with the same data. As such, it is doubtful whether experts can reliably determine defectiveness as the assessment of fault becomes subjective. The inquiry thus shifts from a technical fault-finding exercise to a fundamental policy decision regarding who should ultimately bear the liability for AI-driven harms.[107] As producers retain significant influence over the system's design, self-learning, and continuous operation, a degree of control far greater than with conventional products, it is only fair for liability to be re-anchored to the producer's superior capacity to control risk. Additionally, with an effective liability framework in place, the manufacturer is both positioned and motivated to adjust the pricing of an AI system in line with how intensively it is used.[108]

In order to assess the producer's efforts to mitigate risks requires showing control over factors, such as sensors and data, and potentially imposing a duty to prove safety assurance. But still, can a producer demonstrate reasonable assurance over non-deterministic, self-learning algorithms? While efforts to improve AI assurance are ongoing, the current answer is generally

[104] [2018] EWHC 1208 (QB).
[105] DG Owen, *Products Liability Law* (3rd edn, West Academic Publishing 2015), 300.
[106] Jean-Sébastien Borghetti, *Civil liability for artificial intelligence: What should its basis be?* (2019) La Revue des Juristes de Sciences Po 94.
[107] *Ibid.*
[108] Gerhard Wagner, *Liability Rules for the Digital Age - Aiming for the Brussels Effect* 13 JETL 191 (2022).

negative. This answer may, however, change as future safety standards and testing protocols for autonomous UAS evolve.

4.5 The timing of the defect

One of the defences provided for the producer is that "the defect did not exist in the product at the relevant time".[109] The relevant time in s 4(1)(b) of the CPA 1987 is defined as the time of supply,[110] whereas the PLD in Article 7(a) uses a different wording which refers to put into circulation.[111] Thus, the producer is not obligated to bear a monitoring duty over its product.

Since the producers' liability is limited to defects present before the product's supply, any defect that occurs after supply—such as those in upgrades, intangible components related to the product, elements accessible via cloud computing, or issues caused by the product's self-learning and decision-making—falls outside the scope of the CPA's strict liability.

4.6 The new PLD 2024/2853 solution

The new PLD retains the concept of "the safety that a person is entitled to expect".[112] The term is to be determined by reference to "…inter alia, the intended purpose, reasonably foreseeable use, presentation, objective characteristics and properties of the product in question, including its expected lifespan, as well as the specific requirements of the group of users for whom the product is intended".[113] However, it resolves this ambiguity by extending the definition of "defect" to cover software and data integrity vulnerabilities, as well as the safety implications of a product's self-learning capabilities and post-placement-in-the-market modifications.

The new PLD's expanded criteria for assessing defectiveness related to UAS now explicitly include:

a. "the specific needs of the group of users for whose use the product is intended"(the users of UAS, in our case);[114]

b. "the effect on the product of any ability to continue to learn or acquire new features after it is placed on the market or put into service" (Self-learning);[115]

c. "the reasonably foreseeable effect on the product of other products that can be expected to be used together with the product, including by means of inter-connection'' (Cloud Computing - IoT – Inter-connection);[116]

d. "the moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that moment, the moment

[109] CPA 1987, s 4(1)(d).
[110] If the person facing liability is not the original producer (such as an importer referred to in CPA 1987, s. 2(2)), the relevant time of supply is when the product was last supplied by any person to whom section 2(2) applies in relation to that product.
[111] For the discussion about the difference between "put into circulation" and "the time of supply", whether this was an inadvertent change as well as the difficulties arising out of this difference, see Fairgrieve & Goldberg, *supra* n 58, 8.53- 8. 64.
[112] Directive 2024/2853, *supra* n 65, Art. 7(1)
[113] *Ibid*, recital no 30.
[114] *Ibid*, Art. 7(2)(h).
[115] *Ibid*., Art. 7(2)(c)
[116] *Ibid*., Art. 7(2)(d)

in time when the product left the control of the manufacturer'' (Manufacturer's control);[117]

e. "relevant product safety requirements, including safety-relevant cybersecurity requirements" (Safety requirements - Cybersecurity).[118]

First, the new PLD explicitly shifts the focus for determining a defect to the group of users for whom the product is intended, rather than relying on what persons generally are entitled to expect. Consequently, the safety standard for a specialised, commercial UAS used for infrastructure inspection will be higher and different from that of a consumer UAS, aligning the boundaries of a defect with the product's specific operational sector.

Second, the manufacturer's control emerges as the foundational criterion for liability. This control covers situations where the manufacturer "performs or, with regard to actions of a third party, authorises or consents to the integration, inter-connection or supply of a component, including software updates or upgrades or the modification of the product, including substantial modifications", or where the manufacturer has "the ability to supply software updates or upgrades, themselves or via a third party".[119] As such, the manufacturer's liability now extends to and follows their digital content throughout the product's life.

Third, digital services integrated into or interconnected with a product are now considered relevant to its safety. These services are included in the definition, thereby addressing the liability challenge posed by the reliance on IoT. Suppose a UAS depends on an interconnected cloud service or a required digital application to function safely (see Scenario B). In that case, a failure in that intangible service can now render the physical UAS defective and create strict liability for its manufacturer.

Moreover, manufacturers are still exempted from liability for a defect that did not exist when they put the product into circulation ("it is probable that the defectiveness that caused the damage did not exist at the time the product was placed on the market");[120] however, the Act explicitly creates a list of digital components (the derogation list) for which manufacturers lose this post-service defence, if the damage was caused by things they did or controlled later, such as a defective software, failing to provide a necessary safety update ("a lack of software updates and upgrades necessary to maintain safety"), a connected digital service ("related service") that failed, or a substantial modification of the product.[121]

Applying this approach to our Scenarios A and B, the producer would be liable for damage or loss resulting from defects in stabilisation software updates or reasonably foreseeable data produced or provided by them or by any other software producer through various means, including interconnected platforms, as long as they give authorisation or consent, along with the liability of those other software producers; and in Scenario C, for the self-learning mechanism.[122] Nonetheless, it is crucial to recognise that these subsequent adjustments or

[117] *Ibid*., Art. 7(2)(e).
[118] *Ibid*., Art. 7(2)(f)
[119] *Ibid*., Art 4(5).
[120] *Ibid*., Art 11(1)(c).
[121] *Ibid*., Art. 11(2).
[122] *Ibid*., Art. 11(1)(f) gives right to the manufacturer of a defective component to be exempted from liability in case where "the defectiveness of the product in which that component has been integrated is attributable to the

improvements do not, by themselves, establish that the previous version of the product was inherently defective.

The new PLD addresses any reluctance to provide updates by creating an obligation for continuous safety assurance, ensuring that the producer can be held liable even when a lack of necessary software updates or upgrades causes the damage. Specifically, the derogation list maintains producer liability even where the damage is caused by a lack of software updates or upgrades necessary to maintain safety. This requirement for ongoing monitoring and updating aims to ensure that public safety guides the maintenance of cyber-physical UAS, rather than the manufacturer's fear of litigation. Thus, manufacturers of UAS will need to ensure that their safety mechanisms can detect any potential defects arising from data, updates, or upgrades relevant to the product, regardless of the persons or entities providing such items.

The most significant challenge remains self-learning. While manufacturer control is the overall criterion, it is controversial to apply strict liability to self-learning algorithms, as their autonomous evolution is prone to exceeding the manufacturer's original design specifications. However, the derogation list does not exclude liability for defects caused by self-learning. This means that, if the manufacturer has proven that they provided all necessary software updates or upgrades required to maintain the system's safety, they might be able to rely on the defence that the underlying defect was created post-circulation by the algorithm's independent learning. Thus, the successful defence of the UAS manufacturer in Scenario C will depend on demonstrating continuous oversight of the algorithm and fulfilling its ongoing obligation to supply updates or upgrades necessary to maintain safety on board.

4.7 Causal link and burden of proof

The PLD still requires proof of defect, damage, and the establishment of a causal link between the defect of the UAS and the damage. The requirement to prove a defect has been criticised on the basis that such proof is often technically complex and expensive due to the need for expert opinions.[123] This challenge is amplified in the case of UAS, because the evidence often lies within the proprietary data and algorithms controlled by the producer. The CJEU attempted to address this issue by encouraging national courts to allow circumstantial evidence to prove a defect where scientific proof is impossible.[124]

In contrast to this limited judicial remedy, the new PLD introduces comprehensive legislative solutions designed to alleviate this burden. It is still a requirement to prove the defectiveness, the damage and the causal link between that defectiveness and that damage.[125] If the claimant presents sufficient facts and evidence "to support the plausibility of the claim for compensation", the defendant is then obligated to disclose the evidence in their possession.[126]

---

design of that product or to the instructions given by the manufacturer of that product to the manufacturer of that component".

[123] European Commission, *Green Paper on Liability for Defective Products* (28 July 1999) COM(1999) 396 final, 2.

[124] Case C-621/15 *NW and others v Sanofi Pasteur MSD SNC and others* ECLI:EU:C:2017:484 (21 July 2017), paras 19 and 24.

[125] Directive 2024/2853, *supra* no 65, Art.10(1).

[126] *Ibid*., Art.9(1).

If the defendant fails to disclose relevant evidence, the court should assume the existence of a defect.[127]

Moreover, the PLD introduces the following presumptions of defectiveness:[128]

a) when the product does not comply with mandatory product safety requirements.
b) when an obvious malfunction caused the damage during reasonably foreseeable use;
c) in a situation where the claimant encounters excessive difficulties due to the technical or scientific complexity of the case, with the defendant retaining the right to rebut the existence of such excessive difficulties.[129]

These provisions are significant when a defect results from the self-learning mechanism, as demonstrated in our Scenario C, as producers will now be required to rebut this presumption of defectiveness by showing they have made their best efforts to establish a safe infrastructure to support this mechanism.

4.8 Development risk defence

The CPA 1987 incorporates the "development risk" defence (s 4(1)(e)), which allows a producer to escape liability if the defect could not have been discovered at the time of supply, given the objective state of scientific and technical knowledge. This provision aims to encourage innovation, yet it is controversial, as it transfers the burden of scientifically unknowable risks onto the consumer —a policy choice influenced by industry concerns during the drafting of the original PLD.

The defence requires proof that no producer in the sector could have discovered the defect and as clarified by the CJEU in *Commission v UK*,[130] the test looks into the objective state of scientific and technical knowledge and its accessibility, not the producer's subjective awareness. This means producers are presumed to be informed by all relevant international research, regardless of language or publication venue, though the reliability of those sources can still be challenged. The objective knowledge standard and the burden of proving that a defect was "undiscoverable" provide the only protection against the producer's use of this defence.

Critically, this defence clashes with autonomous UAS and AI systems due to the nature of non-deterministic algorithms. Unlike traditional defects (which can be tested and predicted), a defect in a self-learning system might only appear after months of operational experience, resulting from interactions among the software, sensor data, and the real-world environment. But then a fundamental question arises: Can a producer successfully argue that a defect arising from emergent, non-deterministic learning was "undiscoverable" when the design choice was to create a system intended to generate unknowable outcomes? The ambiguity in applying the

[127] *Ibid*., Art10(2) (a).
[128] *Ibid*., Art.10 (2)(b),(c) and 10 (4).
[129] *Ibid*., Art.10(5).
[130] *See*, *supra* n. 67.

"objective knowledge" standard to inherently unpredictable AI behaviours poses a significant challenge, which provides producers with a high degree of protection.

Despite the significant overall strengthening of consumer protection under the new PLD, the development risk defence is specifically retained and exempt from liability (Article 11(1)(e)). We are now eager to see how the courts will interpret and apply this defence, particularly in light of the presumptions mentioned above and the producer's control over software, upgrades, and updates that are necessary to maintain safety.

5. CONCLUSION

Our central conclusion is that the shift of UAS from operational error to product defect requires statutory intervention, as the CPA Act 1987 cannot cope with cyber-physical systems, allowing producers to escape liability for failures in design, software, and non-deterministic processes. At the same time, the near-absolute scheme of the CAA 1982 shifts the risk of product failure to UAS operators. From the perspective of deploying UAS in the UK, we propose the following essential reforms to the CPA 1987 (these form the priorities of our reform-related analysis in Chapter 4 above):

A. Modernise the definition of "product" to include intangible elements

The UK must broaden the definition of "product" under s 1(2)(c) CPA 1987 to cover digital content, including standalone software (and the AI/algorithmic system), as well as any data supplied as part of a commercial activity, irrespective of the delivery method (physical medium, cloud service, or communication link).

B. Anchor liability to producer control

Defects in subsequent software updates or upgrades must be part of producer's liability, provided they retain control or consent to the modification. This change addresses the liability gap for post-circulation software enhancements that are essential for UAS safety. Furthermore, the current defence that a defect did not exist at the time of supply must be modified. For autonomous UAS, liability should extend beyond the point of initial circulation to the moment the product leaves the producer's control. This change would capture self-learning errors by linking liability to ongoing control; As such producers would be incentivised to monitor risks arising from self-learning or non-deterministic algorithms, ensuring safety expectations evolve with the product's operational experience.

Aligning with PLD 2024/2853, the revised Act must derogate from the development risk defence where the producer fails to supply necessary software updates or upgrades required to maintain the safety of the UAS.

C. Presumption of defectiveness and causal link

To make the strict liability regime effective against opaque AI systems, the burden of proof under the CPA 1987 should be eased for claimants in cases involving complex technical failures. Courts should be empowered to assume a defect and/or a causal link where:

a. a system (like DAA or C2 Link) suffers an apparent malfunction during reasonably foreseeable use, or where the claimant demonstrates excessive difficulties due to the technical complexity of the case; or

b. the producer is shown to have failed to comply with mandatory product safety requirements, (e.g. related to cybersecurity, DAA integrity, or airworthiness certification).

This change compels the producer, as the entity with proprietary access to the product's design, code, and flight logs, to actively rebut the presumption of defect—a necessary mechanism to achieve the public safety objectives of strict product liability in the age of autonomy.

The ambition of the UK to integrate routine BVLOS and autonomous UAS operations is commercially necessary, but it cannot proceed without an updated product liability framework. Section 76(2) – (4) serves only as a blunt instrument against the operator, failing to compel the necessary scrutiny of product design. At the same time, the CPA 1987 fails to capture the risk of cyber-physical products. Therefore, a new product liability framework is required to support the expansion of autonomous UAS.