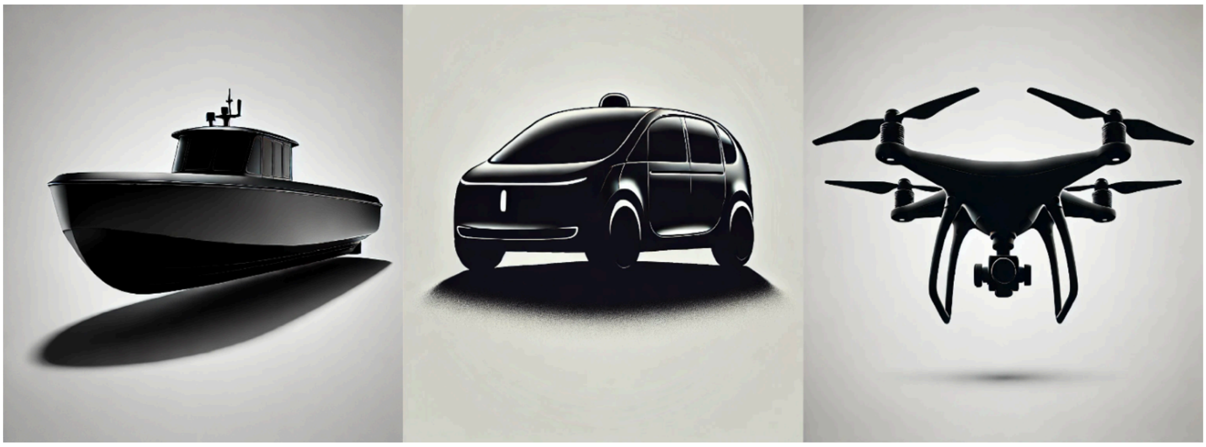

Drone Delivery Group

Protect Automated Transportation Systems

(or autonomy will be too exciting!)

Preface

This third white paper from the Drone Delivery Group (DDG), acknowledges the relentless march of increasing data-driven content in transport systems, which will be further fuelled by Artificial Intelligence (AI), and suggests a series of recommendations to policymakers to ensure that future transport systems are safe and secure.

Our first paper urged the UK Government to improve its processes to enable commercialisation through faster development of the safety clearances required to allow commercial operators to trial new ways of using drones[1]. Our second paper considered the current relationship between regulations and (safety and quality) standards. It examined how rapid dynamic safety developments/improvements could be differently facilitated, if regulations were underpinned by (easier to change) standards versus the challenges of regulatory change. It also defined the differences between technical and safety and quality standards[2].

Notably, the second paper outlined the utility of developing common digital accessibility standards for remote and autonomous vehicles across all domains (land, sea, air, and space). This is key, it argued, both in relation to safety and security, given that the future is anticipated to involve many more interactions across and between these advanced transport systems.

This 3rd paper accepts the relentless march of increasing data driven content in transport systems, which will be further fuelled by AI, and suggests a series of recommendations to policy makers to ensure that future transport systems are safe and secure.

Introduction

This paper departs from the DDG's previous two papers to focus on the assurance of data quality and security in advanced transportation systems. It acknowledges the growing influence of data-driven automation in transport systems and considers the need to evolve safety practices to cope with these transport 'systems of systems'[3]. Modern transport systems are controlled by external digital influences:

[1] https://www.dronedeliverygroup.org/images/DDG/PAPERS/WHITEPAPER-REPORT-1.pdf

[2] https://www.dronedeliverygroup.org/images/DDG/PAPERS/A_National_Strategy_for_Drones_Across_Land_Sea_and_Ai.pdf

[3] **System of systems** is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems. https://en.wikipedia.org/wiki/System_of_systems#:~:text=System%20of%20systems%20is%20a,sum%20of%20the%20constituent%20systems.

internal Internet of Things (IoT) data (often shared), diverse components (sometimes of unknown integrity), and electronic supply chains – all of which encompass distinct vulnerabilities which may result from poor system engineering or system issues, or perhaps as a result of malicious action by a 3rd party, or even both. The inevitable adoption of AI will be offered as a solution for the focused challenge but may bring unintended consequences to associated systems. This paper will examine data issues and their potential security impacts in relation to advanced transport systems (across all domains) and will provide a series of recommendations relevant to key stakeholders, including policymakers and industry. Our aim is to continue to ensure that 'all drones are safe to operate and operated safely[4]'. If we can develop class-leading digital control for our evolving transportation systems, while assuring their safety and resilience, we will have an ideal model for transport industry growth and a sustainable future.

This paper will first examine what we mean by the term 'drone', and then it will look at the current developments of transportation systems and how data is at the heart of these advanced and autonomous systems. It will break that data use down into component parts to show how many influences are needed both to enable these machines to work, and to make up the whole system of systems. All those elements are vulnerable to malpractice and therefore need protection to avoid serious crashes involving whole batches of transportation means. Finally, it will examine how we should protect all these systems, from the simplest to the most advanced and complex. The outcome will be a proposed policy statement which we suggest should be adopted by the UK Government to ensure that our advancing transportations systems evolve with increasing safety by ensuring a focus on data quality at their heart.

Alongside the proliferation in drone usage across domains (land, sea and air) and their increasing role as part of the IoT, there will be business pressures to produce the most commercially attractive solution at the right cost point. Accordingly, the potential use of unregulated/grey components, software and AI needs to be rigorously controlled as these will create major safety and security issues which, without appropriate regulation, will frustrate drone adoption and the UK's ability to capitalise on its market advantage. Assuring both data quality and security is vital to prevent chaos and to ensure our advanced

[4] Surely and simplistically the core mandate upon which all regulations and standards are based.

transportation systems build upon the safety and efficiency we have created through the evolution of combined experience.

Regulatory authorities have been improving vehicle safety operations across land, sea and air for decades and, in very simple terms, the regulations aim to ensure that vehicles are ‘safe to operate and operated safely’. We have lost many lives in the past that would not be lost today because of the lessons we have identified, learned and applied as regulations, most successfully when underpinned by safety and quality standards. As analogue systems with high manual content increasingly give way to digital – inevitably autonomous – control, vehicles become transport systems of systems. They are no longer isolated boxes, and a decreasing number of experts have access to, or understanding of, the technology inside. These advanced vehicles are highly automated and human actions, augmented by digital systems, are enhancing the experience of transportation. However, they remain associated with, and may usher in, distinct risks which need to be addressed as part of the system development and evolution, lest they require urgent confrontation.

This is an evolution in the way drones (land, sea and air) operate – it is not a revolution. Advanced vehicles are systems of systems[5] and the safety and integrity of these complete systems must be considered. Advanced and autonomous vehicles will use external data inputs for navigation and collision avoidance; they will produce and use IoT[6] data from electronic components analysed and used by manufacturers. It is expected that manufacturers will seek to introduce the latest technologies that they think will provide market advantages, such as 5G and 6G connectivity, the use of AI and Machine Learning (ML), and on-board entertainment systems. There is a high risk that components of unknown integrity will be used (perhaps even from a potentially hostile source) and will vary in source through

[5] **System of systems** is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems.

https://en.m.wikipedia.org/wiki/System_of_systems#:~:text=System%20of%20systems%20is%20a,sum%20of%20the%20constituent%20systems.

[6]The **Internet of things** (**IoT**) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

supply chains with vulnerability problems. They will have extensive electronic supply chains, organised to support both the performance and functionality of the vehicle and its lowest cost. All these data systems are vulnerable to malpractice, both malicious and unintended, and therefore there is a new safety problem that is growing at the same rate as the electronic assistance to transport systems builds. In trying to address these vulnerabilities, the US Government is calling for a shift from reaction to strategic preparation[7].

1. Modern Drones – Digital Systems of Systems

All drones have some form of digital control: as they move from Visual Line of Sight (VLOS) control to Beyond Visual Line of Sight (BVLOS) control, to fully autonomous systems – with or without AI/ML – the notion of them being just one element in a system of systems increases. Vulnerability to error – be that unintentional or malicious – increases rapidly with external influences from, for example, GNSS, 5/6G, radar and Lidar, as well as internal systems which generate and exchange IoT data with manufacturers and others, electronic supply chains, and rapidly developed components of unknown integrity.

2. Areas of Influence

[7] https://www.whitehouse.gov/oncd/briefing-room/2024/02/26/video-technical-report-launch/

https://www.gao.gov/assets/gao-25-107179.pdf

Figure 1.4 Areas of Influence

This section will consider the vulnerability extant in all four areas of influence that affect advanced and autonomous vehicle systems, namely: external influences, IoT data, component integrity, and electronic supply chain vulnerabilities. This vulnerability is often referred to as ‘cyber security’. However, billing this as a cyber security problem may cause many of us to push it in the direction of cyber security experts, which would be an error because the issue is not just data security; data quality will also affect the efficiency and safety of our systems, particularly when using AI techniques. Many of us sit at PCs manipulating data every day, yet most do not feel competent to deal with cyber security issues, simply because we automatically assume they need a software or hardware fix. However, most of these problems relate to procedural issues, often deep inside the supply chain and which can lay dormant for several years.

Far better to talk of **Data Security**: the practice of protecting digital information from unauthorised access, corruption or theft throughout its entire lifecycle. Better still: **Data Resilience** which relates to the ability of an organisation or its systems to continue business operations in case of unexpected disruptions that directly impact data availability. A few examples of such incidents include hardware or software failures, malicious data attacks, natural disasters and power outages. It is equally important that we assure **Data Quality** which aims to ensure the data we use is available and of at least a minimum quality to achieve the functions required. All can be affected by software or hardware, and any electronic and physical malpractice.

Malicious attacks on society typically create headlines showing ransom activities and can lead to the capture of credit card details from reputable retail stores' databases. A different level of crime would be achieved should a protagonist decide to deactivate a fleet of autonomous vessels dispatching pharmaceutical payloads to the Hebrides.

2a. External Influences

Advanced and autonomous transportation systems need external influences to facilitate navigation and to dynamically control their operations. These influences include GNSS, 5/6G GSM and sensor inputs such as optical systems, radar/LiDAR inputs. Maintaining the data quality from these inputs is vital, as is the data resilience of these systems. Internal systems are inherently accurate in the short term, but long-term accuracy will often involve the use of external influences. Rail transportation systems have a clear advantage in this area due to physical restrictions on movement and highly automated signalling systems.

We are all used to poor GSM signals and jamming GNSS signals is becoming commonplace in modern conflict situations. Indeed, jamming has been commonplace already for 3 years and not only in conflict situations. GPSJAM GPS/GNSS Interference Map shows how civilian airspace is also often jammed. Indeed, in 2024 in what is thought to be the first of its kind incident in Europe, Tartu (Estonia) airport had to be closed for a month due to jamming. Furthermore, we are very aware that the electromagnetic spectrum inputs can be affected by reflections and absorption changes related to material inconsistencies. Assuring the quality of data inputs is fundamental to safe advanced and autonomous transportation systems.

2b. The Internet of Things

Data-hungry advanced transportation systems also generate lots of their own data related to the state of their physical systems and that is useful to both operators and manufacturers. They also carry sensors which produce additional data, and all of this can be transmitted across networks. This is commonly referred to as data going into the Internet of Things, hence the term 'IoT data'. There is an argument that drones bring significant development into the IoT marketplace[8], maybe even creating a 'super IoT.' The general concept (originally) of an IoT device was instrumentation that could measure a particular function of a wider system of systems, for example smart measurement of the heat from the gas exhaust of a commercial airliner engine. Such 'instruments' would be connected to a network, and processors would determine such data into intelligence, for operators (or AI systems) to make informed decisions.

The growth of new platform models, predominantly in defence programmes, emerged to meet the dynamics of government expenditure challenges, transposing from asset purchase to an operational cost. Furthermore, an assurance to Original Equipment Manufacturers (OEMs) of decades of business to recover R&D effort, often created political and domestic industry demands. In this dynamic grew the uptake of existing industrial IoT devices and furthered the creation of such devices with far greater capability.

Originally, such IoT devices were highly bespoke, designed and made for a specific job, with the material of construction often being as equally as important as the purpose and function (for example due to its environment). It is important to note that given the nature of the commercial aviation industry, most assets turn round in approximately twenty-five-year cycles. However, more recent positive developments have improved robustness, they are not generally 'hackable' because they are well engineered to do exactly what they are supposed to do (and nothing else), they meet DO-178 and are often independently assessed/certified. They are subject to controlled access throughout the supply chain and consequently are difficult to attack.

As cycle times contract, often driven by the pace of conflict, so the propensity to use a succession of 'quick fixes' – building on sand – increases. Some cycle times for UA development in Ukraine are a matter of days or a few weeks.

[8] ISO/IEC 27001https://www.iso.org/standard/27001

2c. Component Integrity

The fast-moving pace of drone systems' electronic developments encourages innovation which, when coupled with the increasing utility of drones, ensures rapid developments that often race ahead of the ability of regulators and standards authorities to keep up with technological advancements. Flight, navigation and stability control systems are regularly updated with firmware, and components arrive via electronic supply systems with the latest models replacing legacy ones with no apparent need for independent testing. This may make the drones more vulnerable to malpractice, or failure, subsequently increasing the operating risk.

Commercial Uncrewed Aerial Vehicles (UAVs) from the likes of DJI[9], are also useful military tools and, just like civilian aircraft being converted to military use, the same is true in the UAV market, but at a much faster rate. Importantly, the same safety concerns of 'safe to operate; operated safely', apply to Uncrewed Ground Vehicles (UGV) and Uncrewed Surface Vessels (USVs). For all of these, (UAV, UGV and USV) the drone industry electronic control system development more resembles the rapid development in the smartphone/PC market in terms of speed of capability development and refresh rate, alongside relatively low entry costs (particularly when compared to normal defence rates and costs). However, purely commercial systems have a potentially 'softer' market in that users can (unknowingly) do some beta testing (notwithstanding the Samsung battery issue) and the potential of a new offering being immediately adopted into a mission critical system without further evaluation is unlikely. The same might not be true of UX related systems, particularly in wartime.

The consumerisation of electronic components creates a wide and highly commoditised supply chain. The cost of components and sourcing of such is far easier and cheaper than typical aerospace experiences. Components are produced rapidly with new and improved versions of these being continuously being developed and sourced through electronic supply chains. Although the competitiveness of commercial supply chains is high, the market is still attractive enough to invite 'grey' or counterfeit components. UAV development could take a matter of weeks or months, depending

[9] DJI, headquartered in Shenzhen, widely considered China's Silicon Valley

on the complexity and capability.[10] However, the nature of the operation remains close to all aircraft. The question is, are we assuring the integrity of those components which may come from less well known and undocumented sources?

2d. Digital Supply Chain

Having drawn on the commoditisation of a significant share of the parts, logically the supply chain opens a growing number of suppliers. The air drone battery market size was circa $5 billion in 2022, rising to $13 billion by 2031 with approximately 2.4 million units delivered in 2023. With 120 major battery suppliers, the supply chain resembles that of components to the original PC marketplace, an electronics industry – which in fact it is.

The wider and disparate supply chain is endemic to a newly emerging industry with many different suppliers and locations. From a resilience perspective and as in most industries, a product, service, or capability provider's supply chain, is only as strong as its weakest connected partner, as addressed in the Australian Government's Flight Critical' Paper[11]

3. Domain Developments Likely Over the Next 10 Years

In this section, we look at likely drone developments over the next 10 years and how that may affect the vulnerability of these data-hungry, advanced and autonomous land, sea and air transportation systems. **Fundamental to these developments is that evolution will always be a safer approach than revolution**.

[10] Implementing the UK's AI Regulatory Principles https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf

[11] https://cybersecuritycrc.org.au/sites/default/files/2024-05/Flight%20Critical.pdf

3a. Regulations: 'Safe to Operate/Operated Safely'

This backbone of regulations will hold good but, as **Safe to Operate** will rely more significantly on assurance of the autonomous systems/software, **Operated Safely** will place more of an overriding reliance on the same assurance of software/autonomous systems, and how any 'human in the loop' can influence the mission – is it remote or autonomous control? The logical safety steps are:

- Human at controls
- Remotely controlled by human
- Optionally direct or remote human control
- Autonomous system with no human control, direct or remote

However, context is king! Where and how we plan to operate could provide a step to development, demonstrating that progressive automation moving towards autonomy presents limited risk and should allow for special circumstances before applying production principles. The next 10 years of development will be constrained by our ability to regulate at a rate that will not stifle innovation. Pace should be proportionate but MUST maintain appropriate public safety, thereby minimising Risk to Life (RtL).

For efficiency, the key points of each domain are consolidated in a table and the full content are detailed in ....**See Annex A**.

3b. Domain Specific Developments

Each domain has developments which have been driven by the specific needs of land, sea and air transport challenges. Those developments are listed below:

Domain	Key points
Land Drone Development	

SMART technology	▪ Driver assistance technologies will become more widespread and expand and be normalised
Autonomous cars	▪ Self-driving vehicles could be on British roads by 2026 ▪ Many unknowns, too few standard processes and too few people capable of designing and developing products with the rigour needed to inspire confidence in the general public ▪ Many examples of driverless rail transport systems – the structure is more pliable to agreements on standards and rules etc. ▪ Autonomous trucks are likely to be on our roads before autonomous cars ▪ It is likely that this autonomy will be constrained to 'open roads' rather than areas of high traffic – possibly specifically designed – limiting factors will be risk and infrastructure availability
Maritime Drone Development	
Small automated boats	▪ Advancements in the smaller drone boat category have been rapid (Category is less than 7 m) ▪ Limited in platforms and purposes ▪ Shipping segment currently anticipating global rules to be established
Survey and research	▪ Autonomous surveying already exists for monitoring (e.g. environmental) ▪ Increased through development of sensor technology

	▪ Increased emergence of very specialist companies and SMEs
Private/semi commercial	● Current – typically remote-control units linked into the vessel management systems (VMS)
Defence/law enforcement	▪ Hulls and RIBS developed to prototype stage – (Royal Navy has over 200 examples but just a few on autonomous trials) ▪ Considerable activity to 'adapt' existing small boats (drones) during Ukraine conflict. ▪ The underwater battlespace is starting to see an increase in drone adoption, especially large unmanned underwater vessels ▪ Passive deployments have seen a visible increase in interest in surface and subsurface ▪ Autonomous tenders are seen as a large opportunity for manufacturers of pleasure craft
Large system ship development	▪ Further advancements in situational awareness technology ▪ Although the focus is fully autonomous capability it appears that some human intervention/interaction will be needed ▪ The fully autonomous vessel (i.e. uncrewed) is to be expected to emerge in the small ships category
Air Drone Development	
Air drones	▪ Many tasks currently undertaken by crewed aircraft could, in the near future, be carried out by UAV (See SQEP comment in Annex A)

	▪ The market was worth $36.7 billion in 2024 and is expected to grow to $93.1 billion by 2029 [12] ▪ Appears that software will be predominantly downloaded locally with keys allowing us to do so (similar to existing IT industry) ▪ Reduction of risk to aircrew grows the demand for autonomous capability (same holds for other domains) ▪ The air domain is where proliferation in military drones will bring early financial success and will help to develop the civilian use of drones in the commercial environment ▪ The Ukraine conflict has shown that stealth and stand-off range are the current best tactics to defeat air defence systems

4. Artificial Intelligence

AI does not refer to one technology but rather to a set of diverse approaches, datasets, methods, and technologies which, to different degrees and in different ways, show intelligent behaviour such as logical reasoning, problem solving, and learning in various contexts. [13] Currently, we would recommend that care is taken before any form of AI is incorporated into the designs of any transportation systems. It is critical that as we integrate AI systems, due diligence is achieved across all dimensions of

[121]3https://www.thebusinessresearchcompany.com/report/drones-global-market-report?utm_source=chatgpt.com

[13] Implementing the UK's AI Regulatory Principles https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf

AI trustworthiness from the inception to deployment and maintenance of the AI system, including (but not limited to): AI fairness, accountability, transparency, law and regulation, and safety. It is also important to consider at which stages in the AI system pipeline to have various humans-in-the-loop for regular assessment, evaluation and checks, alongside intervention if necessary. Furthermore, all AI systems must have an independently proven, non-AI safety monitor at the same level of integrity as the function being provided by the AI. This requirement has been in aerospace software standards since 1992, DO-178B/C section 2.4.3. The increasingly complex and scalable nature of advanced AI systems poses assurance challenges related to technologies and government. The Highly Automated Safety Centre of Excellence (HASCE) of the US Transportation Department has produced some useful definitions of the tools required for AI assurance in transportation systems ……

……………………………………………………………………………………………………**See Annex A:**

5. Data Quality

Governments, organisations and individuals are increasingly acting and relying on data sourced from, delivered through, or processed by a multiplicity of emerging technologies and established techniques. Understanding these technologies, trusting the data they generate and providing the confidence needed to act on the information they provide will be vital for the future societal and economic wellbeing of the UK in an increasingly digitised world.

Any time people make decisions based on data it is essential that they understand how suitable that data is for making that decision. 'Garbage in/garbage out' is a cliché, but one that exists for a reason. Understanding 'data quality' is therefore critical to digitalisation and there must be agreement of what this means. The following principles state that data quality is:

- the degree to which data is **fit for its intended purpose**
- measured and tracked through **data quality dimensions**
- a prerequisite for use of data in **decision making**
- intrinsically connected with **data trustworthiness**

Data quality can be conceptualised as the aggregation of various data quality dimensions that can be measured quantitatively with respect to data objects and the processes which generate them. To realise data quality requires the application of the following:

- Data quality frameworks to provide a structure which enables end users to be confident and to be able to quantify their confidence; that their data, software and algorithms are appropriate for the decision they are making. The primary benefit of implementing a Data Quality framework is that these quality measures enhance and validate the trustworthiness of data objects, thereby allowing them to be used with confidence in decision making.
- Technologies to ensure traceability by propagating contextual information with data to give confidence in its end use.
- Developing modelling and uncertainty quantification tools for new measurement challenges to deliver measurement results to end users in a way that improves decision making.
- Data Quality assessment, allowing organisations to understand and quantify the risks associated with data in their system. The system can be designed to manage or mitigate issues in the event of poor data quality.

6. Mitigation of Vulnerabilities

Having explained how these drone systems of systems use and generate data and having reviewed the likely developments in drone technology over the next 10 years, this paper will now examine how to mitigate the vulnerabilities that are associated with these enhanced digital technologies.

7. Countering Intended or Unintended Malpractice

Those operators of advanced and automated transport systems are vulnerable to malpractice both intended (hacking) and unintended (procedural failures).

Further consideration and recognition that the dynamic of lower barriers to entry (for product development and market entry), readily available skills and pervasive associated technologies, can increase risk of malpractice resulting in a product that is 'unsafe to operate'. Particular effort should focus on software for core functions such as navigation, flight controls and code for embedded operational technology, noting that any advanced transportation system is a 'system of systems.'

Additionally, the asymmetric value that autonomous systems can bring may also increase the vulnerability at a 'pinch point of weakness' disrupting a 'fleet' or even a product range through 'menace'. An event like this may not be too dissimilar to the process of ransomware. Additionally, any failure to recognise and act on general due diligence could have similar results. Therefore, this section centres more around unintended malpractice, as one would hope that sufficient discipline and processes around this activity will also aim to mitigate those people or organisations that purposely intend to disrupt. A recognised general attitude towards mitigation of such could dissuade low level 'hostile actors'. The alternative may create an opportunity to disrupt – namely 'behaviour breeds behaviour'. Further, it is worth highlighting that unintended and intended have a very fine line of distinction. For example, a drone manufacturer who was considering taking risks regarding the resilience of the system, may resort to a different conclusion if internal awareness of increasing the products status to 'an unsafe to operate vehicle' can be proven.

7a. Intended Malpractice

The vulnerability of our transport systems will vary dependent upon the nature of that system[14]: automotive, commercial aviation, private aviation, commercial maritime or rail networks. In addition, we should consider the benefit to the hacker. For private transport it may be a nefarious purpose, with the hacker establishing where High Net Worth individuals or cargo is heading. Commercial and state transport systems could be seen as targets for terrorists or, if the hacker works for an active environmental group, they may wish to cause substantial delays (i.e. drones in Gatwick ATZ caused the airport to be closed for up to 33 hours, resulting in the cancellation of approximately 800 flights, and disrupting travel for approximately 120,000 people). A hack into the rail network or the UK National Air

[14] https://www.npsa.gov.uk/counter-uncrewed-aerial-systems-c-uas

Traffic System [15] would cause massive disruption, chaos or incidents and accidents. Large-scale maritime vessels carry immense logistics loads and any disruption in their operations would have a massive effect on worldwide supply chains. This aspect of Critical National Infrastructure is outside the scope of this paper but is addressed by NPSA.[16]

Although not specifically covered in this paper, in a less aggressive sense, commercial rivals may conduct industrial espionage via hacking. Intended malpractice can result in many effects, ranging from loss of commercial profit, loss of reliability in transport systems, loss of reputation, rewards for terrorists' actions and ultimately chaos and deaths in extreme cases. An observation can be made that it would be very difficult for a 'hostile actor' to identify a drone (in assembly) that could be used for a specific task and infiltrate its intended purpose or activity for a specific setting. It is, however, more likely that such motivations may be to disrupt a product line or a large-scale organisation (for example, a 'last mile delivery service') for the purposes to hold to account through ransom or reputational damage.

7b. Unintended Malpractice

Unintended malpractice or neglect of professional duty[17] is defined, for this paper, as a process failure or lack of process existence which can increase the probability of a negative outcome to a product or operation of that product. We have pointed out that the whole eco system of any advanced transportation systems is complex and often drone operators are not aware of their vulnerabilities in terms of data quality assurance and resilience. All operators must be aware of not adopting the appropriate procedures to mitigate risks to electronic data systems. However, data quality and security measures are often not outlined in operating procedures or in the training of vehicle systems operators.

[15] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3378277)

[16] https://www.npsa.gov.uk

[17] https://ico.org.uk/media/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-report-1-0.pdf

The list below gives some examples of outcomes which may ensue if processes and procedures for drones and AI systems are not adhered to or are unclear:

- A potential for operational failure/crash
- A failure in the lack of performance of a product as designed, i.e. poor performance due to poor procedures being applied, or not applied at all
- A supply chain failure (including quality and 'secure' product integration)
- A procedural, or non-procedural, activity that increases the risk of failure in all aspects of product support and service delivery

It is important to note that sources of such failures can emanate at all levels: failure to comply to existing procedures at operational levels, or failure to ensure due diligence and process gap/reviews are managed and led from the executive level. Further, it is important to note that not all relevant organisations and companies operate at such risk, but the purpose here is in fact to highlight the potential consequences of failure from behaviours, culture[18] or effective management systems. For this section, categorisation is made through three subsections. It is key to note that the dynamics of each may impact the organisation deliverable and influence other categories potentially unfavourably:

- Macro level: industry nature
- Micro level: organisational culture and behaviour
- Micro level: organisational effectiveness – management systems

Further, all drone or autonomous system types, in each setting, represent potential risks to operators, the public and other drones. However, the applicability of this content is 'absolute' over the nature of all drone platforms and settings, whether construction, assembly and integration. Further, all capability and assets that these platforms deliver, use or support still (certainly if connected) need similar consideration. It is important to note that the context and specific nature of the autonomous systems marketplace can be seen as influential in decision making and behaviours internally in organisations.

[18] https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/12/01/the-impact-of-culture-in-the-

8. Proposal for Data Resilience and Quality Assurance in Automated and Autonomous Vehicle Systems (Land, Sea and Air)

As we evolve our transportation systems in all domains, so we must respect the lessons identified and, in most cases, learned, over many decades to ensure our transportation systems will be safer, more efficient and more sustainable in the future. Data-dependent transportation systems bring new vulnerabilities that require new policies and regulations, underpinned by standards, to assure the resilience and quality of that data upon which these systems are heavily dependent.

This is the third in a series of DDG papers, intended to raise issues which are of import in terms of UK developing best value from the emerging drone and autonomy markets. This paper prosecutes the case that, without proper regulation across land, sea and air domains, the increasing all-pervasive Internet of Things, fuelled by complex, highly dispersed supply chains and commercially driven Artificial Intelligence, presents uncontrolled safety and security issues.

The UK Government needs to be cognisant of the emerging threat to our rapidly developing advanced and autonomous transportation systems. Consideration must be given to whole-system, end-to-end and through-life safety, coupled with a fuller understanding of the risk that corrupted data quality, and a lack of resilience can bring, otherwise, drones or systems in which drones are a part, could be seized for malicious intent by a hostile actor. These potential threats, if left unaddressed, will not only frustrate development of value from a transformation market but pose a very real risk to life and social and disruption to industrial and government processes.

Advancing technology and rapid lifecycles in autonomous air/land/sea vehicles (time to obsolescence); cost points driving either implementation of software, components or design of unknown provenance; or driving business and organisation practices that ignore risk, or themselves build risk into products, are inherent risks. The accumulation of the above could drive a 'perfect storm' in autonomy, in which an avoidable (if DQRMS policy/standards are not implemented) rogue event could stall development in this area, to the detriment of UK PLC – worse still, chaos in our developing transportation systems.

In conclusion, at the highest level, the UK Government must introduce a policy which requires:

> **All manufacturers and operators of advanced and autonomous vehicle systems to establish Data Quality and Resilience Management Systems (DQRMS) that can mitigate the effects of data malpractice, intended (hacking) or unintended (procedural), in proportion to the likely threats they may face.**

Without DSRMS protection, which must be regularly updated and maintained relevant to the threats faced, our data-hungry, advanced and autonomous transportation systems are vulnerable to malpractice which could result in the complete breakdown of transport infrastructure facilities across multiple sites and vehicle types. A 'crash', in data terms, could mean whole batches of vehicle systems malfunctioning, resulting in chaos across a wide range of our transportation systems.

Epilogue

The DDG is a not-for-profit organisation with approximately 400 members. The core aim of the DDG is to provide a voice for drone industry manufacturers, operators and user groups through which strong and reasoned opinion can be aired with respect to the health and needs of the industry at large. Being commercially independent, we are also able to provide impartial advice to the UK Government on advanced and autonomous uncrewed transportation systems across land, sea and air.

We have used the wealth of our members' industry experience to construct this white paper and have proposed a policy that we believe is a stepping stone that can cascade down to regulations, standards and the enforcement of Data Quality and Security Management Systems, aimed at assuring a high level of data quality and security in these systems.

The DDG is available and open to requests from HMG to assist in turning this policy into a workable and effective set of regulations, standards and procedures, aimed at keeping our transportation systems safe from malpractice for all users.

REFERENCES

Note	SOURCE	LINK
1	The Consequences of not having a formulised quality management system – S Kuldeep	https://www.linkedin.com/advice/0/what-most-important-data-management-standards-guidelines#:~:text=Data%20management%20standards%20and%20guidelines%20are%20the%20best%20practices%20and,security%2C%20compliance%2C%20and%20value.
		1. Inconsistent Product or Service *Quality: Without standardized procedures and guidelines, employees may lack clear instructions on how to achieve desired quality standards resulting in variations in product specifications, defective outputs, and dissatisfied customers.* ***2. Increased Operational Costs:*** *Without a formalized QMS, organizations may experience increased operational costs. Inefficient processes, lack of quality control measures, and frequent rework contribute to unnecessary expenses.* ***3. Compliance and Regulatory Risks:*** *Organizations without a formalized QMS are more vulnerable to compliance and regulatory risks. In industries with strict quality standards and regulations, non-compliance can result in severe penalties, legal actions, and loss of business opportunities.* ***4. Lack of Continual Improvement:*** *A formalized QMS provides a framework for continual improvement. It encourages organizations to monitor performance, collect data, and analyse trends to identify areas for enhancement. Without a structured approach to quality management, organizations miss out on opportunities for innovation, process optimization, and staying ahead of competitors.*

		5. Damaged Reputation and Customer Dissatisfaction: *Not having a formalized QMS can lead to a damaged reputation and customer dissatisfaction. Quality issues, such as product defects or service failures, can quickly spread through word-of-mouth and social media platforms.*

Protect Automated Transportation Systems

(Or autonomy will be too exciting!)

Executive Summary

This paper acknowledges the growing influence of data-driven automation in transport systems and considers the need to evolve safety practices to cope with these transport ‘systems of systems’[1]. Modern transport systems are controlled by external digital influences: internal Internet of Things (IoT) data (often shared); diverse components (sometimes of unknown integrity); and electronic supply chains – all of which encompass distinct vulnerabilities. The inevitable adoption of Artificial Intelligence (AI) will be a solution for some but may produce unintended consequence(s) to associated systems. This paper examines data issues and their potential security impacts in relation to advanced transport systems (across all domains) and provides a policy recommendation relevant to key legislators. The aim is to continue to ensure that ‘all advanced transportation systems are safe to operate and operated safely[2]’.

Data is at the heart of current advanced and autonomous systems. If we break that data use down into it component parts, we can show that many influences enable these systems of systems. All these elements are vulnerable to malpractice and therefore need protection to avoid serious crashes involving whole batches of transportation means. So how do we protect these systems, from the simplest to the most advanced and complex?

[1] **System of systems** is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system which offers more functionality and performance than simply the sum of the constituent systems. https://en.wikipedia.org/wiki/System_of_systems#:~:text=System%20of%20systems%20is%20a,sum%20of%20the%20constituent%20systems.

[2] Surely and simplistically the core mandate upon which all regulations and standards are based.

Regulatory authorities have been improving vehicle safety operations across land, sea and air for decades and these regulations aim to ensure that vehicles are 'safe to operate and operated safely'. We have lost many lives in the past that would not be lost today because of the lessons we have identified, learned and applied as regulations, most successfully when underpinned by safety and quality standards. As analogue systems increasingly give way to digital control, vehicles become transport systems of systems. They are no longer isolated boxes, and a decreasing number of experts have access to, or understanding of, the technology embedded within them. These advanced vehicles are highly automated and human actions, augmented by digital systems, are enhancing the experience of transportation; they remain associated with, and are ushering in, distinct risks requiring confrontation. This is an evolution in the way drones (land, sea and air) operate – it is not a revolution.

Proposal for Data Quality & Safety Assurance in Automated and Autonomous Vehicle Systems

This paper prosecutes the case that, without proper regulation across land, sea and air domains, the increasing all-pervasive IoT, fuelled by complex, highly dispersed supply chains and commercially driven Artificial Intelligence, presents uncontrolled safety and security issues. The output of this paper is a policy statement which we suggest should be adopted by the UK Government to ensure that our advancing transportations systems evolve with increasing safety through a focus on data quality at their heart. Assuring both data quality and resilience is vital to prevent chaos and to ensure our advanced transportation systems build upon the safety and efficiency we have created through the evolution of combined experience.

The UK Government needs to be cognisant of the emerging threat to our rapidly developing advanced and autonomous transportation systems. Consideration must be given to whole-system, end-to-end and through-life safety, coupled with a fuller understanding of the risk that corrupted data quality and a lack of resilience can bring, otherwise, drones – or systems in which drones are a part – could be seized for malicious intent by a rogue actor. In conclusion, at the highest level, the UK Government must introduce a policy which requires: **All manufacturers and operators of advanced and autonomous vehicle systems to establish Data Quality and Resilience Management Systems (DQRMS) that can mitigate the effects of data malpractice, intended (hacking) or unintended (procedural), in proportion to the likely threats they may face.**

Without DQRMS protection, which must be regularly updated and maintained relevant to the threats faced, our data-hungry, advanced and autonomous transportation systems are vulnerable to malpractice which could result in the complete breakdown of transport infrastructure facilities across multiple sites and vehicle types. A 'crash', in data terms, could mean whole batches of vehicle systems malfunctioning, resulting in chaos across a wide range of our transportation systems. In sum, advancing technology encouraging rapid lifecycles in autonomous air/land/sea vehicles (time to obsolescence) and cost points driving either implementation of software and components or design of unknown provenance, may drive business and organisation practices that ignore risk or themselves build risk into products. The accumulation of the above could drive a ‘perfect storm’ in autonomy, in which avoidable (if policy/standards are not implemented) rogue events could stall development in this area, to the detriment of UK PLC.