PETRAS

Industry Briefing

Cybersecurity for the Internet of Things and Artificial Intelligence in the Transport and Mobility Sector

Zakiyya Adam

About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 16 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate and the University of Warwick.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

In addition, we build the capacity of the UK to remain a world leader in IoT through our training and development programmes for early career researchers. Finally, we offer consultancy services to the public and private sectors to provide decision makers with insight and advice on a range of cybersecurity related issues.

The wider PETRAS community has played a role in creating this report - in particular Professor Carsten Maple, Sector Lead for Transport and Mobility at PETRAS, at the University of Warwick for his critical role in review, and Caroline Wijnbladh and Emilie Didier from the PETRAS Business Development Team for their editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Adam, Z. 2021. *Industry Briefing: Cybersecurity for the Internet of Things and Artificial Intelligence in the Transport and Mobility Sector,* PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI:

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence in the Transport and Mobility Sector. This is the third in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, AgriTech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the Transport and Mobility sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

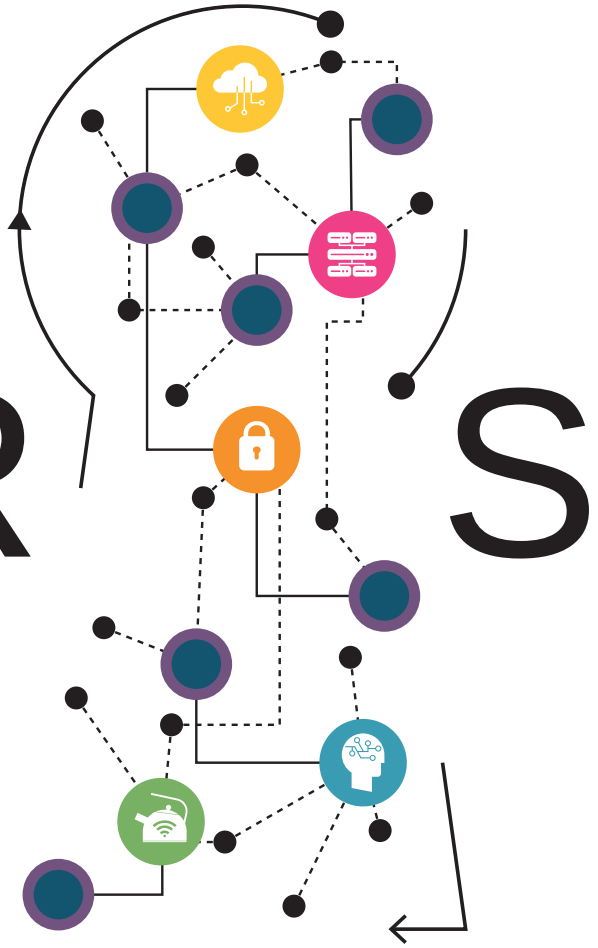
Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

UKRI Engineering and Physical Sciences Research Council

Contents

PETRAS

THE PETRAS NATIONAL
CENTRE OF EXCELLENCE
FOR IoT SYSTEMS
CYBERSECURITY



Executive Summary

The PETRAS National Centre of Excellence aims to ensure that technological advances in the Internet of Things (IoT) and Artificial Intelligence (AI) are developed and applied safely, and securely by considering social and technical issues in a variety of sectors.

The global smart transportation market is undergoing rapid growth, in large part due to developments in the Internet of Things. There are a number of different applications of IoT within the sector. This report focuses on two broad areas:

1. IoT-enabled vehicles
2. Mobility as a Service (MaaS).

These advancements have the potential to bring significant benefits, including:

- Reduced congestion;
- Increased safety;
- Greater accessibility;
- Improved air quality;
- More reliable service;
- Better transport management.

Based on research undertaken over the last few years, this brief offers insights into general trends and challenges in cybersecurity research and policy for IoT devices and AI within the Transport and Mobility sector in the UK, EU and at the global level.

Challenges

Wide adoption of IoT technology in the sector poses numerous challenges:

- **Cybersecurity** concerns need to be addressed. This involves designing devices and systems that are both resilient to, and capable of detecting, cyber attacks;
- **Data**-related issues emerge at each stage of the process, from acquisition and storage, to labelling and management;
- **Cloud** capabilities, **5G** availability and **GDPR** considerations need to be accounted for;
- **Ethics** should inform design choices;
- Successful implementation requires overcoming numerous **technical** obstacles;
- The broader industry **mindset** needs to adapt to a collaborative approach to transport and mobility.

Policy

The UK is recognised as one of the most open testing environments in the world for automated vehicles. Some of the key policy developments for connected and autonomous vehicles include:

- The **UK Code of Practice** provides guidance on testing automated vehicles on UK roads;
- **CAV PASS** ensures safety and security through a certification and approval scheme;
- The **BSI** has developed a range of industry standards;
- **CertiCAV** will develop scenario-based safety criteria to be met, and assessment methods to demonstrate compliance;
- The **Automated and Electric Vehicles Act 2018** extended insurance provisions to cover automated vehicles;
- A **three-year review of the UK's legal framework** for automated vehicles is currently underway.

MaaS implementation is in its early stages. The regulatory framework to support it is currently being reviewed.

- Current guidance, codes of practice and regulations are to be **updated** to ensure that legislation on transport, data protection and consumer protection accounts for MaaS.
- A **new framework** may be developed to regulate the elements of MaaS not covered by existing legislation.

Opportunities

The challenges faced by IoT-enabled vehicles and MaaS offer opportunities for further research. Both of these areas have specific research needs, detailed in this report. Broad areas of interest across the sector, that are essential for effective adoption of IoT, include:

- **Technological** issues;
- Developing supportive **regulatory frameworks**;
- Cultivating **social acceptance** of the changing transport and mobility landscape.

PETRAS has rich and expanding experience of working within the sector, and is well-placed to face the privacy, ethics, trust, reliability, acceptability, and security concerns that will emerge as IoT becomes increasingly more embedded in the fabric of how society moves.

Introduction

Scope of this brief

This brief offers a summary of general trends and challenges in cybersecurity research and policy for IoT (Internet of Things) devices and AI (Artificial Intelligence) in the Transport and Mobility sector. The geographic scope encompasses the UK, EU and the global level, based on research collected up to 2021. In addition, the document will offer insights into PETRAS activities that focus on Transport and Mobility.

The intended audience is primarily external industry and government organisations, including small, medium and large companies working around IoT, AI, security and cybersecurity in the Transport and Mobility sector, who would like to gain insights into PETRAS's work and collaboration offers.

Within the context of this brief, IoT devices are viewed as a component of a larger ecosystem comprising of data communication, data aggregation and processing, data analytics and inference, and data visualisation.

The Transport and Mobility sector is broad. Within this brief, vehicles that facilitate the movement of people and goods are explored, as well as services that enhance mobility. Vehicles whose primary purpose is not transportation – for example, construction cranes, farming vehicles and warehouse tractors - are not included. Similarly, the focus of this brief does not extend to IoT-enhanced traffic management tools (such as smart motorways) or transport infrastructure (such as the use of wireless smart sensors on bridges).

Sector background

Development of IoT in the Transport and Mobility sector is enabling rapid growth of the global smart transportation market, predicted to rise from USD 94.5 billion (approx. £68 billion) in 2020 to USD 156.5 billion (approx. £112.5 billion) by 2025, at a Compound Annual Growth Rate (CAGR) of 10.6%[1].

There are a number of different applications of IoT within the sector. This report focuses on two broad areas. The first area concerns **IoT-enabled vehicles**. The second one considers the wider ecosystem within which these vehicles operate, with the increasing adoption of **Mobility as a Service** (MaaS) across the world.

IoT-enabled vehicles

IoT-enabled vehicles are found across all forms of transport: road, rail, aviation and marine. They may be Connected Vehicles (CVs), Autonomous Vehicles (AVs), or Connected and Autonomous Vehicles (CAVs).

- CVs utilise wireless networks to communicate with nearby vehicles, infrastructure and mobile devices.
- AVs use sensors - such as cameras and lidar - to communicate with driving systems, such as steering, braking and parking assistance.
- CAVs combine CV and AV capabilities to realise the potential benefits of a fully automated driving system[2].

Mobility as a Service (MaaS)

Mobility as a Service (MaaS) is a concept that is changing how people think about moving around their cities. It looks to make transport so simple and easily accessible that it would be the most efficient choice for individuals, negating the need to own a private vehicle. MaaS is a one-stop online interface, typically a mobile app, which serves as:

1. An intermodal **journey planner** that operates in real time, providing combinations of different transport modes (such as taxi, underground, rail, bus, bike-sharing, car-sharing, car rental etc.);
2. A **booking system** incorporating the entire end-to-end journey stages; and
3. A **single payment portal** across multi-modal journey[3].

MaaS has the potential to reduce **road congestion**, improve **air quality** (due to decreased car use and congestion), improve users' **physical health** (by encouraging active modes of travel), improve passengers' **travel experiences** (through simplified booking and payment processes, and more personalised journeys), improve **customer choice** by increasing awareness of and access to various transport modes, and facilitate better **management of travel demand and transport infrastructure** (by using the collected data to optimise use of the existing network and plan necessary enhancements)[4].

Internet of Things and AI Cybersecurity

Some challenges and threats are shared across all transport modes. Others are specific to vehicles operating on the roads, railways, air and sea.

IoT-enabled vehicles 

Shared challenges

Cybersecurity	Key principles to be addressed include: secure **storage** and **transmission**; security **risk assessment** and management, including across the supply chain; cybersecurity **monitoring** and incident response; security of software managed throughout vehicle **lifetime**; vehicle should be designed to be **resilient** to cyber attacks; vehicles designed with capability to **detect** cyber attacks and respond appropriately; organisational security and **governance** at the highest level; **third party risk** management and cooperation on security; vehicle manufacturer **testing** procedures on security functions[5].
Data	In just one day, a single test AV on the road produces as much data as the Hubble Space Telescope produces in a full year. These vast volumes of data pose challenges regarding: (1) **Data Acquisition**: AI must be exposed to a diverse range of scenarios in order to identify patterns and learn what the vehicle may encounter on the road; (2) **Data Storage**: require secure, accessible and economical data storage systems; (3) **Data Management**: information on the data's journey over time should be tracked to maintain data integrity and usability; and (4) **Data Labelling**: each hour of data collected can take almost 800 human hours to annotate[6].
Cloud	Data is stored and processed in the cloud. Traditional cloud computing has serious disadvantages and challenges. Edge computing may resolve these issues. It decentralises data processing, analysing data at the network edge close to where it is generated. Lowering dependence on the cloud has numerous benefits, including: increased data **security** and **privacy**; more responsive and robust application **performance**; reduced **operational costs**; unlimited **scalability**; conserving network and computing **resources**, and reduced **latency**[7,8].

Shared challenges (continued)

5G	Expected to deliver a step change of **ultrafast, low latency, reliable, mobile connectivity**[9]. The automotive industry is forecast to become the largest market opportunity for 5G IoT solutions, representing 53% of overall applications of 5G[10]. In order for 5G to be utilised for vehicular connectivity, there would need to be **extensive coverage nationwide**[11].
GDPR	The General Data Protection Regulation (GDPR) came into effect in 2018 and is the *toughest privacy and security law in the world*[12]. In 2020, the European Data Protection Board (EDPB) published guidelines on processing personal data in the context of connected vehicles and mobility-related applications. The guidelines emphasise compliance with the principle of **data minimisation** and that the purpose for any data processing must be *"specified, explicit and legitimate"*. They recommend that only data required for the vehicle to function properly should be processed by default. In all other circumstances, data processing should only take place where the data subject has opted in[13,14].
Mindset	A general change of industry mindset is required to one which is open to **sharing resources**, **consolidating business solutions** and the **creation of new value** from transport services, both within and outside of their own ecosystems[15].
Ethics	Ethical considerations regarding AVs and CAVs, including the ethical dilemmas of autonomy, have been the focus of much academic and public scrutiny. In June 2020, the **European Commission published a set of 20 ethical recommendations** on the ethics of CAVs regarding their future development and use of CAVs. For example, ensuring accountability for CAVs' behaviour, and auditing CAV algorithms[16].

Road

Specific challenges for road vehicles were identified by The European Union Agency for Cybersecurity (ENISA)[17] and include:

Hijacking Eavesdropping Intercepting	Man-in-the-Middle Attack (e.g. disclosure/ modification of information, communication disruption); Communication Protocol Hijacking (e.g. password/ information disclosure)
Nefarious Activity/ Abuse	Denial of Services (e.g. shutting down the RSU, jamming radio communications); Manipulation of Information (e.g. information/ intellectual values disclosure, map data poisoning, loss of data); Manipulation of Hardware & Software (e.g. configuration, malicious OTA updates); Unauthorised Activities (e.g. unauthorised access to information/ system/ network, unauthorised installation/ use of software); Identity Theft (e.g. impersonating ambulance/ police car, financial fraud such as tolls); Abuse of Authorisations; Original Equipment Manufacturer (OEM) Targeted Attacks
Threat Against Autonomous Systems	Targeting Autonomous Sensors (e.g. radar/ lidar jamming, sensors blinding); Targeting AI/ ML (e.g. hide objects, fake data perception)
Other challenges	Outages (network outage, loss of signal); Failure/ Malfunctions (failure or disruption of services, failure or malfunction of sensors, software vulnerabilities exploitation); Unintentional Damages (unintentional change of car components configuration, information leakage); Legal; Physical Attack

Rail

The Department for Transport identifies the following vulnerabilities in the rail industry: policy and procedure, architecture and design, configuration and maintenance, physical intrusion, software development, communication and network, and lack of training and awareness (Department for Transport, 2016).

Specific challenges for rail vehicles include:

Hacking	Railway networks are particularly vulnerable. They often combine modern technological components with archaic physical ones. Train companies typically use safety systems designed to last 30 years or more, meaning that they were put in place before contemporary hacking tools were available or threats were known. The security gap between old and new technologies needs to be closed and systems put in place for cyber threat detection[18].
Obstacles	Trains operate in open environments and may encounter unexpected obstacles, such as animals, a person crossing the tracks, or fallen trees. Thus, autonomous trains require train positioning technology with a high level of precision[19].
Subsystems	Operation of a train involves complex interactions between various subsystems. If any of the numerous subsystems fails to judge the situation accurately, they will defensively slow down or stop the train, disrupting the train network[20].

Aviation

Specific challenges for aviation include:

Hacking	High levels of connectivity of modern aircrafts create numerous vulnerabilities to cyber attacks. Both small planes and commercial aircraft are vulnerable to hacking. Attacks may range from introducing malicious code to hacking aircraft communication data links[21].
Collisions	Autonomous aircraft need to be able to manoeuvre out of danger, in order to do so they must Detect and Avoid (DAA). As drones are barely visible to other pilots, the onus is on the drone to move out of the way. This requires advanced sensors that will enable them to spot other aircrafts, often against busy backgrounds, and estimate the probability of danger early enough to have time to manoeuvre back to safety[22,23].
Cyber-physical attacks	Drones used for deliveries are vulnerable to cyber-physical attacks due to their altitude limitations. In these cases, an adversary aims to compromise the drone, take over control, and destroy, delay or steal the transported goods[24].
Holistic risk management	Efficient and effective mitigation of cyber risks in the UK's aviation sector requires a collaborative approach between the Government, regulators and the aviation industry. There are also dependencies between cybersecurity, physical security and personnel security; thus, a holistic approach to risk management is essential[25].

Marine

Specific challenges for marine vehicles include:

Cybersecurity	Many of the protocols in the maritime sector were developed before cybersecurity became a concern. It has a lower security culture than other transportation sub-sectors[26]. A ship comprises five main asset types used to provide a range of operational services: plant and machinery, operational technology, information technology, radio frequency (RF) communications, and navigation systems. As technology plays an increasingly important role in these areas, so does the need to protect them from cyber attacks. Six aims of an attack on a ship are identified: destroy, degrade, deny, delay, deter, detect, and distract[27].
Phishing	Malware may invade a system within weeks whilst a response from a regulator can take months or years. This raises the issue of cyber awareness amongst individuals involved in the maritime sector; it is estimated that the industry currently lacks 50,000 to 100,000 people who are trained in cyber[26] .
Extreme weather conditions	Selection of the best path for the AV – through an environment containing static or moving obstacles - is impacted by weather conditions, such as waves, wind and sea currents[28].

Mobility as a Service (MaaS)

The MaaS Alliance is a public-private partnership creating the foundations for a common approach to MaaS. It identified the main areas to be addressed with regards to MaaS implementation[29]:

Undefined Principles for Data Sharing & Access	Data sharing and data access are a recurring issue for MaaS. Privacy and security, low quality and availability, poor data management, fragmentation of data, lack of well-defined standards, and whether the data obtained from public-funded systems can be used to improve and develop private mobility services, all pose questions/ concerns.
Developing of Trust for Collaboration	The fear of losing control leads to risk aversion behaviour within the ecosystem and deficit of trust. There might also be fears related to fairness and neutrality of the new ecosystem i.e. whether they can trust that a MaaS platform will display their services in a fair manner to the end users.
Scalability	Often hindered by multiple regulatory layers encompassing the different acts of law present locally, regionally and nationally. Having a solution that can be used across several jurisdictions is not possible, impeding the use of business models based on global approaches.
Public-Private Partnership	MaaS value proposition means a paradigm shift for all stakeholders involved. It includes everything from administrative processes to vision and approach to mobility.
Market Access and Integration Barriers	The current legislation occasionally prevents new mobility service providers from entering the market. Fragmented regulatory frameworks, as well as operational interoperability issues, hinder scalability of services and integration.

Policy

The UK is recognised as one of the most open testing environments in the world. Close and unrivalled cross-sector collaboration across government, industry and academia in CAV development and regulation sets the UK apart[30].

IoT-enabled vehicles

Safety

UK Code of Practice: In 2015, the UK Code of Practice for testing automated vehicles on public roads was published, stating that testing of automated vehicles is possible on any UK road – without the need to obtain permits or pay surety bonds – as long as UK law is complied with[31]. In 2019, the Code of Practice was updated to provide further guidance to support organisations in conducting safe and responsible trials in the UK: the update did not introduce any new legal requirements or barriers[32].

CAV PASS: In September 2019, the Government built on the Code of Practice in announcing the CAV PASS (Connected and Automated Vehicle Process for Assuring Safety and Security) project. CAV PASS is a certification and approval scheme, a world-first safety regime that ensures self-driving vehicles are safe and secure by design and minimises any defects ahead of their testing, sale and wider deployment on UK roads[30,33,34].

British Standards Institute (BSI): BSI is developing a range of Publicly Available Specifications (PAS) standards on connected and autonomous vehicles to complement UK policy[35].

CertiCAV: The CertiCAV framework is in development; it will propose scenario-based operational safety criteria to be met, as well as assessment methods used to demonstrate compliance with them[34,36].

Cybersecurity

The UK ranked number one in the world for cybersecurity in the 2020 Autonomous Vehicles Readiness Index published by KPMG[37].

In 2017, the Government published T*he Key Principles of Cybersecurity for Connected and Automated Vehicles guidance*[38]. Aimed at all parties in the supply chain, the principles provide a holistic approach to considering the security of vehicles and their wider ecosystem, throughout the life cycle of the vehicle[30].

Building on these principles, a new standard focusing on cybersecurity of vehicles was developed by the BSI in collaboration with the government and industry in 2018: PAS 1885 The Fundamental Principles of Automotive Cybersecurity[39].

Regulation

In 2018, the UK's first regulation for automated vehicles received Royal Assent, the *Automated and Electric Vehicles Act 2017*[40]. The Act extended insurance provisions to cover automated vehicles, stating that insurers will be liable for damage stemming from an accident caused by a CAV when the vehicle is in self-driving mode. The Law Commission has suggested that the legislation be developed further to define the role of the 'user-in-charge' [41,42].

The Law Commission of England and Wales and the Scottish Law Commission are currently undertaking a three-year review of the UK's legal framework for automated vehicles. The review will consider issues of safety as well as the use of automated vehicles as part of public transport networks and on-demand passenger services[30].

Comparative standing

The UK scored ninth out of 30 countries in KPMG's 2020 Autonomous Vehicles Readiness Index, dropping two places from the previous year[37]. For each of the four pillars that comprise the index, the UK ranked:

- Policy and Legislation: second;
- Technology and Innovation: ninth;
- Infrastructure: sixteenth;
- Consumer Acceptance: twelfth.

The top five ranked countries were: Singapore, The Netherlands, Norway, United States, and Finland.

Mobility as a Service (MaaS)

The Transport Data Initiative[43] identified four issues regarding MaaS implementation relating to governance and contractual matters:

1. **Co-operation** – between the various entities involved in a MaaS solution, both private and public sector organisations;
2. **Approach to Data** – what data can be shared in line with Data Protection Regulations, what standards there are for data, and whether the various parties have the correct technology and interfaces to manipulate the data;
3. **Governance** – in the form of legislations and regulations, crucial for both building barriers and breaking them down; and
4. **Security** – with regards to data, technology and overall security of the end user.

A Transport Committee report[4] suggests that the Government has a role in ensuring "*that MaaS can evolve effectively*" through its governance with regards three areas, detailed below.

Incentivising Data Sharing. Data is crucial to MaaS schemes, and any agreements between transport operators will be underpinned by how data is shared. The Transport Committee recommended that Government works with local authorities on a "no data, no service" policy. This would stipulate that transport operators who want to provide a service in a given area must agree to share data.

Passenger Rights and Protection. The Transport Committee concludes that the Government should assess the risks to MaaS users' interests, including fair market competition, pricing of MaaS packages, and individuals' personal safety.

Regulatory Framework. The Transport Committee called on the Government to do two things: (1) Review and update current guidance, codes of practice and regulations to ensure that legislation on transport, data protection and consumer protection accounts for MaaS. (2) Develop a framework to regulate the elements of MaaS not covered by existing legislation.

The Future of Mobility Regulatory Review was announced by the Department of Transport in 2019[44] and a report of the findings was published in October 2020[45]. The review found that central government should be responsible for setting an overarching regulatory framework for MaaS, provide funding for research and development and the infrastructure underpinning the transport system, set the strategic goals and policy, and provide guidance to local authorities (LAs) in the deployment of MaaS platforms. Several local councils felt that the Government should develop a national framework.

There was general consensus that regulation should focus on safety, personal data use, interoperable data standards and open Application Programme Interfaces (APIs), consumer protection, accessibility enforcement and review competition rules regarding collaboration between transport operators. It was also agreed that central government should be responsible for the monitoring and evaluation of MaaS platforms, sharing lessons learnt and disseminating best practices.

Opportunities

Gaps in research and barriers to deployment of connected and autonomous vehicles across all transport modes, and then specifically for road, rail, air and waterborne transport, are presented in this section.

IoT-enabled vehicles

Shared challenges

Common themes across all transport modes include[46]:

- **Technological development**
- **Social acceptability:** including traffic safety, personal security, and privacy and protection from cyber-crime
- **Regulatory frameworks:** guaranteeing safe operation of unmanned systems and allowing a variety of innovative transport solutions
- **Financial frameworks:** for using public infrastructure and as a demand management instrument

Road

In their analysis of existing research on AVs, Mora and colleagues[47] demonstrated that greater focus is required on the environmental consequences, and the socio-economic, cultural, political, institutional, and organisational implications, that a mass market for autonomous driving technology can generate.

The European Commission[46] identified specific gaps in research and barriers to deployment, these included:

- Artificial intelligence to allow automated cars to act more similar to humans (complex perception and decision making, predictive driving), including moral dilemmas;
- Handling of mixed traffic situations;
- Understanding user needs and social attitudes, to enable influencing the end user in the process of deployment and actual use of connected and automated vehicles;
- Handling and potential use of the generated big data;
- Spatial impacts on land use, urban planning, design of roads, parking, etc.
- Need of a supportive regulatory framework (traffic rules, exemption frameworks, liability, data traffic, cybersecurity, on road beta-testing, etc.) that allows experimental research and benefits from its outputs;
- International standards for communication of information and intention between vehicles, their occupants and other road users.

Rail

Gaps in research and barriers to deployment include[46]:

- Concerns about emerging cybersecurity and resilient communication aspects;
- A high number of national technical and operational rules;
- Long life cycles of existing systems;
- Highly defragmented picture of railway regulations and technical solutions among European countries;
- Expectation of new digital technologies which could deliver break through innovations hinder organic developments;
- Culture of ex-post coordination instead of ex-ante cooperation.

Aviation

Specific to airborne drones, a systematic literature review into their use and future strategic directions for their control was carried out in 2020. The paper concluded that there is a need for further policy and management guidance to both efficiently manage the rapid growth of drone usage, and to facilitate innovation[48].

- Gaps in research and barriers to deployment identified by the European Commission[46] included:
- Management of safety and security threats;
- Change in terms of liability, environmental and economic impact;
- Social factors, such as social resistance and the level of role/responsibility;
- Lack of harmonisation and globalisation of certification;
- Limited standardisation;
- Limited opportunities for social engagement although significant changes in society are to be expected;
- Lack of collaborative mindset in a fully privatised and highly competitive industry.

Marine

Three avenues for further research were identified in Policy Implications of Autonomous Vehicles, published in 2020[49]:

- Governance frameworks to facilitate safe navigation of autonomous vessels. Especially important during the earlier stages when mixed traffics of conventional, autonomous or remotely controlled vessels exist simultaneously;
- Connectivity and data governance. Requires robust internet connectivity free from cyber attacks and malfunctions. And this secure and reliable service needs to be available in the middle of oceans;
- Long-term impacts on the maritime workforce market.

Obstacles delaying the development of autonomous shipping were identified by Claassen[50] to include:

- Communication between ships must function reliably. Ships need to be able to communicate wherever they are, even under bad weather conditions;
- Technology has to be integrated into the existing infrastructure;
- Harbours need to have the necessary infrastructure;
- Solutions have to be compulsively cost-effective.

Some additional gaps in research and barriers to deployment, identified by The European Commission (2017), include:

- Developments in cybersecurity and standardised data exchange protocols;
- Need to develop much better systems for technical maintenance of ship systems, including system monitoring and condition based maintenance planning;
- Lack of open standards for integration between systems as well as for adding new and open innovation based products to the ship;
- Legislation hinders deployment of more automated and autonomous vessels in local ports, nationally, regionally and internationally;
- Safety and evacuation of passengers on unmanned vessels;
- Regulations on equipment and integration on merchant ships hinders open innovation and development of new and innovative energy saving systems.

Mobility as a Service (MaaS)

Barriers to MaaS adoption in cities include, on the supply side:

1. lack of cooperation among stakeholders;
2. lack of business interest;
3. lack of service coverage;
4. lack of a clear, shared vision;
5. lack of data and cybersecurity.

And on the demand side:

1. overcoming the lack of appeal with older generations;
2. overcoming the lack of appeal with public transport users;
3. need to provide a platform that is attractive and easy to use;
4. customer willingness-to-pay;
5. overcoming the culture of private vehicle travel[51].

A couple of these barriers are expanded on below.

Service Coverage: This barrier presents in two ways. Firstly, network coverage. MaaS depends on reliable network coverage across its operating region. And secondly, provision of the MaaS service across an entire area. Low density areas are often associated with longer travel distances, lack of existing public transport services and less variety in the range of transport modes available. Smaller administrative areas may also lack funding, staff and general technological capabilities to support services[51].

Data and Cybersecurity: MaaS systems contain a large variety of data including personal information (such as payment details and travel logs), business data (such as costs, fees and service records) and other open data (including timetabling and service locations). For users, there is the risk that their personal information may be accessed by nefarious sources, resulting in issues related to both financial and personal safety. For mobility providers, there are concerns that intellectual property may be breached, resulting in their business losing competitive advantage and possible insider threat[51].

PETRAS in the UK Research Landscape

There are numerous research centres focused on IoT and cybersecurity related issues in the Transport and Mobility sector. A few notable ones include: (1) The Centre for Connected and Autonomous Vehicles (CCAV), established by the UK Government in 2015 and a joint entity between the Department for Business, Energy & Industrial Strategy (BEIS) and Department for Transport (DfT); (2) Zenzic, created by the UK government and industry to focus on the connected and self-driving sector, and to lead the move to a safer, more inclusive and productive mobile future; (3) Connected Places Catapult, operating at the intersection between the public and private sectors, local governments and transport authorities, and focusing on innovations in mobility services and the built environment that enable new levels of physical, digital and social connectedness; and (4) The Intelligent Mobility Design Centre (IMDC), established by the Royal College of Art in London and which conducts interdisciplinary research at the intersection of people, mobility and technology, in collaboration with business, academic, government and voluntary sector partners.

PETRAS has a strong, and expanding, research focus in the sector. There are a number of completed and on-going projects, detailed in Tables 1 and 2 below.

Table 1. Completed PETRAS projects in cybersecurity in Transport and Mobility

Project	Partners	Description	Industrial relevance
Privacy in Connected Autonomous Cars and Smart Transport Systems (P-CARS)	• Ordnance Survey; • Pinsent Masons; • TRL; • Thales	• Proposed and analysed effective solutions for preserving users' privacy during V2X communications	• Connected and Autonomous Vehicles
Transport and Mobility Demonstrator Audit (TMDA)	• Ordnance Survey	• Developed guidelines and policy recommendations for UK government and industry	• Transport Policy

Table 1. (continued) PETRAS projects in cybersecurity in Transport and Mobility

Project	Partners	Description	Industrial relevance
Smart Road and Street Maintenance, Pricing and Planning (RoadMaPP)	• Transport for London; • Smart Streets Hub; • InTouch Ltd; • Connect Plus Services; • Costain; • UK Power Networks; • JustPark	• Identified trust issues related to placing highways maintenance data into an IoT hub, looked at dynamic pricing in combined electric vehicle parking and charging markets, and developed efficient and scalable tools and algorithms to clean, integrate and analyse the vast amounts of heterogeneous, real-time data obtained from large-scale sensor deployment	• Transport Infrastructure; • Data Management
Blockchain Technology for IoT in Intelligent Transportation Systems (B-IoT)	• Ordnance Survey; • Wallet Services; • Telefonica • (Also, XAIN AG developed a pilot with Porche)	• Demonstrated the potential use of distributed ledgers, such as blockchain, as a method of securing the integrity of Intelligent Transportation Systems, such as autonomous vehicles	• Connected and Autonomous Vehicles; • Mobility as a Service; • Cybersecurity; • Supply Chain
Lightweight Security and Privacy for Geographic Personal Data and Location Based Services (GEOSEC)	• Ordnance Survey	• Analysed security and privacy related weaknesses of existing techniques for location, place and geography information delivery (such as personally identifiable information) and proposed secure and privacy-preserving solutions	• Connected and Autonomous Vehicles; • Mobility as a Service; • Cybersecurity; • Data Privacy
Designing Dynamic Insurance Policies using IoT (DDIP-IoT)	• Supported by Lloyd's Register Foundation	• Explored how real-time adjustable insurance policies may be designed and managed using IoT technology	• Insurance
Internet of Things for Transport and Mobility (IoT-TRaM)	• University of Warwick; • University of Surrey; • University of Edinburgh; • Imperial College London; • Lloyd's Register Foundation • Ordnance Survey; • Costain; • Telefonica; • TRL; • Meridian; • Centre for Connected and Autonomous Vehicles (CCAV)	• Tested ground-breaking technology utilising distributed ledgers that could enable more private and secure V2V and V2I communications	• Connected and Autonomous Vehicles; • Cybersecurity; • Data Privacy

Table 2. Ongoing PETRAS projects in cybersecurity in Transport and Mobility

Project	Partners	Description	Industrial relevance
Multi-Perspective Design of IoT Cybersecurity in Ground and Aerial Vehicles (MAGIC)	• NPX Semiconductors • Blue Bear Systems Research Ltd	• Looks to achieve security and resilience for future vehicular systems	• Connected and Autonomous Vehicles; • Cybersecurity
AI for Key Management and Mitigating Attacks (AIKEMA)	• Telefonica	• Explores how machine learning approaches to automated key management within the transport sector may help to manage network load and intrusion detection.	• Connected and Autonomous Vehicles; • Mobility as a Service; • Cybersecurity; • Data Management

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Glossary

AI (Artificial Intelligence) is “the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages”[52]

Denial of Service “describes the ultimate goal of a class of cyber attacks designed to render a service inaccessible”[53]

ITS (Intelligent Transport Systems) are “a combination of Information Technology and telecommunications, allowing the provision of on-line information in all areas of public and private administration”[54]

ML (Machine Learning) is “the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data”[55]

OEM is the Original Equipment Manufacturer, a company that manufactures and sells products or parts of a product that their buyer, another company, sells to its own customers while putting the products under its own branding[56]

OTA (Over-the-Air) update is ““wireless transmission of information often used to deliver software, firmware or configuration updates”[57]

RSU (Road-Side Unit) is a computing device located on the roadside that provides connectivity support to passing vehicles[58]

V2I (Vehicle-to-Infrastructure) is data that is shared between vehicles and infrastructure

V2V (Vehicle-to-Vehicle) is data that is shared between vehicles.

V2X (Vehicle-to-Everything) is data that is shared between vehicles and infrastructure

End Notes

[1] MarketsandMarkets, “Smart Transportation Market,” MarketsandMarkets, Jul. 2020. https://www.marketsandmarkets.com/Market-Reports/smart-transportation-market-692.html (accessed Feb. 08, 2021).

[2] MetroPlan Orlando, “CAV Readiness Study,” MetroPlan Orlando, Jul. 2019. https://metroplanorlando.org/programs-resources/transportation-system-management-operations/cav-readiness-study/ (accessed Jan. 21, 2021).

[3] M. Enoch, “Mobility as a Service (MaaS) in the UK: change and its implications,” Government Office for Science, London, Dec. 2018. Accessed: Jan. 25, 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/766759/Mobilityasaservice.pdf.

[4] Transport Committee, Mobility as a Service. London: House of Commons, 2018.

[5] Deloitte, Cybersecurity for Connected and Autonomous Vehicles: Considerations and opportunities for growth. Deloitte LLP & Ontario Centres of Excellence, 2019.

[6] Accenture, Autonomous Vehicles: The Race Is On. 2018.

[7] IEEE, “Real-Life Use Cases for Edge Computing,” IEEE Innovation at Work, 2019. https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/ (accessed Jan. 29, 2021).

[8] H. Khayyam, B. Javadi, M. Jalili, and R. N. Jazar, “Artificial Intelligence and Internet of Things for Autonomous Vehicles,” in Nonlinear Approaches in Engineering Applications: Automotive Applications of Engineering Problems, R. N. Jazar and L. Dai, Eds. Cham: Springer International Publishing, 2020, pp. 39–68.

[9] J. Bullas, T. Andriejauskas, P. D. Sanders, and M. J. Greene, “The relationship between connected and autonomous vehicles, and skidding resistance: A literature review,” TRL Limited, London, PPR962, Jul. 2020. Accessed: Jan. 29, 2021. [Online]. Available: https://trl.co.uk/uploads/trl/documents/PPR962---CAVs-and-skidding-resistance---literature-review.pdf.

[10] Gartner, “Gartner Predicts Outdoor Surveillance Cameras Will Be Largest Market for 5G Internet of Things Solutions Over Next Three Years,” Gartner, Oct. 2019. https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be (accessed Jan. 29, 2021).

[11] J. Sanders, “Why 5G is a crucial technology for autonomous vehicles,” ZDNet, Nov. 2019. https://www.zdnet.com/article/why-5g-is-a-crucial-technology-for-autonomous-vehicles/ (accessed Jan. 29, 2021).

[12] GDPR.EU, “What is GDPR, the EU’s new data protection law?,” GDPR.EU, 2019. https://gdpr.eu/what-is-gdpr/ (accessed Feb. 15, 2021).

[13] LexisNexis, “Autonomous and connected vehicles—data protection and privacy issues,” LexisNexis, n.d. https://www.lexisnexis.co.uk/legal/guidance/autonomous-connected-vehicles-data-protection-privacy-issues (accessed Feb. 15, 2021).

[14] EDPB, Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. EDPB, 2020.

[15] J. Pieriegud, Digital Transformation of Railways. Poland: Siemens, 2018.

[16] European Commission, “Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability and responsibility,” European Union, Luxembourg, EO3659, Jun. 2020. Accessed: Jan. 29, 2021. [Online]. Available: https://ec.europa.eu/info/sites/info/files/research_and_innovation/ethics_of_connected_and_automated_vehicles_report.pdf.

[17] ENISA, ENISA Good Practices For Security Of Smart Cars. Greece: ENISA, 2019.

[18] R. van Hooijdonk, “The race is on to protect trains, planes, and ships from devastating cyber-attacks,” Nov. 2019. https://blog.richardvanhooijdonk.com/en/the-race-is-on-to-protect-trains-planes-and-ships-from-devastating-cyber-attacks/ (accessed Jan. 29, 2021).

[19] M. Niestadt, A. Debyser, D. Scordamaglia, and M. Pape, Artificial intelligence in transport: Current and future developments, opportunities and challenges. European Parliament, 2019.

[20] J. Harb, “Challenges of the Autonomous Train,” Mar. 2019. https://blog.irt-systemx.fr/challenges-of-the-autonomous-train/ (accessed Jan. 29, 2021).

[21] Aerospace Manufacturing, “Enhancing cybersecurity for aircraft systems,” Aerospace Manufacturing, Nov. 2020. https://www.aero-mag.com/enhancing-cybersecurity-for-aircraft-systems/ (accessed Jan. 29, 2021).

[22] R. Harwood, “The Challenges to Developing Fully Autonomous Drone Technology,” Ansys, Nov. 2019. https://www.ansys.com/blog/challenges-developing-fully-autonomous-drone-technology (accessed Jan. 29, 2021).

[23] E. Schafer, “Collision Avoidance System: What it is and how it works,” Iris Automation, Dec. 2020. https://www.irisonboard.com/collision-avoidance-system-what-it-is-and-how-it-works/ (accessed Jan. 29, 2021).

[24] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, “Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs,” IEEE Wireless Communications, vol. 26, no. 1, pp. 28–35, Feb. 2019, doi: 10.1109/MWC.2018.1800155.

[25] Department for Transport, Aviation Cyber Security Strategy. London: Department for Transport, 2018.

[26] N. Hasratyan et al., ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea. WG3 I Sectoral Demand. European Cyber Security Organisation, 2020.

[27] H. Boyes and R. Isbell, Code of Practice: Cyber Security for Ships. London: Institution of Engineering and Technology, 2017.

[28] Rolls-Royce, Remote and Autonomous Ships: The Next Steps. Rolls-Royce, 2016.

[29] MaaS Alliance, Main challenges associated with MaaS & Approaches for overcoming them. MaaS Alliance, 2019.

[30] CCAV, Innovation is great: connected and automated vehicles. London: HM Government, 2020.

[31] Department for Transport, The Pathway to Driverless Cars: A Code for Practice for Testing. London: Department for Transport, 2015.

[32] CCAV, Department for Business, Energy & Industrial Strategy, and Department for Transport, "Code of Practice: Automated vehicle trialling," GOV.UK, Feb. 2019. https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling (accessed Jan. 27, 2021).

[33] Department for Transport, CCAV, and G. Freeman, "New system to ensure safety of self-driving vehicles ahead of their sale," GOV.UK, Sep. 2019. https://www.gov.uk/government/news/new-system-to-ensure-safety-of-self-driving-vehicles-ahead-of-their-sale (accessed Jan. 27, 2021).

[34] World Economic Forum, Safe Drive Initiative: Creating safe autonomous vehicle policy. World Economic Forum, 2020.

[35] BSI, "CAV Resources," BSI, 2021. https://www.bsigroup.com/en-GB/CAV/cav-resources/ (accessed Jan. 27, 2021).

[36] Connected Places Catapult, "The CertiCAV Safety Assurance Framework for CAVs: Consultation Workshop," Connected Places Catapult, 2020. https://cp.catapult.org.uk/event/the-certicav-safety-assurance-framework-for-cavs-consultation-workshop/ (accessed Jan. 27, 2021).

[37] KPMG, 2020 Autonomous Vehicles Readiness Index. KPMG International, 2020.

[38] CCAV, Centre for the Protection of National Infrastructure, and Department for Transport, The key principles of vehicle cyber security for connected and automated vehicles. London: HM Government, 2017.

[39] BSI, "PAS 1885:2018," BSI, 2018. https://shop.bsigroup.com/ProductDetail?pid=000000000030365446&_ga=2.193450349.139025177.1611758741-1079891664.1611519891 (accessed Jan. 27, 2021).

[40] C. Grayling and L. Sugg, Automated and Electric Vehicles Act 2018. 2018.

[41] J. Bond, "AUTOMATED AND ELECTRIC VEHICLES ACT 2018 BECOMES LAW," Penningtons Manches Cooper, Jul. 2018. https://www.penningtonslaw.com/news-publications/latest-news/2018/automated-and-electric-vehicles-act-2018-becomes-law#:~:text=The%20Automated%20and%20Electric%20Vehicles,Royal%20Assent%20on%2019%20July.&text=The%20purpose%20of%20this%20legislation,hydrogen%20powered%20vehicle%20charging%20infrastructure. (accessed Jan. 27, 2021).

[42] S. Baker, "How UK law is adapting to cope with autonomous vehicles," The IET, May 27, 2020. https://eandt.theiet.org/content/articles/2020/05/how-uk-law-is-adapting-to-cope-with-autonomous-vehicles/ (accessed Jan. 28, 2021).

[43] Transport Data Initiative, Mobility as a Service (MaaS) for Local Authorities. London: Transport Data Initiative, 2019.

[44] Department for Transport, Future of Mobility: Urban Strategy. London: Department for Transport, 2019.

[45] Department for Transport, Future of Transport Regulatory Review: Summary of Responses. London: Department for Transport, 2020.

[46] European Commission, Connected and Automated Transport. Brussels: European Commission, 2017.

[47] L. Mora, X. Wu, and A. Panori, "Mind the gap: Developments in autonomous driving research and the sustainability challenge," J Clean Prod, vol. 275, pp. 124087–124087, Dec. 2020, doi: 10.1016/j.jclepro.2020.124087.

[48] R. Merkert and J. Bushell, "Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control," J Air Transp Manag, vol. 89, pp. 101929–101929, Oct. 2020, doi: 10.1016/j.jairtraman.2020.101929.

[49] H. Ghaderi, "Chapter Eleven - Wider implications of autonomous vessels for the maritime industry: Mapping the unprecedented challenges," in Advances in Transport Policy and Planning, vol. 5, D. Milakis, N. Thomopoulos, and B. van Wee, Eds. Academic Press, 2020, pp. 263–289.

[50] R. Claassen, "Autonomous Transport: Trains and Boats and Planes," Jun. 2019. https://www.smart-industry.net/autonomous-transport-trains-and-boats-and-planes/ (accessed Jan. 29, 2021).

[51] L. Butler, T. Yigitcanlar, and A. Paz, "Barriers and risks of Mobility-as-a-Service (MaaS) adoption in cities: A systematic review of the literature," Cities, vol. 109, p. 103036, 2021, doi: https://doi.org/10.1016/j.cities.2020.103036.

[52] Lexico, "Artificial Intelligence," Lexico, n.d. https://www.lexico.com/definition/artificial_intelligence (accessed Feb. 14, 2021).

[53] NCSC, "Denial of Service (DoS) Guidance," National Cyber Security Centre, Nov. 2020. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection (accessed Feb. 14, 2021).

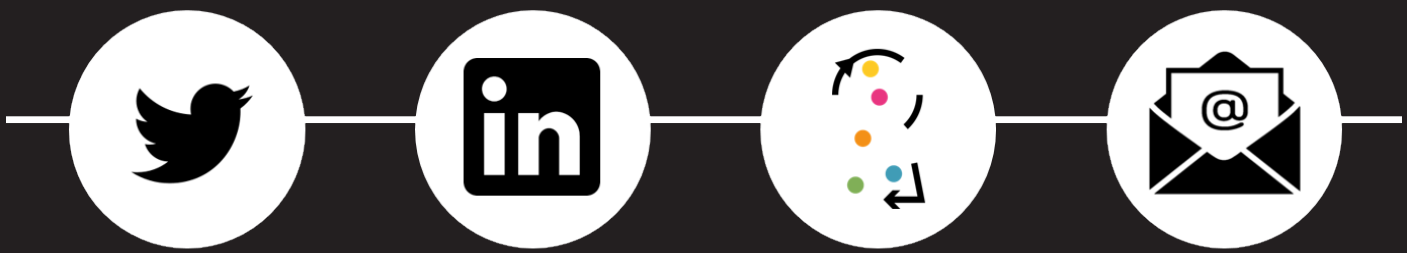
[54] ITS UK, "What is ITS?," ITS UK, n.d. https://its-uk.org.uk/about-its-uk/ (accessed Feb. 14, 2021).

[55] Lexico, "Machine Learning," Lexico, n.d. https://www.lexico.com/definition/machine_learning (accessed Feb. 14, 2021).

[56] CFI (2020) Original Equipment Manufacturer (OEM) - Definition, Example, Benefits, Corporate Finance Institute. Available at: https://corporatefinanceinstitute.com/resources/knowledge/other/original-equipment-manufacturer-oem/ (Accessed: 22 April 2021).

[57] BSI (n.d.) Over-the-air (OTA), BSI. Available at: https://www.bsigroup.com/en-GB/CAV/cav-vocabulary/over-the-air/ (Accessed: 23 April 2021).

[58] IGI Global, "What is Roadside Unit (RSU)," IGI Global, n.d. https://www.igi-global.com/dictionary/roadside-unit-rsu/37000#:~:text=1.,Wireless%20Networks%20for%20Vehicular%20Support (accessed Feb. 10, 2021).



TWITTER
@PETRASiot

LINKEDIN
linkedin.com/
school/petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.ac.uk