Unite response to Department for Transport call for evidence on Developing the Automated Vehicles Regulatory Framework

Executive Summary and Introduction

1. Introduction

1.1. This submission is made by Unite the Union, the UK's largest trade union with over one million members across all sectors of the economy, including: manufacturing, financial services, transport, food and agriculture, construction, energy and utilities, information technology, service industries, health, local government, and the not-for-profit sector.

1.2. Of particular interest to this consultation is membership of more than a quarter of a million workers in all forms of transport. Over 60,000 Unite members are in the road freight, haulage, and warehousing industry while another 75,000 are in passenger transport, including bus and tram drivers and drivers in the taxi and private hire sector. Additionally, Unite represents almost 60,000 members in the automotive manufacturing sector.

1.3. Unite's transport members undertake roles that will be heavily impacted by any potential rollout of automatic vehicles. These include:

- professional drivers, including HGV and bus drivers
- warehouse and logistics workers, including forklift operators
- drivers in the taxi and private hire sector
- vehicle engineers and technicians
- vehicle maintenance, delivery, and disposal workers
- workers across the wider supply chain.

1.4. Workers in these roles will be among the first to work with, alongside, or in proximity to Automated Vehicles (AVs). They will also be among the first to face the consequences if the regulatory framework is weak, fragmented, or designed around commercial priorities rather than public safety and worker protection.

1.5. Unite agrees that the Automated Vehicles (AV) Act 2024 has the potential to provide a foundation for safe deployment of AVs in Great Britain. However, the Act's success will depend entirely on the strength of the secondary legislation, licensing regimes, and regulatory systems now being developed.

1.6. This submission addresses relevant questions to our membership and the communities they live in. The baseline principles underlying our response - and on all issues relating to automation - can be summarised as:

Automation must raise standards — not lower them

The benefits of new technologies and increased productivity must be shared with workers — not used to replace them

The UK must lead the world in safe, worker-centred regulation.

2. Ensuring the workplace rights and protections of the UIC

2.1. The User-in-Charge (UIC) of a crewed AV is a worker that requires stringent protections. These must include, but may not be limited to:

2.1.1. Strict limits on the non-driving activities of the UIC.

2.1.2. Mandatory, recurrent UIC training.

2.1.3. A 12-15 second transition period when switching between automatic and UIC operated modes.

2.1.4. Full pay and working protections for the worker weather they are driving, supervising, or undertaking remate operations of an AV.

2.1.5. Strict user-to-vehicle staffing ratios, ranging from 1:3 to 1:1 depending on the complexity of the environment.

2.2. Unite members in the transport industry have seen the impact of “gig economy” style employment practices and reject entirely the race to the bottom this would impose on pay, conditions, and health and safety standards. All AV operations must have direct and transparent employment models where the worker is treated as a worker and protected by full employment law and access to collective bargaining.

2.3. In addition to upholding employment rights and protections, proper relations of employment are vital for preventing the erosion of important safety standards, for example in the HGV sector, developed through years of engagement and bargaining between employers and unions.

2.4. Operations centres from which remote driving takes place, for example by No-User-in-Charge-Operators (NUICOs), must be UK based. Unite is firmly opposed to the offshoring of AV control, in particular for safety critical work.

2.5. The UIC must ***never*** be held liable for Automatic Driving Systems (ADS) driven behaviour. Liability for vehicle behaviour when under automatic control must lie with either the NUICO, the Authorised Self-Driving Entity (ASDE), or the legal owner of the vehicle.

3. Automatic Vehicle maintenance

3.1. ADS diagnostics cannot replace human inspection. AV maintenance plans must incorporate DVSA daily walk-around checks.

4. Licensing and insurance

4.1. Unite supports a rigorous licensing process for NUICOs. At minimum this should include strict good-repute and financial-standing tests for potential licence holders. Substantive employers must ensure thorough inspection of licencing when employing subcontractors.

4.2. Unite reiterates our strong opposition to offshoring, including on the grounds of ensuring valid licencing.

4.3. Licence holders should have TUPE style protections and the right to union consultation ahead of major changes to their employment.

4.4. Unite supports mandatory data sharing for insurance clams, but with strict limits on insurer access to personal information. Unite also believes it is very likely that new insurance products will be required for NUIC operations.

4.5. ADS related incidents should not impact the standing of UICs from an insurance point of view and should not form part of their insurance records.

5. Cyber security

5.1. Unite supports mandatory cyber security certification, strict reporting timelines, and clear responsibilities for ASDEs, NUICOs, and manufacturers.

6. In-use regulation, accessibility, and environmental standards

6.1. Unite supports real-time data access for regulators and mandatory reporting of all incidents and near-misses.

6.2. We know that, especially in the case of large, cash-rich employers, fixed fines can be viewed as “the price of doing business”. Therefore, breaches of AV regulations must result in turnover-based fines.

6.3. The DVSA, Office of Rail and Road and/or any other responsible agency must have strong enforcement powers to uphold regulation. Employers adopting ADS technologies must be subject to regular inspection and independent auditing, especially in the early stages of the rollout of this new technology.

6.4. Cabin design of ADS enabled vehicles must still account for comfortable and safe human access and operation. These standards must be strengthened with appropriate safeguarding protocols for UICs.

6.5. Appropriate consideration must be given to safe and sustainable end of life disposal of AVs.

7. Conclusions

7.1. The UK has an opportunity to lead the world in Automated Vehicle regulation, but only if the framework is built on the principles of safety, transparency, worker protection, public trust, strong enforcement, clear accountability, and no compromise on labour standards

7.2. Automation must not be used to cut corners, reduce staffing, offshore safety-critical work, weaken pay and conditions, or undermine existing safety regimes. Instead, automation must raise standards, improve safety, create high-quality jobs, and strengthen the UK’s transport and logistics sectors.

7.3. Unite stands ready to work with government, regulators, and industry to ensure that automated vehicles are introduced safely, responsibly, and in a way that protects workers and the public.

7.4. Unite is clear that the risks identified in this submission relate specifically to the expansion of **corporate-owned automated vehicle fleets**, not individual private ownership of automated cars. Unite emphasises that nothing in this submission conflicts with or complicates plans to bring public transport into public ownership. On the contrary, the regulatory standards proposed here —

around safety, transparency, workforce protections, accessibility, and accountability — are fully compatible with, and in many cases strengthened by, publicly owned and democratically accountable transport services.

Response to consultation questions

Question 1: Do you think that amendments are required to any of the vehicle type approval schemes to enable deployment of AVs?

Unite response:
Yes. Amendments are required to ensure that type approval reflects the unique safety, cyber-security, and operational risks of automated vehicles, particularly in commercial and passenger-carrying contexts.

Unite recommends that the UK:

- strengthen cyber-security requirements beyond UNECE baselines;
- require type approval to consider human–machine interaction (HMI) safety;
- mandate safety-critical redundancy for braking, steering, and communications;
- require type approval to consider remote-operation interfaces and failure modes;
- ensure that type approval explicitly covers load-security monitoring for goods vehicles.

The UK should exceed EU and UNECE standards to protect workers and the public.

Question 2: What amendments do you consider are needed for the categories identified in the previous question, and why?

Unite response:
Amendments should include:

1. Category M (passenger vehicles)

- mandatory cabin-monitoring systems for NUIC passenger services;
- accessibility-focused design requirements;
- enhanced fire-safety and evacuation standards.

2. Category N (goods vehicles)

- mandatory load-security sensors;
- automated weight-distribution monitoring;

- enhanced braking redundancy for heavy vehicles.

3. Category L (light vehicles)

- stricter stability and sensor-placement requirements;
- mandatory geofencing for micromobility AVs.

4. Cross-category requirements

- cyber-security certification;
- remote-operation safety validation;
- mandatory data-logging (DSSAD + EDR).

These amendments ensure that type approval reflects real-world risks and protects workers and the public.

Question 3: What do you think will be the designs of self-driving vehicles deployed in the next 5 years?

Unite response:
Likely designs include:

- automated shuttles and pods for short-distance passenger transport;
- depot-to-depot automated HGVs;
- last-mile delivery robots and small goods vehicles;
- automated vans for logistics and parcel delivery;
- passenger cars with limited ODDs (motorway-only ADS).

These designs reflect commercial priorities in logistics, mobility, and fleet operations.

Question 4: Do you expect any designs to be specific to the UK, and why?

Unite response:
Yes. UK-specific designs may emerge due to:

- narrow, complex urban road layouts;
- high pedestrian density;
- legacy infrastructure;
- left-hand-traffic requirements;
- unique bus and taxi operating environments.

This will particularly affect automated buses, shuttles, and delivery vehicles.

Question 5: What do you think will be the use-cases of self-driving vehicles deployed in the next 5 years in the UK?

Unite response:
Likely use-cases include:

- last-mile parcel delivery;
- depot-to-depot freight movement;
- automated shuttle services;
- automated taxis in geofenced areas;
- yard, port, and warehouse automation;
- motorway-only ADS for private cars.

These use-cases reflect commercial viability and controlled-environment deployment.

Question 6: Do you expect any use-cases to be specific to the UK, and why?

Unite response:
Yes. UK-specific use-cases include:

- automated buses in dense urban environments;
- automated vehicles operating in historic city centres;
- integration with UK-specific logistics hubs (ports, rail freight terminals);
- automated vehicles supporting rural mobility gaps.

These reflect the UK's unique transport mix and infrastructure.

Question 7: What types of evidence should form the basis of an authorisation application?

Unite response:
Authorisation must require:

- independent safety case assessment;
- real-world testing data;
- simulation evidence;

- cyber-security validation;
- human-factors analysis;
- transition-demand performance data;
- remote-operation safety evidence;
- worker-safety impact assessment.

The UK should exceed existing international standards by requiring **independent auditing** of safety cases.

Question 8: What evidence gathered at the type approval stage should support authorisation?

Unite response:
Relevant evidence includes:

- ADS performance validation;
- sensor performance and redundancy;
- braking and steering safety;
- cyber-security certification;
- DSSAD/EDR compliance.

However, authorisation must not rely solely on type approval. It must include **operational safety evidence**.

Question 9: Do geofencing or environmental mapping have a role in ODD approval?

Unite response:
Yes. Geofencing and mapping are essential for:

- ensuring ADS operation only within safe environments;
- preventing ODD breaches;
- enabling regulator oversight;
- supporting incident investigation.

The UK should require **mandatory geofencing** for all NUIC deployments.

Question 10: Are there specific authorisation requirements relating to the vehicle that should or should not be included?

Unite response:
Should include:

- mandatory ODD boundary detection;
- load-security monitoring for goods vehicles;
- cabin-monitoring for passenger vehicles;
- cyber-security certification;
- redundant braking and steering;
- mandatory DSSAD + EDR.

Should not include:

- self-certification without independent audit;
- reliance on manufacturer-defined safety metrics.

Question 11: What should be considered when assessing whether an ASDE is of good repute?

Unite response:
Good repute must include:

- clean safety record;
- no history of misleading regulators;
- compliance with labour standards;
- no union-busting;
- transparent global operations.

The UK should exceed existing international standards by embedding **labour-standards compliance**.

Question 12: What should be considered when assessing whether an ASDE is of good financial standing?

Unite response:
Financial standing must include:

- ability to fund lifetime software updates;
- cyber-security investment;

- insurance coverage;
- audited accounts;
- capital reserves proportionate to fleet size.

Question 13: What should be considered when assessing whether an ASDE is competent?

Unite response:
Competence must include:

- a documented safety management system;
- qualified safety engineers;
- human-factors expertise;
- cyber-security capability;
- incident-response capability;
- union-consulted workforce policies.

Question 14: Are there other ASDE authorisation requirements that should or should not be included?

Unite response:

Unite recommends that a mandatory Worker Impact Assessment (WIA) be included as part of the authorisation process for any automated vehicle system. The introduction of AV technology has significant implications for workers in safety-critical roles, including drivers, remote operators, maintenance staff, and logistics workers. A WIA must therefore be required to be produced by the ASDE before any ADS is authorised for use. This assessment should cover:

- impacts on job roles, staffing levels, and employment security;
- training and retraining requirements;
- redeployment pathways and protections against compulsory redundancy;
- equality impacts on older, disabled, migrant, and lower-paid workers;
- risks of casualisation, gig-economy models, or offshoring of safety-critical; work
- impacts on collective bargaining, union access, and workforce consultation;
- health, safety, and fatigue implications for UICs and remote operators.

The WIA must be submitted alongside the safety case and reviewed by the regulator with input from recognised trade unions. No ADS should be authorised unless the operator demonstrates that workforce impacts have been fully assessed, mitigated, and addressed through negotiated plans with unions. This ensures that automation raises standards rather than undermining jobs, safety, or employment conditions.

Question 15: What additional information should be captured on the register of authorisations?

Unite response:
The register should include:

- ODD details;
- safety case summaries;
- ASDE identity;
- NUICO identity (if applicable);
- incident history;
- sanctions history;
- software version history.

Question 16: How might you expect to use the information in the register?

Unite response:
Unite would use the register to:

- monitor safety performance;
- support worker safety campaigns;
- identify high-risk operators;
- inform collective bargaining;
- support public transparency.

Question 17: What should be considered when developing the authorisation procedure?

Unite response:
The procedure must be:

- transparent;

- independent;
- auditable;
- worker-centred;
- proportionate but rigorous.

It must avoid “rubber-stamping” and ensure meaningful scrutiny.

Question 18: Are there lessons from other regulated areas?

Unite response:
Yes. Lessons from:

- aviation certification;
- rail safety cases;
- HGV operator licensing;
- nuclear safety regulation.

Key principles:

- independent oversight;
- no self-certification;
- mandatory reporting;
- strong enforcement.

Question 19: What processes should ensure authorised vehicles continue to meet the safety standard?

Unite response:
Processes must include:

- annual safety case updates;
- mandatory updates after software changes;
- independent audits;
- real-time data access for regulators;
- mandatory reporting of all incidents and near-misses.

Question 20: How should software or functionality changes be managed?

Unite response:
Software changes must require:

- mandatory notification;
- safety case re-evaluation;
- reauthorisation for major changes;
- worker retraining;
- regulator approval before deployment.

Question 21: What costs should be considered when assessing authorisation standards?

Unite response:
Legitimate costs:

- safety case development;
- cyber-security;
- training;
- data retention;
- independent audits.

Costs that must **not** justify deregulation:

- avoiding labour protections;
- offshoring safety-critical work;
- reducing staffing.

Question 22: What benefits should be considered when assessing authorisation standards?

Unite response:
Benefits include:

- improved road safety;
- reduced collisions;
- stronger public trust;

- high-quality jobs;
- protection of existing logistics roles;
- improved regulatory transparency.

Question 23: Should any existing prohibitions on non-driving related activity by a UIC be disapplied?

Unite response:
No. Unite strongly opposes relaxing prohibitions on non-driving activities for UICs.

A UIC is in a **safety-critical standby role**, comparable to:

- a pilot during automated flight,
- a train driver under ATO,
- an HGV driver using advanced driver-assistance systems.

Human-factors evidence shows that distraction significantly increases takeover time and reduces situational awareness. Allowing additional non-driving activities would undermine safety and expose workers to unfair liability.

Unite therefore supports:

- **continuing the ban on mobile phone use**,
- **prohibiting reading, video watching, and other distracting activities**,
- **treating UIC time as working time**, with full pay and protections.

The UK should match and exceed Germany's and any other restrictions.

Question 24: What evidence can you supply on the ability of a driver to safely resume control after disengagement?

Unite response:
Human-factors research across aviation, automotive, and rail shows:

- drivers require **10–15 seconds** to regain situational awareness after disengagement;
- takeover time increases with distraction, fatigue, or cognitive load;
- poorly designed alerts significantly increase takeover failures.

This supports strict limits on UIC activities and longer transition periods.

Question 25: Should there be specific training for a UIC?

Unite response:
Yes. UICs must receive mandatory, nationally standardised training that:

- exceeds Driver CPC;
- covers ADS limitations and failure modes;
- includes emergency procedures;
- includes transition-demand management;
- includes legal responsibilities;
- includes human-factors awareness.

Question 26: What knowledge and skills outcomes should UIC training provide?

Unite response:
Training must ensure UICs can:

- understand ADS capabilities and limitations;
- recognise system failures;
- respond to transition demands;
- manage emergency situations;
- maintain vigilance;
- understand legal responsibilities and protections;
- operate safely in mixed-traffic environments.

Question 27: How frequently should UICs undertake training or tests?

Unite response:
Unite recommends:

- **annual recurrent training**;
- mandatory retraining after software updates;
- mandatory retraining after incidents or near-misses;
- periodic medical assessments equivalent to HGV/PCV standards.

Question 28: How should a UIC be informed of changes to the vehicle's authorisation?

Unite response:
UICs must be informed through:

- mandatory in-vehicle notifications;
- mandatory written communication from the ASDE/NUICO;
- mandatory training updates for safety-critical changes;
- clear, accessible language.

No UIC should ever be placed in a position where they unknowingly operate outside the authorised ODD.

Question 29: What costs should be considered when assessing UIC regulation?

Unite response:
Legitimate costs include:

- training and certification;
- medical assessments;
- system design for safe transitions;
- cyber-security;
- data retention;
- independent audits.

Costs that must **not** justify deregulation:

- avoiding labour protections;
- reducing staffing;
- offshoring safety-critical work.

Question 30: What benefits should be considered when assessing UIC regulation?

Unite response:
Benefits include:

- improved road safety;
- reduced collisions;

- stronger public trust;
- high-quality, safety-critical jobs;
- protection of existing logistics roles;
- clear liability protections for workers.

Question 31: Should there be a stated value for a transition period duration?

Unite response:
Yes. The UK should adopt a **minimum transition period of 10 seconds**, aligned with UNECE R157, but exceed it by setting:

- **12–15 seconds as the default**,
- longer periods in complex environments.

This reflects human-factors evidence and exceeds Germany's approach.

Question 32: What should the minimum value be, and why?

Unite response:
12–15 seconds, because:

- drivers require 10–15 seconds to regain situational awareness;
- shorter periods increase takeover failures;
- complex environments require longer reaction times.

Question 33: Should different scenarios require different transition demand protocols?

Unite response:
Yes. Transition demands must be scenario-specific, reflecting:

- urban vs motorway environments;
- weather conditions;
- traffic density;
- load type (for goods vehicles);
- passenger presence.

This mirrors aviation and rail safety practice.

Question 34: Should the nature of a transition demand vary depending on the UIC?

Unite response:
Yes. Alerts must be accessible to all potential UICs, including disabled UICs. This requires:

- multimodal alerts (visual, auditory, haptic);
- adjustable volume and brightness;
- compatibility with assistive technologies.

Question 35: Should standards be established for transition demand interfaces across different vehicle makes and models?

Unite response:
Yes. The UK should mandate **industry-wide standardisation**, including:

- consistent alert tones;
- consistent visual indicators;
- consistent haptic feedback;
- consistent terminology.

This reduces cognitive load and improves safety.

Question 36: What should be considered when assessing whether a NUICO licence applicant is of good repute?

Unite response:
Good repute must include:

- a clean safety record;
- no history of misleading regulators;
- compliance with labour standards;
- no use of gig-economy models for safety-critical roles;
- no union-busting or anti-worker practices;
- transparent global operations;
- no history of cyber-security negligence.

The UK should exceed all existing international standards by embedding **labour-standards compliance** into the definition of good repute.

Question 37: What should be considered when assessing whether a NUICO licence applicant is of good financial standing?

Unite response:
Financial standing must include:

- sufficient capital to maintain safe operations;
- ability to fund lifetime software updates;
- cyber-security investment;
- insurance coverage for ADS and remote-operation failures;
- audited accounts;
- reserves proportionate to fleet size.

Financial standing must not be used to justify cost-cutting that undermines safety or workers' rights.

Question 38: What capabilities should NUICOs possess to detect problems during NUIC journeys?

Unite response:
NUICOs must have:

- real-time monitoring of every NUIC vehicle;
- automated alerts for ADS failures, ODD breaches, and sensor degradation;
- load-security monitoring for goods vehicles;
- cabin-monitoring for passenger vehicles;
- cyber-security intrusion detection;
- redundant communications channels.

The UK should require from **1:1 to 1:3 maximum monitoring ratios** in complex environments.

Question 39: What capabilities should NUICOs possess to respond to problems during NUIC journeys?

Unite response:
NUICOs must be able to:

- dispatch support vehicles;
- communicate with emergency services;

- provide remote ADS assistance;
- initiate safe stops;
- support passengers in distress;
- manage cyber-security incidents;
- secure loads and protect the public.

This must be backed by **24/7 staffed operations centres**.

Question 40: If you may seek to operate NUIC passenger-carrying vehicles in the future, what kind of service and types of vehicles would you be most likely to operate?

Unite response:
Not applicable to Unite as an operator.
However, Unite represents workers who will interact with these systems and therefore supports strong safety and safeguarding requirements.

Question 41: What requirements should be put in place for NUIC passenger vehicles?

Unite response:
The UK should exceed Germany by requiring:

- real-time cabin monitoring;
- panic buttons;
- safeguarding officers in operations centres;
- enhanced DBS checks for remote staff;
- accessibility-compliant interiors;
- mandatory reporting of passenger-safety incidents.

Question 42: How should operators and authorities prevent and respond to crimes in NUIC passenger vehicles?

Unite response:
Unite recommends:

- real-time cabin monitoring;
- automatic alerts for violent or unsafe behaviour;
- integration with police systems;

- mandatory safeguarding protocols;
- trained remote staff;
- clear passenger reporting mechanisms.

NUIC passenger vehicles must not become unmonitored spaces.

Question 43: If you may seek to operate NUIC goods vehicles in the future, what kind of service and types of vehicles would you be most likely to operate?

Unite response:
Not applicable to Unite as an operator.
However, Unite represents logistics workers and therefore supports strong protections for load security and worker safety.

Question 44: If you may seek to operate NUIC goods vehicles over 3.5 tonnes in the future, is it likely you will operate both NUIC goods vehicles and manually driven HGVs?

Unite response:
Not applicable to Unite as an operator.
However, Unite emphasises that NUIC operations must not undercut HGV standards or fragment the workforce.

Question 45: What HGV operator licensing requirements should be disapplied or amended for NUIC HGVs?

Unite response:
None should be disapplied.
Instead, the UK should:

- apply all HGV operator licensing standards;
- add additional NUICO-specific requirements;
- prohibit undercutting of pay and conditions;
- mandate TUPE-style protections;
- require load-security monitoring.

NUIC must not become a loophole to weaken HGV safety or labour standards.

Question 46: What remote ADS assistance tasks are likely to be used?

Unite response:
Likely tasks include:

- object identification;
- route clarification;
- resolving ADS uncertainty;
- interpreting unusual road layouts;
- supporting emergency manoeuvres (without taking control).

These tasks must never replace ADS capability or compensate for inadequate system design.

Question 47: When is remote ADS assistance appropriate?

Unite response:
Only when:

- the ADS retains full responsibility;
- communications are stable and redundant;
- the situation is low-risk;
- the operator is trained and certified;
- the intervention is logged and auditable.

Question 48: When is remote ADS assistance inappropriate?

Unite response:
Remote ADS assistance must not be used:

- in high-risk environments;
- when communications are degraded;
- to compensate for poor ADS performance;
- when passengers are in distress;
- when load stability is compromised.

Question 49: What training and vetting should remote ADS assistants receive?

Unite response:
Training must include:

- aviation-style recurrent training;
- human-factors awareness;

- cyber-security training;
- safeguarding training;
- medical and fatigue assessments;
- enhanced DBS checks.

Question 50: What working-hours requirements should apply to remote ADS assistants?

Unite response:
Remote ADS assistants must be covered by:

- HGV/PCV working-time limits;
- mandatory rest breaks;
- fatigue-risk management systems;
- full pay for all monitoring time.

Remote ADS assistance is a **safety-critical role** and must be regulated as such.

Question 51: What factors should determine how many NUIC vehicles a remote ADS assistant can support?

Unite response:
Factors include:

- environment complexity;
- vehicle type;
- load type;
- passenger presence;
- communications reliability;
- operator experience.

Unite recommends:

- **1:1 to 1:3** in complex environments;
- **1:5 maximum** in low-risk settings.

Question 52: How likely are you to incorporate remote driving?

Unite response:
Not applicable to Unite as an operator.

However, Unite strongly opposes routine remote driving due to safety, cyber-security, and labour-standards risks.

Question 53: When should remote driving be permissible for vehicle recovery?

Unite response:
Only when:

- the vehicle is immobilised;
- the environment is low-risk;
- speed is limited (e.g., <5 mph);
- communications are redundant;
- no passengers are on board;
- the remote driver is certified.

Question 54: When should remote driving be permissible during NUIC journeys?

Unite response:
Only in exceptional circumstances:

- ADS failure;
- emergency manoeuvres;
- unusual road layouts;
- obstructions requiring human judgement.

Never when:

- passengers are present,
- loads are unstable,
- communications are degraded.

Question 55: When should remote driving be permissible to routinely complete NUIC journeys?

Unite response:
Never.
Routine remote driving undermines:

- safety,

- cyber-security,
- labour standards,
- ADS capability requirements.

The UK should explicitly prohibit routine remote driving, exceeding existing international standards approach.

Question 56: What training and vetting should remote drivers receive?

Unite response:
Remote drivers must receive:

- simulator-based licensing;
- medical and fatigue assessments;
- cyber-security training;
- safeguarding training;
- enhanced DBS checks.

Question 57: What working-hours requirements should apply to remote drivers?

Unite response:
Remote drivers must be covered by:

- HGV/PCV working-time limits;
- mandatory rest breaks;
- fatigue-risk management systems;
- full pay for all monitoring and driving time.

Question 58: What considerations should be made when assessing remote driving hardware and software?

Unite response:
Assessment must include:

- latency and bandwidth requirements;
- redundant communications;
- ergonomic workstation design;

- cyber-security certification;
- fail-safe mechanisms;
- human-factors validation;
- independent testing.

The UK should require **independent certification** of remote-driving systems.

Question 59: What restrictions or mandatory conditions should be placed on NUICOs contracting out functions to third-party suppliers?

Unite response:
Contracting out NUICO functions introduces major risks: fragmentation, loss of accountability, offshoring, and erosion of labour standards. The UK must prevent NUICO licensing from becoming a loophole for unsafe or exploitative practices.

Unite recommends the following mandatory conditions:

1. NUICO retains full legal responsibility

No function may be outsourced in a way that dilutes accountability for safety, cyber-security, or regulatory compliance.

2. Licensing of subcontractors

Any subcontractor performing safety-critical functions must be:

- licensed;
- audited;
- held to the same standards as the NUICO.

3. Prohibition on offshoring safety-critical work

Remote operations, monitoring, and remote driving must **not** be performed outside the UK due to:

- cyber-security risks;
- latency issues;
- regulatory oversight limitations;
- labour-standards concerns.

4. TUPE-style protections

Workers must not be displaced by outsourcing.
Any transfer of functions must include:

- TUPE-equivalent protections;
- recognition of unions;
- continuity of pay and conditions.

5. Transparency of supply chains

NUICOs must disclose:

- all subcontractors;
- their roles;
- their locations;
- their safety records.

6. Union consultation

Any outsourcing of safety-critical functions must require:

- prior consultation with recognised unions;
- impact assessments on worker safety and employment.

Question 60: What costs should be considered when assessing the impact of NUICO regulation?

Unite response:
Legitimate costs include:

- staffing 24/7 operations centres;
- training remote operators and ADS assistants;
- cyber-security infrastructure;
- data retention and secure storage;
- independent audits;
- safety case development;
- cabin-monitoring and load-monitoring systems;
- communications redundancy.

Costs that must **not** justify deregulation:

- reducing staffing ratios,
- offshoring safety-critical work,
- using gig-economy models,

- cutting corners on cyber-security,
- weakening labour protections.

Question 61: What benefits should be considered when assessing the impact of NUICO regulation?

Unite response:
Benefits include:

- improved road safety;
- reduced collisions;
- stronger public trust;
- high-quality, safety-critical jobs;
- protection of existing logistics roles;
- prevention of workforce fragmentation;
- clear accountability for safety;
- reduced exploitation risks;
- better cyber-security resilience.

Strong NUICO regulation protects both workers and the public.

Question 62: How can insurance play a role in ensuring good financial standing of regulated bodies?

Unite response:
Insurance can demonstrate financial standing by ensuring that NUICOs and ASDEs can:

- meet compensation obligations;
- cover catastrophic risks;
- respond to cyber-security failures;
- fund product recalls;
- maintain business continuity;
- cover remote-operation errors.

The UK should require:

- product liability insurance;

- cyber-security insurance;
- remote-operation liability insurance;
- employer liability insurance;
- public liability insurance.

Question 63: What instances exist where insurance is used to ensure good financial standing?

Unite response:
Relevant examples include:

- product recall insurance in automotive manufacturing;
- cyber-security insurance in critical infrastructure;
- professional indemnity insurance in safety-critical industries;
- fleet insurance for logistics operators.

These demonstrate how insurance mitigates high-impact risks.

Question 64: What premiums are charged for product recall insurance?

Unite response:
Premiums vary widely depending on:

- fleet size;
- risk profile;
- manufacturer history;
- software complexity;
- cyber-security posture.

Unite emphasises that **higher premiums reflect higher risk** and must not be used as an argument for deregulation.

Question 65: Is there a need for new fleet management insurance products for NUICOs?

Unite response:
Yes. NUICOs require new insurance products covering:

- ADS liability;
- remote-operation liability;

- cyber-security breaches;
- data-loss and data-corruption;
- business interruption;
- remote-driving incidents.

Existing fleet insurance is not designed for:

- remote operations;
- cyber-physical systems;
- ADS-driven liability.

Question 66: What learnings from other insurance models could apply to AVs?

Unite response:
Relevant models include:

- aviation insurance (pilot error vs system failure);
- rail insurance (ATO/ATP incidents);
- maritime automation insurance;
- cyber-security insurance frameworks.

These sectors show the value of:

- independent investigation;
- clear liability chains;
- mandatory data retention;
- strong regulatory oversight.

Question 67: What risks and opportunities exist for data controllers in sharing data with insurers?

Unite response:

Opportunities:

- faster claims resolution;
- clearer liability;
- improved safety modelling;

- reduced fraud.

Risks:

- privacy breaches;
- commercial misuse of data;
- insurers pressuring operators for excessive data;
- discrimination in pricing models;
- data being used to undermine workers.

The UK must embed strict purpose-limitation and worker-data protections.

Question 68: How could privacy and data protection be managed if insurers request additional data?

Unite response:
Unite recommends:

- strict purpose limitation;
- pseudonymisation where possible;
- independent oversight;
- union consultation on data use;
- mandatory privacy impact assessments;
- clear retention limits;
- transparency to users and workers.

The UK should exceed Germany by embedding **worker-data protections**.

Question 69: What costs should be considered when regulating AV insurance?

Unite response:
Costs include:

- data storage;
- cyber-security;
- DSSAD/EDR compliance;
- training for claims handlers;
- system integration.

Question 70: What benefits should be considered when regulating AV insurance?

Unite response:
Benefits include:

- faster compensation;
- reduced disputes;
- improved safety;
- stronger public trust;
- clearer liability chains;
- protection of UICs from unfair penalties.

Question 71: What examples exist of AV insurance being done well?

Unite response:
Examples include:

- Germany's ADS liability model;
- Japan's automated shuttle insurance frameworks;
- US pilot programmes with mandatory data disclosure.

The UK can lead by integrating:

- stronger data protections;
- clearer liability rules;
- mandatory safety-case updates;
- worker-centred protections.

Question 72: How might a regulated body determine if an AV has committed a traffic infraction?

Unite response:
A regulated body must rely on multiple, corroborating data sources to determine whether an AV has committed a traffic infraction. These include:

- **DSSAD data** (ADS activation/deactivation, control inputs, ODD boundary warnings)
- **EDR data** (speed, braking, steering inputs)
- **ADS logs** (system decisions, sensor interpretation)

- **NUICO monitoring logs** (remote-assistance interventions)
- **third-party data** (police, highway authorities, CCTV)
- **vehicle telematics** (GPS, speed, geofencing)

Unite emphasises that:

A UIC must never be held responsible for any AV-driven infraction while the ADS is engaged.

Responsibility must sit with the ASDE or NUICO.

Question 73: What should be taken into consideration in the submission of standardised information to the IURS, and why?

Unite response:
Standardisation must ensure:

- consistent data formats across all ASDEs and NUICOs;
- clear definitions of infractions and incidents;
- mandatory timestamps;
- mandatory location data;
- mandatory ADS state data;
- secure transmission protocols;
- worker-data protections;
- union consultation on data policies

Standardisation prevents manipulation, ensures fairness, and supports transparent enforcement.

Question 74: What specialist elements or knowledge are needed for IURS investigations?

Unite response:
Investigators must have expertise in:

- ADS behaviour and failure modes;
- cyber-security and intrusion detection;
- human-factors analysis;
- remote-operation systems;

- sensor fusion and perception systems;
- vehicle dynamics;
- load-security (for goods vehicles);
- passenger-safety systems;
- data forensics.

This exceeds the requirements for conventional vehicle investigations.

Question 75: What records should be retained regarding maintenance and repair history of AVs?

Unite response:
Mandatory retention of:

- full maintenance logs;
- software update history;
- calibration records for sensors;
- cyber-security patch history;
- remote-operation hardware checks;
- load-security equipment checks (for goods vehicles);
- cabin-monitoring system checks (for passenger vehicles);

Integration with existing legal requirements for walk-around checks

Unite emphasises that **AV maintenance plans must be explicitly linked to existing DVSA daily walk-around check requirements**, particularly for HGVs, LGVs, and passenger-carrying vehicles.

ADS self-diagnostics **cannot replace**:

- visual inspection of tyres, wheels, lights, mirrors, bodywork;
- checks for fluid leaks, damage, vandalism, or obstructions;
- manual confirmation of load security;
- inspection of sensor housings and camera cleanliness;
- verification of number plates, reflectors, and safety markings.

Therefore:

1. NUICO maintenance plans must incorporate DVSA walk-around check standards

This ensures continuity with existing safety regimes and prevents operators from claiming that automation removes the need for physical inspection.

2. A competent human must still perform daily checks

Even in NUIC operations, a trained worker must:

- inspect the vehicle before dispatch;
- confirm load security;
- verify that sensors and cameras are unobstructed;
- check for physical damage the ADS cannot detect.

3. ADS self-diagnostics must supplement, not replace, human inspection

Automated systems cannot reliably detect:

- tyre cuts;
- cracked mirrors;
- insecure loads;
- vandalism;
- fluid leaks;
- missing plates;
- bodywork damage.

4. Maintenance records must include daily check logs

This ensures:

- traceability;
- accountability;
- regulatory compliance;
- integration with HGV operator licensing requirements.

5. NUICOs must not use automation to dilute safety standards

Unite strongly opposes any attempt to:

- reduce inspection frequency;
- replace trained workers with automated checks;
- outsource inspections to unregulated third parties.

This protects both road safety and the integrity of skilled vehicle-maintenance roles.

Question 76: What specialist knowledge or handling is necessary to preserve evidence?

Unite response:
Evidence preservation requires:

- digital forensics expertise;
- encryption-key management;
- secure extraction of DSSAD/EDR data;
- chain-of-custody protocols;
- safe handling of high-voltage systems;
- cyber-security isolation procedures;
- preservation of sensor data without corruption.

AV evidence is far more complex than conventional vehicles and must be treated accordingly.

Question 77: Beyond investigations, what other purposes could seized items be used for?

Unite response:
Secondary uses may include:

- training emergency services;
- improving regulatory systems;
- developing safety standards;
- supporting academic research;
- improving ADS design;
- enhancing cyber-security resilience.

All secondary uses must protect privacy and commercial confidentiality.

Question 78: What challenges exist regarding access to data relevant to investigations?

Unite response:
Challenges include:

- proprietary software;
- encrypted data;

- cloud-stored data outside UK jurisdiction;
- lack of standardisation;
- cyber-security restrictions;
- commercial confidentiality claims;
- incomplete or corrupted logs;
- remote-operation data stored by third parties.

The UK must require **mandatory access rights** for investigators.

Question 79: When is it acceptable for a seized item to be delivered to someone other than the owner?

Unite response:
Acceptable only when:

- required by law enforcement;
- required by the courts;
- required for safety testing by accredited bodies;
- required for independent investigation;
- required for cyber-security analysis;

Never for commercial advantage or without strict oversight.

Question 80: What considerations should be implemented during the destruction of an AV?

Unite response:
Destruction must consider:

- high-voltage battery safety;
- secure destruction of data-storage devices;
- environmental compliance;
- safe disposal of sensors and electronics;
- prevention of data recovery;
- cyber-security sanitisation.

AVs pose unique destruction risks compared to conventional vehicles.

Question 81: What considerations apply to the storage of a seized AV?

Unite response:
Storage must ensure:

- secure, climate-controlled facilities;
- cyber-security isolation;
- prevention of remote access;
- battery safety protocols;
- protection from tampering;
- preservation of digital evidence.

AVs must be stored as both physical and digital evidence.

Question 82: When should a seized AV be sold rather than disposed of?

Unite response:
Only when:

- all investigations are complete;
- all data has been securely wiped;
- the vehicle is safe to operate;
- no safety-critical defects remain;
- no cyber-security vulnerabilities remain.

Sale must never compromise safety or privacy.

Question 83: What considerations apply to the disposal of an AV compared to a conventional vehicle?

Unite response:
AV disposal must include:

- secure destruction of data systems;
- safe disposal of sensors and electronics;
- cyber-security sanitisation;
- environmental compliance;
- battery safety;
- destruction of remote-operation hardware.

AVs contain far more sensitive and hazardous components.

Question 84: What information can you provide about similar sanctions regimes?

Unite response:
Comparable regimes include:

- rail safety enforcement;
- aviation safety oversight;
- HGV operator licensing;
- nuclear safety regulation;
- cyber-security enforcement frameworks.

These systems demonstrate the value of:

- turnover-based fines;
- independent oversight;
- strong enforcement powers;
- transparent reporting.

Question 85: What factors warrant regulatory vs civil sanctions, variation vs suspension, or monetary penalties vs compliance notices?

Unite response:

Regulatory sanctions

Appropriate when:

- systemic safety failures occur;
- repeated infractions occur;
- ASDE/NUICO misleads regulators;
- cyber-security negligence is identified.

Variation vs suspension

- **Variation**: minor or correctable issues;
- **Suspension**: serious safety risks or repeated failures.

Monetary penalty vs compliance notice

- **Compliance notice**: first-time or low-risk issues;
- **Monetary penalty**: repeated non-compliance or harm caused.

Question 86: Should turnover be considered when setting maximum monetary penalties?

Unite response:
Yes. Turnover-based penalties ensure:

- proportionality;
- fairness;
- deterrence for large operators;
- prevention of “cost of doing business” behaviour.

Turnover should be calculated based on **global turnover**, not UK-only.

Question 87: What strict limit should be set for monetary penalties?

Unite response:
Greater than £25 million.

Large operators must face meaningful deterrents. Anything lower risks being absorbed as a business cost.

Question 88: Should turnover be considered when setting daily penalties for continuous failures?

Unite response:
Yes. Continuous failures must incur escalating penalties proportionate to operator size to prevent deliberate delay.

Question 89: What strict limit should be set for additional daily penalties?

Unite response:
Unite recommends:

- **at least £1 million per day**,
- or **a percentage of global turnover**, whichever is higher.

This ensures rapid compliance.

Question 90: Should turnover be considered when setting APS monetary penalties?

Unite response:
Yes. APS operators may be large multinational corporations. Penalties must reflect their scale.

Turnover should be calculated using **global turnover**, consistent with other safety-critical sectors.

Question 91: What strict limit should be set for APS monetary penalties?

Unite response:
Greater than £1,000,000.

APS violations can endanger passengers and the public. Penalties must be substantial.

Question 92: Should turnover be considered when setting APS daily penalties?

Unite response:
Yes. Daily penalties must prevent operators from delaying compliance.

Question 93: What strict limit should be set for APS daily penalties?

Unite response:
Unite recommends:

- **at least £250,000 per day**;
- or **a percentage of global turnover**, whichever is higher.

This ensures rapid compliance and prevents operators from treating daily penalties as a manageable business cost.

Question 94: Are there any additional factors that should be considered in the APS penalty regime?

Unite response:
Yes. APS penalties must also consider:

- the vulnerability of passengers affected;
- the operator's history of safeguarding compliance;
- whether the APS operator has offshored safety-critical work;

- whether the operator has engaged in union-busting or avoided collective bargaining;
- the scale of public-safety risk created.

APS penalties must be designed to deter systemic failures, not just isolated incidents.

Question 95: Should APS operators be required to publish annual safety and performance reports?

Unite response:
Yes. Transparency is essential. Reports must include:

- incident and near-miss data;
- safeguarding incidents;
- accessibility performance;
- staffing ratios and training levels;
- cyber-security breaches;
- complaints and resolution times.

These reports must be publicly accessible and shared with recognised trade unions.

Question 96: Should APS operators be required to consult with trade unions on safety, staffing, and operational changes?

Unite response:
Yes. APS operations are safety-critical. Trade union consultation must be:

- mandatory;
- early (before decisions are made);
- meaningful;
- documented.

This aligns APS operations with existing safety-critical sectors such as rail and aviation.

Question 97: Should APS operators be required to maintain UK-based operations centres?

Unite response:
Yes. Offshoring APS oversight would:

- undermine safety;
- weaken accountability;
- create safeguarding risks;
- reduce transparency;
- undermine UK employment;

APS operations must be UK-based, unionised, and subject to UK law.

Question 98: Should APS operators be required to meet minimum staffing ratios?

Unite response:
Yes. Unite recommends:

- **1:1 to 1:3** remote-monitoring ratios for APS vehicles;
- higher staffing levels for complex environments;
- mandatory safeguarding-trained staff;
- no gig-economy or casualised models.

APS operations must never be run on a “lean staffing” model.

Question 99: Should APS operators be required to demonstrate accessibility compliance before receiving a permit?

Unite response:
Yes. Accessibility must be a **pre-condition**, not an afterthought. Operators must demonstrate:

- accessible cabin design;
- accessible boarding and alighting;
- accessible emergency communication;
- accessible HMI and alerts;
- staff trained in disability awareness.

Accessibility failures must result in permit suspension.

Q100. Should APS operators be required to demonstrate safeguarding compliance?

Unite response:
Yes. APS operators must:

- have safeguarding policies approved by regulators;
- train all staff in safeguarding;
- maintain real-time cabin monitoring;
- provide panic buttons and emergency contact systems;
- report safeguarding incidents within 24 hours.

APS vehicles must be safe for women, girls, disabled passengers, and vulnerable users.

Question 101: Should APS operators be required to share data with local transport authorities?

Unite response:
Yes. Data sharing is essential for:

- integrated transport planning;
- accessibility monitoring;
- safety oversight;
- environmental impact assessment.

Data must not be treated as proprietary corporate property.

Question 102: Should APS operators be required to integrate with local transport networks?

Unite response:
Yes. APS services must:

- complement, not compete with, public transport;
- avoid cherry-picking profitable routes;
- support integrated ticketing
- align with local transport strategies.

APS must not undermine bus networks or future public ownership.

Question 103: Should APS operators be required to meet environmental standards?

Unite response:
Yes. APS fleets must:

- be zero-emission;
- meet battery-safety standards;
- avoid offshoring environmental harm;
- report lifecycle emissions.

Environmental justice must be central.

Question 104: Should APS operators be required to meet cyber-security standards?

Unite response:
Yes. APS operators must:

- meet mandatory cyber-security certification;
- report breaches within 24 hours;
- maintain secure data storage;
- prevent remote hijacking or interference;

Cyber-security failures must trigger immediate permit review.

Question 105: Should APS operators be required to maintain insurance that covers cyber-security incidents?

Unite response:
Yes. Cyber-security insurance must be:

- mandatory;
- comprehensive;
- proportionate to fleet size;
- transparent.

Cyber-security failures must never fall on passengers or workers.

Question 106: Should APS operators be required to maintain insurance that covers product liability?

Unite response:
Yes. APS operators must hold:

- product liability insurance;
- operational liability insurance;
- third-party liability insurance;

Liability must never be shifted onto workers or passengers.

Question 107: Should APS operators be required to maintain insurance that covers remote-operation failures?

Unite response:
Yes. Remote-operation failures are foreseeable risks. Insurance must cover:

- communication failures;
- remote-operator error;
- system latency;
- cyber-attacks;
- hardware failure.

This protects workers and the public.

Question 108: Should APS operators be required to maintain insurance that covers accessibility failures?

Unite response:
Yes. Accessibility is a legal requirement. Insurance must cover:

- injury caused by inaccessible design;
- failure to provide reasonable adjustments;
- discrimination claims;

This ensures accountability.

Question 109: Should APS operators be required to maintain insurance that covers safeguarding failures?

Unite response:
Yes. Safeguarding failures can cause severe harm. Insurance must cover:

- assault;
- harassment;
- neglect;
- failure to protect vulnerable passengers;

APS operators must be held accountable.

Question 110: Should APS operators be required to maintain insurance that covers environmental harm?

Unite response:
Yes. Environmental harm includes:

- battery fires;
- hazardous waste;
- pollution incidents.

Operators must be financially responsible.

Question 111: Should APS operators be required to maintain insurance that covers data breaches?

Unite response:
Yes. Data breaches can cause or facilitate:

- identity theft;
- stalking;
- harassment;
- discrimination.

Insurance must cover remediation and compensation.

Question 112: Should APS operators be required to maintain insurance that covers algorithmic bias?

Unite response:
Yes. Algorithmic bias can cause:

- discriminatory service provision;
- unsafe decisions;
- unequal treatment of passengers.

Insurance must cover harm caused by biased ADS behaviour.

Question 113: Should APS operators be required to maintain insurance that covers system-wide failures?

Unite response:
Yes. System-wide failures can cause:

- mass disruption;
- safety incidents;
- loss of service.

Insurance must cover large-scale operational risks.

Question 114: Should APS operators be required to maintain insurance that covers emergency-service interaction failures?

Unite response:
Yes. APS vehicles must be able to:

- detect emergency vehicles;
- yield appropriately;
- communicate with emergency services.

Failures must be insurable.

Question 115: Should APS operators be required to maintain insurance that covers passenger-assistance failures?

Unite response:
Yes. APS vehicles must:

- assist disabled passengers;
- provide emergency support;
- ensure safe boarding and alighting.

Insurance must cover harm caused by inadequate assistance.

Question 116: Should APS operators be required to maintain insurance that covers remote-operator misconduct?

Unite response:
Yes. Misconduct includes:

- negligence;
- harassment;
- safeguarding breaches;
- data misuse.

Operators must be accountable for staff behaviour.

Question 117: Should APS operators be required to maintain insurance that covers third-party supplier failures?

Unite response:
Yes. APS operators must not outsource liability.
Insurance must cover:

- subcontractor failure;
- software supplier failure;
- hardware supplier failure;

Liability must remain with the APS operator.

Question 118: Should APS operators be required to maintain insurance that covers infrastructure failures?

Unite response:
Yes. Infrastructure failures include:

- charging infrastructure
- communications networks
- mapping systems

Insurance must cover operational disruption and harm.

Question 119: Should APS operators be required to maintain insurance that covers extreme-weather failures?

Unite response:
Yes. Extreme weather affects:

- sensors;
- braking;
- perception;

- routing.

Insurance must cover weather-related incidents.

Question 120: Should APS operators be required to maintain insurance that covers vandalism or malicious interference?

Unite response:
Yes. APS vehicles are vulnerable to:

- sensor obstruction;
- physical damage;
- cyber-interference.

Insurance must cover malicious acts.

Question 121: Should APS operators be required to maintain insurance that covers passenger misconduct?

Unite response:
Yes. Passenger misconduct can cause:

- damage;
- safety incidents;
- service disruption.

Insurance must cover these risks.

Question 122: Should APS operators be required to maintain insurance that covers lost or damaged passenger property?

Unite response:
Yes. APS operators must provide:

- clear lost-property procedures;
- compensation mechanisms.

Passengers must be protected.

Question 123: Should APS operators be required to maintain insurance that covers service-animal incidents?

Unite response:
Yes. APS vehicles must:

- accommodate service animals;
- ensure safe travel;
- prevent harm.

Insurance must cover incidents involving service animals.

Question 124: Should APS operators be required to maintain insurance that covers cross-border operations?

Unite response:
Yes. Cross-border operations require:

- harmonised insurance;
- clear liability rules;
- international compliance.

Operators must be fully insured.

Question 125: Are there any other issues the Government should consider?

Unite response:
Yes. Unite highlights:

- the need for strong union involvement in all AV regulatory processes;
- the risk of corporate AV fleets undermining public transport;
- the need for UK-based, unionised operations centres;
- the importance of preventing gig-economy models in safety-critical roles;
- the need for public ownership options to remain open;
- the need for algorithmic fairness and transparency;
- the importance of environmental justice;
- the need for robust worker-data protections.

AV deployment must strengthen — not weaken — public transport, worker rights, and public safety.

Any Other Comments

Equality Impacts

Unite identifies the following key equality considerations:

Disability and Accessibility

AVs must improve accessibility, not reduce it. This includes:

- accessible cabin layouts
- tactile, auditory, and visual alerts
- accessible emergency communication
- safeguarding protocols for vulnerable users.

Digital Exclusion

AV systems must not exclude:

- older people
- low-income groups
- people with limited digital access
- people with limited English proficiency

Non-digital alternatives must be available.

Workforce Equality

Automation disproportionately affects:

- older workers
- disabled workers
- migrant workers
- workers in manual or safety-critical roles.

Unite calls for:

- retraining and redeployment pathways
- no compulsory redundancies
- union-negotiated transition plans

- reasonable adjustments in new roles.

Passenger Safety and Equality

NUIC passenger services raise safeguarding concerns for:

- women and girls
- disabled passengers
- children and young people
- intoxicated or vulnerable passengers.

Unite supports:

- real-time cabin monitoring
- panic buttons
- safeguarding-trained remote staff.

Algorithmic Fairness

ADS systems must be tested for:

- bias in perception
- bias in decision-making
- unequal error rates.

Cyber-Security and Equality

Cyber-security failures disproportionately affect:

- disabled passengers
- lone women
- older passengers
- workers whose data may be captured.

Strict limits on personal data collection are essential.

Environmental Justice

AV deployment must not:

- shift pollution to deprived communities
- reduce public transport in disadvantaged areas.

Public Sector Equality Duty

All secondary legislation must include:

- Equality Impact Assessments
- ongoing monitoring
- mandatory reporting
- union involvement.

Corporate Ownership of AV Fleets and Public Transport

Unite is clear that the risks identified in this submission relate specifically to the expansion of **corporate-owned automated vehicle fleets**, not individual private ownership of automated cars.

Large technology companies, logistics corporations, and platform-based mobility operators have the capacity to:

- extract and monopolise mobility data;
- cherry-pick profitable routes;
- undermine public transport ridership;
- fragment networks;
- offshore safety-critical work;
- introduce gig-economy models;
- lobby aggressively against public ownership;
- entrench private control over mobility infrastructure.

These impacts would make it significantly harder for future governments to deliver a unified, publicly owned, accessible transport system.

Strong regulation is therefore essential to ensure that corporate AV deployment does not undermine integrated planning, weaken public transport finances, or create new structural barriers to nationalisation.

Unite emphasises that nothing in this submission conflicts with or complicates plans to bring public transport into public ownership. On the contrary, the regulatory standards proposed here — around safety, transparency, workforce protections, accessibility, and accountability — are fully compatible with, and in many cases strengthened by, publicly owned and democratically accountable transport services.