Consultation Paper on the Regulatory and Legal Framework for Autonomous Vehicles (AV) in Singapore

Ministry of Transport

May 2026

Contents

Executive summary

1. The Government is seeking feedback on the legal and regulatory framework for autonomous vehicles (AV), with a view to develop a piece of legislation to govern them in a more holistic manner, building on lessons learnt from the existing regulatory sandbox for AV trials and from other jurisdictions. Implementation details will be worked through thereafter at the subsidiary legislation level.

2. The central objective of the AV legislation is to ensure the safe functioning of AVs on Singapore roads. AVs, by definition, do not require human drivers. However, our current traffic regulations, insurance practices and enforcement regime are centred on the role which the driver plays. Thus, to ensure that AVs can operate safely, we need to establish a separate and robust regulatory regime.

3. To this end, we have outlined the key issues in four areas: (a) responsibility and accountability of various AV actors, (b) compensation and insurance, (c) data and cybersecurity management, and (d) use of Advanced Driver Assistance Systems (ADAS) and conditional automation.

    a. Responsibility and accountability of various AV actors. A clear delineation of roles and responsibilities among various AV actors will form the basis for accountability and liability attribution when they fail to adequately fulfil their functions. We have identified four key actors: the entity in-charge of AV technology, fleet operator, onboard Safety Operator, and Remote Operator with conceptually distinct functions. To regulate and hold these AV actors accountable during both testing and full commercial deployment phases, we considered the appropriate regulatory levers (e.g. vehicle homologation, licensing), criminal offences to impose for egregious wrongdoings, and ways to improve the civil liability regime as applied to AVs. We welcome views on the AV actors identified, their roles and responsibilities, and the means to hold them accountable for safety.

    b. Compensation and insurance. In the event of AV accidents, timely compensation to victims is crucial for justice, accountability and public assurance. To achieve this, stakeholders such as industry, insurers and the Government must work together closely. The key considerations include how AV insurance will interact with the existing motor insurance regime, the affordability of premiums, the speed of compensation especially if the civil liability of accidents is disputed, and the type of risks insured. We welcome views on the different ways to achieve timely compensation and safeguard against cybersecurity risks.

c. Data and cybersecurity management. AVs collect, make use of and generate significant amount of data. The data must be managed carefully, to ensure personal data protection and public security. Data are also key for regulators to maintain oversight of the AVs and investigate any accidents effectively. Rigorous cybersecurity standards must also be met to prevent attacks on AVs, which could have grave consequences. We welcome views on how best to calibrate the requirements, to achieve these important objectives while minimising compliance burden.

d. ADAS and conditional automation. Lastly, the line between conventional manned motor vehicles and AVs are getting blurred with ADAS and SAE[1] Level 3 (conditional automation) features. We generally classify AVs as vehicles with autonomous technology that operates at SAE Level 4 and above; i.e. vehicles which can operate in a very wide range of operational domains, and only require human interventions in exceptional situations, upon moving the vehicle to a safe position. Conversely, SAE Level 3 vehicles can handle driving tasks autonomously under specific conditions (i.e. more limited that Level 4), and thus the human driver is required to pay attention and must take over when requested. To allow for such vehicles in Singapore, we must work through the liability issues if accidents occur during the transition of vehicular control. We welcome views on the appropriate approach.

4. To comment on these issues (see **Annex A** for the full list of questions), please submit any written responses at https://go.gov.sg/avpublicconsult by **30 June 2026**. Submissions will be reviewed by the Government and summarised for public release following the conclusion of the consultation.

[1] SAE International, formerly Society of Automotive Engineers (SAE), is a global non-profit professional association and standards organisation for engineering. Refer to page 5 for more details on the SAE levels of driving automation.

Introduction

1. Background. Today, autonomous vehicles (AV) trials on public roads are facilitated by the regulatory sandbox under Section 6C-6E of the Road Traffic Act (RTA) 1961.

    a. The industry has claimed that AVs are designed to be at least as safe as human drivers[2].

    b. Legal entities wishing to deploy AVs must apply to LTA, pass the relevant technical assessments that validates the safety of the AVs, and obtain the authorisation approval.

    c. They are also subject to the Road Traffic (Autonomous Motor Vehicles) Rules 2017, which mandates liability insurance and impose duties like maintaining AVs in good condition and proper functioning, among others.

    d. Other prevailing regimes such as road traffic offences and the Penal Code still apply where relevant.

2. Key concepts.

    a. The SAE International defines the various levels of driving automation, which provide a useful technical classification for different levels of autonomy for a vehicle.

<table>
<tr><th></th><th>Level 0
(No automation)</th><th>Level 1
(Driver assistance)</th><th>Level 2
(Partial automation)</th><th>Level 3
(Conditional automation)</th><th>Level 4
(High automation)</th><th>Level 5
(Full automation)</th></tr>
<tr><td rowspan="2">Technical features available</td><td colspan="3">Driver support features</td><td colspan="3">Automated driving features</td></tr>
<tr><td>Limited to providing warnings and momentary assistance</td><td>Steering or brake/ acceleration support</td><td>Steering and brake/ acceleration support</td><td colspan="2">Able to drive the vehicle under limited conditions</td><td>Able to drive the vehicle under all conditions</td></tr>
<tr><td>Role of human driver</td><td colspan="3">Human driver:
• is still driving when the technical features are engaged (even if feet are off the pedals or not steering)
• must constantly supervise the support features (e.g. steer, brake or accelerate as needed to maintain safety)</td><td>Human must drive when requested by the features</td><td colspan="2">Human not required to take over driving</td></tr>
</table>

Source: SAE International

[2] Waymo reported an 81% reduction in injury-causing crashes compared to average human drivers (as of Feb 2026). Baidu said the accident rate of their AVs was 1/14 that of human drivers (as of Feb 2025).

b. The operational design domain (ODD) of an AV refers to the operating conditions under which the automated driving system (ADS) is designed to operate safely and effectively. This could include the geographical areas, environmental/weather conditions, traffic situations, etc.

c. An onboard safety operator (SO) maintains oversight of the AV's operations and takes control when necessary and/or when prompted by the ADS. Depending on the vehicle design, an SO could be an individual seated inside the AV or within the line of sight of the vehicle.

d. On the other hand, remote operators (RO) control or assist the AVs from a remote location (i.e. not within line of sight of vehicle). In Singapore's context, we expect ROs to be deployed in lieu of SOs for safety assurance upon full deployment[3]. A single remote operator may oversee multiple AVs at once, conditional on the technical and operational readiness. This is known as 1:N remote operations.

e. When the ADS detected failures/errors or environmental anomalies outside the vehicles' ODD, it typically performs certain manoeuvres automatically to achieve a state that minimises the risk of accidents. This state is known as the minimal risk condition (MRC). One example is coming to a safe stop.

f. A summary of the AV regulatory and legal approaches in other jurisdictions is included in **Annex B**, for reference.

3. Impetus and objectives.

a. As we scale up the deployment of AVs and develop different use cases in Singapore, we need to develop a clear and more comprehensive regulatory framework for AVs. This will help to build up public confidence and provide more legal clarity as to the responsibilities of different stakeholders involved in operating AVs, as well as other motorists and users of public roads.

b. As such, the Government aims to develop and table an "AV Act" (working name) in Parliament in 2027, to set out the overall legal framework governing the use of AVs in Singapore.

[3] Under Singapore's current Deployment Readiness Assessment (DRA) Phase of the authorisation process as part of the regulatory sandbox, a SO will remain onboard the vehicle while testing for remote operations by the RO is conducted to serve as a safeguard.

4. Scope.

    a. For a start, we are considering the legal framework for motor vehicles that do not require human control or immediate interventions for safe operations. These are AVs at SAE Level 4 and above. While safety or remote operators may still be involved, the ADS – by design – should be capable of entering MRC when needed before passing over control to a SO/RO.

    b. For vehicles with advanced driver assistance systems (ADAS) or SAE Level 3 conditional automation capabilities where the human driver must monitor and take over readily, we have elaborated on the considerations in Chapter D.

Chapter A. Responsibility and accountability

1. There are multiple actors involved in AV operations. Having a clear delineation of roles could form the basis from which responsibility and accountability are attributed, when an AV actor has failed to adequately fulfil its functions.

2. As we move towards full driverless operations, there should be a corresponding shift away from individual responsibility (e.g. on drivers, SOs or ROs) towards corporate responsibility (e.g. on corporate entities developing and/or operating the AVs). This is because individuals have relatively lesser control than the ADS in operating a SAE L4 and above vehicle. Corporate entities have more responsibilities to maintain the AV to ensure their proper functioning given the heavier reliance on technology for its operations.

3. We also note generally that in the event of any breach of the law, AV actors could be held accountable via different means:

    a. Regulatory sanctions such as suspension of authorisation/licence or fines could be imposed.

    b. Criminal offences and liability could be introduced for more egregious wrongdoings, leading to fines and/or imprisonment.

    c. AV actors may also face civil liability claims from others for compensation.

<u>Delineating functions and responsibilities of key AV actors</u>

4. We have set out a preliminary and simplified proposal on the delineation of responsibilities in *Table 1* below.

5. There are multiple upstream players involved in the development and manufacturing of the AV, and they may or may not be based locally. Given the different degrees of vertical integration across industry players, we are considering an approach to **appoint a single entity in-charge of the AV technology**, which could be identified from within the relevant consortium involving the system developer, original equipment manufacturer or even authorised distributor of specific AV models.

6. As we plan for fleet-based deployment, the role of the **fleet operator** will be key. They choose the specific AVs to bring in for deployment, maintain the overall fleet operations, have substantial corporate presence and physical assets domestically, and interface with both the entity in charge of the AV technology and passengers.

7. Individual **SOs** or **ROs** would be employed by the fleet operators to operate the AV passenger services. Their function is to intervene when needed in

accordance with established protocol in their respective roles. For the avoidance of doubt, a SO and a RO can only be concurrently involved in AV operations during the assessment phase to validate the AV's remote operations; in such cases, they are responsible for performing their respective functions.

Table 1. Simplified delineation of functions among AV actors (non-exhaustive)

<table>
<tr><td colspan="2">Entity in-charge of AV technology
Obtaining type-approval / homologation of AV for use in Singapore
Overall performance and integration of autonomous driving system (ADS) and hardware (e.g. dynamic driving task, adherence to traffic rules), as well as network security (e.g. cybersecurity standards)
Patching/rectifications of AV defects (incl. through timely software updates)
Assist authorities in investigation and enforcement</td></tr>
<tr><td colspan="2">Fleet operator
Regular maintenance and renewal of the fleet
Develop and implement sound Concept of Operations (CONOPS)
Train and deploy proficient workers, especially safety and remote operators
Assist authorities in investigation and enforcement</td></tr>
<tr><td>Onboard SO
Monitor ADS health and maintain situation awareness; If ADS fails to perform safely, intervene appropriately within reasonable time and available means (e.g. take over as driver, trigger emergency brake)</td><td>RO
Respond to system prompts/alerts appropriately and in accordance with Standard Operating Procedures (SOP) within a reasonable time</td></tr>
</table>

Legend: Corporate entities | Individuals

Holding AV actors accountable – regulations and legal liability

8. To allow for continued innovation while requiring safe commercial services for more mature operating models, we propose to have a two-tier regulatory structure for operations under different phases of development:

    a. Research and development (R&D) / testing phase operations (under an authorisation regime similar to today's regulatory sandbox); and

    b. Full commercial deployment, to reflect appropriate scope of operations and regulatory oversight required.

9. During the R&D/testing phase, the vehicle's autonomous driving or remote operations capabilities are being validated. An SO will often be deployed onboard to serve as a safeguard. If the system prompted the SO to take over and an accident occurred because of the SO's manual manoeuvre or failure to

take over within a reasonable time (to be stipulated), the SO would be subject to prevailing road traffic offences.

10. To hold AV actors accountable under full commercial deployment, we propose the following as well as *Chart 1* based on the distinct responsibilities of different AV actors.

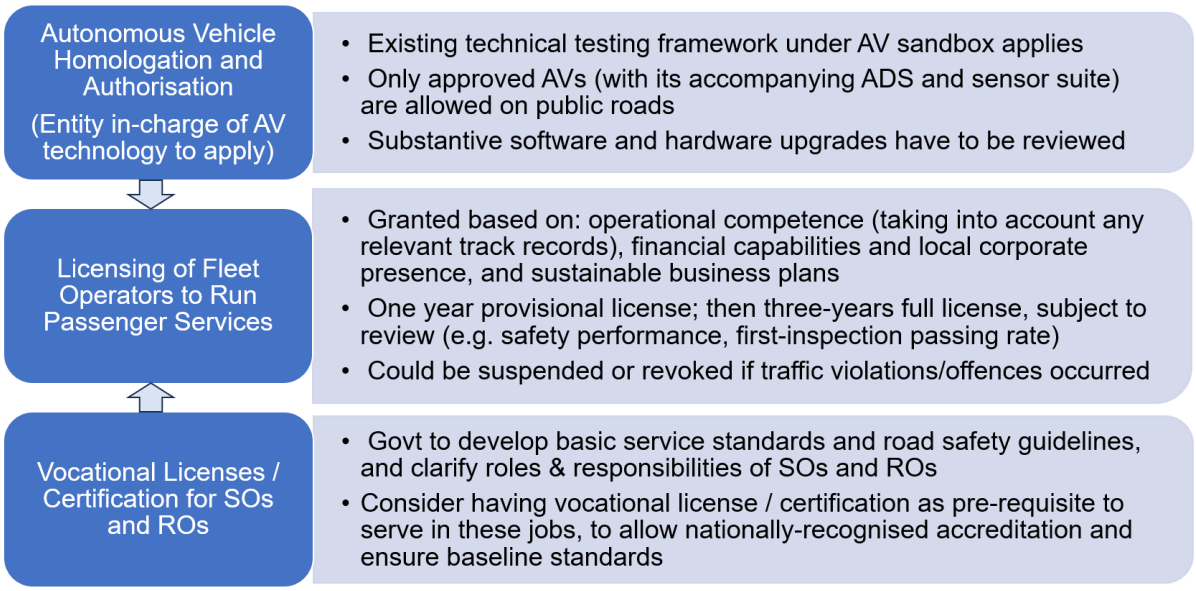
    a. The entity in-charge of AV technology will be held responsible and accountable via licensing. They must fulfil local corporate presence and financial capabilities requirements, and demonstrate technical competency and safety engineering capabilities. To homologate the AV, comprehensive testing requirements and appropriate recognition of safety certification from established jurisdictions would be the foundation.

    b. The fleet operator is responsible and accountable for meeting operational management and maintenance requirements. Among others, these include ensuring that the software on the AVs are properly updated and safeguarded, and that there are necessary and rigorous protocols to manage any exceptional incidents during the operation of the AVs.

    c. Individual SOs/ROs are responsible for the fulfilment of their expected functions outlined in *Table 1* based on safety-critical best practices/SOPs. The Government is also considering vocational licenses / certifications to hold them accountable in the steady state. This could be accompanied by a standardised set of competencies to ensure that they have the skillsets required for the roles, to be issued as guidelines for the industry.

    d. If the actors fail to discharge their stipulated responsibilities, their respective authorisation/licenses could be suspended or revoked depending on the severity of the non-compliance. Rectification or remedial actions might also be necessary to maintain the validity of the authorisation/licenses.

Chart 1. Proposed architecture of regulatory regime for full commercial deployment



11. In terms of criminal offences to deter and punish egregious wrongdoings related to AVs, our preliminary proposal is in *Table 2*. Where negligence, recklessness or malicious intent occurs, existing criminal offences such as those under Penal Code and RTA may also apply.

12. When the AV is in autonomous mode, SO/ROs are not actively controlling the vehicle and traditional road traffic offences for drivers should not apply. Instead, the corporate entities (i.e. the entity in-charge or fleet operator) will be responsible in the event of accidents, on top of meeting the regulatory requirements before their AVs are allowed on the road as outlined above. Corporate criminal liability could apply to lapses committed by the employees in the course of their work (e.g. algorithmic errors by software engineers), even if the senior executives (i.e. the "directing minds" of the companies) did not directly contribute to the lapses.

13. When the AV is not in autonomous mode, but rather manually driven by the onboard SO, or after the expiry of the takeover transition period following system prompt, prevailing road traffic offences will be the responsibility of the SO where relevant. Whether the vehicle is in autonomous or manual mode at the point of accident is thus critical.

Table 2. Proposed criminal offences related to AVs

<table>
<tr><th>Entity in-charge of AV tech</th><th>Fleet operator</th><th>SO/RO</th><th>Others</th></tr>
<tr><td colspan="2">Failure to provide information required by regulations or notices
Falsification or withholding of information relevant to vehicle safety, with heavier penalty if death or serious injury occurs
Obstruction of investigation or failure to cooperate</td><td></td><td></td></tr>
<tr><td colspan="2">False marketing/advertising of AVs or passenger services</td><td></td><td></td></tr>
<tr><td colspan="2">Failure to take reasonable steps to prevent, mitigate or cease harm caused by AVs under purview</td><td></td><td></td></tr>
<tr><td>Provision of defective AV (incl. software)</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Use or operation of unauthorised AVs and/or without license</td></tr>
<tr><td></td><td colspan="2">Rash, negligent or intentional wrongful operation of AVs</td><td></td></tr>
<tr><td></td><td>Failure to ensure AV remains safe and in a state of proper functioning, leading to injuries, deaths and property damage[4]</td><td></td><td></td></tr>
<tr><td colspan="4">Tampering and/or interference of AVs</td></tr>
</table>

14. For civil liability, AV actors can rely on existing rights of action based in contractual arrangements, tort of negligence, and product liability.

15. On the challenges of proving the exact cause(s) of AV accident (e.g. defects of the autonomous driving system, operational lapse), we are studying the use of statutory presumptions to overcome the potential difficulties faced by victims, for example in terms of gathering evidence that may reside only with the fleet operator or the AV technology provider.

16. The AV could be presumed defective and had caused the accident, unless contrary evidence is shown. This places the burden of proof on the entity in-charge of the AV technology, which has access to the data and information regarding the crash. Such entities may be exposed to more civil liability risks and incur additional compliance burden and costs to retain the information.

[4] For lapses with no injuries, deaths or property damage, regulatory penalties may still apply.

17. To limit specific AV actors' civil liability if reasonable standards have been met, safe harbour provisions could be introduced. Japan took a similar approach. Some examples are as follows.

    a. The entity-in-charge of the AV technology could avoid liability if it can be shown that the AV's operation and decision-making were sound.

    b. The fleet operator could avoid liability if it can be shown that the AVs are duly maintained at a specific cadence (to be stipulated) and it has implemented the approved CONOPS given the authorised ODD.

    c. The SO/ROs could avoid liability if it can be shown that they followed the relevant SOP based on reasonable judgement of the circumstances.

<u>Key questions</u>

1. Does *Table 1* appropriately capture the key AV actors and their respective functions? Are the responsibilities of different AV actors clear and distinct? What other actors (e.g. passengers, individual owners) should be considered, and why?

2. What approach should authorities take to protect public safety while allowing for innovation? Who should authorities hold responsible to oversee AV system updates?

3. What adjustments to the previously approved AVs should require the explicit re-approval of the authorities (e.g. safety-critical functions, hardware modifications, operational scope expansions)?

4. With respect to recognising safety certification from other jurisdictions, how should we strike a balance between minimising red-tape for the industry and safeguarding safety in local conditions?

5. In the event of road safety violations or accidents, would you support holding a single actor responsible in the first instance to facilitate timely compensation for victims? This actor can recover from the at-fault parties subsequently (if it so chooses).

6. If yes for question 5, which AV actor would be in the best position to take on the responsibility? Should it be the entities in-charge of AV tech, fleet operators, or others?

a. Entity in-charge of AV technology – best understand the underlying technology, have access to the necessary data, can rectify ADS errors quickly, and have the financial capabilities to wear the responsibility.

b. Fleet operator – have control over the overall service operations and AV maintenance, maintain contractual relationships with both AV providers and passengers, and more likely to be able to deploy customer service / incident response teams onsite to manage the accident.

7. Are there any offences listed in *Table 2* that you think should not be criminal in nature? Is so, should regulatory or financial penalties be used instead? Why?

8. Are there views on how we should more precisely scope the criminal offences in *Table 2*?

9. Are there any additional criminal offences we should consider?

10. Should we introduce statutory presumptions to help victims of AV accidents overcome evidential difficulties in civil cases? What are the possible risks and concerns with doing so? How may these be addressed?

11. Should safe harbour provisions be introduced to limit specific AV actors' liability if reasonable standards have been met? If so, how should they be scoped?

Chapter B. Compensation and insurance

1. The National Steering Committee for AVs has stressed the importance of timely compensation for victims in the event of accidents leading to injuries, deaths and property damages.

    a. In the near to medium term, this is necessary to provide public assurance and facilitate the smooth rollout of AVs in Singapore.

    b. In the longer term, as AVs become more ubiquitous, the demands for timely compensation would likely persist, both as a practical remedy for victims who have suffered loss as well as for the purpose of natural justice and public accountability.

2. Status quo. Today, authorisation holders under the RTA sandbox are required to have liability insurance for the AVs.

    a. Singapore's motor insurance regime is fault-based.

    b. In the event of accidents, insurance will pay out according to the State Courts' Motor Accident Guide or the Barometer of Liability Agreement (BOLA), which is an existing industry agreement for insurers to determine fault in motor accidents and facilitate faster subrogation claims settlement among insurers.

    c. If the fault apportionment is disputed, parties may go to the Financial Industry Disputes Resolution Centre or initiate court proceedings if needed.

3. To achieve timely compensation for AV accidents, at least in the near term, stakeholders such as industry, insurers and the Government must work together closely.

4. Some relevant considerations are as follows:

    a. Given a mixed fleet of both AVs and manned vehicles on the roads in the foreseeable future, any divergence in their motor insurance treatments can create distortions. For instance, if AVs are accorded stronger protections than conventional vehicles, it could create moral hazard (e.g. AV actors taking less care to ensure safety), perverse incentives (e.g. insurance fraud to receive generous payouts) and system-level distortions (e.g. choosing to collide with an AV over a manned vehicle since it is easier to get an insurance payout from an AV).

b. On the other hand, given that AV technology is new, more favourable treatment for victims of accidents involving AVs could be justifiable as we scale up AV deployment and build public confidence.

c. Additional risks, liability and uncertainty would translate to higher insurance premiums. The insurability of AVs and affordability of premiums would be critical for the AV deployment in Singapore.

d. To the extent that AV insurance continues to be fault-based, the decisions in Chapter A (e.g. whether any entity is held responsible in the first instance) will affect the speed of compensation, especially if the at-fault party liable for compensation is disputed and investigations/litigations are long-drawn.

e. Finally, there could be alternative ways to conceptualise AV insurance beyond motor insurance, especially for fleet-based deployment. For example, it could be subsumed under comprehensive corporate insurance that covers various business risks. AV companies with better technology and strong financial capabilities could also "self-insure". This is already done by some larger players in international markets.

5. On this basis, we have set out <u>three possible options</u> to achieve timely compensation for AV accidents in *Chart 2* below.

Chart 2. Possible ways to achieve timely compensation

Increasing support for victims

	Option A	Option B	Option C
	Fault-based		No-fault
Payout Mechanism	Similar to status quo, but require AV insurance to pay out within a prescribed time if undisputed.	"Victim-first" model whereby AV insurance pays out in full if *AV caused accident (at least partly)*, and recovers from other at-fault parties subsequently	AV insurance always pays out and does not recover downstream
Limitation/ downside	Risk of drawn-out court proceedings for disputed cases remains	Subsequent recovery / subrogation by AV insurers may be difficult, which may lead to higher premiums	• Radical departure from existing fault-based regime • High risk of moral hazards and perverse incentives, which may lead to exorbitant premiums, or AVs becoming uninsurable

<u>If we go with Option A, consider providing goodwill compensation for disputed cases:</u>

1. **AV operator/developer involved to provide goodwill payments first**, before pursuing recovery after fault has been established
   a. <u>*Downside*</u>: Challenging for companies with less financial means and legal capabilities
2. **Industry can set aside a pool of money** for this purpose
   a. <u>*Downside:*</u> Onerous administration of fund and subsequent recovery from at-fault party

Key questions

1. To what extent should AV insurance lean towards being more favourable to victims in terms of process than the existing motor insurance regime to achieve timely compensation, at least in the initial phases of deployment? If yes, which option should be selected? Why? Are there other suggestions? How will this affect the overall cost of insurance?

    a. If Option A is selected, how should we allow for goodwill compensation for drawn-out disputed cases? How should we size the quantum, and how should it be funded? Who should administer it? Under what criteria should it be provided?

    b. If Option B is selected, what challenges may AV insurers face when pursuing subrogation claims, and what regulatory provisions should authorities implement to address these obstacles?

    c. If Option C is selected, how can the risk of moral hazards and perverse incentives be mitigated?

2. What is your view on self-insurance, allowing large AV entities to manage their own risk pools rather than purchasing traditional commercial policies?

Chapter C. Data and cybersecurity management

1. Clear data and cybersecurity management frameworks are key to ensuring safety and natural justice outcomes, which are crucial to fostering public trust and acceptance in AVs.

    a. This includes maintaining oversight of AVs' operations, facilitating effective downstream investigation, and reducing the risk of cyber-threats to AVs.

    b. At the same time, personal data protection, commercial interests and national security considerations must be taken into account.

2. For Data Management, we are considering regulations on the use and sharing of data generated and collected by AVs and AV operators, to safeguard personal privacy and national security. Some possible measures include:

    a. Strongly encouraging AV operators to implement and regularly conduct data protection and security reviews using existing frameworks such as IMDA's Data Protection Essentials (DPE) Checklist[5]. These reviews could be required as part of AV licensing applications to establish an initial baseline. This would be supported by an annual review (as recommended by the framework) to ensure that data protection measures remain updated and aligned with evolving operational needs.

    b. Limiting AV operations near sensitive/protected areas under the Infrastructure Protection Act 2017.

    c. Implementing calibrated data residency requirements (i.e. data to be stored locally and not transferred overseas) and cross-border data transfer logging/control requirements.

3. We are also looking to obtain the datasets in *Table 3* below from AV fleet operators and/or AV developers, for the use cases listed. These are to ensure safety and legal compliance, facilitate incident management and investigations, and inform transport planning.

    a. The requirements for frequency, latency, and other data characteristics would vary according to operational needs, e.g. real-time streaming for immediate incident response, to end-of-day batch submissions for routine monitoring.

    b. For accidents involving investigation and/or court proceedings, we are studying both technical and process measures to ensure the integrity

[5] Details are available at Data Protection Essentials (DPE) Programme | IMDA.

and utility of evidence in the event data recorder (EDR), taking into account the relevant standards governing the EDR.

c. For safety and legal compliance, we propose retaining data for 3 years, which is consistent with the existing authorisation regime under the RTA regulatory sandbox.

Table 3. Datasets to obtain from fleet operators and/or AV developers

Purpose	Use case	Datasets required
Safety and legality	Compliance to approved ODDs	Vehicle telematics (e.g., vehicle location, drive mode)
	Monitoring of safety performance	Vehicle telematics (e.g., throttle/brake, velocity)
	System integrity verification	Software version and update logs
	Post-incident investigations (e.g. investigate and reconstruct sequence of events)	Event data recorder (e.g. vehicle telematics, camera footages, perception data for detected objects and road infrastructure)
Incident and traffic flow management	Facilitate incident detection	Vehicle telematics; incident indicator(s) (e.g. vehicle location, acceleration, velocity, bumper impact sensor, emergency button)
	Provide visual evidence of incident circumstances	Onboard camera video footages; LiDAR data
	Passenger safety verification, emergency response	Vehicle telematics; in-cabin video and audio; AV operator sitrep updates
	Minimising disruption to traffic flow for other vehicles not involved in incident	Vehicle location; planned and alternative routes of AVs

Transport planning [Similar to existing regulations][6]	Route optimisation, service planning, demand forecasting	Passenger trip data (boarding/alighting, journey times, occupancy rates, fares); Vehicle loading and capacity; Route schedule

4. For cybersecurity, the preliminary view is that cybersecurity requirements will need to protect AV cyber-physical asset against all possible attacks, including attacks against sensors and the ADS, to ensure safety.

5. Having considered various international regulatory benchmarks for AVs[7], cybersecurity requirements being considered include not only software update management systems, but also testing requirements on sensors and the automatic driving system.

    a. We are considering implementing UN R155 (Cybersecurity) and UN R156 (Software Updates), as baseline requirements for cybersecurity and software update standards for AVs.

    b. Additional cybersecurity requirements/standards could include ISO 21448 (Safety of the Intended Functionality) and ISO 26262 (Functional Safety).

    c. If these are deemed insufficient, additional specific requirements may be implemented. In general, these will adopt a risk-based approach to be commensurate to operational risks while facilitating technology adoption.

6. In addition, cybersecurity risks present a distinct challenge to the insurability of AVs. As the number of AVs in the fleet increases, the expected damages in the event of a cyber-attack or incident likewise scale up. The potential systemic nature of cybersecurity risks on the fleet-level could lead to prohibitively high premiums. To ameliorate this, we are studying whether to allow for insurance payout caps or exclusions for injuries and property damages caused by cybersecurity breaches.

[6] Data requirements are similar to those under existing regulations (e.g. Point-to-point Passenger Transport Industry Act 2019).

[7] These include (but not limited to) UN Regulations No. 155 and 156 for cybersecurity and software updates, as well as China's GB 44495-2024, GB 44497-2024 and California's Consumer Privacy Act, Code of Regulations (Title 13, Article 3.8) for data management.

Key questions

Data management

1. On data collection for safety validation/performance (i.e. not investigation and liability), a key decision point is the frequency for data transfer to enable quick identification and response to emerging safety issues.

    a. Are there potential concerns and challenges for data to be transferred real-time (e.g. streamed from the AVs or the operators' fleet management systems)?

    b. Would these concerns and challenges be addressed if data is batch-transferred instead (e.g. daily basis when vehicles are returned to the depot)? If yes, how often should such data transfers be?

2. On data collection for incident and traffic flow management, two key decision points are:

    a. Latency for data transfer. What are potential concerns and challenges for the notification to be made immediately after incident occurs (e.g., via bumper sensor data) to facilitate swift incident management? One alternative is to require the notification to be made immediately after the operator is aware (e.g., operators to separately notify via calls/messages) instead – would this alternative be preferred, and why?

    b. Level of detail. To improve on-site incident management and coordination across all parties, we are considering the extent of visual, audio and textual data needed when an incident occurs, so as to minimise the need for frequent and repeated text-only situational reports. Are there potential concerns and challenges with this approach?

3. What are potential concerns and challenges involved in provision of the proposed data, while ensuring data protection and security?

4. Are there alternative suggestions (both technical and process-based) that can address the concerns/challenges while achieving similar purposes and outcomes?

5. What safeguards would help to address data privacy concerns (e.g. anonymisation or pseudonymisation)? What are the industry's views on the technical feasibility and cost of implementing such safeguards?

Cybersecurity

6. What are the industry's views on the proposed cybersecurity baseline requirements and standards (R155, R156, ISO 21448, ISO 26262), and what timeline would be considered practical for implementation? Are there other relevant requirements and standards that we could consider?

7. What cybersecurity testing and validation approaches would the industry be open to undertake to demonstrate comprehensive AV cybersecurity (such as penetration testing, vulnerability assessment, and fuzz testing)? What frameworks or methodologies would be considered effective and feasible?

8. How can injuries, deaths and property damages caused by cyberattacks on AVs be compensated in a financially sustainable way? Are payout caps and exclusions for cybersecurity insurance acceptable?

Chapter D. Advanced Driver Assistance Systems (ADAS) and conditional automation

1. As mentioned in the introduction, the Government's focus in the earlier part of the paper is on AVs that are at high driving automation, where the ADS can handle all aspects of driving within specific ODDs without human takeover.

2. However, the line between conventional manned motor vehicles and AVs are getting blurred with Advanced Driver Assistance Systems (ADAS) and SAE Level 3 (Conditional Automation) vehicles.

3. ADAS in SAE L2 vehicles serve as driver-assist tools under the RTA 1961 and its subsidiary legislations in Singapore.

    a. ADAS features approved for use in Singapore comply with the relevant United Nations (UN) regulations, which put in place constraints to clearly assign responsibility to the drivers (e.g. hands must be on steering wheels when ADAS is engaged).

    b. As such, drivers still oversee the vehicles' automated manoeuvres (if any), and are expected to take over immediately when needed, being ultimately responsible for the vehicles' behaviours on the roads.

    c. Currently, LTA has approved vehicles with L2 features for use on public roads. However, the more advanced L2 features like Tesla's Full Self-Driving (Supervised) has not been evaluated for use in Singapore as it has not been granted type approval under the relevant UN Regulations.

4. SAE Level 3 vehicles with conditional automation can handle driving tasks autonomously under specific conditions, but the human drivers must take over when requested. When active, the human driver is legally allowed to disengage from the actual driving task. This shift necessitates a way to address liability that arises during the transition of control, which is absent in our existing legal regimes.

    a. The takeover transition period (i.e. the window between a clear "Request to Intervene" from the system and the human taking over control) is key. To allow for such vehicles on our roads, we must clarify where the liability lies if accidents take place during this period.

    b. Jurisdictions such as the UK stipulate a maximum transition period, likely based on reasonable human reaction time with buffer. Once this maximum transition period has elapsed, the human driver is expected to gain situational awareness and will be considered in control of and responsible for the vehicle in law, even if he had not physically steered or manoeuvred it.

Key questions

1. For SAE Level 3 vehicles, should we adopt a similar approach as the UK? In other words, have a clear shift of responsibility and liability from the ADS to the human “driver” after the transition period.

2. Alternatively, should we consider:

    a. A shared-responsibility / joint-liability model – both the ADS and human driver are responsible and liable if accidents occur during the transition?

    b. Holding the human driver responsible and liable only if he has physically taken over control of the vehicle?

        i. This means that such SAE Level 3 vehicles must be able to operate safely without immediate human intervention, since the ADS is still responsible if the human driver does not take over despite system prompts.

        ii. The standards for homologation would thus be equivalent to that of SAE Level 4 AVs.

3. Given the regulatory and legal complications, should we have SAE Level 3 vehicles in Singapore?

Annex A. Full list of questions

Chapter A. Responsibility and accountability

1. Does *Table 1* appropriately capture the key AV actors and their respective functions? Are the responsibilities of different AV actors clear and distinct? What other actors (e.g. passengers, individual owners) should be considered, and why?

2. What approach should authorities take to protect public safety while allowing for innovation? Who should authorities hold responsible to oversee AV system updates?

3. What adjustments to the previously approved AVs should require the explicit re-approval of the authorities (e.g. safety-critical functions, hardware modifications, operational scope expansions)?

4. With respect to recognising safety certification from other jurisdictions, how should we strike a balance between minimising red-tape for the industry and safeguarding safety in local conditions?

5. In the event of road safety violations or accidents, would you support holding a single actor responsible in the first instance to facilitate timely compensation for victims? This actor can recover from the at-fault parties subsequently (if it so chooses).

6. If yes for question 5, which AV actor would be in the best position to take on the responsibility? Should it be the entities in-charge of AV tech, fleet operators, or others?

    a. Entity in-charge of AV technology – best understand the underlying technology, have access to the necessary data, can rectify ADS errors quickly, and have the financial capabilities to wear the responsibility.

    b. Fleet operator – have control over the overall service operations and AV maintenance, maintain contractual relationships with both AV providers and passengers, and more likely to be able to deploy customer service / incident response teams onsite to manage the accident.

7. Are there any offences listed in *Table 2* that you think should not be criminal in nature? Is so, should regulatory or financial penalties be used instead? Why?

8. Are there views on how we should more precisely scope the criminal offences in *Table 2*?

9. Are there any additional criminal offences we should consider?

10. Should we introduce statutory presumptions to help victims of AV accidents overcome evidential difficulties in civil cases? What are the possible risks and concerns with doing so? How may these be addressed?

11. Should safe harbour provisions be introduced to limit specific AV actors' liability if reasonable standards have been met? If so, how should they be scoped?

Chapter B. Compensation and insurance

1. To what extent should AV insurance lean towards being more favourable to victims in terms of process than the existing motor insurance regime to achieve timely compensation, at least in the initial phases of deployment? If yes, which option should be selected? Why? Are there other suggestions? How will this affect the overall cost of insurance?

    a. If Option A is selected, how should we allow for goodwill compensation for drawn-out disputed cases? How should we size the quantum, and how should it be funded? Who should administer it? Under what criteria should it be provided?

    b. If Option B is selected, what challenges may AV insurers face when pursuing subrogation claims, and what regulatory provisions should authorities implement to address these obstacles?

    c. If Option C is selected, how can the risk of moral hazards and perverse incentives be mitigated?

2. What is your view on self-insurance, allowing large AV entities to manage their own risk pools rather than purchasing traditional commercial policies?

Chapter C. Data and cybersecurity management

Data management

1. On data collection for safety validation/performance (i.e. not investigation and liability), a key decision point is the frequency for data transfer to enable quick identification and response to emerging safety issues.

    a. Are there potential concerns and challenges for data to be transferred real-time (e.g. streamed from the AVs or the operators' fleet management systems)?

b. Would these concerns and challenges be addressed if data is batch-transferred instead (e.g. daily basis when vehicles are returned to the depot)? If yes, how often should such data transfers be?

2. On data collection for incident and traffic flow management, two key decision points are:

    a. Latency for data transfer. What are potential concerns and challenges for the notification to be made immediately after incident occurs (e.g., via bumper sensor data) to facilitate swift incident management? One alternative is to require the notification to be made immediately after the operator is aware (e.g., operators to separately notify via calls/messages) instead – would this alternative be preferred, and why?

    b. Level of detail. To improve on-site incident management and coordination across all parties, we are considering the extent of visual, audio and textual data needed when an incident occurs, so as to minimise the need for frequent and repeated text-only situational reports. Are there potential concerns and challenges with this approach?

3. What are potential concerns and challenges involved in provision of the proposed data, while ensuring data protection and security?

4. Are there alternative suggestions (both technical and process-based) that can address the concerns/challenges while achieving similar purposes and outcomes?

5. What safeguards would help to address data privacy concerns (e.g. anonymisation or pseudonymisation)? What are the industry's views on the technical feasibility and cost of implementing such safeguards?

Cybersecurity

6. What are the industry's views on the proposed cybersecurity baseline requirements and standards (R155, R156, ISO 21448, ISO 26262), and what timeline would be considered practical for implementation? Are there other relevant requirements and standards that we could consider?

7. What cybersecurity testing and validation approaches would the industry be open to undertake to demonstrate comprehensive AV cybersecurity (such as penetration testing, vulnerability assessment, and fuzz testing)? What frameworks or methodologies would be considered effective and feasible?

8. How can injuries, deaths and property damages caused by cyberattacks on AVs be compensated in a financially sustainable way? Are payout caps and exclusions for cybersecurity insurance acceptable?

Chapter D. ADAS and conditional automation

1. For SAE Level 3 vehicles, should we adopt a similar approach as the UK? In other words, have a clear shift of responsibility and liability from the ADS to the human "driver" after the transition period.

2. Alternatively, should we consider:

    a. A shared-responsibility / joint-liability model – both the ADS and human driver are responsible and liable if accidents occur during the transition?

    b. Holding the human driver responsible and liable only if he has physically taken over control of the vehicle?

        i. This means that such SAE Level 3 vehicles must be able to operate safely without immediate human intervention, since the ADS is still responsible if the human driver does not take over despite system prompts.

        ii. The standards for homologation would thus be equivalent to that of SAE Level 4 AVs.

3. Given the regulatory and legal complications, should we have SAE Level 3 vehicles in Singapore?

Annex B. Summary of regulatory and legal frameworks in other jurisdictions

	Great Britain	China	United States	Germany
Overview	Passed *Automated Vehicles Act (AVA) 2024*, which has yet to come into force pending secondary legislations. The *Automated and Electric Vehicles Act (AEVA) 2018* interacts with the *Automated Vehicles Act (AVA) 2024*, particularly in terms of first-instance liability insurance (see below).	No unified national framework. Regulators and fleet operators/technology provider based in China work very closely, with real-time and direct data access. Generally, liability is attributed based on identified fault of human party or corporate body upon investigations. **Beijing** 1. AV manufacturers responsible for software, hardware and network safety. 2. On-road use case trial entity responsible for overall operations and maintenance.	No unified federal-level framework **Texas** 1. Limited AV-specific provisions 2. Prevailing traffic laws apply to AV owners or authorisation holders **More details on California's approach below.**	*The Autonomous Driving Act 2021* was first enacted through amendments to the Road Traffic Act (StVG) and touches on authorisation process to test AVs on public roads

	Great Britain	China	United States	Germany
		More details on Shenzhen's approach below.		
Key concepts/ definitions	A vehicle travels "**autonomously**" if (i) it is being controlled not by an individual but by equipment of the vehicle, and (ii) neither the vehicle nor its surroundings are being monitored by an individual with a view to immediate intervention in the driving of the vehicle. An "**authorised automated vehicle**" should satisfy a mandatory "self-driving test", which requires the vehicle to: 1. be controlled exclusively by its own equipment, without a human needing to monitor the vehicle or the road environment to intervene.	**Intelligent Connected Vehicles** (ICVs) defined as vehicles that can be operated safely by an automatic driving system instead of a person. The regulations categorise ICVs into three levels: conditional (L3), highly (L4), and fully (L5) automatic driving. Recognises autonomous driving systems as "traffic participants" with defined legal status.	An "**autonomous vehicle**" is any vehicle equipped with "autonomous technology" that meets the definition of SAE Level 3, 4, or 5. "**Autonomous technology**" is defined as technology that has the capability to drive a vehicle without the active physical control or monitoring by a human operator; this explicitly excludes standard driver assistance systems like adaptive cruise control or lane-keep assist.	A "**motor vehicle with autonomous driving capabilities**" is defined as one that can perform the driving task independently within a defined operating area without a person driving the vehicle. This framework specifically addresses SAE Level 4 automation. Introduced the role of a "**Technical Supervisor**", a natural person (i.e. human) who monitors fully driverless vehicle from the outside and can deactivate it or enable manoeuvres remotely.

	Great Britain	China	United States	Germany
	2. achieve a safety level equivalent to, or higher than, that of careful and competent human drivers; and 3. be able to follow all traffic regulations without a human driver. Authorised Self-Driving Entities (**ASDE**): Entity legally responsible for ensuring an AV's compliance with safety standards when in autonomous mode. User-in-Charge (**UiC**): A person is in the vehicle, ready to take control if needed. No-User-in-Charge (**NUiC**): No person is in the vehicle. Instead, a licensed NUiC operator oversees the journey remotely, ensuring safety and compliance.			

	Great Britain	China	United States	Germany
Licensing	Automated Passenger Services (**APS**) permitting scheme 1. A new licensing regime introduced for services offering automated passenger transport (e.g., robotaxis and driverless shuttles) 2. These services must meet rigorous safety, operational, and regulatory requirements before being allowed to operate. 3. APS operators must submit safety cases, monitor real-world performance, and comply with incident reporting regulations.	For ICVs to be included in the Shenzhen-specific catalog and be sold/registered, manufacturers must submit documentation proving products meet local standards and undergo review by municipal industry and information technology authorities. Fully automated (driverless) vehicles are restricted to designated zones and sections approved by municipal traffic authorities; companies must obtain a Commercial Operation Permit.	To move to commercial deployment, manufacturers must certify a safe "minimal risk state" (ability to come to a complete stop) if a system failure occurs. Commercial robotaxis passenger services require an additional layer of licensing.	-
Responsibilities / Liability	When the vehicle is operating in automated mode, the UiC is not liable for driving-specific offences, unless a transition demand is	In human-driver operation (L3/L4), the human driver bears primary liability for compensation.	AV developers/ manufacturers responsible for product defects and incidents reporting.	Assigns "strict liability" through the “Halter" (Keeper) Principle – vehicle keeper (owner / fleet operator) remains strictly liable

	Great Britain	China	United States	Germany
	issued and the UiC fails to take control when required by the system. This immunity only applies when the vehicle is engaged in automated driving. UiC also re-acquires the legal obligations of a driver at the end of the transition demand period, whether or not they have taken control of the vehicle.	In driverless operation (L4/L5), primary liability shifts to the vehicle owner or operation manager (the Operation Entity).	They must provide evidence of financial responsibility in the amount of USD5 million (e.g. insurance, surety bonds, or proof of ability to self-insure) before testing can commence.	for damages regardless of fault. Up to €10 million for personal injury and €2 million for property damage. Mandates third-party motor insurance explicitly covering the autonomous system. AV manufacturers are subject to existing product liability.
Compensation and insurance	First-instance liability refers to the insurance payout made to the victim immediately after an incident, even before fault is determined. AEVA required insurers to cover accidents involving automated vehicles, with insurers making the first-instance payout. AVA builds on this framework, clarifying that	"Pay First, Recover Later" compensation rule to ensure victims are compensated immediately by the responsible party, who then has a statutory right to seek recovery from the manufacturer for product defects.	Prevailing negligence-based liability applies to AV operators/owners, and strict product liability for AV manufacturers (i.e. liable if the technology was defective and unreasonably dangerous when it left their control, even without proof of negligence).	AV owners must get additional liability insurance for the Technical Supervisor, who carries liability for negligence.

	Great Britain	China	United States	Germany
	insurance obligations shift when the vehicle is operating in automated mode. The ASDE/NUiC operator remains legally accountable for any further compensation claims following the incident. A "User-in-Charge" is treated as a third party and can claim compensation from their own vehicle's insurer for injuries during a system-led crash. Insurers have a statutory right to recover the outlay from the manufacturer if a software defect is found.	Registrants must prove they have Compulsory Traffic Accident Liability Insurance and additional Passenger Insurance for taxis.		
Data requirements	New criminal offences address manufacturers who misrepresent safety or withhold critical information.	Regulations mandate the use of Event Data Recorders (EDRs) to capture safety-critical parameters Incident data must be shared with statutory	Under California Vehicle Code §38750, a specialised autonomous technology data recorder is required for AVs. It must capture and store autonomous technology sensor data for at least	The StVG (§ 1g) requires operational data storage for six months, extended to three years if an accident occurs.

	Great Britain	China	United States	Germany
		inspectors under a "no-blame" model: 1. Intended for systemic learning. Focus is on data as an enabler for safety and "no-blame" investigation. 2. ASDEs must provide accurate safety data EDRs and withholding it is a criminal offense. 3. Manufacturers must implement "privacy-by-design" to minimise personal data collection. 4. Listed ICVs must be registered and connected to the government supervision platform.	30 seconds before a collision and only in read-only format The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) prioritises consumer rights allowing residents to opt-out of data sales. Manufacturers must obtain written approval for non-essential data (commercial profiling/entertainment) and cannot deny service if a user withholds this consent. Strictly necessary data (LiDAR/GPS/Black box logs) is defined as direct input for the driving task or accident reconstruction.	AVs must record manual versus automated control and instances of supervisor intervention. While the StVG mandates storage, the Federal Data Protection Act (BDSG) ensures that identifiers like Vehicle Identification Numbers (VINs) are treated as personal data, requiring high levels of encryption and access control.

	Great Britain	China	United States	Germany
		5. Sensitive data must be stored on domestic servers within China; cross-border transfer requires security review.	Transparency is maintained through mandatory collision reports and annual disengagement reports.	