Risk assessment of cybersecurity for route buses and electric vehicles

Trafikselskabet Movia

September 2026

The better the question. The better the answer.
The better the world works.

Shape the future with confidence

Glossary

Abbreviation	Definition(s)
A.	Annex (as used in UN Regulations and ISO standards)
ADAS	Advanced Driver Assistance Systems
APC	Automatic Passenger Counting
BMS	Battery Management System
CAN	Controller Area Network
CoC	Certificate of Compliance
CSMS	Cyber Security Management System (as defined in UN Regulation R155)
CCTV	Closed-Circuit Television
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DoS	Denial of Service
ECU	Electronic Control Unit
EEA	European Economic Area
EU	European Union
EV	Electric Vehicle
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
GPS	Global Positioning System
HSM	Hardware Security Module
IAM	Identity and Access Management
IR	Incident Response
ISMS	Information Security Management System (as defined in ISO/IEC 27001)
ISO	International Organization for Standardization
ISO 24089	International standard for road vehicle software update engineering
ISO 26262	International standard for functional safety of road-vehicle electrical and electronic systems
ISO/IEC 27001	International standard for Information Security Management Systems

Abbreviation	Definition(s)
ISO/SAE 21434	International standard for Road Vehicle Cybersecurity Engineering
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
OTA	Over-The-Air (software update or communication mechanism)
PSIRT	Product Security Incident Response Team
PTA	Public Transport Authority
PTO	Private Transport Operator
RXSWIN	Software Identification Number Register (as defined in UN Regulation R156)
R155	UN Regulation No. 155 - Cybersecurity and Cybersecurity Management System
R156	UN Regulation No. 156 - Software Update and Software Update Management System
R157	UN Regulation No. 157 - Automated Lane Keeping Systems (type-approval of automated driving functions)
SBOM	Software Bill of Materials
SCC	Standard Contractual Clauses (for international data transfers under GDPR)
SLA	SLA - Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedure
SUMS	Software Update Management System (as defined in UN Regulation R156)
TARA	Threat Analysis and Risk Assessment
USB	Universal Serial Bus
VIN	Vehicle Identification Number
V&V	Verification and Validation
Wi-Fi	Wireless Fidelity

Executive summary

This report assesses cybersecurity risks related to electric buses used by operators on Movia's routes and selected electric vehicles relevant to Movia's Flextrafik. Movia does not own or operate the buses. Movia acts as the public transport authority (PTA), while private transport operators (PTOs) procure, own, operate and maintain the buses and are responsible for compliance with applicable vehicle regulation. Movia's direct cybersecurity responsibility for onboard equipment is limited to systems owned or controlled by Movia, such as the Basiskort ticketing system.

The electric buses in scope are the models currently used by operators on Movia's routes, supplied by Yutong, BYD, MAN, Ebusco, Volvo, Golden Dragon, Mercedes-Benz/Daimler Buses and VDL. For Flextrafik, the assessment includes Tesla Model 3/Model Y and a Chinese EV reference platform, BYD Seal U. The assessment is based on questionnaire responses, available documentation and desktop analysis. It does not constitute technical testing, audit assurance or a guarantee that vehicles are free from vulnerabilities.

1. Is the existing cybersecurity regulation for buses and cars sufficient?

UN R155 and UN R156 are vehicle type-approval regulatory requirements applicable in the EU and Denmark. They are complemented by ISO/SAE 21434 and ISO 24089, which are standards and engineering frameworks rather than legislation. GDPR applies where vehicle systems, onboard systems or backend systems process personal data, including external cameras, ADAS sensors, GPS/location data, CCTV, ticketing data or telemetry where individuals can be identified. NIS2 and its Danish implementing legislation are relevant to Movia and to operators and suppliers where they are within scope, particularly for organisational cybersecurity, governance and incident handling. Together, these instruments provide a largely sufficient baseline for modern connected vehicles, provided that they are implemented, maintained and documented in practice.

2. Do the electric buses used on Movia's routes and selected EVs for Flextrafik comply with the regulation?

The assessment shows clear differences in the level of documented evidence provided for manufacturers and vehicle models. In this report, "compliance" means demonstrable alignment with the requirements assessed in the questionnaire. It is not a formal legal certification opinion and it is not a direct risk rating.

The detailed domain scores are presented in section 2.2 and should be read together with the methodology limitations in section 1.3 and the risk assessment in section 3. High documented maturity does not mean that operational risk is eliminated. Conversely, low documented maturity does not automatically mean immediate unsafe operation. The findings should primarily be used to define assurance, evidence and contractual governance requirements.

Table 1: Documented alignment scores by domain

Domain	VDL	EBUSCO	BYD	Golden Dragon	Yutong	Daimler/ Mercedes-Benz	MAN	Tesla[1]	BYD Seal U
Governance	10%	90%	100%	86%	100%	86%	100%	100%	100%
Risk analysis	0%	95%	100%	100%	95%	90%	85%	100%	100%
Architecture	56%	100%	100%	100%	100%	78%	100%	100%	100%
Software updates	40%	60%	90%	90%	100%	70%	90%	100%	90%
Validation	8%	100%	100%	92%	100%	92%	100%	100%	100%
Incident response	14%	43%	79%	86%	93%	64%	86%	100%	79%

1) The assessment for Tesla and BYD Seal is based exclusively on publicly available information derived from model type approvals and related documentation from supervisory authorities and regulators. This indirect source of evidence does not provide the same level of detail or confirmation as manufacturer-completed questionnaires and should be interpreted accordingly when comparing results across manufacturers. The models that were analyzed this way are Tesla Model 3 and Model Y and the BYD Seal U.

Yutong, BYD, Golden Dragon and MAN demonstrate high documented cybersecurity maturity across most assessed domains. Ebusco demonstrates an intermediate maturity level. Daimler Buses/Mercedes-Benz shows generally strong maturity, though some gaps remain. VDL shows low demonstrability for the assessed Citea SLF 120 E and Citea SLFA 180 E buses. These buses were delivered before UN R155 and UN R156 entered into force and are understood not to be OTA-enabled, which reduces the practical risk of remote fleet-wide software compromise but also limits formal lifecycle assurance, monitoring and auditability.

Volvo 7900E is included in the operational scope. No questionnaire or equivalent evidence has been received for Volvo, which should be treated as an evidence gap and not as a negative cybersecurity conclusion. Tesla is assessed on public regulatory documentation. BYD Seal U is included as the selected Chinese EV reference platform and scored using the BYD evidence profile; it should be interpreted as an EV platform assessment rather than a bus-model questionnaire result.

3. What are the risks of remote control of buses and cars, and what can Movia do?

The main risks arise from legitimate remote access, OTA software updates, backend dependencies, privileged supplier access, insider misuse or error, non-OEM onboard systems and charging infrastructure dependencies. These risks may affect vehicle availability, service continuity, safety-relevant functions, data protection and public trust.

The highest priority risks for Movia are:

Priority	Risk area	Recommended mitigation focus
1	Remote access, OTA updates and backend dependencies	Transparency, logging, deactivation rights, incident escalation, staged rollout and rollback
2	Software-update governance and incident-response gaps	R155/R156 evidence, update governance, response-time targets and audit rights
3	Legacy vehicles outside R155/R156	Minimum cybersecurity baseline, workshop-access controls, documented update process and incident contacts
4	Non-OEM onboard systems and personal data	Segmentation, supplier controls, access logging, data retention and incident reporting
5	Charging infrastructure dependency	IEC 62443 or equivalent, physical/network security, incident handling and fallback plans
6	Advanced ADAS/autonomous functions	Manual fallback, disablement of automated functions, weak-signal reporting and operational thresholds

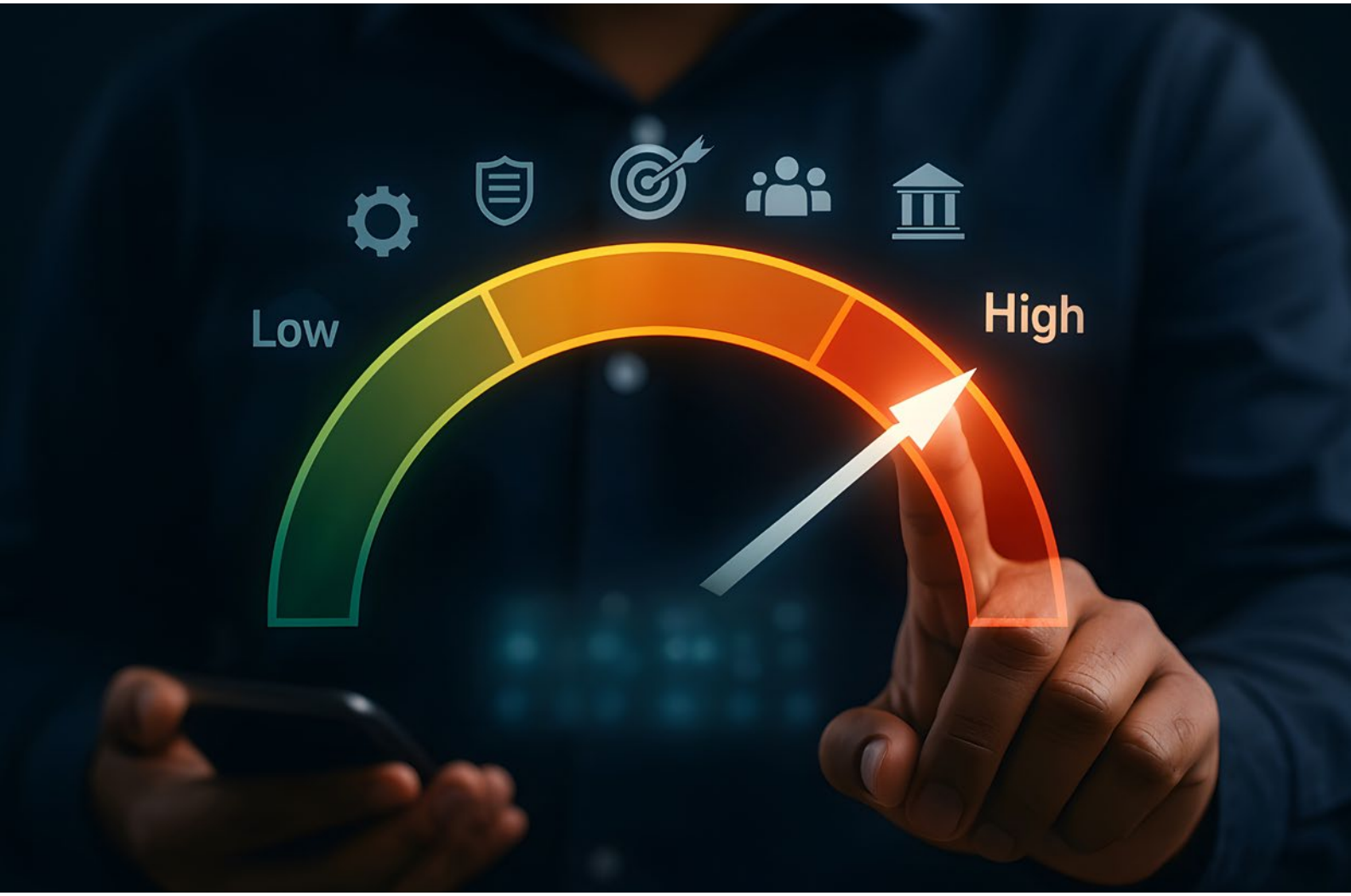
High manufacturer cybersecurity maturity is necessary but not sufficient. Movia's exposure depends less on direct technical control and more on its ability to demand transparency, define decision rights in advance, require evidence and contain fleet-level impact when uncertainty arises.

4. Will further implementation of autonomous technology increase remote-control risk?

Further automation and Advanced Driver Assistance Systems (ADAS) maturity increase reliance on software, sensor fusion, backend services and remote configuration. This can increase the scale and speed at which failures, misconfigurations or compromised remote pathways may affect multiple vehicles. The most significant risk increase is therefore not only the probability of intrusion, but the potential fleet-wide impact. Movia should require safe fallback behavior, full driver takeover, staged software rollout, rollback capability, monitoring of weak signals, and predefined containment measures.

5. Which contract changes should Movia make?

Movia should avoid bespoke cybersecurity requirements that are difficult to verify and enforce. Instead, future tenders and contracts should rely primarily on recognized standards and objective, evidence-based requirements. Recommended requirements include compliance with UN R155 and UN R156 where applicable, ISO/SAE 21434 alignment for vehicle cybersecurity engineering, ISO 24089 alignment for software update engineering, ISO/IEC 27001 or equivalent for relevant operator and backend environments, IEC 62443 or equivalent for charging infrastructure, incident notification obligations, audit and evidence rights, minimum requirements for older non-R155/R156 vehicles, GDPR-compliant data handling, and concrete rights to deactivate connected functions such as OTA updates, remote access and automatic data transfer on short notice.



Content

1 Introduction

1. Introduction

1.1. Background

Movia is the public transport authority (PTA) for Eastern Denmark, except the island of Bornholm. Movia plans the public bus network, prepares tenders, defines functional and technical requirements for bus services, and awards contracts to private transport operators (PTOs). The PTOs are responsible for procuring, owning, operating and maintaining the buses, including the choice of vehicle manufacturer and model, the deployment of charging infrastructure and compliance with applicable regulations.

The buses used by operators on Movia's routes increasingly rely on software-defined functionality, remote diagnostics, backend services and, for some models, Advanced Driver Assistance Systems (ADAS) and over-the-air (OTA) update capabilities. These technologies can improve safety, maintenance and operational efficiency, but they also expand the cybersecurity attack surface beyond the physical vehicle to include vehicle networks, operator IT systems, OEM backend platforms, cloud services, workshop tools, charging infrastructure and remote maintenance interfaces.

Movia's direct cybersecurity responsibility for onboard systems is limited to systems owned or controlled by Movia, such as the Basiskort ticketing system. Other onboard systems, including OEM vehicle systems, operator-procured passenger information systems, infotainment, automatic passenger counting equipment and charging systems, are primarily the responsibility of the relevant operator and its suppliers.

Operators contracted by Movia use electric buses manufactured by Yutong, BYD, MAN, Ebusco, Volvo, Golden Dragon, Mercedes-Benz/Daimler Buses and VDL. Recent findings in Norway[2], including Ruter's test of electric buses from Yutong and VDL, confirmed that remote access capabilities may exist in modern electric buses. The Ruter test indicated that the Yutong bus could receive remote updates through built-in connectivity, while the older VDL bus tested was not OTA-equipped. These findings illustrate that safety, cybersecurity and service continuity increasingly depend on systems and suppliers outside Movia's direct technical control.

The purpose of this assessment is therefore to assess whether the existing cybersecurity regulation is adequate, whether the relevant electric buses and selected EVs demonstrate alignment with that regulation, what risks arise from remote access and increasing vehicle automation, and what contractual measures Movia can use to reduce cybersecurity risk.

1.2. Purpose

The purpose of this assessment is to provide Movia with an understanding of cybersecurity and cyber-physical risks related to electric buses used by operators on Movia's routes and selected electric vehicles relevant to Movia's Flextrafik.

The assessment addresses five questions:

1. whether the existing cybersecurity regulation for buses and cars is adequate;
2. whether the electric buses used by operators on Movia's routes and selected EVs relevant to Flextrafik demonstrate alignment with the applicable regulation;
3. what risks arise from remote access, remote control or remote deactivation of buses and cars, and how Movia can mitigate these risks;
4. whether further implementation of autonomous or highly automated vehicle technologies may increase cybersecurity and remote-control risks, and how Movia can mitigate such risks; and
5. which changes Movia should consider for bus and Flextrafik contracts to reduce cybersecurity risks for electric buses and EVs.

The assessment covers electric bus models currently used by operators on Movia's routes, including models with and without ADAS and OTA capabilities. It also covers selected EV platforms relevant to Flextrafik. Tesla Model 3 and Model Y are included as highly software-defined EVs with extensive connectivity and ADAS functionality. BYD Seal U is included as a Chinese EV reference platform to address the Chinese EV element of the Terms of Reference.

The assessment does not assume that Movia has technical control over OEM vehicle systems. Instead, it focuses on how cybersecurity risks may affect Movia as PTA and contracting authority, and how Movia can manage these risks through tender requirements, contractual obligations, evidence rights, escalation mechanisms and governance.

2) https://ruter.no/ruter-med-omfattende-sikkerhetstest-av-elektriske-busser

1.3. Methodology and scope

The assessment consists of two main parts: a compliance-oriented desktop assessment and a risk assessment.

The compliance-oriented assessment is based on a structured questionnaire aligned with UN R155, UN R156 and ISO/SAE 21434. The questionnaire assesses whether manufacturers can demonstrate the existence and documented application of cybersecurity governance, risk analysis, architecture, software-update management, validation and incident-response processes for the assessed vehicle types.

The assessment is inquiry-based. It reflects the presence and description of processes and controls as reported by manufacturers or identified in available documentation. Responses have not been independently verified, tested or validated through technical testing, onsite inspection, penetration testing or audit. The assessment therefore does not constitute an assurance opinion on the operational effectiveness or security of vehicles.

The questionnaire's results concern the specific electric bus models currently used by operators on Movia's routes. They do not necessarily reflect cybersecurity practices in newer or different vehicle models from the same manufacturers. Where manufacturers or operators have stated that cybersecurity protection does not materially differ between versions or year variants of the same assessed model, this has been treated as part of the evidence base. Where such evidence is missing, the assessment is limited accordingly.

The risk assessment builds on the compliance-oriented findings, market knowledge and publicly available threat information. Because the available data does not support statistical assessment of incident probability, risks are ranked qualitatively based on potential impact for Movia, systemic exposure, dependency on external parties and availability of practical mitigation measures.

No questionnaire or equivalent evidence has been received for Volvo, which should be treated as an evidence gap and not as a negative cybersecurity conclusion.

Selected EV platforms in scope are Tesla Model 3, Tesla Model Y and BYD Seal U.

The EV assessment for Flextrafik is based on available documentation for Tesla Model 3/Model Y and BYD Seal U. The evidence base for EVs is less detailed than for manufacturers that completed the questionnaire, and EV conclusions should therefore be interpreted as indicative of risk categories rather than as a full comparative market assessment.

Electric bus models in scope

Manufacturer	Model(s) in scope	Number of in-service buses
Yutong	E12, U12, E15, E9	299
BYD	B12E03, B13E01, B19, K9UD	259
MAN	Lion's City 12 E	67
Ebusco	Ebusco 2.2, 12 m	49
Volvo	7900E	29
Golden Dragon	E12, E13	27
Daimler Buses / Mercedes-Benz	eCitaro	26
VDL	Citea SLF 120 E, Citea SLFA 180 E	23

The number of buses refers to in-service buses and does not include spare buses. The assessment concerns the listed vehicle models used by operators on Movia's routes and should not be read as a general assessment of all current or future models from the same manufacturers.

2 Compliance Assessment

2. Compliance Assessment

2.1. Analysis of existing legislation

Jointly, UN R155, UN R156, ISO/SAE 21434, ISO 24089 and the General Data Protection Regulation (GDPR) provide a complementary framework for addressing cybersecurity and data-protection risks associated with electric buses and EVs. The framework covers cybersecurity governance and lifecycle risk management, control of software updates, cybersecurity engineering, validation practices and data-protection principles for systems that process personal data.

2.1.1. UN Regulation 155

UN R155 addresses cybersecurity risks at the vehicle-type and lifecycle level and requires manufacturers to establish and operate a Cyber Security Management System (CSMS). The CSMS provides the organizational and governance framework through which cybersecurity risks are systematically identified, assessed, treated, monitored and reviewed across the development, production and post-production phases of the vehicle lifecycle.

A core function of the CSMS is to ensure that cybersecurity risks are continuously managed over time, including post-production monitoring, incident handling and vulnerability management. Under UN R155, manufacturers are required to perform a Threat Analysis and Risk Assessment (TARA) covering vehicle systems, interfaces, backend connectivity and supplier dependencies, and to update this analysis when changes or incidents occur.

2.1.2. UN Regulation 156

UN R156 addresses cybersecurity and integrity risks associated with software updates. It requires manufacturers to establish and operate a Software Update Management System (SUMS), which provides the governance and control framework for managing software updates in a secure, controlled and auditable manner throughout the vehicle lifecycle.

The SUMS limits the risk that faulty, incompatible or malicious updates are deployed at scale. It requires traceability and version control, compatibility verification, integrity and authenticity controls, and safe execution or recovery where updates fail or affect safety-relevant systems.

2.1.3. ISO/SAE 21434 and ISO 26262

ISO/SAE 21434 provides an engineering framework for implementing cybersecurity controls at system, software and organizational levels. It supports security-by-design and security-by-default principles throughout the engineering lifecycle and provides traceability from risks to requirements, implementation and verification. It should be read as an implementation standard complementing UN R155.

ISO 26262 is the established standard for functional safety of road-vehicle electrical and electronic systems. It is closely related to ISO/SAE 21434: cybersecurity weaknesses can have functional-safety consequences, and mature manufacturers coordinate the two disciplines so that security controls do not undermine safety and vice versa. For this assessment, the application of ISO 26262 alongside ISO/SAE 21434 is treated as an indicator of engineering maturity, because it shows that the manufacturer manages the interaction between safety and cybersecurity in a structured way.

2.1.4. ISO 24089

ISO 24089 provides guidance for road vehicle software update engineering. It complements UN R156 by describing engineering practices for planning, developing, validating, releasing and maintaining software updates across the vehicle lifecycle.

Where UN R156 defines regulatory expectations for the Software Update Management System (SUMS), ISO 24089 provides more detailed support for how software update activities can be engineered and controlled in practice. This includes update planning, compatibility considerations, release management, update verification, documentation, traceability and post-update monitoring.

For this assessment, ISO 24089 is relevant because software updates are a key risk vector for connected electric buses and EVs. Use of ISO 24089 or equivalent practices strengthens assurance that software updates are not only governed at management-system level, but also engineered, validated and deployed in a controlled and auditable way.

2.1.5. General Data Protection Regulation (GDPR)

GDPR applies where personal data is processed by vehicle systems, backend systems, operator systems or Movia-owned systems. This is not limited to ADAS-equipped buses. It may include CCTV, passenger counting, ticketing systems, vehicle telemetry, GPS data, driver-related records and remote connectivity data where individuals are identifiable or can reasonably be linked to data.

Article 25 requires data protection by design and by default, including data minimization and purpose limitation. Article 5(1)(f) requires appropriate security to protect personal data against unauthorized or unlawful processing and accidental loss, destruction or damage. These obligations align with cybersecurity objectives but apply specifically to personal-data processing.

2.1.6. Sufficiency of existing legislation

UN R155, UN R156, ISO/SAE 21434 and ISO 24089 provide a largely sufficient framework for managing cybersecurity risks in modern connected electric buses and EVs. If manufacturers fully and demonstrably comply with these frameworks, the main cybersecurity risks are addressed through lifecycle cybersecurity governance, structured risk analysis, secure architecture, controlled software updates, validation, monitoring and incident response.

However, the framework should not be understood as a guarantee that vehicles are secure in operation. First, the practical effect depends on demonstrable implementation, not only formal certification. Second, older vehicle models

placed into service before UN R155 and UN R156 became mandatory may not be covered by the same lifecycle requirements. Third, the framework primarily addresses OEM vehicle systems and does not fully address non-OEM onboard systems installed by operators or Movia, such as passenger counting, infotainment, ticketing or CCTV systems. Fourth, the regulation itself does not give Movia contractual transparency, escalation rights or operational decision rights.

The answer to whether electric buses would be secure if manufacturers comply with existing regulations is therefore: largely yes from a vehicle cybersecurity governance and engineering perspective, but not absolutely. Compliance materially reduces risk, but residual risk remains in relation to operational use, supplier dependencies, non-OEM equipment, data protection, legacy vehicles and fleet-level incident handling.

For Movia, the regulatory framework is therefore sufficient as a baseline for future tenders, but it must be translated into enforceable contractual requirements requiring evidence, transparency, incident notification, audit rights and operational escalation mechanisms.

The sufficiency of the framework must also be judged against the specific connected subsystems that capture or transmit data, including cameras, microphones, GPS, impact and motion sensors, and the traction battery and its battery management system (BMS). UN R155 brings these within scope through its threat catalogue (Annex 5) and its requirement for a vehicle-level cybersecurity risk assessment, and UN R156 governs the integrity of software updates to the electronic control units behind them. The framework is therefore largely sufficient to require manufacturers to consider these subsystems, but it does not in itself guarantee that any individual camera, microphone, positioning function or battery interface is protected to a defined level. For Movia, this means that contractual requirements should explicitly address the confidentiality, integrity and availability of camera, microphone, positioning, motion-sensor and traction-battery data rather than relying on type-approval alone.

2.2. Manufacturer compliance

To assess the degree to which cybersecurity is structurally embedded in the design, governance and lifecycle management of the assessed vehicles, manufacturers were assessed using a structured questionnaire aligned with UN R155, UN R156 and relevant clauses of ISO/SAE 21434. The questionnaire is structured around six domains: governance, risk analysis, architecture, software updates, validation and incident response.

Compliance in this report means demonstrable alignment with the requirements assessed in the questionnaire. It is not a formal legal certification opinion. Positive responses indicate that the manufacturer demonstrates traceable and auditable implementation of a requirement, while negative responses indicate that the requirement is not demonstrated, only partially implemented, or out of scope for the assessed vehicle type.

The questionnaire responses and scores relate to the specific in-service electric bus models used by operators on Movia's routes. They should not be interpreted as a general assessment of all current or future vehicles from the same manufacturers. In particular, older vehicles placed into service before UN R155 and UN R156 became mandatory may have a different cybersecurity profile than newer vehicles from the same OEM. Conversely, newer models may comply with regulatory requirements that did not apply when older vehicles were delivered.

Manufacturer domain scores

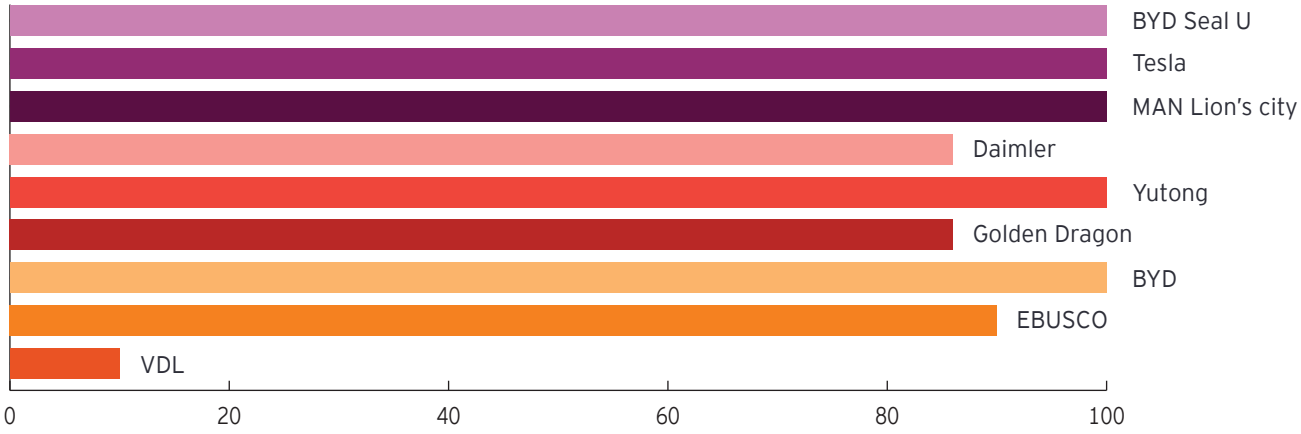
Domain	VDL	EBUSCO	BYD	Golden Dragon	Yutong	Daimler	MAN Lion's city	Tesla	BYD Seal U
Governance	10%	90%	100%	86%	100%	86%	100%	100%	100%
Risk analysis	0%	95%	100%	100%	95%	90%	85%	100%	100%
Architecture	56%	100%	100%	100%	100%	78%	100%	100%	100%
Software updates	40%	60%	90%	90%	100%	70%	90%	100%	90%
Validation	8%	100%	100%	92%	100%	92%	100%	100%	100%
Incident response	14%	43%	79%	86%	93%	64%	86%	100%	79%

2.2.1. Governance

Under UN R155 and R156, manufacturers are required to establish and operate CSMS and SUMS frameworks. BYD, BYD Seal U, Yutong, MAN and Tesla demonstrate full coverage in the assessed governance requirements. Ebusco, Golden Dragon and Daimler Buses demonstrate strong but not complete alignment.

For the assessed VDL Citea SLF 120 E and Citea SLFA 180 E buses, governance demonstrability is low. These VDL buses were delivered to one of Movia's operators in 2019, before UN R155 and UN R156 entered into force. The result should therefore be understood as an assessment of legacy vehicles rather than as a general assessment of VDL's current cybersecurity maturity or newer VDL models. Available information indicates that the assessed VDL buses are not OTA-equipped and that software access is primarily workshop-based. This reduces practical remote-update exposure but does not remove concerns regarding limited lifecycle assurance, monitoring and auditability.

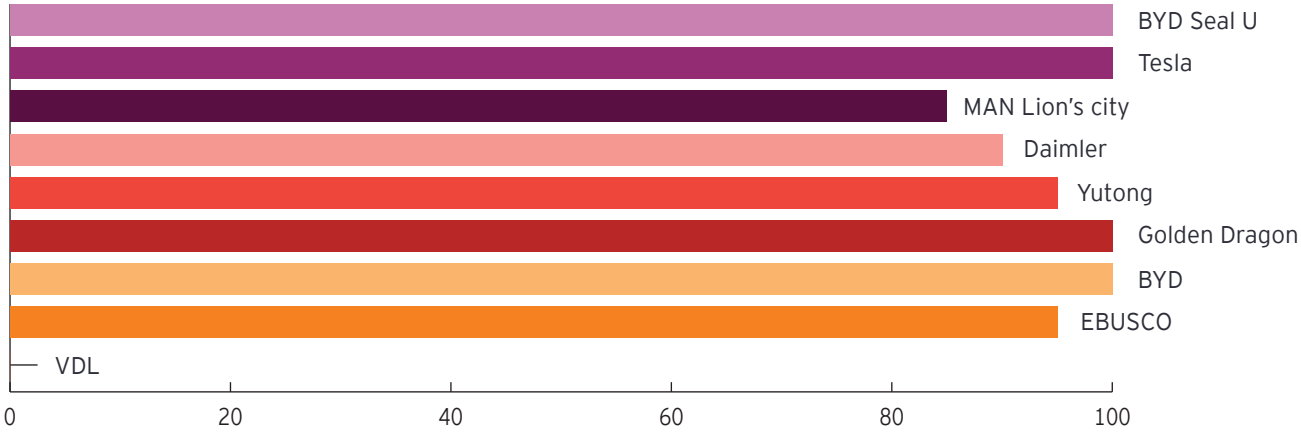
Governance



2.2.2. Risk analysis

UN R155 requires vehicle-type-specific cybersecurity risk analysis across the vehicle lifecycle. BYD, BYD Seal U, Golden Dragon and Tesla show full demonstrability in the assessed risk-analysis requirements. Ebusco and Yutong show high maturity with minor evidence gaps, while Daimler Buses and MAN show generally strong practices with specific gaps in documented TARA work products, retest evidence or formal risk acceptance. VDL shows no demonstrable alignment in the risk-analysis domain for the assessed legacy models, which limits transparency regarding residual cybersecurity risk.

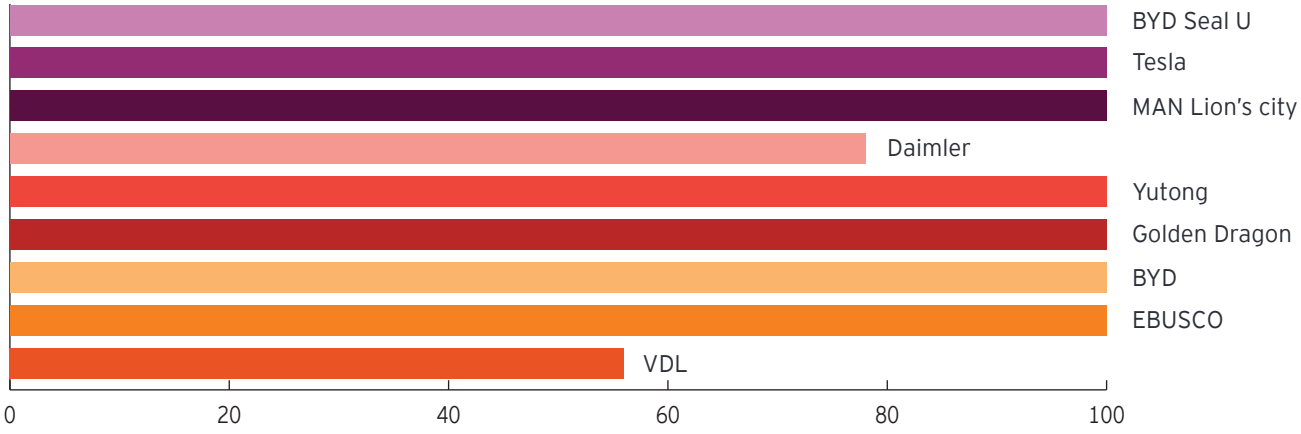
Risk analysis



2.2.3. Architecture

A mature cybersecurity architecture limits propagation from non-critical systems to safety-relevant domains through segmentation, trust boundaries and controlled interfaces. Ebusco, BYD, BYD Seal U, Golden Dragon, Yutong, MAN and Tesla demonstrate full alignment in the assessed architecture requirements. Daimler Buses demonstrates moderate to high maturity but with gaps related to network segregation and secure boot/runtime integrity evidence. VDL demonstrates partial architectural controls, including protected diagnostics and disabled development interfaces, but lacks full documentation of interfaces, cybersecurity requirements and zoning.

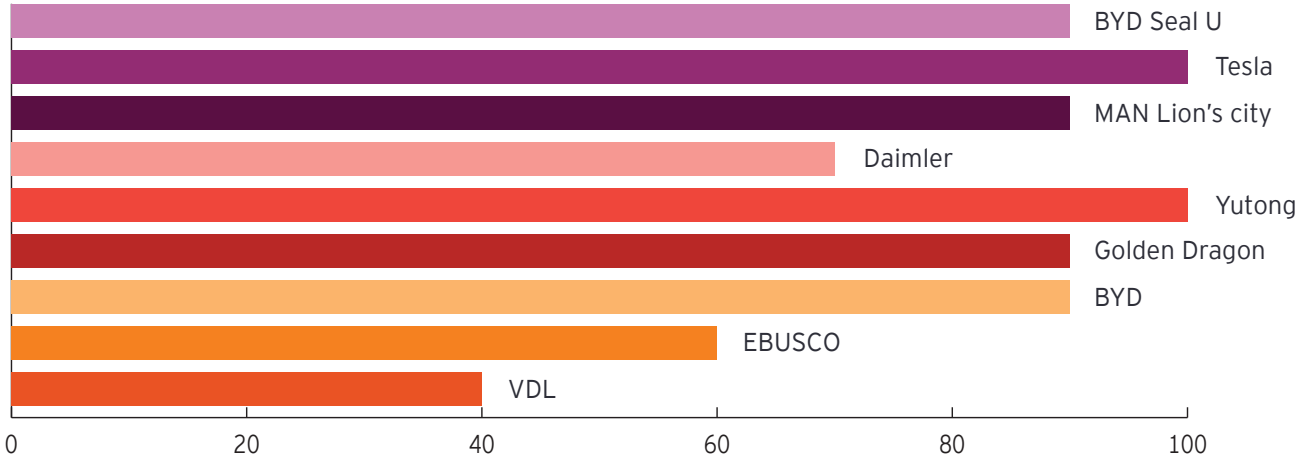
Architecture



2.2.4. Software updates

UN R156 requires controlled software update processes, including authenticity, integrity, compatibility, traceability, safe execution and recovery. Yutong and Tesla demonstrate full documented alignment in the assessed update domain. BYD, BYD Seal U, Golden Dragon and MAN demonstrate high maturity with specific gaps such as SBOM availability or safe-state evidence during updates. Daimler Buses and Ebusco show moderate maturity with gaps in cryptographic signing, rollback, SBOM or rollout evidence. For the assessed VDL legacy buses, the absence of OTA capability reduces remote update exposure, but workshop-based updates should still be controlled, logged and restricted to authorized personnel.

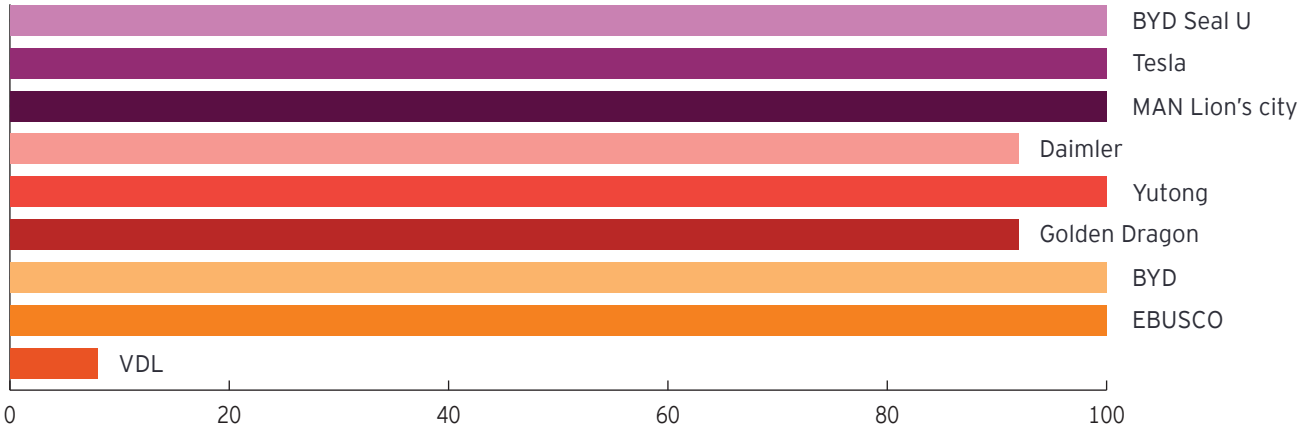
Software updates



2.2.5. Validation

Validation concerns whether cybersecurity measures are tested and operated as intended. BYD, BYD Seal U, Ebusco, Yutong, MAN and Tesla demonstrate full alignment in the assessed validation requirements. Golden Dragon and Daimler Buses show substantial alignment with limited gaps, such as real operational scenario coverage or vehicle-level validation evidence. VDL shows limited demonstrability, increasing uncertainty regarding the effectiveness of controls on the assessed legacy platform.

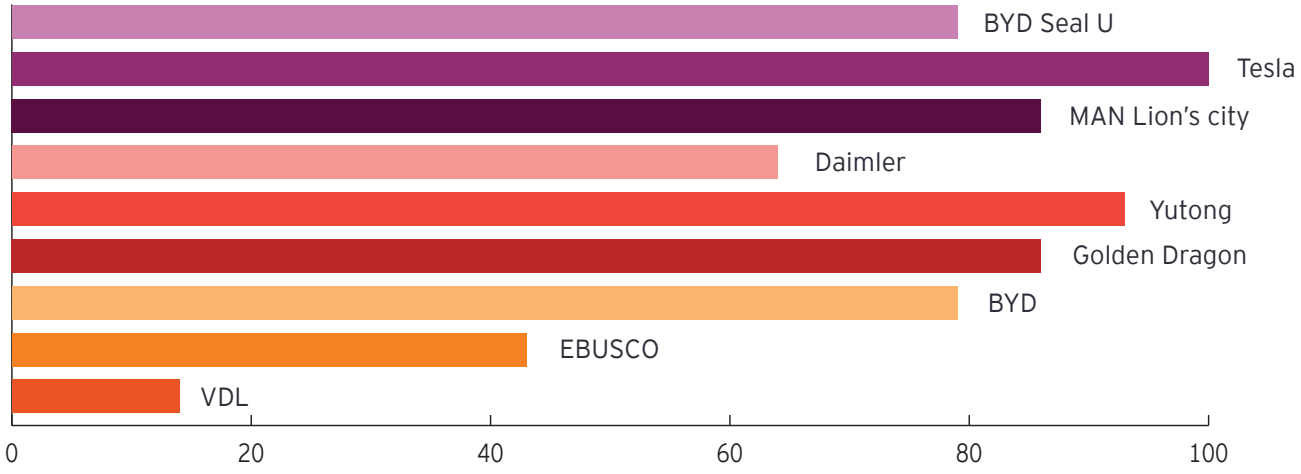
Validation



2.2.6. Incident response

Incident response addresses the ability to monitor, detect, respond to and learn from cybersecurity incidents. Tesla and Yutong demonstrate the highest assessed incident-response maturity. Golden Dragon, MAN, BYD and BYD Seal U demonstrate relatively strong capabilities, while Daimler Buses and Ebusco show moderate capabilities with gaps in technical detection, backend resilience, triage or forensic evidence. VDL shows limited incident-response demonstrability for the assessed legacy models. For legacy non-OTA vehicles, the main concern is less remote fleet-wide update compromise and more limited monitoring, logging, escalation and workshop-access traceability.

Incident response



2.3. Non-OEM onboard systems, personal data and cybersecurity management

The manufacturer questionnaire primarily concerns OEM vehicle systems. It does not fully cover non-OEM systems installed in buses by operators, subcontractors or Movia. These systems include automatic passenger counting equipment, passenger information and infotainment systems, CCTV and video surveillance systems, operator IT equipment, charging-related systems and depot interfaces, and Movia-owned or Movia-controlled systems, including the Basiskort ticketing system.

These systems may generate or process personal data. CCTV and video surveillance data are personal data where individuals can be identified. Passenger counting systems may process images, sensor signals or movement data before generating aggregated passenger counts, depending on the technical design. Ticketing systems may process travel, transaction or identifier data. Vehicle telemetry, GPS and operational logs may also become personal data where linked to drivers, routes, operational events or other identifiable persons.

The personal data generated by these systems is generally not expected to create the same direct safety risk as compromise of vehicle control, braking, steering, propulsion or OTA-update systems. However, the data can still be relevant from a GDPR, confidentiality, integrity and public-trust perspective. The fact that buses are publicly accessible does not remove GDPR protection, particularly for CCTV, travel patterns, ticketing data and identifiable operational records.

From a cybersecurity perspective, the main risk is that non-OEM systems increase the vehicle and operator attack surface. If such systems are poorly segmented, insufficiently updated, or connected to operator or supplier backend systems without appropriate access control, they may create entry points for compromise, data leakage or service disruption. They may also complicate incident handling if ownership and responsibility are unclear.

Responsibility should be allocated as follows:

- Operators remain responsible for cybersecurity and GDPR compliance for systems they procure, install or operate, including passenger counting, infotainment and supplier-managed onboard equipment.
- Movia remains responsible for systems owned or controlled by Movia, including Basiskort.
- OEMs remain responsible for OEM vehicle systems and backend services within their control.
- Suppliers and subcontractors should be contractually bound by the operator or Movia, depending on system ownership.

Future contracts should require that non-OEM systems are documented, securely configured, updated, access-controlled and segmented from safety-critical vehicle systems. Contracts should also require clear data ownership, supplier responsibility, network segmentation, retention periods, incident notification, audit rights and GDPR-compliant processing arrangements.

Personal data mapping

System / data source	Data generated	Personal-data relevance	Primary responsibility
CCTV / video surveillance	Video images of passengers, drivers and road users	Personal data where individuals are identifiable	Operator / system owner
Passenger counting equipment	Counts, sensor data, images or movement patterns depending on technology	May be personal data if raw images or identifiable sensor data are processed	Operator / supplier
Ticketing / Basiskort	Ticketing events, identifiers, transaction or validation data	Personal data where linked to passengers or travel patterns	Movia
GPS / vehicle telemetry	Position, route, speed, operational events	May be personal data where linked to drivers or identifiable trips	Operator / OEM
Diagnostics and logs	Fault codes, software status, service events, access logs	Usually technical data, but may become personal data if linked to users, drivers or maintainers	OEM / operator
ADAS sensors	Camera, radar or sensor-derived driving-environment data	May be personal data if individuals, vehicles or behaviour can be identified	OEM / operator

The most sensitive data categories are CCTV/video surveillance, ticketing data and any raw passenger-counting data that includes images or identifiable movement patterns. Vehicle telemetry and diagnostics are generally less sensitive but may still become personal data where linked to drivers, routes, timestamps or identifiable incidents.

The cybersecurity relevance is primarily confidentiality, integrity and availability rather than direct vehicle control. However, poor segmentation or weak supplier access controls for non-OEM systems may increase the overall attack surface. Future contracts should therefore require clear ownership, documented data categories, retention periods, access logging, segmentation from safety-critical vehicle systems, and GDPR-compliant deletion procedures.

2.4. Conclusion on questionnaire analysis

Across the assessed domains, Yutong, BYD, BYD Seal U, Golden Dragon and MAN demonstrate the strongest documented cybersecurity maturity. Ebusco occupies an intermediate position, while Daimler Buses demonstrates generally strong maturity with recurring gaps that reduce auditability and assurance. VDL demonstrates markedly lower demonstrability for the assessed legacy models, but the absence of OTA functionality reduces the practical likelihood of certain remote-update scenarios.

The results should not be interpreted as proof that any vehicle is immune to cybersecurity incidents. They indicate whether the assessed manufacturers and vehicle types can demonstrate documented cybersecurity governance, engineering, update and incident-response structures aligned with UN R155, UN R156 and ISO/SAE 21434.

For Tesla, findings are based on available public documentation. BYD Seal U is included as the selected Chinese EV reference platform and scored using the BYD evidence profile. Both should be treated as EV reference assessments rather than bus-model questionnaire results.

The main practical implication for Movia is that the identified gaps do not automatically indicate immediate unsafe operation. Rather, they indicate different levels of assurance, transparency and contractual reliance. Movia should address these differences through future tender requirements, evidence rights and minimum cybersecurity baselines, particularly for vehicles not covered by UN R155/R156 and for non-OEM onboard systems.

3

Risk Assessment

3. Risk Assessment

3.1. Purpose and risk framing

This chapter assesses cybersecurity and cyber-physical risks associated with electric buses used on Movia's routes and selected EVs relevant to Flextrafik. The purpose is not to re-assess legal compliance or to evaluate technical implementation in individual vehicles, but to clarify how technically plausible events may propagate into operational disruption, safety exposure, personal-data issues or loss of public trust for Movia.

The available information does not support a quantitative probability assessment of cybersecurity incidents for each vehicle model. The assessment therefore does not assign statistical likelihood values. Instead, risks are prioritized qualitatively based on potential impact for Movia, degree of systemic exposure, dependency on external parties, and the feasibility of mitigation through contracts and governance.

A low questionnaire score does not automatically mean that a cybersecurity incident is likely, and a high questionnaire score does not eliminate risk. The assessment therefore focuses on which risks are most important for Movia to address through proportionate contractual and governance measures.

3.1.1. Prioritized risk and mitigation overview

Priority	Risk area	Relevance for Movia	Recommended mitigation focus
1	Remote access, OTA updates and backend dependencies	Potential fleet-wide service disruption or safety-relevant impact	Transparency, logging, deactivation rights, incident escalation, staged rollout and rollback
2	Software-update governance and incident-response gaps	Faulty or compromised updates may scale quickly across vehicles	R155/R156 evidence, update governance, incident SLAs and audit rights
3	Legacy vehicles outside R155/ R156	Lower OTA risk for non-OTA vehicles, but weaker lifecycle assurance	Minimum cybersecurity baseline, workshop-access controls, documented update process and incident contacts
4	Non-OEM onboard systems and personal data	GDPR, confidentiality, reputational risk and possible attack surface expansion	Segmentation, supplier controls, access logging, data retention and incident reporting
5	Charging infrastructure dependency	Service availability and depot continuity	IEC 62443 or equivalent, physical/ network security, incident handling and fallback plans
6	Advanced ADAS/autonomous functions	Low-frequency but potentially high-impact safety and trust exposure	Manual fallback, disablement of autonomous functions, weak-signal reporting and operational thresholds

3.1.2. Risk level escalation model for remote access and remote deactivation

The escalation model translates changes in the external threat environment into predefined, proportionate governance and operational actions. It does not assume direct technical control by Movia over vehicles or onboard systems, but defines how Movia, operators and relevant suppliers should act when risk conditions change.

Risk level	Typical triggers	Primary Movia focus	Expected actions
Normal	No specific threat indicators	Governance and assurance	Standard contracts, routine monitoring
Elevated	Authority advisories, credible warnings, reduced transparency, vehicle-relevant vulnerabilities	Preparedness and visibility	Enhanced monitoring, log availability, reaffirmed escalation rights
Critical	Verified incidents, authority instructions, loss of control or immediate fleet-wide exposure	Containment and continuity	Precautionary measures, documented decisions, possible restrictions or withdrawal

The Danish threat assessment for the transport sector indicates an elevated cyber threat environment, including a very high threat from cyber espionage. This does not automatically mean that every vehicle type or route should be treated as being in a critical cybersecurity condition. General sector-level threat does, however, justify that Movia and operators maintain Level 2 preparedness capabilities as a baseline.

In practice, this means that operators should already be able to provide enhanced visibility, incident contact points, logs, clarification of remote-access activity and update status when requested. Full activation of Level 2 measures should be tied to more specific triggers, such as authority warnings concerning vehicle systems, credible incidents affecting OEM platforms, unusual remote-access activity, reduced manufacturer transparency, or vulnerabilities with possible fleet-wide relevance.

A concrete example of a graded measure is connectivity control. Operators can be required to use SIM cards from European mobile network operators and to retain the ability to deactivate this connectivity, individually or fleet wide. At an elevated risk level this can mean disabling non-essential data transmission, and at a critical risk level it can mean fully deactivating SIM-based connectivity so that affected vehicles can no longer be reached remotely.

3.2. Risk cluster A: Remote access and insider dependency

Modern electric buses and EVs may remain connected throughout their lifecycle. Manufacturers or service providers may retain remote capabilities for diagnostics, software updates, configuration, fault monitoring and regulatory obligations related to safety and recall management. These capabilities are legitimate and often necessary, but they introduce a structural insider-dependency risk.

Safety- or operation-relevant actions may be technically authorized and executed from outside the vehicle without physical access and without direct involvement of the operator at the time of execution. This risk is distinct from classic external hacking. It also includes error, misconfiguration, procedural failure, inadequate escalation handling or misuse of legitimate privileged access.

For older non-OTA vehicles, such as the assessed VDL models, the practical likelihood of remote OTA-based compromise is lower than for OTA-capable vehicles. The relevant residual risks for such vehicles are primarily workshop access, diagnostic tools, local software update procedures, supplier access, insufficient logging and limited incident-response visibility. These vehicles should therefore not be treated as having the same remote-update risk profile as modern OTA-capable buses, but they should still be subject to a minimum cybersecurity baseline.

Operational scenarios include remote stopping or deactivation, remote actuation or suppression of actuation support, and unauthorized access to data-generating systems such as surveillance, telemetry or operational logs. These scenarios vary in severity but share a common feature: the initiating access may appear technically legitimate, which complicates detection, attribution and decision-making.

3.3. Risk cluster B: ADAS and increasing automation

ADAS are evolving from isolated driver-assistance functions into software-defined, continuously updated systems that increasingly influence vehicle behavior, backend services and fleet-level performance. This shifts risk from deterministic to probabilistic behavior, from isolated vehicles to shared platforms, and from local faults to systemic failure potential.

Key ADAS-related risks are degraded perception and decision-making, manipulated or unintended actuation support, systemic dependency on shared software stacks and backend services, and fleet-wide propagation of failures through centralized update mechanisms. As ADAS maturity increases, operational benefits increase, but so does systemic coupling and the potential blast radius of failures.

Movia's strategic challenge is not whether ADAS should be deployed, but how ADAS-related risk is governed. Movia should require reporting of weak signals such as repeated driver overrides, unexpected braking, abnormal ADAS disengagements or confidence warnings, and should require predefined thresholds for disabling functions or removing vehicles from service.

From a regulatory perspective, UN Regulation 157 (Automated Lane Keeping Systems) is the first binding international framework for the type-approval of automated driving functions and is directly relevant to this risk cluster. UN R157 sets requirements for the safe operation of automated driving systems, including system boundaries, transitions to the driver and event data recording, and it interacts with the cybersecurity requirements of UN R155 and the software-update requirements of UN R156. As ADAS functionality matures towards higher levels of automation, UN R157 and its successors will increasingly govern the vehicle functions whose compromise would have the most direct cyber-physical consequences. Movia should therefore expect future automated bus and EV models to fall within the scope of UN R157 and should require evidence of compliance accordingly.

3.4. Risk cluster C: Non-OEM systems and personal data

Non-OEM onboard systems, including passenger counting, CCTV, infotainment and ticketing systems, are generally less likely to affect direct vehicle control than OEM drivetrain, braking, steering or OTA systems. However, they may generate cybersecurity, GDPR and reputational risks. They may also increase the attack surface if not segmented from vehicle systems or operator networks.

The most relevant Movia exposure concerns confidentiality and integrity of data, service continuity, supplier accountability and public trust. CCTV and passenger counting data may involve identifiable individuals, while ticketing data may reveal travel patterns or transactional information. Basiskort remains a Movia-owned or Movia-controlled system and should be managed separately from operator-owned systems.

3.5. Risk cluster D: Charging infrastructure dependency

Charging infrastructure introduces additional digital interfaces externally to the vehicle. While well-segmented architectures should prevent direct control impact, compromised or unavailable charging systems may lead to large-scale service disruption. The dominant risk is therefore availability and continuity rather than direct remote control of vehicles.

Movia should rely on standards-based assurance, such as IEC 62443 or equivalent, and require clear ownership of physical and network security at depots, incident handling procedures and fallback arrangements for charging-related disruption.

3.6. Mitigating activities

Across all risk clusters, the effective mitigation strategy is governance-led rather than technically prescriptive. The decisive controls for Movia are transparency instead of trust-based reliance, predefined decision rights instead of ad hoc negotiation, early signals instead of post-incident explanation, and containment capability instead of root-cause certainty.

- Require transparency on remote access, OTA functionality and backend dependencies.
- Require access to logs and audit trails for safety- or operation-relevant remote actions.
- Define escalation rights and decision authority for precautionary suspension, restriction or withdrawal.
- Require ability to deactivate connected functions and automated functions where necessary.
- Require that vehicle connectivity can be provided through European mobile network operators and that SIM-based connectivity can be selectively or fully deactivated, individually or fleet-wide, in response to a heightened threat level.
- Require staged update rollout, rollback principles and customer communication for material updates.
- Require minimum cybersecurity baselines for legacy vehicles not covered by UN R155/R156.
- Require segmentation and supplier controls for non-OEM onboard systems.
- Require GDPR-compliant handling of CCTV, passenger counting, ticketing and telemetry data.

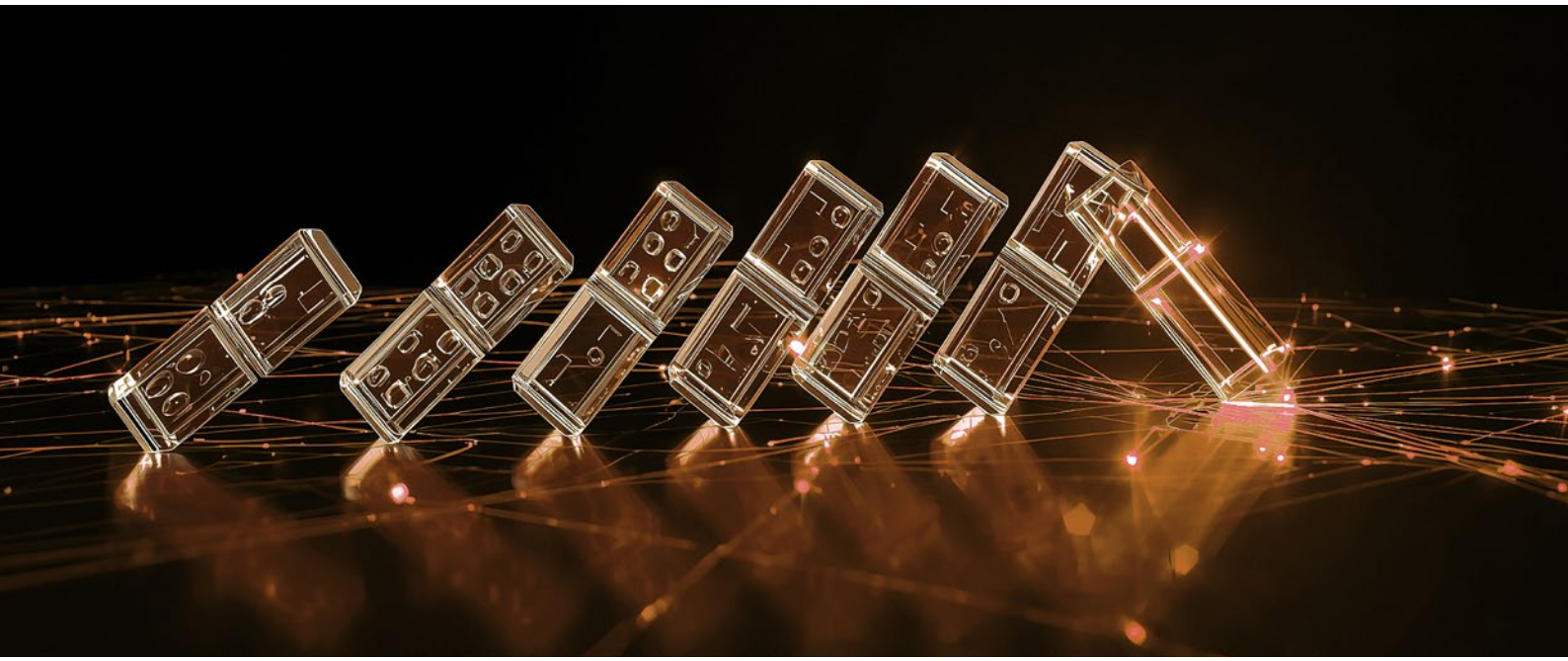
3.7. Consolidated risk overview

Risk cluster	Primary exposure for Movia	Typical trigger	Effective leverage
Remote access and insider dependency	Safety, service continuity, trust, governance	Privileged misuse, error, backend compromise or reduced transparency	Contractual transparency, logging, escalation and deactivation rights
Software update governance	Continuity, safety, fleet-wide impact	Faulty or compromised update	R155/R156 assurance, staged rollout, rollback and notification
Legacy vehicles	Assurance and traceability	Workshop access, unlogged diagnostics, limited support	Minimum baseline and access controls
ADAS and automation	Safety, liability, reputation	Unexpected actuation, perception degradation, backend dependency	Manual fallback, disablement, thresholds and weak-signal reporting
Non-OEM systems and personal data	GDPR, confidentiality, attack surface	Supplier compromise, weak segmentation, data leakage	Segmentation, supplier controls, retention and incident reporting
Charging infrastructure	Availability and continuity	Depot or charger compromise/outage	IEC 62443 or equivalent, incident handling and fallback plans

3.8. Overall conclusion

High manufacturer cybersecurity maturity is necessary but not sufficient. Several risks arise not from weak controls, but from structural characteristics of modern vehicle ecosystems: remote dependencies, shared software stacks, supplier access, backend services and non-OEM onboard systems.

Movia's exposure depends less on direct technical implementation and more on its ability to demand transparency, define decision rights in advance, require evidence, and contain fleet-level impact when uncertainty arises. Risk management at this level is fundamentally a matter of governance, procurement and contract design, not direct technical operation by Movia.



4 Recommended requirements for future tenders and contracts

4. Recommended requirements for future tenders and contracts

4.1. Introduction

The purpose of this chapter is to translate the findings of the assessment into practical tender and contract requirements. Movia's tender model is primarily based on compliance requirements, with price as a central evaluation factor. Requirements should therefore be objective, verifiable and possible to monitor during contract execution.

Movia should avoid bespoke cybersecurity requirements that require qualitative scoring of operators' cybersecurity maturity unless Movia also establishes clear scoring criteria and monitoring capabilities. Instead, Movia should rely primarily on recognized standards, certifications and concrete technical obligations.

The recommended approach is to use recognized standards as the baseline, require objective evidence where possible, define concrete rights for deactivation, incident notification and audit, include minimum requirements for older vehicles not covered by UN R155/R156, and clearly allocate responsibilities between Movia, operators, OEMs and suppliers.

In line with the mandate for this assessment, the recommended requirements are intended to be realistic and proportionate to Movia's exposure and to the risks identified in this report. Before final tender wording is adopted, Movia should test the requirements through market dialogue with operators and, where relevant, their OEMs and system suppliers, in order to clarify feasibility, implementation lead times, cost implications and operational consequences. Requirements that cannot be verified or maintained in ordinary contract follow-up should either be simplified, deferred or treated as lower-priority assurance requirements. They should be enforceable in a tender context, achievable for operators and manufacturers, and proportionate to the actual cybersecurity risk, rather than imposing controls that cannot be verified or maintained.

The requirements operate at two levels. Some requirements concern the Operator's own governance, procedures, escalation paths and contract management. Other requirements must be implemented through the Operator's agreements with OEMs, charging providers or non-OEM IT suppliers. The Operator's obligation should therefore be understood as an obligation to ensure that the relevant capability, documentation and supplier support are available, not as an obligation for the Operator to technically operate OEM-controlled systems itself.

Contract-ready requirement overview

Area	Recommended requirement
Regulatory and standards compliance	Vehicles shall comply with UN R155/R156 where applicable; where not applicable, the operator shall provide equivalent evidence. OEM cybersecurity engineering should align with ISO/SAE 21434, and software update engineering should align with ISO 24089.
Connected functions and deactivation	OTA updates, remote access and automatic transfer of vehicle, operational and position data shall be capable of full or partial deactivation at short notice upon Movia's request, where legally and technically possible.
Software updates	Updates affecting functionality, cybersecurity, safety, data processing or availability shall follow a documented process including compatibility checks, authenticity and integrity protection, validation, staged rollout where feasible, rollback/recovery and traceability.; ISO 24089
Incident notification	Movia shall be notified without undue delay of cybersecurity incidents or suspected incidents affecting safety, service continuity, remote access, OTA updates, personal data, charging infrastructure, Movia-owned onboard systems or public confidence.
Older vehicles outside UN R155/R156	Operators shall document external interfaces, connectivity, update methods, diagnostic/service-tool access controls, logging, support arrangements and incident contacts.
Non-OEM systems and personal data	Passenger counting, infotainment, CCTV/video surveillance and operator IT equipment shall be securely configured, maintained, updated and segmented from safety-critical vehicle systems.
Evidence and audit	Operators shall provide evidence of compliance on request, and Movia may request third-party verification where there is reasonable suspicion of non-compliance or material cybersecurity impact.

4.2. Standards-based baseline requirements

Recommended requirement:

The Operator shall ensure that vehicles used under the contract comply with UN R155 and UN R156 where applicable. Where UN R155 or UN R156 does not apply, the Operator shall provide equivalent evidence demonstrating cybersecurity governance, software-update management, access control, vulnerability management, incident response and secure update procedures.

For OEM vehicle cybersecurity engineering, the Operator shall ensure alignment with ISO/SAE 21434 or equivalent recognized automotive cybersecurity engineering practices. The Operator shall ensure that software update engineering is aligned with ISO 24089 or equivalent recognized practices. For relevant operator-controlled IT systems and backend environments, the Operator shall maintain appropriate information-security controls proportionate to the data and operational risk. Where a subcontractor stores, processes or has privileged access to personal data, vehicle data or operational data on behalf of the Operator, Movia may require evidence of ISO/IEC 27001 certification or equivalent documented information-security controls.

For charging infrastructure and depot systems, the Operator shall apply IEC 62443 or equivalent recognized industrial cybersecurity principles where relevant and proportionate to the role of the charging infrastructure in the contracted service. This requirement should be treated as a lower-priority assurance requirement unless the charging infrastructure is assessed to create material service-continuity exposure.

NIS2 and its Danish implementing legislation are relevant to Movia and to operators and suppliers where they are within scope. NIS2 regulates organisational cybersecurity, governance, risk management and incident handling, and should therefore be reflected in operator governance and escalation requirements. NIS2 is, however, not vehicle-specific and does not replace the vehicle type-approval requirements in UN R155 and UN R156 or the automotive engineering practices described in ISO/SAE 21434 and ISO 24089.

4.3. Connected functions and remote access

Recommended requirement:

Before Contract start, or before a new vehicle type is introduced, the Operator shall obtain from the OEM and provide to Movia a description of connected functions, including OTA updates, remote access and automatic transfer of vehicle, operational and position data.

The description shall state whether such functions can be fully or partially deactivated, how deactivation is performed, who can perform it, expected implementation time, reactivation procedure, and any consequences for vehicle safety, type approval, mandatory legal functions, warranty, service functions, vehicle performance, data transfer or operational availability.

The Operator shall ensure, through its own governance and supplier agreements where feasible, that a request from Movia for deactivation or restriction of connected functions can be received, assessed, escalated and implemented within agreed timeframes.

Where legally and technically possible, and where the operational consequences have been assessed, Movia may request full or partial deactivation of connected functions. If connected functions are deactivated, autonomous or automated driving functions capable of influencing steering, acceleration or braking shall also be deactivated where necessary. The vehicle shall revert to manual mode with full driver control.

The practical implementation, timeframes, costs and operational consequences of such deactivation rights should be clarified through market dialogue and reflected in the final contract wording.

4.4. Software updates and vulnerability management

Recommended requirement:

The Operator shall ensure, primarily through OEM compliance with UN R156 and, where relevant, ISO 24089 or equivalent evidence, that software updates affecting vehicle functionality, safety, cybersecurity, data processing or availability are handled through a documented and controlled process.

Where updates are managed by the OEM, the Operator is not expected to perform technical validation itself, but shall ensure that the OEM can provide reasonable evidence of compatibility checks, authenticity and integrity protection, validation before release, staged rollout where feasible, rollback or recovery principles and traceability of affected vehicles.

Movia may require the Operator to provide information about planned, ongoing or completed software updates that may materially affect vehicle availability, ADAS functions, remote access, data transfer, safety-relevant functionality or service continuity.

Upon Movia's request, the Operator shall provide a reasonable overview of the expected and actual frequency of material software updates for the relevant vehicle types.

The Operator shall ensure that critical cybersecurity vulnerabilities affecting vehicles, charging infrastructure, backend systems or non-OEM onboard systems are remediated within defined timeframes proportionate to severity, relying on OEM or supplier processes where applicable.

4.5. Incident notification and escalation

Recommended requirement:

The Operator shall notify Movia without undue delay of known or suspected cybersecurity incidents, credible authority advisories, or OEM/supplier notifications that may materially affect vehicle safety, service continuity, remote

access, OTA updates, personal data, charging availability, Movia-owned onboard systems, non-OEM onboard systems or public confidence.

The notification shall include, to the extent available: affected vehicle types and number of vehicles; affected systems or suppliers; immediate operational impact; containment measures taken; whether remote access, OTA updates or data transfer are involved; expected timeline for resolution; and contact point for escalation.

The Operator shall maintain proportionate escalation arrangements and contact points appropriate to the risk and operational importance of the affected systems. This does not require a permanent cybersecurity operations function unless expressly agreed, but the Operator shall ensure that relevant OEMs and suppliers can provide timely support for material incidents.

4.6. Evidence, audit and assurance

Recommended requirement:

The Operator shall, as part of ordinary contract follow-up and upon Movia's reasonable request, provide reasonable evidence of compliance with agreed cybersecurity requirements. Evidence may include certificates, policies, process descriptions, update records, incident-response procedures, supplier declarations, penetration test summaries, risk assessments or audit reports.

Any request for third-party verification shall be proportionate to the suspected non-compliance or incident impact. Movia shall have the right to request third-party verification where there is a reasonable basis to suspect non-compliance or where a cybersecurity incident may affect safety, service continuity or personal data. Audit rights shall be proportionate and shall not require disclosure of source code or trade secrets unless strictly necessary and subject to appropriate confidentiality protections.

4.7. Requirements for older vehicles not covered by UN R155/R156

Recommended requirement:

Where the Operator offers or uses electric buses under the Contract that are not covered by UN R155 or UN R156, the Operator shall maintain a proportionate minimum cybersecurity baseline for those vehicles. The Operator shall document external interfaces and connectivity; whether OTA updates, remote access or automatic data transfer are possible; software update method and approval process; service-tool and diagnostic access controls; logging and traceability of maintenance and software actions; cybersecurity incident contact points; supplier support arrangements; and any known limitations in cybersecurity support or monitoring.

Where vehicles are not OTA-capable and software access is workshop-based, the Operator shall ensure that workshop tools, diagnostic access and local update procedures are access-controlled, logged and restricted to authorized personnel.

4.8. Non-OEM onboard systems

Recommended requirement:

This section specifies the concrete controls for non-OEM onboard systems and should be read together with section 4.2. Section 4.2 sets the general information-security baseline, while this section defines the minimum practical requirements for the onboard systems themselves. Any ISO/IEC 27001 or equivalent evidence required under section 4.2 does not replace the concrete requirements in this section.

The Operator shall ensure that non-OEM onboard systems, including passenger counting, passenger information, infotainment, CCTV/video surveillance and operator IT equipment, are securely configured, maintained and segmented from safety-critical vehicle systems. The Operator shall ensure that suppliers of such systems are subject to appropriate cybersecurity, data protection, incident notification and update-management obligations.

Movia-owned systems, including Basiskort, shall remain under Movia's responsibility. The Operator shall ensure that integration with Movia-owned systems does not compromise vehicle systems, operator systems or Movia systems, and that responsibilities for interfaces, network connectivity and incident handling are clearly documented.

4.9. Data protection

Recommended requirement:

The Operator shall ensure that all processing and transfer of personal data generated or processed in vehicles complies with applicable data protection and security legislation. Transfer of personal data, vehicle data, operational data or position data outside the EU/EEA shall not take place without Movia's prior approval unless required by mandatory law.

The Operator shall document categories of data processed, purposes, retention periods, recipients, transfer locations, access controls and deletion procedures for relevant onboard and backend systems.

4.10. Recommended prioritization

Movia should prioritize implementation of requirements in the following order:

1. connected-function deactivation rights;
2. incident notification and escalation obligations;
3. UN R155/R156 or equivalent assurance for vehicles;
4. minimum cybersecurity baseline for older vehicles;
5. non-OEM onboard system controls;
6. data transfer and GDPR controls;
7. audit and evidence rights; and
8. charging infrastructure cybersecurity requirements.

References

- Ruter, "Ruter med omfattende sikkerhetstest av elektriske busser", https://ruter.no/ruter-med-omfattende-sikkerhetstest-av-elektriske-busser
- Styrelsen for Samfundssikkerhed, threat assessment for the transport sector, available via https://samsik.dk/kladde-publikationer/transport/
- UN Regulation No. 155 - Cybersecurity and Cybersecurity Management System.
- UN Regulation No. 156 - Software Update and Software Update Management System.
- ISO 24089 - Road vehicles - Software update engineering.
- ISO/SAE 21434 - Road vehicles - Cybersecurity engineering.
- ISO 26262 – Road vehicle - Functional safety of electrical and electronic systems.
- Regulation (EU) 2016/679 - General Data Protection Regulation.

Appendix 1
Plain-language questionnaire

	Question	Expected details	Evidence
1	Do you have a security and update process for this part (similar to CSMS/SUMS)?	Name of process/certificate	Certificate or policy/process excerpt
2	What is the part and where is it used on the bus?	Official name/model and where it is used	Photo or datasheet, if available
3	Which connections does the part have?	Telematics/internet, Wi-Fi/ Bluetooth, OBD/diagnostics, USB, charger, workshop tool	Diagram or short list
4	How are updates delivered and are update files signed and checked?	OTA/local and signature check	Screenshot or procedure step
5	Before updating, do you check that the update fits the bus it is sent to?	Per VIN/group/version/hardware checks	Example record or tool screenshot
6	During an update, can the bus be driven?	Drive/do not drive rule and driver instruction	Instruction card or HMI message
7	Are service/diagnostic tools protected and are actions logged?	Login, roles, logging	Screenshot or redacted log extract
8	If something looks wrong, how should it be reported?	Contact path and log retention time	Contact details or one-pager
9	Has this part been security-tested in bus context and were high issues fixed and re-tested?	Test performed and status	Summary report or sign-off
10	Do you have a security team and process for fixes, SLAs, controlled rollout and end-of-support?	Team, SLA, rollout, EoS	Policy excerpt or one-pager

Appendix 2
Detailed questionnaire domains

The detailed questionnaire used for the assessment is aligned with UN R155, UN R156 and ISO/SAE 21434 clauses 9, 10, 11, 12, 13 and 15. The full questionnaire consists of 83 yes/no questions covering the domains below.

Domain	Primary references	Representative questions
Governance	UN R155 sections 6, 7.2 and 7.3; UN R156 sections 6 and 7	CSMS/SUMS certificates, lifecycle coverage, supplier dependency management, cybersecurity support duration
Risk analysis	UN R155 Annex 5; ISO/SAE 21434 clauses 9 and 15	TARA method, asset inventory, damage scenarios, attack feasibility, risk acceptance and traceability
Architecture	UN R155 Annex 5; ISO/SAE 21434 clause 10	External interfaces, segmentation, diagnostics protection, secure boot, key management, firmware flashing controls
Software updates	UN R156 sections 7.1 and 7.2; ISO 24089	Update targeting, compatibility, RXSWIN, cryptographic signing, safe-state execution, rollback/recovery
Validation	UN R155 section 7.3.6; UN R156 validation requirements; ISO/SAE 21434 clause 11	Vehicle-level validation, penetration tests, operational scenarios, remediation and residual risk acceptance
Production and service	ISO/SAE 21434 clause 12	Controlled flashing, provisioning, service tools, VIN-to-software traceability and secure rework
Incident response	UN R155 section 7.4; ISO/SAE 21434 clause 13	Detection sources, triage, safety escalation, PSIRT/CVD, incident SLAs, update rollout and continuous improvement

Appendix 3
Detailed questionnaire

R155 / R156 with ISO/SAE 21434 (Clauses 9, 10, 11, 12, 13, 15)

This questionnaire assesses compliance with UN Regulations R155, R156 and consolidates relevant requirements from ISO/SAE 21434 (Clauses 9, 10, 11, 12, 13 and 15). All questions require factual answers. Where Yes/No is requested, select one and provide verifiable evidence and motivate the answer.

#	Section	Reference	Question
1	R155	R155 §7.3.1 (+ §6.5 issuance)	Do you hold a currently valid Certificate of Compliance for the CSMS, and is it applicable to the OEM vehicle type(s) operated by Movia? (Yes/No)
2	R155	R155 §7.2.2.1	Does your CSMS explicitly cover development, production, and post-production phases for these vehicles? (Yes/No)
3	R155	R155 §7.2.2.5	Do you have documented CSMS processes to manage cybersecurity dependencies with suppliers, service providers, and sub-organisations for the in-scope vehicle type? (Yes/No)
4	R155	R155 §7.3.2	Have supplier-related cybersecurity risks been identified and managed for the in-scope vehicle type? (Yes/No)
5	R155	R155 §7.3.3	Has a vehicle-type cybersecurity risk assessment been performed that includes all relevant threats listed in Annex 5 Part A? (Yes/No)
6	R155	R155 §7.3.6	Has appropriate and sufficient testing been performed to verify the effectiveness of implemented cybersecurity measures for the in-scope vehicle type? (Yes/No)
7	R155	R155 §7.3.7(a)-(c)	Are measures implemented to detect and/or prevent cyberattacks, support monitoring, and provide forensic capability for post-incident analysis? (Yes/No)
8	R155	R155 §7.3.7(c)	Do available vehicle and backend logs support forensic analysis of attempted or successful cyberattacks? (Yes/No)

9	R155	R155 §7.2.2.4	Is continuous cybersecurity monitoring performed after first registration for the in-scope vehicle type(s)? (Yes/No)
10	R155	R155 Annex 5 - 2.1	Can disruption or loss of back-end services affect vehicle operation, and are mitigations implemented? (Yes/No)
11	R155	R155 Annex 5 - 24.1	Can in-vehicle network or ECU denial-of-service attacks disrupt vehicle functions, and are mitigations implemented? (Yes/No)
12	R155	R155 Annex 5 - 19.2	Is unauthorized access to or extraction of privacy/personal data from the vehicle technically prevented and monitored? (Yes/No)
13	R155	R155 Annex 5 - 19.3	Is extraction of cryptographic keys from vehicle systems technically prevented and monitored? (Yes/No)
14	R155	R155 Annex 5 - 20.x	Is unauthorized modification of vehicle data, parameters, or identifiers technically prevented and detectable? (Yes/No)
15	R155	R155 Annex 5 - 23.1	Is unauthorized software overwrite/fabrication (control logic manipulation) technically prevented and detectable? (Yes/No)
16	R155	R155 Annex 5 - 16.1	Is remote immobilization, shutdown, or restriction of vehicle functions possible via backend, telematics, or other remote-operation pathways, and if yes, is it access-controlled and auditable? (Yes/No)
17	R155	R155 Annex 5 - 1.x / 2.x / 16.x	Do OEM-backend or -cloud systems have technical capability to issue commands that directly affect in-vehicle ECUs, and is this capability segmented, authenticated, and monitored? (Yes/No)
18	R155	R155 Annex 5 - 28.2	Are debug ports, developer credentials, and development interfaces disabled or removed in production vehicles? (Yes/No)
19	R156	R156 §7.1.1.1 (+ §6.5 issuance)	Do you hold a currently valid Certificate of Compliance for the SUMS, and is it applicable to the in-scope OEM vehicle type(s)? (Yes/No)

20	R156	R156 §7.1.1.6	Can you uniquely identify and selectively target individual vehicles for software updates? (Yes/No)
21	R156	R156 §7.1.1.7 / §7.1.2.4	Is compatibility of each software update with the target vehicle's last known software/hardware configuration verified and documented before deployment? (Yes/No)
22	R156	R156 §7.1.2.3	Is there a complete auditable RXSWIN register for the relevant vehicle type(s), and can it be filtered/audited for the Movia fleet? (Yes/No)
23	R156	R156 §7.1.3.1	Do you have a documented process ensuring software updates are protected against manipulation before update initiation? (Yes/No)
24	R156	ISO/SAE 21434 Clause 10/13 (supporting control)	Are software update packages cryptographically signed, and are signing keys segregated from operational backend roles? (Yes/No)
25	R156	R156 §7.1.3.2	Are update processes, including the update delivery system, protected to reasonably prevent compromise? (Yes/No)
26	R156	R156 §7.1.3.3	Are software verification and validation processes for vehicle software formally defined and demonstrably applied? (Yes/No)
27	R156	R156 §7.1.4.1	Do you perform and document a safety impact assessment for OTA updates, including assessment of whether execution while driving affects safety? (Yes/No)
28	R156	R156 §7.2.1.1	Are authenticity and integrity of software updates protected to reasonably prevent compromise and invalid updates? (Yes/No)
29	R156	R156 §7.2.2.1.1	If an update fails, does the vehicle automatically revert to a safe state or to a previous software version as appropriate? (Yes/No)
30	R156	R156 §7.2.2.1.3	Where updates can affect safety-critical systems, do you demonstrate technical means ensuring the vehicle is in a safe state during update execution? (Yes/No)

31	R156	R156 §7.2.2.3	Where update execution while driving may be unsafe, are controls implemented to prevent driving or disable affected functions during execution? (Yes/No)
32	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Has a concept phase cybersecurity analysis been completed for the specific bus platform/model(s) operated by Movia? (Yes/No)
33	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Is there a documented item definition for the in-scope vehicle platform/functions, including boundaries, assumptions, and intended operational environment? (Yes/No)
34	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Does the item definition explicitly list all external interfaces (OTA, telematics/backend, diagnostics/OBD, Wi-Fi/Bluetooth, USB, charging, mobile/service tools)? (Yes/No)
35	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Is an asset inventory documented for the item, covering safety-relevant assets and data assets (including CCTV/ microphone/GPS where applicable)? (Yes/No)
36	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Are documented damage scenarios present that explicitly include potential physical harm to road users (passengers/driver/other road users)? (Yes/No)
37	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Are cybersecurity goals defined for all safety-relevant functions identified in scope (e.g., braking, propulsion, steering, doors, HV/BMS)? (Yes/No)
38	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Is there a cybersecurity concept that links damage/ threat scenarios to cybersecurity goals and concept-level requirements? (Yes/No)
39	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Is traceability maintained from damage/threat scenarios to cybersecurity goals to concept requirements (traceability matrix)? (Yes/No)
40	ISO/SAE 21434 Clause 9	ISO/SAE 21434 Clause 9	Is there an explicit linkage between cybersecurity damage scenarios and the safety analysis process (functional safety / safety case), including safety-critical categorization? (Yes/No)
41	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Do you use a documented, repeatable TARA method for this vehicle platform (including impact and attack feasibility)? (Yes/No)

42	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Does your TARA method explicitly include asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility rating, risk determination, and risk treatment decision? (Yes/No)
43	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Are risk acceptance and treatment criteria formally defined, approved, and applied consistently? (Yes/No)
44	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Is impact rated explicitly for scenarios with potential physical harm to road users, and is the rationale documented? (Yes/No)
45	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Is attack feasibility scored using defined factors (e.g., expertise, equipment, access, time) rather than qualitative labels only? (Yes/No)
46	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Are TARA results reviewed and approved by named accountable roles (cybersecurity, engineering, safety, management)? (Yes/No)
47	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Is TARA re-opened/updated upon software updates, architecture changes, newly discovered vulnerabilities, or field incidents? (Yes/No)
48	ISO/SAE 21434 Clause 15	ISO/SAE 21434 Clause 15	Can you provide a completed (redacted if required) TARA work product for this platform showing traceability to goals and requirements? (Yes/No)
49	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Are cybersecurity requirements specified at system, hardware, and software levels for the in-scope platform? (Yes/No)
50	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Do cybersecurity requirements include explicit verification/acceptance criteria and allocated responsibility (OEM vs supplier)? (Yes/No)
51	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is there a documented cybersecurity architecture (zoning/segmentation, trust boundaries, gateway controls) for the platform? (Yes/No)
52	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is safety-critical network traffic separated from non-safety domains (e.g., telematics/infotainment) by design and verified? (Yes/No)

53	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Are diagnostic functions protected against unauthorized access (authentication and authorization), including workshop tools and remote diagnostics? (Yes/No)
54	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is secure boot and runtime integrity enforcement implemented on safety-relevant ECUs? (Yes/No)
55	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is cryptographic key and certificate management governed (generation, storage, rotation, revocation) with protections against insider misuse? (Yes/No)
56	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is there a documented process to prevent unauthorized firmware flashing (local and remote) and to detect attempted flashing? (Yes/No)
57	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Are coding guidelines defined and enforced for security-relevant code, and is static analysis performed against those guidelines? (Yes/No)
58	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Are weaknesses/vulnerabilities identified during development tracked to closure with retest evidence? (Yes/No)
59	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is there an SBOM (or equivalent third-party component inventory) for the platform, including open-source libraries? (Yes/No)
60	ISO/SAE 21434 Clause 10	ISO/SAE 21434 Clause 10	Is end-to-end traceability maintained from TARA/goals to requirements to architecture to implementation to verification results? (Yes/No)
61	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Has cybersecurity validation been performed at vehicle/item level (not only component level) for this platform? (Yes/No)
62	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Does validation cover real operational scenarios (in-service driving, depot, charging, maintenance, remote connectivity)? (Yes/No)
63	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Were penetration tests or attack simulations performed against vehicle plus backend/telematics/OTA pathways? (Yes/No)

64	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Were safety-impact cyber scenarios tested (braking, propulsion, steering, doors, HV systems), including fail-safe or fail-operational behavior? (Yes/No)
65	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Were validation activities conducted with independent involvement (external or separate internal team)? (Yes/No)
66	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Is there a validation plan and validation report demonstrating coverage of cybersecurity goals and claims? (Yes/No)
67	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Were any high or critical findings remediated with retest evidence before release? (Yes/No)
68	ISO/SAE 21434 Clause 11	ISO/SAE 21434 Clause 11	Is residual cybersecurity risk at release formally accepted by named accountable roles? (Yes/No)
69	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Are production and assembly processes controlled to ensure only authorized software images are flashed and provisioned? (Yes/No)
70	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Is authenticity and integrity of software verified before flashing in production and in-service rework? (Yes/No)
71	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Are cryptographic keys and device identities provisioned using protected processes (e.g., HSM, separation of duties, limited access)? (Yes/No)
72	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Are production and service tools authenticated and authorized with unique user accounts and audited logs? (Yes/No)
73	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Is there traceability from each vehicle (VIN/serial) to software versions and security provisioning status at shipment? (Yes/No)
74	ISO/SAE 21434 Clause 12	ISO/SAE 21434 Clause 12	Are deviations and rework (failed flashing, ECU replacement) handled through a documented secure procedure and audit trail? (Yes/No)

75	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Do you have a documented cybersecurity incident response process for vehicles in the field, including fleet customers? (Yes/No)
76	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Are detection sources defined and monitored (vehicle logs, backend telemetry, operator reports, supplier notices)? (Yes/No)
77	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Are triage criteria and severity levels defined, including explicit safety-impact escalation? (Yes/No)
78	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Are response time targets (SLAs) defined for critical incidents or vulnerabilities that may impact safety? (Yes/No)
79	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Do you operate a PSIRT (or equivalent) and a coordinated vulnerability disclosure intake for external researchers? (Yes/No)
80	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Is there a defined process to validate security updates prior to rollout (test plan plus evidence)? (Yes/No)
81	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Are update rollouts controlled (targeting, phased deployment, rollback/recovery) with documented customer communication? (Yes/No)
82	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Is the guaranteed cybersecurity support duration defined for this platform, and are end-of-support notifications managed? (Yes/No)
83	ISO/SAE 21434 Clause 13	ISO/SAE 21434 Clause 13	Do incidents and vulnerabilities feed back into updated TARA, goals, and requirements (continuous improvement loop)? (Yes/No)

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ED None
ey.com/dk