Cybersecurity for connected vehicles

September 2024

pwc

A famous comedian often used an automobile as a prop for his most comedic stunts. However, he would not have been able to use this prop in the early 70s when diodes were used to operate alternators and starters. One didn't have to kick the car to make it work by then. Soon after, the auto industry managed to make this core function smarter – even as theatre lost this element of fun to technology.

Similarly, the shift from vacuum tube-operated radios in the 50s to electronically controlled fuel injection systems in the 80s marked a significant change in the industry, from innovation to compulsions of the economy. Furthermore, the jet and space ages marked a profusion of electronic functions, making cars affordable for the common man. Due to heavy industrialisation, urbanisation and diminishing time zones, the need for speed seems to have accelerated the electronic makeover of automobiles. Faster engines, synchronisation between multiple components (such as actuators, oil and fuel flow), pressure sensing, and lubrication were incorporated, which would've been overwhelming for older mechanical systems.

With cinema playing an active role in pushing the desirability of vehicles, especially cars, the complexity and number of functions within a single car just accelerated with time, gradually leading up to the development of autonomous cars in recent times.

Mobility risks

Any car that was built in the last decade or so has between 10 to 100 computers on board. These embedded controls, acting as the heart of vehicle intelligence, allow the computation of signals from various parts of the vehicle at extremely small intervals. A distributed intelligence system incorporates edge computation and facilitates a network of intelligent sub-systems – like the steering, brake, lighting – to work together as a holistic unit. A high-speed central information bus, similar to the human central nervous system, enables these specialised sub-systems made by different technologies and component vendors to synchronise their actions in real time.

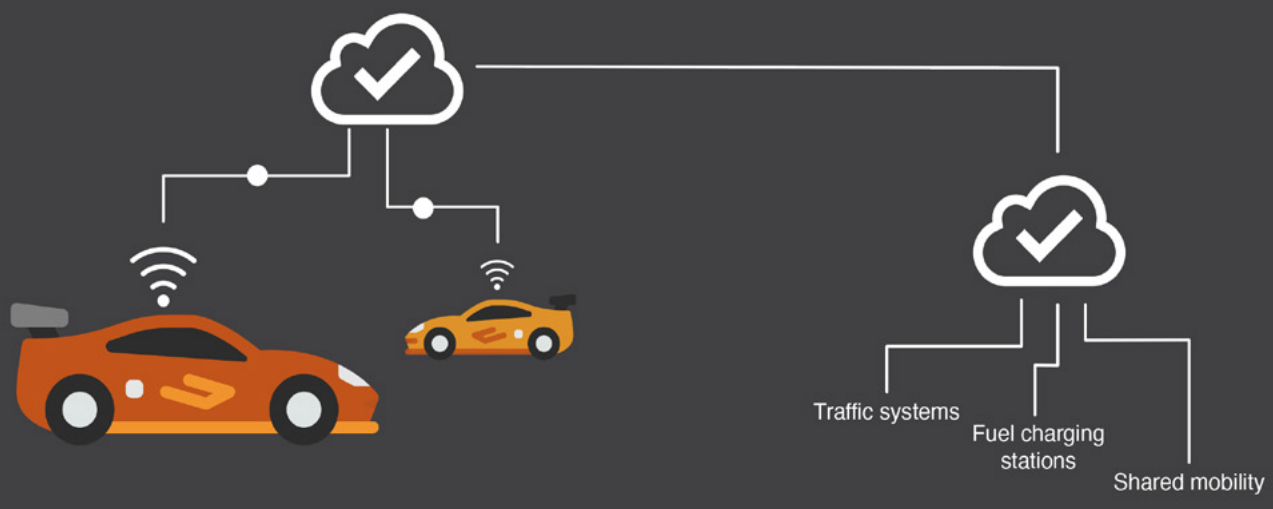
Most core elements in a car – such as engines, gear boxes and lighting systems – have several layered functions, offering a wide range of monetisable features to users.

Mobility has leveraged this connected phenomenon to a massive scale, and is still expanding. Services for predicting early wear, braking patterns, recommending route-based solutions, etc., are a part of such mobility-based services. Services offered by cab aggregators and cargo fleet management use functions like tracking the status and monitoring vehicle functions to make up their business model. This is done by connecting their business functions to cloud-based services on the internet.

Facilitated by sensor, cloud and telecommunication technologies, vehicular systems comprise a powerful internet of things (IoT) package. These systems are connected to the internet, and constantly fed information to make split-second decisions. Therefore, automobiles are now considered a part of the wide network of other systems such as traffic systems, fuel charging stations, shared mobility, cargo tracking and connected people.

However, this also makes such systems vulnerable to a variety of threat actors like cybercriminals, terrorists and malicious individuals/groups, who can leverage this connectedness to trigger serious damage on a local or global scale.

The risks of mobility, which were earlier random in nature and restricted to local driving errors, malfunctions and accidents, have now evolved to targeted attacks on an individual or group of vehicles, service providers, cloud services and electric charging units. The risks posed by such phenomena and their impact cannot be understated and are a possible threat to society, unless appropriate safety regulations are established while ensuring their strict implementation without exception.



Safety standards

The International Organization for Standardization (ISO), with a membership of 169 national standards bodies, is an independent and non-governmental body. The ISO 26262:2018 'Road vehicles and functional safety' standards was a comprehensive effort to imbibe functional safety of electronic and electrical systems in vehicles. It enabled the evaluation of functional safety of electrical and electronics (E/E) in vehicles, and framed safety management principles as automotive-specific risk-based classification of safety goals (ASIL). However, these standards are only focused on the local evaluation of risks.

In due time, the evolution of vehicle connectivity transformed their overall vulnerability from issues having a local impact to a wider scope of attacks by cybercriminals.

Thus, vehicular cybersecurity standards aggregated, as ISO/SAE 21434 framed clear requirements to embed cyber risk management throughout the life cycle of a vehicle.[1] This standard envisaged a change from a component-based point of failure to scenario-based possibilities of vulnerabilities and incidents from external sources which could be risky or fatal in nature, thus widening the scope of impact.

Furthermore, the United Nations Economic Commission for Europe (UNECE) has been actively working to evolve its guidelines for cybersecurity considering the risks posed by an increasingly connected world. It serves as a worldwide regulatory forum for the harmonisation of vehicular regulations (UNECE WP.29).[2]

The UNECE R155 agreement specifies guidelines for granting certificates of approval for cybersecurity and cybersecurity management systems for wheeled vehicles.[3] This initiative aims at streamlining the approach towards cyber risk across the automotive industry and enables it to actively counter threats. Cybersecurity approvals as per the guidelines are expected to be mandatory in Europe from July 2024 onwards.[4]

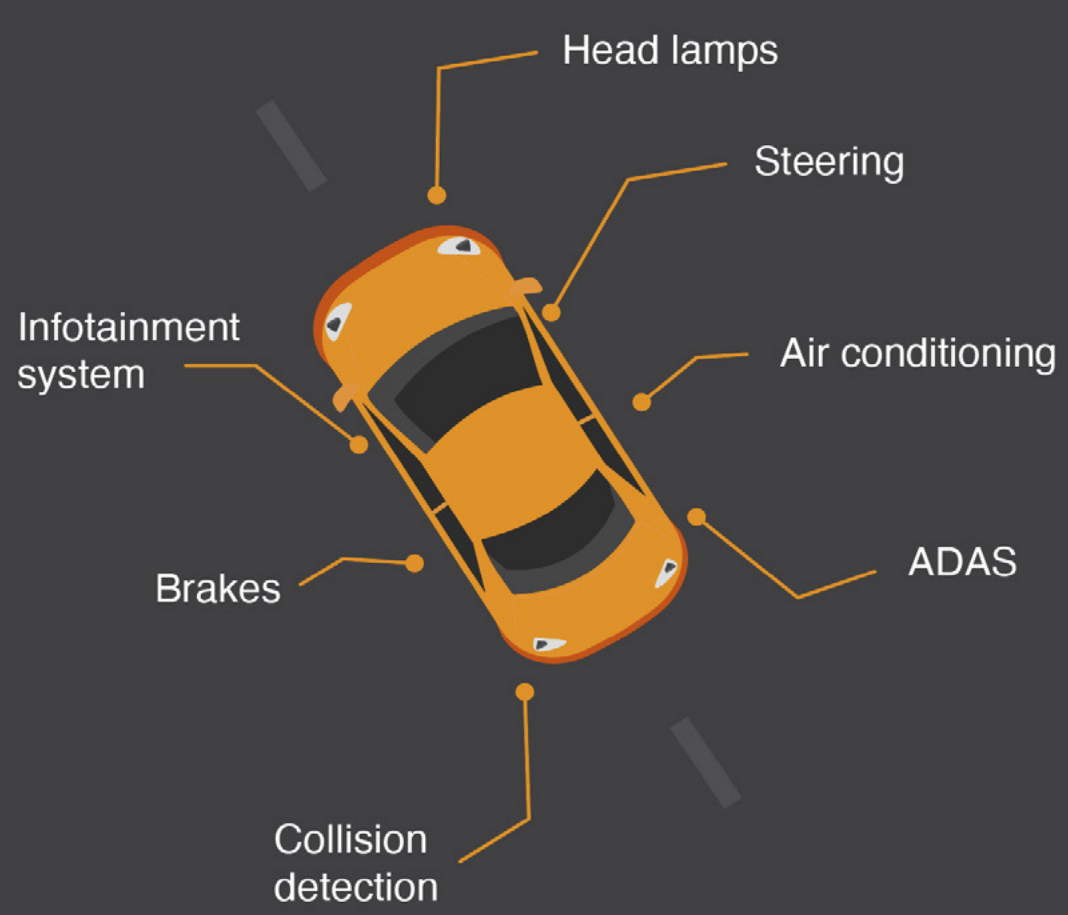
The Automotive Industry Standards (AIS) in India – AIS 189 and AIS 190 – are currently under preparation. These standards (drafts on the ARAI websites) specify the framework for Indian manufacturers to include cybersecurity and related management systems in their vehicle programmes.[5] The dates of implementation and mandatory compliance are still awaited.

However, once these standards are in place, the adoption of ISO 21434:2018 with AIS 189 and AIS 190 could make a paradigm shift in the cybersecurity safety standards in India and help it redefine its global competitiveness.

1. Road vehicles
2. UN Regulation No. 155 - Cyber security and cyber security management system
3. Ibid.
4. Three landmark UN vehicle regulations enter into force
5. Approval of vehicles with regards to Cyber Security and Cyber Security management system

Key highlights

1. Smart vehicles have evolved from basic mechanical systems to complex, electronically controlled units with autonomous capabilities.
2. Modern vehicles integrate 10 to 100 computers, forming a networked intelligence system for holistic control.
3. Connected vehicles are vulnerable to cyberattacks, impacting everything from individual cars to entire networks like traffic systems.
4. International standards like ISO 26262:2018 focus on the functional safety of vehicle electronics.
5. Cybersecurity regulations such as ISO/SAE 21434 and UNECE R155 aim to protect vehicles from cyberthreats, with mandatory implementations pending in regions like Europe.
6. India is developing its own standards (AIS 189 and AIS 190) to enhance vehicular cybersecurity and align with global practices.



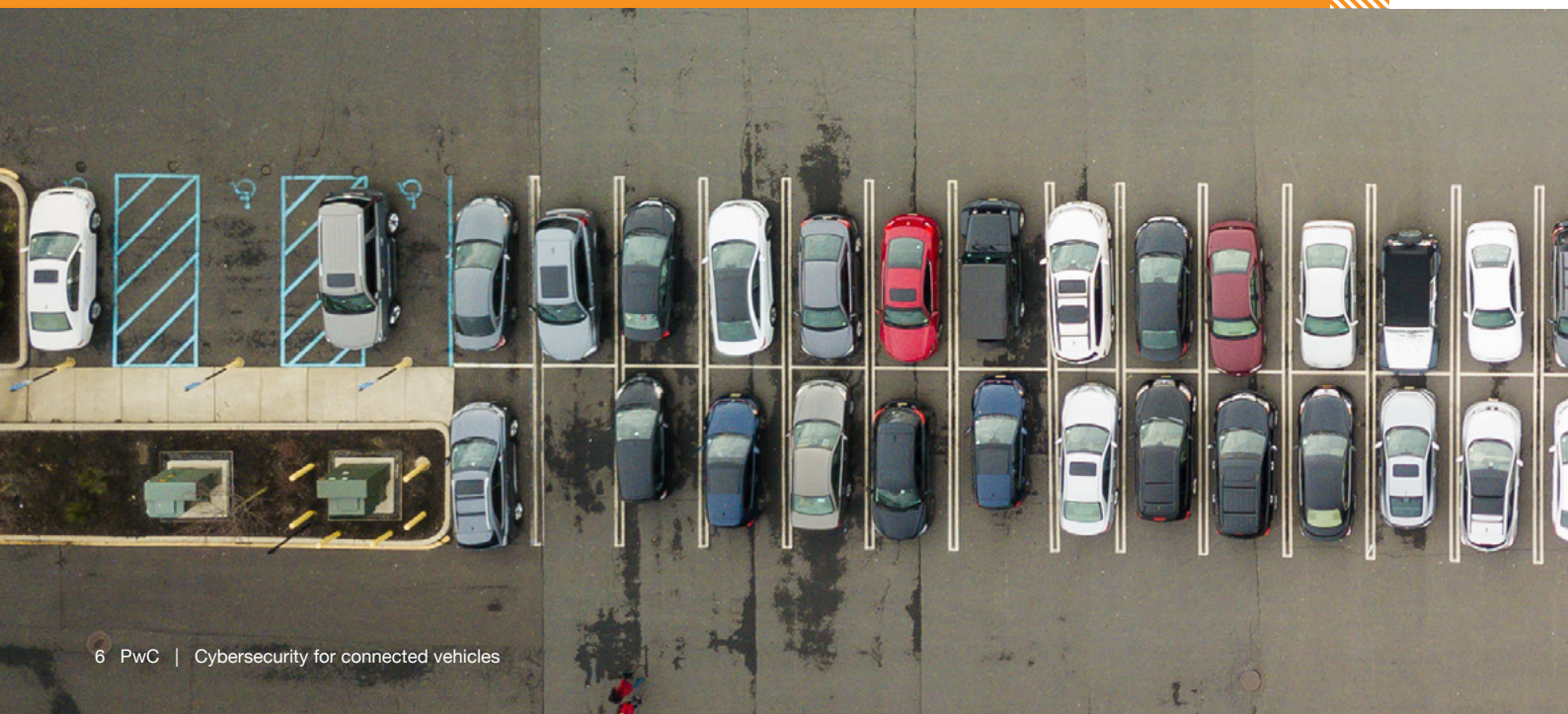
The connected ecosystem of vehicles

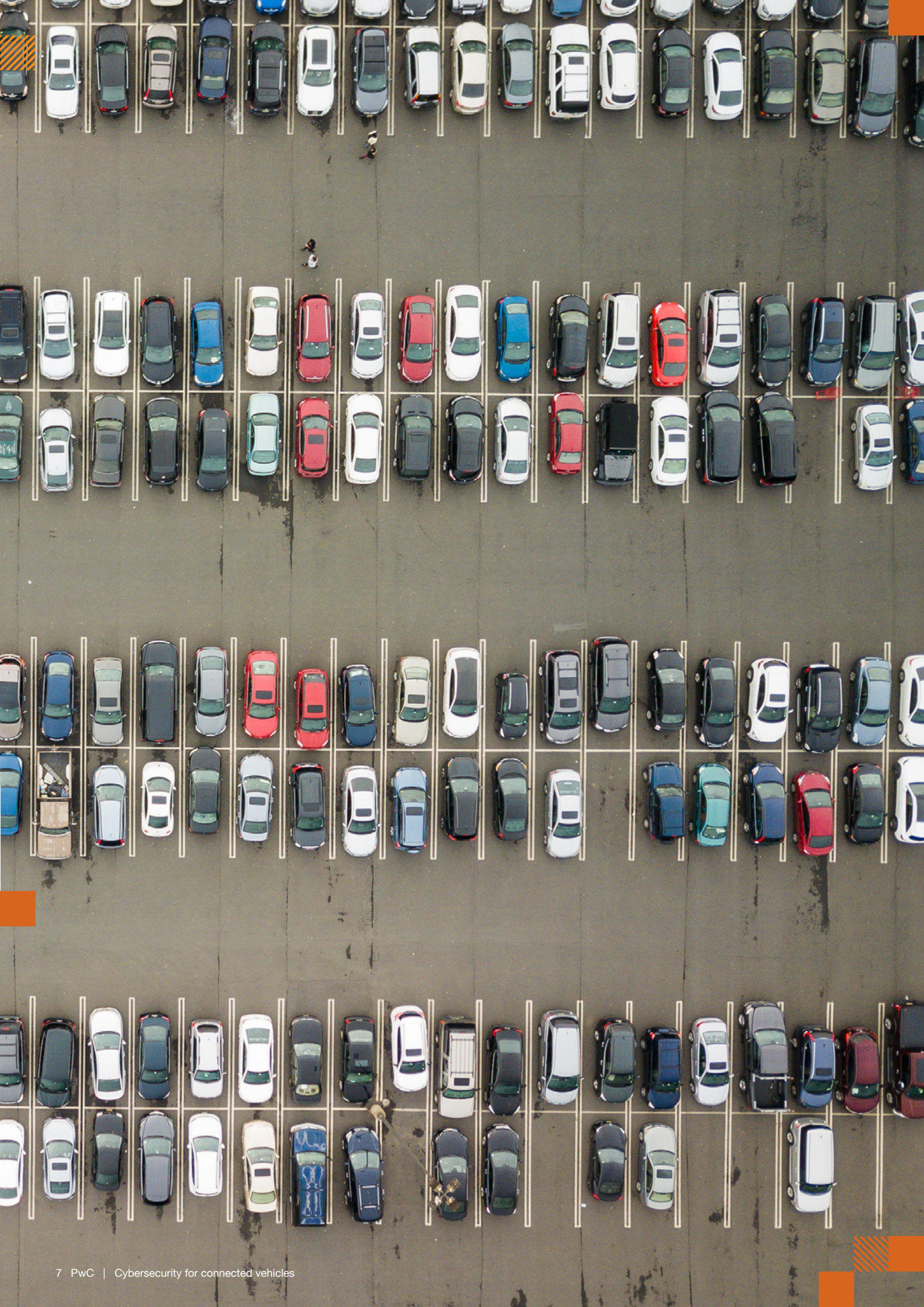
The world today has evolved into a networked entity and the mobility ecosystem is undergoing a dynamic transformation. Passenger cars are being incorporated with a myriad of features, bringing the future home for their owners.

Features such as starting the vehicle remotely, monitoring tyre pressure, door locking and unlocking, and climate control with the help of a remote have been around for a few years now. Today, however, there are a host of new-age features on demand for mobility customers – like geographical information system (GIS)-based functionalities, connectivity to road traffic systems, and exponentially multiplying interfaces between smartwatches, cars and mobile devices, cloud-based application support systems – emerging due to technological and other advancements. Moreover, some new features such as real-time traffic flow help you avoid the crowd, while some apps help update your contacts about your arrival time. GIS enables street-level views which help you recognise your surroundings while driving, while integrations with other apps provide you updated parking slots, thus saving the hassle of scouting for parking or paying a premium. Electric vehicles (EVs) have integrated services that help you recharge your car at the nearest EV charging station while minimising charging time. Vehicle telematics has further enabled the introduction of many new services – such as collision detection, road safety, recognition of driver behaviour and tracking of vehicles. These, in turn, are finding new use cases – both for fleet owners and personal drivers – thus enhancing car ownership and usage experience for all.

India's supply chain has undergone significant change, fuelled by heavy vehicles. India's cargo manufacturers are increasingly offering personalised services in order to stay relevant in a highly competitive market. This is also being increasingly driven by consumers who need real-time tracking of consignments, changes due to traffic and optimisation of upcoming routes. Fleet managers are invested in increasing the on-road utilisation of their vehicles for a faster turnaround. Trucks, trailers and heavy cargo are pre-fitted with diagnostics, which not only predict issues in advance, but are also able to work out improvements in the performance of entire fleets through centralised route optimisation customised for geographical areas, drivers and specific consignments.

All of the above examples point to multiple entities connected through multiple interfaces, enabling data to pass through different stakeholders. This involves authentication of data, ensuring data validation, data control and visualisation.





Changing the narrative: From one-to-one to one-to-many

The one-to-one 'individual–vehicle' or 'individual–vehicle–services dealer' relationship is undergoing a significant change. In the present scenario, this relationship has transformed into a more complex ecosystem comprising multiple entities – such as third-party aggregators, data or services providers, cloud providers, internet service providers (ISP) and access control services, GIS providers, mobile services, charging stations, banks, payment portals, and power suppliers.

The physical infrastructure composed of roads, highways, bridges, weigh stations, fuel pumps, service centres, traffic lights, etc., has been superimposed with data networks inside and outside the vehicles, interfaces with public networks through traffic cameras, radio frequency identification (RFID), EV charging points, smart licence plates, Wi-Fi access points in the vehicles, and interfaces with multiple third-party integrators for public utility services.

While the legacy brick-mortar infrastructure has well-established rules regulations, compliances (like traffic markers and signals, tolls), and also measures for remediation, the digital layer of the connected vehicle infrastructure is not under the ambit of clear compliances and regulations for cybersecurity, yet. Data generated from vehicles now undergoes various processes with multiple stopovers. Similar to how vehicle owners ensure safety and awareness at certain points while driving, it is imperative to have checkpoints in order to secure vehicle data.

While vehicle exporters to Europe are now mandated to be certified for cyber safety through the UNECE R155 certification, India is on the threshold of mandating cyber safety certification with a finalised draft of AIS-189 and AIS-190 regulations.[6]

This is crucial considering the increasing incidents of cyberattacks globally. What may be of immediate concern is the existing difference in the readiness and skills of cyber criminals to attack any system of value, and the availability of such exploits in the underbelly of a digital universe. Here, the lack of cybersecurity awareness in an innocent (unsuspecting) consumer of connected services often results in unfavourable consequences. Therefore, it is of immediate importance for consumers of connected mobility to ask for cybersecurity certification for their cars in India when they decide on a new purchase. This would make the connected universe much safer than what it is today.

Although vehicle manufacturers, service providers, sensor manufacturers, application and content creators are collectively enhancing a consumer's experience through connected services, they are also actively contributing towards the growth of the auto sector. However, as customers become more demanding and technology gets more intrusive, addressing aspects related to safety and the possible risks associated with such connected features is crucial, in order to avoid possible cyber or driving-related crises. In addition to that, establishing the right checks, taking stock of balances, making investments and leveraging the latest technologies to make connected vehicles more secure will help make the auto sector fit for future.

6. Approval of vehicles with regards to Cyber Security and Cyber Security management system

Key highlights

1. Smart vehicles have evolved from basic mechanical systems to complex, electronically controlled units with autonomous capabilities.

2. Integration of services like vehicle telematics, collision detection, and real-time tracking is transforming both fleet management and personal vehicle use.

3. The shift from individual–vehicle relationships to complex ecosystems involves multiple stakeholders, including cloud and internet service providers.

4. Digital infrastructure in connected vehicles lacks clear cybersecurity regulations, raising concerns about data safety and vehicle security.

5. Vehicle manufacturers and service providers are enhancing consumer experiences through connected services but must address associated cybersecurity risks.

6. India is nearing the implementation of cybersecurity certifications (AIS-189 and AIS-190) to ensure safer connected vehicle ecosystems.

Making connected vehicles cybersecure

Does cybersecurity feature on your checklist for buying a new car today? If it doesn't , you can derive some satisfaction from the fact that it isn't part of new cars today. However, all this is set to change in India in 2027 with regulatory bodies specifying that all vehicle manufacturers will have to include cybersecurity as a mandatory feature for all connected vehicles from that year onwards.

Disrupted value chains

Fuelled by energy differentiators, e.g. fuses, software-based load shedding, reduced current utilisation, automatic adjustment of seatbelt force, better suspension on rough roads, and a shift to smart cockpits – traditional models of product development are being rapidly replaced. The conventional supply chain would have a tier-1 product comprising electronics and hardware, tool software, basic software, and pure Software to the original equipment manufacturer (OEM). The tier-1 would in turn depend on tier-2 vendors for either the software or middleware (OS + firmware) which would comply with standards such as AUTomotive Open System ARchitecture (AUTOSAR). With software-defined vehicles (SDVs) becoming the new normal, OEMs are directly adopting full stack architecture, which integrates AI into the architecture of computing chips and allows them to build functions which would have been previously build by tier-1 suppliers.

Security remains a challenge

As vehicles continue to evolve with expected lifespans of 20 years ensured by hardware redundancy and over the air (OTA) updates, the auto industry faces an increasing challenge of cybersecurity. Even if customers accept that a new car may not be at its finest when it leaves the factory and may require an update or two to make it tick, they would still prefer to eliminate all ambiguity when it comes to the security of a car. As connected and electric vehicles present new paradigms for mobility and extensibility of locomotion, AI provides a new paradigm for edge intelligence and cloud-based computing, significantly enhancing the functions of conventional mobility. However, multiple designs and systems and the increasing role of software make vehicles vulnerable to cyberattacks. This increases the possibility of hackers and criminal forces exploiting weaknesses in either the code or increasing interfaces between devices, thus causing a lot of negative impact on individual mobility users and the general public.

Guardrails and regulatory compliances

Regulations in Europe such as the UNECE R155/R156 and AIS-189/190 in India aim to provide a framework for implementing cybersecurity for enterprises making smart vehicles. In addition, ISO/SAE 21434 standards provide the guiding standards to help contextualise security in terms of the vehicle, supply chain and concept to design and manufacturing ecosystems.

A cybersecurity management system (CSMS) is a central theme for the active cybersecurity requirements of connected vehicles.

Situation on ground

PwC conducted a survey of OEMs, suppliers and market experts across 11 countries.[7] The survey revealed many interesting insights.

From July 2024, 60+ signatories to the UNECE will need to have a CSMS in place to produce new vehicles. OEMs (vehicle makers) are ultimately responsible for verifying that their supply chain is compliant with regulations and standards. While most of the OEMs agree and have a design for a CSMS, the maturity of the system is low or moderate. This prevents its deployment. There is also a lack of transparency on CSMS implementation across the global automotive industry. There, however, seems to be a consensus on cybersecurity being the biggest threat in the automotive industry and that an effective CSMS would prove to be a competitive advantage.

In India, as in other countries, the OEM-supplier agreement on cybersecurity remains vague. Hence, while individual component risk ratings might be expected, an overall vehicle-level risk rating, which is key to approvals, homologation and ultimately ensuring passenger protection from cybercrime, does not exist as yet (in 2024).

Further, there is lack of agreement among suppliers, who remain core to the security programme, about which frameworks and standards will be helpful to establish an effective CSMS. OEMs, however, have a different view from suppliers.

7. PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022

Stumbling blocks

Despite the industry recognising cybersecurity as a major challenge, systemic problems like shortage of skilled staff, lack of know-how and supply chain complexities slow down CSMS adoption and integration. A clear business strategy for digital transformation could drive a CSMS approach, rather than one based on mere compliance. This becomes more relevant as OEMs insource important parts of the value chain to create differentiators. Software becomes pivotal as the implementation of a CSMS takes centre stage. Modularity and scalability of software and computing become essential for effective long-term production and operation of vehicle programmes. Perceptions of CSMS and design thus vary for an OEM vis-à-vis a supplier based on their respective responsibility for security. Our experience indicates that an average 30-month cycle of preparation is required to adopt an effective CSMS. With October 2027 being set as the date of implementation for AIS-189/190 approval-related rules for cybersecurity, the clock is already ticking.

Key highlights

1. Regulatory bodies in India have made cybersecurity a mandatory feature in all connected vehicles by 2027.

2. The increasing role of software in vehicles make them vulnerable to cyberattacks.

3. PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022 states that while most vehicle manufacturers agree and have a design for a CSMS, the maturity of the system is low or moderate.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact

Manu Dwivedi
Partner and Leader - Cybersecurity and Risk Consulting GCC,
PwC India
manu.dwivedi@pwc.com

Sundareshwar Krishnamurthy
Partner and Leader - Cybersecurity,
PwC India
sundareshwar.krishnamurthy@pwc.com

Rahul Aggarwal
Partner and Leader - Manufacturing, Industrial Products and Government,
Risk Consulting, PwC India
rahul2.aggarwal@pwc.com

Aniruddha Kadkol
Executive Director - Cybersecurity and Lead Connected Vehicles & IIoT
PwC India
aniruddha.kadkol@pwc.com

Editorial support

Rashi Gupta

Design

Pooja Sharma

pwc.in

Data Classification: DC0 (Public)

PS/September 2024-M&C 38919