Cyber securing connected cars 2.0

Navigating opportunities and risks in the digital era

EY Parthenon

Building a better working world

EY-Parthenon Foreword

A connected car and in-car connectivity have moved from being mere buzzwords to becoming ubiquitous ask by the Indian consumer. The industry is already focused on multiple aspects of this transformation, which include making connectivity a standard feature (as opposed to being an optional add-on), creating new business and pricing models for connectivity solutions and working with regulatory bodies to establish standards to enable a faster roll out.

We believe that the end consumer's continuous demand for seamless in-car technology will continue to fuel innovation and collaboration between organizations spanning multiple sectors like telecom, internet service providers, automakers and component manufacturers. Most OEMs are gradually expanding their internal organizational teams to work with these new competency areas while also solving challenges related to integrating vehicle platform development cycle time with the speed of development in the entertainment, communication and information technology space.

This revolution of automotive connectivity with humans and infrastructure presents an enormous challenge, i.e., cybersecurity.

Auto manufacturers and hackers have both demonstrated the value and perils of this connectivity and thus it necessitates a sharp focus from all stakeholders in the ecosystem – OEMs, regulators, component suppliers, insurance companies and even consumers to make the connected world safe.

We live in a connected world today and in the foreseeable future, this trend is likely to increase. Historically, our experience in the industry has largely been around the use of information technology, which is now supplemented by operational technology. This combined flood of data is both voluminous, instant and can be open to the outside world. This evolution opens up all of us to the threats of cybersecurity, if not managed carefully.

As responsible corporate citizens, we believe it is the duty of all stakeholders in this ecosystem to not only appreciate the threats of cyber but to also effectively take steps to prevent and mitigate risks. We at EY realize the enormity of the task at hand, the significant costs involved in terms of training of our people, the broader ecosystem, systems and checks and balances to be incorporated to safeguard our business.

Recognizing the challenges, EY team is pleased to bring forward compiled thought provoking scenarios and questions to collectively address the concern on connected car and cyber security.

Neville M Dumasia
EY India Leader, Advanced
Manufacturing, Mobility & Infrastructure

Vinay Raghunath
EY India Sector Leader,
Automotive and Transportation

Table of contents

03

Risk to connected
car architecture

04

Scenarios of
cyberattack

▸ Quick Snapshot

▸ Attack Scenario:

  ▸ In-vehicle infotainment
    system

  ▸ Wifi Hotspot

  ▸ 5G SIM

  ▸ Mobile application

  ▸ Inside threat

  ▸ Attack scenario: ADAS

05

How can EY
help?

Section 01

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Indian landscape:
digital consumer and connected cars

The changing Indian consumer is at the confluence of aspiration and technology

Smart office · **Smart transport** · **Smart health** · **Smart energy** · **Smart home** · **Smart manufacturing** · **Smart cities** · Devices · AI · Robotics · Data

Paradigm shift in usage patterns

During 2018, it was estimated that

49.15%
of the global population or

692
million people will use the internet

Active mobile-broadband subscriptions have increased from

1.42 billion
by December 2024

38 million
5G subscribers by December 2024

As per 2024 statistics, On average people spend

194 minutes
a day on social media.
On an average, people spent 46 minutes on online games and 44 minutes on over-the-top (OTT) platforms

Nearly three-quarters of the world will use just their smarphones to access the internet by 2028.

Changing patterns of consumers

1. Mobile and technology- enabled
2. More sophisticated in their financial services needs
3. More demanding -expecting more customization, personalization, flexibility and metricity
4. Increasingly looking towards other people for real-time recommendations
5. Fast and trouble-free solutions

"India to grow faster than China in MBB subscriptions and data traffic"

"Focus on content for enhancing customer experience"

"5G to account for 5% of total connections by 2025"

Source: EY Database, EY Secondary Research

Globally, smartphone mobile network subscriptions reached almost

6.4 billion in 2022, and is forecasted to exceed 7.7 billion by 2028; 5G to account for 57% of Indian mobile subscriptions in 2028

Online Travel

Online Indian travel market size is estimated at

$17.24 billion

In 2024 and is expected to reach $28.40 billion by 2029

42%

of the Indian travelers trust online travel platform for their travel

On-the-go access for host of e-services:

- e-rail ticketing
- e-air ticketing
- e-cabs
- e-travel itinerary
- e-tourism
- e-wallets
- e-bookings

Transport

Online CAB industry reached

$13 billion in '23

Ride-hailing market in India is projected to reach

$6.6 billion in '24

The global Online Taxi Service market size was valued at $35455.46 million in 2022 and will reach $71131.81 million in 2028, with a CAGR of 12.3% during 2022-2028.

More affordability, accessible

- Dynamic pricing
- Wider portfolio of on-demand services
- Autos
- Bicycles
- Eat on the go (food ordering)
- Cashless travel
- Electric cabs
- Shuttles

Online retail market

Online shoppers were

250 million

In 2023

India's ecommerce market is expected to hit

$111 billion

by 2024.
The market size of the online retail industry in India amounted to $60 billion in FY 2023

Consumer is the king

- Ease of 24x7 shopping
- Huge discounts
- Competitive deals
- Power to choose from millions of products
- Time saving door stop delivery and returns
- Connecting people to buy/sell used products

Financial services

Volume of digital payments in India is

11.39 billion

In 2023

Mobile wallets are anticipated to grow at a CAGR of 23.9% between 2023 and 2027

Mobile wallets market in India to reach

$5.7 trillion in 2027

Transition to cash-less culture

- Water and electricity bills
- Mobile recharges
- Cab-booking
- Online money transfer
- Grocery shopping
- Movie ticketing
- Travel booking
- Online trading
- Online insurance
- Online food delivery

Source: EY Database, EY Secondary Research

Transforming the lives of
2 billion people

India's digital and social media outlook

Growing digital media consumption, in the form of multi-play offerings, is increasing the data subscriber base for Indian telcos

Video streaming contributes

70%-80%
of mobile data traffic in India

79%
digital media and content consumption is on mobile devices

93%
of time was spent on videos in Hindi and other regional languages

The amount of time an average consumer spends on mobile content is 3.5 times greater than web content.

3.2 times
more time on mobile content, than on web

550 million
people viewed videos online in 2023, a growth of ~ 100% over 2018

80%
of the content consumed was less than a year old

India has the largest number of Facebook users in the world

Million, Jan '23

India · · · · · · · · · **385**

179 · · · · · · · · **US**

194 · · · · · · · · · · · · · · · **Indonesia**

109 · · · · · · · · · · · · · · · **Brazil**

Mexico · · · · · · · · · · · **99**

Daily active users on Facebook reached 2.06 billion worldwide in 2023
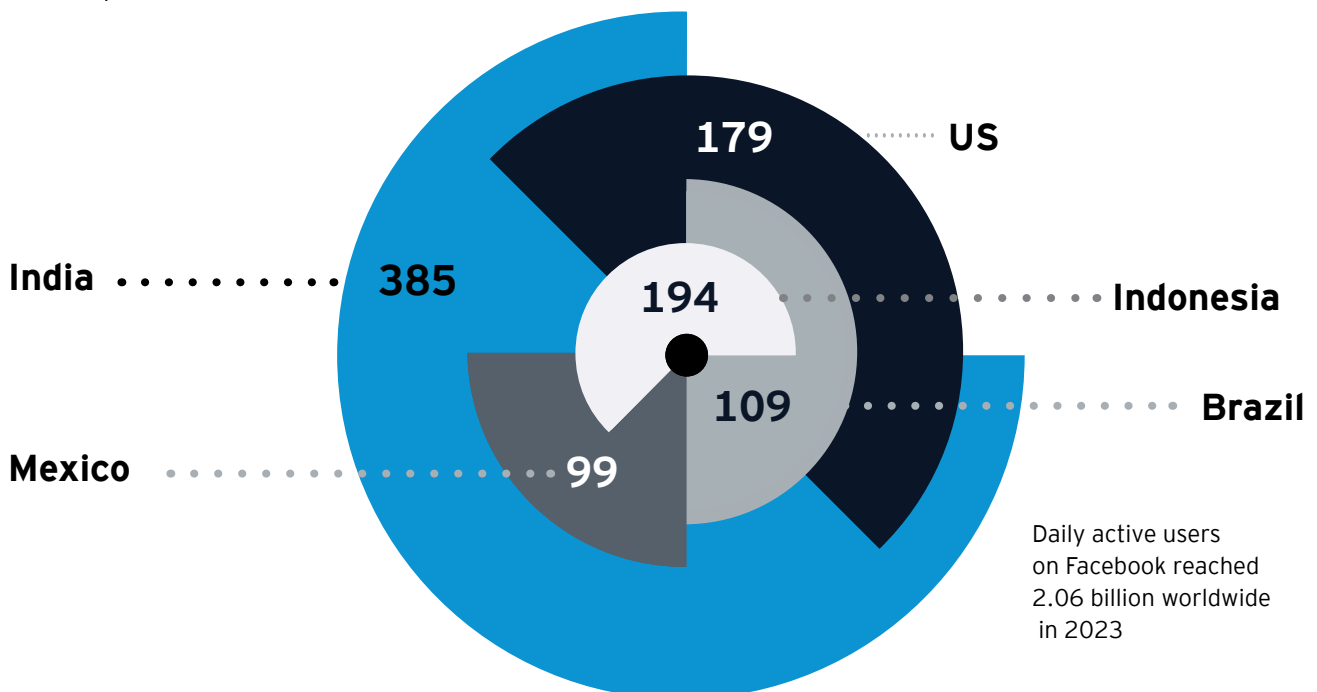
Source: EY Database & EY Secondary Research

Digital opportunities to drive the next wave of growth in India

India to grow faster than China in MBB subscriptions and data traffic

Mobile broadband subscription in India	Smartphone subscription to witness strong growth	Mobile data traffic/month to grow faster than China
2018 : 0.5b	**2018 : 0.6b**	**2018 : 3 EB**
2024 : 1.2b ▲	**2024 : 1.0b** ▲	**2024 : 12 EB** ▲
CAGR ·············· 15% - India 2% - China	CAGR ·············· 10% - India 3% - China	CAGR ·············· 26% - India 22% - China

Operators have showcased a number of 5G use cases

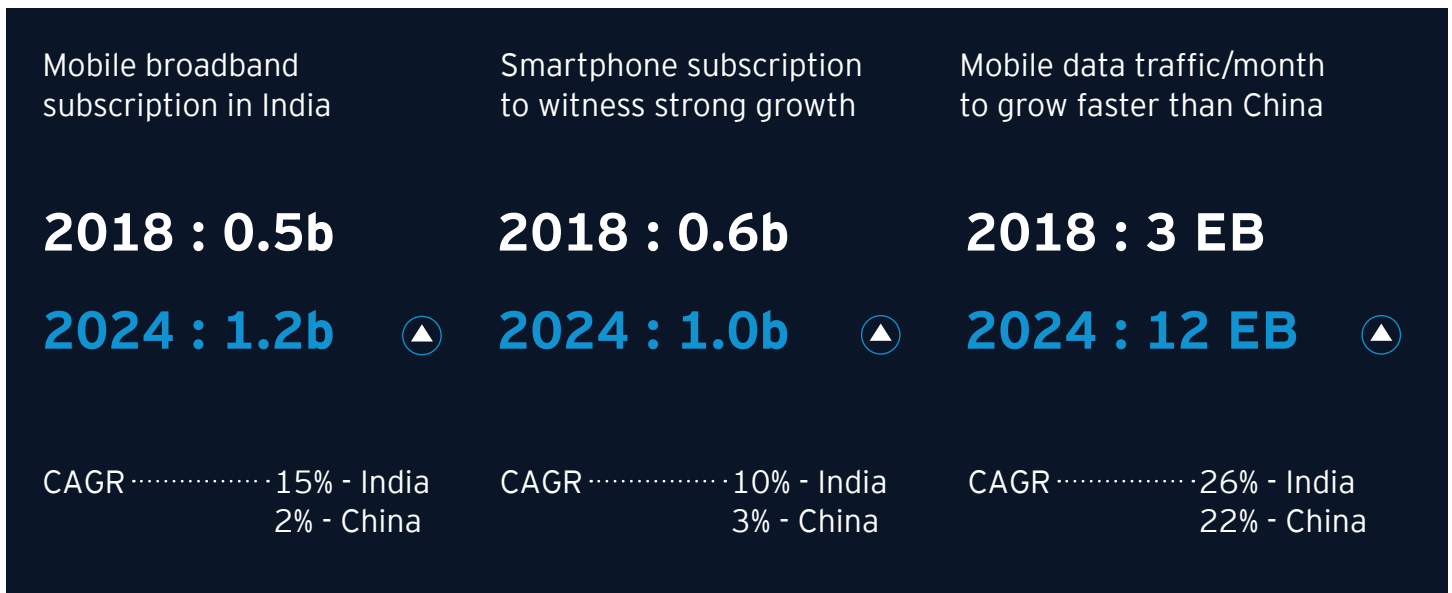|		
Connected cars	RJio and Ericsson demonstrated 5G connected car and VR-enabled driving using 5G	Airtel demonstrates how IoT can empower drivers through auto telemetry
VR-based 360° content	Airtel and Nokia demonstrated VR-based 360° content that can be streamed in a 5G live environment	
Connected homes	Airtel showcased a replica of modern connected homes intelligent devices and appliances	
BVLOS autonomous drones	Airtel and Ericsson showcased Beyond Visual Line of Sight (BVLOS) autonomous drones over 5G networks	

Source: EY Database & EY Secondary Research

Focus areas: stakeholder's watch

Financial services

- Application and subscriber
- Over-the-air software updates
- Service management web portal
- Customer service helpdesk

Infotainment delivery

- Personalized content delivery
- Driver CRM via email and SMS
- Driver smartphone app and portal
- Customer service helpdesk

Electric vehicles

- Battery health and charge status
- Charging location POI reservation
- Eco-trip planning and navigation
- Battery charge time scheduling

Safety and security features

- Automatic crash notification
- Crash recording
- Remote alerts and theft tracking
- Remote vehicle immobilization
- Roadside assistance

Intelligent vehicle

- Vehicle health reports and notification
- Dealer location and service scheduling
- Driver reports and coaching
- Driver monitor, limits, and alerts

OTA software management

- Policy-driven dependency, rollback, and recovery
- Standards-based certification, authentication and encryption
- Dynamic data collection and upgradable analytics
- Customized consumer notifications prompts, and consent
- OTA capability as additional revenue streams for OE End customer/ vehicle owner & Dealerships providing value added features such as on-demand additional power for a particular ride, change to better UI/UX on infotainment.

Connected vehicle features

- Connected car programs are becoming increasingly important for differentiating brands and vehicles from the competition while contributing to consumer engagement, satisfaction and loyalty for the next purchase.

- Leading automakers need to create connected car experiences that are intuitive, personalized and updatable.

- Automakers are increasingly developing electric, hybrid and plug-in hybrid vehicles to meet consumer demand and comply with current and future government fuel efficiency mandates.

Source: EY Database & EY Secondary Research

Right business model: stakeholder's watch

IT infrastructure	Data noise - information gap	New business

Existing business	Existing processes	Customer relationship

Strategy medium/short term plans

Strategy discussions among shareholders are essential to overcome frictions in the organization

as there are several key questions and issues to be addressed.

Key questions for all stakeholders

The question	What the answer should be about
Are the available telematics services technically feasible in my target market? What are the key challenges faced?	Understanding the IT landscape, its strength and weaknesses and customer requirement
Are the services commercially viable? What is the end result (top line and bottom line)?	Building up the business plan also to anticipate issues/concerns end estimate pricing improvement
How are the black boxes / devices installed and maintained and who will bear the cost?	Keeping a flexible approach ready for "device independency"
Who will store and analyze the data (i.e., in-house or outsourced)?	Understanding the path to develop access to adequate technology and skill
What are current consumer attitudes? What would they expect by telematics?	Identifying "differentiating services" to avoid the "commodity pricing trap"
How do I attract new customers without cannibalizing my existing portfolio?	Comparing company's portfolio and clients with market trends and existing threats
What strategic partnerships would add value to my proposition (e.g., car dealerships, road side assist service providers, technology partners, official bodies)?	Building a vision behind that of a gadget that enhance risk selection, to leverage telematics ecosystem

Connected car ecosystem
Multiplicity of services and stakeholders

What are connected car end-services?

On-demand infotainment

Higher bandwidth

▶ Radio-music, news: live news feed
▶ Video: on-demand and real-time content
▶ Other in-vehicle services enabled by cloud computing

Lower bandwidth

Lower bandwidth

▶ News, stocks and sports
▶ Apps store
▶ Multimedia, internet services, social networking, etc.

Navigation

▶ Navigation (point of interest, parking)
▶ Route optimization
▶ Traffic/journey times
▶ Travel and traffic assistance/ off-board route guidance
▶ Location-based services

Safety and security

▶ Roadside assistance
▶ Emergency notification
▶ Theft tracking
▶ Remote control of vehicle environment/ car features
▶ Geo-fencing
▶ Lane jumping alert
▶ Fuel Pilferage Alert

Diagnostics

▶ Vehicle health
▶ Scheduled maintenance
▶ Recall information
▶ Service coupons
▶ Service scheduling
▶ Electrical vehicle: battery charge monitoring/ control

Others

▶ Usage based insurance
▶ Fleet management
▶ Payment (tolling, parking, etc.)
▶ In car health services
▶ Embedded financial GPS units

Vehicle-to-vehicle

▶ Traffic information
▶ Driver warnings
▶ Pre-emptive actions to avoid and mitigate crashes
▶ Threat and hazard sensing: 360 degree awareness of the position of other vehicles

Source: EY knowledge

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era
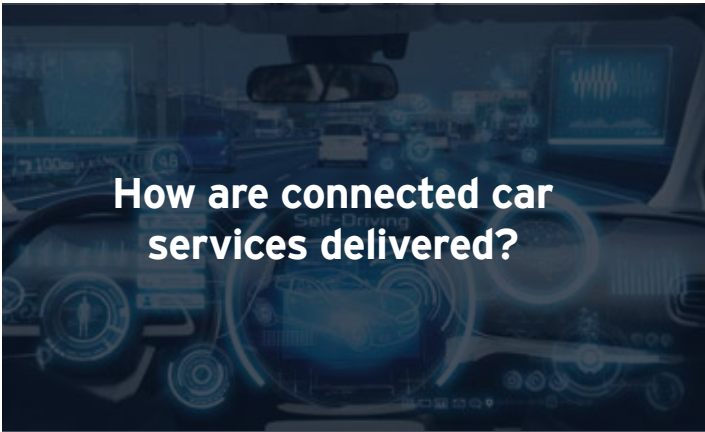
How are connected car services delivered?

Service delivery architecture

- Telematics service platform/access portal
- Security services
- Content creation
- Content aggregation
- Application development
- Application delivery

User interface

Device-to-vehicle connectivity

- Embedded
- Tethered
- Integrated

Human-machine interface

- Visual
- Haptic
- Voice

Wireless network (connectivity)

- Low speed data services (2G)
- High speed data services (5G or LTE)

Customer support/service

- Call centers
- Online support
- Subscription management
- Charging and billing

Source: EY knowledge

Stakeholders

Automotive industry

- Vehicle manufacturers
- Auto component suppliers
- Repairer networks/service centers

Information technology

- Packaged software vendors
- IT services companies

City/State regulators

Telecom

- Telecom operators

Telematics service provider

- Telematics service platform providers

Device manufacturers

- Smartphone manufacturers
- Portable navigation and infotainment device manufacturers

Insurance industry

- Insurance providers
- Insurance distributors (brokers and aggregators)

Others

- M2M service providers
- BPO
- Roadside assistance providers

We see connected vehicles as a part of the overall mobility solutions landscape

Mobility solutions considerations: who, what, why, where and how

Who and why

The audience considerations of mobility

"Who is the mobility service designed for and why is it important to them?"

Where

The geographic considerations

"Where are people and things moving to and from?"

HOW
Some key questions for OEMs to consider

Private
(Business to consumer)

Urban
- Ride sharing
- Car sharing
- Brand sharing
- Predictive/optimized maintenance and repair

Regional
- Share-a-car
- Autonomous driving
- Hybrid engines

Global
- "World citizens": people living in the various areas of the world at the same time

Some other pertinent questions:

- What do consumers value and what are they willing to pay for?
- How do we prioritize the various mobility concepts to implement?
- How do we monetize our investments in mobility (and telematics)?

Commercial
(Business to business)

- Corporate car sharing mobile
- Corporate BRT: mobile working space
- Integrated logistics

- Fleet cost optimization
- Mixed fleet management
- Intermodal solutions
- Hybrid engines

- Material/product logistics
- Human capital/people mobility
- Corporate dwellers

Public
(Business to government)

- Bus rapid transit solutions
- New traffic management tools
- Dynamic space pricing

- Integration of renewable energy (with energy needs of the ecosystem)
- Tolls system
- Intermodal solutions

- Connecting journey endpoints across major metropolitan areas (e.g., cab, train, plane, etc.)

What
the programmatic aspects or topics within mobility

"What needs to be considered and/or addressed in implementing a mobility strategy?"

- What do business and fleet customers value and what are they willing to pay for?
- How do we monetize opportunities for emission reduction targets?
- How integrated is our overall strategy for corporate clients?

- What are governments looking to accomplish?
- What is our "city-focused" go-to-market approach?
- How can we access new private/public business models to help finance new mobility concepts?

Section 02

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Stakeholder benefit

- Reduce range anxiety
- Safety through ADAS - crash avoidance
- Telematics for tracking insurance and efficiency
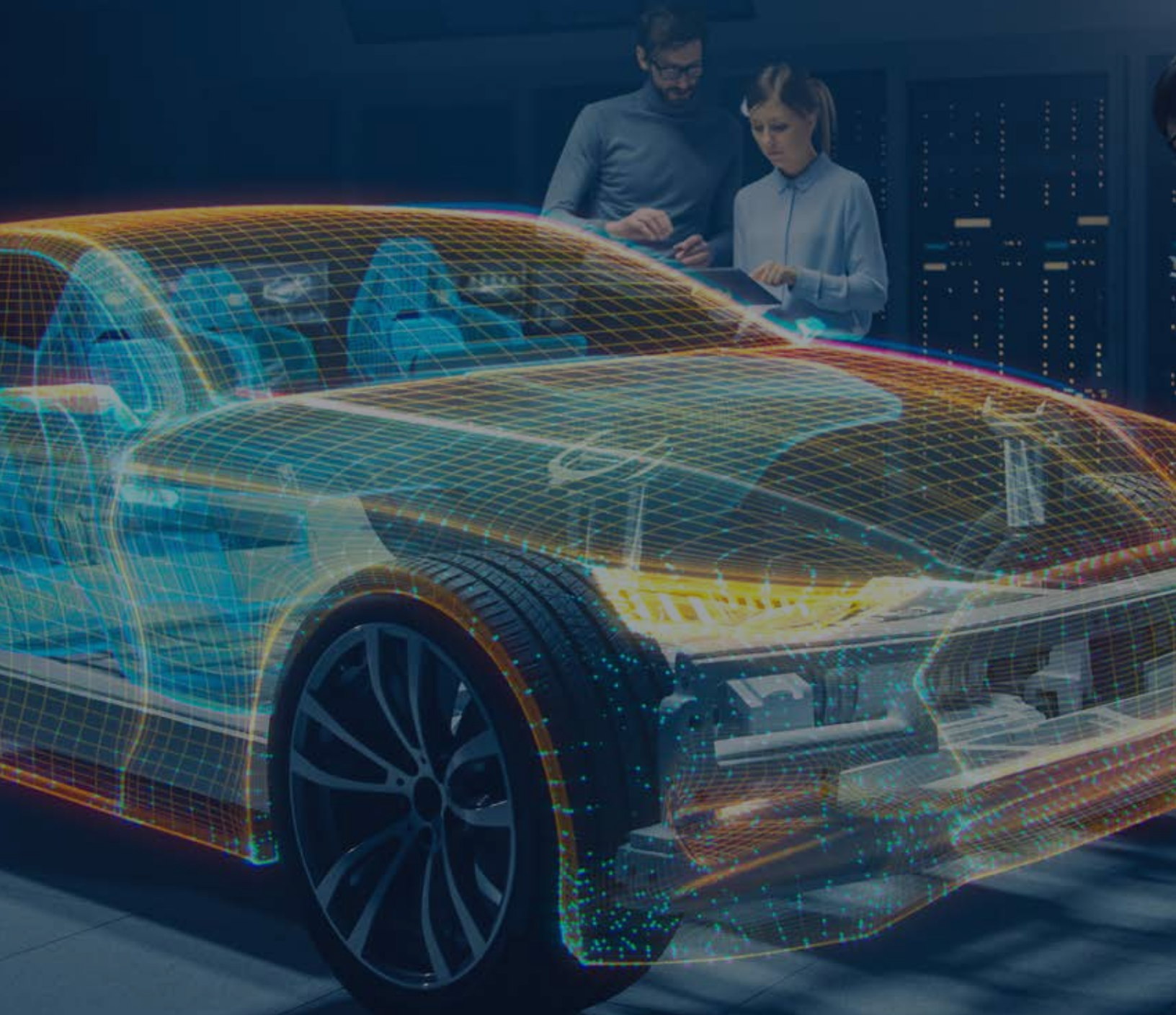
"

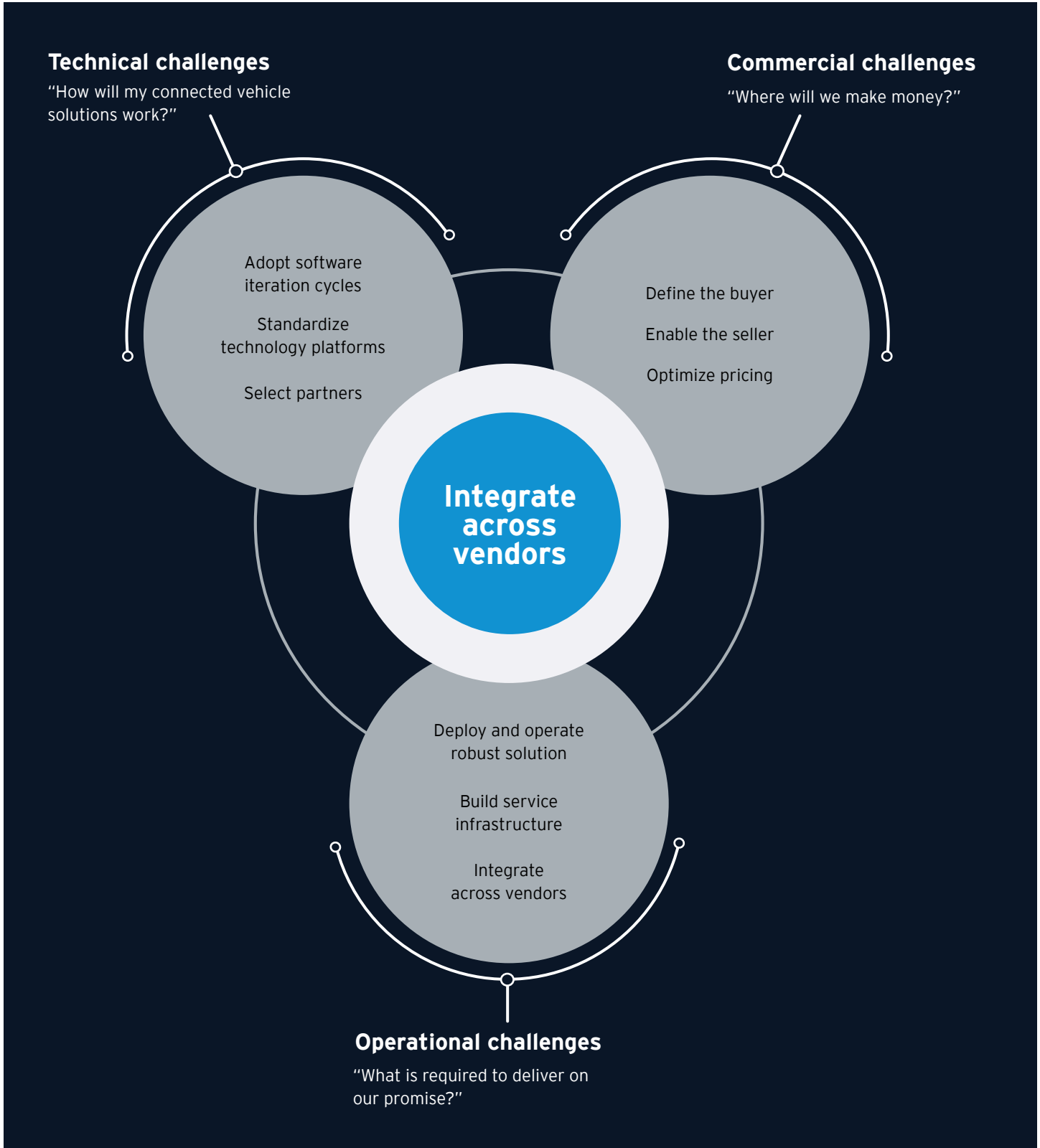**Connected car mobility marks one of the most groundbreaking opportunities. However, it introduces a unique challenge for OEMs - the necessity to innovate and conceptualize new business models. Success in this evolving landscape lies in effectively monetizing connected services and unlocking sustainable revenue streams."**

Som Kapoor
Partner, Future of Mobility

Technical challenges

How will my connected vehicle solutions work?

Technical challenges

''How will my connected vehicle solutions work?''

Adopt software iteration cycles

Standardize technology platforms

Select partners

Commercial challenges

''Where will we make money?''

Define the buyer

Enable the seller

Optimize pricing

Integrate across vendors

Deploy and operate robust solution

Build service infrastructure

Integrate across vendors

Operational challenges

''What is required to deliver on our promise?''

Connected vehicles: opportunities and challenges for vehicle manufacturers

Internet-enabled telematics

From

- Managed as feature/ functionality item
- Owned by product development/engineering
- VM branded
- Unclear value proposition
- Optional item bundled in a package

To

- Key element of customer engagement
- Application across ownership lifecycle
- Services-driven value proposition
- Multi-vendor, multi-brand solutions
- Standard item
- Tight smartphone integration

Many definitions exist – we propose

Mobility – moving people and things from point A to point B

Connected vehicles – internet-enabled, mobile equipment

Telematics – hardware and software to connect vehicles

Challenges

- Defining value and willingness to pay for dealers and customers
- KISS: Keep it simple for users
- Organizing for success
- Operating a services business
- Managing partnerships vs. vendors
- Owning and using data

Opportunities

- Differentiate through the connected vehicle experience
- Build direct relationships with customers
- Use data to improve quality/ reduce warranty expense
- Increase share of post warranty, customer pay parts and services spend
- Determine insurance premiums for customers

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Success in connected vehicles requires focus and diligence in strategy and execution

Connected vehicle strategy: Define, Develop, Monitor

1

Assess /define

The first step is to define the fields of play - the focus areas, or points of concern, relative to your overall mobility and telematics program(s)

Strategy alignment	Ensuring the alignment of telematics and mobility with overall corporate strategy across different BUs
Risk management	Creating an integrated and dynamic control environment for the connected vehicle strategy that balances value, cost and risk
Customer definition	Defining the key stakeholder and customer groups and determining key solution requirements and pricing
Integration and monitoring	Effectively integrating and monitoring mobility and telematics program efforts and results across BUs

2

Design/ develop

After identifying one or more focus areas, the next step is to design and develop an integrated and holistic connected vehicle strategy

Connected vehicle strategy

Technical

CVS challenges and issues
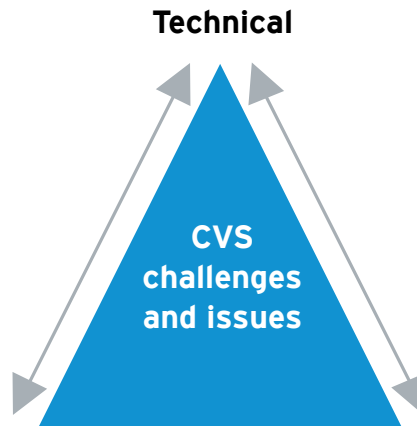
Commercial

Operational

3

Implement/ monitor

New revenue streams for all stakeholders

Vehicle information package

▶ Standard onboard function

▶ Determines vehicle chassis details, engine number, date of manufacturing and all legal attachment

Convenience package

▶ Locates the nearest OEM dealerships and workshops

▶ Records and shares the user feedback regarding the dealer with the OEM

Warning package

▶ Onboard engine safety package

▶ Warnings include gear shift indication, rev recognition to avoid engine over revving

Company app downloads

▶ On-board engine safety package

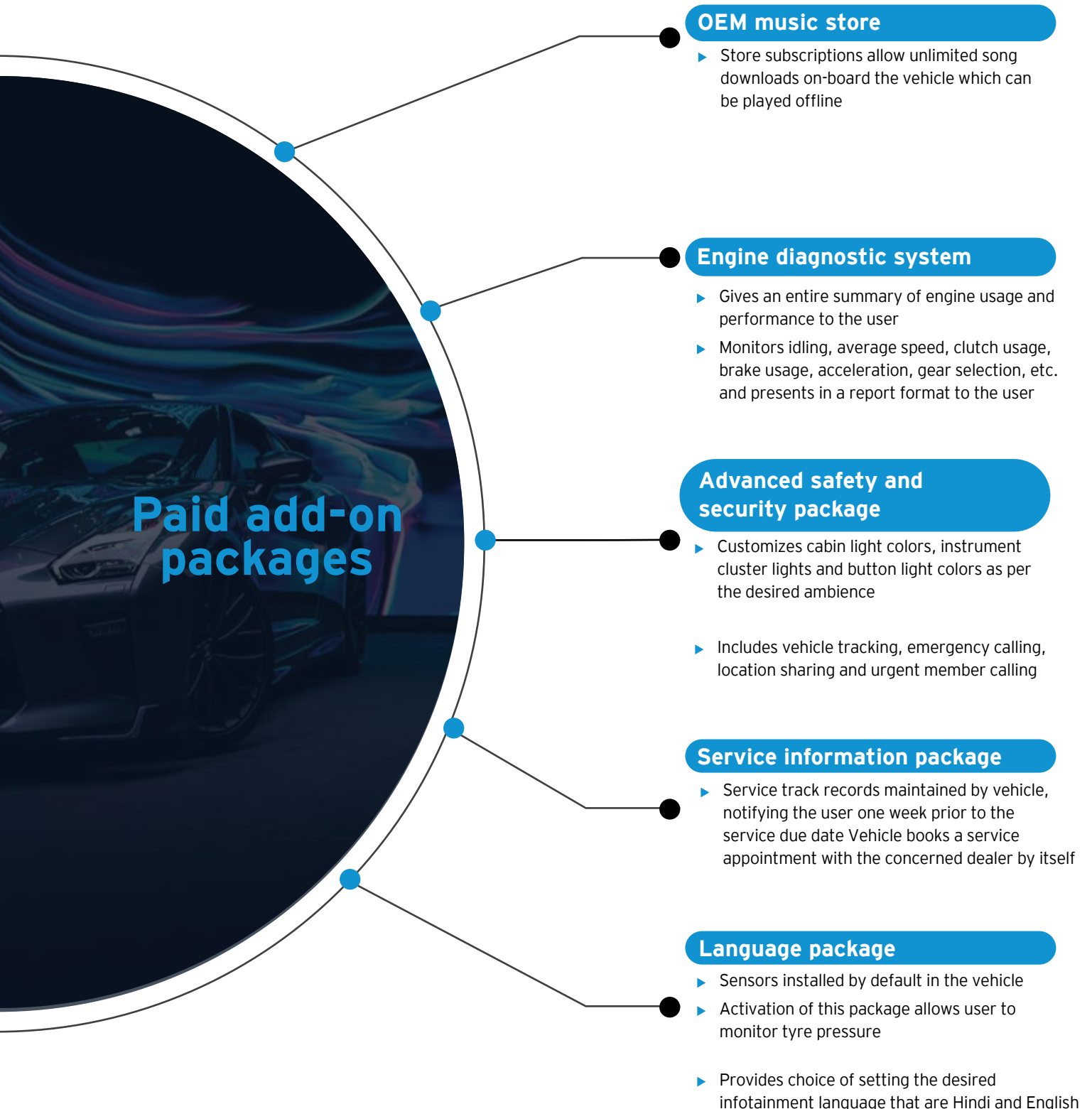▶ Warnings include gear shift indication, rev recognition to avoid engine over revving

OEM chat connect

▶ End-to-end encrypted messaging system allowing users to chat with friends using the chat connect app of the same OEM and also through the vehicles command system.
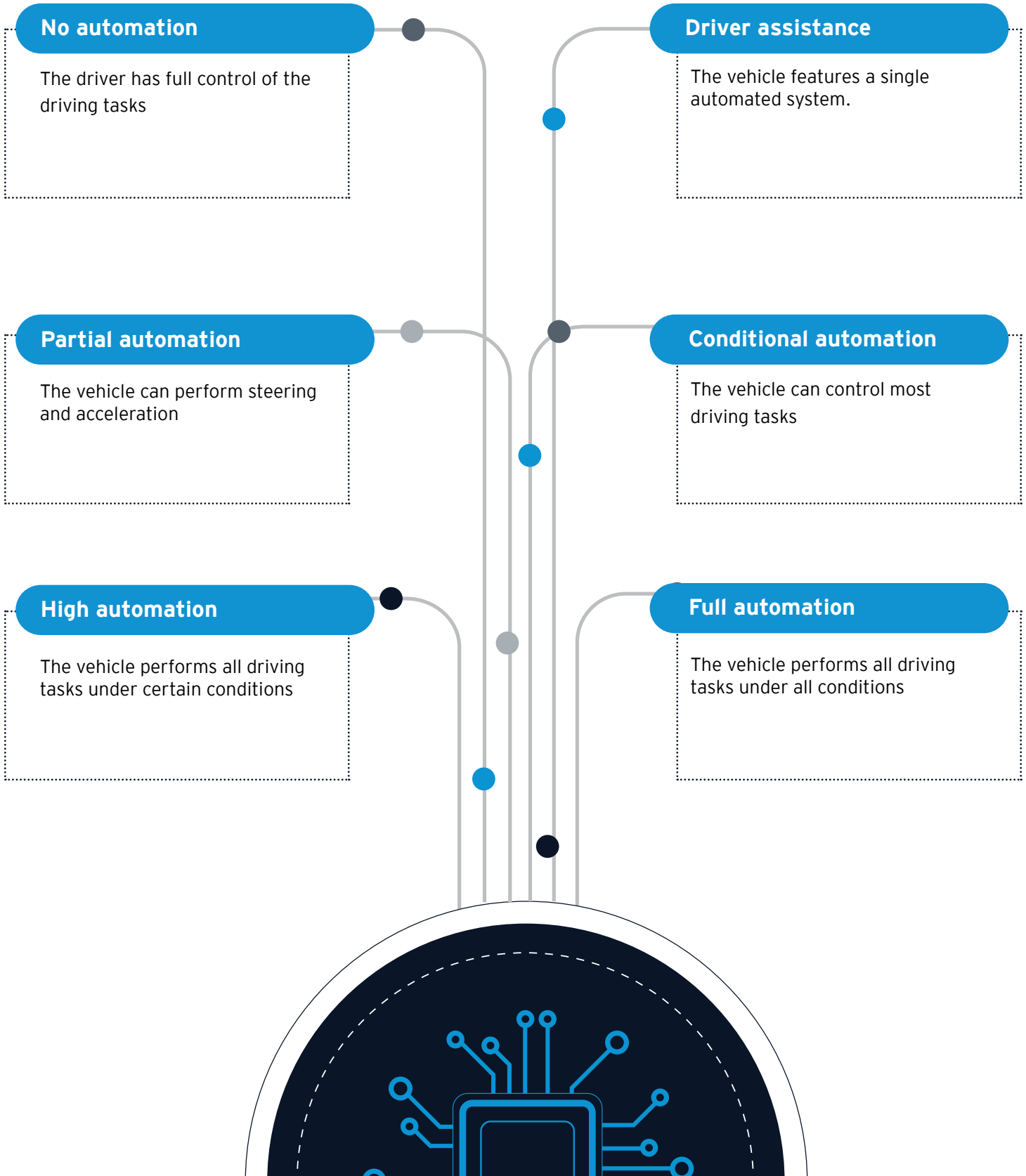
Unpaid basic packages

The connected car opportunity: who will provide the infrastructure and who will give the content?

Paid add-on packages

OEM music store
- Store subscriptions allow unlimited song downloads on-board the vehicle which can be played offline

Engine diagnostic system
- Gives an entire summary of engine usage and performance to the user
- Monitors idling, average speed, clutch usage, brake usage, acceleration, gear selection, etc. and presents in a report format to the user

Advanced safety and security package
- Customizes cabin light colors, instrument cluster lights and button light colors as per the desired ambience
- Includes vehicle tracking, emergency calling, location sharing and urgent member calling

Service information package
- Service track records maintained by vehicle, notifying the user one week prior to the service due date Vehicle books a service appointment with the concerned dealer by itself

Language package
- Sensors installed by default in the vehicle
- Activation of this package allows user to monitor tyre pressure
- Provides choice of setting the desired infotainment language that are Hindi and English

Advanced Driver Assistance System (ADAS)

ADAS or Advanced Driver Assistance System refers to a suite of features that are designed to improve the safety and convenience of driving a vehicle. ADAS technology uses sensors, cameras, and radar among other systems to monitor the environment around a vehicle. Based on this, ADAS provides drivers with real-time information and alerts to help them avoid collisions and other potential hazards. Depending on the level of the ADAS tech, the system can either warn the driver by alerting through sound, vibration, and signals on the display or could take complete control of the vehicle to help in preventing any mishaps.

No automation

The driver has full control of the driving tasks

Driver assistance

The vehicle features a single automated system.

Partial automation

The vehicle can perform steering and acceleration

Conditional automation

The vehicle can control most driving tasks

High automation

The vehicle performs all driving tasks under certain conditions

Full automation

The vehicle performs all driving tasks under all conditions

Case study on EVs:
how connected can help reduce range anxiety?

Information at the user's fingertips about charging infrastructure and timely alerts

Nearest charging station and availability for type of charger

(Case study 1)

North-West

Rapid charger	1
Fast charger	2
Slow charger	5

South

Rapid charger	4
Fast charger	6
Slow charger	8

To alleviate range anxiety, electric vehicle battery will need to be safer, cheaper, charge faster and feature a high energy density for greater range.
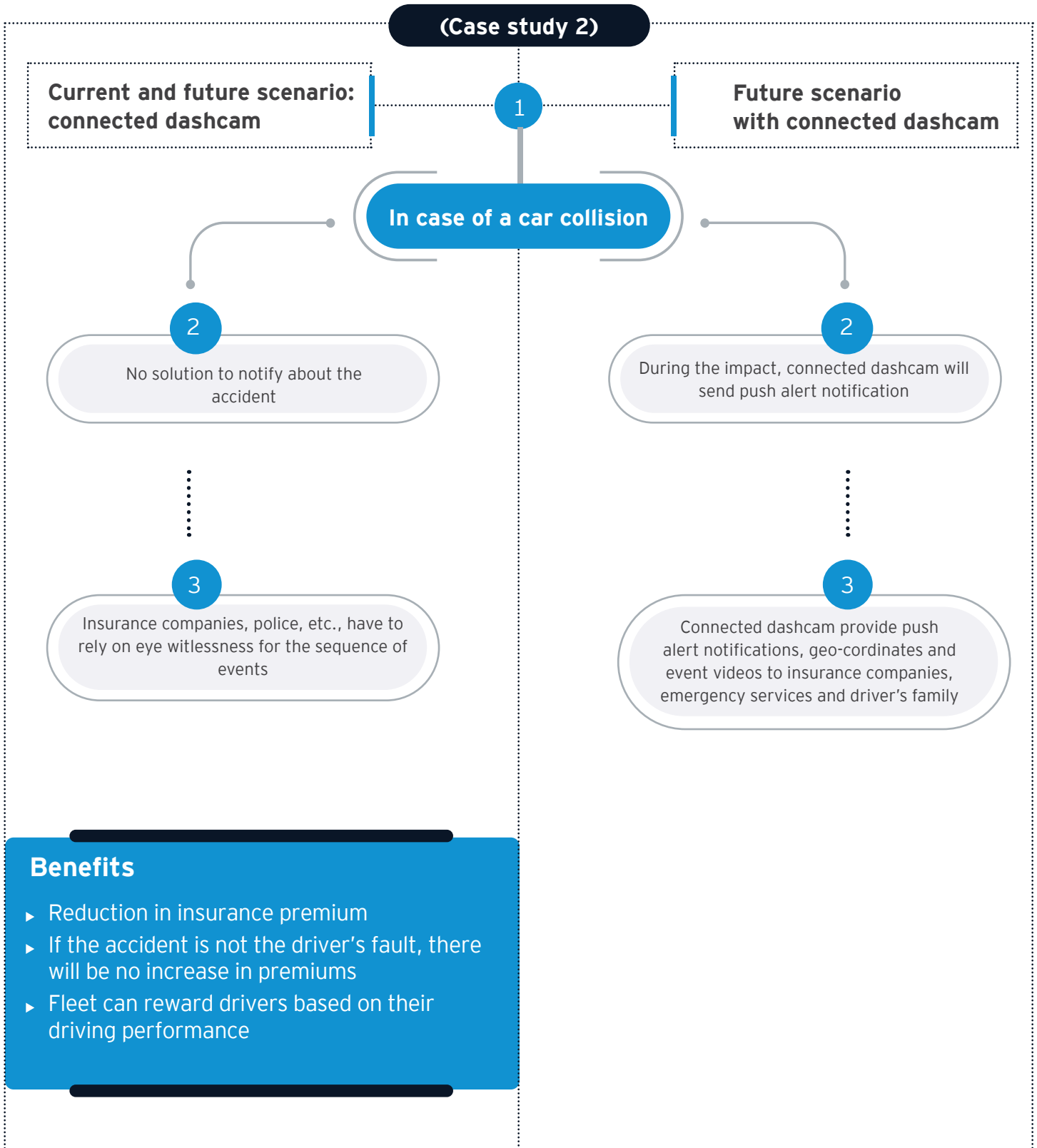
Peak and off peak pricing (surge pricing)

Estimated waiting time

Case study:
connected dashcam

(Case study 2)

Current and future scenario: connected dashcam

Future scenario with connected dashcam

1

In case of a car collision

2

No solution to notify about the accident

2

During the impact, connected dashcam will send push alert notification

3

Insurance companies, police, etc., have to rely on eye witlessness for the sequence of events

3

Connected dashcam provide push alert notifications, geo-cordinates and event videos to insurance companies, emergency services and driver's family

Benefits

- Reduction in insurance premium
- If the accident is not the driver's fault, there will be no increase in premiums
- Fleet can reward drivers based on their driving performance

Telematics in claims provide real customer protection and drive down insurance losses

Telematics as a survivor

(Case study 3)

Real time data transmission

- Location
- Motion
- Speed
- Vin number
- Acceleration
- Force of impact
- Other external environment such weather, traffic and road conditions

>> **Extra information via telematics devices will help manage insurance losses by enabling claims operators to determine the exact circumstance of the claim, including nature, type and extent of damage to the vehicle, as well as early indication of likely bodily injury**

- Reduction in underwriting and claim fraud
- Reduces the first notice of loss process
- Two-way communication can help identify individuals involved in the accident
- Improves the accuracy of case estimation damages, reducing the uncertainty in property damage and small injury claims

>> **Telematics enables a superior seamless claims process for a more holistic protection cover for customers**

- Theft
- Theft alarm is activated
- Theft notification to customer

- Provide vehicle recovery information to customer/police
- Avoiding total losses

>> **Accident**

- Instant crash/emergency notification
- Send relevant emergency services to the confirmed location
- Check customer record and contact family
- Remain in contract with the customer
- Confirm arrival of emergency service
- Saving lives

>> **Breakdown**

- Instant notification and location of the vehicle
- Direct the nearest recovery team to the vehicle's location

Core offering of telematics insurance and connected dashcam

Managing customer needs through core offerings

01

Core UBI offering

▶ Design usage-based insurance suited for the business individual and insurers

▶ Design operation model including aspects of product design, IT capacity, analytical function, claim management and capital

▶ As the product is still in its early stage of acceptance, guide the UBIs to understand the target market and test different product offerings

02

Risk selection: Driving behavior modifier

▶ Continuous improvement in risk selection by capturing and analyzing increasingly accurate information about individual driving behavior

▶ Actively manage claim costs through real feedback on driving behavior and instant notification of loss events

▶ Reduction of claims cost

03

Product innovation: Leverage through value-added services that are highly desired by the customer

▶ Provide value-added vehicle services, such as emergency services, breakdown services, theft notifications and early vehicle diagnostic services

▶ Additional opportunities exist around integration platforms, content provision and providing access to infotainment and navigation/traffic services

▶ Portal functions for new embedded applications, such as tracking of stolen vehicles, parental control, infotainment systems and viewer of journeys

▶ Support for a single point responsible for charging and billing for various services is necessary. This is a main reason for the increasing involvement of insurers in the value chain.

▶ For insurers aiming to become more deeply involved in the value chain, strategic alliances in the development of vehicle-independent services is an option

▶ Increased revenue and profitability from non-insurance product

▶ Increased retention for core insurance product

Increasing the product offering with additional services that match the customer's needs (emotional and logical) with the motor insurance product (traditionally, a begrudged purchase)
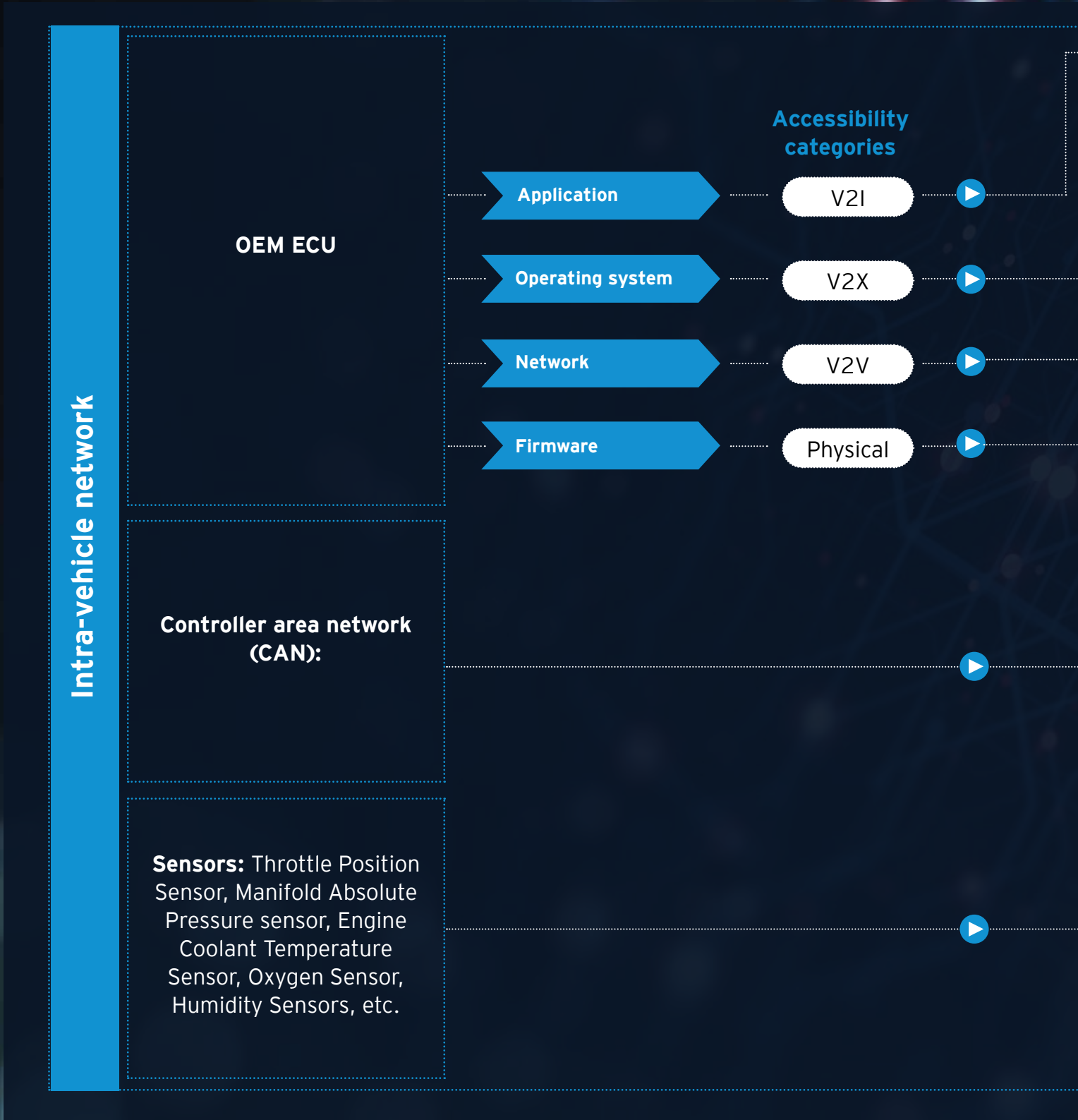
Section 03

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Risk to connected car architecture

Architecture of a connected car

Overall architecture and implementation view

Intra-vehicle network

OEM ECU

Application

Operating system

Network

Firmware

Accessibility categories

V2I

V2X

V2V

Physical

Controller area network (CAN):

Sensors: Throttle Position Sensor, Manifold Absolute Pressure sensor, Engine Coolant Temperature Sensor, Oxygen Sensor, Humidity Sensors, etc.

Network communication

LTE/GPS

RFID

Long-range wireless

Cloud services

Broadcast services

Breach at OEM data centres aimed at stealing customer's personal files, disabling vehicle's operation or spreading malicious activities.

Short-range wireless

Bluetooth

Consumer smart devices

Wireless network

Vehicle

Keyfob

Unauthorized access to vehicle internal network and infotainment system in order to steal private and corporate data, track individual vehicles or entire fleets and hijack non-safety and safety-critical function.

Physical connection

USB

Consumer media devices

ODB-II

Programming/ diagnostic device

Physical access and tampering of OBD device leading to compromise of critical functions.
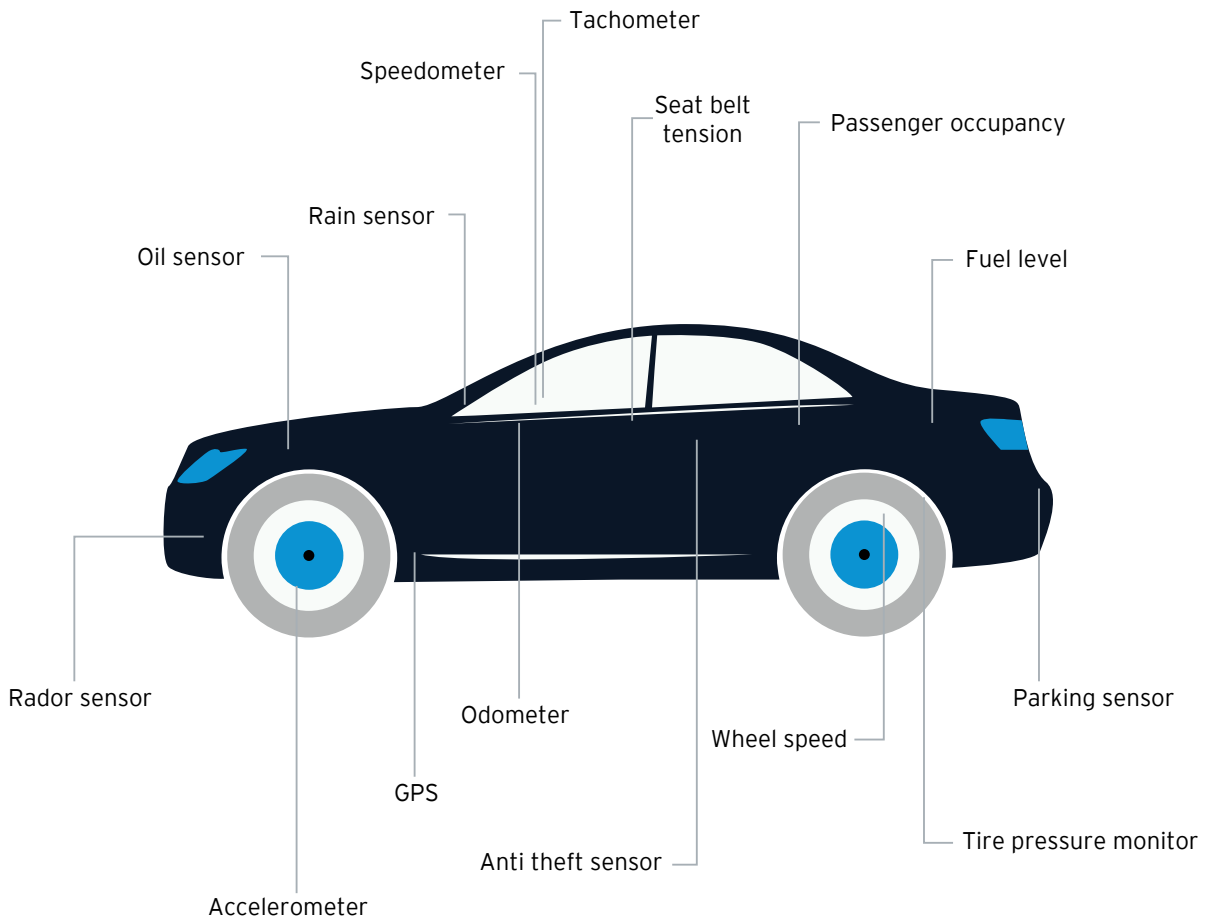
V2I : Vehicle-to-infrastructure

V2X : Vehicle-to-anything

V2V : Vehicle-to-vehicle

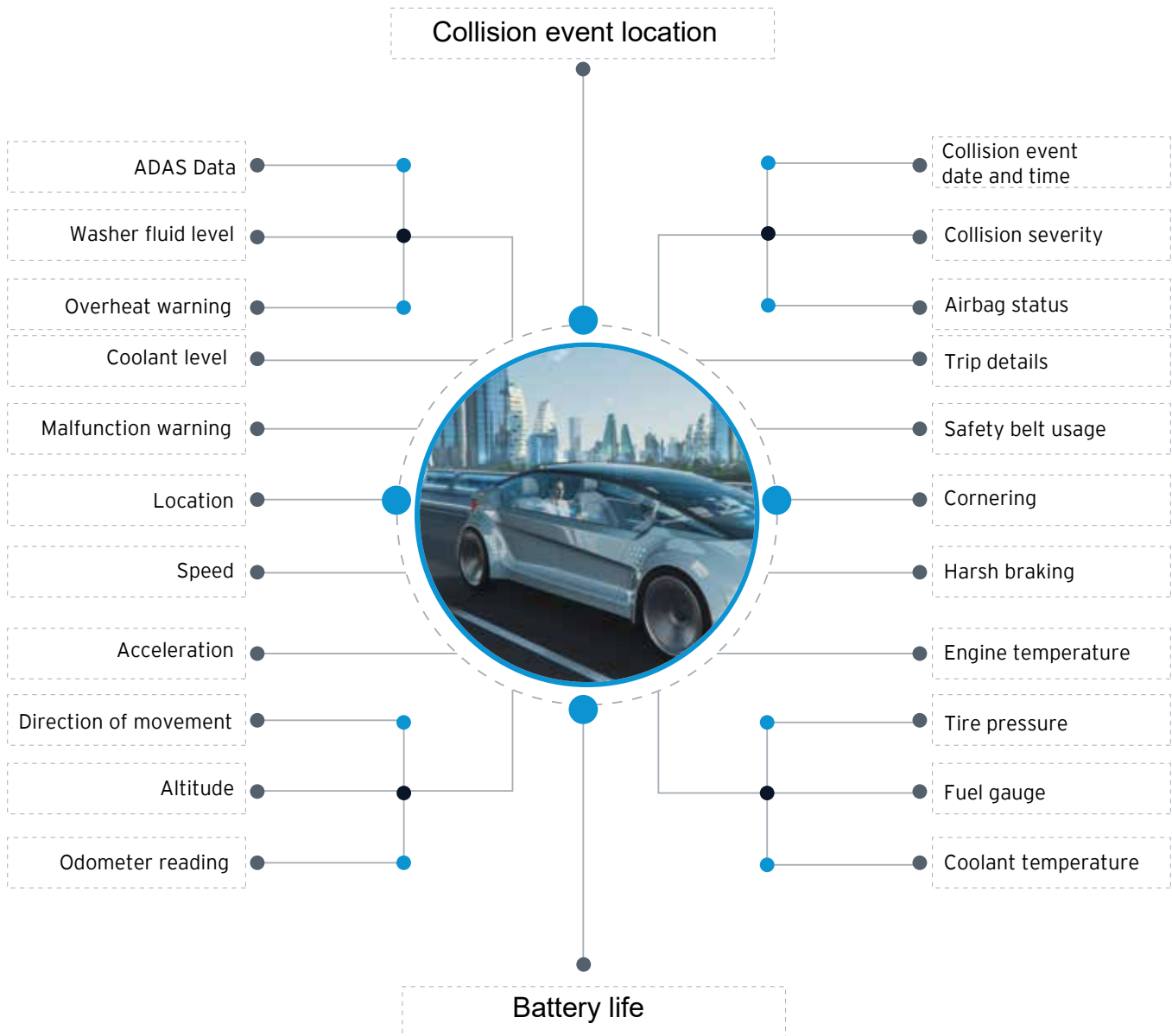**RFID :** Radio Frequency Identification

Data points in connected

Connected car record and collate a wide variety of data attributes specific to the car, driver, driving environment, and more. This data is then shared with apps and services for mutual benefits
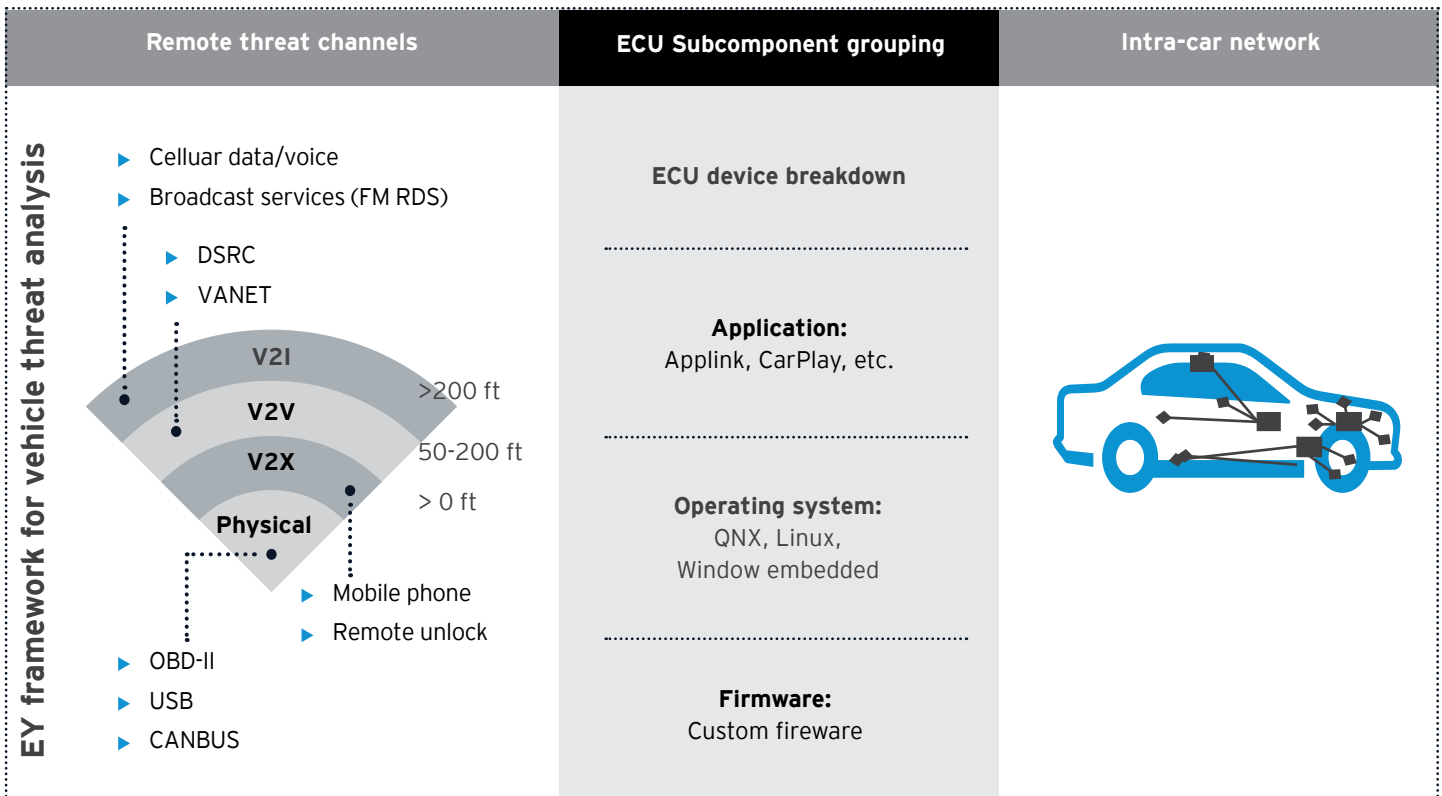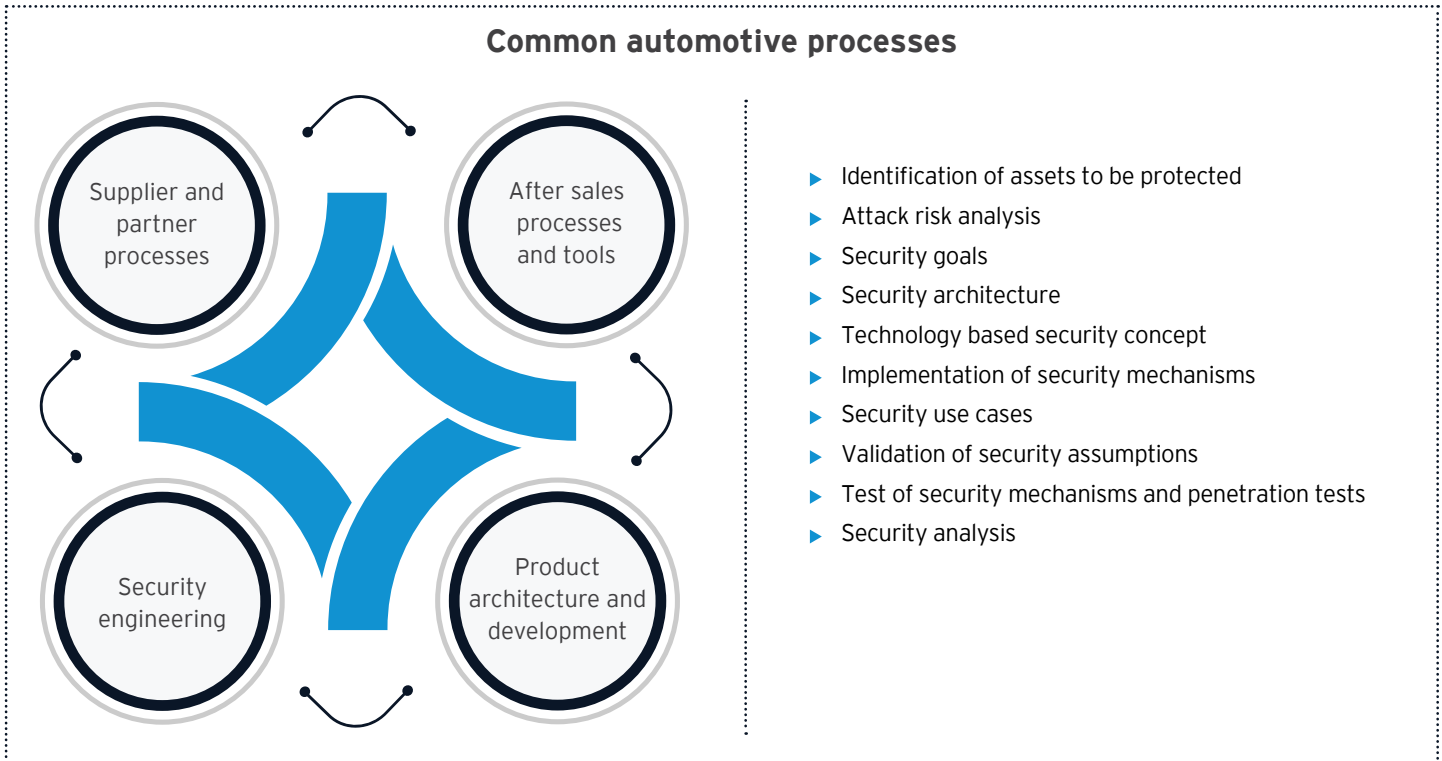

Tachometer

Speedometer

Seat belt tension

Passenger occupancy

Rain sensor

Oil sensor

Fuel level

Rador sensor

Odometer

Parking sensor

Wheel speed

GPS

Anti theft sensor

Tire pressure monitor

Accelerometer

Data points in connected

Collision event location

ADAS Data

Washer fluid level

Overheat warning

Coolant level

Malfunction warning

Location

Speed

Acceleration

Direction of movement

Altitude

Odometer reading

Collision event date and time

Collision severity

Airbag status

Trip details

Safety belt usage

Cornering

Harsh braking

Engine temperature

Tire pressure

Fuel gauge

Coolant temperature

Battery life

Assessment of security testing in connected car

Security oriented implementation of architecture and functions for connected cars

Common automotive processes

- Supplier and partner processes
- After sales processes and tools
- Security engineering
- Product architecture and development

- ▶ Identification of assets to be protected
- ▶ Attack risk analysis
- ▶ Security goals
- ▶ Security architecture
- ▶ Technology based security concept
- ▶ Implementation of security mechanisms
- ▶ Security use cases
- ▶ Validation of security assumptions
- ▶ Test of security mechanisms and penetration tests
- ▶ Security analysis

Remote threat channels	ECU Subcomponent grouping	Intra-car network

EY framework for vehicle threat analysis

- ▶ Celluar data/voice
- ▶ Broadcast services (FM RDS)
  - ▶ DSRC
  - ▶ VANET

V2I

V2V >200 ft

V2X 50-200 ft

> 0 ft

Physical

- ▶ Mobile phone
- ▶ Remote unlock
- ▶ OBD-II
- ▶ USB
- ▶ CANBUS

ECU device breakdown

Application:
Applink, CarPlay, etc.

Operating system:
QNX, Linux,
Window embedded

Firmware:
Custom fireware

How big is the problem?

Canada ranked #1 in total number of cyber crime complaints received in 2022

Top five countries by the total number of cyber crime complaints received

S.no.	Country	Complaint %	Total number of complaints received
1	Canada	33.07%	5,517
2	India	28.8%	2,550
3	Australia	20.90%	2,489
4	France	8.90%	2,061
5	South Africa	8.33%	1,929

Cyber crime - major statistics - 2022

Victim losses in 2022 amounted to US$10.13 billion*

Over 2175 complaints received per day on an average

Age	Complaint %	Total Loss (US$ m)
Under 20	9,129	210.5
20-29	40,924	383.1
30-39	46,342	1,300
40-49	50,545	1,600
50-59	48,642	1,800
Over 60	62,085	3,100

Source: 2022 Internet Crime Report, FBI I3C

Section 04

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Scenarios of cyberattack

- Quick Snapshot
- Attack Scenario:
    - In-vehicle infotainment system
    - Wifi Hotspot
    - 5G SIM
    - Mobile application
    - Inside threat
    - Attack scenario: ADAS

Quick snapshot: cybersecurity market for cars

▶ The cybersecurity market for cars was valued at US$186.63 million in 2019 and is expected to reach a value of US$2460.9 million by 2025, registering a CAGR of 52.15%.

▶ The cybersecurity market for cars is primarily driven by the increasing connectivity of vehicles, the growing adoption of telematics services in automobiles and increasing integration of advanced features.

▶ The automotive industry across the globe is undergoing a wave of innovation and advancements, with the emergence of ground-breaking technologies, such as the Internet of Things (IoT), enhanced GPS, location and maintenance live recording, reminders, driving assistance, and Wi-Fi services, the demand for connected cars has been rapidly increasing, driving the market forward.

▶ As all connected vehicles rely entirely on connected software for all aspects of their operation, they are vulnerable to a wide range of cybersecurity attacks. This vulnerability increases the need for cybersecurity solutions, which is driving the market forward

▶ The presence of in-vehicle infotainment systems and improved wireless network systems in automobiles has boosted the sales of connected cars in the Asia-Pacific region, thereby, driving the overall cybersecurity market for cars in the region.

EY cyberattack scenarios
Attacker levels and test scenarios

Attackers posses varying levels of skill which we group into four levels as shown in the table below. Against each of the four levels EY has devised a set of test scenarios that we would recommend performing to provide confidence that the component is able to withstand the associated level of attack and associated attack vectors. A process of threat assessment is used to identify the likely attacker, the attack vectors used, their motivations and typical attack targets.

Attacker level	Capability	Example attack vectors
1 Beginner (script Kiddie)	▶ Has a basic security understanding ▶ Is able to use public exploits or reproduce trivial security findings	▶ Tries out known attack vectors against the WiFi of the headunit, e.g., breaks the WEP and brute forces easy WPA keys ▶ Port-scans the head unit and looks for commonly known vulnerabilities ▶ Tries to get firmware images of ECUs online and looks through them directly for strings with credentials ▶ Reads car-hacking papers to reproduce findings of the past or is able to reproduce back-doors which are known on Internet forums
2 Professional (experienced attacker)	▶ Profound security understanding and experience ▶ Able to adapt existing exploits ▶ Has some basic hardware-level exploitation experience	▶ Opens embedded devices and tries to read the memory chips ▶ Uses open debug ports to attach debuggers ▶ Reverse engineers K-matrixes ▶ Identifies simple buffer overflows in firmware which can be accessed via debug interfaces ▶ Is able to discover multi-hop attack vectors from the car to the IT infrastructure ▶ Is able to attack RF communication with known flaws in WiFi, GSM and Bluetooth, and well understood busses, e.g., CAN and LIN

Attack vectors: in-vehicle infotainment (IVI)
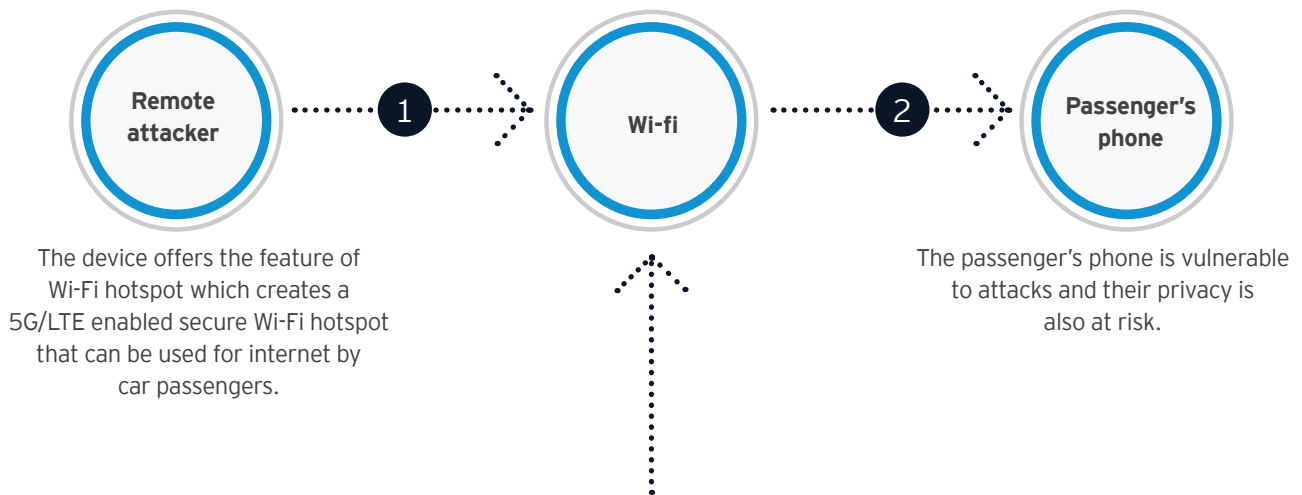

Scenario 1

In-vehicle infotainment

Remote attacker → **1** → **Malicious song file** → **2** → **Passenger's phone**

The remote attacker sends a malicious code masked as an entertainment file.

The file is sent to a phone which has access to the car or is already connected to the IVI system.

3

Connected via USB cable

Connected car device ← **4** ← **IVI system**

Exploited

The attacker now has gained access to the device and can control its operation, utilizing and can use its feature to cause different types of attacks.

Unknowingly the phone owner opens the file while the phone is connected to the IVI system and the malicious code starts running.

Attack vectors: Wi-Fi hotspot

Wi-Fi hotspot

Anyone in the car with a mobile device
can now connect to the hotspot created
by the device's Wi-Fi.

Remote attacker → **1** → **Wi-fi** → **2** → **Passenger's phone**

The device offers the feature of Wi-Fi hotspot which creates a 5G/LTE enabled secure Wi-Fi hotspot that can be used for internet by car passengers.

The passenger's phone is vulnerable to attacks and their privacy is also at risk.

▶ An attacker can hijack the browsing session and snoop on the websites visited over an LTE connection using an attack called aLTEr.

▶ Attacker using this exploit in the LTE service can gain access to the mobile device and can use it to spy, spam, track and spoof.

Attack vectors: 5G SIM

Scenario 3

5G SIM

Remote attacker → 1 → **5G SIM** → 2 → **Device**

A remote attacker can try to remotely hack the SIM by getting the encrypted key (which can be obtained in a number of ways).

The 5G SIM stores the video recordings and the conversation that took place in the car. It also gives a hotspot option to the passengers of the car.

The 5G SIM is introduced in the device to enable data transfer to cloud storage and to create connectivity within the car.

Vehicle ← 4

The device is mounted in the car and having control of the device gives the attacker the control of the car and they can invade the privacy of the owner.

Attack vectors: mobile application

Scenario 4

Mobile application

Remote attacker → 1 → **Mobile application** → 2 → **Owner's mobile**

A remote attacker can hack the application of the device and get access to the device as well as the mobile phone.

The mobile application can be used by people other than the owner. The application itself may have inherent vulnerabilities which leaves it susceptible to multiple types of attacks, thus rendering the device vulnerable.

3 ↓

Car with device ← 4 ← **Connected car device**

The device can have a mobile application which the owner can use to monitor the device, the car and get real time alerts.

Unknowingly the phone owner opens the file while the phone is connected to the IVI system and the malicious code starts running.

Attack vectors: inside threat (servicing)

Scenario 5

Inside threat

Car whilst servicing

2

Device

3

Access to device-mounted car
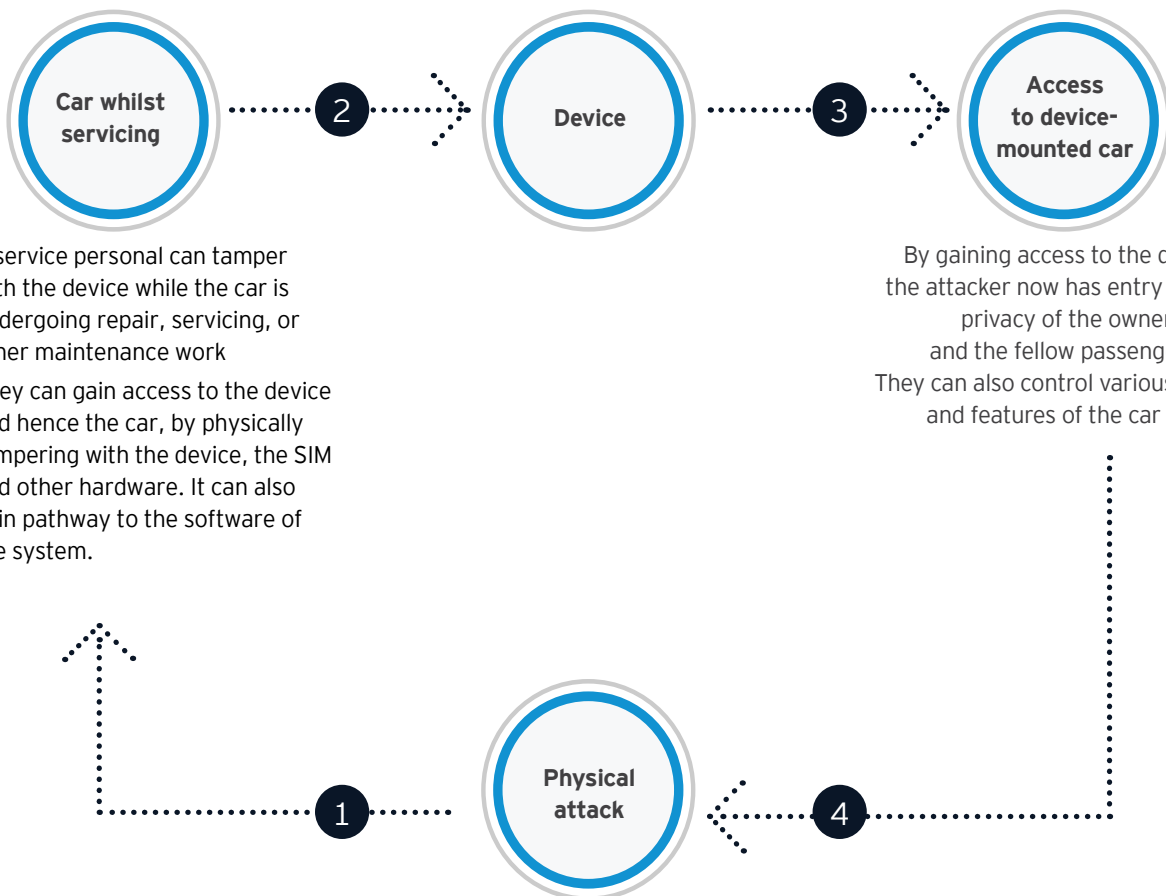
- ▶ A service personal can tamper with the device while the car is undergoing repair, servicing, or other maintenance work
- ▶ They can gain access to the device and hence the car, by physically tampering with the device, the SIM and other hardware. It can also gain pathway to the software of the system.

By gaining access to the device, the attacker now has entry into the privacy of the owner and the fellow passengers. They can also control various aspects and features of the car too.

1

Physical attack

4

Attack vectors: insider threat

Scenario 6
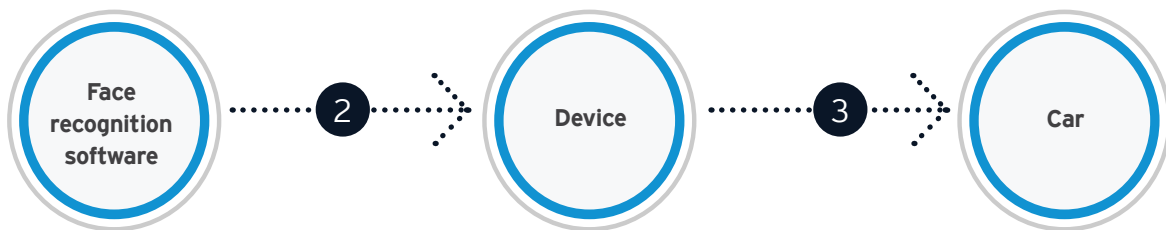
Face recognition software
Face recognition software identifies the driver from the list of familiar drivers added to the account and then only give him/her access to the car.

2

Device
The attacker can fool the software by using disguise or by sending a **counter code** to the device to access the facial recognition software.

3

Car
Once the software mistakenly gives access to the attacker, they gain control of the car.

1

Physical attack

4

Attack vectors: insider threat (OBD port)

Scenario 7

Debug port → **3** → **Device** → **4** → **Vehicle**

Debug contains two CAN bus ports which allows microcontrollers and devices to communicate with each other.

An attacker can gain access to the device by plugging in a malicious code via the debug port.

Gaining access to the device provides the attacker with access to the car.

5

2 ← **Computer needed to connect to debug Port** ← **1** ← **Malicious attacker**

Common cyberattacks on ADAS system

Multiple sensors in cars and vehicles are utilized to gather driver information and convert raw data into intelligent outputs. However, these sensors can be misconfigured by the attackers to perform malicious attacks

Sensor spoofing

Attackers may attempt to manipulate the sensors (such as cameras, radar, lidar) in ADAS to provide false information to the system. This could mislead the vehicle into making incorrect decisions, potentially leading to accidents

Denial of Service (DoS)

A denial-of-service attack could disrupt the normal functioning of ADAS by overwhelming its communication channels or sensors with excessive traffic. This could temporarily disable critical safety features
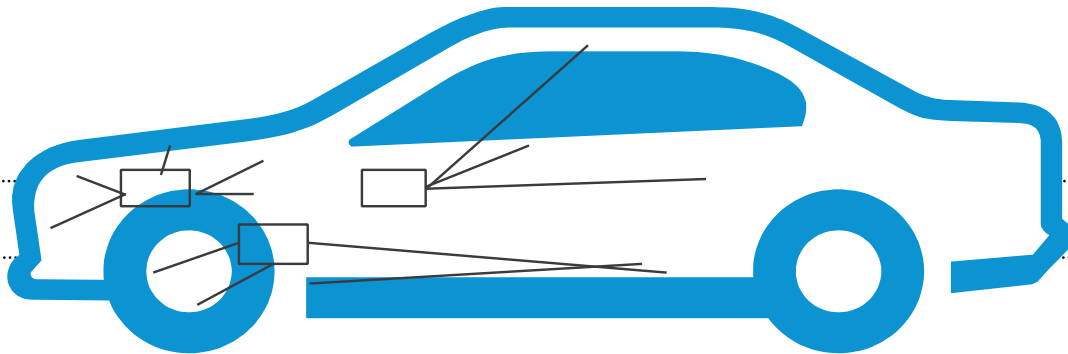
Data injection

Cybercriminals might inject malicious data into the communication networks of ADAS, affecting the decision-making process of the system. This could result in unsafe driving conditions or compromise the overall functionality of the vehicle

Firmware attacks

Attackers may target the firmware of ADAS components, exploiting vulnerabilities in the software that controls the hardware. This could lead to unauthorized access or manipulation of critical functions.

Section 05

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

How can EY help?
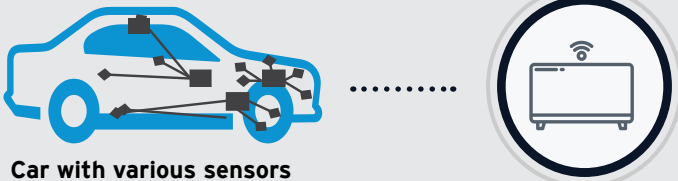
Connected car: how we see it

EY capabilities

- Connected car strategy formulation
- Big data analytics

- Implementation support
- Predictive maintenance and asset planning

- Monetization strategy
- Digital risk and cybersecurity

Automotive companies can reap sustained benefits by effectively implementing a connected car strategy

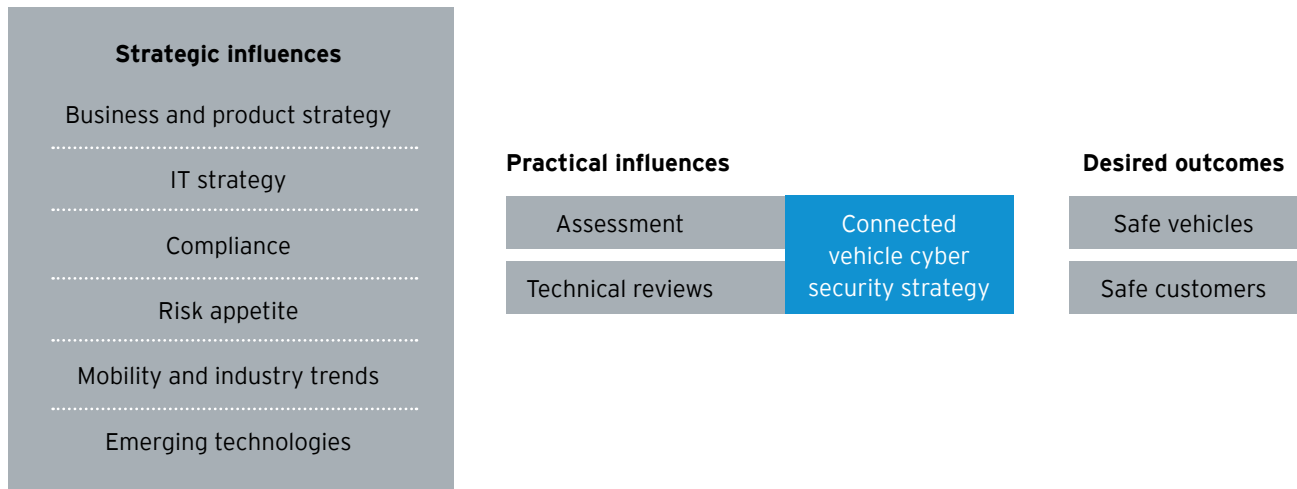| OEMs	Third party/others	Customer
- Remote diagnostic and prognostic services - Improve after sales and support service - Leverage connected car offering as unique differentiator and improve customer loyalty	- Telematics for fleet management - Content creation and management services - Opportunities for telecom companies in machine-to-machine communication in vehicle	- Advanced assisted driving capabilities - On demand infotainment - Augmented navigation

- OEMs can offer significant value to its customers by combining various elements from online applications, driver assistance, call center services and solutions for the integration of mobile devices
- Services provided by the company can include vehicle management, travel and navigation, parking, entertainment, information, emergency call, vision and drive assistance
	- Companies can use driving usage and car performance data to:
	  - Optimize inventory for spares
	  - Feedback into new product development
	  - Sending maintenance alert to customers and dealership
	  - Over-the-air tuning of the vehicle
		- Customers can be provided with customized web portals, where they can view diagnostic reports, download directions to the vehicle or even unlock the car's doors
		- The connected car exists within the network and is susceptible to cyber threats. Companies must strike a balance between trust and risk, considering not only the level of risk but also the level of trust. Assessing how much assurance they have regarding the security of their connected car systems.
		- Advanced assisted driving capabilities can be provided by leveraging sensors, analytics, NLP, RPA and cloud computing

Car with various sensors

To secure the connected car, cybersecurity needs to be embedded across the entire ecosystem

Our strategic partnering value
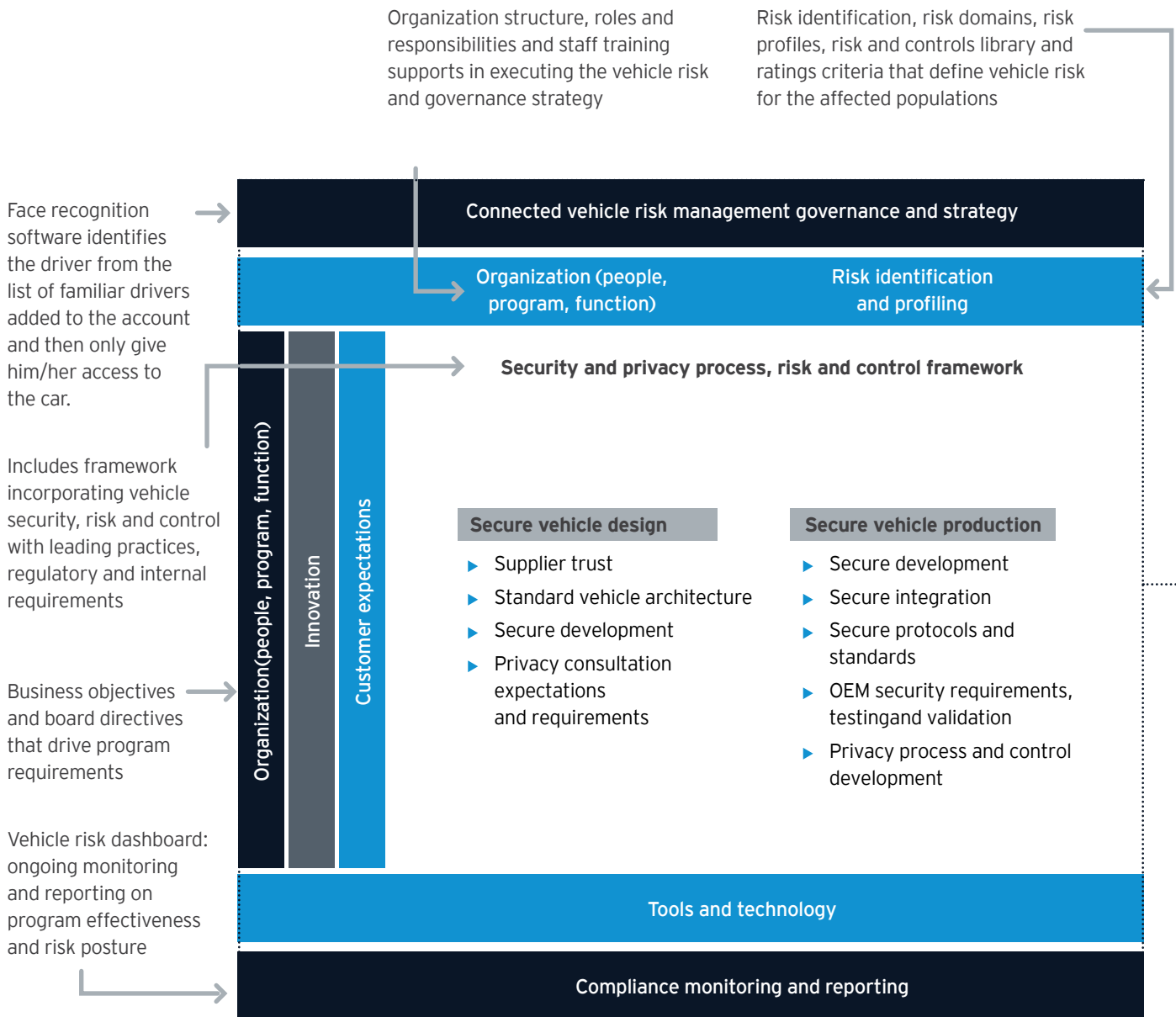
- We use knowledge to build and deploy meaningful solutions consistent with client's objectives and expectations of EY.
- Our approach is technology and partner agnostic, we leverage the best tools and team with the industry experts to deliver a complete end-to-end service.
- The depth and breadth of our firm allows us to tap into globally renowned subject matter resources and industry leading methodologies.

- EY is known and respected for the comprehensive and extensive nature of our cybersecurity practice.
- We are the market leaders in building, operating, and sustaining cyber security.
- Our approach is founded in a firm repeatable process that is capable of flexing with the unique needs of connected vehicle.

A robust connected vehicle cyber security strategy....

Strategic influences

Business and product strategy

IT strategy

Compliance

Risk appetite

Mobility and industry trends

Emerging technologies

Practical influences

| Assessment | Connected vehicle cyber security strategy |
| Technical reviews | |

Desired outcomes

Safe vehicles

Safe customers

EY's vehicle ecosystems: cyber security and privacy framework

Connected car: how we see it!

Organization structure, roles and responsibilities and staff training supports in executing the vehicle risk and governance strategy

Risk identification, risk domains, risk profiles, risk and controls library and ratings criteria that define vehicle risk for the affected populations

Face recognition software identifies the driver from the list of familiar drivers added to the account and then only give him/her access to the car.

Includes framework incorporating vehicle security, risk and control with leading practices, regulatory and internal requirements

Business objectives and board directives that drive program requirements

Vehicle risk dashboard: ongoing monitoring and reporting on program effectiveness and risk posture

Connected vehicle risk management governance and strategy

Organization (people, program, function)

Risk identification and profiling

Security and privacy process, risk and control framework

Organization(people, program, function)

Innovation

Customer expectations

Secure vehicle design	Secure vehicle production
▶ Supplier trust	▶ Secure development
▶ Standard vehicle architecture	▶ Secure integration
▶ Secure development	▶ Secure protocols and standards
▶ Privacy consultation expectations and requirements	▶ OEM security requirements, testingand validation
	▶ Privacy process and control development

Tools and technology

Compliance monitoring and reporting

Cyber securing connected cars 2.0: navigating opportunities and risks in the digital era

Operational policies and standards
that assist in achieving vehicle risk
management objectives and effective
management of IT risk

Connected vehicle risk management governance and strategy

Policies and standards

Security and privacy process, risk and control framework

Alignment with the
regulatory require-
ments for maintaining
a secure vehicle
ecosystem

Design
methodologies and
procedures to enable
secure vehicles

New and emerging requirements

National and regional variation

Regulatory requirements

Security vehicle operations

▶ Risk management

▶ Security monitoring

▶ Change management

▶ Incident management

▶ Privacy, communication and
preference management

Processes, proce-
dures and methods
for operating the
vehicle security
framework

Tools to facilitate
vehicle risk
management
governance and
strategy operational
processes and
reporting framework

Tools and technology

Compliance monitoring and reporting

EY's vehicle ecosystems: cyber security and privacy framework

EY's Cybersecurity offerings for Connected Cars

Cybersecurity Management System – Assessment / Implementation / Audit

Various security standards and regulations:

ISO/SAE 21434

UN Regulation No. 155

NHTSA Cybersecurity Best Practices

GDPR and Data Privacy Regulations

Automotive Cybersecurity Best Practices

Functional Safety Standards (ISO 26262)

Automotive SPICE

SAE J3061

Threat Assessment and Risk Assessment (TARA) as a Service

DevSecOps as a Service	Supply Chain Security
Vulnerability Management As a Service	Vulnerable Components Threat intelligence
Penetration Testing for SDV Ecosystem	Plant Security – ICS / IIoT
Zero Trust Architecture – Design and Review	Vehicle SOC
Static Code Review / Open-Source Code Review	Incident Response as a Service

Notes:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

For more information please contact us.

Our team will happy to serve you.

Our Mobility Leadership

Vinay Raghunath
vinay.raghunath@parthenon.ey.com

Srihari Mulgund
srihari.mulgund@parthenon.ey.com

Som Kapoor
som.kapoor@parthenon.ey.com

Pratik Shah
pratik.s@parthenon.ey.com

Cybersecurity Team

Burgess S Cooper
Burgess.Cooper@in.ey.com

Sumit Malhotra
Sumit1.Malhotra@in.ey.com

Akshay Tiku
akshay.tiku@in.ey.com

Sambit Sinha
Sambit.Sinha@in.ey.com

Key Contributors

Amit Punjani
Amit.Punjani@in.ey.com

Payel Ray Chaudhury
payel.chaudhury@parthenon.ey.com

Nikhil Joshi
nikhil1.joshi@in.ey.com

Kanika Sharma
Kanika.Sharma@in.ey.com

Our office

Ahmedabad
22nd Floor, B Wing, Privilon
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway
Ahmedabad - 380 059
Tel: + 91 79 6608 3800

Bengaluru
12th & 13th floor
"UB City", Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
11, Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh
Elante offices, Unit No. B-613 & 614
6th Floor, Plot No- 178-178A
Industrial & Business Park, Phase-I
Chandigarh - 160 002
Tel: + 91 172 6717800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Ground Floor
67, Institutional Area
Sector 44, Gurugram - 122 003
Haryana
Tel: +91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000

Hyderabad
THE SKYVIEW 10
18th Floor, "SOUTH LOBBY"
Survey No 83/1, Raidurgam
Hyderabad - 500 032
Tel: + 91 40 6736 2000

Jamshedpur
1st Floor, Fairdeal Complex
Holding No. 7, SB Shop Area Bistupur,
Jamshedpur – 831 001
East Singhbhum Jharkhand
Tel: + 91 657 663 1000

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 304 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

ey.com/en_in

@EY_India   EY   EY India   EY Careers India   @ey_indiacareers