Infotainment & Telematics

Connected Car Security

STRATEGY ANALYTICS

Roger C. Lanctot

Director, Automotive Connected Mobility

Global Automotive Practice

AUTOMOTIVE PRACTICE – SINCE 1988

STRATEGY ANALYTICS

LEADING-NAME CLIENTS ACROSS THE VALUE-CHAIN

70% of T1 Suppliers

90% of Major Auto Semi Suppliers

70% of top OEMs

FIVE SERVICES TO COVER ALL AUTOMOTIVE OPPORTUNITIES

Infotainment & Telematics

Powertrain, Body, Chassis & Safety

Autonomous Vehicles

In-Vehicle UX

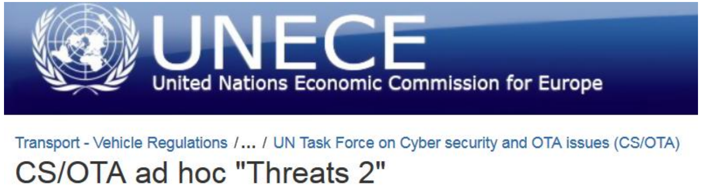
CONNECTED MOBILITY

AGENDA

- **Vehicle Vulnerability:** From theft to cyber crime
- **Connectivity:** Status of adotion
- **Automated Driving:** From driver control to remote control

- **Implications for Security and Law Enforcement**

UNECE – CONNECTIVITY CONTRADICTIONS



UNECE
United Nations Economic Commission for Europe

Transport - Vehicle Regulations /... / UN Task Force on Cyber security and OTA issues (CS/OTA)

CS/OTA ad hoc "Threats 2"

1		External hacking/contamination of: • safety-critical functions; • non-safety functions; • information systems
2		Illegal/unauthorised changes to vehicle's electronic ID
3		Hacking/tampering to circumvent monitoring systems or falsify data
4		Jamming (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems
5		Spoofing of sensor data
6		Interference with control units, master data and firmware/software
7		Unintended impact caused by mistaken action by owner, operator or maintenance engineer
8		Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action

We need connectivity

Connectivity is a problem

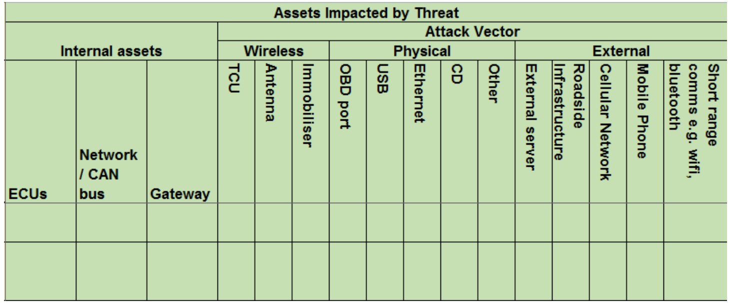
We need software updates

Software updates are problematic

Automotive systems must be secure

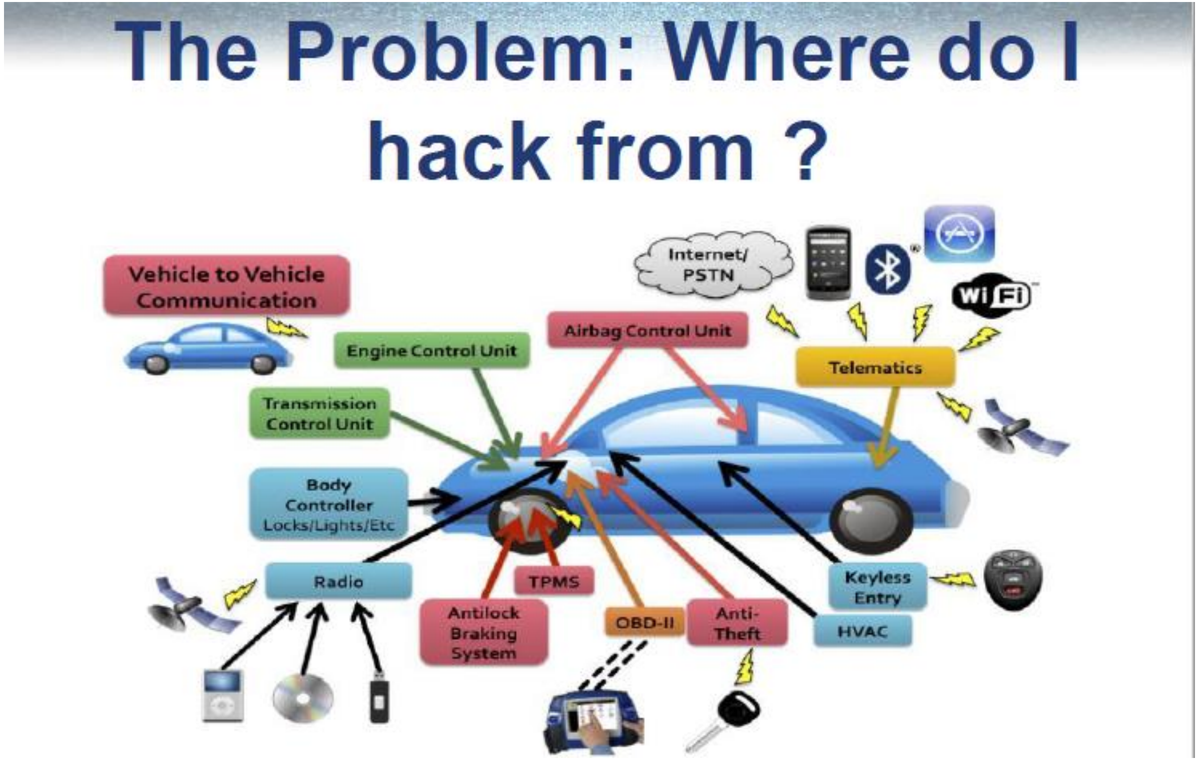
Automotive systems will never be secure

100-150 ECUs, 7 networks, multiple gateways



Assets Impacted by Threat																
			Attack Vector													
Internal assets			Wireless			Physical					External					
ECUs	Network / CAN bus	Gateway	TCU	Antenna	Immobiliser	OBD port	USB	Ethernet	CD	Other	External server	Roadside Infrastructure	Cellular Network	Mobile Phone	Short range comms e.g. wifi, bluetooth	

THE CAR AS A SIEVE



The Problem: Where do I hack from ?

VEHICLE THEFT MAKING A COMEBACK

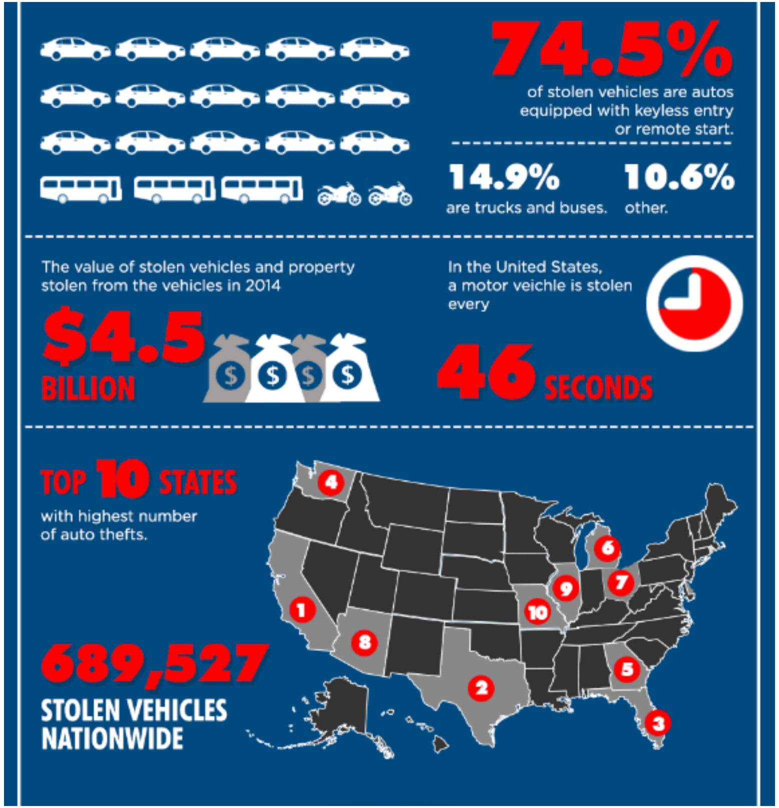
On the rise in the U.S. and U.K.

Widespread perception that problem is solved – FALSE!

Most press attention to white hat hacks, stunts – Jeep hack!

Keyless entry primary point of vulnerability

Car makers struggling to respond



74.5% of stolen vehicles are autos equipped with keyless entry or remote start.

14.9% are trucks and buses.

10.6% other.

The value of stolen vehicles and property stolen from the vehicles in 2014

$4.5 BILLION

In the United States, a motor veichle is stolen every

46 SECONDS

TOP 10 STATES with highest number of auto thefts.

689,527 STOLEN VEHICLES NATIONWIDE

GUARDKNOX HARDWARE SOLUTION

Centralized

Single ECU

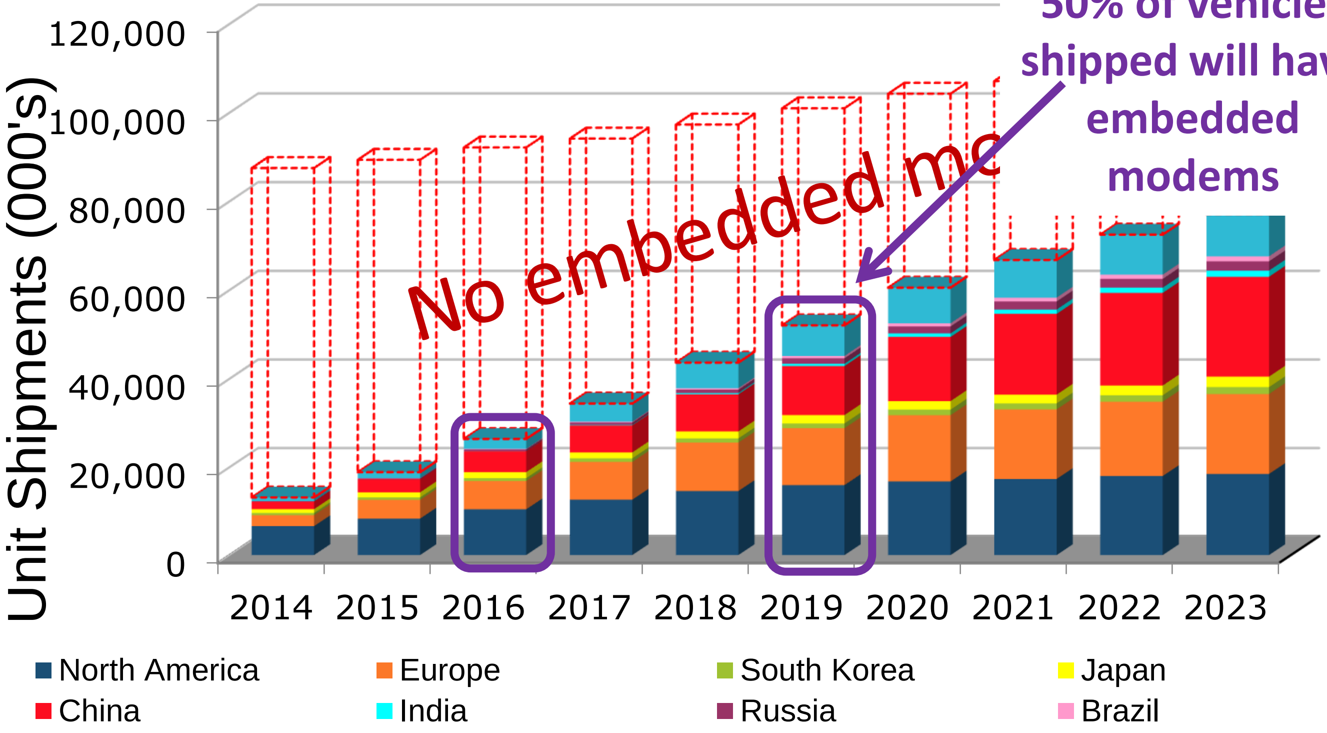
Certified

ISO

ISO 26262

COMMON CRITERIA CERTIFIED

AUTOMOTIVE EMBEDDED MODEMS GLOBAL ANNUAL SHIPMENTS



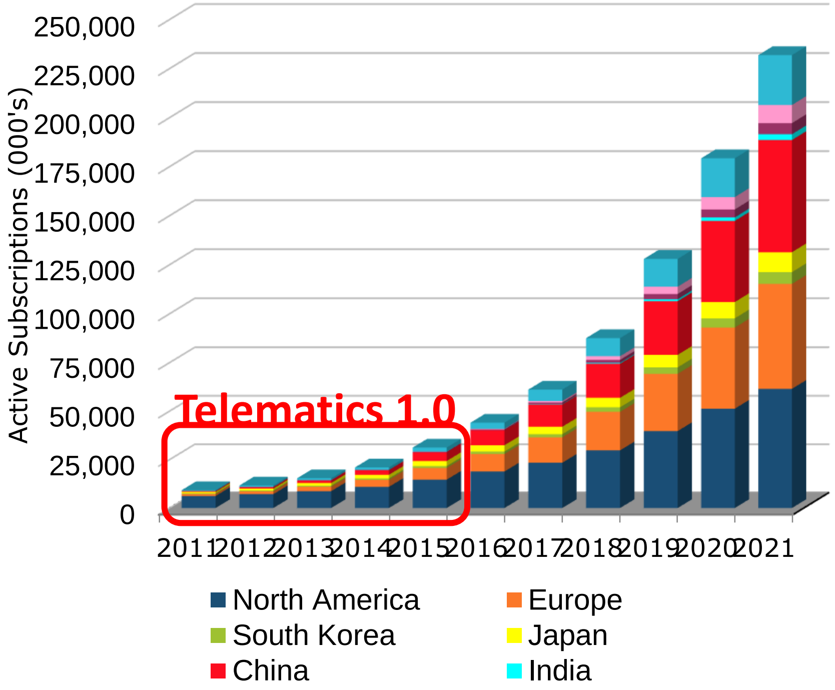
50% of vehicles shipped will have embedded modems

Source: Infotainment & Telematics Service

OEM EMBEDDED TELEMATICS ACTIVE VEHICLE SUBSCRIPTIONS BY REGION

STRATEGY ANALYTICS

Global Active subscriptions will exceed 250 Million by 2022



Leading Regions:

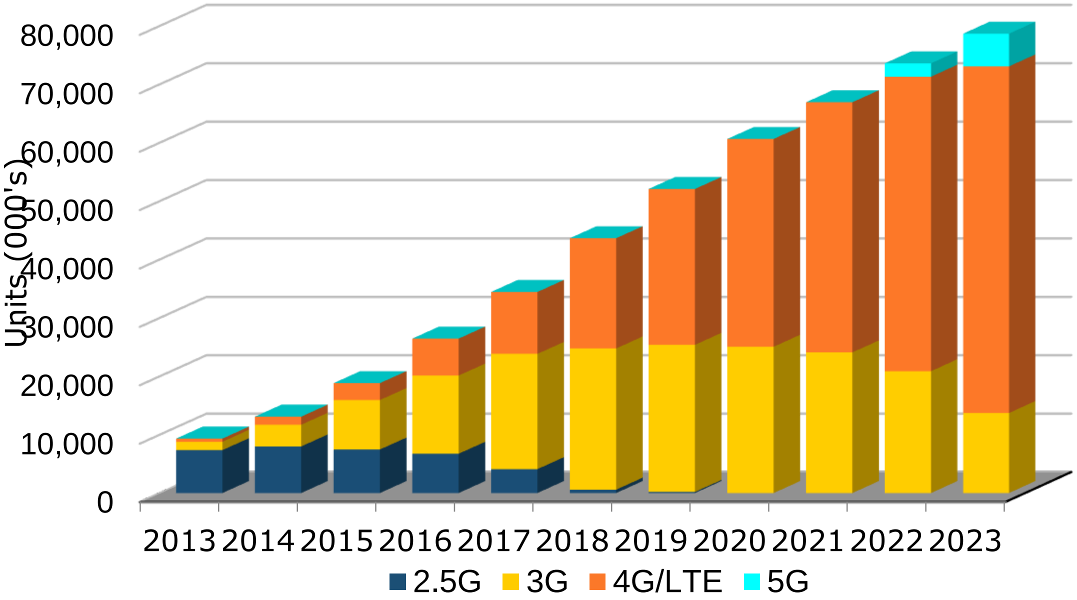
- ➢ **North America: Market Driver – Early Adoption**
- ➢ **Europe: Market Driver – eCall**
- ➢ **China: Market Driver – Biggest Global car market**

Source: Infotainment & Telematics Service

OEM EMBEDDED TELEMATICS CELLULAR MODEM SHIPMENTS - GLOBAL

STRATEGY ANALYTICS

Telematics Forecast 2015 vs. 2023 (18.8 Mil. units → 78.6 Mil. units)

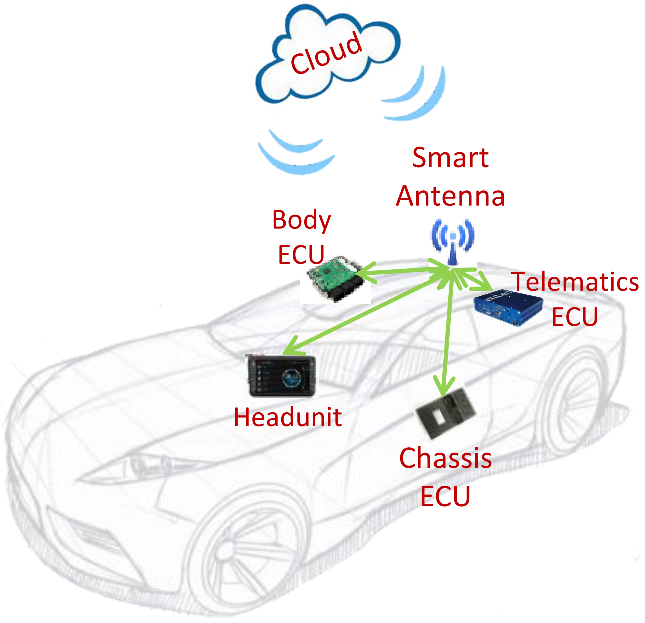


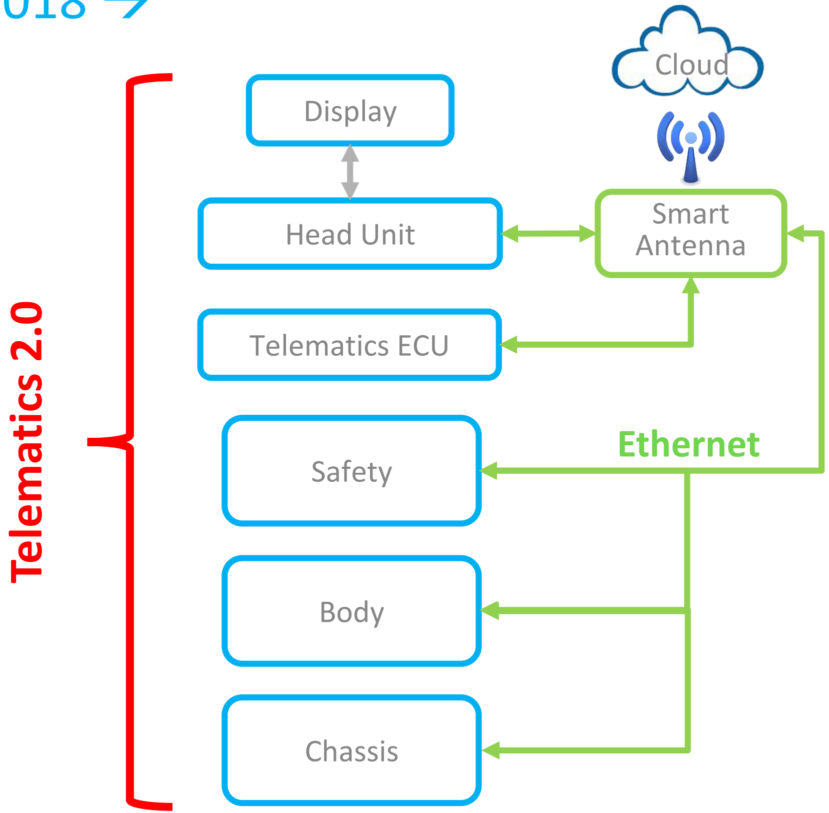
- **2.5G Network:** 7.4 Mil units in 2015 to 0K units from 2020
- **3G Network:** 8.4 Mil in 2015 units to 13.7 Mil units in 2023
- **4G/LTE Network:** 2.8 Million units in 2015 to 58 Mil units in 2023
- **5G Network:** 5.6 Million in 2023

Source: Infotainment & Telematics Service

NEXT GEN CONNECTED CAR DESIGN → DOMAIN & BUS CONVERGENCE

2018 →





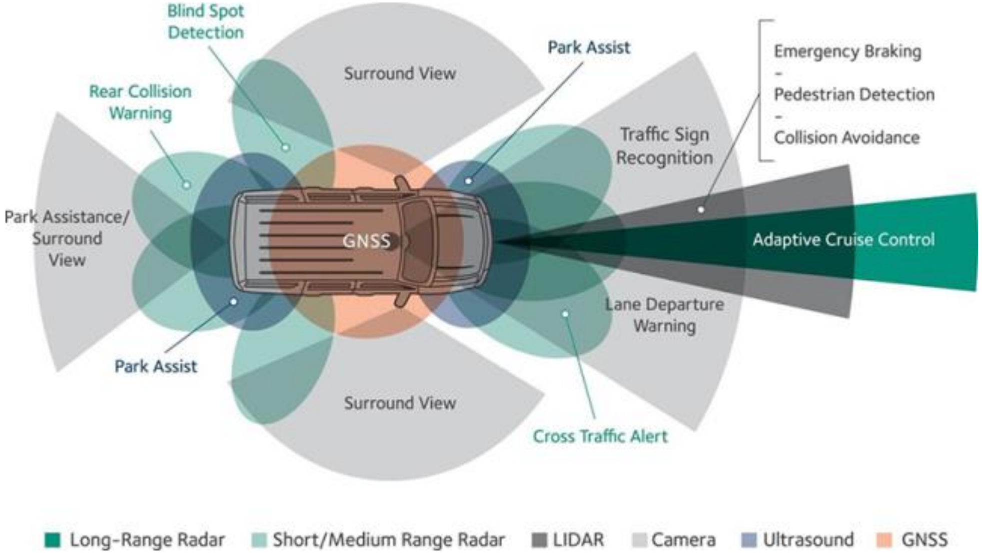
Source: Infotainment & Telematics Service

COMPLEX CRITICAL SYSTEMS NEED RAPID UPDATE CYCLES…

STRATEGY ANALYTICS

Example is Safety - There is increasing reliance on:

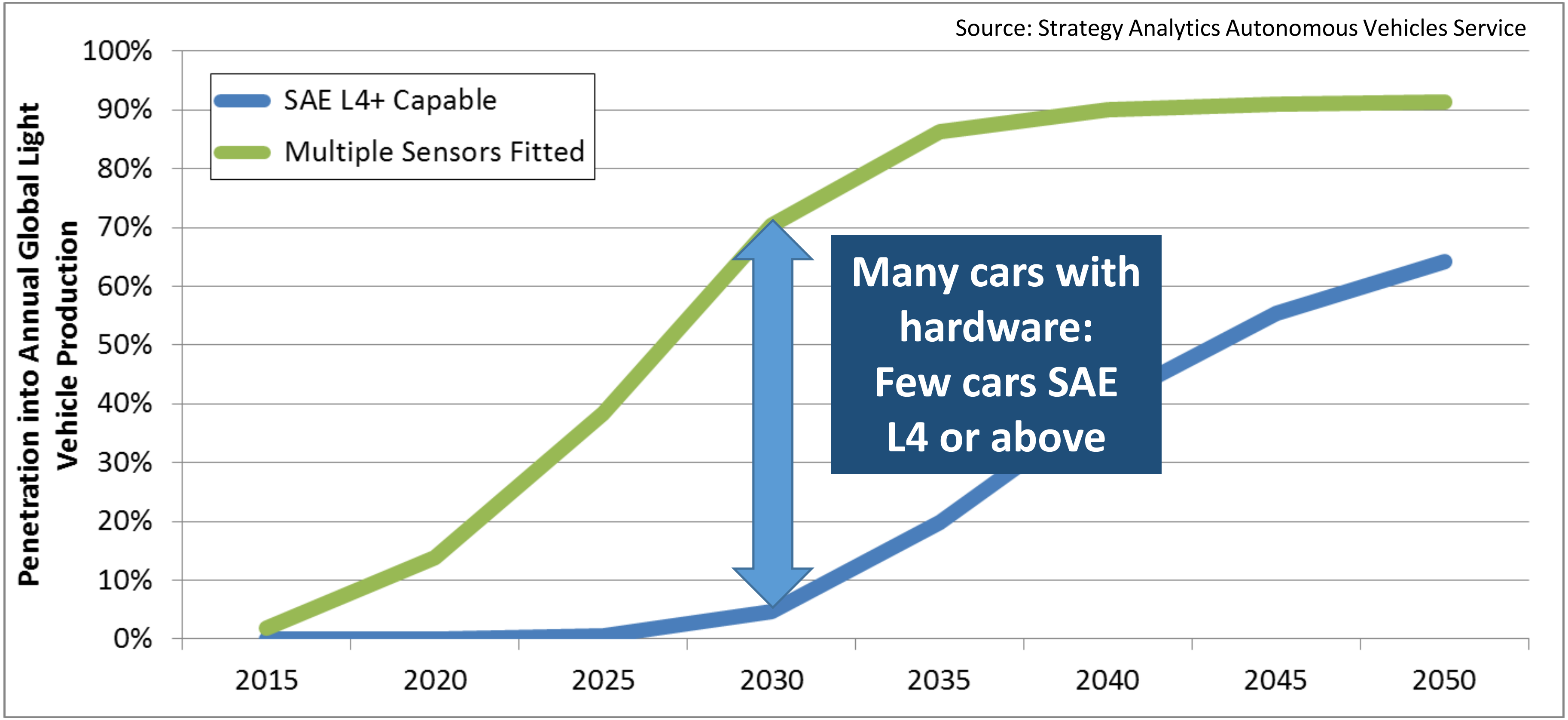
- LIDAR, RADAR
- Cameras
- Contextual awareness with the objective of collision avoidance



…most of these systems have COMPLEX software…

Source: Infotainment & Telematics Service

AUTONOMOUS IS A SOFTWARE PROBLEM



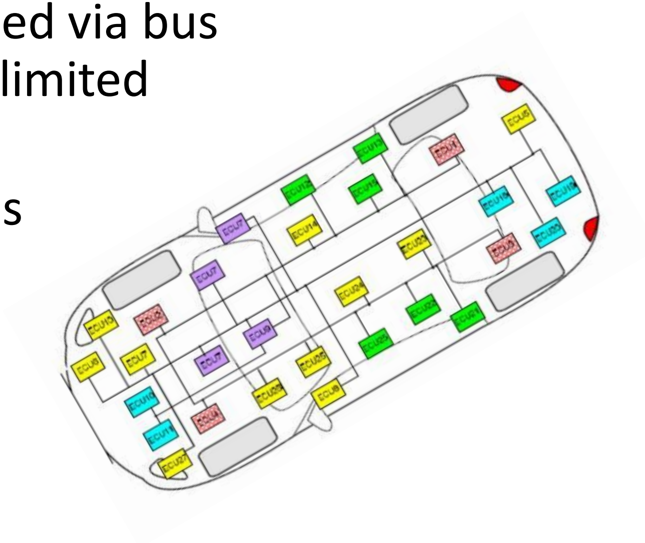
Source: Strategy Analytics Autonomous Vehicles Service

Many cars with hardware: Few cars SAE L4 or above

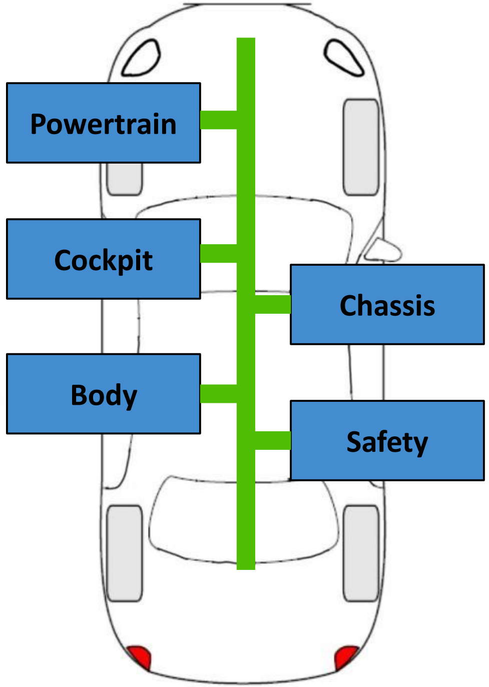
ETHERNET AS BACKBONE?

- Today
  - High Number of ECUs each typically performing a single function
  - ECUs connected via bus systems with limited bandwidth
  - Security issues

  with CAN bus
  - COMPLEX!

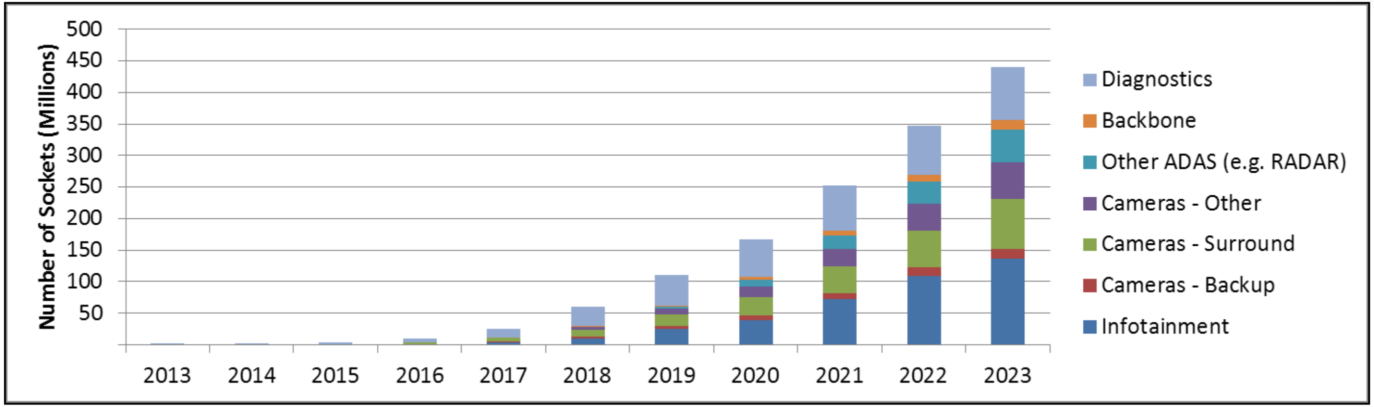


- Tomorrow?



STRATEGY ANALYTICS

ETHERNET AS BACKBONE?



Assumptions:

- **~60%** of global production in 2020 to feature Ethernet Diagnostics Port
- **~10 %** of Backup cameras to be Ethernet in 2020
- **~30%** of surround view systems to be Ethernet in 2020
- **~25%** of other cameras (e.g. front for LDWS etc.) to be Ethernet in 2020
- **~10%** of RADARs for be Ethernet in 2020
- **~20%** of premium audio & **5%** of mid-range audio to be Ethernet in 2020

BMW plus one other to start using Ethernet as backbone by 2020 – BMW in lead & other only just emerging

AUTOMOTIVE ETHERNET MARKET ISSUES

STRATEGY ANALYTICS

1. Timing: Exact timings of mass-market demand **still unclear** with many still "sitting on the fence" as to exactly what they will adopt and when

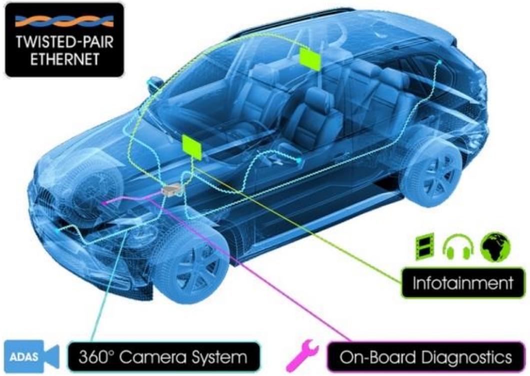
- CAAGR of socket demand over 2015 to 2020 is around 100%
- Means that delay/advance of market by one year could halve/double demand from expected values!

2. Current Market: We have seen **less Ethernet adoption than was anticipated** for camera systems. Rapid move to HD-class cameras has "forced" OEMs to choose new technologies and many have chosen LVDS.

- HDBaseT (which can transport Ethernet traffic) also gaining support from GM, Delphi, Daimler – although momentum seems to have stalled?

3. Suppliers: Wider range of semiconductor solutions is STILL needed…

- Integration of PHY into other semiconductor devices will be highly important in achieving mass-market adoption
- Silicon prices were seen as hampering wider-scale adoption – but these are falling as more vendors enter market
- Announcements such as Marvell 88Q2112 and Broadcom BCM8953x will help



Cyber Security – 2 Major challenges for Auto Industry:

1. Securing future vehicles
2. Securing the fleet of vehicles driving on roads today

- **Achieving 1** : Change to Auto industry culture, training, automotive network architecture design, and willingness to cooperate

  → A range of technical solutions exist and are actively being investigated and developed

- **Achieving 2** : **Is very difficult** and existing "bolt-on" methods will result in less-than-adequate security (e.g. adding intrusion detection/protection software)

Source: Infotainment & Telematics Service

VEHICLE CYBER SECURITY ‘ATTACK’ POINTS

- **Attack Surfaces:** Cellular, Wi-Fi, BT, DSRC, RKE, TPMS, USB, OBD II port, etc.
- **Interaction:** Each node can be secure in itself but is it secure when connected to the rest of the vehicle?
- **Many ECU’s:** (~50 to 100) ECUs and related processors to secure
- **CAN Protocol:** Was not designed with security in mind (no message or ECU authentication, low bandwidth, etc.)
- **Security testing:** Happening too far into production process to be effective
- **“Black box” problem:** Suppliers won’t share code due to interest in protecting IP
- **Security perception issue:** Security isn’t perceived as valuable until after a vehicle has been hacked
- **Updates:** Cannot rely on “always on” connectivity
- **Safety:** Often requires a vehicle be parked during an update
- **Auto industry security training/education:** Perceived to be not as sophisticated as in other sectors nor as much of a priority

Cannot certify security

Source: Infotainment & Telematics Service

VEHICLE CYBER SECURITY CHALLENGES AND THREATS

Challenges	Overview
Autonomous Driving	Relies on connectivity and requires significant computing power to sense and perceive all manner of obstacles and driving conditions. Connectivity to control systems, safety.
Wireless Connections	More attack surfaces from multiple connections such as cellular, Wi-Fi, Bluetooth, and DSRC will grow considerably
Brought-in Devices	Smartphones, tablets, OBD dongles can be used to connect/tether the car to networks.

Threats	Overview
Connected Infrastructure	Traffic signals, ramp meters, roadside sensors, and dynamic message signs.
Remote Monitoring & Control	Reduces maintenance or operation costs and enables new business models (i.e. car sharing), adds security challenges
Internet Companies	Working with the automotive industry for design, R&D and manufacturing. Their competitive advantage of fast iteration and "fix-it later" mentality may cause security issues.
Over-the-Air Updates	Enables fast-fixes for bugs and reduces vulnerability by keeping legacy systems up-to-date, also increases the "attack surface"

Source: Infotainment & Telematics Service

VEHICLE CYBER SECURITY ORGANIZATIONS & STANDARDS ACTIVITY

Organizations	Recent Activities	Links
SAE	SAE has formally released its guidebook for securing automotive cyber physical systems.	http://standards.sae.org/j3061_201601/
ENISA	The EU's ENISA has launched a study on automotive cyber security to develop policies and provide a list of resources. The EU has also released rules for network and information system security.	https://www.enisa.europa.eu/news/enisa-news/securing-smart-cars-join-enisa-study-and-workshop http://www.hldataprotection.com/2016/07/articles/international-eu-privacy/european-unions-cybersecurity-nis-directive-adopted/
U.S. DOT/NHTSA	The U.S. DOT/NHTSA has released basic guidelines for automotive cyber security.	http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016
Auto ISAC	The Auto ISAC has released its own set of guidelines.	http://www.totaltele.com/view.aspx?ID=495278#sthash.S32doAMK.dpbs

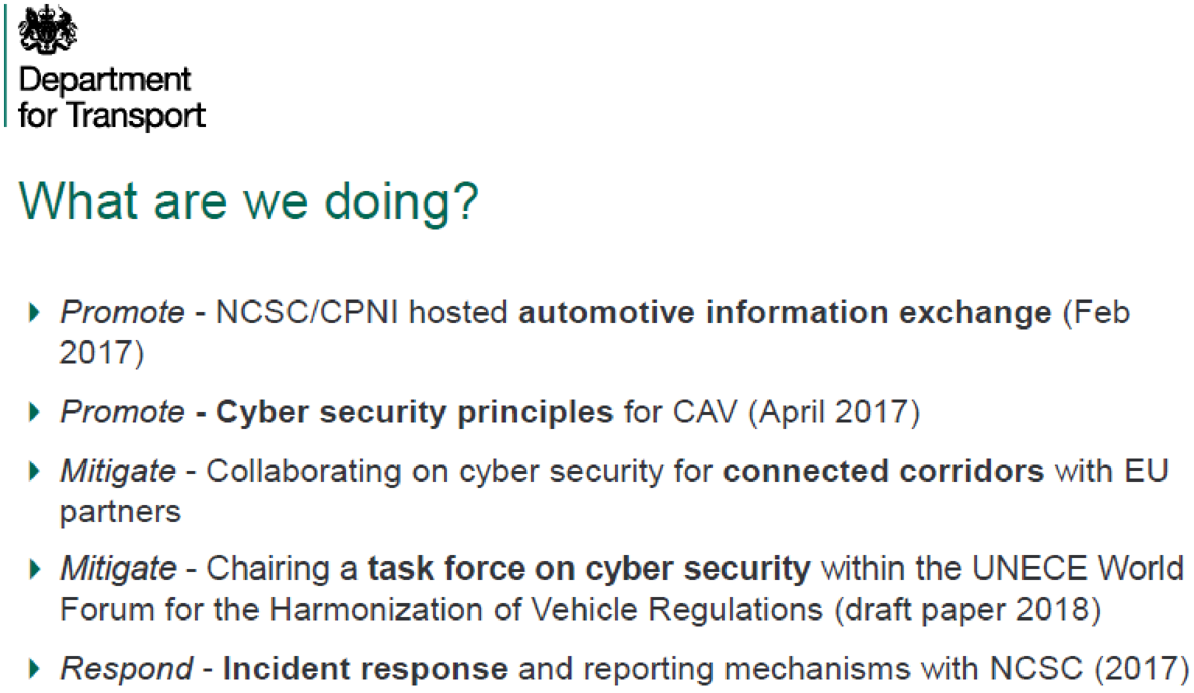
Source: Infotainment & Telematics Service

VEHICLE CYBER SECURITY REGIONAL LEGISLATION

Region	Overview
U.S.	• NHTSA – The National Highway Traffic Safety Administration continues to produce guidelines and has thus far issued four reports on this subject. • NIST – National Institute of Standards and Technology is developing a voluntary cyber security framework for reducing risks to infrastructure (including vehicles and transportation systems). • SPY CAR Act – Proposed by Senators Market and Blumenthal in 2015. Rulemaking set during 2016, early 2017. The Security and Privacy in Your Car (SPY) Act would set federal cyber security standards for vehicles. • U.S. Copyright Office – A change in the Digital Millennium Copyright Act (DMCA) now allows vehicle owners to legally access the software in their vehicles.
E.U.	• ENISA – The European Union Agency for Network and Information Security is forming a group to address automotive cyber security guidelines and plans to suggest draft legislation in 2017.
Japan	• IAC - Internal Affairs and Communications Ministry has created automotive cyber security guidelines designed to work with Intelligent Transportation Systems in Japan.

Source: Infotainment & Telematics Service

DEPARTMENT FOR TRANSPORT

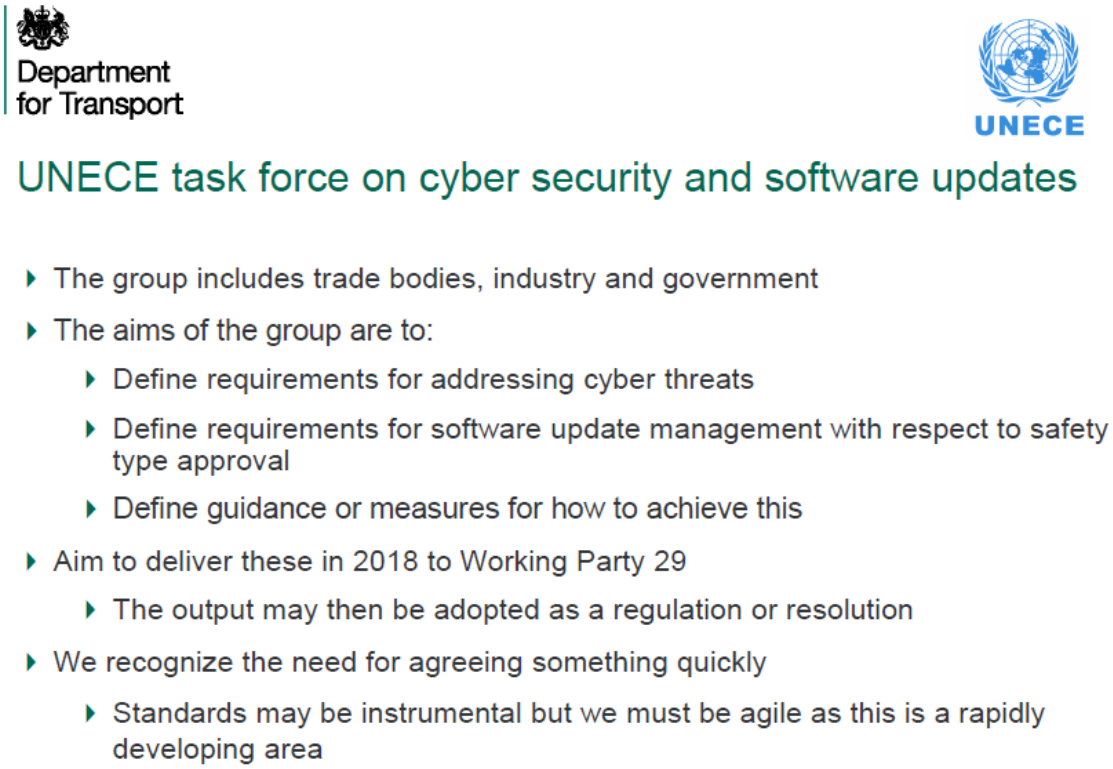


Department for Transport

What are we doing?

- *Promote* - NCSC/CPNI hosted **automotive information exchange** (Feb 2017)
- *Promote* **- Cyber security principles** for CAV (April 2017)
- *Mitigate* - Collaborating on cyber security for **connected corridors** with EU partners
- *Mitigate* - Chairing a **task force on cyber security** within the UNECE World Forum for the Harmonization of Vehicle Regulations (draft paper 2018)
- *Respond* - **Incident response** and reporting mechanisms with NCSC (2017)

WORKING WITH UNECE



Department for Transport

UNECE

UNECE task force on cyber security and software updates

- The group includes trade bodies, industry and government
- The aims of the group are to:
  - Define requirements for addressing cyber threats
  - Define requirements for software update management with respect to safety type approval
  - Define guidance or measures for how to achieve this
- Aim to deliver these in 2018 to Working Party 29
  - The output may then be adopted as a regulation or resolution
- We recognize the need for agreeing something quickly
  - Standards may be instrumental but we must be agile as this is a rapidly developing area

VEHICLE CYBER SECURITY SOLUTION PROVIDERS

Example Cyber Security Solution Providers

Intrusion Detection/Protection

Argus Cyber Security

Irdeto

Karamba Cyber Security

Symantec

TowerSec (owned by Harman)

Firewalls, White Listing, and Access Control

Arilou (owned by NNG)

Harman

Runsafe Security (aftermarket)

Symantec

VisualThreat

Digital Certificate Management

Certicom (owned by Blackberry)

Symantec

Hardware Security Solutions and Related Support

Elektrobit

Escrypt (owned by Bosch)

Infineon

Intrinsic-ID

Qualcomm/NXP

Rambus

Texas Instruments

OTA Update Security and PKI Solutions

Abalta

Arynga (owned by Wind River/Intel)

Certicom/QNX (owned by Blackberry)

Escrypt (owned by Bosch)

Harman

Movimento

Rambus

In-Vehicle Network Security

Harman

Irdeto

Security Innovation

Symantec

Trillium

Testing Solutions

Synopsys

Virtualization Solutions

Green Hills

Harman (using RedBend hypervisor)

QNX (owned by Blackberry)

VMWare

Source: Infotainment & Telematics Service

THE SECURITY CHALLENGE

- Keyfob, OBDII, Dealerships + Denial (video)
- Limited talent pool
- Security source of cost/liability

"Mystery Device" Can Unlock and Start Your Vehicle

https://www.nicb.com/newsroom/news-releases/nicb-reveals-mystery-device-that-opens-and-starts-vehicles

AUDI

TOYOTA

DETECT, AND THEN WHAT?

- Suppliers to the auto industry are bringing detection and prevention systems to the market
- Will take years to implement and deploy
- No strategy for response/notification protocols – consumers, government regulators, law enforcement

VEHICLE AUTONOMY, 5G CHANGES ALL

- Remote access/control
- Inter-vehicle communication
- What does it mean?
- How will consumers, criminals react?

MORE DATA FLOWING TO/FROM CARS

- More data to and from vehicles!
  - **BUT!** Linked to wider trends than just automated driving: FOTA/SOTA; CRM/VRM; 5G for V2V/V2X etc.
  - The automated car may be gathering Gigabytes / km – but data to the cloud will be more like kilobytes / km
  - Around **90 million** active automotive data subscriptions in 2018, vs. **4.7 billion** active mobile device data subscriptions
- Key challenge - **SECURITY**

SUMMARY & RECOMMENDATIONS

SUMMARY & RECOMMENDATIONS (1/2)

- Car ownership patterns **will evolve**. The imminent death of car ownership is overstated, but shared cars will change traditional understanding
- Car companies are entering the **fleet and B2C** business space –altering the distribution channel roles
- **Regulators and legislators** are becoming increasingly interested in transportation generally and cars particularly

SUMMARY & RECOMMENDATIONS (2/2)

- **Mobile commerce** will play an increasing role – tolls, fuel, parking, content, services – more opportunity for criminals
- V2X creates **new challenges** for car companies to interact with government/municipal authorities and infrastructure companies – ultimately exposes cars to mass attacks
- **Cybersecurity** will remain a concern for the foreseeable future – can never certify vehicle security – industry response protocols/definition remains in flux – problem will only get worse – connectivity = opportunity for law enforcement