ACEA European Automobile Manufacturers Association

Cooperative, Connected and Automated Mobility

QUO VADIS ?
CHALLENGES FOR THE AUTOMOTIVE INDUSTRY

Joost Vantomme
Smart Mobility Director

PZPM CONFERENCE
WARSAW, 26 FEBRUARY 2018

AGENDA

1. Context of Cooperative, Connected and Automated Mobility
2. Data Economy and access to data
3. Cooperative Intelligent Transport Systems (C-ITS)
4. Data Protection and Privacy, Telecoms Code
5. Cyber security

ACEA European Automobile Manufacturers Association

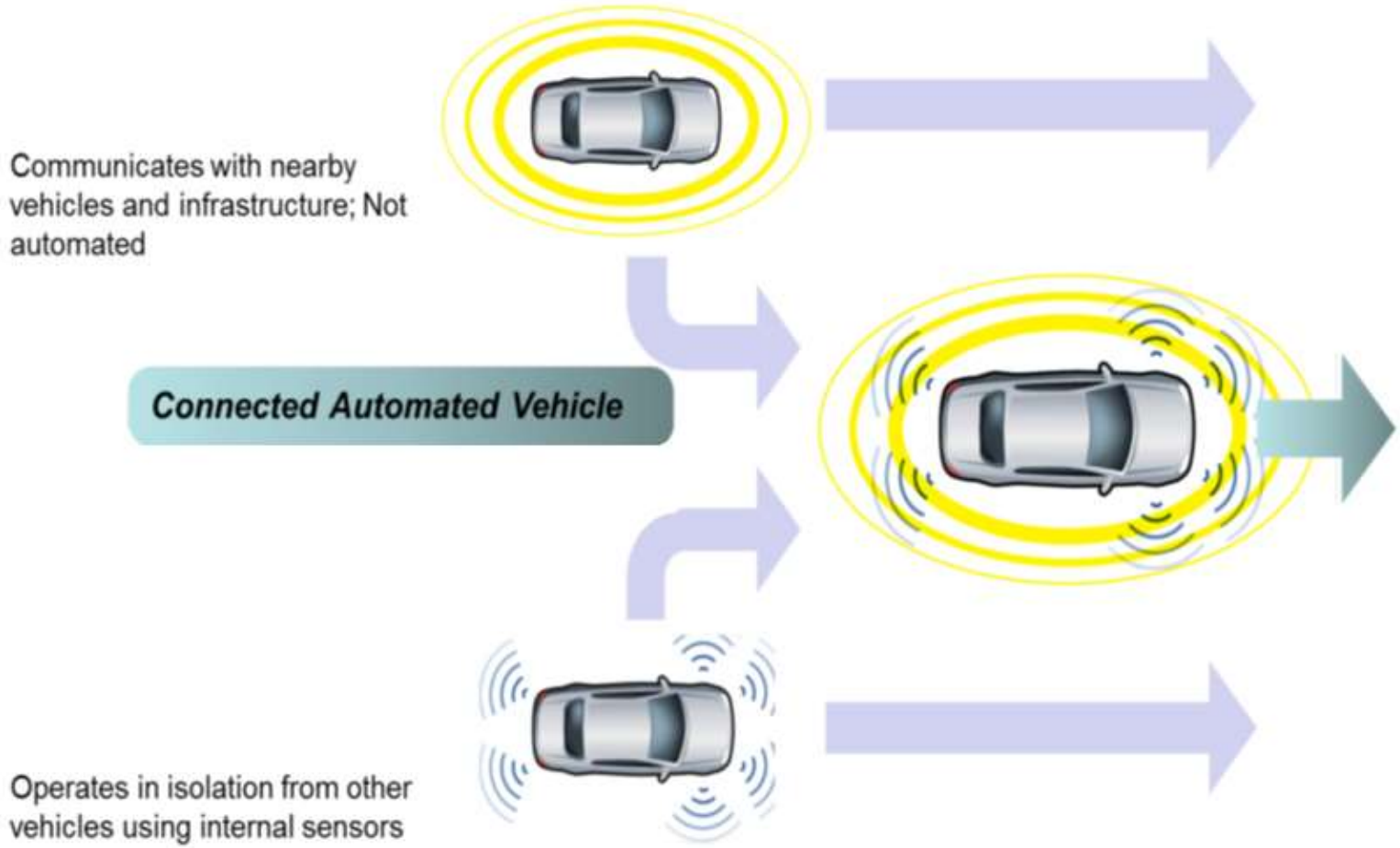
1. Context of Cooperative, Connected and Automated Mobility

CONNECTIVITY VS AUTOMATION

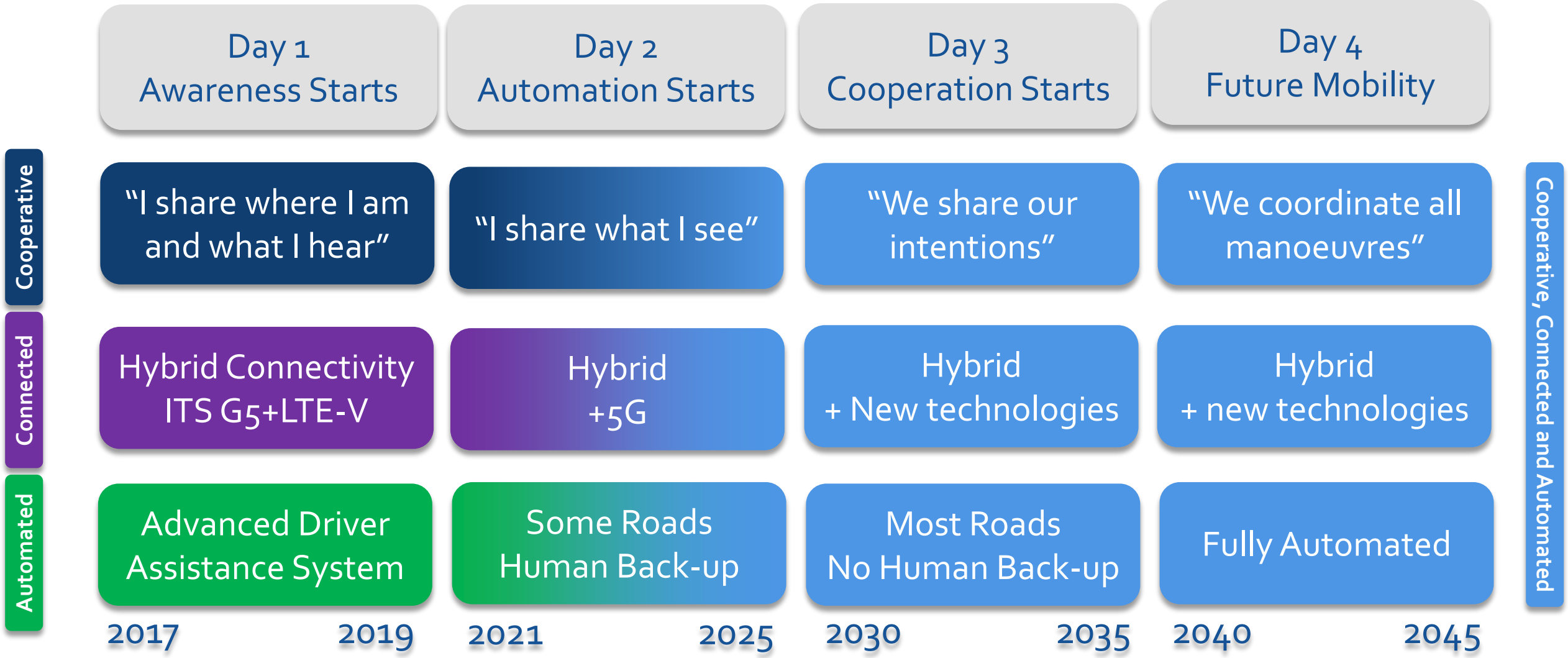
Connected vehicle

- Vehicle-to-vehicle
- Vehicle-to-infrastructure

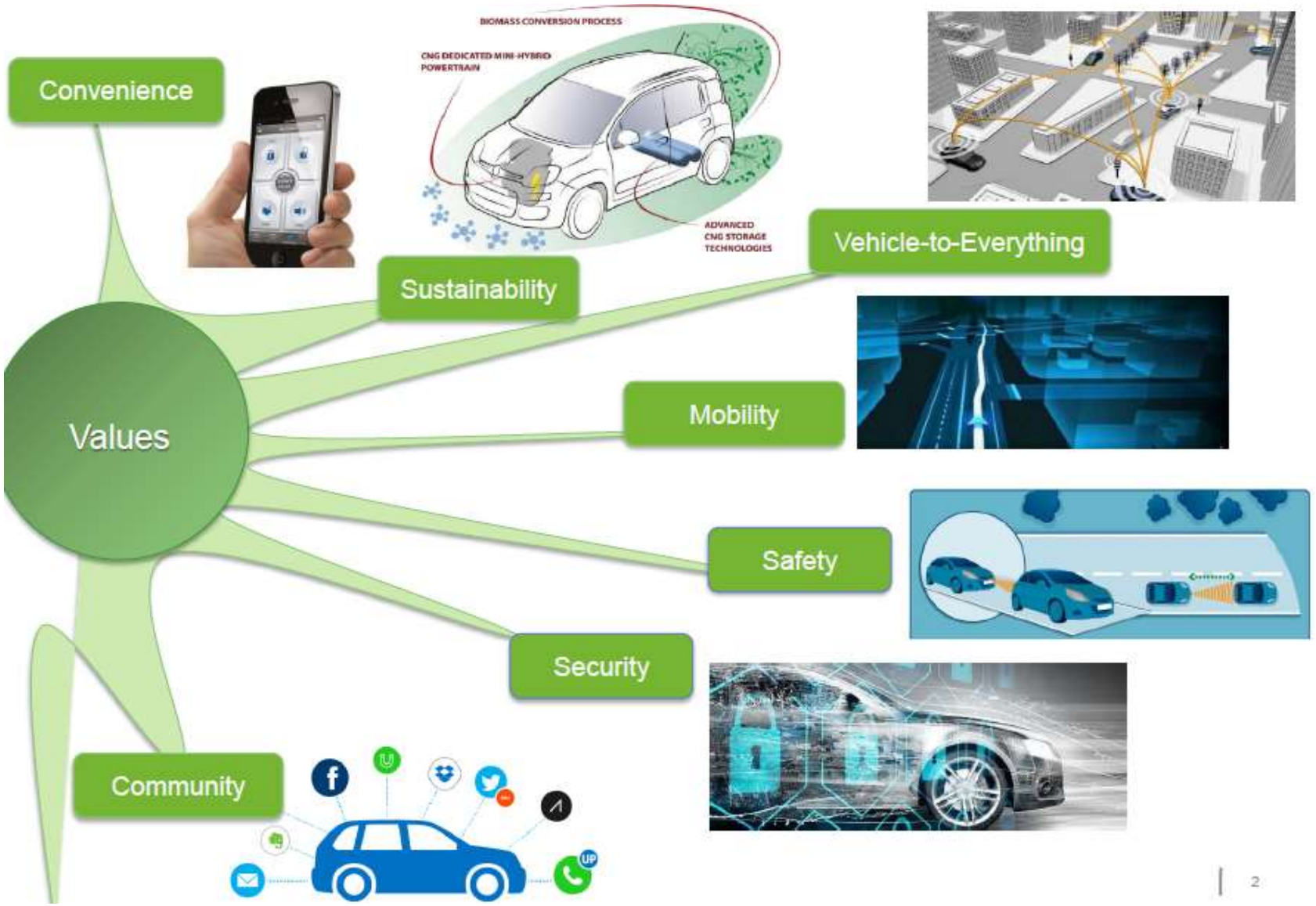
Automated vehicle



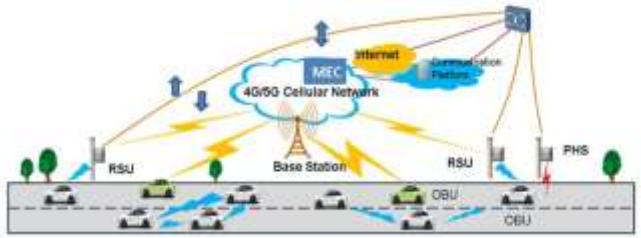
TOWARDS COOPERATIVE, CONNECTED AND AUTOMATED MOBILITY



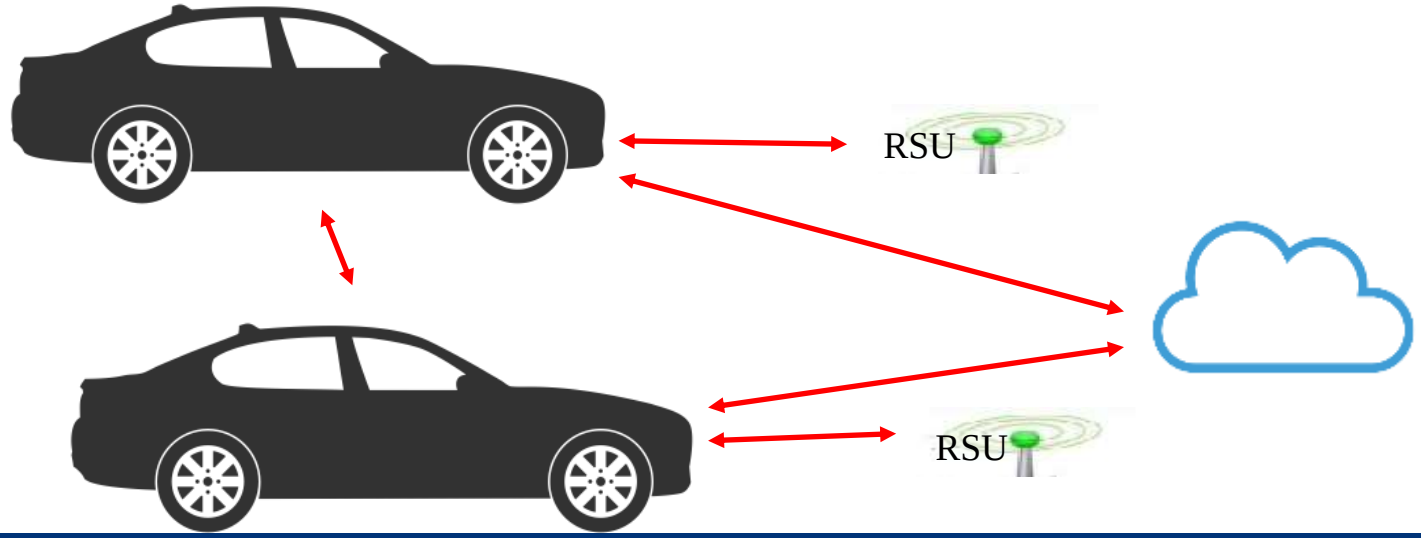
CONNECTIVITY SERVICES



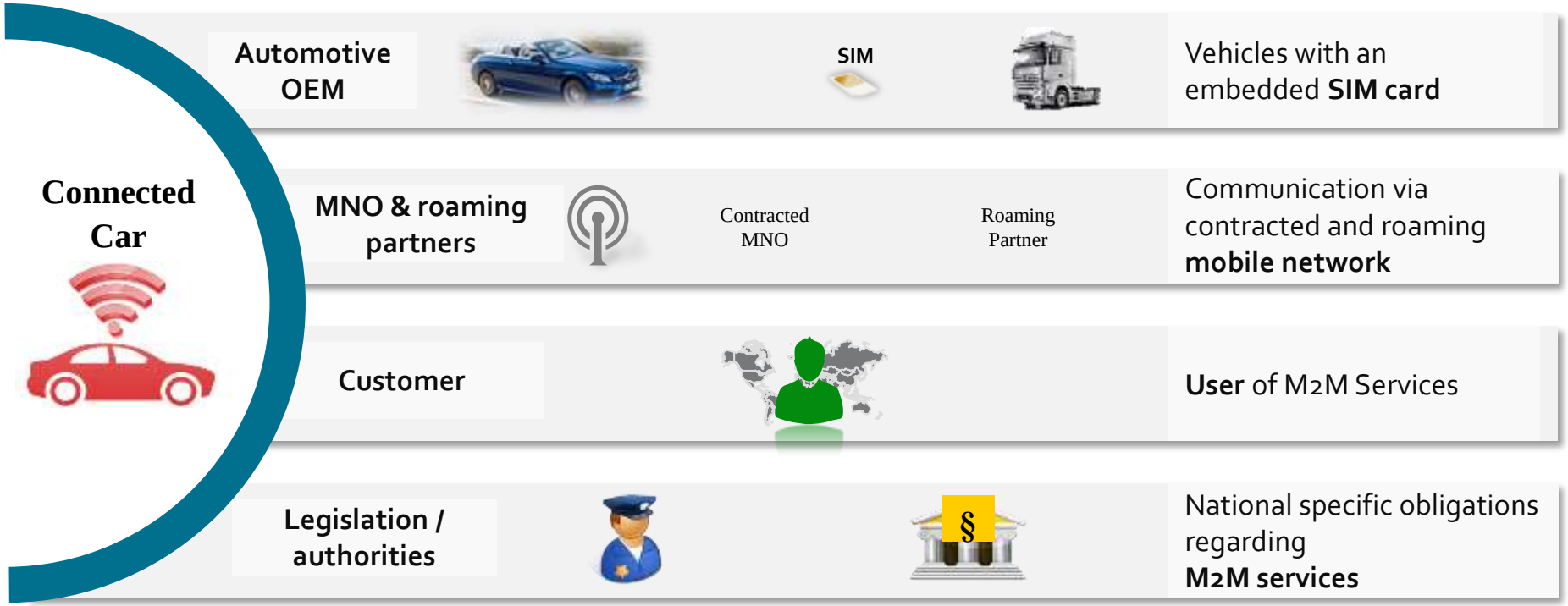
CONNECTIVITY NEEDS



- Attribution of the right messages using the right communication channels according to the requested performances
- The combination of different short- and long-range communication systems, mobile edge computing and cloud applications, should increase the reliability and safety
- V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), V2N (vehicle to network/cloud)



EXAMPLES (SIM BASED SERVICES)



SHORT RANGE TECHNOLOGY

- Communication range of up to 1000 meters depending on scenario
- Vehicles communicate directly with each other in *ad hoc* mode
- No communication infrastructure is used (no coverage by access points or base stations)
- Called vehicle-to-vehicle communication, V2V
- Smart infrastructure can also be equipped with short-range wireless communication (traffic lights, speed signs, etc), vehicle-to-infrastructure (V2I)
- Smart infrastructure and vehicles are peers in the network, no one is governing the other one
- Use cases : cooperative ITS services, safety related applications, truck platooning, …

SHORT RANGE TECHNOLOGY

ITS G 5

Dedicated ad hoc short range communication

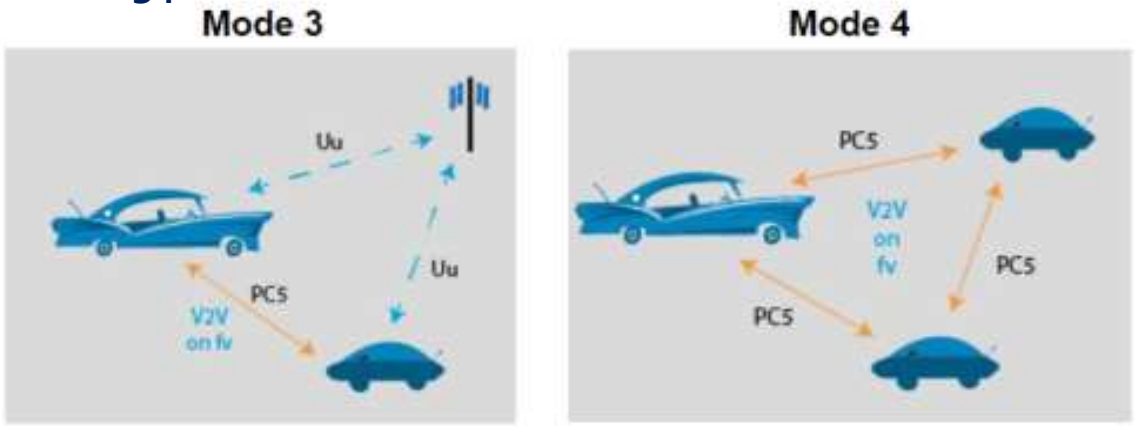
Operates in European ITS frequency bands dedicated to ITS for safety related applications in the frequency range 5,875 GHz to 5,905 GHz.

EC proposes to widen the range with an additional 20 MHz.

In deployment mode by some road authorities and OEM's

LTE-V

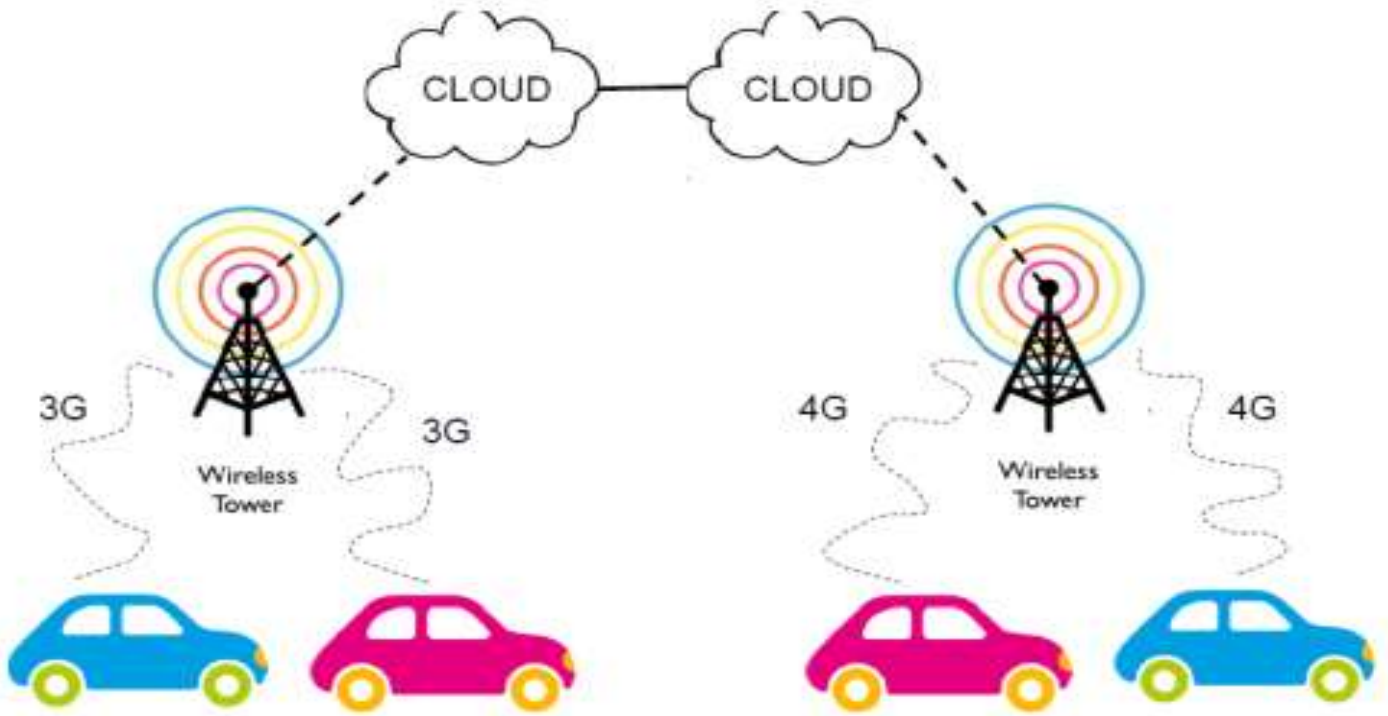
Dedicated ad hoc short range communication
Cellular network (unmanaged and managed mode)
Testing phase



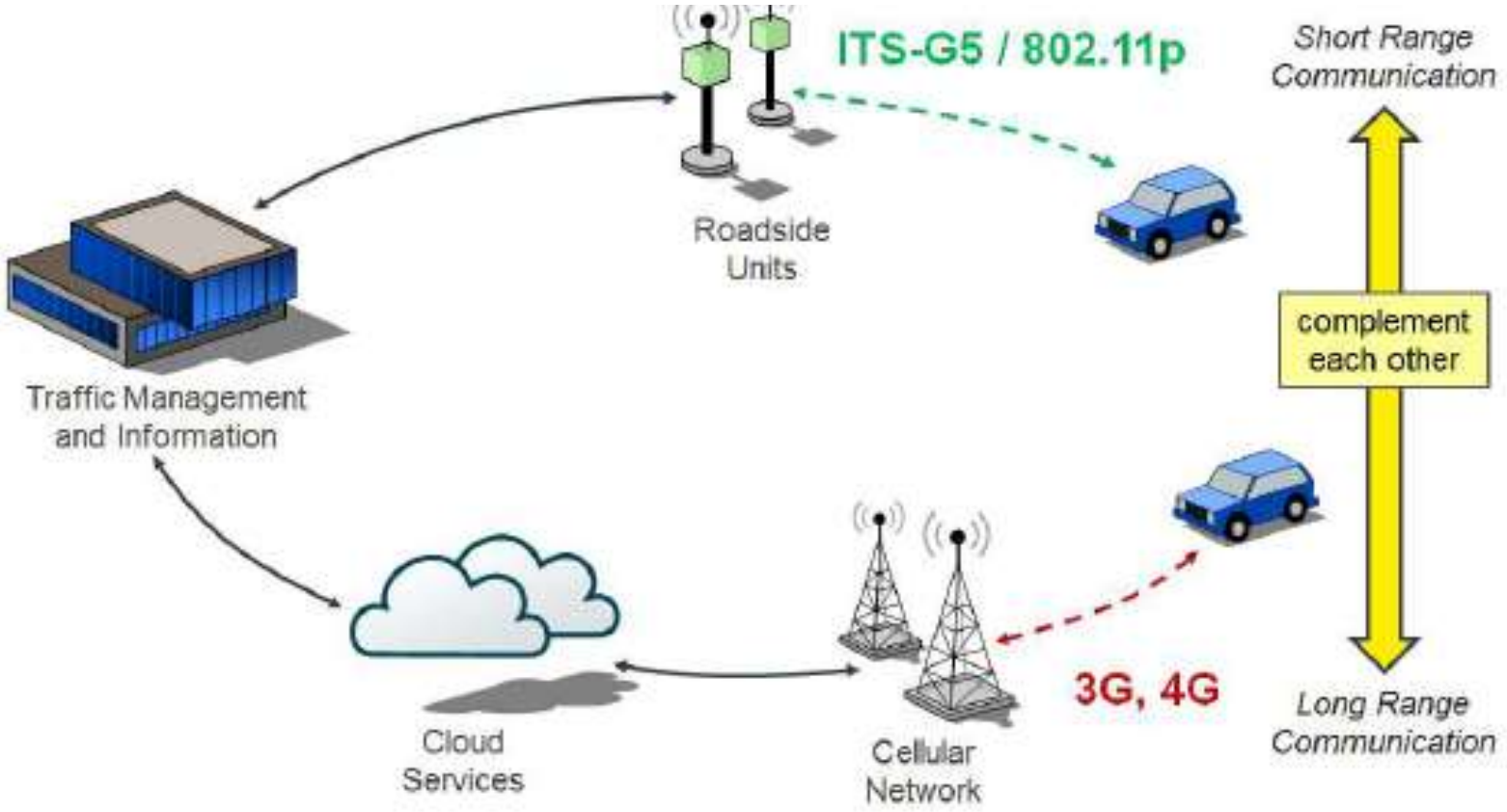
SPECTRUM

ETSI and CEPT tasked to study interference issues in the 5,9 GHz frequency band

LONG RANGE CELLULAR TECHNOLOGY



CONNECTIVITY POSSIBILITIES



M2M services through :
- **ITS G5**
- **LTE-V (cellular C-V2X)**

Long range cellular (cloud based)

M2M: dedicated 30 MHz spectrum band for safety purposes in the 5,9 GHz range

Cooperative services : need to be able to "talk to each other"

Source : C-ROADS,position paper on the usage of the 5,9 GHz band
https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/C-Roads_Position_paper_on_59GHz_final.pdf

REGULATORY AND POLICY CHALLENGES

Vehicle meets Infrastructures

VEHICLE

- Privacy & data protection
- Third-party access to data
- Certification of software updates & type approval
- Security and safety regulations
- Permissible tasks/safety in Levels 3, 4 and 5

PHYSICAL INFRA

- New road design
- Digitisation of physical infrastructure
- Testing on public roads
- Road safety
- City planning

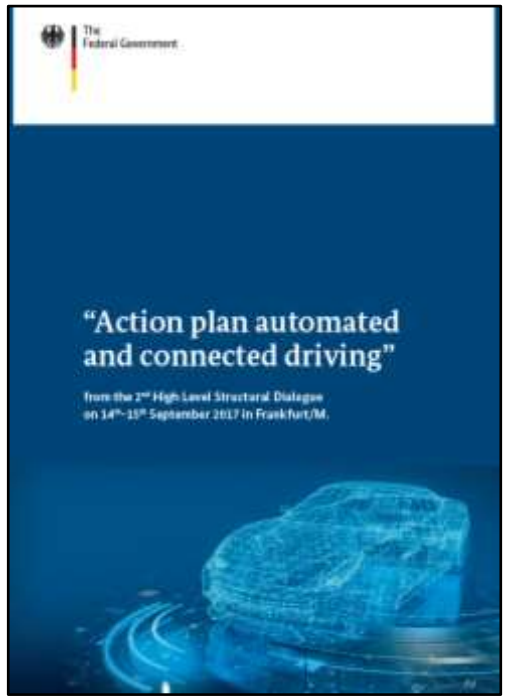
DIGITAL INFRA

- Technology mix
- 5G deployment
- Spectrum Low latency
- Ubiquity
- Guaranteed quality of service
- Seamless across borders

EU ROADMAP ON CONNECTIVITY & AUTOMATION

FOLLOW-UP ON DECLARATION OF AMSTERDAM

- **Declaration of April 2016 (Dutch presidency)**
- **Follow-up via High Level Structural Dialogue on CCAM: Amsterdam, 15 Feb 2017 - Frankfurt, 14/15 Sept 2017 - Gothenburg, June 2018**
- **Letter of Intent, Rome March 2017 -> Digital Day Brussels, 10 April 2018**



NEW CORRIDORS

5 new corridors for CCAM:

- Metz-Merzig-Luxembourg
- Rotterdam-Antwerp-Eindhoven
- Porto-Vigo and Merida-Evora (corridor Lisbon – Madrid)
- The E8 'Aurora Borealis' corridor between Tromsø (Norway) and Oulu (Finland)
- The 'Nordic Way' between Sweden, Finland and Norway

Press release COM: https://ec.europa.eu/digital-single-market/en/news/cooperative-connected-and-automated-mobility-stepping-efforts-frankfurt

EATA

- European Automotive and Telecoms Alliance
- Originated via Round Table approach from the EC
- CONCORDA proposal awarded (CEF funding)
- Hybrid technology
- Various use cases in 5 MS (BE, DE, ES, FR, NL)
- Evolution towards cross-border
- Dialogue with EC every 6 months, combined with High Level Dialogue Transport Ministers

ACEA European Automobile Manufacturers Association

2. Data Economy

BUILDING A EUROPEAN DATA ECONOMY

EC Communication of 10 January 2017

- **Communication "Building a European Data Economy"**
  - Data localisation restriction
  - Data access, re-use and transfer
  - Liability
  - Portability, interoperability and standards
- **Public Consultation**
  - Purpose: To help shape the Commission's policy agenda
  - Report available online
- **Reference to the Automotive Sector**
  - CCAM could be considered as testbed for data economy issues
  - Trial to be carried out it partnership with stakeholders

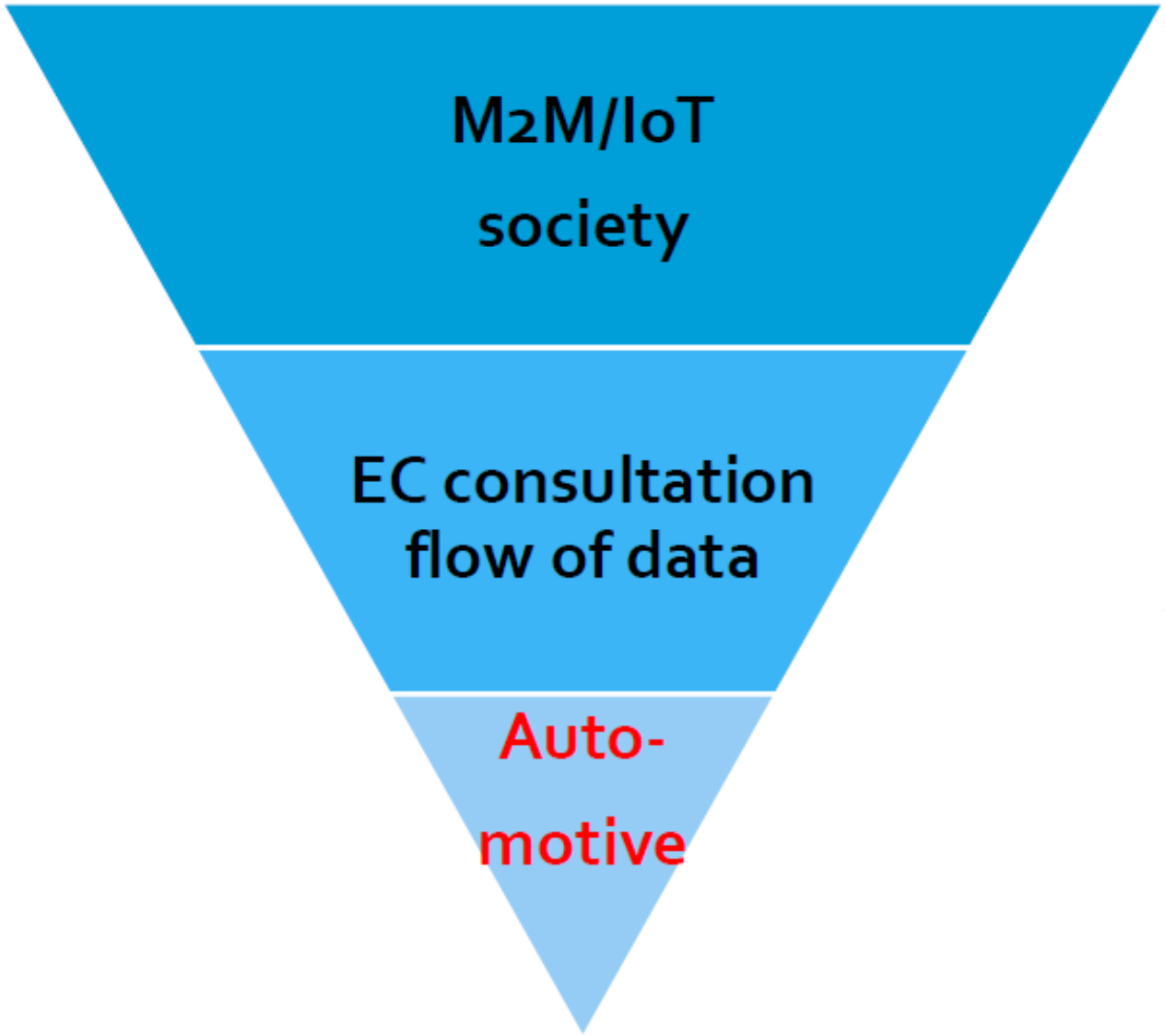
BUILDING A EUROPEAN DATA ECONOMY

Expectations following the consultation

EC initiatives following this consultation:

- **Sept 2017**: **Proposal for Regulation on a framework for the free flow of non-personal data in the EU**
- **April 2018**:
  - EC will Launch an initiative on accessibility and re-use of **public and publicly funded data**
  - EC will further explore the issue of **privately held data of public interest (reverse PSI)**
- Commission intends to continue to **assess the need for action** concerning emerging data issues, notably regarding data access rights.

LEVEL PLAYING FIELD WITH OTHER SECTORS ?



- Unregulated
- Dialogue
- Across industries

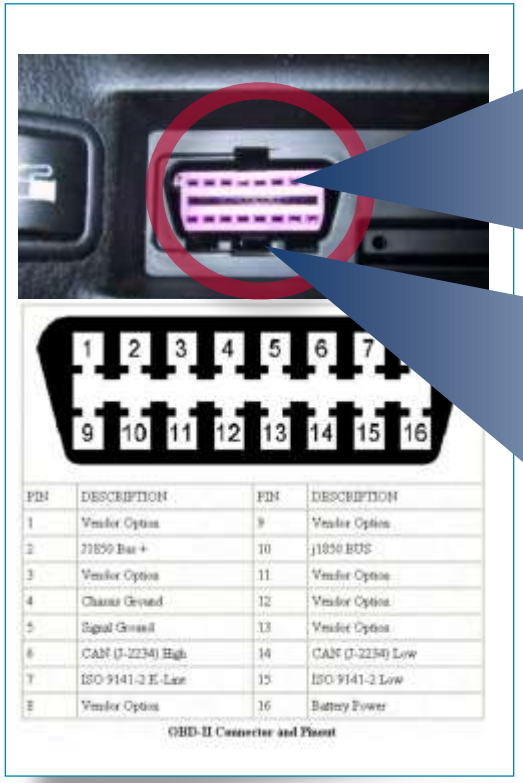
-> Regulated

- eCall, RMI, …

VEHICLE DATA: SAFE AND SECURE ACCESS

ACCESS TO VEHICLE DATA

OBD Interface



PIN	DESCRIPTION	PIN	DESCRIPTION
1	Vendor Option	9	Vendor Option
2	J1850 Bus +	10	j1850 BUS
3	Vendor Option	11	Vendor Option
4	Chassis Ground	12	Vendor Option
5	Signal Ground	13	Vendor Option
6	CAN (J-2234) High	14	CAN (J-2234) Low
7	ISO 9141-2 K-Line	15	ISO 9141-2 Low
8	Vendor Option	16	Battery Power

OBD-II Connector and Pinout

Diagnosis and maintenance

Open gate for hacking

- OBD interface is a well defined interface for diagnosis and maintenance in a defined service station
- Using the OBD interface with a connected dongle can cause serious security/safety problems

A CAR IS NOT A SMARTPHONE

SMARTPHONE

- Communications platform
- Serves communications, entertainment and/or business purposes
- Can easily be rebooted at any point, without any safety implications
- The average smart phone has a lifespan of 2 to 3 years, often seen as a disposable device
- Designed like any other consumer device, does not contain any safety-critical systems

CONNECTED CAR

- Means of transport
- Brings people or goods safely from one place to another
- Cannot be rebooted if a problem occurs while driving
- A motor vehicle has a lifetime of at least 8 to 10 years, so its hardware needs to be resilient and stable
- Designed to comply with road safety regulations and product safety standards to protect lives

THE SIX INTERFACES OF A FULLY CONNECTED VEHICLE

E-Call interface

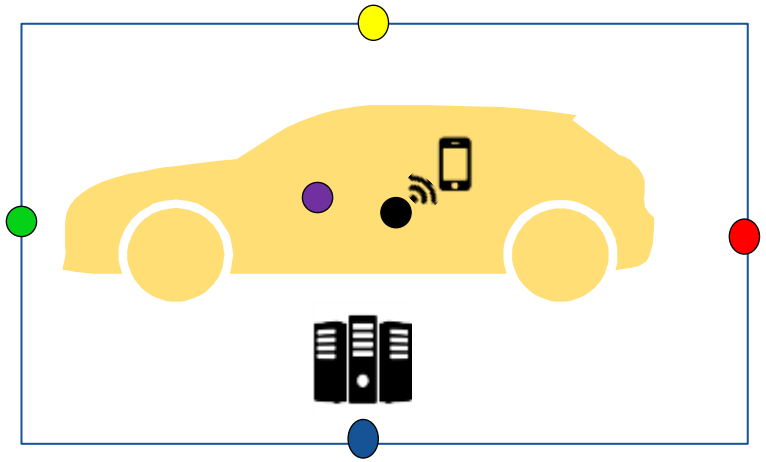
Far field over the air communication used to send regulated data from a vehicle involved in a road traffic accident

Charging interface

Communication with charging station to enable the charging of electric vehicles

Infotainment interface

Near field over the air communication between a customer mobile device and the vehicle infotainment system e.g. hands free telephony, terminal mode to vehicle HMI



Ad hoc interface

Real time near field over the air communication between vehicles or a vehicle and the traffic infrastructure for traffic safety / efficiency use cases

- Point to point
- Low latency (real-time)
- Safety critical
- Low bandwidth

On Board Diagnostics interface (OBD)

Wired communication with test / inspection equipment. Used by trained technicians to gain access to regulated data for emissions, diagnosis, repair and maintenance purposes

Extended Vehicle server interface

Standardized server communication used to enable 3rd parties and neutral servers to access vehicle generated data and predefined in vehicle routines in a secure manner.

ISO 20077-1 "Extended Vehicle"

4 CATEGORIES OF DATA/USE CASES

1. "Public interest" data -> Reciprocity

Data relevant to traffic safety
(e.g. local hazard warning, ITS-related services)

2. Data triggered by the vehicle -> B2B

Services available across brands: non-differentiating vehicle data
(e.g. ambient temperature, traffic flows, road sign recognition, street parking)

3. Vehicle specific technical data -> N/A

Brand-specific services & component analysis/product improvement: link to suppliers, IP protected
(e.g. ECU monitoring, chassis sensor data)

4. Data triggered by driver -> Consent + B2B

Personalised services
(e.g. vehicle position, speed, insurance, fleet, roadside assistance, diagnostic)

ACEA POSITION ON ACCESS TO DATA

Conclusion

- **OEMs prepared to make data available, but only when the following principles are respected:**
  - **Safety, security, vehicle integrity and liability**
  - Customer choice (repair and maintenance, as well as mobility services)
  - Fair competition
  - Privacy and data protection
  - Interoperability (standardised approach, cfr ISO)
  - Return on investment
- **Direct access to data inside the vehicle poses a threat to: safety, security and integrity of the vehicle**
- **Dongles connected to an OBD interface pose a risk to the vehicle**
- **Focus on providing off-board access to data through Extended Vehicle model**

ACEA POSITION ON ACCESS TO DATA

Position Paper, Video and Website

https://goo.gl/6ZacfT

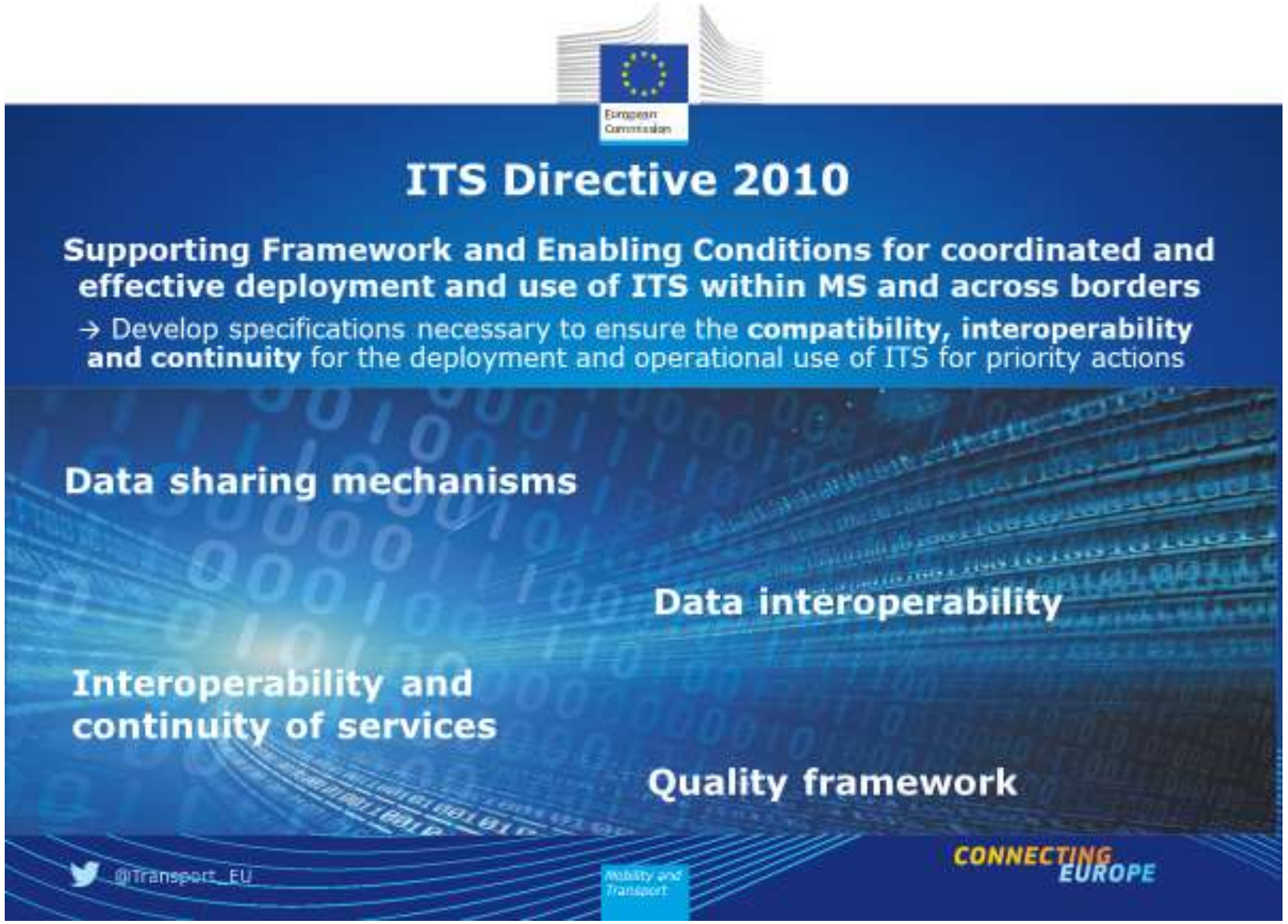
https://youtu.be/haS68vxB25g

http://cardatafacts.eu/

ACEA European Automobile Manufacturers Association

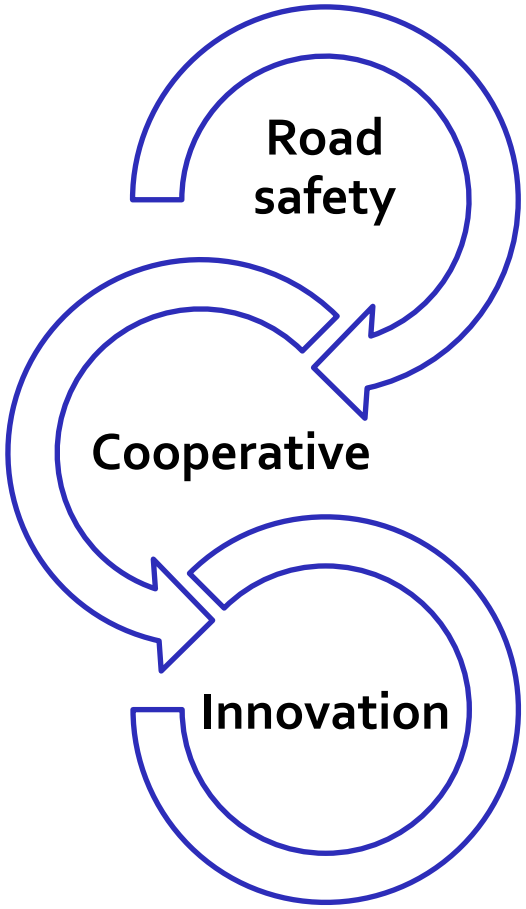
3. C-ITS

CONTEXT


European Commission
ITS Directive 2010
Supporting Framework and Enabling Conditions for coordinated and effective deployment and use of ITS within MS and across borders
→ Develop specifications necessary to ensure the compatibility, interoperability and continuity for the deployment and operational use of ITS for priority actions
Data sharing mechanisms
Data interoperability
Interoperability and continuity of services
Quality framework
@Transport_EU
Mobility and Transport
CONNECTING EUROPE

DELEGATED ACTS

OEM INVOLVEMENT IN ITS



- ✓ Various "ITS G5 initiatives" through pilots deployments such as ETPC (truck platooning), InterCor, Nordic Way, Scoop@F and other C-ROAD initiatives. Started through European projects 2006-2010 such as SAFESPOT, CVIS, COOPER, SCORE@F
- ✓ LTE-V and ITS G5 automotive trials in Germany (A9), via Concorda proposal
- ✓ Active participation of OEMs in C-ITS platform phases 1 & 2
- ✓ OEMs involved in CAR2CAR CC
- ✓ OEMs involved in EATA and 5GAA
- ✓ OEMs involved in the NHTSA V2V NPRM discussions and follow-up in the USA
- ✓ OEMs involved in 5,9 GHz spectrum discussion
- ✓ OEMs involved in the MS Data Task Force
- ✓ …

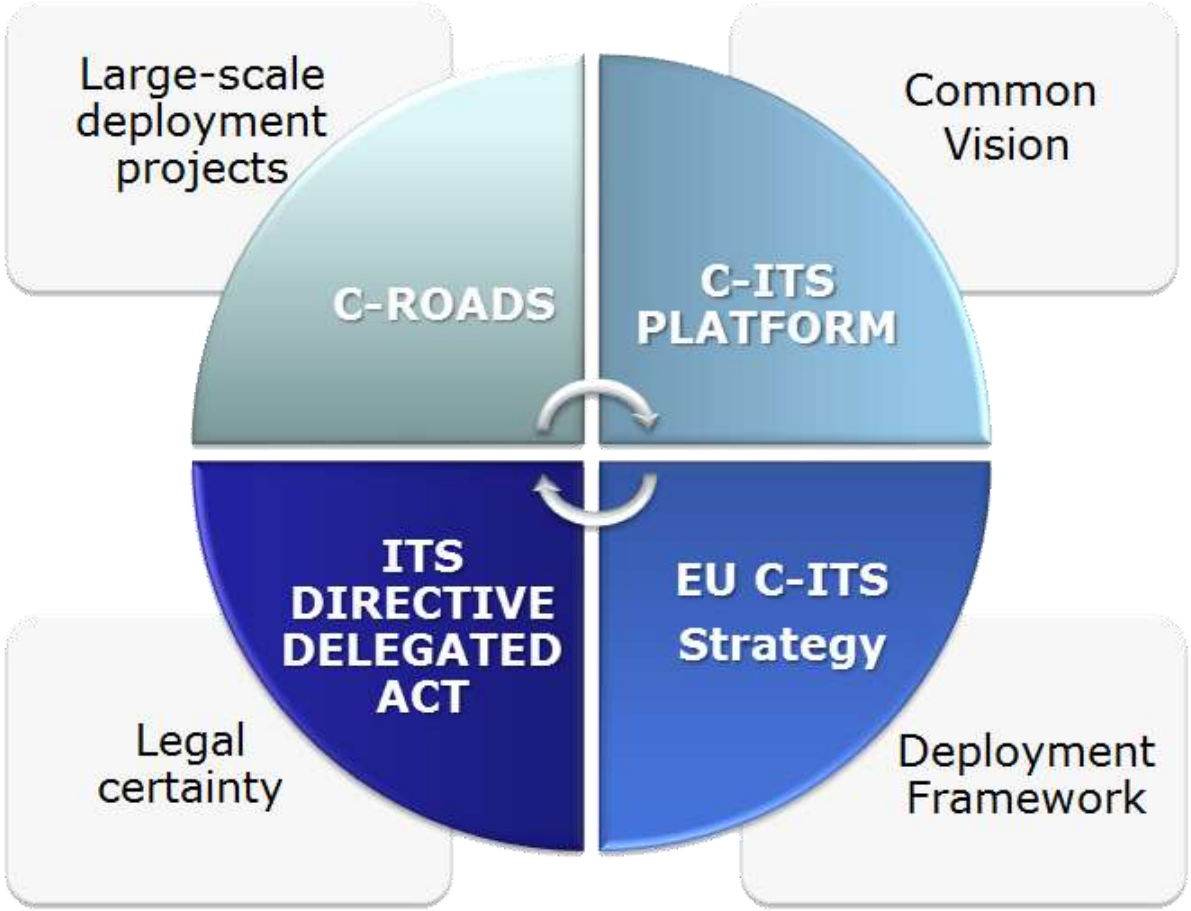
EC STRATEGY

EUROPEAN
COMMISSION

Brussels, 30.11.2016
COM(2016) 766 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility



EC STRATEGY

❑ C-ITS roll-out for V2V, V2I : target remains 2019

- ✓ Use cases on road safety (Day 1 services)
- ✓ Technology : hybrid approach. ITS G5 + LTE-V cellular

❑ C-ITS Platform final report phase 1 : Jan 2016 + phase 2 : 20 Sept 2017

- ✓ Security of V2V and V2I messages
- ✓ Data protection & privacy : unsolved issue -> candidate for delegated act
- ✓ Co-existence of hybrid communication technologies
- ✓ Automation in urban areas
- ✓ Requirements for physical and digital infrastructures
- ✓ Traffic management

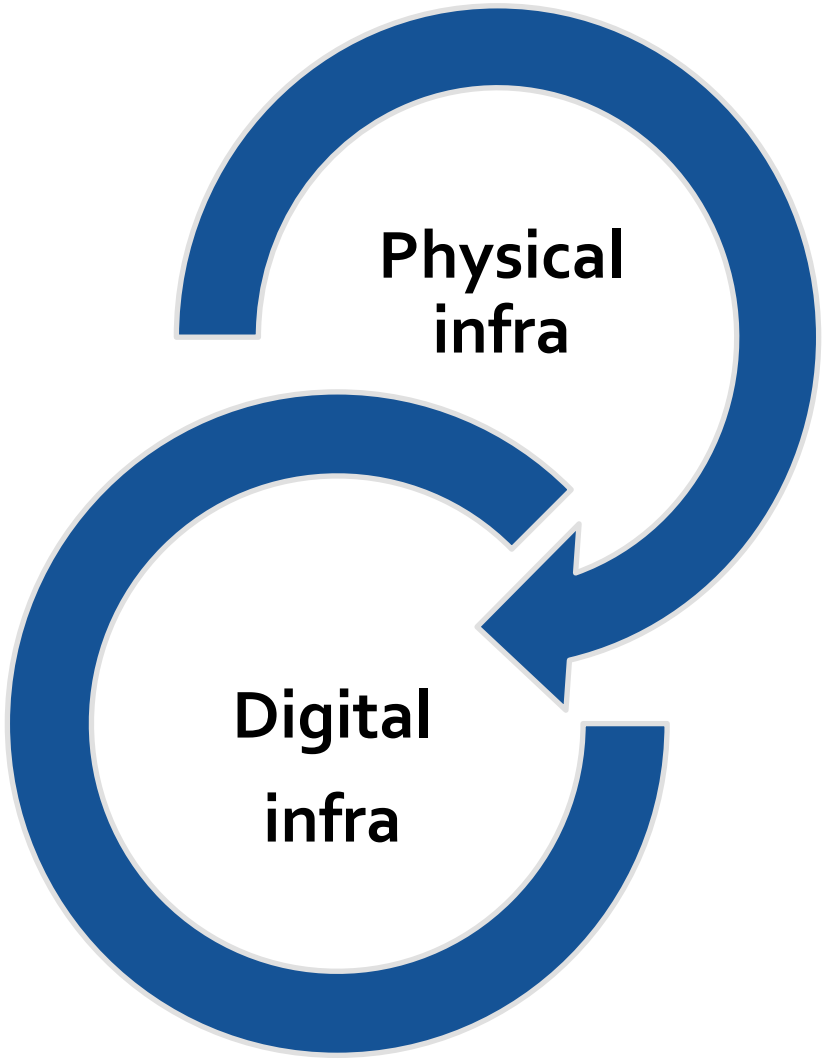
❑ Delegated act in 2018 (ITS directive)

- ✓ Focus on interoperability, security, data protection and technology
- ✓ Expected Autumn 2018

USE CASES

Day 1 C-ITS services list
Hazardous location notifications: • Slow or stationary vehicle(s) & traffic ahead warning; • Road works warning; • Weather conditions; • Emergency brake light; • Emergency vehicle approaching; • Other hazards. Signage applications: • In-vehicle signage; • In-vehicle speed limits; • Signal violation / intersection safety; • Traffic signal priority request by designated vehicles; • Green light optimal speed advisory; • Probe vehicle data; • Shockwave damping (falls under European Telecommunication Standards Institute (ETSI) category 'local hazard warning').
Day 1.5 C-ITS services list
• Information on fuelling & charging stations for alternative fuel vehicles; • Vulnerable road user protection; • On street parking management & information; • Off street parking information; • Park & ride information; • Connected & cooperative navigation into and out of the city (first and last mile, parking, route advice, coordinated traffic lights); • Traffic information & smart routing.

MULTI-LAYER INVESTMENTS



- Roads are more than asphalt, road signs, traffic lights
- Visibility of infra, signs, lane marking, … for vehicle sensors/radars -> predictability
- Static and dynamic traffic rules/signs (also for digital representation)
- Variable messaging systems
- Intact fences
- Communication about levels of platooning (static/dynamic) and other functions of automated driving

- Communication equipment/road side units/cloud solutions
- High coverage and low latency (depending on use case)
- Combination short range & long range
- Appropriate spectrum
- Bidirectional : also I2V exchange
- Interoperability

ACEA European Automobile Manufacturers Association

4. European Electronic Communications Code, GDPR and ePrivacy

EECC – IMPACT ON VEHICLE CONNECTED SERVICES

- Rationale of the new regulatory regime for telecoms
- Comparison with connected vehicles

- Key is the definition of ECS : "Electronic Communications Service" :

  A service normally provided for remuneration via electronic communications networks, which encompasses

  – "internet access service" and/or
  – "interpersonal communications service" and/or
  – services consisting wholly or mainly in the conveyance of signals such as
  ⇨ transmission services used for M2M services and for broadcasting
  ⇨ but excludes services providing, or exercising control over, content transmitted using electronic communications networks and services

NEW OBLIGATIONS FOR CONNECTED VEHICLES ?

Some examples :

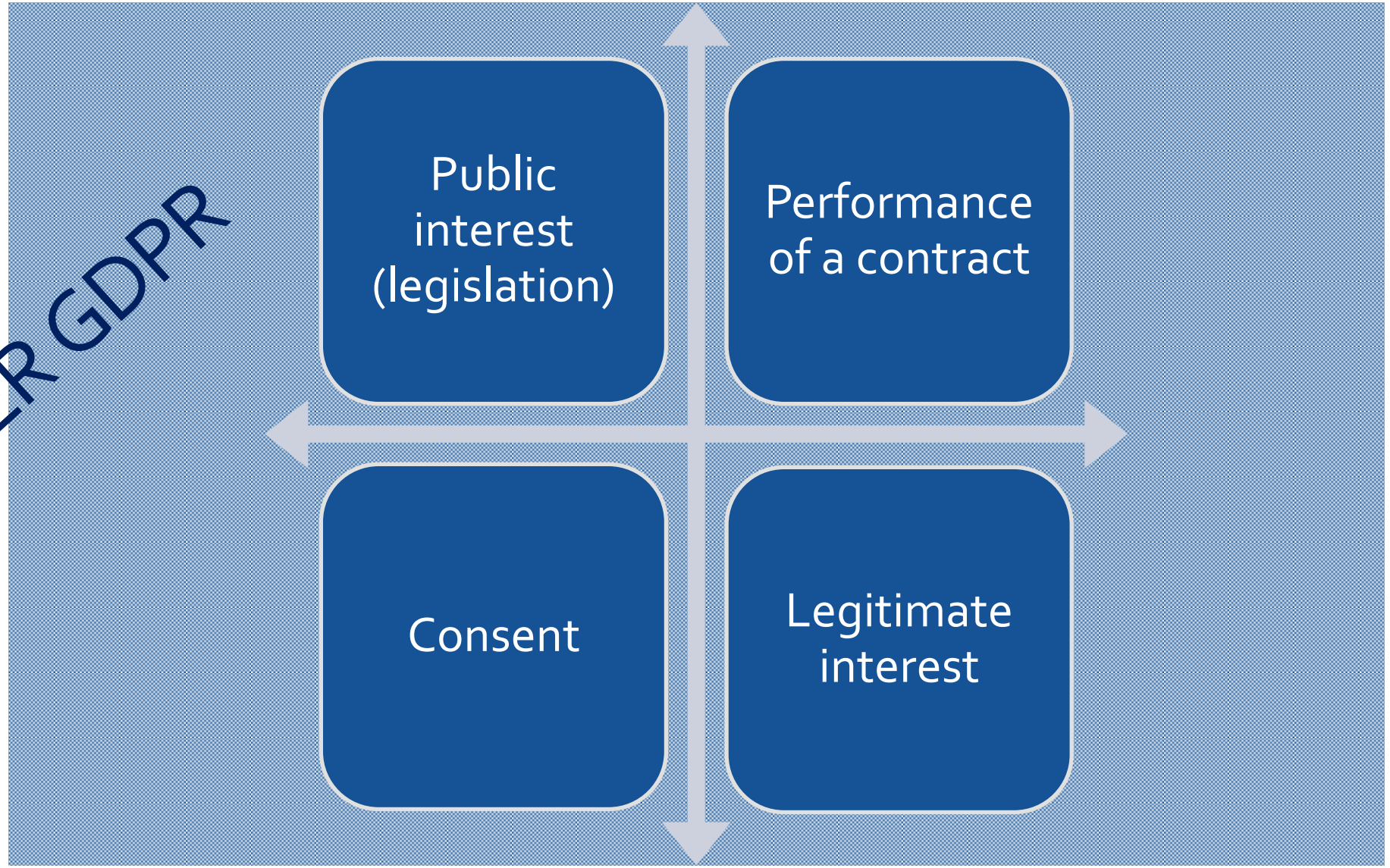
- ⇨ **Provision of information to NRAs (general authorisation schemes) and compliance with authorisation conditions incl. admin charges**
- ⇨ **Technical and organisation measures to manage security risks, integrity of network and ensure continuity of services**
- ⇨ **Notification of security breaches and loss of integrity**
- ⇨ **Security and integrity (authorisation, reporting, …)**
- ⇨ **Prohibition of discriminatory conditions on access to end users (nationality, place, residence)**
- ⇨ **Pre-contractual information provisions to consumers (QoS, restrictions, compensation/refund arrangements, tariffs, switching costs, …)**
- ⇨ **Early contract termination (pro rata refund)**
- ⇨ **Requirements on bundled offers**

DECISION PROCESS

- **Adopted position by EP in Oct 2017 – now in Trilogue**
- **Concerns on M2M one of the focal points discussed and raised by EE and BG Presidency**
- **Expected agreement mid 2018**

COLLECTION, STORAGE, PROCESSING OF DATA

UNDER GDPR



GDPR

Status

- **GDPR to apply as from 25 May 2018**
- **Vehicle manufacturers to ensure compliance**
  - ACEA guidelines
- **Enforcement by national data protection authorities**
  - Risk of diverging interpretations
  - Coordination through European Data Protection Board (EDPB; formerly Article 29 Working Party on Data Protection and Privacy)

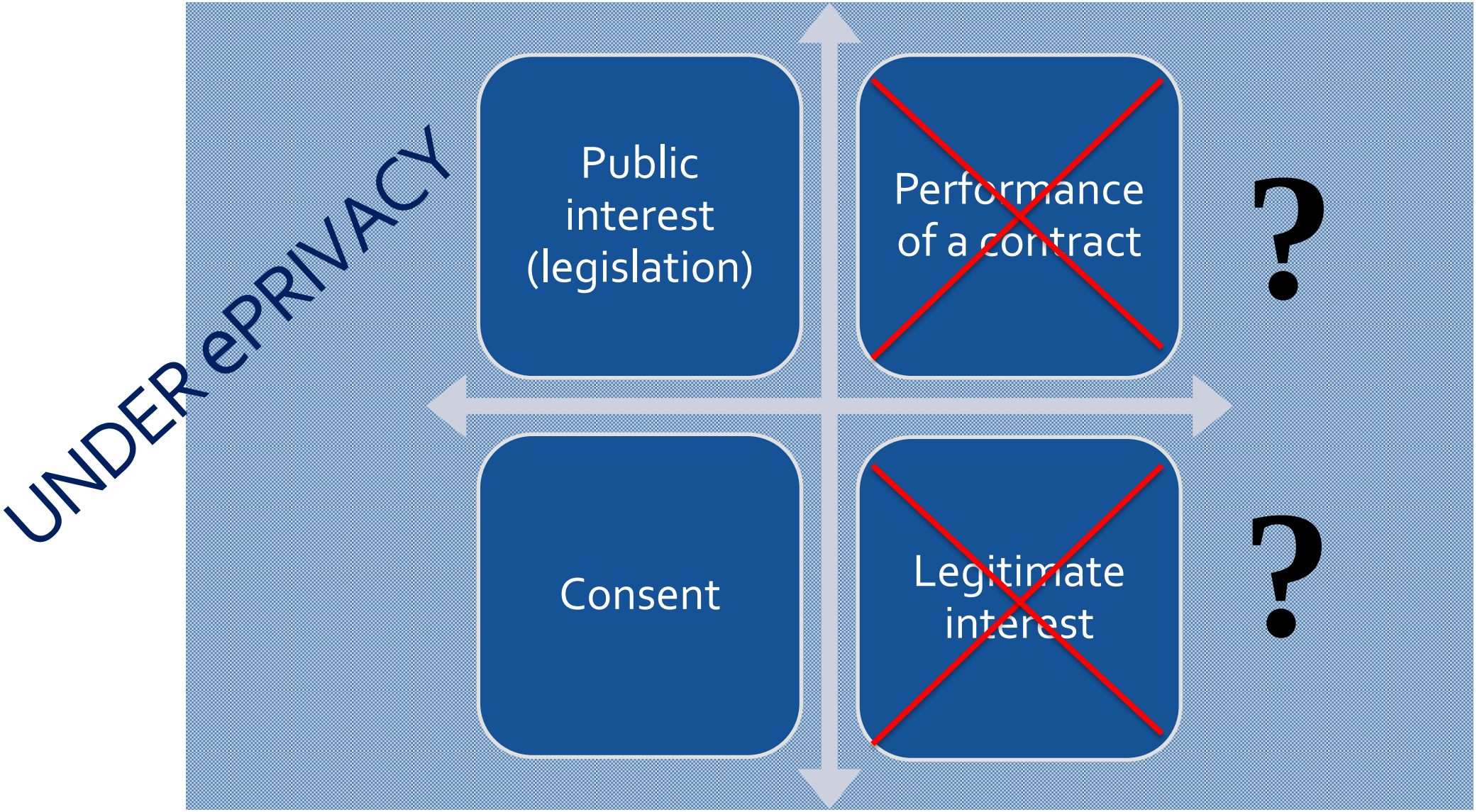
IMPACT ON C-ITS

- **Issue = compliance of C-ITS with EU data protection legislation**
  - Data communicated = personal data
  - Communications technology = permanent broadcast of CAN/DENM

- **Opinions (Oct 2017)**
  - French data protection authority (Conformity pack for connected vehicles)
  - Article 29 Working Party (opinion on C-ITS)

- **Solution through EU regulatory intervention ?**

COLLECTION, STORAGE, PROCESSING OF DATA



E-PRIVACY

Status (1)

- **Complement to GDPR**
- **Scope**
  - Confidentiality of electronic communications
  - All data, not just personal data
- **Content**
  - More limited legal grounds for data processing
    - **Only consent, no legitimate interest or contract**
    - **Potential problem for auto sector**

E-PRIVACY

Status (2)

- **EP**
  - Vote in plenary in October 2017
- **Council**
  - Ongoing discussions on working draft
  - No agreement under EE Presidency
- **Regulation unlikely to apply simultaneously with GDPR (May 2018)**

E-PRIVACY

Implications for auto sector

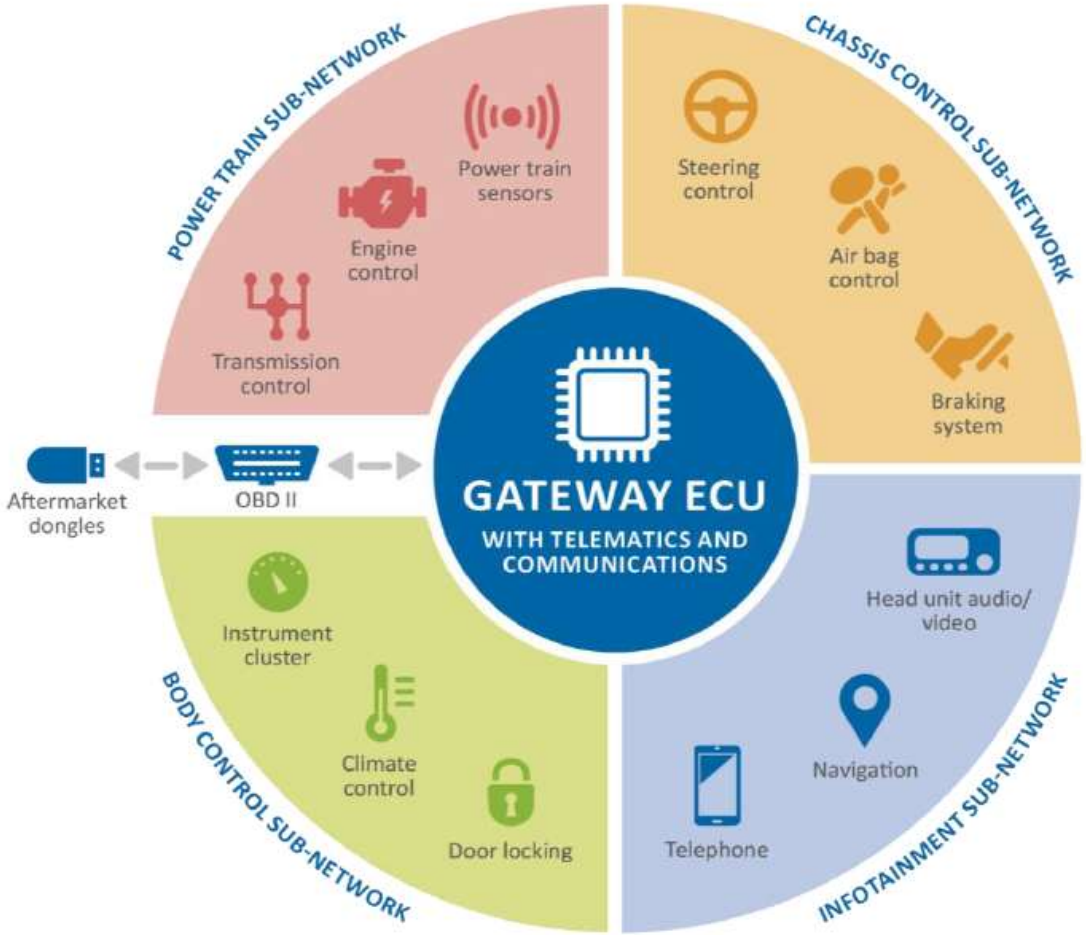
- **Are vehicle manufacturers covered?**
  - Vehicle manufacturers = electronic communication service providers?
- **Does it apply to C-ITS?**
  - M2M communications covered?
- **Article 8 remains critical**
  - Storage or processing of (any) data in "terminal equipment" only with user consent
  - Same rules for computers & smartphones (cookies)

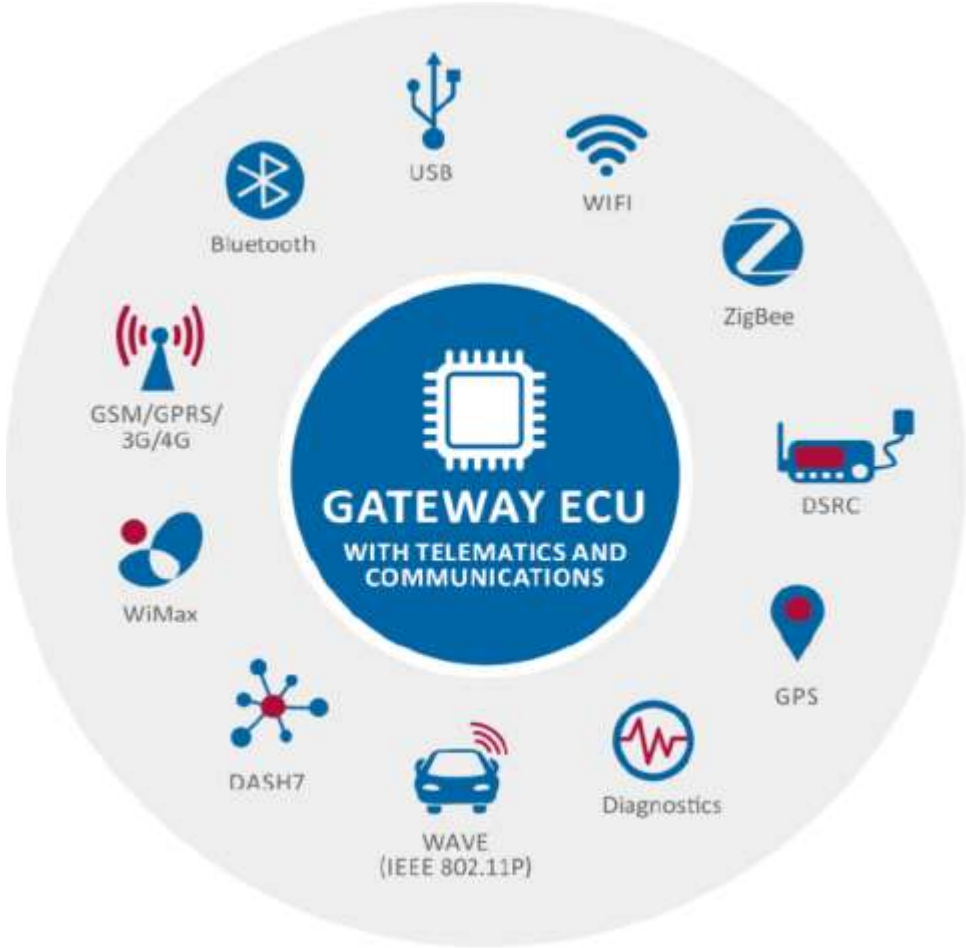
ACEA European Automobile Manufacturers Association

5. Cyber security

AUTOMOTIVE CYBERSECURITY

Vulnerabilities





Source: ENISA, cyber security and resilience of smart cars, Jan 2017

EC COMMUNICATION OF 13 SEPTEMBER 2017

Focus for vehicle manufacturers

Specific sectorial recommendations

"[…], ***specific sectors*** *face specific issues and should be encouraged to develop their own approach* [to cybersecurity]*. In this way, general cybersecurity strategies would be complemented by* ***sector-specific cybersecurity strategies*** *in areas like financial services, energy,* ***transport*** *and health."*

Recommendations

- "A "**security by design**" approach adopted by producers of connected devices, IT software and equipment
- "**Duty of care**" principle, to be further developed together with the industry,
- Goal is to **reduce product/software vulnerabilities** by applying a range of methods from
  - design to **testing and verification**, including formal verification where applicable,
  - **long term maintenance;**
  - the use of **secure development lifecycle processes**;
  - **developing updates and patches** to address previously undiscovered vulnerabilities; and
  - **fast update and repair**.

These recommendations are covered in ACEA's Principles of Automobile Cybersecurity

ACEA POSITION PAPERS

On Smart Mobility and Cybersecurity

Principles of Automotive Cybersecurity

https://goo.gl/L7SdRX

Access to Vehicle Data for Third-party Services

https://goo.gl/Lf8vAB

Principles of Data Protection in relation to CAD

https://goo.gl/37iCHV

ACEA POSITION PAPERS

On Smart Mobility and Cybersecurity

Principles of Automotive Cybersecurity

https://goo.gl/L7SdRX

Access to Vehicle Data for Third-party Services

https://goo.gl/Lf8vAB

Principles of Data Protection in relation to CAD

https://goo.gl/37iCHV

OTHER USEFUL LINKS

- http://www.acea.be/industry-topics/tag/category/connected-and-automated-driving
- https://ec.europa.eu/digital-single-market/en/cooperative-connected-and-automated-mobility-europe
- https://ec.europa.eu/transport/themes/its/c-its_en
- https://www.c-roads.eu/platform.html
- https://scic.ec.europa.eu/fmi/ezreg/RTD-CAD-2017/start
- https://connectedautomateddriving.eu/
- https://ec.europa.eu/digital-single-market/en/news/workshop-short-range-vehicular-communications-59-ghz-band
- https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy
- https://ec.europa.eu/transport/themes/its/studies/its_en

UPCOMING

- March 2018 : adoption by European Parliament of TRAN report on C-ITS
- April 2018 : EC Data Package (artificial intelligence, robotics, PSI, etc.)
- May 2018 : EC Mobility Package (GSR, state of play CCAM, …)
- 2018-2020 : delegated acts under new Type Approval Regulation
- TBD : UN-ECE horizontal view on automation and Vienna/Geneva Conventions, ASCF (R79), various other technical regulations
- TBD : UN-ECE : regulation on in-vehicle cyber
- Etc., etc…

STAY CONNECTED

Joost Vantomme
Smart Mobility Director
jv@acea.be
+32 2 738 73 69

THANK YOU FOR YOUR ATTENTION

European Automobile Manufacturers Association

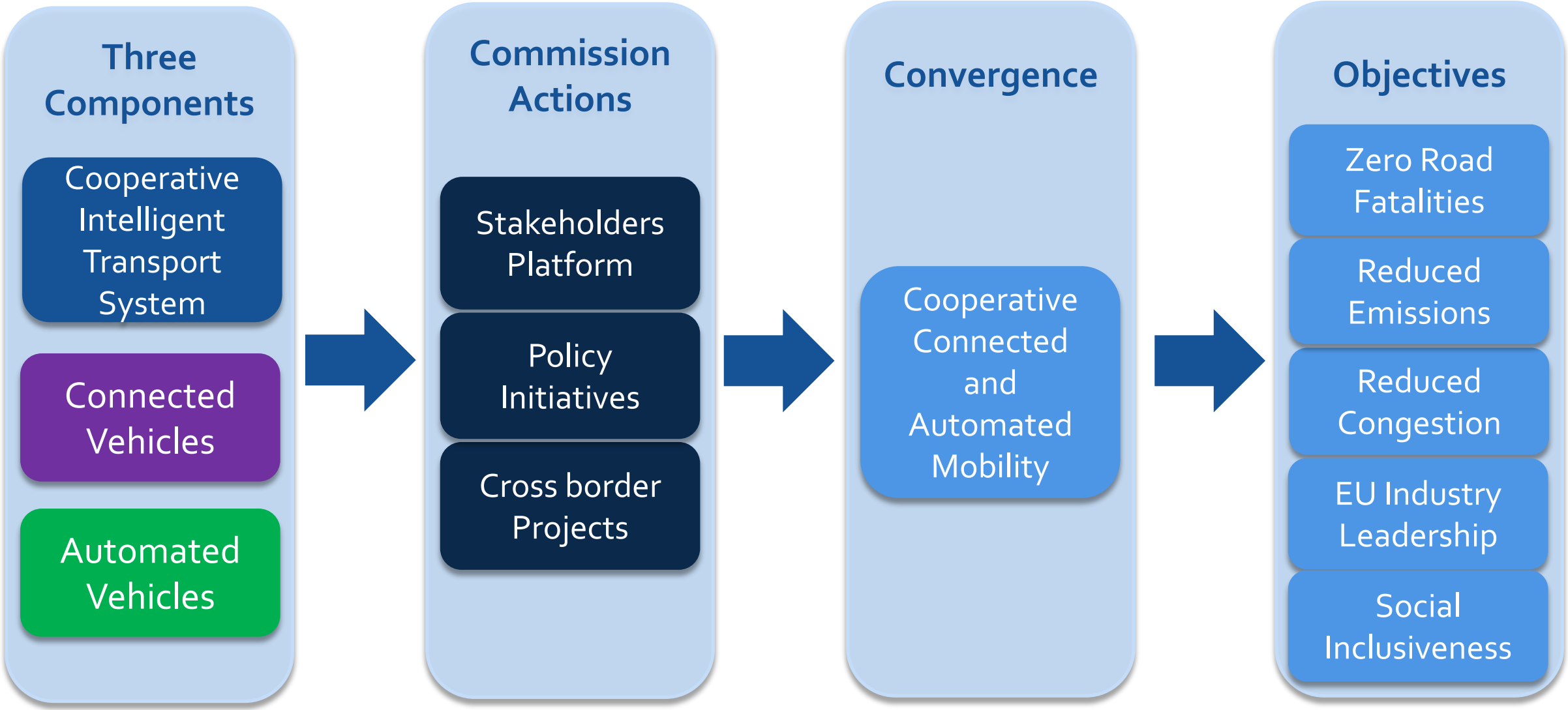
@ACEA_eu

www.ACEA.be

ACEA European Automobile Manufacturers Association

BACK-UP

FROM TECHNOLOGY TO SUSTAINABLE MOBILITY



REGULATORY OVERVIEW - UNECE

TITLE	FOCUS	COMMENTS
UN IWG ITS AD/Task Force on Cyber Security and OTA issues **WP 29** : World Forum for Harmonization of Vehicle Regulations I**WG** : Informal Working Groups **ITS/AD** : Intelligent transport Systems and Automated Driving Task Force on cyber security and OTA (Over The Air) issues	WP.29 decided to establish a task force to address: i) cybersecurity & data protection, and ii) over the air issues for road vehicles	https://www2.unece.org/wiki/pages/viewpage.action?pageId=40829523
	Focus areas: **Cyber Security** issues, relevant for the automotive industry. • Definition of "Cyber Security" in the context of automobile industry • High level principles/objectives to be obtained and their timelines • Revision of existing practice of cyber security in the automobile industry • Detailed guidance to Industry and contracting parties to the 58 Agreement • Assessment or evidence required to demonstrate competence • Outputs to be presented as a regulation or a resolution + **Data protection** issues (focus on cyber security) + **Over-The-Air software updates** • Definition of "Over-The-Air updates" in the context of automobile industry • Revision of existing practice of Security aspects in Over-The-Air updates • Implications related to type approval • Implications related to post registration regulatory compliance and conformity to the type approved • Outputs to be presented as a regulation or a resolution • Develop relevant recommendations, provisions or documentation -> Submit its outcome to the IWG on ITS/AD.	First meeting London, 21 Dec 2016 • Chair : Darren Handley, DfT, UK • Secr. : Jens Schenkenberger, Huyndai/OICA • Contact flow for IWG/AD : Bogdan Bereczki, Audi AG/OICA **UNECE Cyber Security guidelines ITS/AD WP29/2017/46** • UK Gov Centre for Connected and Autonomous vhicles (CAV) coordinates for the UK. UK CAV worked out a set of principles for Cyber Sec : https://www2.unece.org/wiki/download/attachments/40829523/TFSC-01-03e%20DfT%20draft%20CAV%20cyber%20security%20principles.pdf?api=v2 • UK will send survey to OEMs, Tier1/2 suppliers

REGULATORY OVERVIEW - EU

TITLE	FOCUS	COMMENTS
European Commission Communication "*Open, safe and secure cyber space*" 7 Feb 2013	Overall cyber strategy Cyber resilience	https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security No direct focus on automotive
Network and Information Security Directive (NIS) 6 July 2016	First EU-wide legislation on cyber Increased obligations on critical infrastructure operators where under ITS operators and road authorities Establishment of CSIRT (Computer Security Incident Response Teams)	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
General data protection regulation (GDPR) 27 April 2016	Companies who process personal data to report data breaches	http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf http://ec.europa.eu/justice/data-protection/
New **European Commission Communication "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*" 13 September 2017**	Wide range of concrete measures to strengthen the EU's cybersecurity structures and capabilities More cooperation between the Member States and the different EU structures concerned	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN Direct references to transport

REGULATORY OVERVIEW - EU

TITLE	FOCUS	COMMENTS
ENISA : European Network and Information Security Agency	Centre of expertise for the EU • Recommendations • Policy implementation for Member States • 'Hands On' work with direct cooperation with the national CERT teams	ENISA : https://www.enisa.europa.eu/ Cars and Roads SECurity expert group (CarSEC): https://resilience.enisa.europa.eu/carsec-expert-group
	-> 13 Jan 2017: **Report on Cyber Security and Resilience of Smart Cars** https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/ • Identification of good practices that ensure the security of smart cars against cyber threats • Listing of the sensitive assets present in smart cars, as well as the corresponding threats, risks, mitigation factors and possible security measures to implement • Three categories of good practices: *Policy and standards, Organizational measures, and Security functions.*	Out of scope : V2V, autonomous vehicles Recommendations: ✓ Improve cyber security in smart cars. Establish good practices ✓ Improve information sharing amongst industry actors. Cfr US system ✓ Improve exchanges with security researchers and third parties ✓ Clarify liability among industry actors ✓ Achieve consensus on technical standards for good practices ✓ Define an independent third-party evaluation scheme ✓ Build tools for security analysis

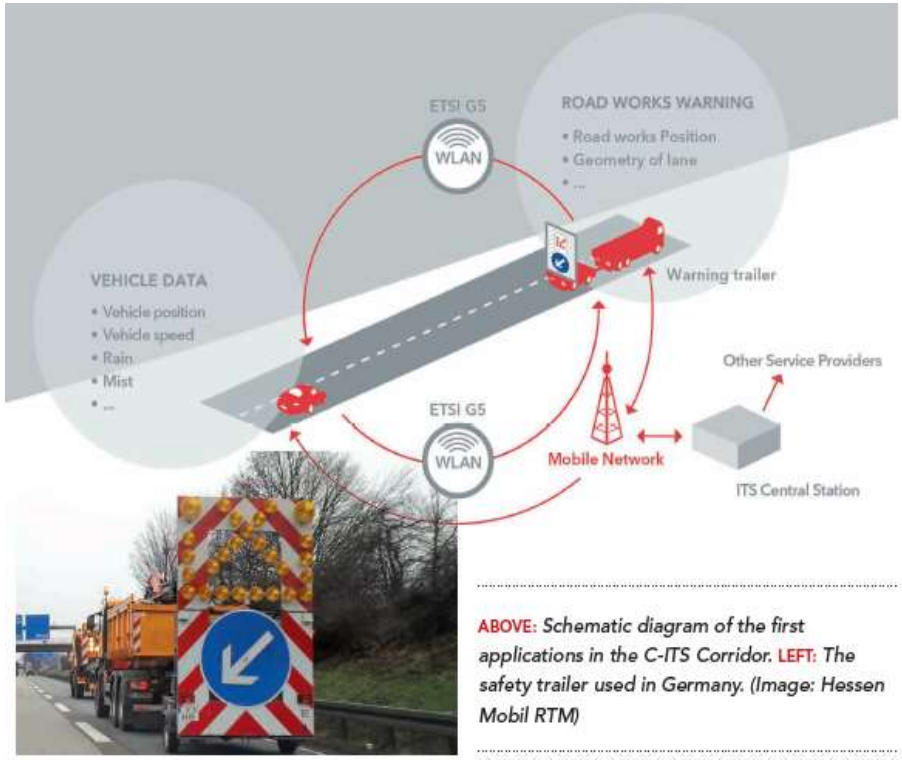
REGULATORY OVERVIEW - EU

TITLE	FOCUS	COMMENTS
DG MOVE **Security of communications for V2V and V2I exchange of messages**	**C-ITS context** Trust model based on a Public Key Infrastructure (PKI) as recommended by the standardization results and by similar initiatives in the world (Connected Vehicles in USA and Australian Gate Keeper). Trust model defined in • Security policy • Certificate Policy • Certification Practise Statement • Trust List Manager Trust model roles: • Police authority • Central point of contact • Root certification authority • Trust list manager	30 Nov 2016: European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility: https://ec.europa.eu/transport/themes/its/c-its_en June 2017 : common security and certificate policy for deployment of C-ITS: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf .

PROJECTS (EU FUNDED)

C-ITS corridor project : Dutch, German and Austrian authorities deploy C-ITS. Rotterdam -> Frankfurt -> Vienna

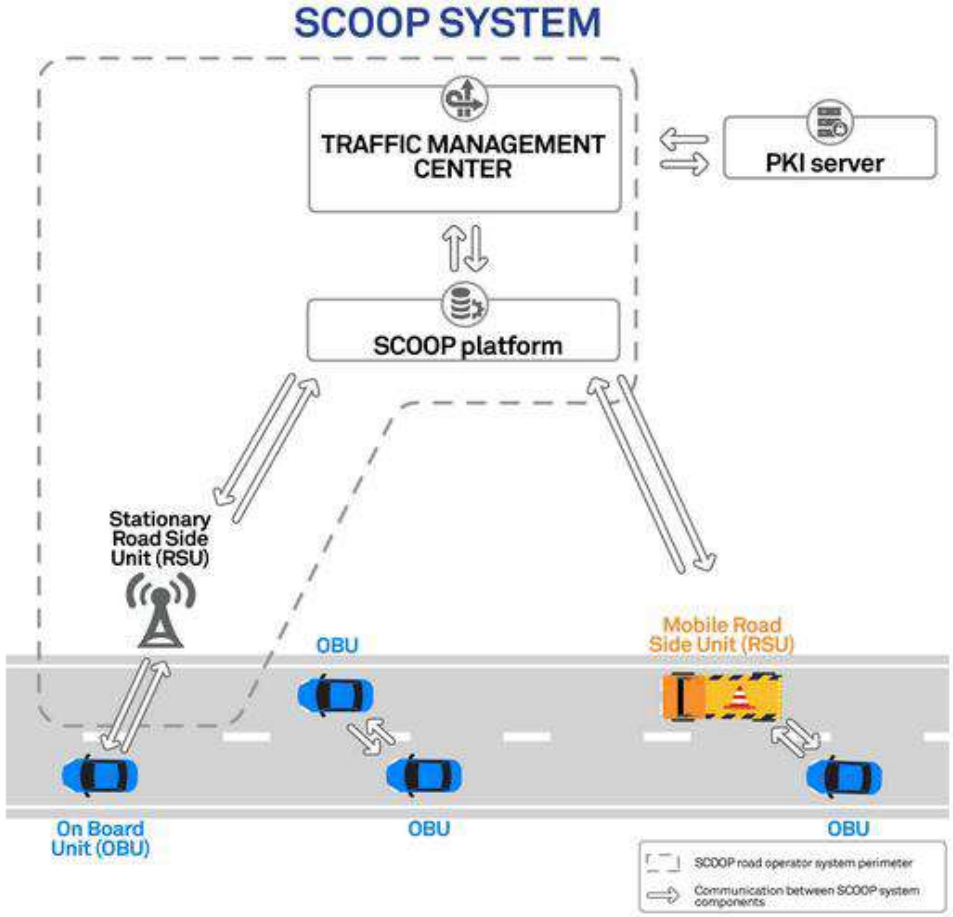
- Common use case : road works warnings.
- Details of how the communication works V2I : http://c-its-korridor.de/data/download/2930_ITS_MayJune_2016.pdf
- Instructive movie : https://vimeo.com/161891734
- Project websites:
  -NL: http://www.c-its-korridor.de/?menuId=1&sp=en
  -DE: http://www.c-its-korridor.de/?menuId=1&sp=en
  -AU: http://eco-at.info/



ABOVE: *Schematic diagram of the first applications in the C-ITS Corridor.* LEFT: *The safety trailer used in Germany. (Image: Hessen Mobil RTM)*

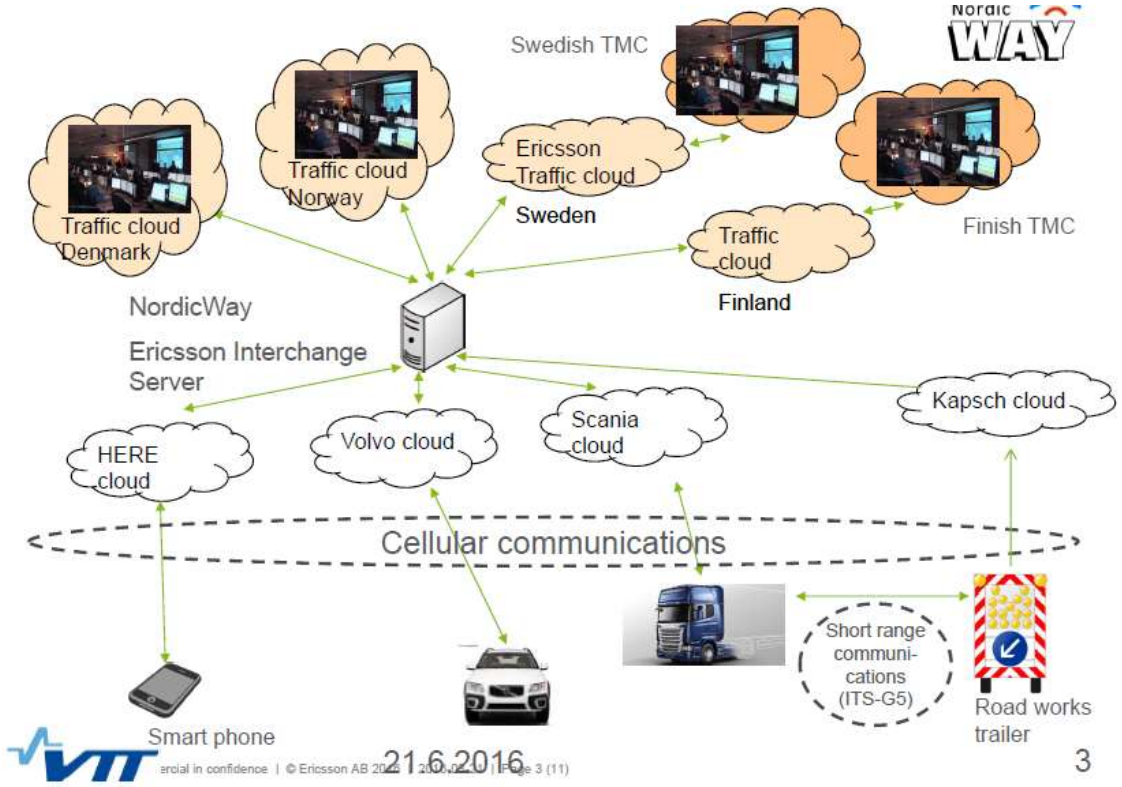
PROJECTS (EU FUNDED)

- French Ministry of Environment, Energy and the Sea is the coordinator for local authorities, road operators, car manufacturers, universities and research institutes
- SCOOP aims at deploying 3000 vehicles over 2000 km of roads on five sites
- Use cases : road work warning, different vehicle warnings such as stationary, slow, hazardous weather conditions
- http://www.scoop.developpement-durable.gouv.fr/en/

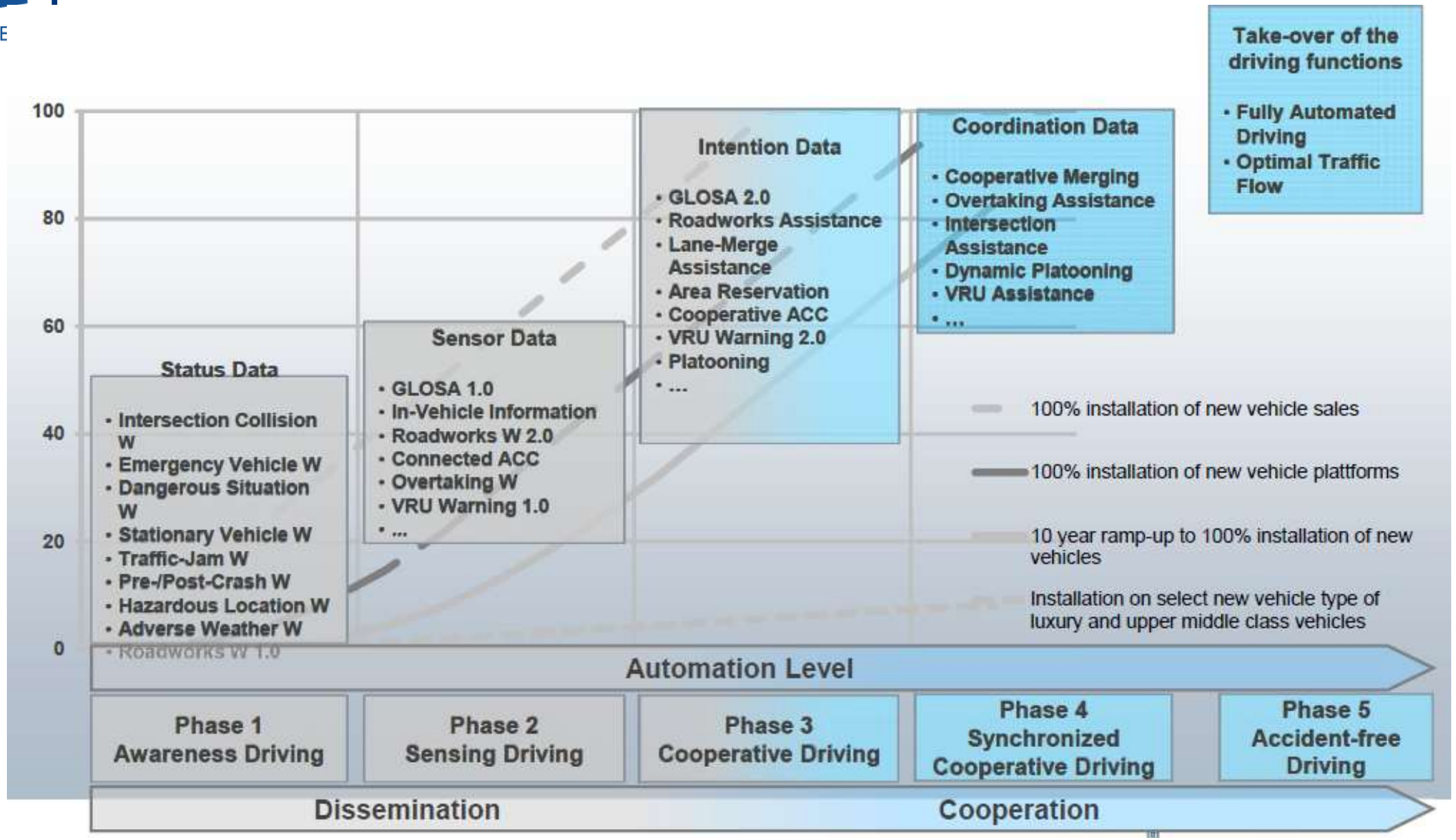


PROJECTS (EU FUNDED)

- Road corridor through Finland, Norway, Sweden and Denmark
- Various use cases
- Hybrid technology
- http://vejdirektoratet.dk/EN/roadsector/Nordicway/Pages/Default.aspx



CAR2CAR CC ROADMAP

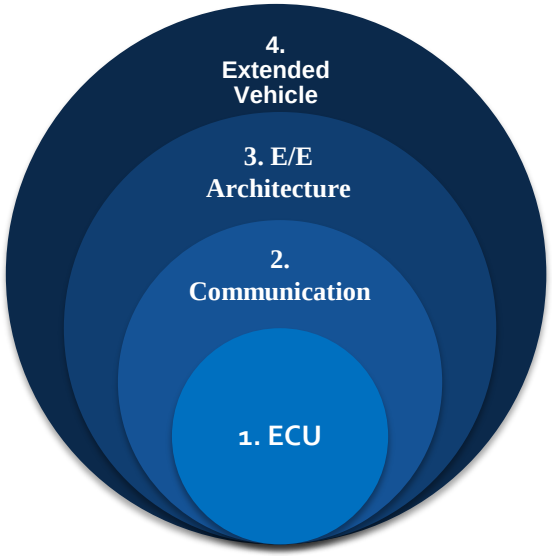


ACEA PRINCIPLES OF AUTOMOTIVE CYBERSECURITY

Summary

1. Cultivating a cybersecurity culture

- Increase **awareness** of cybersecurity issues and concerns in the company
- Rely on in-house and 3rd party **cybersecurity experts** and develop training programs for all staff members.



2. Adopting a cybersecurity life cycle for vehicle development

- Follow a specific **roadmap** for cybersecurity contents introduction
- Provide **Security by Design**
- Rely on a dedicated **Information Security Management System**
- Implement strong **security functions**

ACEA PRINCIPLES OF AUTOMOTIVE CYBERSECURITY

Summary

3. Assessing security functions through testing phases

- Use penetration testing to assess the effectiveness of cybersecurity mechanisms
- Automated security tests are used to exclude well-known vulnerabilities
- Functional security testing is used to assess security functions
- Test both hardware and software

4. Managing a security update policy

- An update policy is required to ensure that cybersecurity mechanisms remain adapted to evolving threat
- Update policy must take account of the specifics of a connected vehicle:
  - **Diversity of components requiring separate updates**
  - **Need to avoid operational disruption**
  - **Need for both secure over-the-air updates and physical updates**

ACEA PRINCIPLES OF AUTOMOTIVE CYBERSECURITY

Summary

5. Providing incident response and recovery

- Incidents response plans must be set up to track incidents affecting the vehicle and help recover vehicle functionality
- It must document the incident response, from identification and containment to remediation and recovery
- It must be adaptive, by building on experience

6. Improving information sharing amongst industry actors

- A high level of collaboration among multiple industry operators is necessary to fight cyberthreats
- OEMS will engage with public authorities as well as other stakeholders, from every sector of the industry.