Part1_Summarize
Connected Vehicle

Fatalities:

World Health Organization : 1.3 millions of fatalities / year in the world→ Human errors lead to 90% of road accidents,

Health impact,

Increase mobility (ex: Seniors & disabled people)

Energy print foot (Oil expected reduction ~15%)

Stringent regulators will

Fatalities:

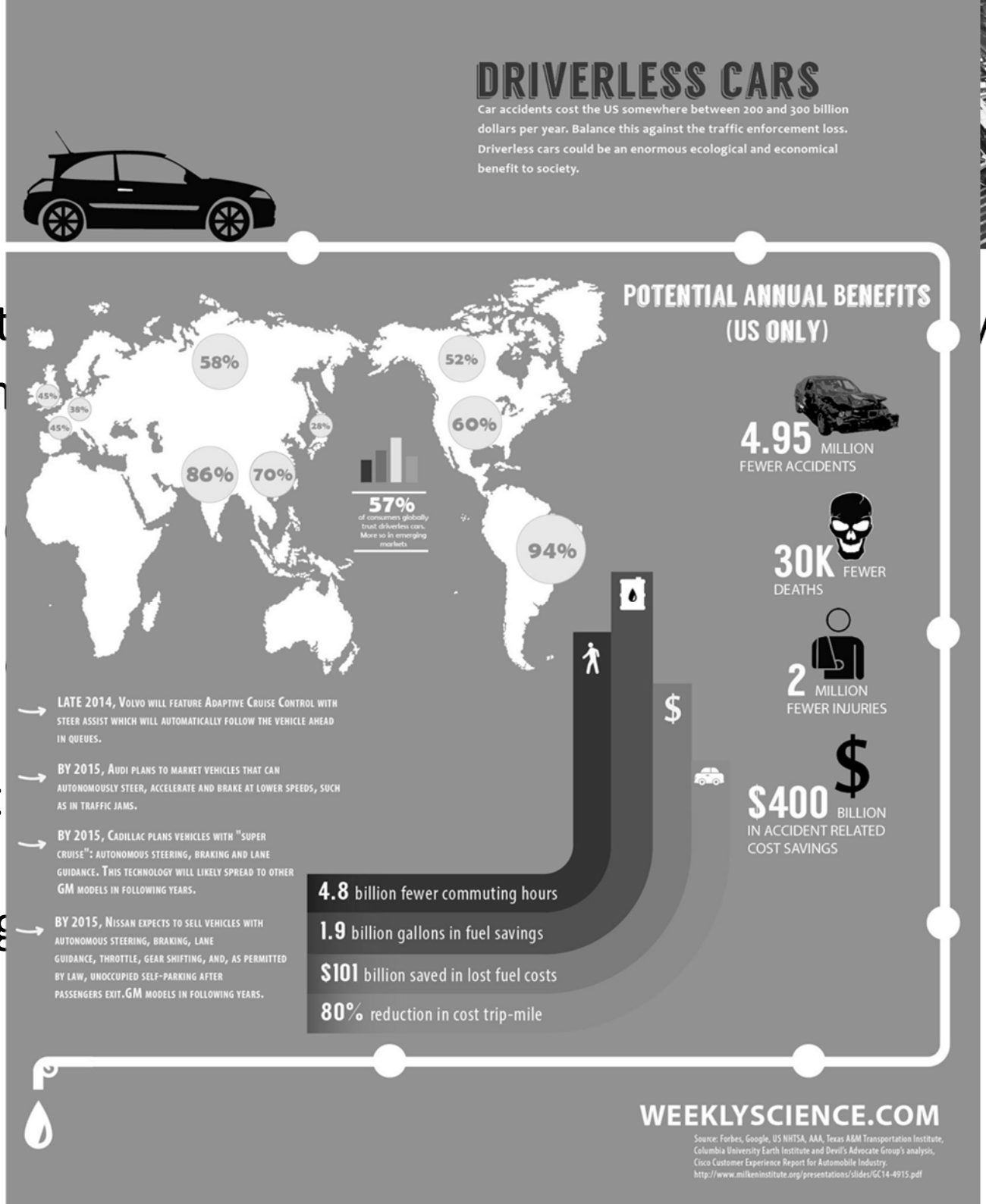
World Healt ear in the world→ Hun

Health impa

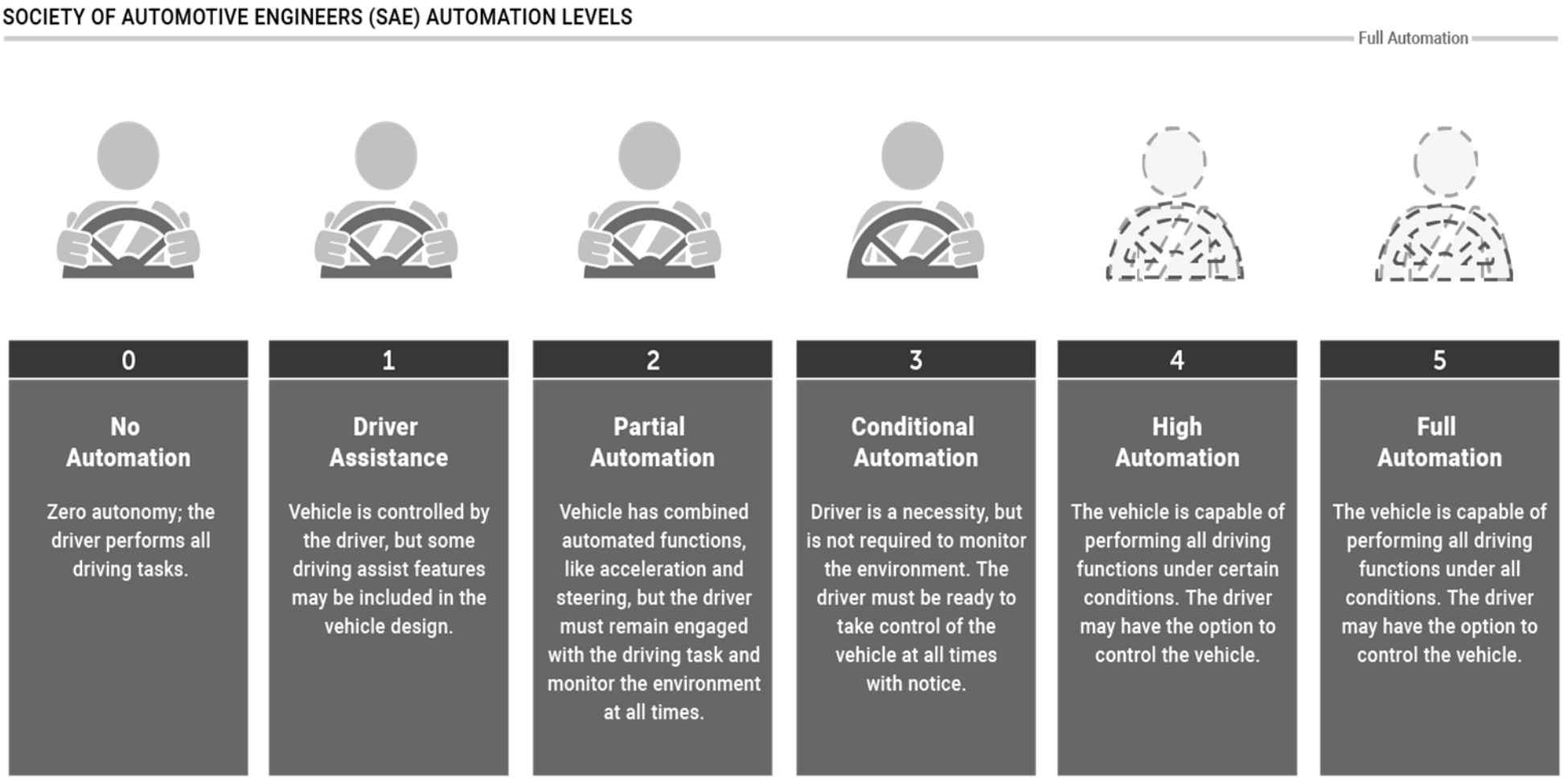
Increase m

Energy print

Stringent reg

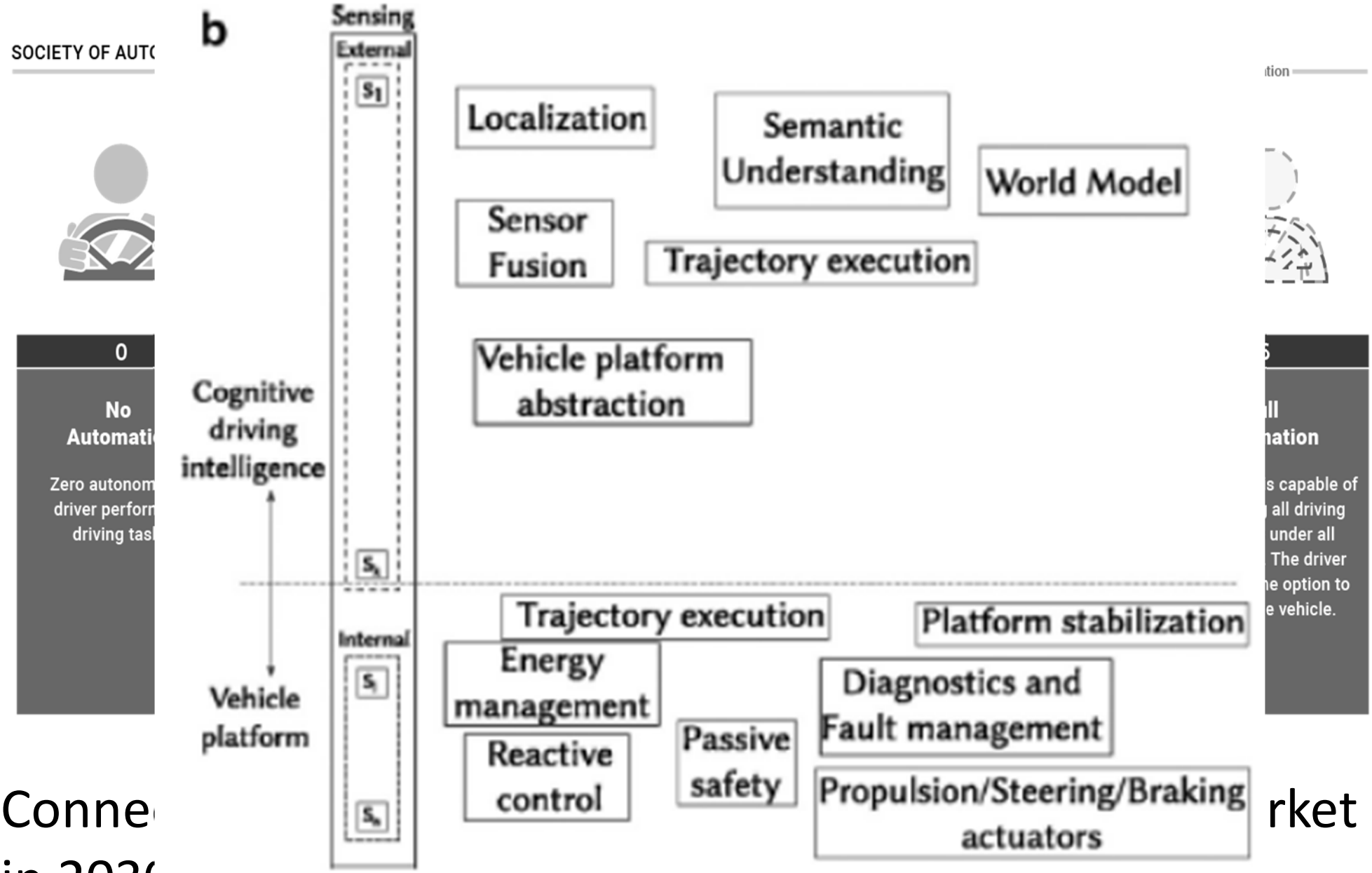


SAE classification : Automation levels



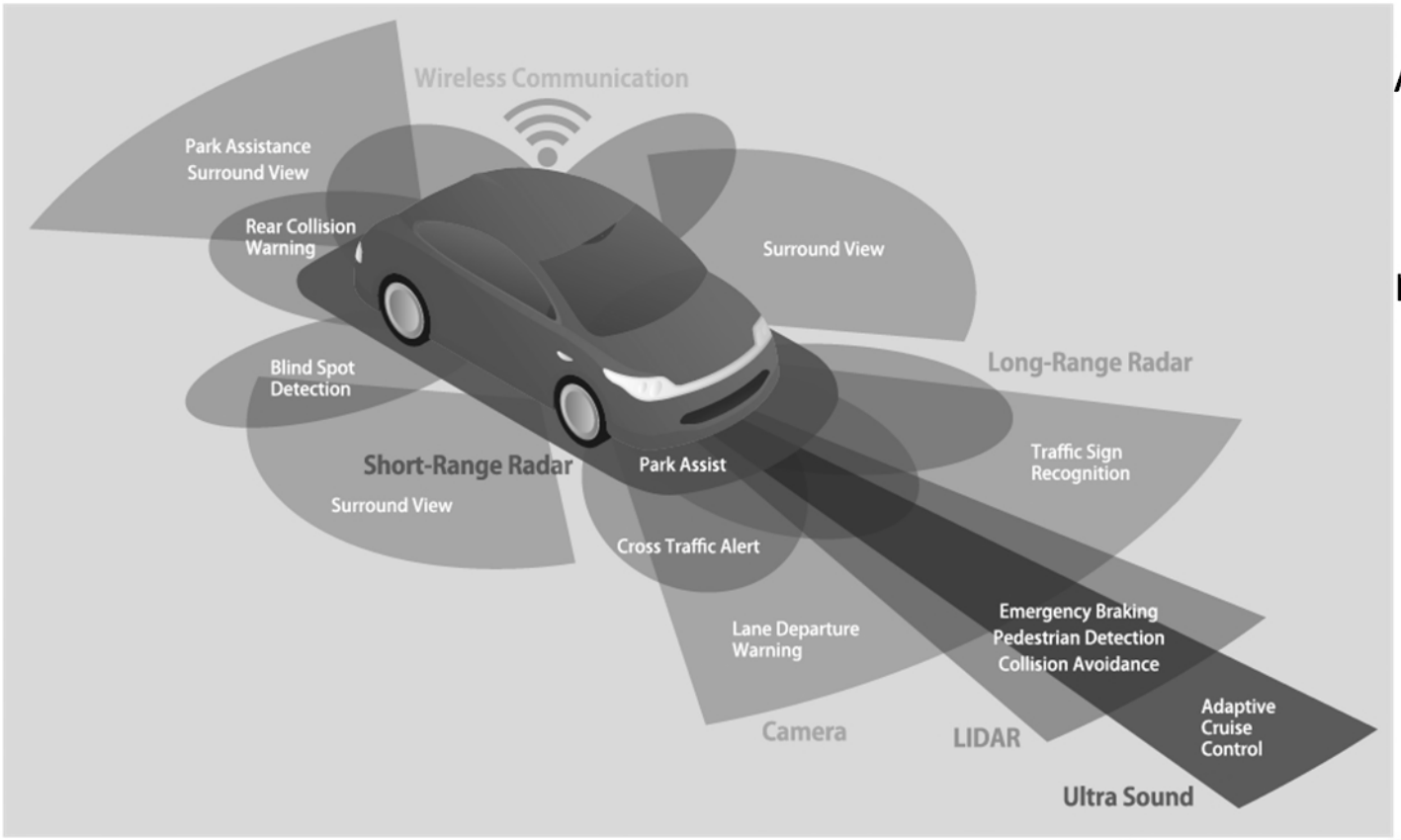
Connected vehicle should be massively occupy the market in 2030 and overreach up to 55% (optimistic) in 2040.

SAE classification : Automation levels



Conne rket in 2030 and overreach up to 55% in 2040.

Sensors Belt



AV need to detect :

- Target range,
- Position and scene recognition,
- Shape & color detection,

CAMERA LIDAR RADAR GPS (RTK) Odometer HD Maps

Sensor fusion is a key to insure precision & accurate nearby and distant target.

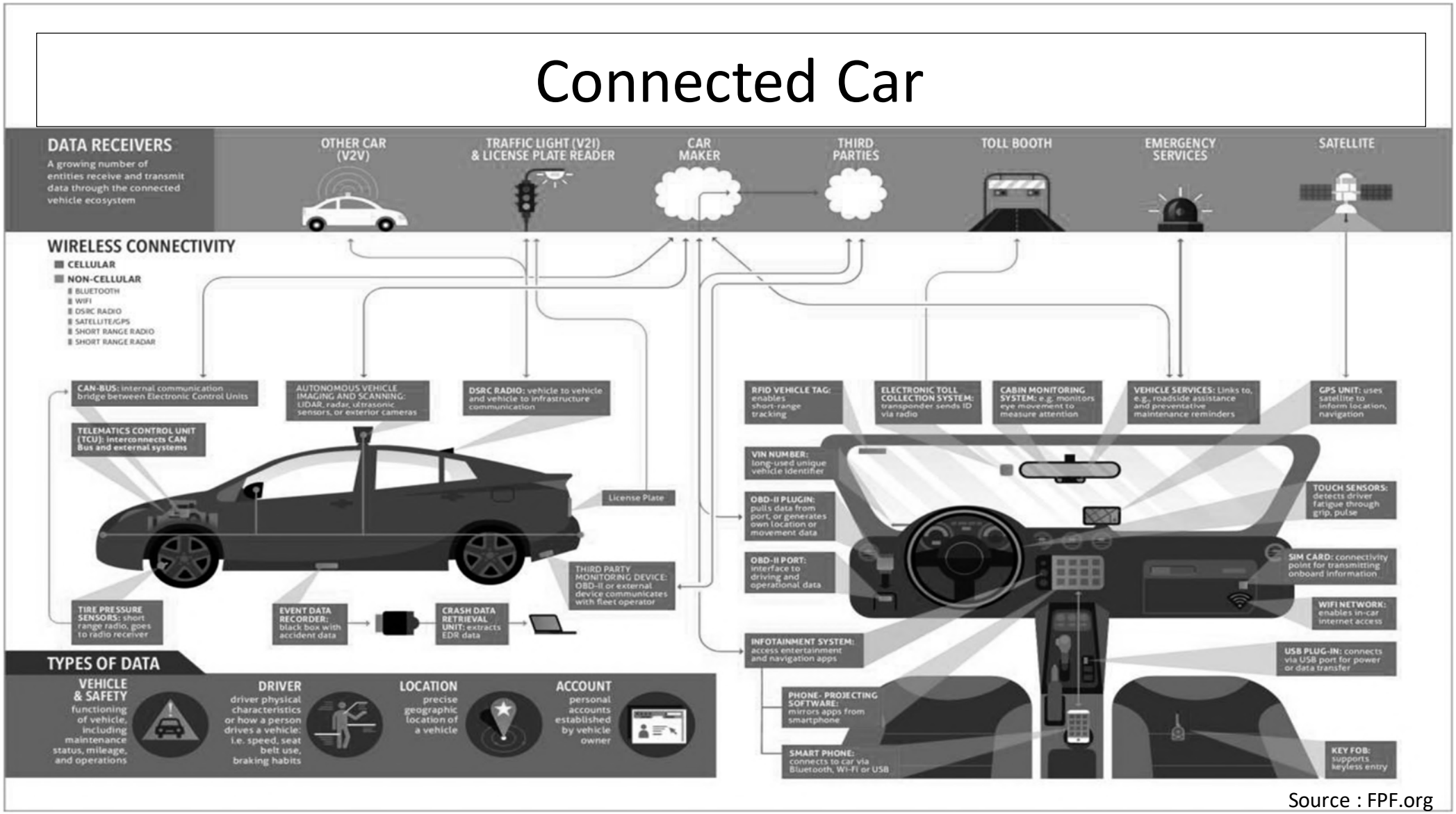
Sensors Belt – Strength & Weakness

Technology	Range (day/ clear)	Range (night/ obscured)	Resolution /Detection	Eye-safe	Price
Radar	Long (200m+)	Excellent	Limited	Yes	$
Optical camera	Short -medium (<50m)	Poor	Good	Yes	$
LiDAR 905nm	Medium (<200m)	Good	Excellent	???	$$
LiDAR 1550nm	Long (200m+)	Good	Excellent	Yes	$$$

Radar is a mature techno, efficient to detect echo whatever weather condition,

Lidar is a new player, efficient to establish a 3D map.

Data flow – See what you can't see !



Source : FPF.org

Data exchanges with road infrastructure, pedestrian and other cars

Quiz

Autonomous vehicles are required for :

- Traffic jam ☐
- Car maker business ☐
- Health protection ☐

Accident massively belongs on human errors for :

- 40% ☐
- 60% ☐
- 90% ☐

Massive autonomous car introduction is expected for :

- 2040 ☐
- 2030 ☐

Quiz

Autonomous vehicles involve :

- Strict functional domain isolation □
- Partial functional domain collaboration □
- Global functional approach □

Disruptive Electronic Architecture is due to :

- Massive computing □
- Big data (cloud included) □
- Network technologies □

Autonomous vehicle safety issues :

- are closed to « in field » requirements □
- require best practices □

Quiz

Radar

	Advantages	Drawback
Cost		
Weather conditions sensibility		
Computation needs		
Range		

Lidar

	Advantages	Drawback
Cost		
Weather conditions sensibility		
Computation needs		
Range		

Quiz

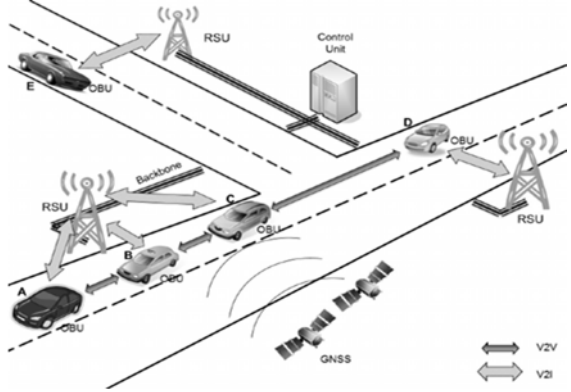
Camera

	Advantages	Drawback
Cost		
Weather conditions sensibility		
Computation needs		
Range		

To improve reliability and precision, supervisor has to :

- Handle sensors fusion □
- belong on high baud rate networks □
- belong on several cores (CPU ; FPGA ; GPU ;... □

After detection… connection !



Surrounding environment detection need sensors and computation but, also :

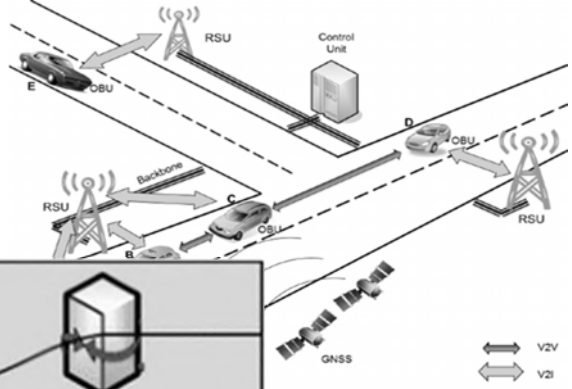
- ✓ Geo-localization, 3D Mapping
- ✓ Data exchanges with infrastructure and other vehicles

Data (up/down) transfer in/out a vehicle is a key point for autonomous capabilities :

- ✓ V2V communication : Short range (DSRC ~300m)
- ✓ Data base using (and loading),
- ✓ Road mapping updating,
- ✓ Infrastructure communication,
- ✓ Outboard services, Diagnostic, Emergency calling
- ✓ …

Long range

After detection… connection !

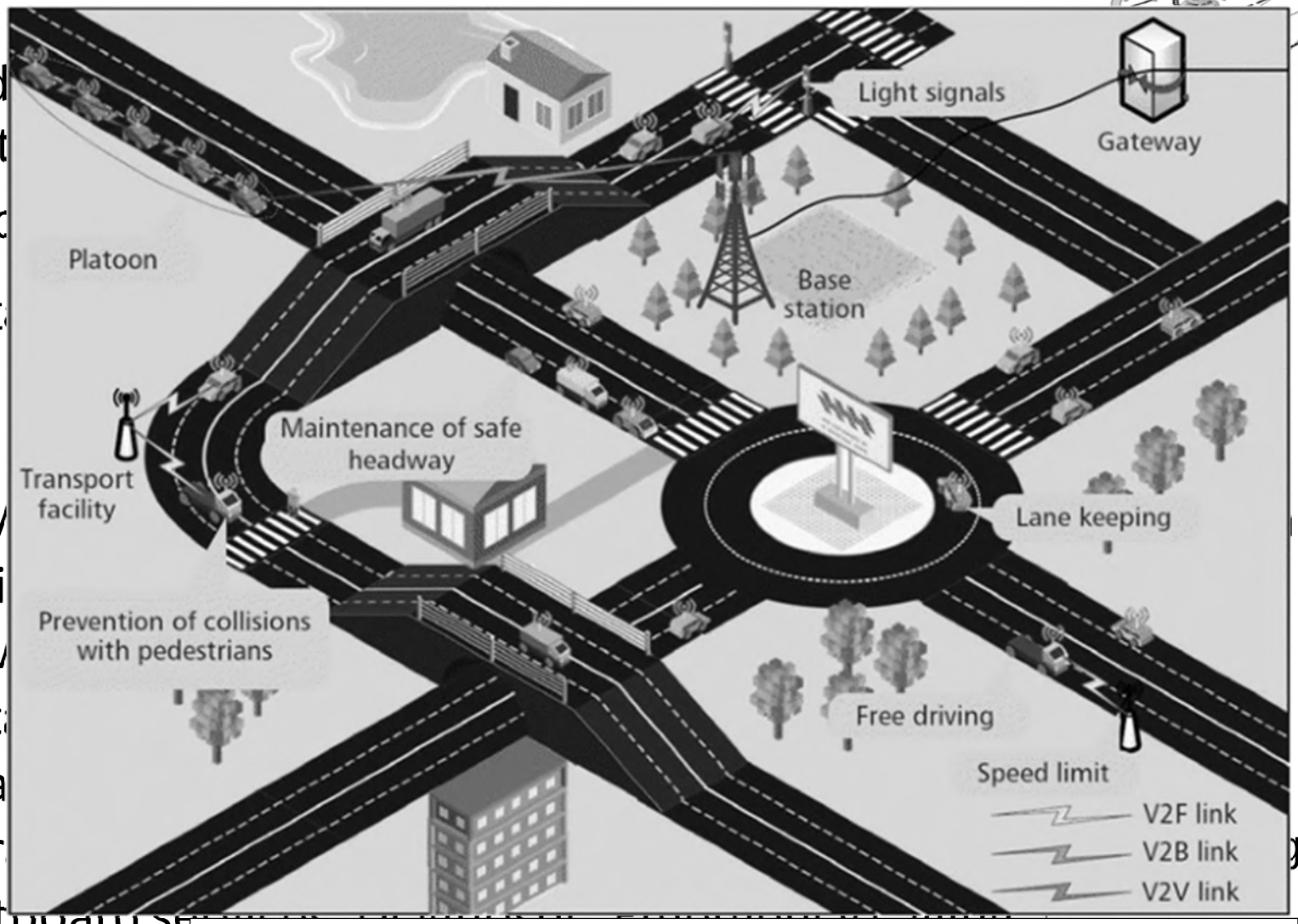


Surround
computat

- ✓ Ged
- ✓ Dat

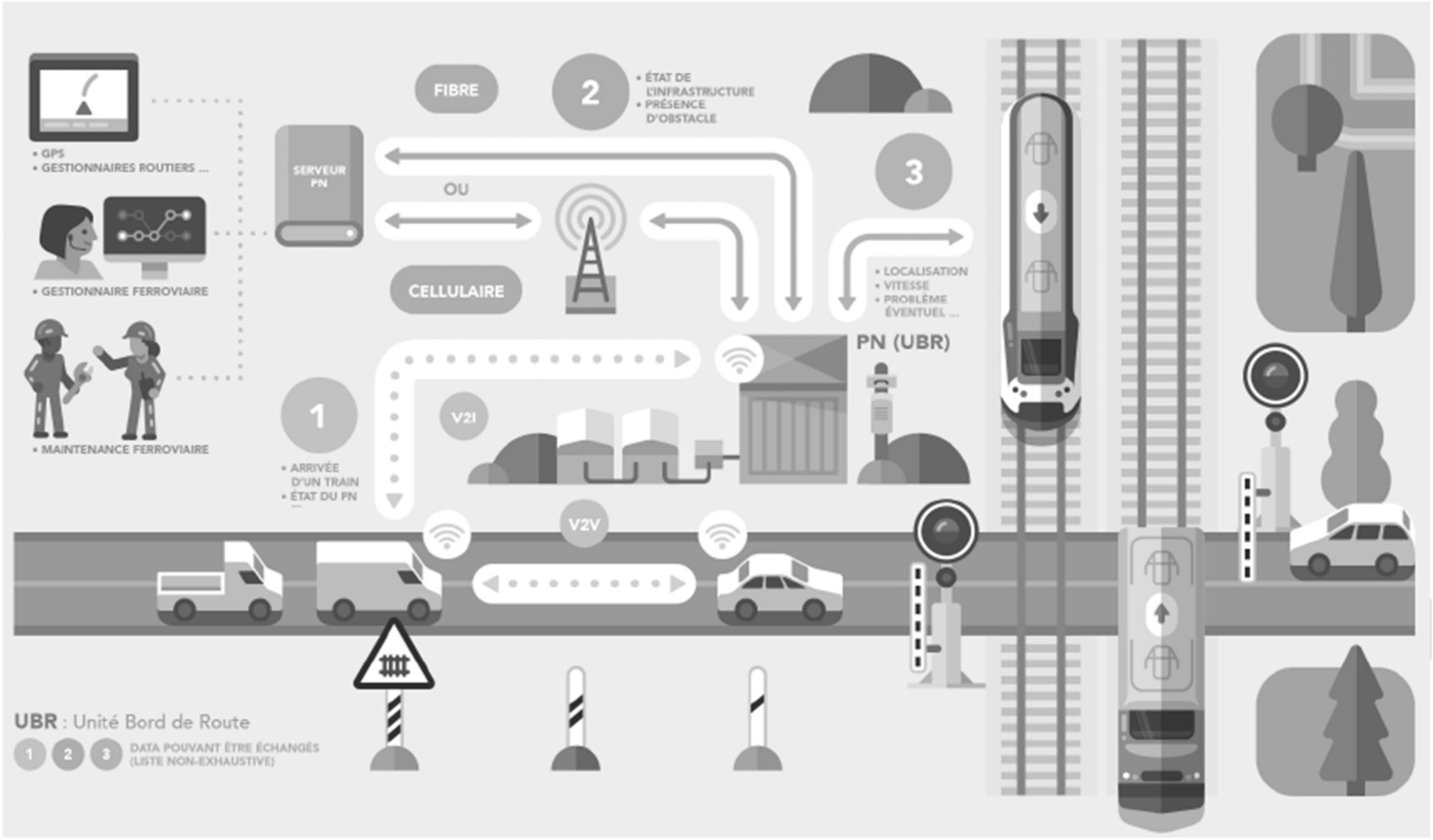
Data (up/ ous
capabiliti

- ✓ V2V
- ✓ Dat
- ✓ Roa
- ✓ Infr ge
- ✓ Outboard se
- ✓ …



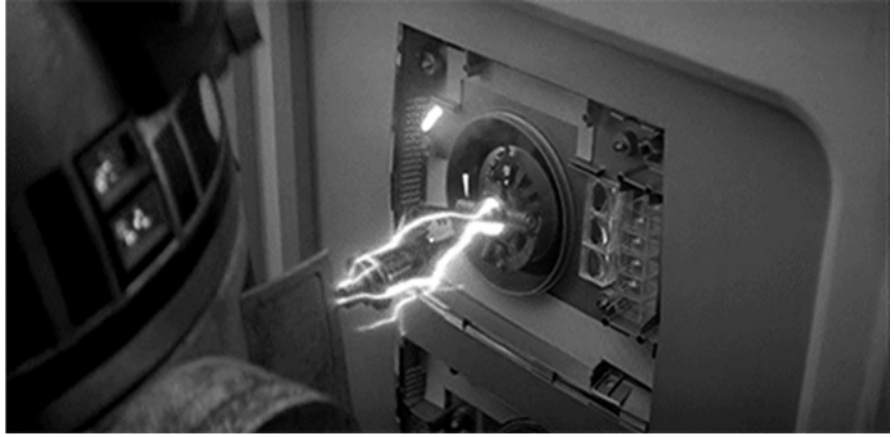
Reliable and efficient autonomous driving: the need for heterogeneous vehicular networks. Commun Mag IEEE 53:72–79#ref-CR16

Road infra & Vehicle connected



European Scoop project - 2019

V2x definition



V2V

Vehicle to vehicle communication allows safety and harmless improvement

(ex : Intersection incoming situation lead to Camera & Radar blind situation).

This communication is also powerful to insure bubble safe area all around the car with up/down stream).

Studies are running for V2V infrastructure & road detection exchanges between vehicles (peer data flow).

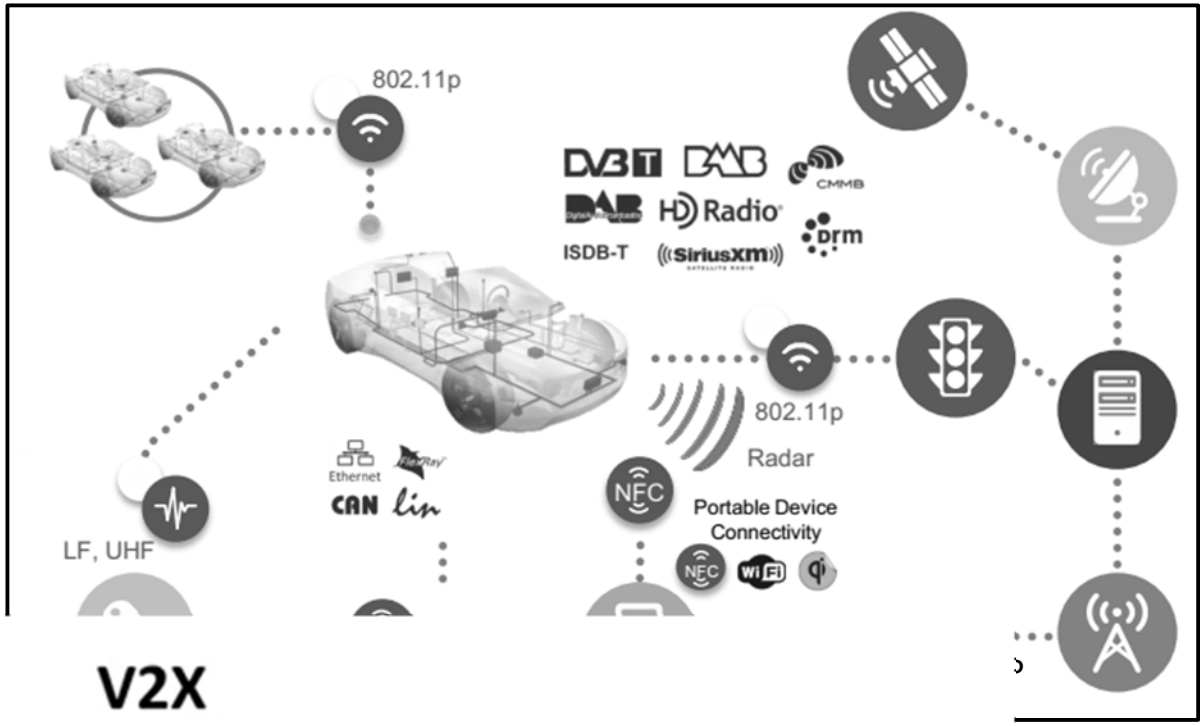
V2I

Will lead to massive cost investment, however, these services will allow to receive traffic information, signalization, weather conditions, on work situation, closed danger,…

Connected vehicle

Data exchange technologies :

- ✓ Cellular : 3G to 5G,
- ✓ WiFi : 802.11p,
- ✓ RFID (keyless,…),
- ✓ Radio broadcast (Digital),
- ✓ …



Coni

- ✓ Con
  BMW

- ✓ Aut

nc,

V2X

- **IEEE 802.11p**
  - USA - Dedicated Short-Range Communication (DSRC)
  - Europe - ITS-G5
  - Japan - ARIB STD-T109
- **IEEE 802.11bd**
  - Evolution of 802.11p, expected to be available in 2021

- Cellular V2X (**C-V2X**) – defined by 3GPP
  - Release-12: D2D
  - Rel-13: eD2D
  - Rel-14: V2V, V2X basic services
  - Rel-15: eV2X
  - Rel-16: 5G NR V2X

Functional needs - V2V

Motivation

- ✓ Exchange information : Real time, short range
- ✓ Avoid collision : “Here I am” principle and “where are the others”
- ✓ First who sees the danger has to broadcast information

Scenarios

- ✓ Blind intersection,
- ✓ Weather conditions,
- ✓ Emergency breaking,
- ✓ Lanes changing

Messages need to be standardized, short but with a guaranty of latency

Functional needs - Car to Cloud

Research consultancy IHS Markit had estimated that in 2022, 160 million vehicles globally will have the capability to upgrade their onboard computer systems over the air.

Motivations to be connected to cloud :

- Software update (S-OTA),
- MAP update (3D MAP & augmented reality, POI,…),
- Data report for maintainability (Diagnostic, Error flags,…),
- Fleet management,
- Custom facilities (Agenda, Media, Navigation, Localization,…)
- Weather conditions, Traffic, on work alert,…

Functional needs - GPS & MAPS

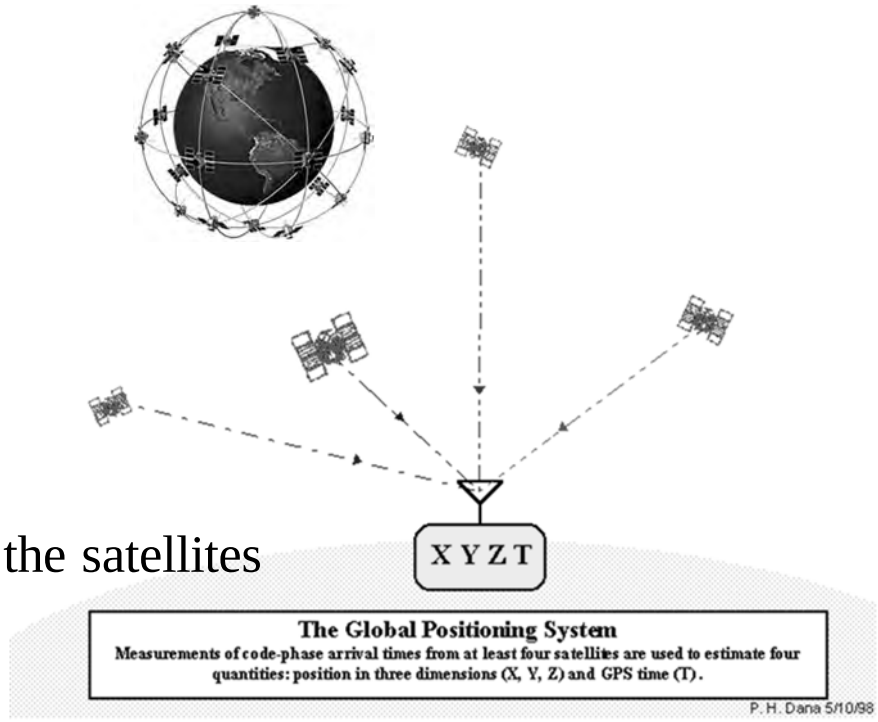
Full Autonomous Driving

Require a **3D localized maps** (Google and Baidu !)with high levels of detail, down to centimeter accuracy… daily updated.

GPS is a receiver,

10+ meter accuracy (at least 3 satellites are needed)

Associated with a MAP

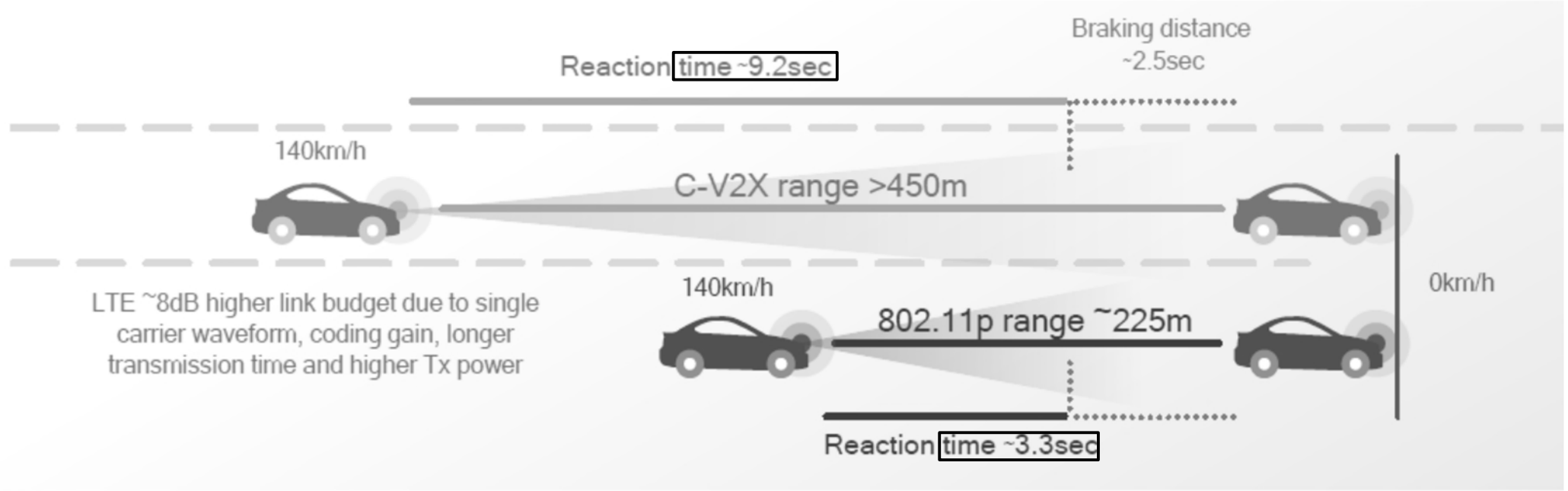


Localization process :

1. The receiver picks up the signals from the satellites
2. Uses the signal travel time to calculate distances to the satellites
3. Triangulates to determine position of the receiver

GPS : L1 (1 575,42 MHz), L2 (1 227,60 MHz) et L5 (1176,45 MHz) ;

V2x performances



Highest challenge : Match budget of time in a highway situation (V2V-DSRC).
- Need to decrease time spent in the different Com stack layers (Lightweight messages encapsulation vs TCP/IP used for V2I).

802.11p
- Useful for Short range (City) & LTE
- Highway situation.

5G : ~5ms end to end

With incoming LTE & 5G technology, latency requirements will be matched !

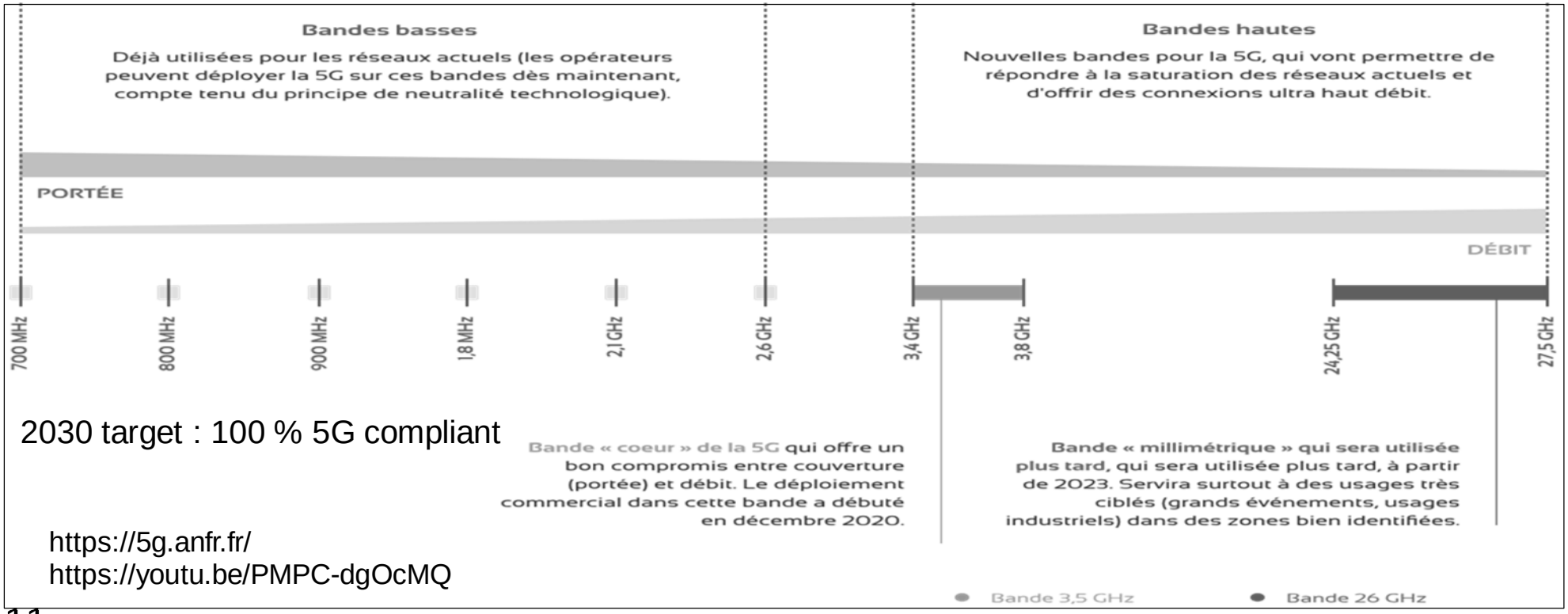
5G Cellular - Basics

Motivation : Bandwith x 10 and Latency / 10 (vs 4G)

Timeline (France, au 31/12/22) :

	Bouygues Telecom	Free Mobile	Orange	SFR
Nombre de sites 5G	**9 645**	**16 356**	**5 597**	**8 404**
Progression des sites depuis le 30/09/2022	+931	+1114	+915	+1519
dont sites équipés en bandes :				
700 & 800 MHz	0	16 270	1	0
1800 & 2100 MHz	9 358	0	310	2 783
3500 MHz	**5 085**	**4 045**	**5 470**	**5 621**

Source : AR



2030 target : 100 % 5G compliant

https://5g.anfr.fr/
https://youtu.be/PMPC-dgOcMQ

WiFi - Basics

WiFi means : Wireless Fidelity. It's based on the IEEE 802.11 family of standards.

2 bands : (crowded and congested) 2,4Ghz and 5Ghz.

Wireless network use radio waves rather than transmitting signals through cables.
2 Modes :

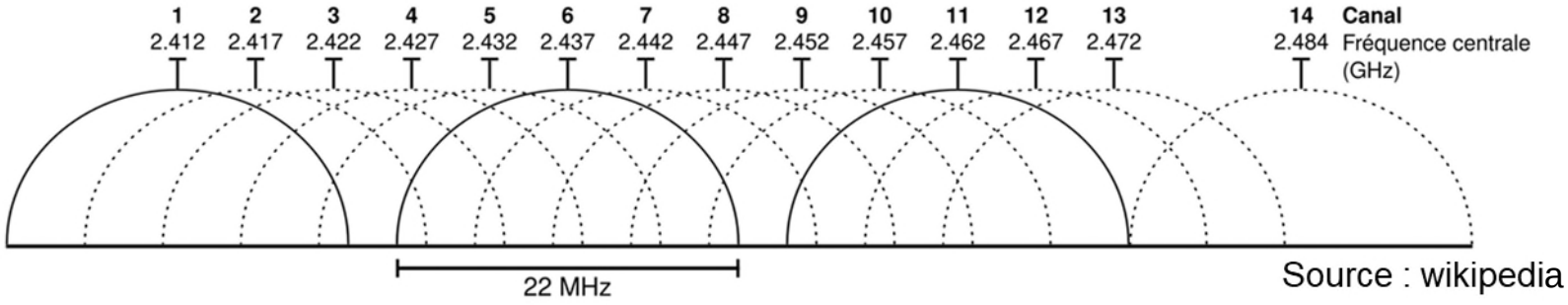
- ✓ AD HOC : P2PCommunication (Pc to Pc) w/o access point,
- ✓ Infrastructure : Communication via an A.P

The name of the network, known as its service set identifier (SSID).

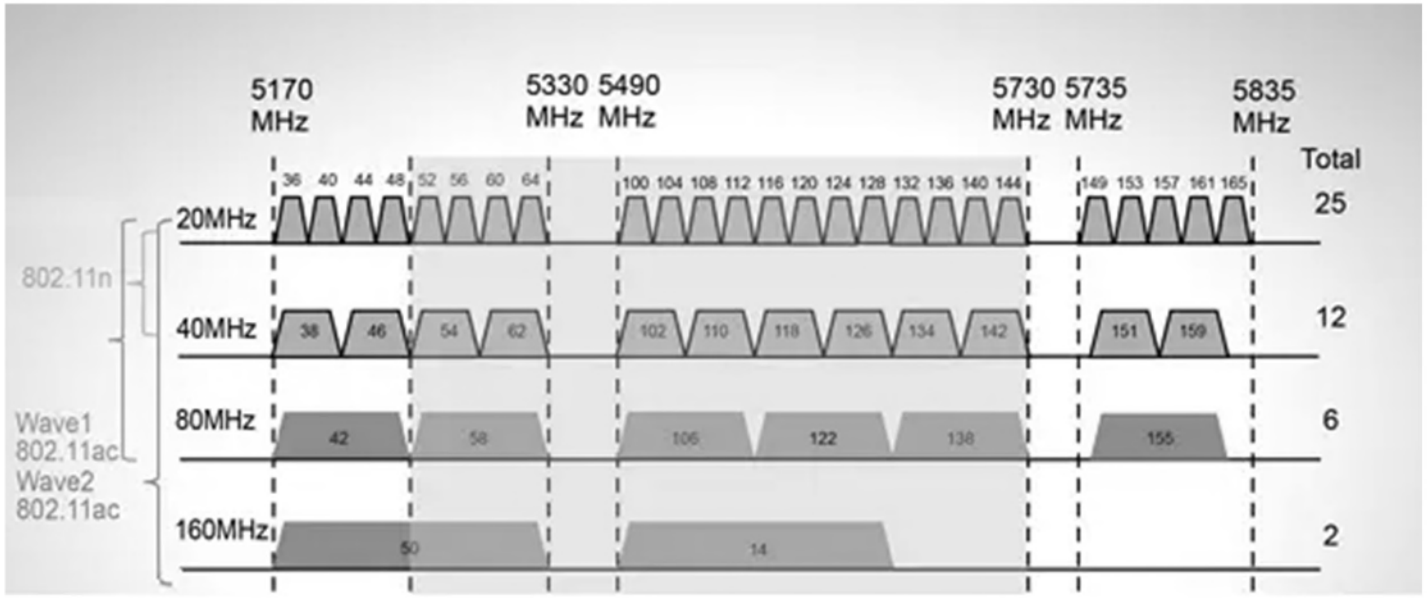
Standard	Année	Fréquence	Vitesse	Taille de canal
802.11	1997	2,4GHz	2Mbits	22MHz
802.11a	1999	5GHz	54Mbits	20Mhz
802.11b	1999	2,4GHz	11Mbits	22MHz
802.11g	2003	2,4GHz	54Mbits	20MHz
802.11n	2009	2,4GHz/5GHz	450Mbits	20/40MHz
802.11ac	2014	5GHz	1300Mbits	20/40/80/160MHz

WiFi - Channels

Each channel overlaps with two or more other channels. Preferable channels for 2.4GHz are 1, 6, and 11 as they are not overlapped.



Source : wikipedia



Although 5 GHz is referred to as a single band, it is actually composed of several fragments, each with its own rules governing the maximum transmitting power, they can be used externally or the obligation to use control mechanisms in order not to interfere with other services.

For the 5 GHz frequency, you can also choose a 20 MHz channel as a 40 MHz channel, but it is more advantageous to use the latter. With such a WiFi channel, it is however better to have separate channels. An 8-channel separation for each wireless transmitter is recommended.

In some cases the bandwidth is doubled to 40 MHz or tripled to 80 MHz. This will require a channel spacing of 8, 42 MHz or 12.

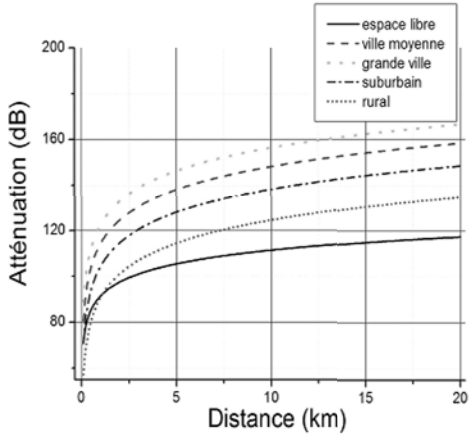
Wifi – 5 GHz focus

- ✓The first 4 channels (36, 40, 44 and 48) are best if you have no neighbors. They do not have DFS, TPC and are not disturbed by radar. For this reason, they are the most used and if there are already many networks, the speed you will get will be less, because you share it with the neighbors.
- ✓The second group of 4 channels (52, 56.60 and 64) are DFS (Dynamic Frequency Selection).
- ✓Channel 100 : more power and outdoor use are allowed.
- ✓Channels 120, 124 and 128 are where DFS regulation is stricter, which is why many routers do not even support them.
- ✓Channels 116, 132, 136 and 140 are not used much because they cannot be grouped together to create larger channels. They are a good option if the spectrum is very saturated in your area.

DFS is a function of using the 5 GHz Wi-Fi frequencies that are usually reserved for radars, such as military radars, satellite communications and weather radars.

Friis formula

Free Space Path Loss



ACKSYS COMMUNICATIONS & SYSTEMS

Wireless link budget calculator

Input:			Compute:	Units:
Frequency:	5900 MHz		Distance	Km
Transmit Power:	30 dBm		Transmit Power	Miles
Cable 1 loss:	1,4 dB		Fade Margin	
Antenna 1 gain:	11 dBi			
Distance		Output:		
Antenna 2 gain:	11 dBi	Distance:	3,7 Km	
Cable 2 loss:	1,4 dB	Free Space Loss:	119,2 dB	
Receiver Sensitivity:	-85 dBm	Receive Signal Strength:	-70,0 dBm	
Fade Margin:	15 dB			

Cable Loss Calculator

Cable Type:	LMR240	Loss per 100 meters: (at 5900 MHz)	67,4 dB
Cable Length:	1 meters		
No. of Connectors:	4	Total Cable Loss:	1,7 dB

Receive Aperture

Frequency Related:

-40dB in the first meter (2.4GHz)

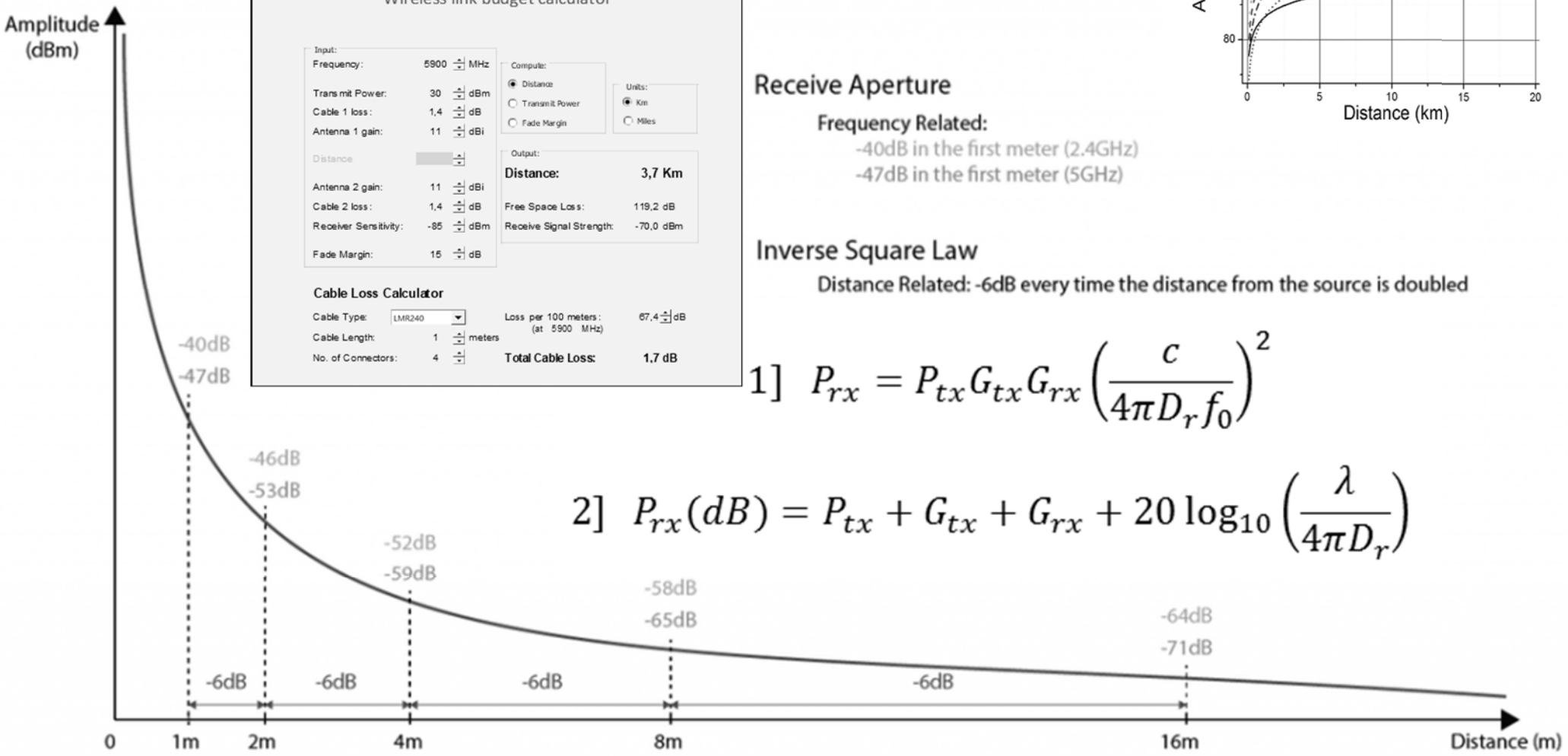
-47dB in the first meter (5GHz)

Inverse Square Law

Distance Related: -6dB every time the distance from the source is doubled

1] $$P_{rx} = P_{tx} G_{tx} G_{rx} \left(\frac{c}{4\pi D_r f_0} \right)^2$$

2] $$P_{rx}(dB) = P_{tx} + G_{tx} + G_{rx} + 20 \log_{10} \left(\frac{\lambda}{4\pi D_r} \right)$$



At 5.9Ghz, first 100m free space loss = 87dBm. Calculator.

And we need to take into account Fading loss (25dBm), Vhcl masking effect, wearing,… (>20dBm more).

Wifi – RSSI & Access

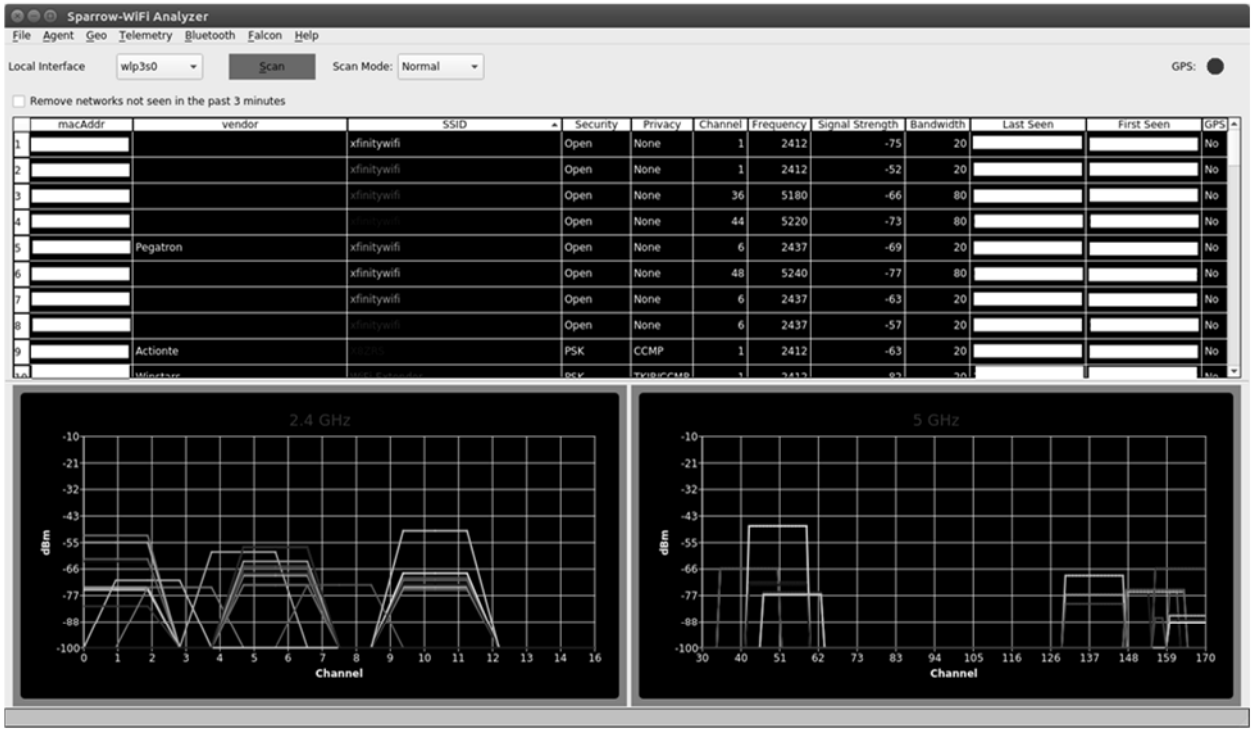
RSSI (Received Signal Strength Indicator) is a common measurement, for engineers, let's consider only dBm (mw).
Order of magnitude :

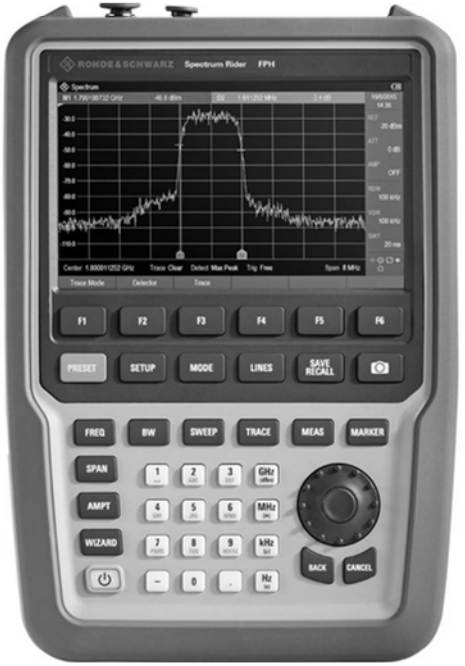
Signal strenght	-30dBm	-60dBm	-70dBm	-80dBm	-90dBm
Evaluation	Top !	Very good	Ok	Not Good	Unusable

Access methods

- ✓DCF CSMA/CA (mandatory)
  - Collision avoidance via exponential back-off
  - Minimum distance (IFS) between consecutive packets
  - ACK packet for acknowledgments (not for broadcasts)
- ✓DCF with RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- ✓PCF (optional) : Access point polls terminals according to a list

Spectrum analysis





A bit of practice !

V2X Consortium - History

First (V2x) studies appeared at the beginning of 80’s in Japan (ex: Association of Electronic Technology for Automobile Traffic and Driving) focused on passenger journey and freight. These studies have pushed forward technologies for autonomous vehicle, smart infrastructure road, communications set-up,…

Several government institutions, all over the world, have managed studies with world wide project where many research labs was involved.

In U.S, the Intelligent Transportation Society of America is in charge to promote, develop and coordinate studies. US government has also established NAHSC consortium.

In Europe, first project was Prometheus (1986), first major project in charge of V2x communications. This project has been ended in 1995. Current project : Car2Car.

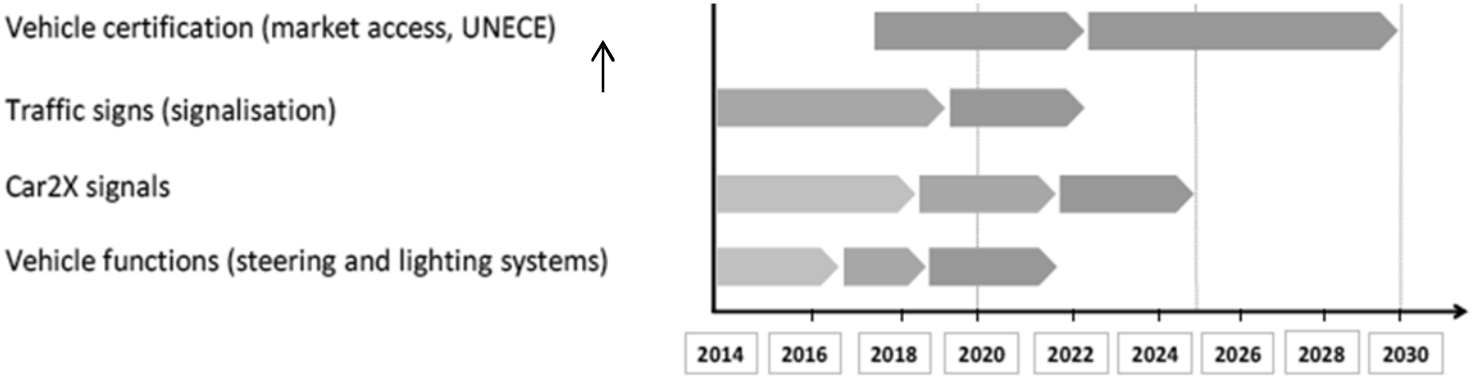
Standardization is the only path to master complexity and mitigate dvpt cost.

Consortium – Car2Car

Car2Car communication consortium has been launched by six Europeans car makers, open for suppliers, research centers and partnership. The target of Car2Car consortium is to improve road safety, traffic flow optimization,… by means of smart infrastructure and connected vehicle (+/- autonomous).

Car2Car communication consortium main's missions are :

- ✓ Open European standard definition for Wireless based V2V communications,
- ✓ Proof of concept with V2Vprototypes and demonstrators for safety road apps,
- ✓ Lobbying to get a dedicated spectrum bandwidth for Car2Car applications,
- ✓ Promote deployment strategy to match economical target and lead to major market spread



Techno is ready but… Deployment need a global political will (Framework investments)

Consortium - Car2x Technology Developments (EU)

Information exchange rules in E.U to enhance safety & optimizing traffic flow.

It belongs on :

- ✓ Standardized messages over the air,
- ✓ V2V & V2I exchanges (ITS*-S stations)

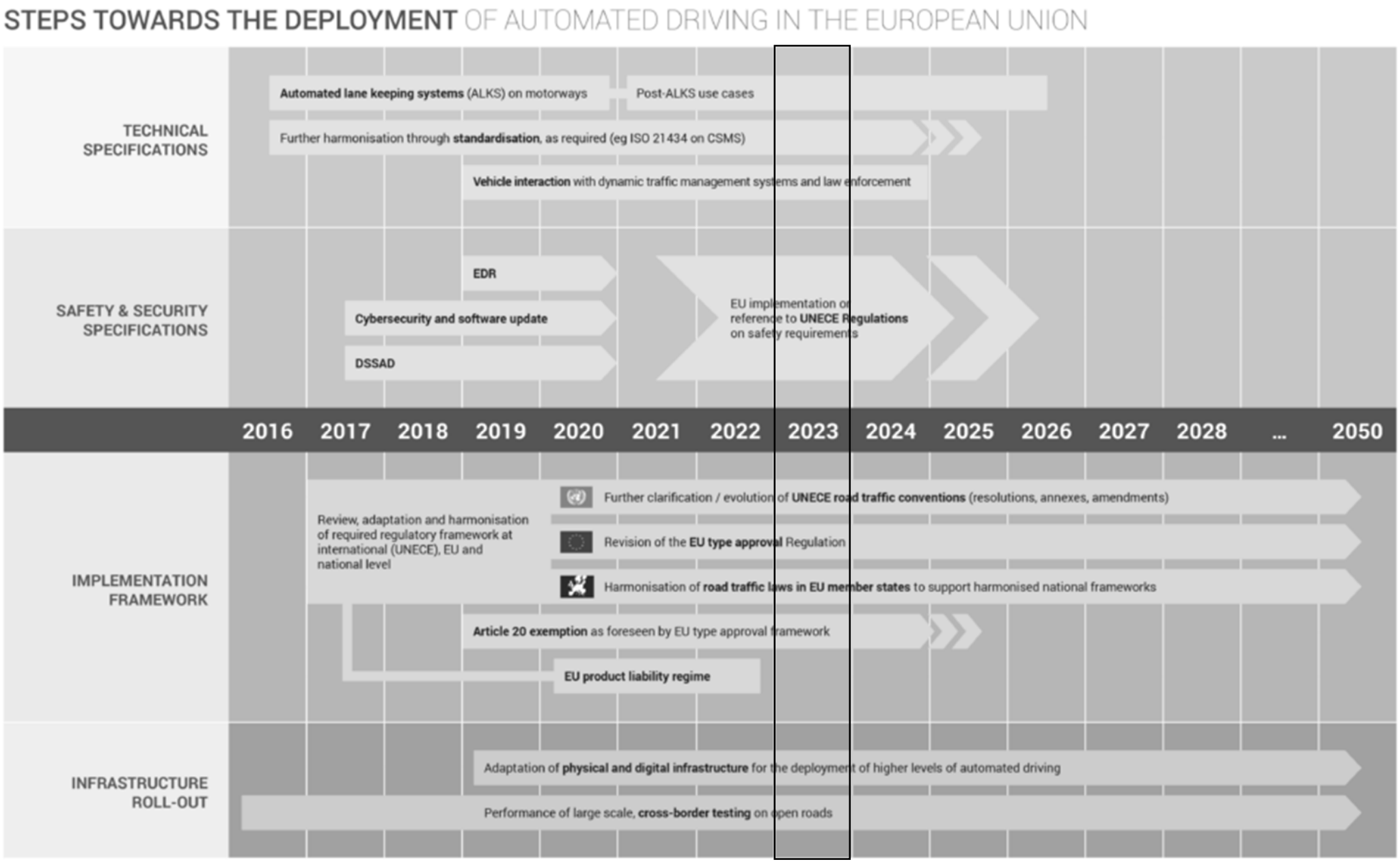
*: Intelligent Transport Systems

The European Institute for Telecommunication Standards (ETSI) has already specified the CAM and DENM messages*.

*: C*ooperative Awareness Message* (CAM)
Decentralized Environmental Notification Message (DENM)

The V2X technologies at the basis of V2X efforts are considering both ETSI-ITS-G5 (which is based on IEEE 802.11p/DSRC) and cellular V2X (both 4G and 5G).

Consortium - Car2x Technology Developments (EU)



V2x - National Highway Traffic Safety Administration (NHTSA)

The **National Highway Traffic Safety Administration (NHTSA)** is an agency of the Executive Branch of the U.S. government, part of the Department of Transportation. It describes its mission as "Save lives, prevent injuries, reduce vehicle-related crashes (Wikipedia).

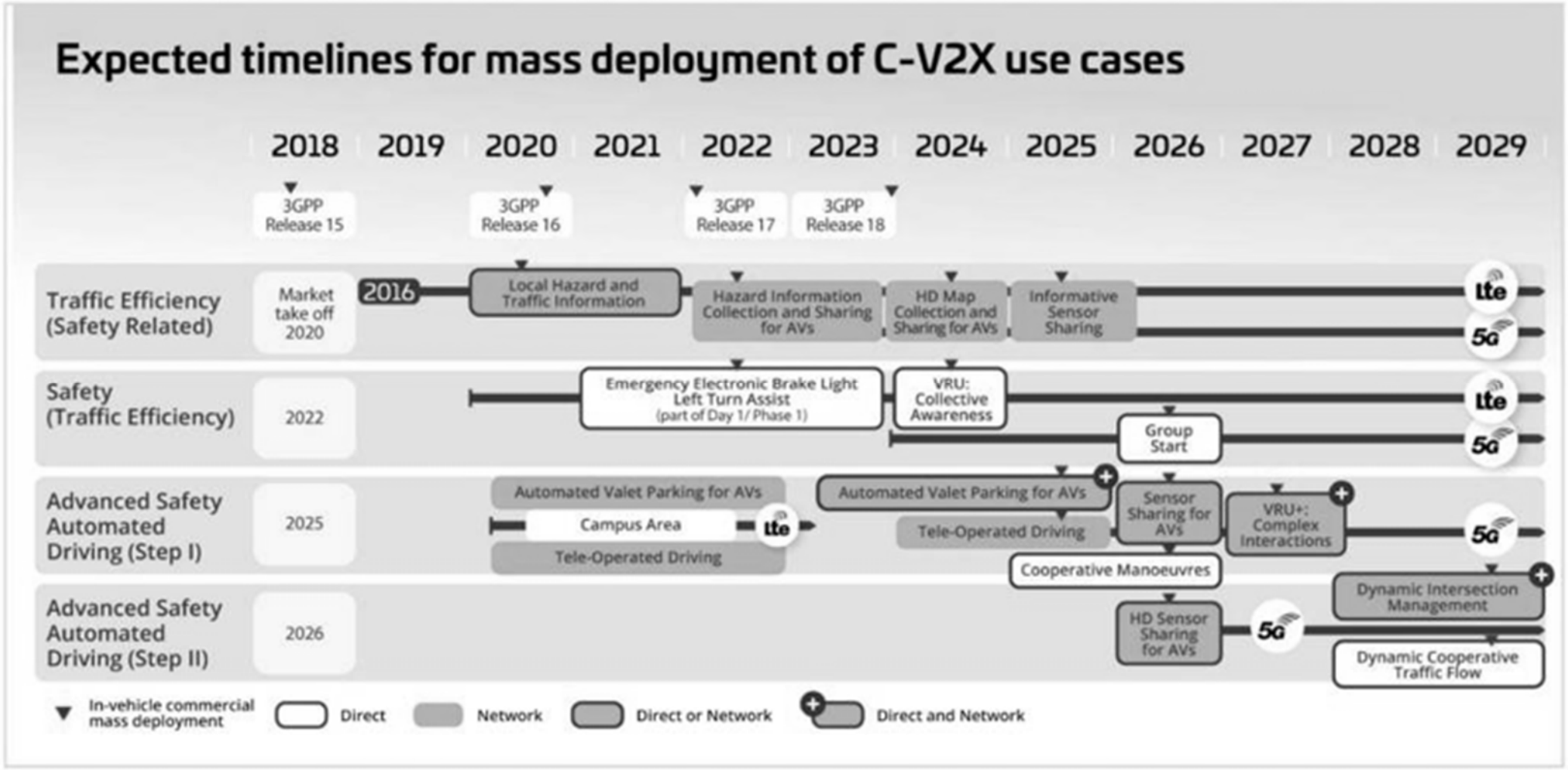
2016 : FMVSS mandated for V2V communications.

- ✓NHTSA expectations was : Beginning in 2021, final rules adopted in 2022 and phase-in completed in 2024 with 100 percent of all new light vehicles

April 24, 2023, the FCC granted a joint waiver allowing deployment of C-V2X technology (Link : https://en.wikipedia.org/wiki/Vehicle-to-everything)

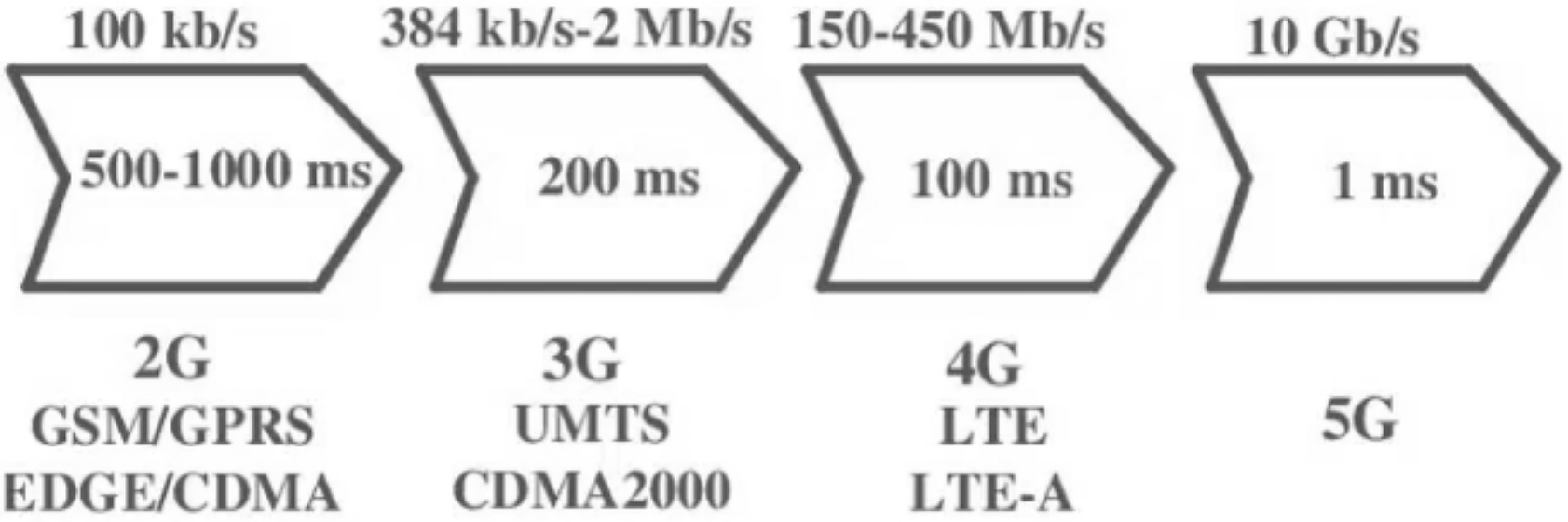
V2x – 5G Automotive Association : C-V2X

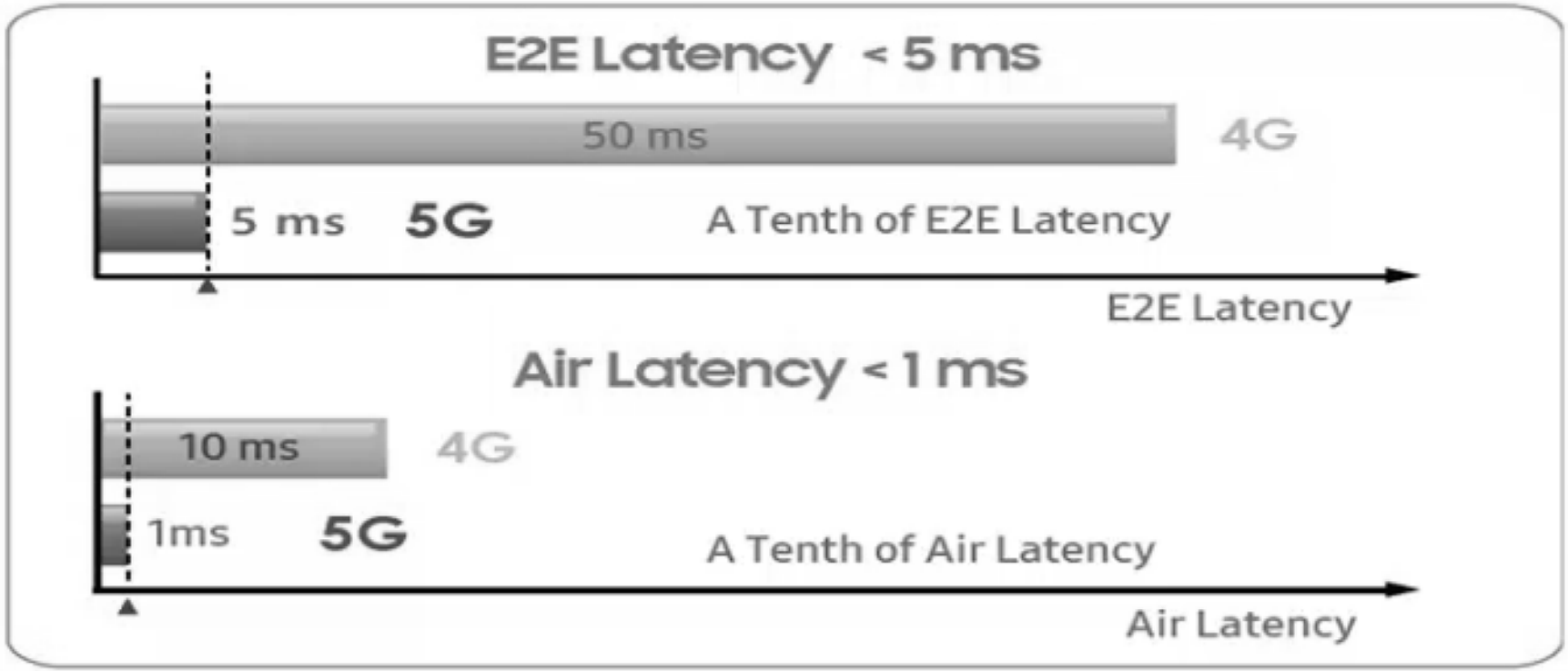
5GAA's Expected Timelines for Mass Deployment of C-V2X Use Cases



Source: 5GAA

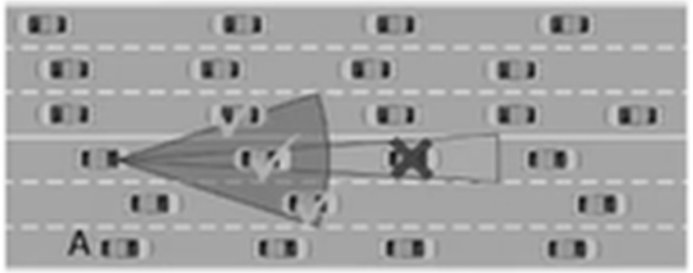
4G/5G Cellular - Latency

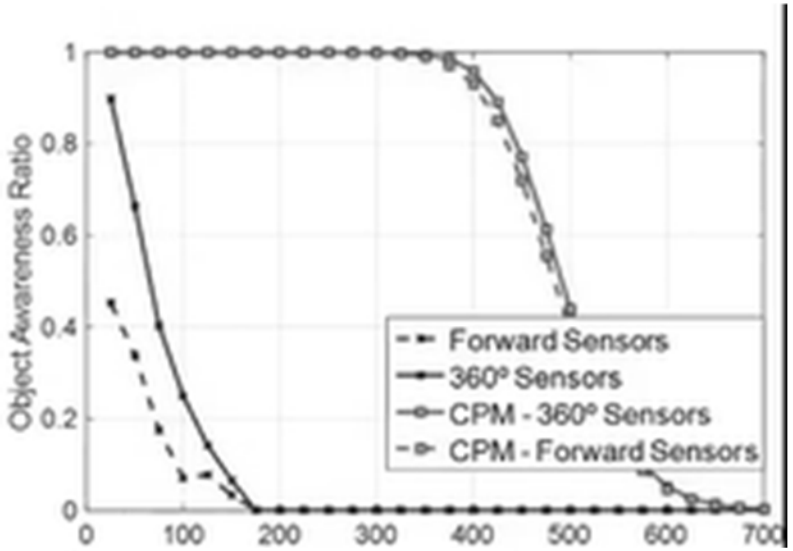




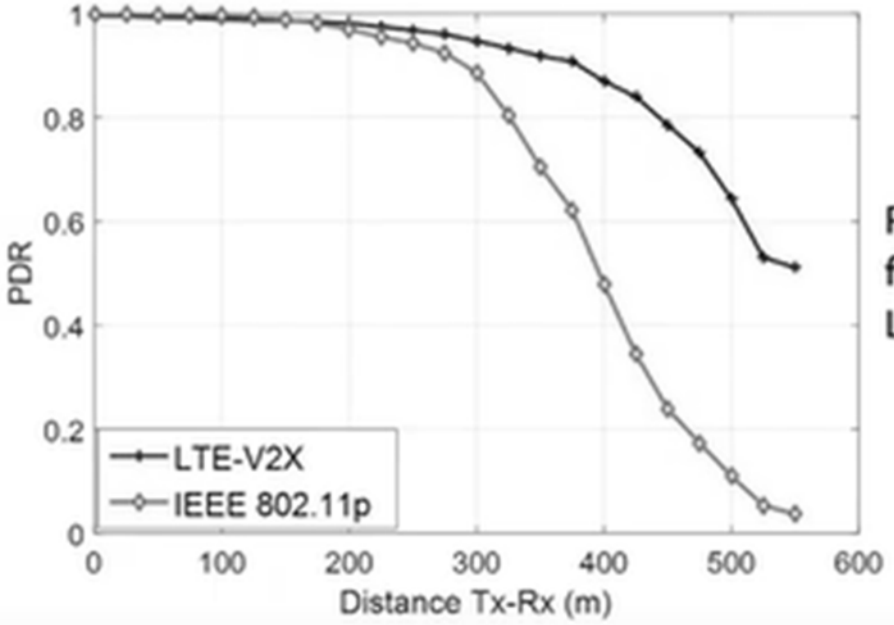
Latency : Sensors vs Communication

Only vehicles in Line of Sight can be detected





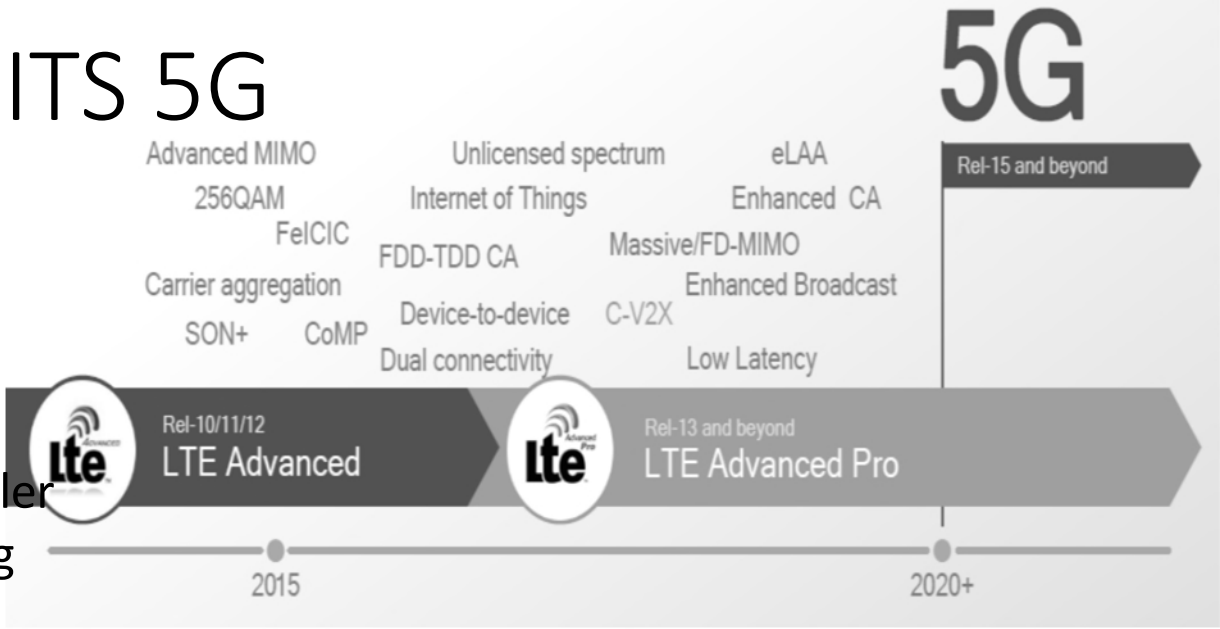
- Packet Delivery Ratio (system-level analysis)
  - Broadcast of CAM (Cooperative Awareness Messages) in highways



Periodic traffic (200ms) of fixed size (190bytes)
Low channel load (CBR ~0.1)

Techno – Cellular-ITS 5G

5G techno is compliant with connected vehicle needs, first components : 2019. The 5GAA, whose founding members include Ericsson, Intel, Huawei, Nokia, Qualcomm, Audi, BMW Group and Daimler AG, prefers Cellular Vehicle-to-Everything (Cellular-V2X) for V2V safety.



Source: Strategy analytics, Jan 16

- 5G techno has the capabilities to match V2x requirements (Release 16)
- 60% Cellular penetration in new light vehicle sales by 2021 (source : Strategy analytics, Jan 16)

Standardization In France : Towards 5G (Ericsson, Orange, Qualcomm, PSA Group).

Very good performances will be reachable but…not before few years (for 5G)

C-V2x support direct D2D communication (PC5), called Sidelink, no SIM required ! GPS time reference is required.

V2X based on wifi - DSRC

DSRC is a short to medium range comm. service, planned to replace the 802.11 wireless standards :

- ✓ 802.11 a : Operates at 5 GHz
- ✓ 802.11 b/g : Operates at 2.4 GHz, Bandwidth of 11/52 Mbps respectively – Lot of traffic.
- ✓ 802.11p : Wireless Access for the Vehicular Environment

Defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications

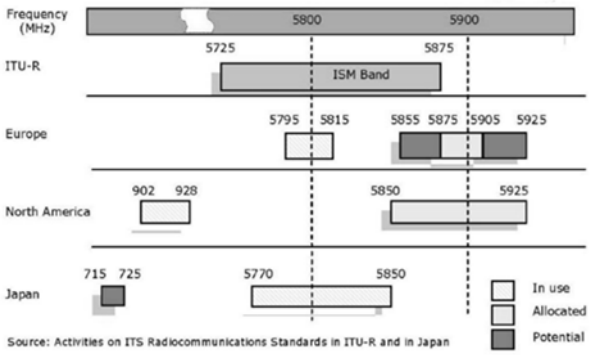
FCC has authorized 75 MHz of spectrum from 5.850 to 5.925 GHz for DSRC Standardization, Interoperability.

- ✓ Europe and Japan use the 5.8 GHz spectrum
- ✓ European organization – CEN – Different Physical and MAC layer standards
- ✓ Japan – ARIB T55

Applicable for both Public and Private operations and both Infrastructure to vehicle and vehicle to vehicle communication. Features :

- ✓ Range – 300m
- ✓ Data Rate – 6 to 27 Mbps (with minimal latency)
- ✓ Channels – 7 Licensed Channels

Techno - 802.11p



Initiated in US for DSRC, techno is available in the market, and is implemented and operational in both Vehicular On-Board Units (OBU) and Road Site Systems (RS **U**nits).
This techno is Wi-Fi based, Adapted for latency-critical V2X communications in the 5.9GHz band. Published in 2010.

Standards :

- 1609 Wireless Access in Vehicular Environment (WAVE) protocol for U.S,
- TC-ITS for the European Telecommunications Standards Institute (ETSI).

ITS defines a set of protocols and parameters that are defined in that document called ITS-G5, operating in the frequency ranges:

- ITS-G5A: 5 875 GHz to 5 905 GHz dedicated to ITS for safety related applications.
- ITS-G5B: 5 855 GHz to 5 875 GHz dedicated to ITS non- safety applications.
- ITS-G5C: 5 470 GHz to 5 725 GHz.

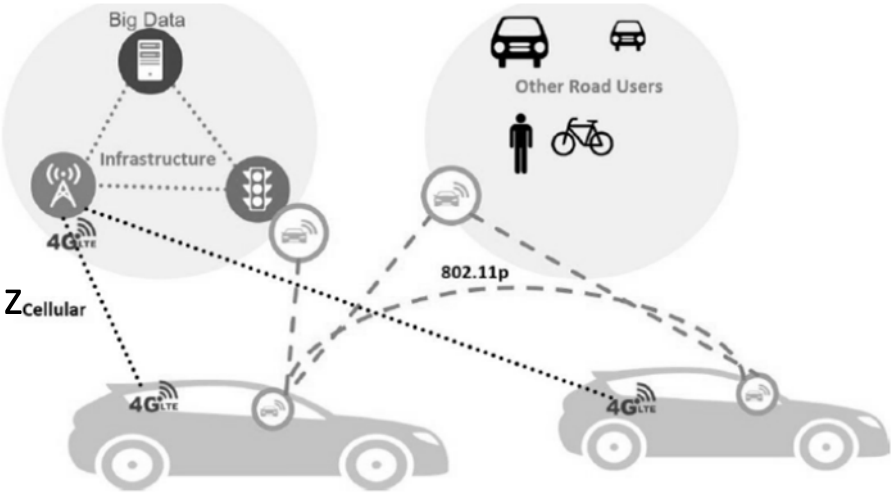
Techno - 802.11p

Motivation

"Relatively short-range, high-bandwidth, low latency communications technology" for traffic safety.

FCC has allocated 75 MHz of bandwidth around 5.9 GHz for V2x, it takes two forms:

- Vehicle-to-vehicle (V2V)
- vehicle-to-roadside communications/Infra (V2R/I)



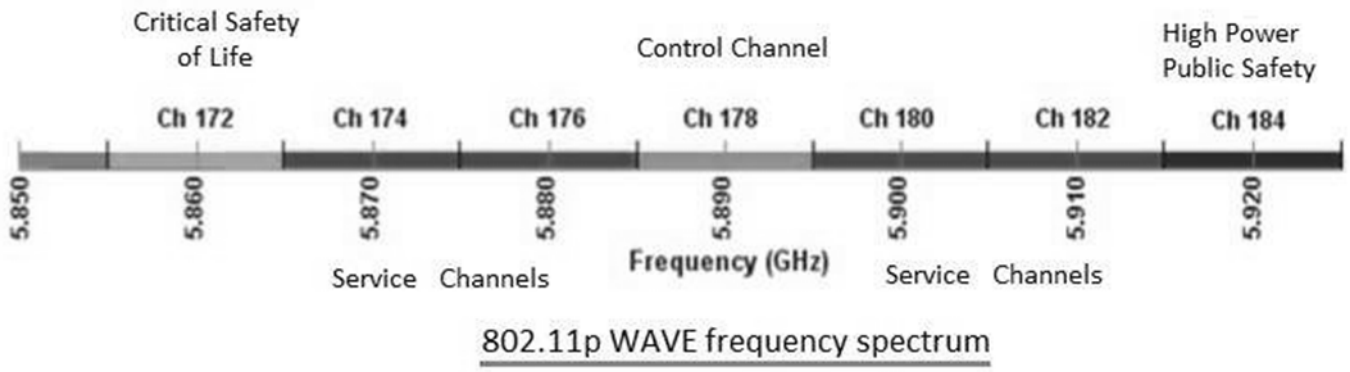
Supporting vehicular wireless communications capabilities within a 1000m range at highway speeds (300m min)

- ✓ Standardization efforts include IEEE 802.11p
- ✓ IEEE 802.11p also known as Wireless Access in Vehicular Environment (WAVE)
- ✓ Relies on location and timing information from GPS

Vehicles will be equipped with On Board Equipment (OBE) to collect sensor information and relay to neighboring vehicles

IEEE 802.11p - Physical Layer

Channels splitting



802.11p WAVE frequency spectrum

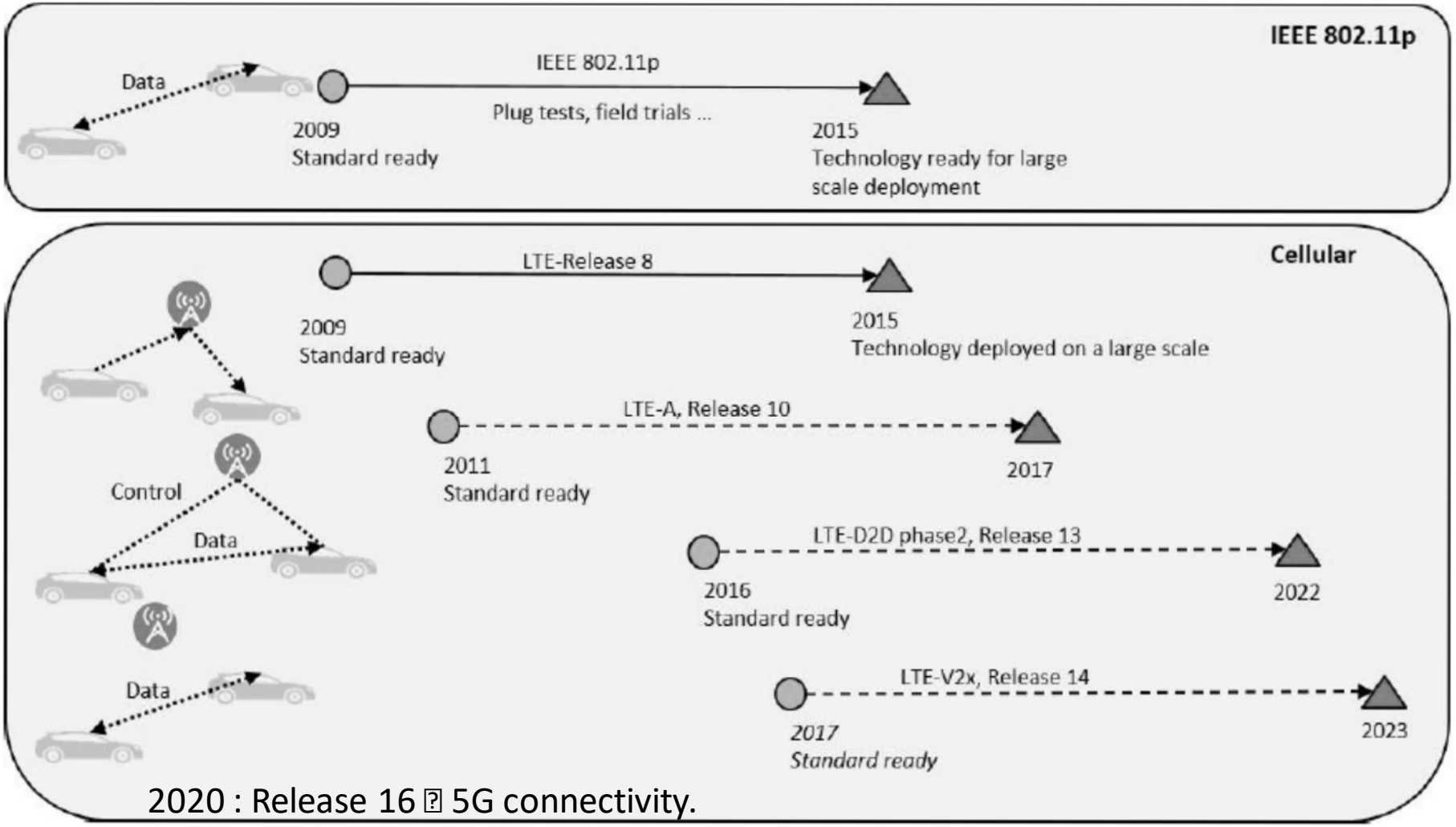
Channels available for IEEE 802.11p

Negotiation for service channels is done on control channel

- The device listens to the channel before sending a packet and sends a packet only if the channel is clear.

Standard is established…but no standard activities running to enhance performances

IEEE 802.11p vs Cellular LTE Roadmap



Wifi 6 vs 5G

Both 5G & WiFi6 have been designed to offer better performances and increase network capacity (ability to connect more devices)

WiFi is indoor oriented, optimized for capacity (throughput)

5G is outdoor oriented, optimized for coverage

Wi-Fi 6 uses unlicensed spectrum, However, 5G and LTE networks typically are managed by operators and use a dedicated, licensed spectrum that requires subscription fees to access.

Timeline for Wi-Fi 6 and 5G

- By mid-2019 several vendors, including Cisco, will have Wi-Fi 6 access points available.

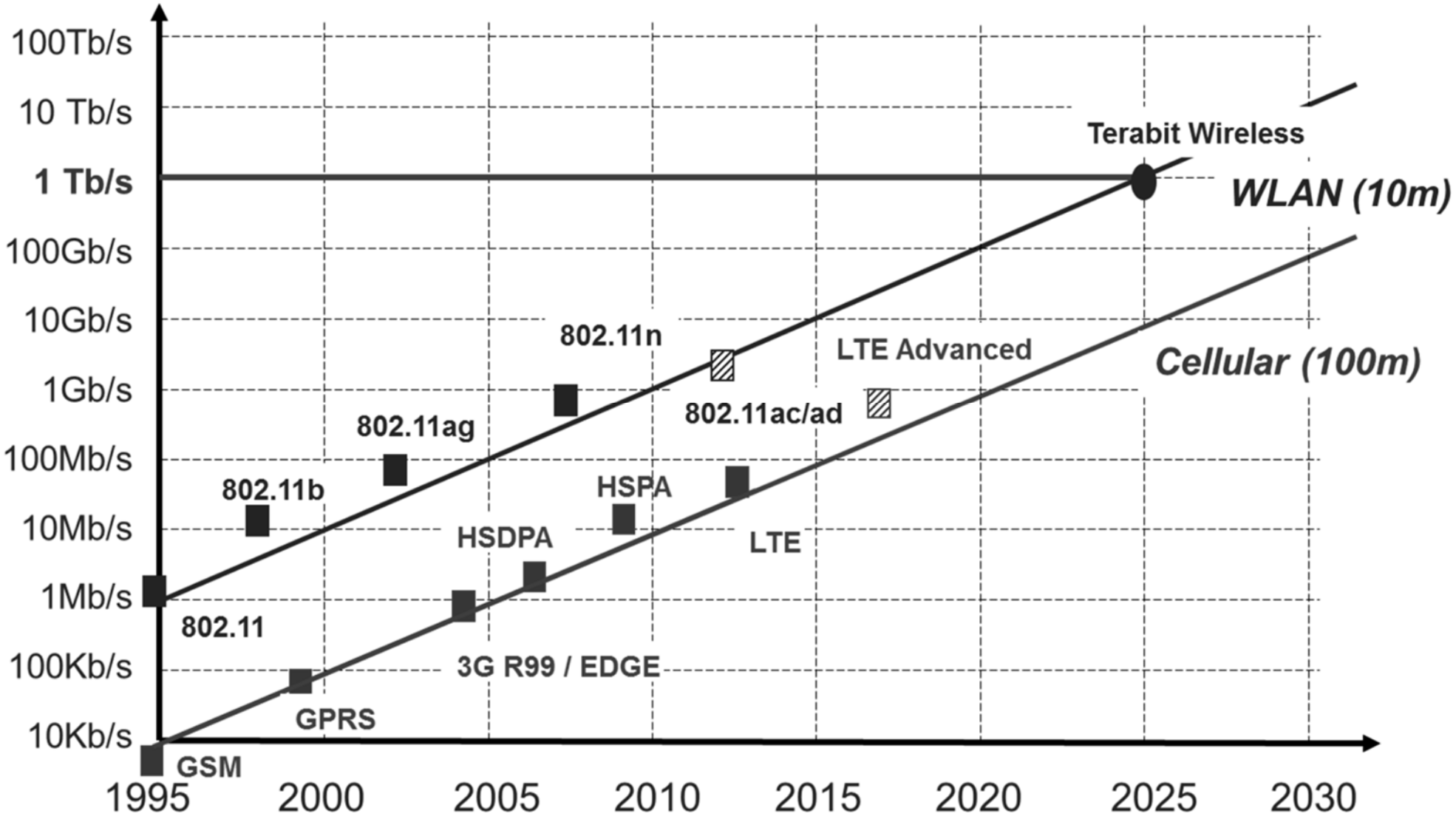
5G networks and services will be deployed in stages over the next several years.
5G will first be used for fixed wireless applications: residential and branch backhaul.

- Starting in mid-2019 and continuing into 2020, service providers will start offering 5G service to select cities.
- And around 2021, 5G service will become common in many big cities in the U.S, EMEAR, Japan, and China, with important rollouts lasting through 2024.

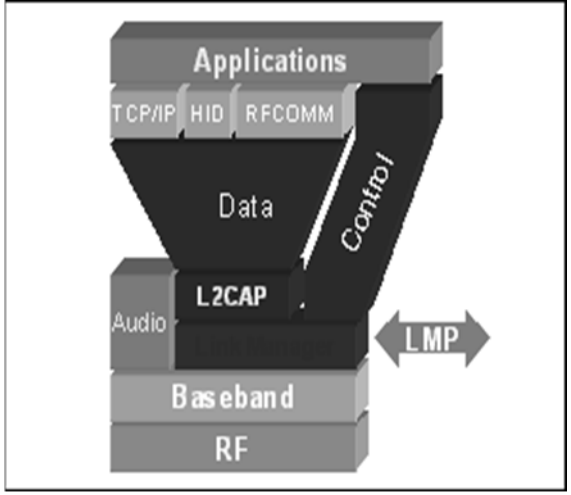
Wifi 6 vs 5G

Item	Wi-Fi 6	5G
Modulation	1024QAM	256QAM
MIMO	8T8R/12T12R-8 streams	Indoor: 4T4R-4 streams Outdoor: 64T64R-16 streams
Typical Frequency Bandwidth	Campus: 80 MHz Household: 160 MHz	100 MHz (in total)
Frequency	Free of charge, no limitation	Limited, controlled by carriers
Per-user rate	100Mbps	100Mbps
Interference	Unlicensed, exist interferences	Licensed, no interference
Terminal Types	Various enterprise terminals (PCs, projectors, monitoring devices, etc.)	Mainly mobile terminals, few enterprise devices embedded with SIM cards
Security	Guaranteed security	High air interface security
Management	Enterprise management personnel	Carriers
Deployment Period	SME: within one month depending on the specific size Large-sized enterprise: 2-3 months	LAN: 4-5 months WAN: 1-1.5 years

Cellular vs Wifi



Connected vehicle - Bluetooth



Bluetooth was developed (~1998) to connect personal equipment (like previous IrDA) :

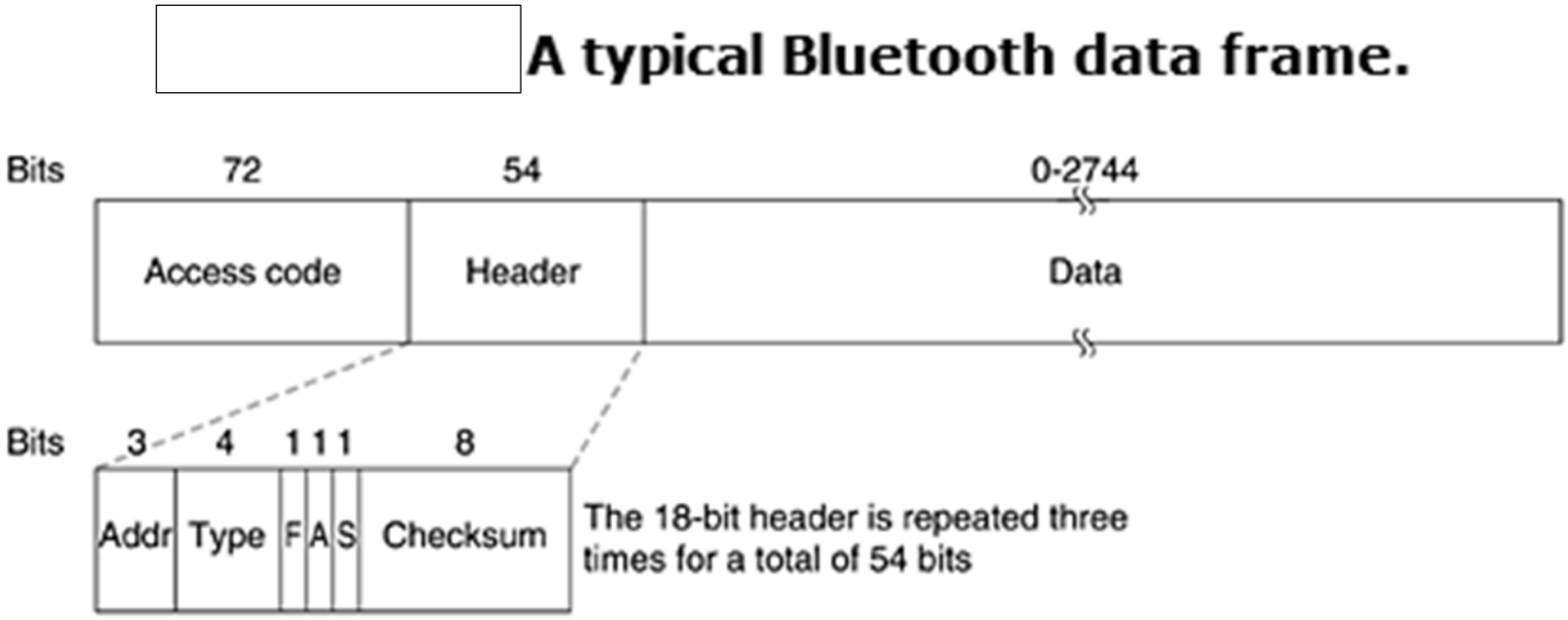
- Easy to use,
- cost efficient,
- Ad hoc fashion (no infrastructure)
- Asynchronous (data) and synchronous (voice) available

During exchanges (piconet) one node is the master, others are slaves. Range : ~10 meters (battery saving).

Support authentication and encryption

Data rates – 721kbps , using the 2.45Ghz radio frequency band

The Bluetooth Frame Structure

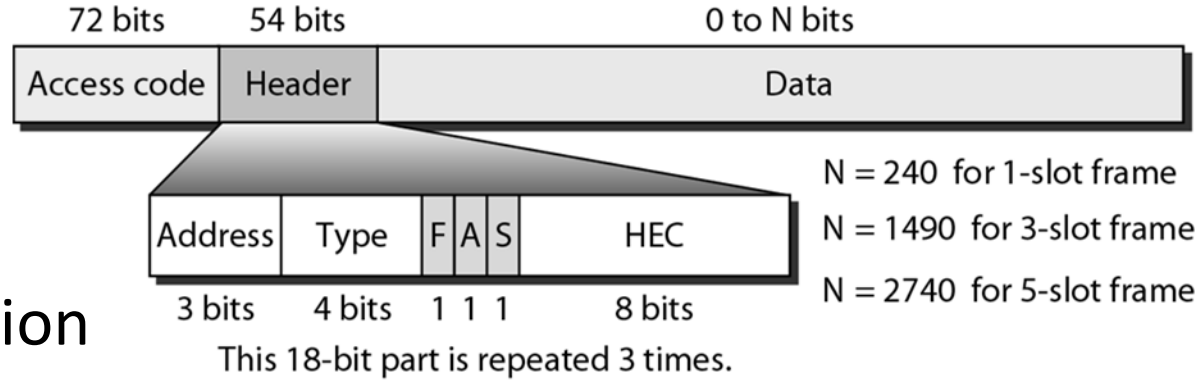


The Address field identifies which of the eight active devices the frame is intended for. The Type field identifies the frame type (ACL, SCO), the type of error correction used in the data field, and how many slots long the frame is.

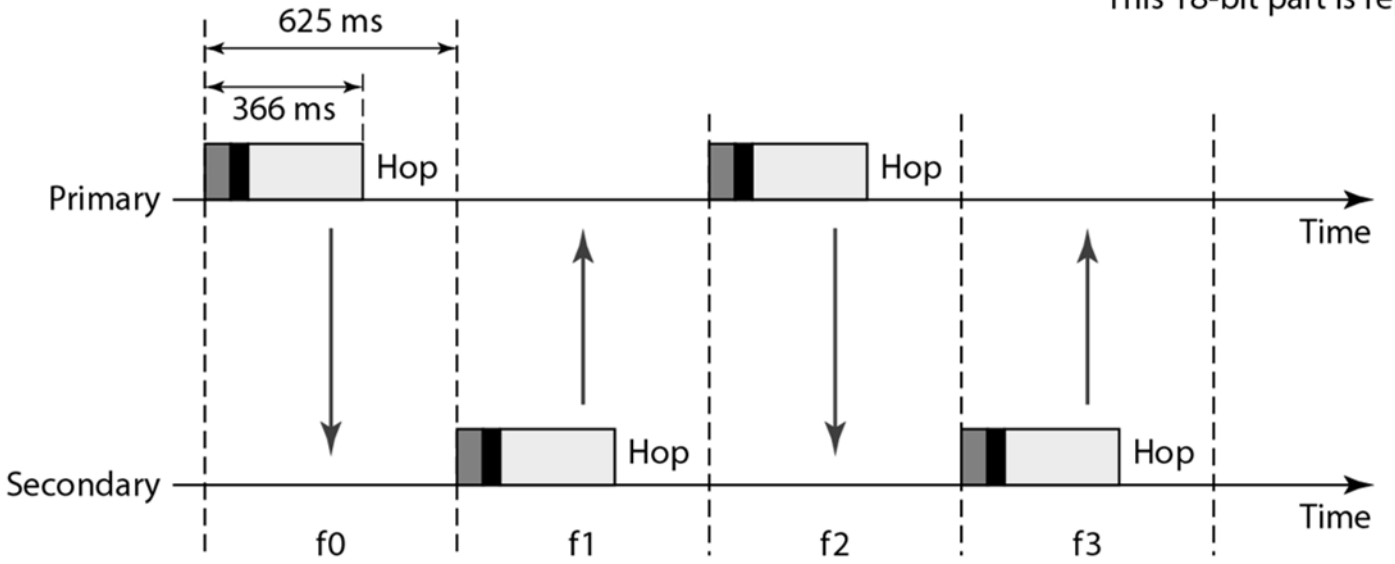
The Flow bit is asserted by a slave when its buffer is full and cannot receive any more data. This is a primitive form of flow control.

The Acknowledgement bit is used to piggyback an ACK onto a frame. The Sequence bit is used to number the frames to detect retransmissions.

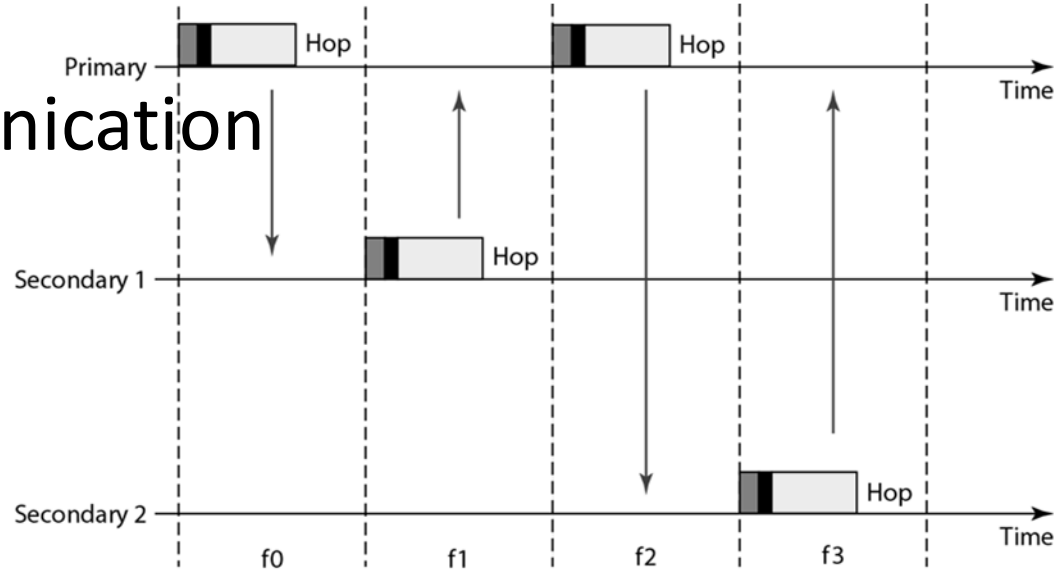
Bluetooth Hopping



Single-secondary communication



Multiple-secondary communication



Techno – Optical Transmission

Brevet UVSQ/INRETS (2009)

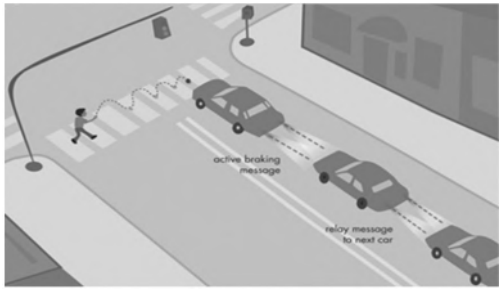
High rate communication technology, Vehicle to Vehicle and vehicle to Infrastructure, it belongs on light LED courant modulation in front & rear of vehicle.

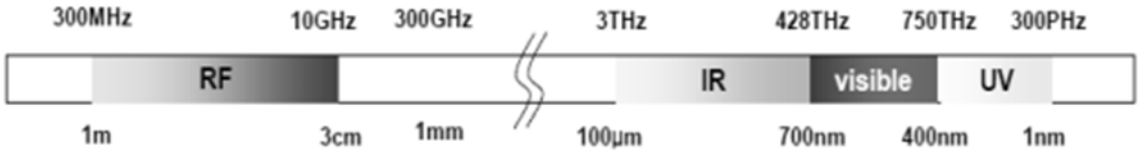
Principle Use LED technology (more & more popular for light vehicle equipment) to sent data flow (LiFi). Radio techno are more efficient in term of range but more sensible to noise & number of transactions.

Figure 2 – Séquence de données pour transmission asynchrone (longueur standarde : 600 bits/séquence)

Carrier : 10 to 15kHz
Range : 20 to 50m (depends on Sun condition, scattering, …)
Baud rate : ~10kbit/s

Advantages : Robust (perturbations), low cost, useful for platooning.
Drawback : Short range, narrow field of Tx/Rx





Source: www.ieee802.org/15

Connected car : Target for Hackers ?

Which of the following breach protection use cases will be a primary focus for your organization over the next year?

63% Discover and patch vulnerabilities in apps and systems

54% Prevention of zero-day malware execution (including ransomware, fileless, exploits, etc.)

17% Detection of advanced threats already active in the environment

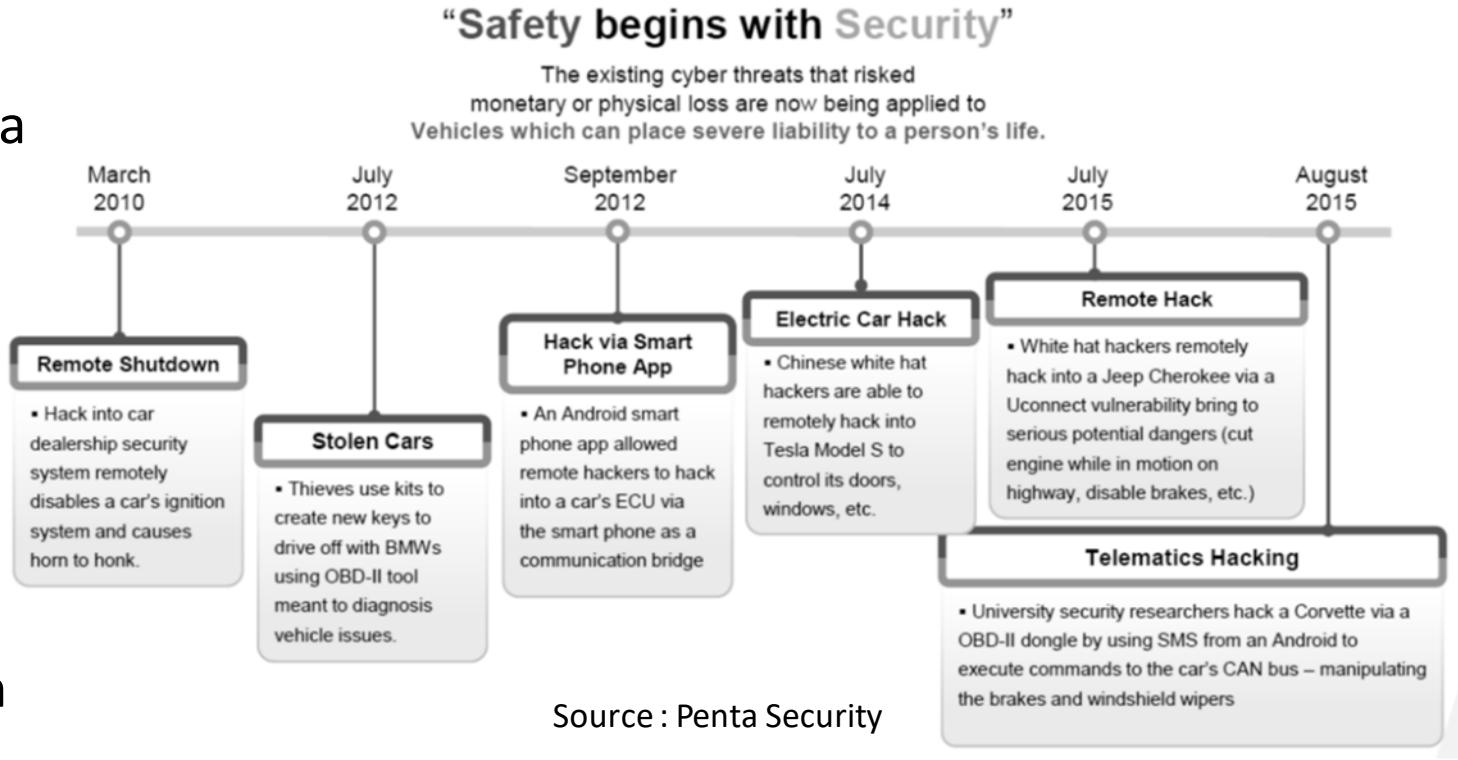
Cynet launched in December 2019 the State of Breach Protection 2020 Survey

just published a paper titled "Comprehensive Experimental Analyses of Automotive Attack Surfaces". Behind that dry title is a very exciting research study. ..They bought a modern reasonably-priced car with lots of fancy features, including a built-in cellular phone interface, and did a serious reverse-engineering exercise to determine whether it had any security vulnerabilities.

Safety issues

Software

To avoid a car “crash” and a costly recall, automotive suppliers should be continually vetting their code to ensure its safety and impenetrability. Governments around the world have begun to help the automotive industry in establishing these practices.



Source : Penta Security

Whatever number of modules (and SW dvpt team),
SW cannot be developed independently and integrated later, even if the interfaces are well defined.

- Versioning & configuration tools for version are mandatory to achieve expected level of quality & maturity
- Validation & test effort : Snake analysis, testing trap, automated testing
  Hacking
- Telematics Hacking (Done by external Network, ex : 3G),
- Malware injection done through USB/SD port,
- Direct access through E-OBD connector (CAN – Packet injection)

Security

To secure the Connected Car, external interfaces

- ✓ Encrypting the data ,
- ✓ Authenticating the messages that are exchanged to protect their authenticity and integrity.
- ✓ The interfaces need to prevent unauthorized access. All access points in the car should be equipped with reasonable measures to protect against hacking attacks, including isolation of critical software systems and evaluated using best security practices, such as penetration testing

This involves processes such as machine-to-machine authentication to check that you are communicating with a known or authorized device.

Hacking mitigation : The vehicle should be equipped with technology that can detect, report and stop hacking attempts in real time.

Some reference books :

- ✓ Series of “Automotive Cybersecurity Best Practices” launched in July 2016 by the Automotive Information Sharing and Analysis Center (Auto-ISAC),
- ✓ “Cybersecurity Best Practices for Modern Vehicles,” published in October 2016 by the U.S. Department of Transportation’s National Highway Traffic Safety Administration (NHTSA).

Recommendations for Securing the Connected Vehicle Environment

Security of the CV platforms, which includes:

Protection of control systems (CANBus, OBD-II port access, OBE) & infotainment systems protection against use of insecure third-party devices and applications recommendations about software security engineering hardware security controls (e.g., to protect MCUs) & interface security configuration security & software maintenance

Security of

- Smartphone applications that interact with vehicles and CV com. systems roadside equipment and infrastructure, to include monitoring for security events, strong authentication/authorization for both local and remote access and cryptographic key management methods

- Messaging and communication protocols that devices rely upon for interaction both today (e.g., DSRC, cloud) and in the near future (e.g., 5G)

- Applications that support CV capabilities, to include assurance of the "quality" of the software

Hackers

A **hacker** is a highly skilled computer expert, including Security hacker, someone who seeks and exploits weaknesses in a computer system or computer network (Wikipedia)

Elon Musk
"I think one of the biggest concerns for autonomous vehicles is somebody achieving a fleet-wide hack“.
Over The Air (OTA) software updating is useful to patch vulnerabilities but… it’s could be also an “open gate” for non-official SW, hacking, personal data steal,…

Solutions :
- Firewall, locked access (need certificates/complex algorithm,..)
- Authentication and/or encryption
- Runtime detection

Hacking

One way to do it :

For each considered ECU Extract its firmware and then explicitly reverse engineer its I/O code and data flow using disassembly, interactive logging and debugging tools.

- In most cases, extracting the firmware is possible directly via the CAN bus,
- If not, since the flash chips are not socketed, such chips can be de-soldered and read directly (the process was quite painful). Having the firmware in hand, we are able to perform three basic types of analysis: raw code analysis, in situ observations, and interactive debugging with controlled inputs on the bench.

Find vulnerabilities :

- Disasemble to map control flow and identify potential vulnerabilities, as well as debugging and logging options that could be enabled to aid in reverse engineering,
- In situ observation with logging enabled allowed us to understand normal operation of the ECU and let us concentrate on potential vulnerabilities near commonly used code paths.
- Final observation is done on “table” (ECUs removed from the car and placed into a test harness) to deeply observe & control all inputs and outputs.
  - Examine memory and identify vulnerable code.

Reflash and/or fake communications :

- Reflash Firmware (Jtag or via CAN) to take control of ECUs,
- Fake communications in case of unprotected messages.

Need high skills, time, tools but… surmountable with dedicated effort.

Incoming – Middle term

- Level 3 autonomous vehicle is still on the market (with restricted speed and conditions), last progress in term silicon (GPU) and AI get level 4 accessible,

- Cellular incoming (>5years) technology (5G) will be consistent regarding safety-related and non-safety-related V2x use-cases. 802.11p is still field proven, compliant ready to be deployed on a large.,

- Cost reduction : Mass product effect (for parts) and OTS SW modules

Anyway, V2x applications will need both solutions and will coexist (802.11p & LTE-A/5G). This incoming heterogeneous vehicular networking system will use the best of both.

  - ~Up to 70% of the road accident are expected to be avoid with this techno.

Incoming – Long term

Fin de la partie 2

In US, DSRC should 100% deployed in 2040,

In Europe : Roadmap for massive deployment ?

Standards merging : Cost reduction !

Massive data fusion (and broadcasted) : Big brother or ?

…

Big city will impose connected vehicle for traffic regulation & health issues,

…

No driving license required to be carried by autonomous car,

Many steps have to be done before Level 5 mass production and massive connected fleet… but pillars and aims are yet here.