

Corso Professionalizzante di Specializzazione (3 CFU)

Ingegneria dell'Informazione o magistrale in Ingegneria Informatica
Automatica, Ingegneria Elettronica,
Ingegneria delle Telecomunicazioni

WSN and VANET Security

Part I: Generalities on WSN and VANET Security

Lecture I.2

VANET Architectures and Application Scenarios

Ing. Marco Pugliese, Ph.D., SMIEEE

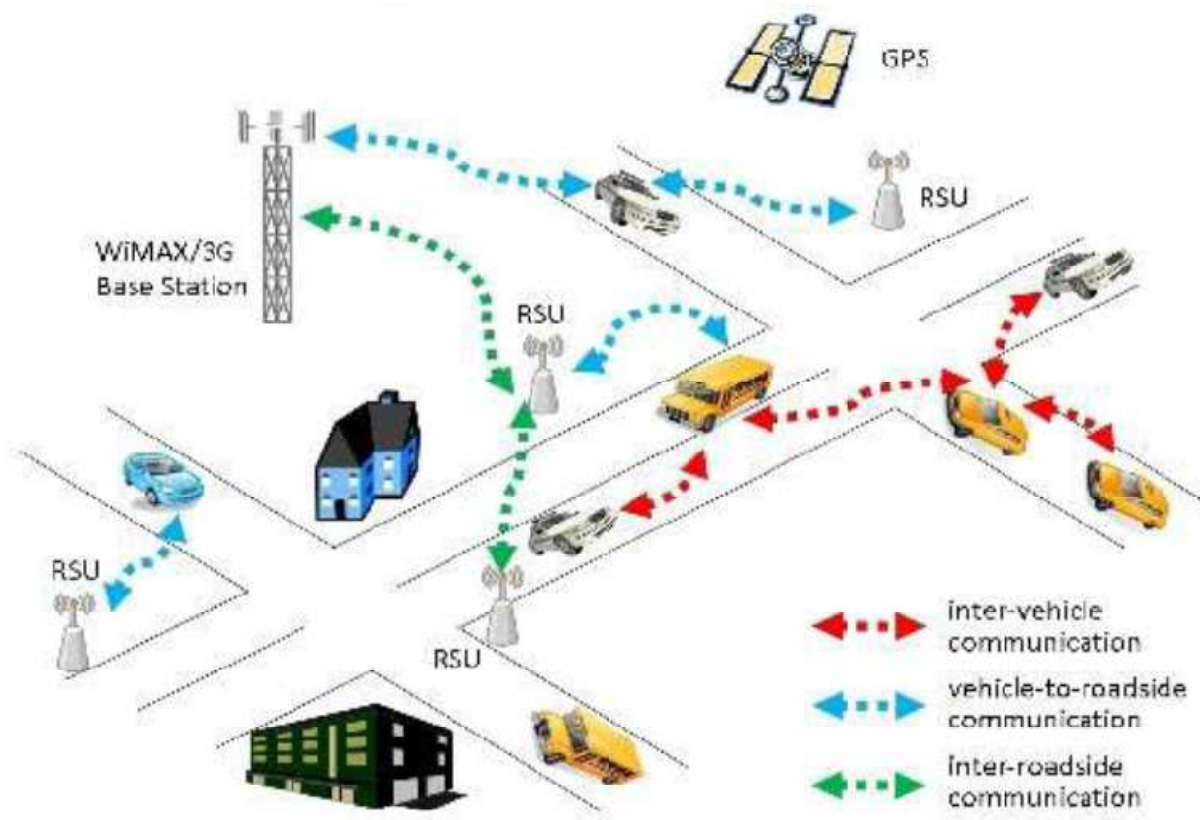
Senior Security Manager cert. UNI 10459-2017

marpug@univaq.it

April 12th, 2024

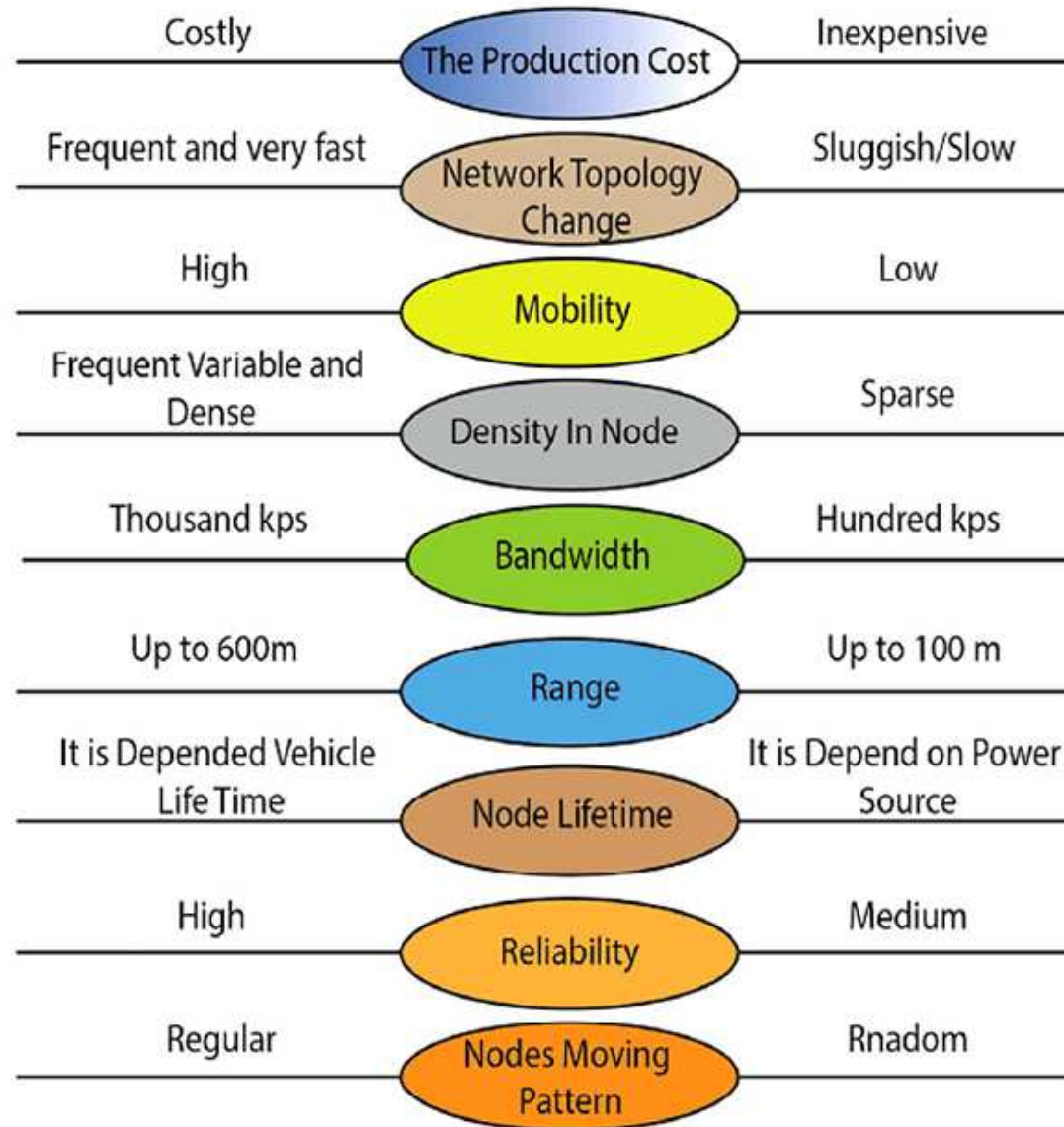
- Definition of VANET
- VANET vs. MANET
- VANET Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems

- Vehicular Ad hoc NETWORK (VANET) defines a specific case of MANET where the mobility of mobile nodes (which are vehicles) is constrained into predefined urban-like paths.
- **Elements of a VANET are vehicles, infrastructures, pedestrians.**
- VANET services are based on inter-vehicular and intra-vehicular communications and are related to Intelligent Transport System (ITS) services.



- Definition of VANET
- VANET vs. MANET
- VANET Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems

VANET vs. MANET



- Definition of VANET
- VANET vs. MANET
- VANET Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems



Most of these problems can be solved by providing appropriate information to the driver in real time.

VANET services deal with drivers safety supported by driving automation functions

The driver still manages all driving operations:

- **Level 0: the automated system issues warnings and may momentarily intervene.**
- **Level 1: the driver and the automated system share control of the vehicle.** Examples are systems where the driver controls steering and the automated system controls engine power to maintain a set speed (Cruise Control) or engine and brake power to maintain and vary speed (Adaptive Cruise Control or ACC); and Parking Assistance, where steering is automated while speed is under manual control. The driver must be ready to retake full control at any time.
- **Level 2: the automated system can take full control of the vehicle under driver monitoring: accelerating, braking, and steering.** The driver must monitor the driving and be prepared to intervene immediately at any time if the automated system fails to respond properly.

The system can manage all driving operations:

- **Level 3: the driver can safely turn their attention away from the driving tasks, e.g. the driver can text or watch a movie.** The vehicle will handle situations that call for an immediate response, like emergency braking. The driver must still be prepared to intervene within some limited time, specified by the manufacturer, when called upon by the vehicle to do so.
- **Level 4: as level 3, but no driver attention is ever required for safety, e.g. the driver may safely go to sleep or leave the driver's seat.** Self-driving is supported only in limited spatial areas (geofenced) or under special circumstances. Outside of these areas or circumstances, the vehicle must be able to safely abort the trip, e.g. park the car, if the driver does not retake control. An example would be a robotic taxi or a robotic delivery service that only covers selected locations in a specific area.
- **Level 5: no human intervention is required at all.** An example would be a robotic taxi that works on all roads all over the world, all year around, in all weather conditions.

□ Active Road-Safety Applications

- Electronic brake warning, cooperative collision warning, pre-crash sensing, lane change, traffic violation warning.
- Traffic safety: Detecting dangerous situations, Sending warning messages to other cars using ad-hoc networking.
- Traffic management services: Traffic congestion, Weather forecast, Road works.
- Platooning: vehicles closely (down to a few inches) follow a leading vehicle by wirelessly receiving acceleration and steering information, thus forming electronically coupled "road trains".




□ Traffic efficiency and management applications

- Enhanced route guidance/navigation, traffic light optimal scheduling, lane merging assistance.

□ Comfort and Infotainment applications

- Point of interest notification, media downloading, map download and update, parking access, media streaming, voice over IP, multiplayer gaming, web browsing, social networking.


Basic

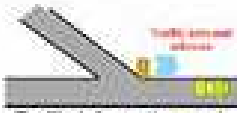
Collision avoidance Road conditions to vehicle Overtaking vehicle warning

Advanced



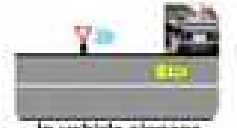
Platooning Cooperative driving, Sensor sharing High-definition map (dynamic creation) Remote Driving



Traffic information and recommended itinerary



Traffic lights to vehicles, speed guidance



In vehicle signage




Video



Mobile Office



Remote Vehicle Health Monitoring



Software updates



Navigation

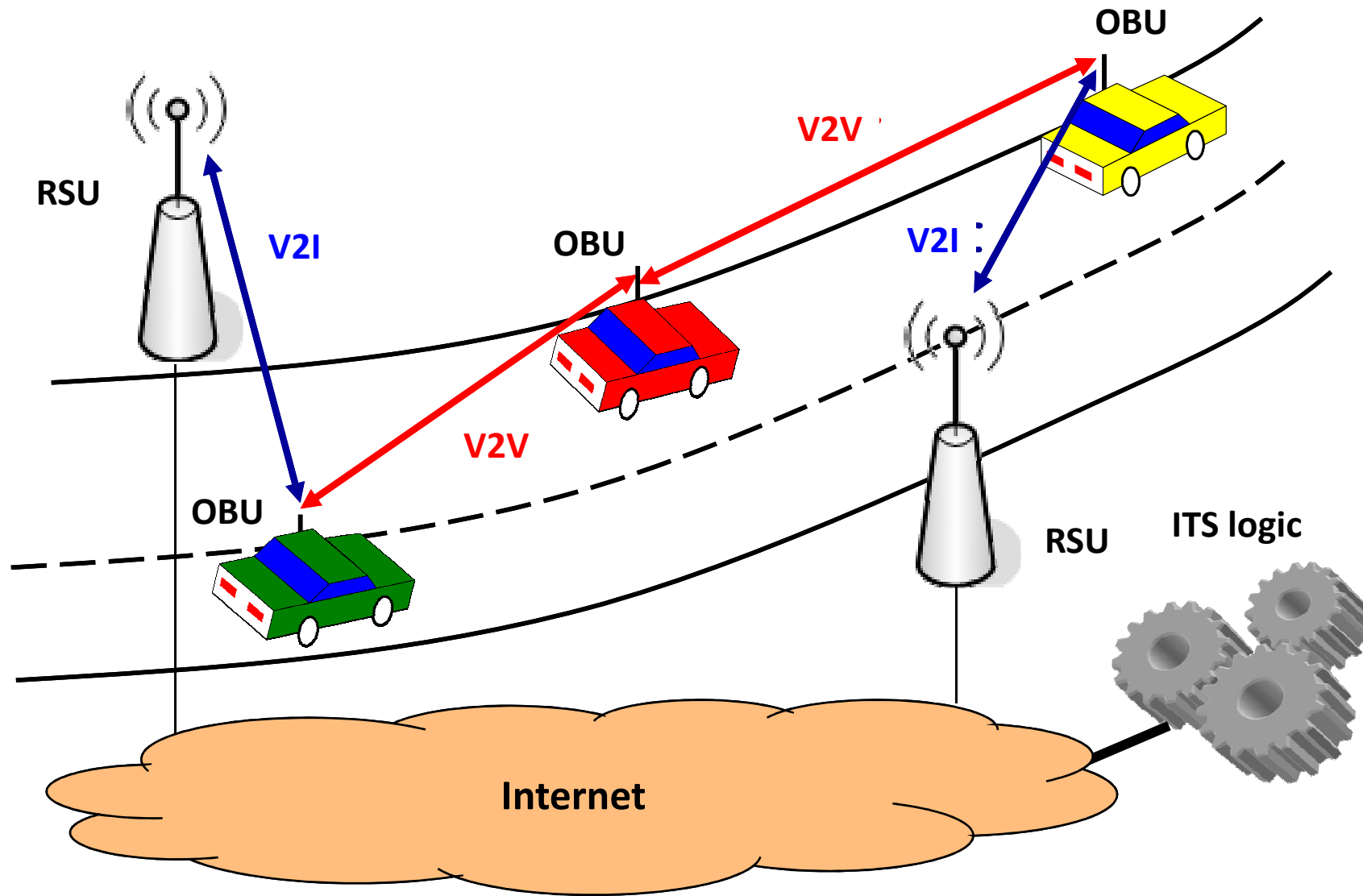


Parking

Tipologia di servizio	Massima latenza end-to-end (ms)	Reliability (%)	Minimo Communication range richiesto (metri)	Data rate (Mbps)	Frequenza messaggi (Mmessage/sec)	Payload (Bytrate)
Platooning	10-500	99,99	80-350	65	2-50	50-6500
Extended Sensor	3-100	90-99,999	50-1000	10-1000	10	1600
Advances Driving	3-100	90-99,999	360-700	10-50	10-100	300-12000
Remote Driving (max 250 km/h)	5	99,999	-	UL:25 DL:1	-	-

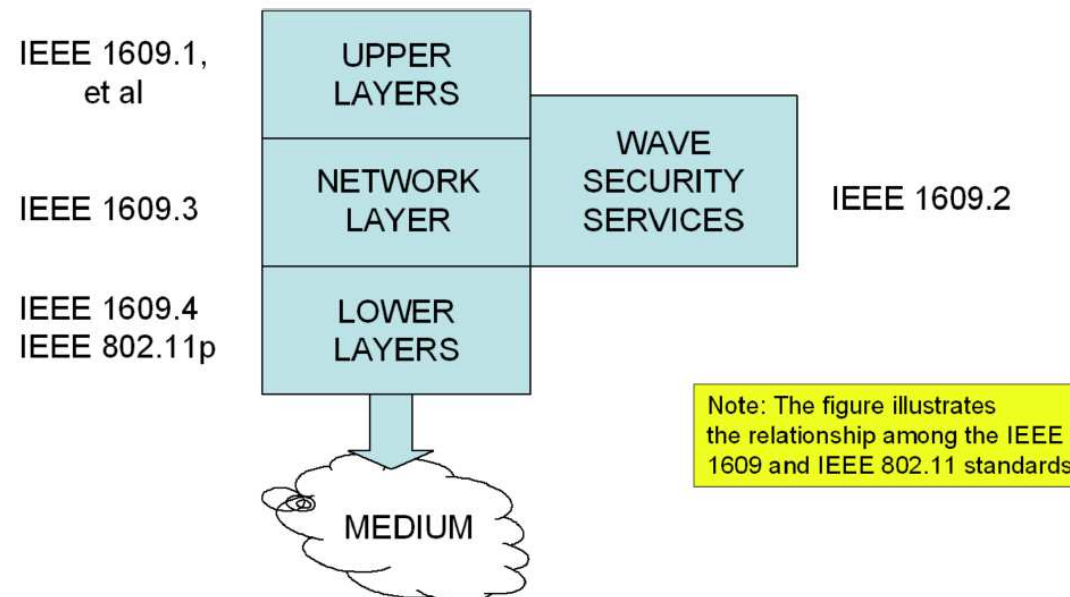
- Definition of VANET
- VANET vs. MANET
- Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems

- Denoted also as V2X (Vehicle-to-X, X = Vehicles, Infrastructures, Pedestrians).
- Parties in V2X communications are: Authorities + Network nodes + Users.
- **RA**: trusted Regional Authority providing authorizations (adm/sec/privacy).
- **Network Nodes**: fixed (**Road Side Unit, RSU**) and mobile (**On Board Unit, OBU**).
 - **RSU**: fixed infrastructure (often placed near traffic lights or road signs) to connect vehicles to external networks and edge device for the RA managing local VANET services.
 - **OBU**: device for **extra vehicle communications** to other OBUs (V2V) or RSU (V2I) and gateway for **intra vehicle communications** with ECUs (**Electronic Control Units**) microcontrollers for on-board sensor networks.
- V2X communication modes:
 - **Vehicle to Infrastructure (V2I)** vehicle to RSU and vice-versa for “high level” ITS information (traffic congestion, weather conditions, cooperative driving, emergency services impacting lot of vehicles, ...) or entertainment services
 - **Vehicle to Vehicle (V2V)** vehicle to vehicle (or Inter-Vehicle, IVC) for “low level” ITS information (incident avoidance, platooning, emergency services impacting just few vehicles, ...)
 - **Vehicle-to-Pedestrians (V2P)** vehicle to pedestrians / private micro-mobility (cyclists, people using wheelchairs) to warn / notify themselves of the car.



- At present, V2X standard approaches can be divided into two categories:
IEEE 802.11p-based vs LTE-based standards.
 - **Dedicated Short-Range Communications (DSRC)** by U.S. IEEE 802.11p-based V2X system.
 - ETSI (European Telecommunications Standards Institute) ITS-G5 is IEEE 802.11p-based systems (large reuse of IEEE 802.11p PHY and MAC layers).
 - **4G/5G Long Term Evolution – Vehicle (LTE-V)** by 3GPP (Third Generation Partnership Project) to support V2X services over cellular systems.
 - First version of Release 14 includes support for V2X communications, commonly referred to as LTE-V, LTE-V2X, or cellular V2X (C-V2X).
 - LTE-V evolutions in Releases 15 and 16 to support 5G-V2X communications, autonomous vehicles' applications and service effectiveness.

- ❑ **WAVE (Wireless Access in Vehicular Environments)** is the reference protocol stack to support automotive applications.
- ❑ WAVE includes IEEE 1609 e IEEE 802.11 standards.
- ❑ IEEE1609.1 defines WAVE components, interfaces, message formats, devices forming an OBU.
- ❑ IEEE1609.2 defines the security protocols fo safe communications.
- ❑ IEEE1609.3 defines network and transport protocols, addressing and routing and WAVE Short Messages Protocol (WSMP).
- ❑ IEEE1609.4 defines the extensions of MAC 802.11 for WAVE.

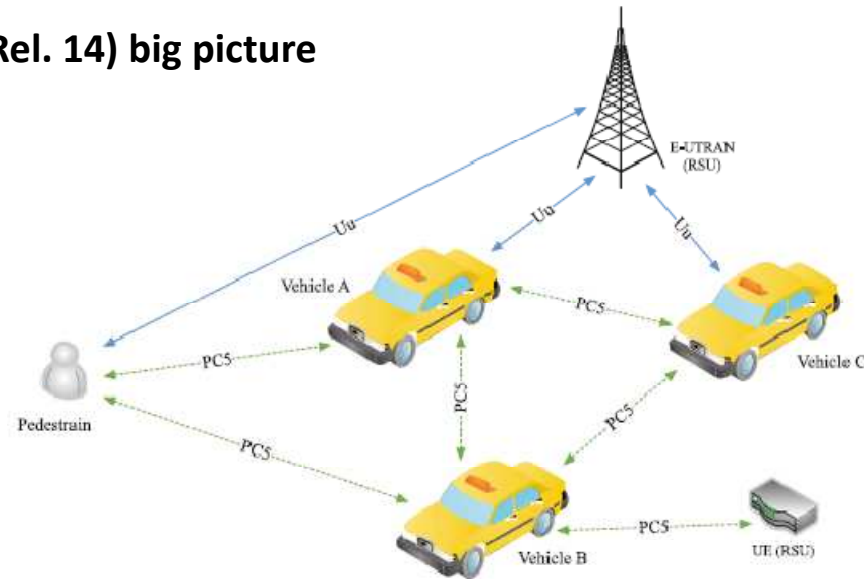


- ❑ **DSRC (Dedicated Short-Range Communications)** consists of a set of standards and protocols for automobile applications.
- ❑ At the bottom layer, DSRC adopts WAVE IEEE 802.11p as its PHY and MAC layer standard.
- ❑ IEEE 1609.4 is employed as a MAC layer extension for channel switching.
- ❑ IEEE 802.2 protocol serves as the logical link control (LLC) sublayer standard.
- ❑ Network layer: IPV6, User Transmission Protocol (UDP), Transmission Control Protocol (TCP).
- ❑ DSRC can also optionally utilize WAVE Short Message Protocol (WSMP) defined in IEEE 1609.3 (for direct comms between vehicles or between vehicles and RSUs).
- ❑ DSRC adopts 1609.2 for security services.

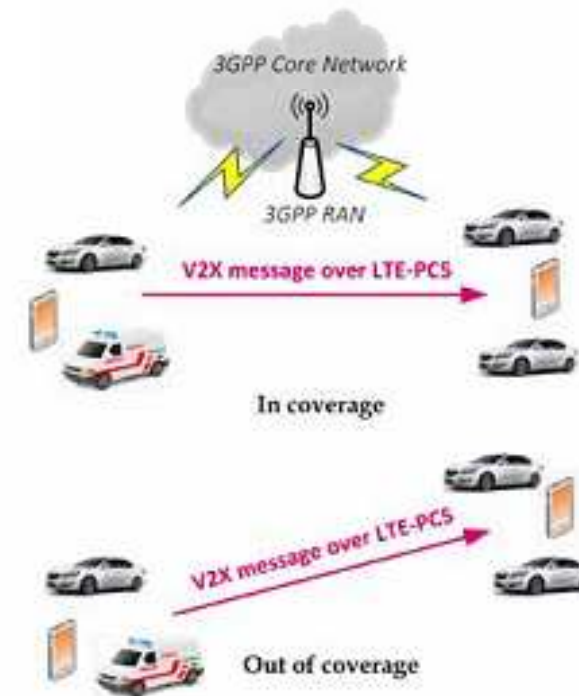
Application layer		Non-safety Application	Safety application (SAE J2735)
Transport layer		TCP/UDP	
Network layer		IPV6	
Data link layer	LLC	IEEE 802.2	
	MAC Extension	IEEE 1609.4	
	MAC	IEEE 802.11p	
Physical layer		IEEE802.11p	

- **Release 14 (partly outdated):** LTE-V standard includes two radio i/f:
 - **Uu to support vehicle-to-infrastructure communications**
 - **PC5 to support V2V communications based on direct LTE.**
 - It introduces two new communication modes replacing mode 1 and mode 2) specifically designed for V2V communications
 - Mode 3 where **the cellular network selects and manages** the radio resources used by vehicles for their direct V2V comms.
 - Mode 4 where **vehicles autonomously select** the radio resources for their direct V2V communications.
 - Positioning accuracy by 100 mt
- **Release 15 (stable):** LTE-V evolutions to support **5G-V2X** communications and autonomous vehicles' applications.
 - New use cases are focused on safety-related services: autonomous driving (include platooning), sensor and map sharing, information sharing for partial/conditional and high/full automated driving, and remote driving. Safety-related applications can require the transmission of up to 50 pps (packets/s), **max. latency between 3 and 10 ms**, and up to a 99.99% reliability level, cope with the high relative speeds between transceivers (up to 200 km/h and above)
 - Able to bridge a substantial distance (several hundred meters up to 1 km) and work under non-line-of-sight (NLOS) conditions.

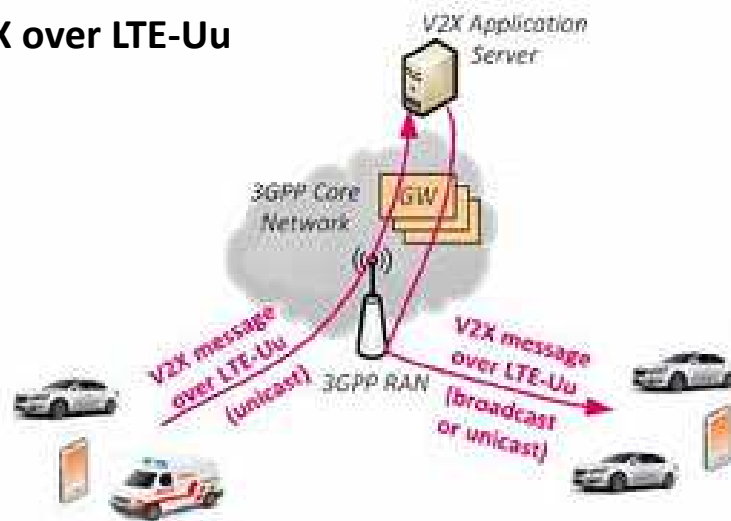
LTE-V (Rel. 14) big picture



V2X over LTE-PC5

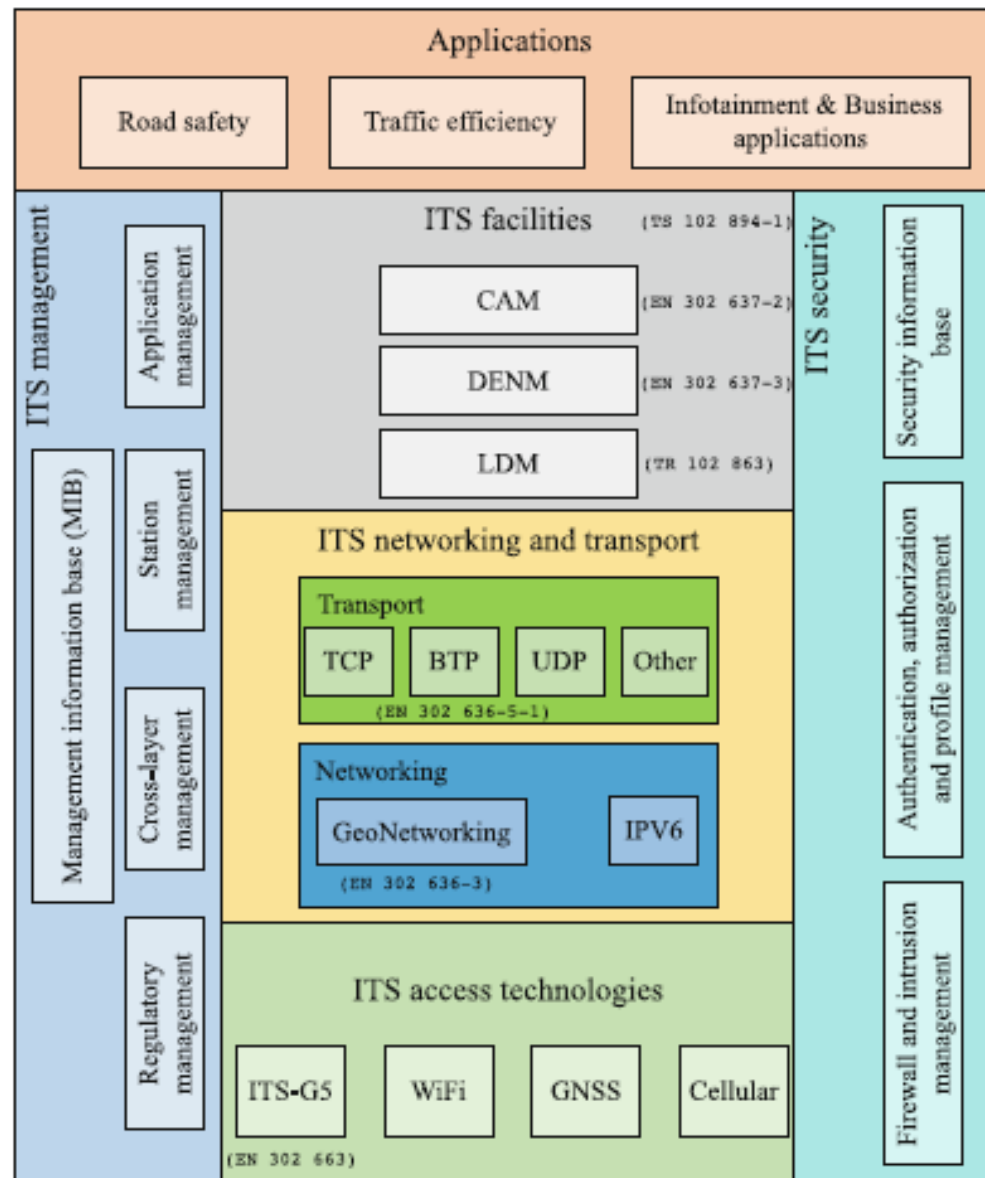


V2X over LTE-Uu



- 802.11 technology is mature, widely tested and ready for large-scale introduction, meets the requirements for safety-related V2V use cases.
- Conservative solution:
 - 802.11p communications for safety-related (time-critical) V2V services
 - Cellular communications for less time-critical V2V services, already be possible with current 4G technology.
- **Release 16 (stable)**: the need for greater interaction between Telco and applications with the aim of improving the effectiveness of V2X services, both with respect to security and in terms of user experience (**positioning accuracy at 10 cm**). In this regard, the ability of the system to offer a prediction of the QoS level available to V2X applications is fundamental: e.g. a network application that assists a self-driving vehicle could alert the driver to take the manual override if, based on the planned trajectory and speed, it foresees a degradation of network connectivity levels.
- **Release 17 (2022)**: NR Multicast broadcast, enhancements on positioning accuracy looking at factory / campus positioning, V2X, 3D positioning.
- **Release 18 (on progress)**: will enhance the support of UE-to-network relay, add support for UE-to-UE relay.

- The system known as ETSI ITS-G5 has been developed since 2007 by the ETSI ITS Technical Committee referring to the previous US project known as WAVE. The WAVE project defined the changes to the IEEE 802.11 standard (underlying Wi-Fi products) to support the requirements of vehicular transport systems, producing the so-called IEEE 802.11p version. The motivation of the ITS-G5 standard was to exploit as much as possible pre-existing standards such as IEEE 802.11 for Wi-Fi, introducing elements capable of managing the high mobility typical of the vehicular context.
- The ITS-G5 system is based on the ETSI EN 302 637-2 specification which defines the CAM messages ("Cooperative Awareness Message") and DENM ("Decentralized Environmental Notification Message").
 - A CAM message contains information about the ITSG5 device in terms of the status of the device itself (what time, speed, position, status of movement, etc) and related attributes (such as size, type of vehicle, role in traffic, etc).
 - A DENM message instead reports the occurrence of specific events (such as incidents, for example) and persists as long as the event in question has not ended.



- CAM can be exploited for early warning / alerting of CCA services: for each vehicle that recently sent a CAM, a trajectory-based algorithm computes its position and its distance with the focus vehicle. Then it computes the time instant t^* at which the distance between the two vehicles is minimum.
 - If $t^* < 0$, the two vehicles are getting farther apart
 - if $t^* > t_{2c}$ ("time to collision") the minimum distance will not be reached within t_{2c} from the current time. The algorithm thus determines that no action is required.
 - If $t^* > 0$ and $t^* < t_{2c}$, the minimum distance d^* at which the two entities will be at time t^* is computed. The algorithm compares d^* against a minimum threshold s_{2c} ("space to collision"): if $d^* < s_{2c}$ then an alert message is scheduled to be sent to the vehicles.
- CAM rate is 10 Hz: if vehicle speed is 50 Km/h, accuracy is $\approx 1,4$ m (!!)
- CCA services must employ local sensors (radar, cameras with image recognition) as well as augmented GNSS position accuracy (< 3 cm).

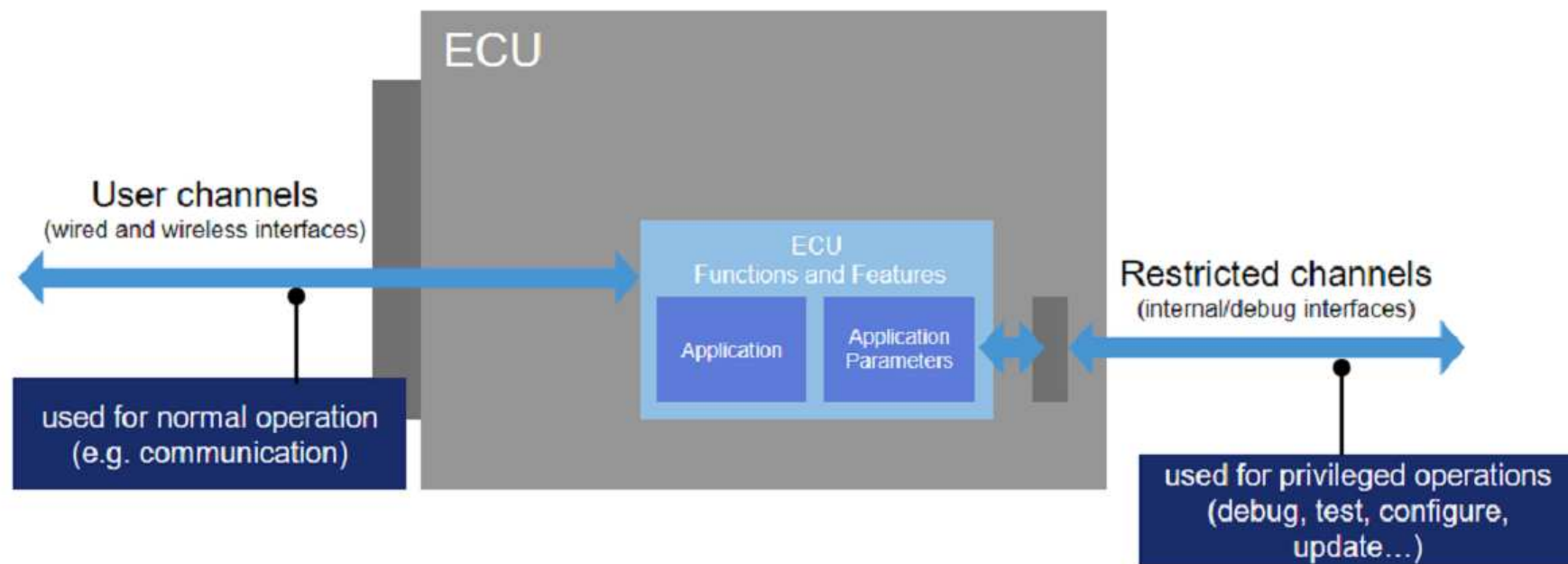
Avoiding Car Crashes Using Cellular V2I Communication, G. Avino, C. Casetti, C. F. Chiasserini, M. Malinverno, Notiziario Tecnico Telecom Italia, anno 27, n. 3/2018, pp. 104-113

Parameter	Vehicle	Pedestrian
t_{2c}	10 s	3 s
s_{2c}	5 m	2 m
Max CAM Age	0.8 s	0.8 s
CAM Frequency	10 Hz	10 Hz
Alert max Frequency	1 Hz	1 Hz

- Definition of VANET
- VANET vs. MANET
- VANET Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems

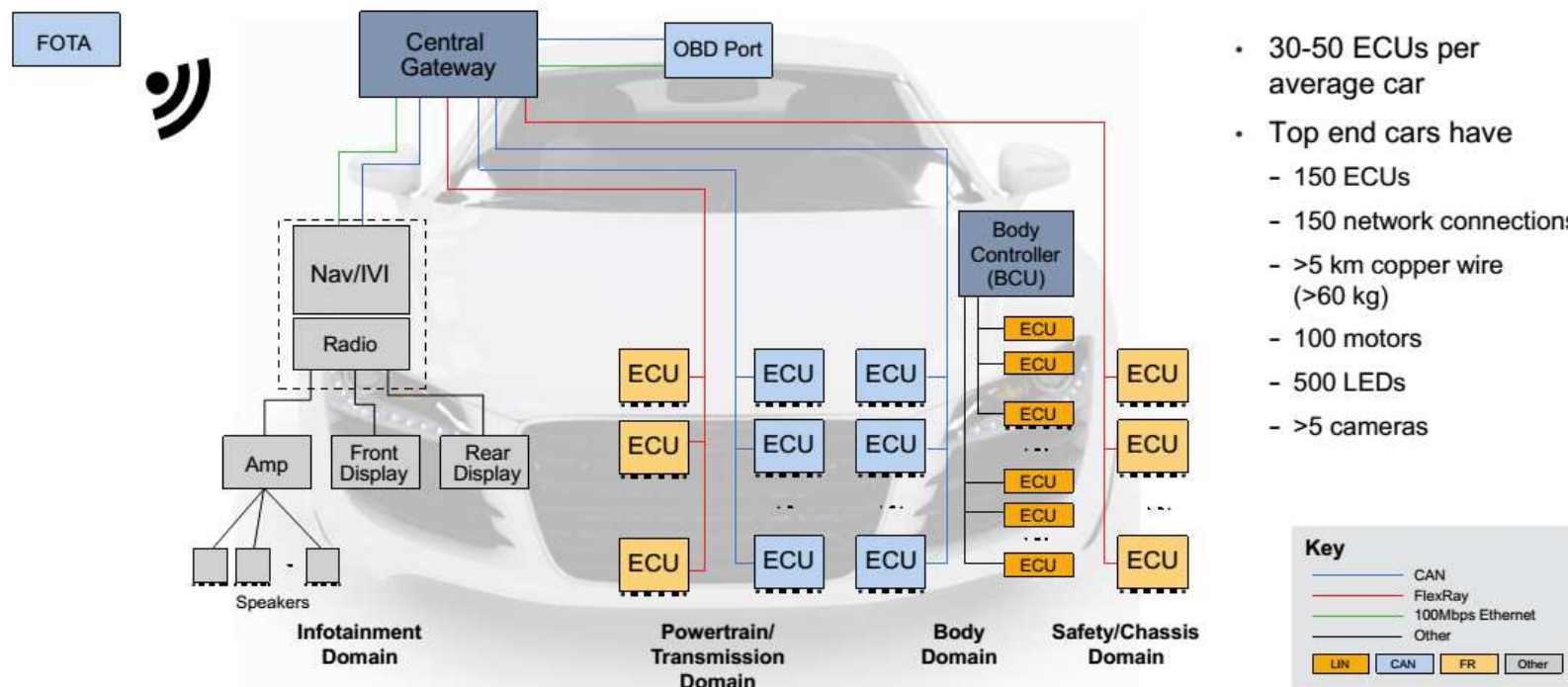
- An **Electronic Control Unit (ECU)** is any embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle (the “Connected Car”)
- A ECU acts as a specific local bus controller and communicate through Intra-Vehicular or Vehicle Communication Systems (VCSs), or subnets, or busses to other ECUS or sensors, actuators, servomechanisms.
- Types of ECU include
 - Engine Control Module (ECM)
 - Powertrain Control Module (PCM)
 - Transmission Control Module (TCM)
 - Brake Control Module (BCM)
 - Central Control Module (CCM)
 - Central Timing Module (CTM)
 - General Electronic Module (GEM)
 - Body Control Module (BCM)
 - Suspension Control Module (SCM)
- These systems are sometimes referred to as the car's computer.
- Some modern vehicles have up to 80 ECUs.

- The main assets of an ECU are its functions and features split into an **Application** (sw code, hardware) and **Application Parameters** (configuration and data). A typical ECU has two categories of interfaces:
 - **User Channels:** being used to communicate to the ECU in normal operation mode
 - **Restricted Channel:** being used for specific, typically privileged, operations such as device debug, test and maintenance.

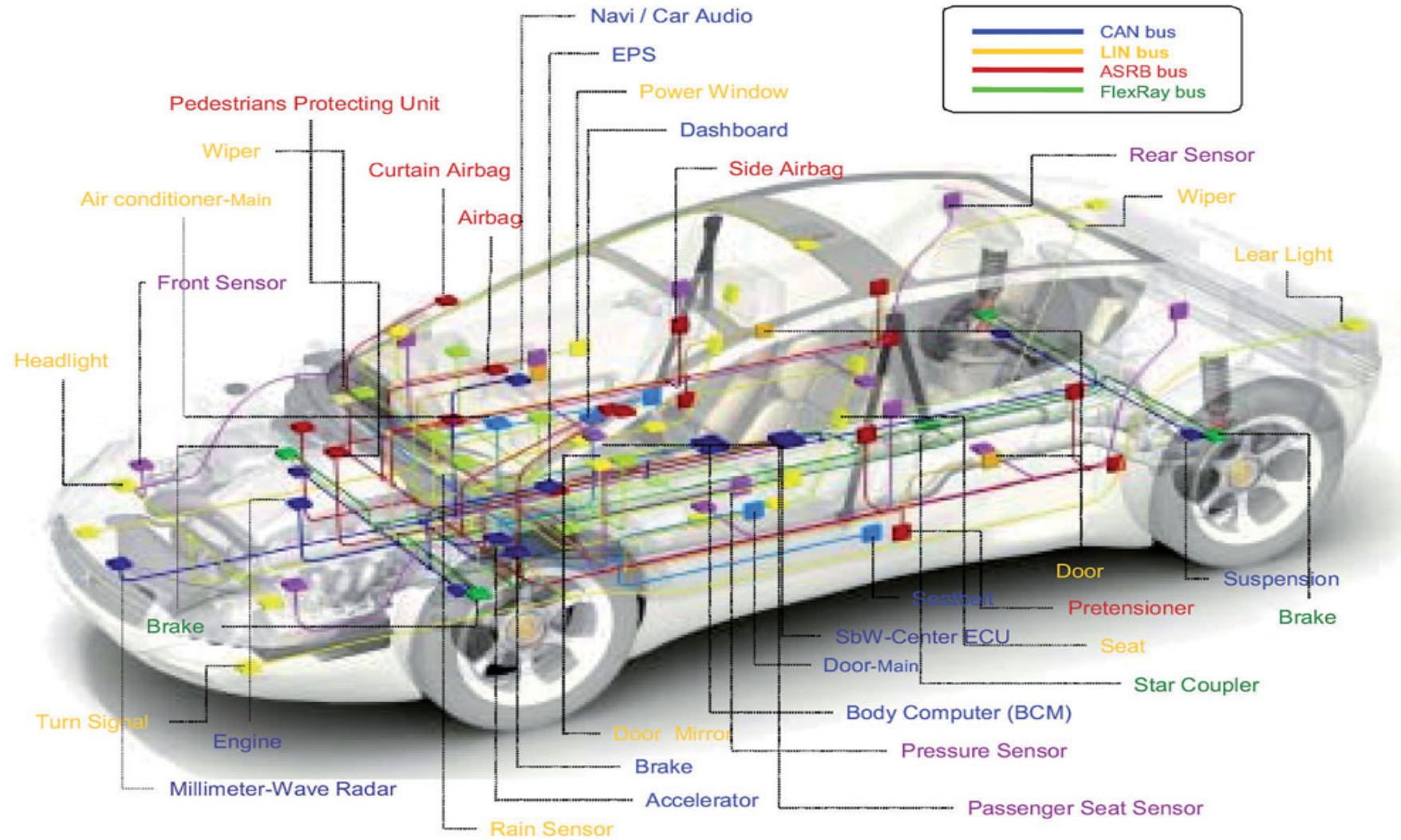


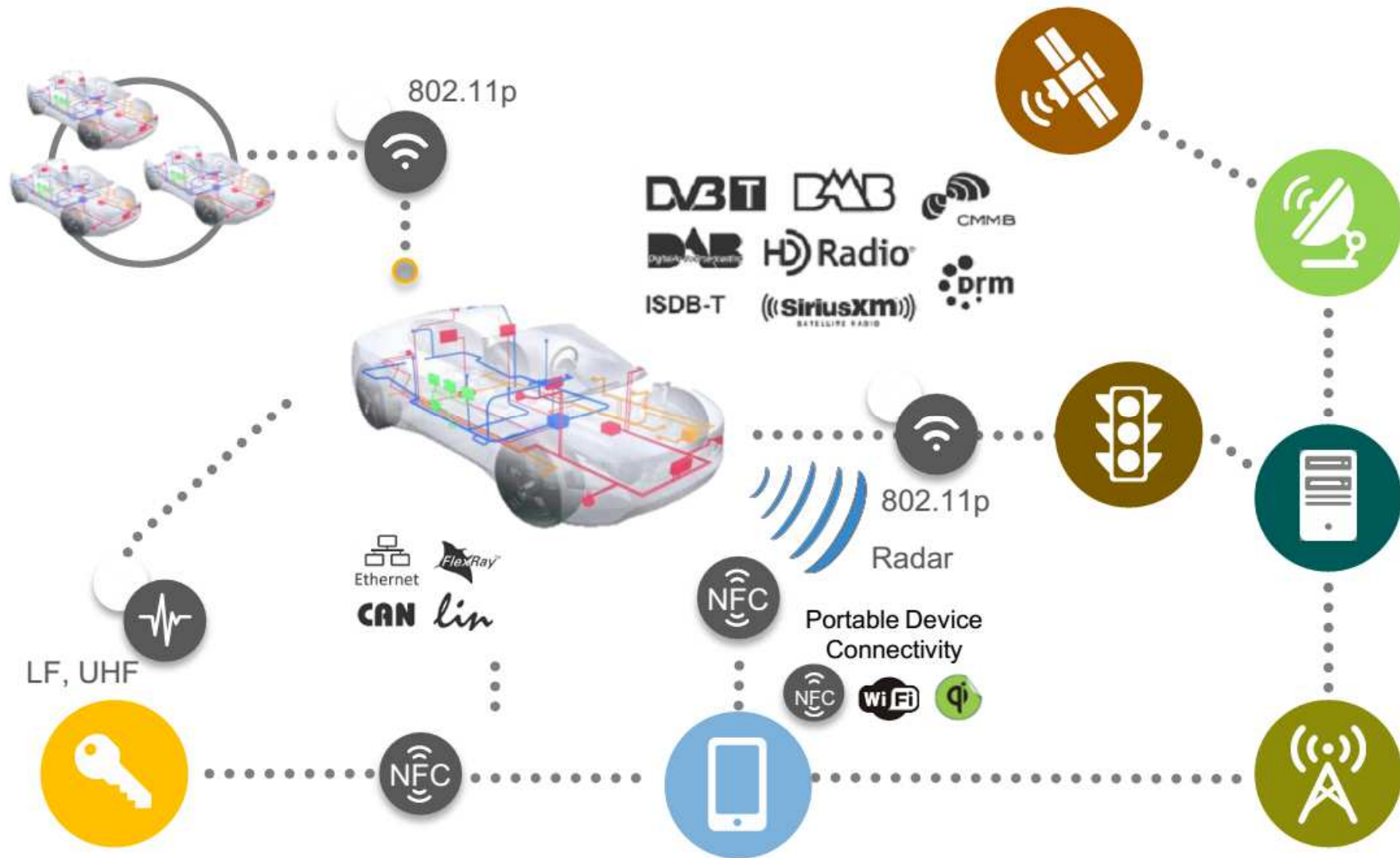
- The on-board diagnostics connector (OBD-II), originally designed as a normal user port to enable emission checks by regulations, was extended to provide a wealth of detailed diagnostic on the internals of the vehicle network that are used **for inspection and maintenance**.
- **In its current form, it can be misused by hackers to manipulate the vehicle network and / or extract data from it.**
- The SAE Data Link Connector Vehicle Security Committee is therefore currently working on specifications J3138 and J3146 that will help to turn the diagnostics port into a (more) restricted port with limited capabilities.

- The presence of the gateway introduces a physical network isolation, particularly in reference to some of the recent vehicle hacks, where the externally connected head unit was on the same network domain as safety critical ECUs controlling braking, chassis, powertrain etc. **By separating OBD diagnostics port and head unit into their own domains, any message to the safety domains need to pass through the gateway and hence pass through the firewall to be checked for validity.**



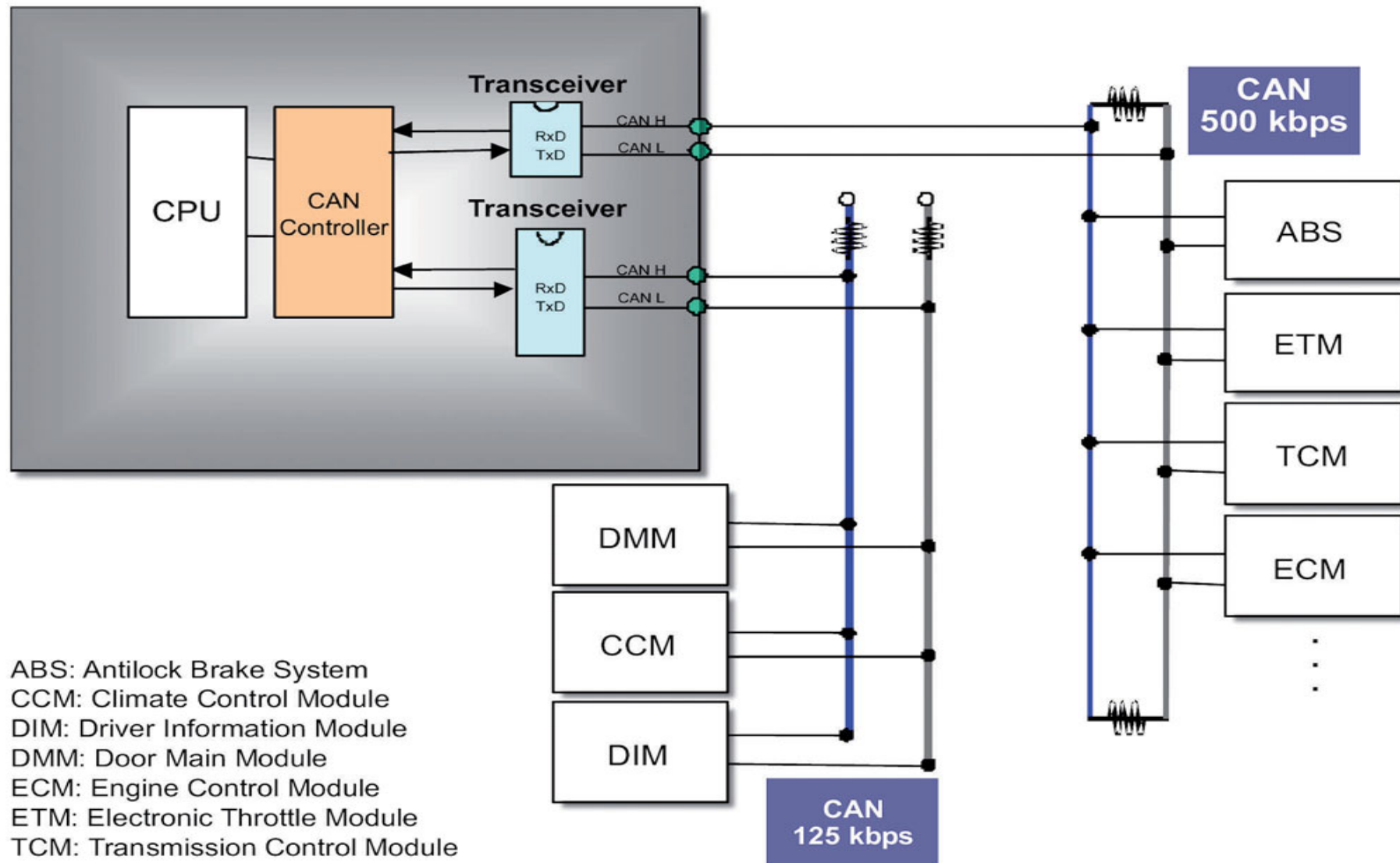
- 30-50 ECUs per average car
- Top end cars have
 - 150 ECUs
 - 150 network connections
 - >5 km copper wire (>60 kg)
 - 100 motors
 - 500 LEDs
 - >5 cameras





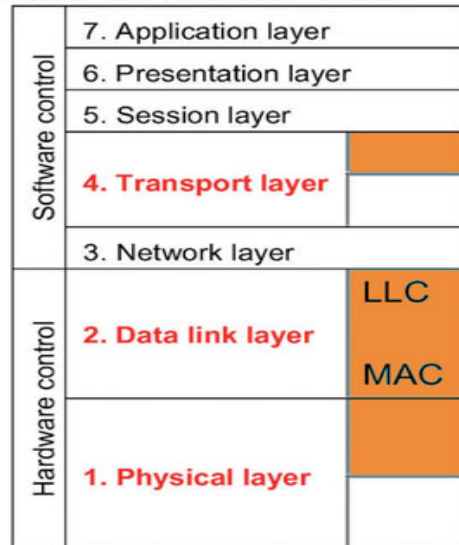
- **Traction domain** includes engine and transmission control and requires highly reliable networks with very tight determinism and reproducibility constraints. Given the high volume of data to be processed by the complex combustion control algorithms or kinetic energy recovery systems, communication protocols must be very fast and reliable.
- **Active Safety domain** deals with the functions of active safety, vehicle dynamics and driver assistance (vital functions) such as anti-lock brake systems (ABS, Antilock Brake System), anti-slip (ASR, AntiSlip Regulation) and control of vehicle stability, electronic power steering and active suspension control. Communication protocols must be very fast and reliable.
- **Passive Safety domain** includes airbags and seat belt pretensioners. Communication protocols must be very fast and reliable.
- **Comfort domain** deals with the systems and accessories that contribute to the comfort of the occupants. Requirements are obviously low criticality. Functions of this domain include: instrumentation of the dashboard, air conditioning system, parking aid electronics, central locking, servo-mechanisms for positioning seats, windows, lights, mirrors.
- **Infotainment domain** deals with external communications, multimedia applications and infotainment. Absolutely non-critical (stereo system, CD and DVD players, wireless voice / data connectivity, the networks of this domain exchange huge amounts of data, require high transmission speeds, but not of the "time-critical" type.

- IVCs are supported by different communication protocols to manage data transfers for intra-vehicle services functions.
- Typically are serial bus: (several devices to be interconnected): for each transaction, the TX device takes the control of the bus (Master), sends an I/O request to the RX device, then the bus is ready for another transaction.
- Each scheme is optimized for the specific requirements in terms of reliability (robustness), temporal transparency, transmission speed
 - **LIN** (Local Interconnect Network): synchronous **polling-based** bus scheme for services in the comfort domain. Typically more LIN buses are interconnected through a CAN bus. Requirements are light: low bit rate (up to 20 kbps), low reliability (no integrity check), no real time.
 - **CAN-bus** (Controller Area Network): asynchronous **event-triggered** bus scheme for **soft real time** and high reliability services in the traction, active and passive safety domains, medium bit-rate (up to 1 Mbps)
 - **TTP/C** (Time-Triggered Protocol for automotive class C), **TTCAN** (Time-Triggered CAN): synchronous **time-triggered** bus schemes for **hard real time** services and high reliability in the active and passive safety domains, medium bit-rate (up to 1 Mbps).
 - **MOST** (Media Oriented Systems Transport), **FlexRay**: for infotainment services, high bit rate (>> 1 Mbps)



- **Multimaster:** any device can send messages. The message sent first will be the one that arrives first at its destination. If multiple units simultaneously send the information, the one with the highest priority (ID) will be the first to be examined.
- **Message Transmission:** the transmitted messages have a particular form. In particular, each unit is identified by a priority factor. The one with higher priority can continue to send messages in the case of simultaneous messages over time.
- **Confinement of Errors:** ability to detect errors and instantaneous communication to all units. **It can be shown that a CAN bus at 1 Mbps with an average bus utilization of 50%, and an average message length of 80 bits and a processing time of 8 hours a day for 365 days I year, it will have an undetected error every 1000 years.** Practically the network is not subject to errors during its life. This is the main strength of CAN bus. Each node is able to detect its own malfunction and to exclude itself from the bus if it is permanent. This is one of the mechanisms that allow CAN technology to maintain the rigidity of timings, preventing a single node from undermining the entire system.
- **Simplicity and wiring flexibility:** CAN is typically implemented on a twisted pair (shielded or not depending on the needs). The nodes do not have an address that identifies them and can therefore be added or removed without having to reorganize the system or part of it.
- **High noise immunity:** ISO 11898 standard recommends that the interface chips can continue to communicate even in extreme conditions, such as the interruption of one of the two wires or the short circuit of one of them with ground or with the power supply.
- **High reliability:** error detection and the request for retransmission is handled directly by HW with five different methods (two at the bit level and three at the message level).
- **Standard maturity:** relatively low cost and good performances has led to a widespread diffusion of CAN-bus in many industrial sectors.

Basic OSI reference model



Items defined in each layer by the CAN protocol

Layer	Defined items	Description
Layer 4	Retransmission control	Retries transmission endlessly.
Layer 2 (LLC)	Received message selection (acceptance filtering)	Permits point-to-point connection, simultaneous broadcast connection, or group broadcast connection.
	Overload notification	Notifies that preparation for reception is not complete yet.
	Error recovery	Retransmits data.
Layer 2 (MAC)	Message framing	There are 4 types of frame: data frame, remote frame, error frame, and overload frame.
	Connection control method	Contention method (multicast supported)
	Arbitration for data collision	The ID with higher priority than others is allowed to continue to send by arbitration.
	Spread of failure suppression function	Temporary and continual errors are automatically discriminated to eliminate a faulty unit.
	Error notification	Notifies an error such as CRC error, stuffing error, bit error, ACK error, or format error.
	Error detection	All units can detect an error at any time.
	Response method	One of two types: ACK or NACK.
	Communication method	Half-duplex communication.
Layer 1	Bit encoding	NRZ-based encoding or 6-bit stuffing.
	Bit timing	Bit timing and bit sampling counts (selectable by user).
	Synchronization method	Synchronization by synchronizing segments (SS) (resynchronization function available)

Error Detecting in 5 steps:

- ❑ CAN Controller detects error in TX or RX and sends an Error Frame;
- ❑ The corrupted message is ignored by all devices in the bus;
- ❑ CAN Controller updates its internal state;
- ❑ The message is sent again. CAN-bus defines 5 different kinds of errors: 3 at bit level and 2 at message level. Errors are detected through the following techniques:
 - **Listening:** any device compares the bits sent with the bits on the bus and in case of a difference, a Bit Error is generated.
 - **Bit stuffing:** after any occurrence of a sequence of 5 identical bits (11111 or 00000), then a sixth complementary bit is sent but automatically ignored by the receiving device.
 - **Cyclic Redundancy Check:** any receiving device computes the CRC corresponding to the received message and compare it with the CRC computed and sent with the message by the sender.
 - **Frame Check:** if the receiver detects that the received message is not compliant to the standard CAN frames structure.
 - **Transmission of the Acknowledgement bit:** any device which correctly receives a Data Frame or a Remote Frame must feedback by setting a specific bit in the ACK field of that frame.

