Corso Professionalizzante di Specializzazione (3 CFU)
Ingegneria delle Telecomunicazioni, Ingegneria Informatica,
Ingegneria dei Sistemi di Controllo e dell'Automazione,
Informatica

WSN and VANET Security

Part I: Security Analysis

Lecture I.3

The case of VANET

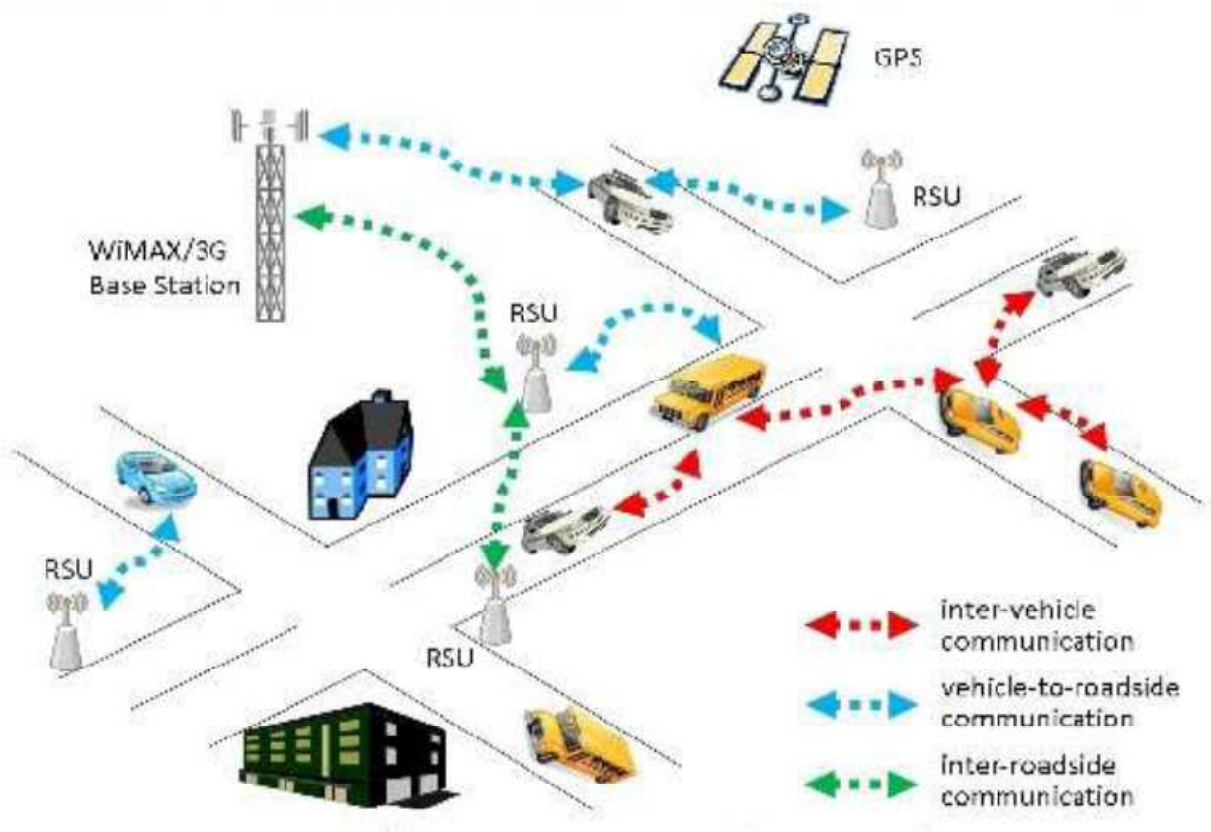
Ing. Marco Pugliese, Ph.D., SMIEEE
Senior Security Manager UNI 10459-2017 ICMQ cert. 25-00238
marco.pugliese@univaq.it
April 11th, 2025

Outline

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

Definition of VANET

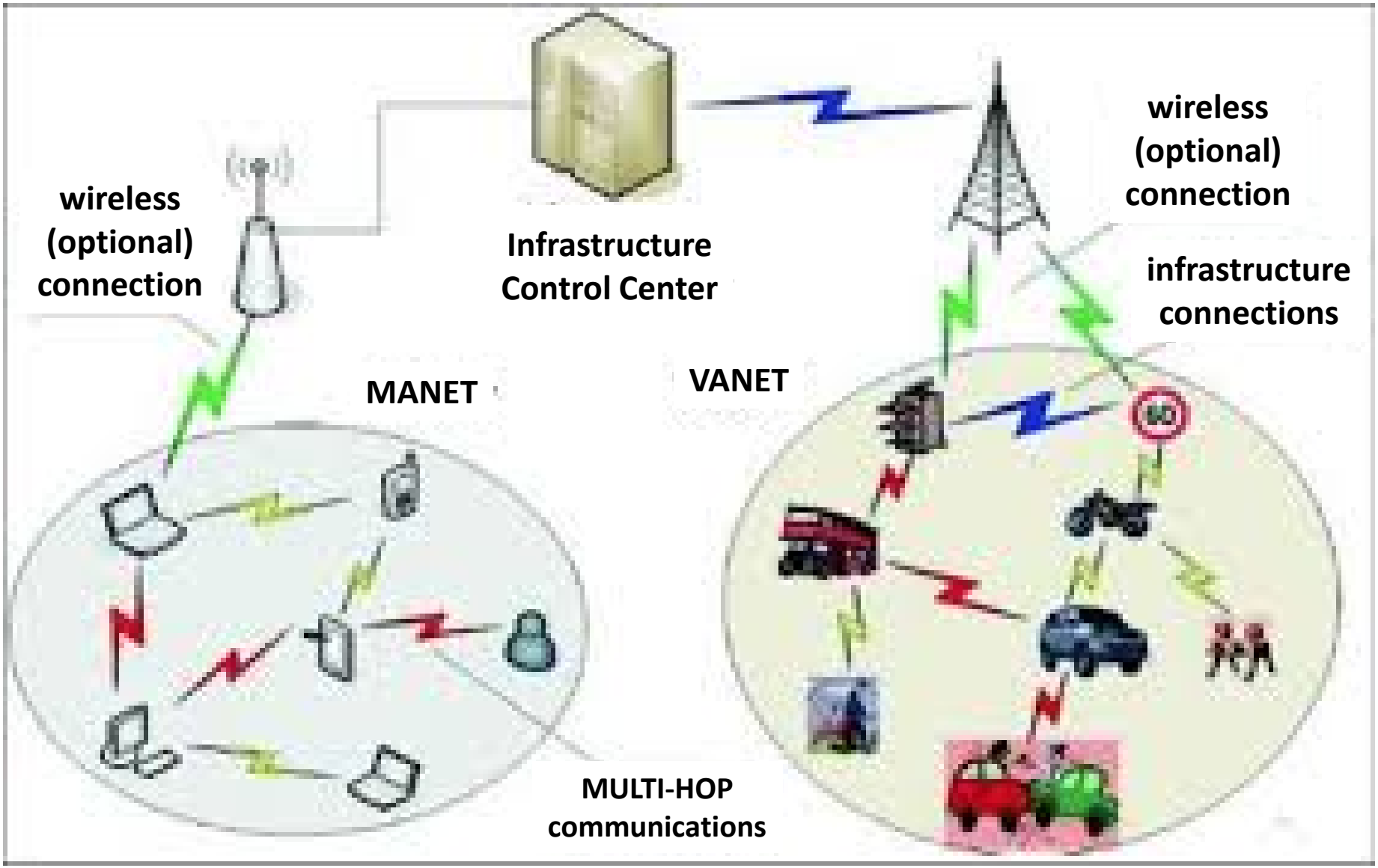
- Vehicular Ad hoc NETwork (VANET) defines a specific case of MANET where the mobility of mobile nodes (which are vehicles) is constrained into predefined urban-like paths.
- **Elements of a VANET are vehicles, infrastructures, pedestrians.**
- VANET services are based on inter-vehicular and intra-vehicular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



Outline

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

VANET vs. MANET



Outline

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

Vehicular services: why?

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

Levels of Driving Automation (SAE J3016)

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.

Levels of Driving Automation (SAE J3016)

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 (georefenced) 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 an all roads all over the world, all year around, in all weather conditions.

VANET Applications

- Mainly two class of services
  - The first category encompasses non-safety-related services, which primarily focus on enhancing traffic efficiency and providing comfort and entertainment for passengers. Examples of such services include in-car gaming, video streaming, and other multimedia applications, which typically require data volumes ranging from several megabytes to hundreds of megabytes. Due to their high data demands, these services rely heavily on high-capacity vehicle-to-infrastructure (V2I) links to ensure seamless connectivity and frequent access to remote servers.
  - The second category comprises safety-related services, which are designed to prevent traffic accidents and ensure the safety of road users. These services are inherently prioritized over non-safety-related applications due to their critical nature and stringent real-time requirements. To meet these requirements, safety-related services predominantly utilize vehicle-to-vehicle (V2V) links, which enable direct and low-latency communication between vehicles, thereby ensuring timely and reliable transmission of safety-critical information. This dual-category framework highlights the diverse and dynamic requirements of V2X communications, underscoring the need for robust and adaptive resource allocation strategies to support both safety and non-safety applications effectively.

VANET Applications

- **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.

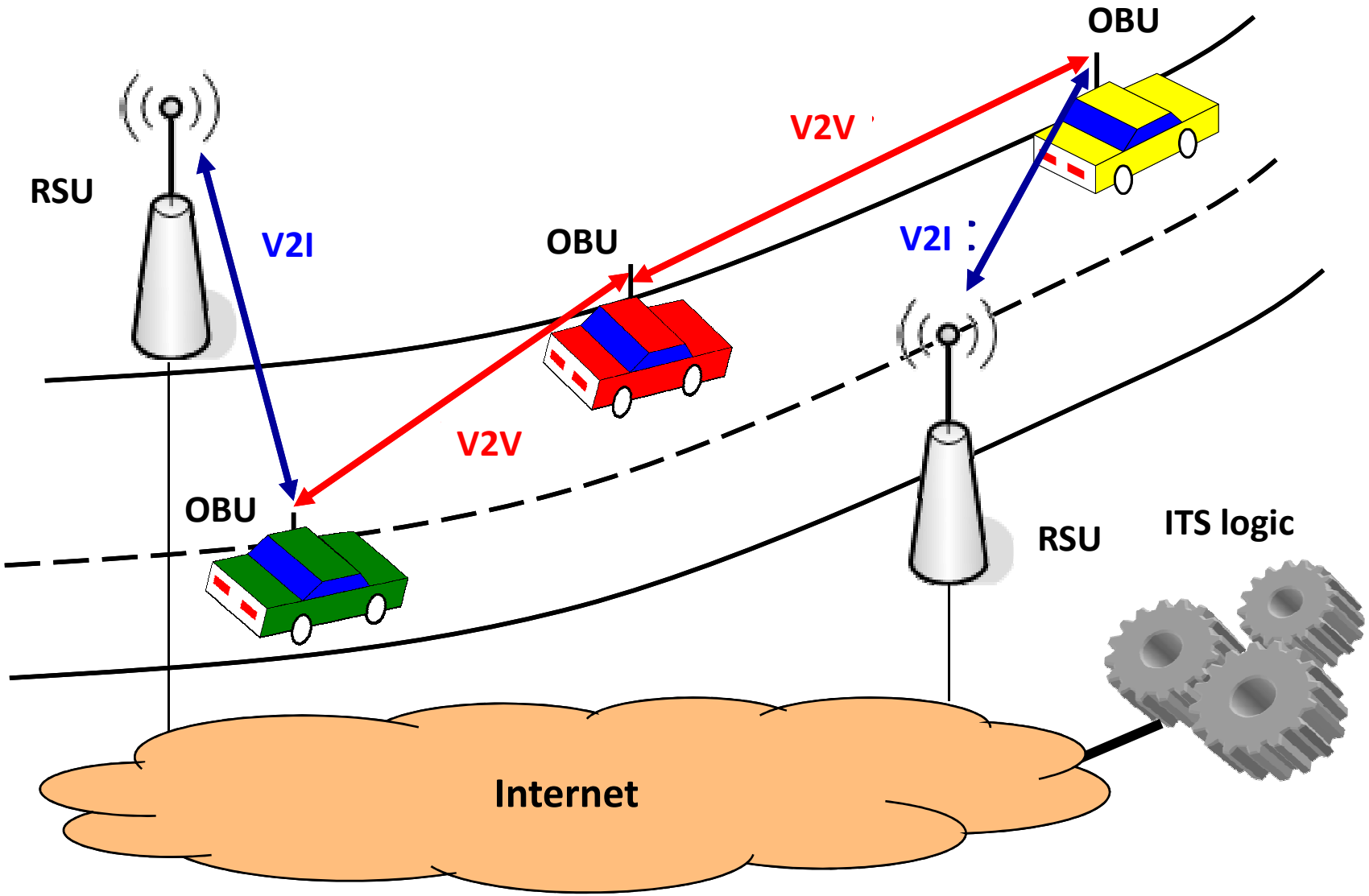
Outline

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

Inter-Vehicular Communication System

- 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 inpacting just few vehicles, …)
  - **Vehicle-to-Pedestrians (V2P)** vehicle to pedestrians / private micro-mobility (cyclists, people using wheelchairs) to warn / notify themselves of the car.

V2I and V2V modes



V2X standard approaches

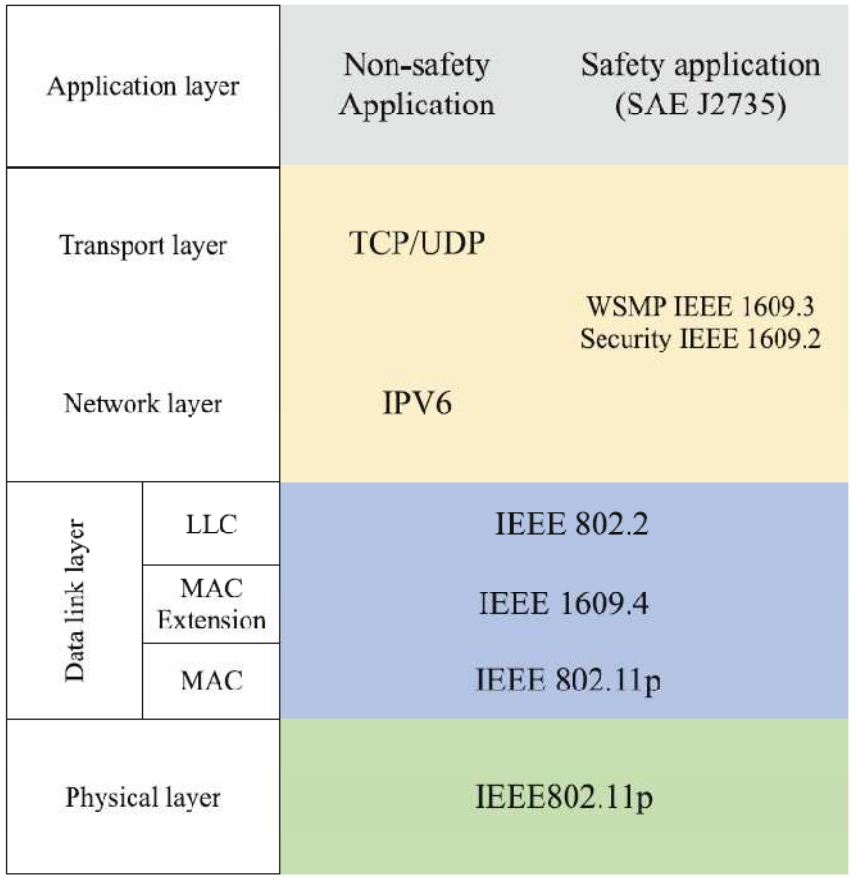
- At present, V2X standard approaches can be divided into two categories: **Short Range (IEEE 802.11p)-based vs. Long Range (cellular)-based standards**.

  - **Dedicated Short-Range Communications (DSRC**) by U.S. IEEE 802.11p-based V2X system.

  - **4G/5G Long Term Evolution – Vehicle** (**LTE-V**) by 3GPP (Third Generation Partnership Project) to support V2X services over cellular systems (Cellular V2X).

DSRC

- **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.

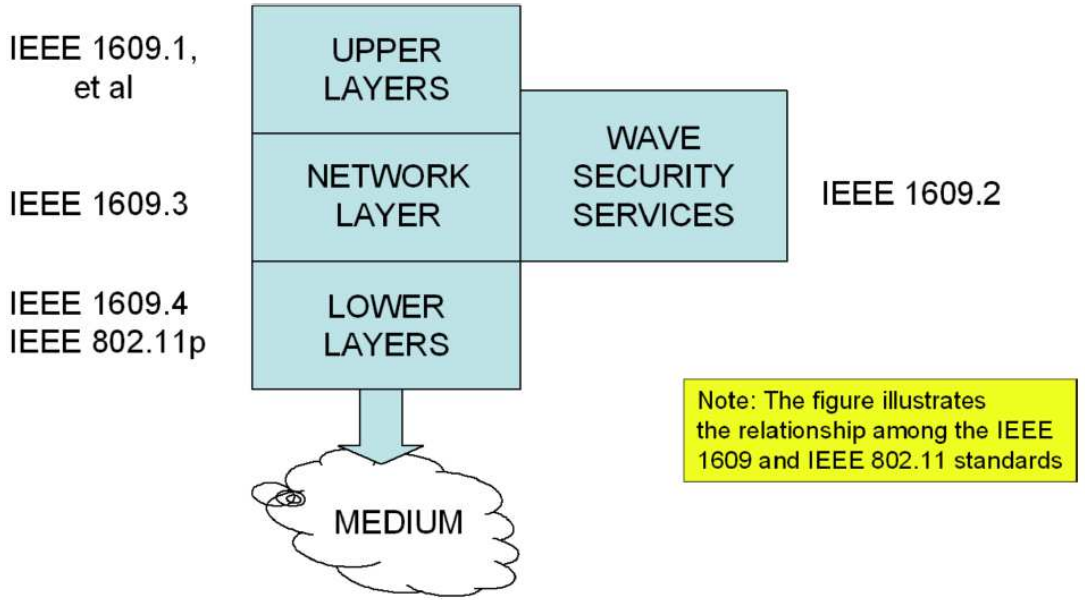


IEEE 802.11p

- IEEE 802.11p, facilitates short-range wireless communication between vehicles and infrastructure through the Carrier Sense Multiple Access (CSMA) mechanism. It enables direct V2V and V2I within the dedicated frequency band of 5.9 GHz. However, the CSMA mechanism employed by IEEE 802.11p exhibits significant limitations, particularly in high-density or congested scenarios. In such environments, frequent packet collisions occur due to the contention-based nature of CSMA, leading to increased communication delays and reduced reliability. These shortcomings severely degrade network performance, making IEEE 802.11p less suitable for applications requiring stringent quality-of-service (QoS) guarantees, e.g. ultra-reliable low-latency communication (URLLC).
- Consequently IEEE 802.11p has been widely adopted for its simplicity and low infrastructure requirements, its performance limitations in congested scenarios.
- Researchers have extensively investigated collision-free medium access control (MAC) protocols to enhance communication reliability and address the issue of high collision rates in vehicular networks by allocating dedicated time slots, frequency bands, and coding sequences to individual vehicles, thereby minimizing interference and ensuring efficient resource utilization. However, the effectiveness of such protocols heavily relies on the accurate knowledge of the communication status of adjacent vehicles. Due to the high mobility and dynamic nature of V2X environments, maintaining collision-free media access control remains a significant challenge, as the rapid changes in network topology and communication conditions complicate the real-time coordination required for optimal performance.

WAVE: IEEE 1609.x

- **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.



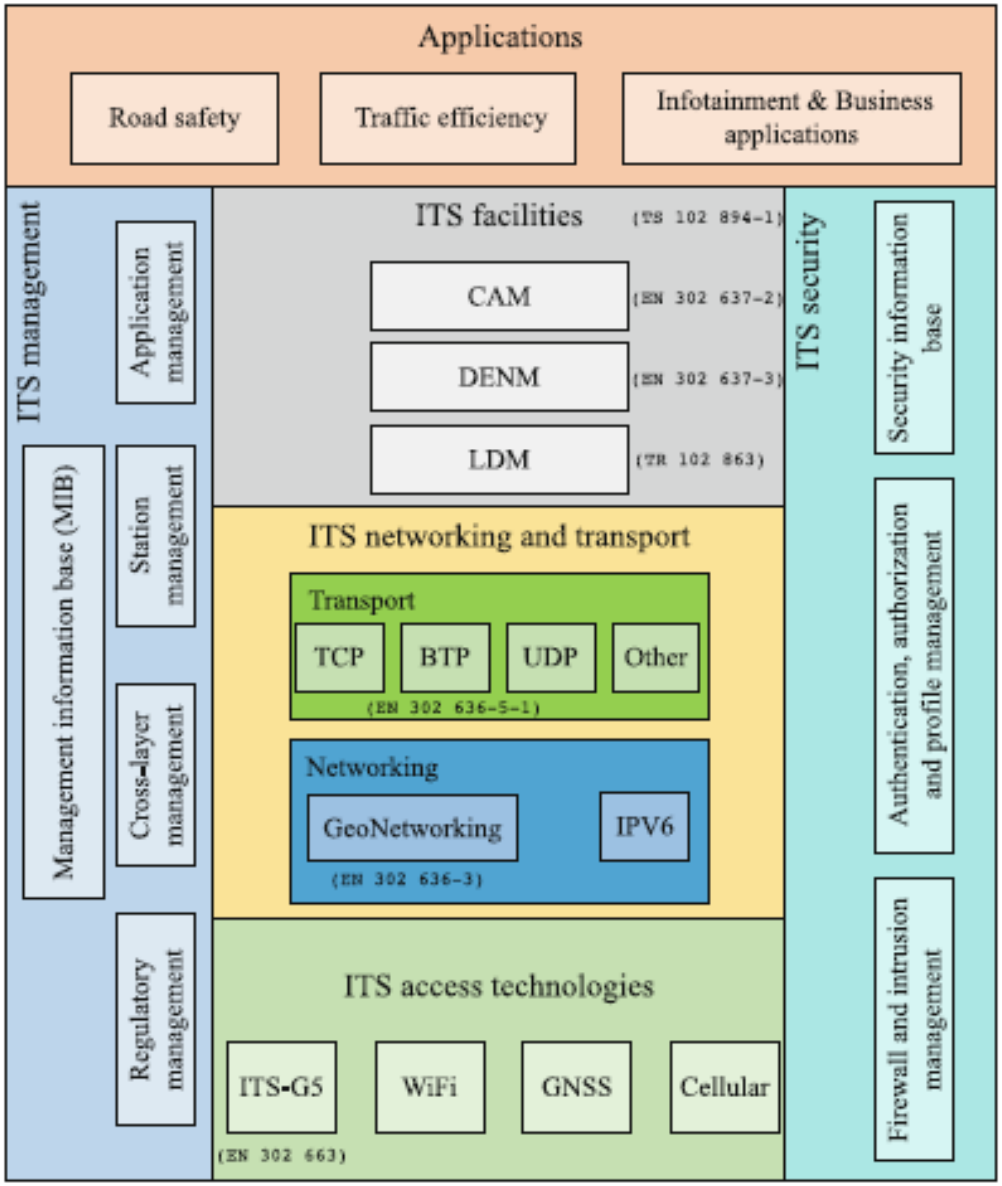
Cellular V2X

- Cellular V2X (C-V2X) offers several distinct advantages, including large capacity, wide coverage, and excellent mobility support, making it well-suited for delivering both vehicle telematics and entertainment information services. By proposing a time-division duplex (TDD) architecture for vehicle communication within the terrestrial radio access framework, C-V2X effectively mitigates collisions caused by hidden terminal problems and provides robust support for V2X communication.
- Furthermore, C-V2X introduces an enhanced device-to-device (D2D) interface, which enables direct communication between vehicles using cellular radio resources, thereby ensuring low-latency and high-reliability connectivity for V2V links. This integration of D2D technology within the cellular network framework represents a promising solution for realizing vehicle communication with stringent requirements for low latency and high reliability, addressing the limitations of traditional collision-free MAC protocols in highly dynamic vehicular environments.
- Currently, much attention has been paid to the resource management for D2D-enabled V2X communication. There are two working modes for D2D users: reused mode and dedicated mode, that is, D2D users share the same spectrum with cellular users and access dedicated radio resources respectively. Effective resource management strategies are studied to deal with interference and different QoS.

ETSI ITS-G5

- 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.

ETSI ITS-G5


Applications
Road safety
Traffic efficiency
Infotainment & Business applications
ITS management
Application management
Management information base (MIB)
Station management
Cross-layer management
Regulatory management
ITS facilities
(TS 102 894-1)
CAM
(EN 302 637-2)
DENM
(EN 302 637-3)
LDM
(TR 102 863)
ITS networking and transport
Transport
TCP
BTP
UDP
Other
(EN 302 636-5-1)
Networking
GeoNetworking
IPV6
(EN 302 636-3)
ITS access technologies
ITS-G5
WiFi
GNSS
Cellular
(EN 302 663)
ITS security
Security information base
Authentication, authorization and profile management
Firewall and intrusion management

Outline

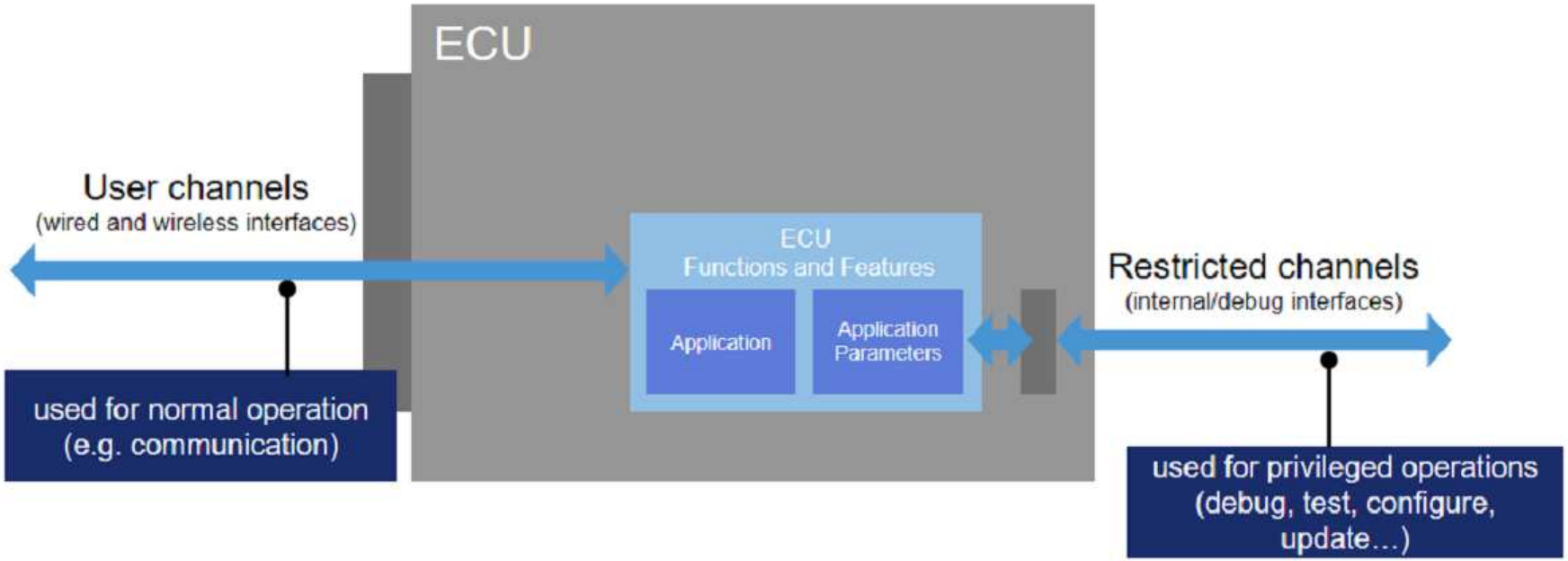
- Definition of VANET
- VANET vs. MANET
- VANET Applications
- Inter-Vehicular Communications Systems
- Intra-Vehicular Communications Systems

Electronic Control Unit

- 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.

Electronic Control Unit

- 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.

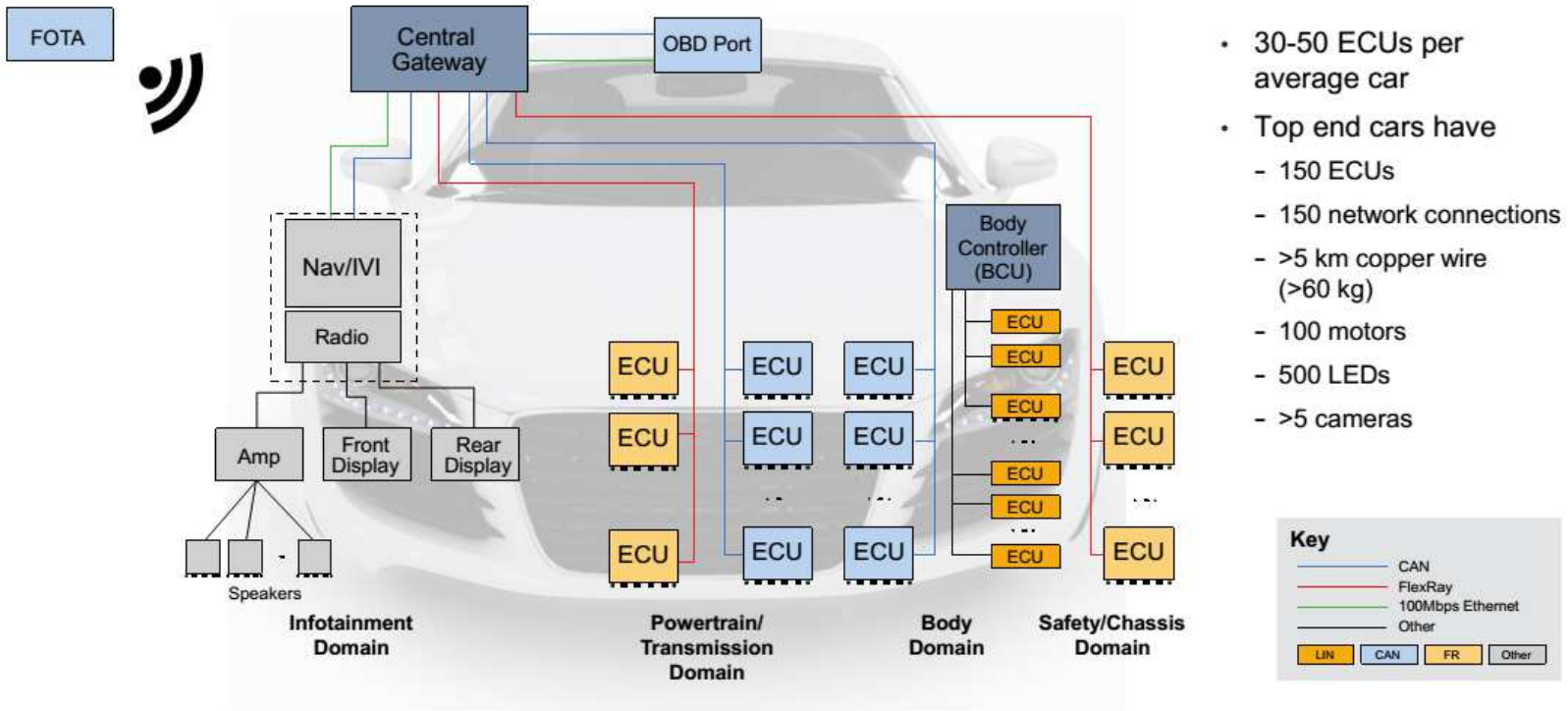


On Board Diagnostics connector

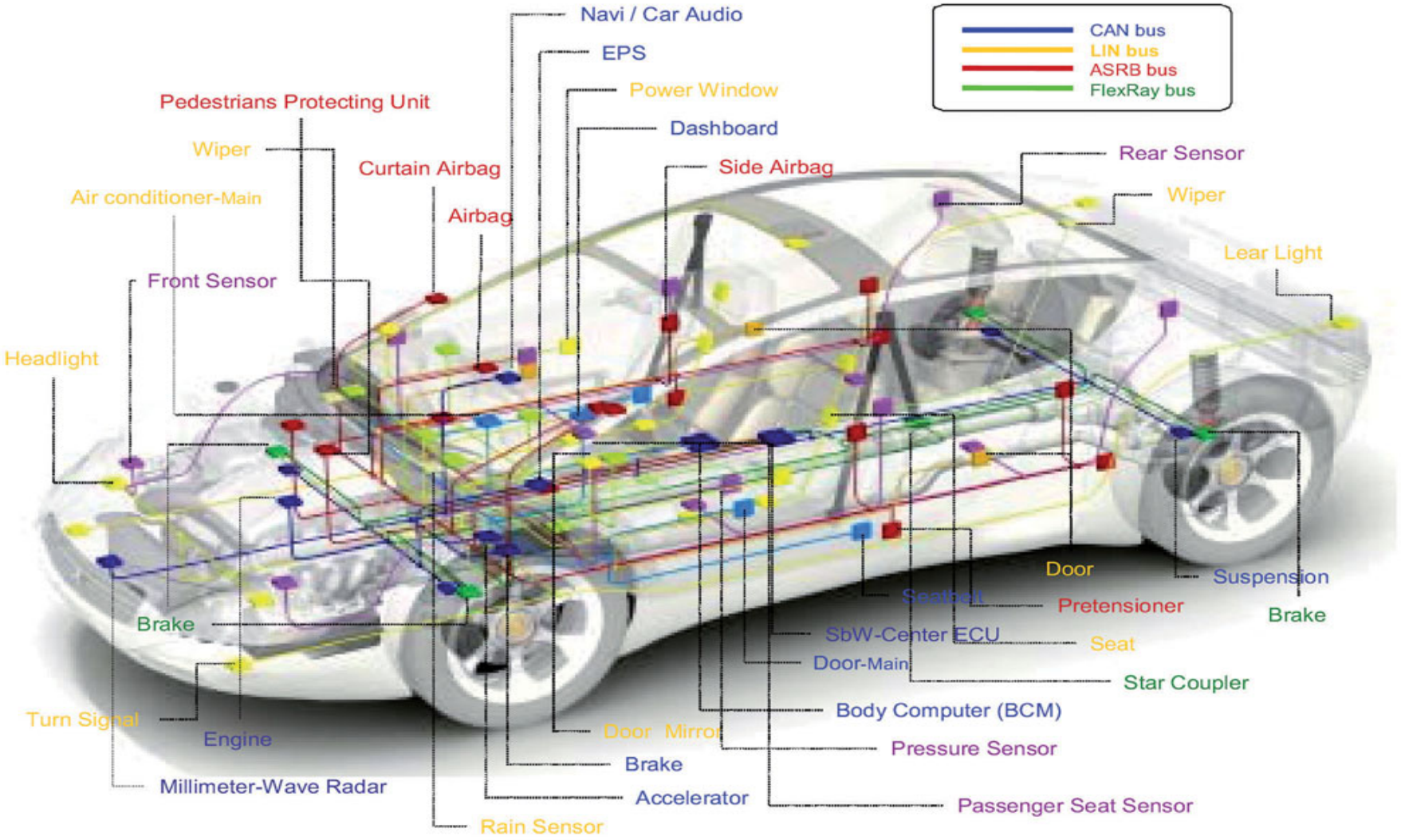
- The on-board diagnostics connector (OBD-II), originally designed as a normal user port to enable emission checks by regulations, was extended to provide a wealth of detailed diagnostic on the internals of the vehicle network that are used **for inspection and maintenance**.
- **In its current form, 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 Central Gateway

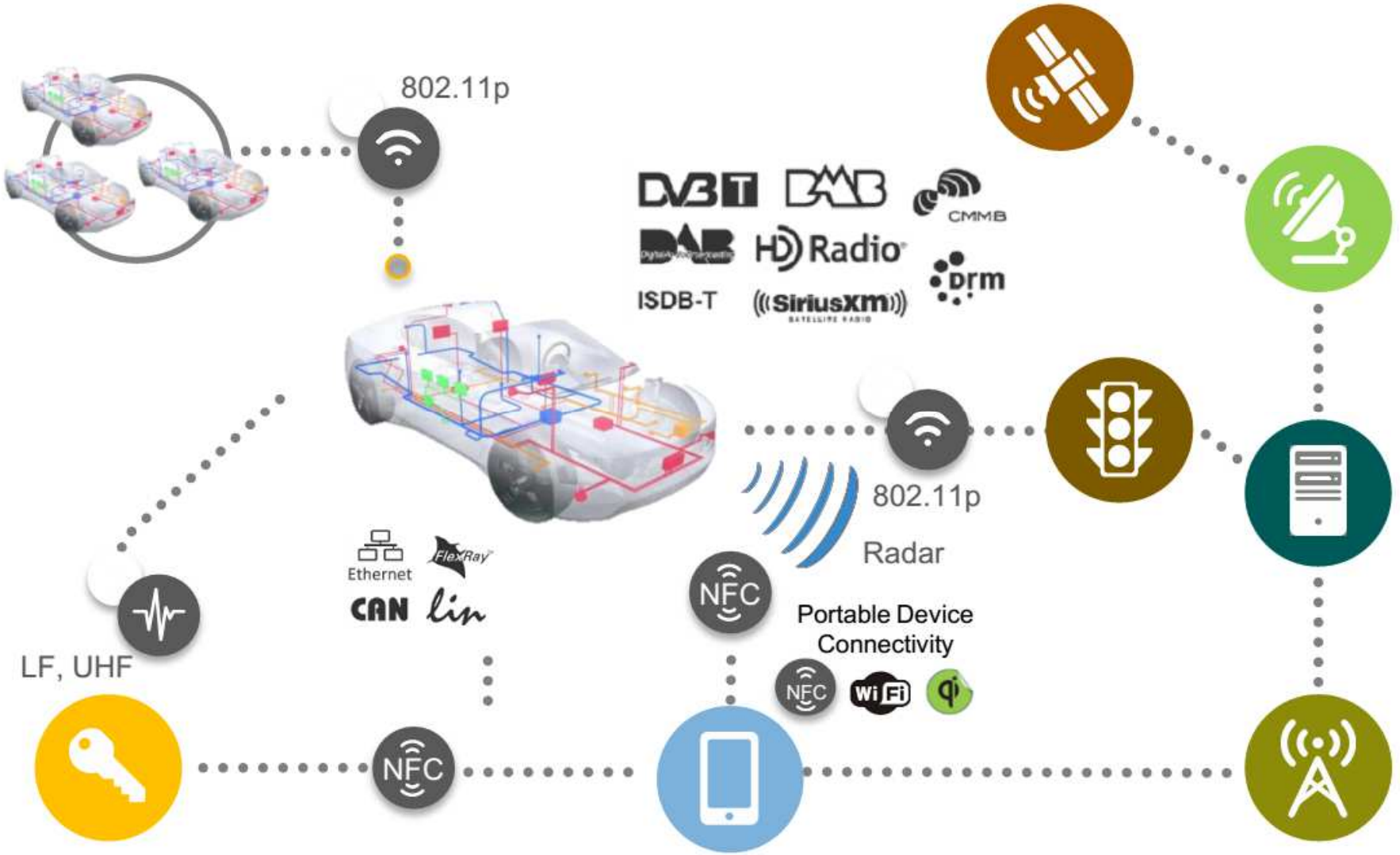
- The presence of the gateway <u>introduces a physical network isolation,</u> particularly in reference to some of the recent vehicle hacks, where the externally connected head unit was on the same network domain as safety critical ECUs controlling braking, chassis, powertrain etc. **By separating OBD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



The Connected Car



The Connected Car



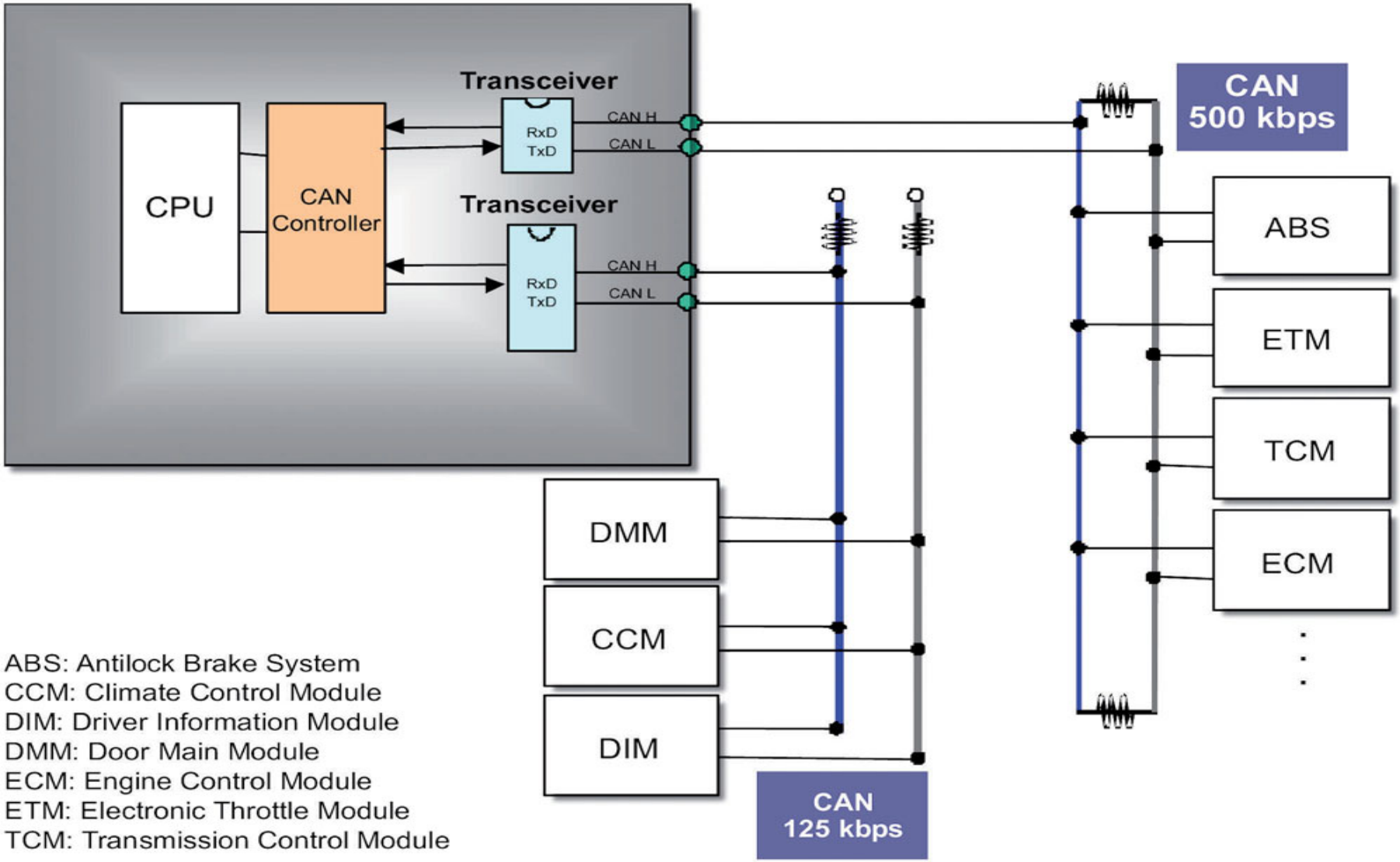
Intra-Vehicle Services

- **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.

Intra-Vehicle Communications

- IVCs are supported by different communication protocols to manage data trasfers for intra-vehicle services functions.
- Typically are serial bus: (several devices to be interconnected): for each transation, the TX devices 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 trasparency, 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 bite–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 realibility 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)

CAN-bus



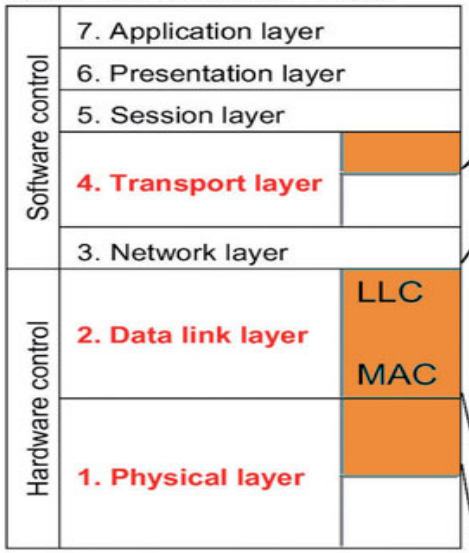
ABS: Antilock Brake System
CCM: Climate Control Module
DIM: Driver Information Module
DMM: Door Main Module
ECM: Engine Control Module
ETM: Electronic Throttle Module
TCM: Transmission Control Module

CAN-bus

- **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: t**he 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 l 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.

CAN-bus

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)

CAN-bus

Error Detecting in 5 steps:

- CAN Controller detects errorr 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 complementar 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.

The Big Picture