IoT Technologies for Connected and Automated Driving Applications

6

IoT Technologies for Connected and Automated Driving Applications

Ovidiu Vermesan[1], Roy Bahr[1], Mariano Falcitelli[2], Daniele Brevi[3], Ilaria Bosi[3], Anton Dekusar[4], Alexander Velizhev[5], Mahdi Ben Alaya[6], Carlotta Firmani[7], Jean-Francois Simeon[8], Louis Touko Tcheumadjeu[9], Gürkan Solmaz[10], Francesco Bisconti[2], Luca Di Mauro[2], Sandro Noto[2], Paolo Pagano[2], Enrico Ferrera[3], Guido Alejandro Gavilanes Castillo[3], Edoardo Bonetto[3], Vincenzo Di Massa[7], Xurxo Legaspi[11], Marcos Cabeza[11], Diego Bernardez[11], Francisco Sanchez[11], Robert Kaul[9], Bram Van den Ende[12], Antoine Schmeitz[12], Johan Scholliers[13], Georgios Karagiannis[14], Jos den Ouden[15], Sven Jansen[12], Hervé Marcasuzaa[16] and Floriane Schreiner[17]

[1]SINTEF AS, Norway
[2]CNIT – PNTLab, Italy
[3]LINKS Foundation, Italy
[4]IBM, Ireland
[5]IBM, Switzerland
[6]Sensinov, France
[7]Thales Italia, Italy
[8]Continental, France
[9]DLR German Aerospace Center, Institute of Transportation Systems, Germany
[10]NEC Laboratories Europe, Germany
[11]CTAG, Spain
[12]TNO, The Netherlands
[13]VTT Technical Research Centre of Finland Ltd, Finland
[14]HUAWEI, Germany
[15]TU Eindhoven, The Netherlands
[16]Valeo, France
[17]VEDECOM, France

Abstract

The applications of the Internet of Things (IoT) technologies connect multiple devices directly and through the Internet. Autonomous vehicles utilise connectivity when updating their algorithms based on user data, interact with the infrastructure to get environmental information, communicate with other vehicles. They exchange information with pedestrians using mobile devices and wearables and provide information about the traffic attributes and data collected by the vehicle sensors. The connected and automated vehicles (CAV) require a significant quantity of collecting and processing data and through IoT applications and services the autonomous vehicles share information about the road, the present path, traffic, and how to navigate around different obstacles. This information can be shared between IoT connected vehicles and uploaded wirelessly to the cloud or/and edge system to be analysed and operated improving the levels of automation and the autonomous driving (AD) functions of each vehicle. This chapter gives an overview of the integration of IoT devices contributing to automated/autonomous driving, and the IoT infrastructure deployed and seamlessly integrated into the AUTOPILOT project use cases and pilot demonstrators, including the IoT platforms integration.

6.1 Introduction

The continuing advancement of intelligent connectivity can provide the responsiveness needed to make automated/autonomous vehicles a reality.

Automated/autonomous vehicles make the roads much safer as human errors can be reduced significantly. Technology makes automated/autonomous vehicles possible to be deployed, and robust networks and powerful IoT solutions are essential parts to achieve this.

Intelligent connectivity enables new transformational capabilities in the mobility and transport sectors. The networks used for connecting IoT devices and vehicles must be ultra-reliable, as many critical tasks are executed remotely, and must rely on cost-effective edge infrastructure to enable low latency and scaling. Connectivity is, therefore, necessary for such services to work optimally. Intelligence enables the enhancement of user experiences through multi-access edge computing using, augmented reality (AR) and virtual reality (VR) technologies [15].

The automated/autonomous vehicles, IoT, and artificial intelligence (AI) connected systems are increasingly relying on information that is

exchanged to perform and conduct their safety-critical operations. Keeping such systems (and the data within) trustworthy, secure, safe, and private for the required cases is a critical element for the acceptance and adoption of such autonomous systems.

IoT devices and technologies can support automated/autonomous driving functions in different ways and enhance these functions for different use cases. The combined autonomous vehicles and IoT ecosystems implemented in the AUTOPILOT use cases integrate the services provided by interoperable IoT platforms and IoT devices that provide additional information to the vehicles about the environment, surroundings and the dynamic events around the vehicles to enhance the automated/autonomous functions.

The AUTOPILOT project addresses automated driving progressed by IoT and is one of the IoT European Large-Scale Pilots Programme (LSPs) [1].

6.2 Automated Vehicles Connectivity Domains

A vehicle with automated features must have established reliable interactions with different domains that are interlinked through devices and systems. The whole ecosystem relies on the interaction among the onboard units (OBUs), roadside units (RSUs), and vulnerable road users (VRUs). Intelligent sensors and actuators in the vehicles, roads and traffic control units in the infrastructures collect various information to serve enhanced automated driving (AD).

6.2.1 Internet of Vehicles

The Internet of Vehicles (IoV) concept and the Vehicle-to-Environment (V2E) or Vehicle-to-Everything (V2X) connectivity applied for enhanced automated/autonomous transportation and mobility applications, requires ecosystems based on safety, security, privacy, reliability and trust to ensure mobility and convenience to consumer-centric transactions and services. The enhanced automated/autonomous vehicles and IoT applications cover several domains of interaction, connectivity, exchange of information and knowledge as illustrated in Figure 6.1 together with communications protocols may be used [1, 13]. Based on the ITS-G5 it can be implemented a process to secure infrastructure, by providing policies and services of strong authentication of both vehicle and infrastructures and by performing more and more Risk Assessments, mapping onto requirements of the ISA/IEC 62443 set of standards. The figure shows “all” the domains of interactions between the vehicle and the environment through communication and sensing capabilities.

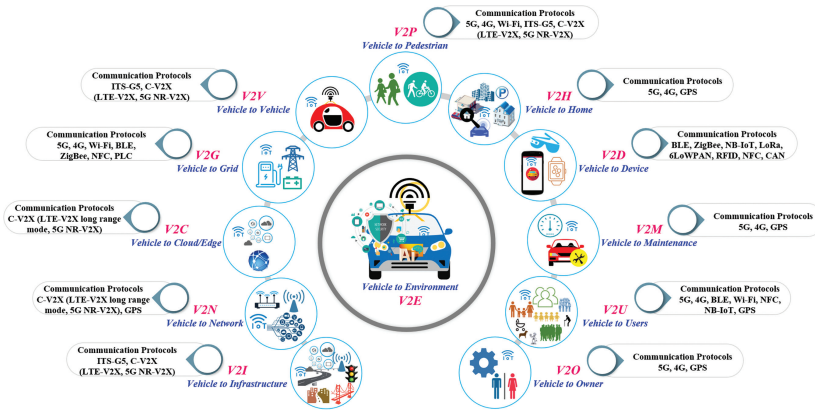

Figure 6.1 Automated vehicle connectivity domains of interaction [1, 13].

- Vehicle-to-Infrastructure (V2I) communication is defined as the wireless exchange of information between vehicles and the roadside units of the infrastructure, such as traffic, road and weather condition alerts, traffic control, upcoming traffic lights information, or parking lot information.
- Vehicle-to-Network (V2N) communication is the wireless exchange of information between vehicles and cellular networks, used for value-added services such as traffic jam information and real-time routing or available charging stations for electric vehicles (EVs).
- Vehicle-to-Cloud/Edge (V2C) communication is defined as the wireless exchange of information between vehicles and the cloud or edge computing centres, for instance, used for tracking and usage-based insurance.
- Vehicle-to-Grid (V2G) communication is wired and/or wireless exchange of information between electric vehicles and the charging station/power grid for such as battery status and correct charging and energy storage and power grid load/peak balancing.
- Vehicle-to-Vehicle (V2V) communication is defined as the wireless exchange of information between vehicles about, for instance, speed and position of surrounding vehicles.
- Vehicle-to-Pedestrian (V2P) communication is the wireless exchange of information between vehicles and vulnerable road users (VRUs) for safety-related services.
- Vehicle-to-Home (V2H) communication is the wireless exchange of information between vehicles and a fixed or temporarily home, for instance, used for real-time routing.

- Vehicle-to-Device (V2D) communication is wired and/or wireless exchange of information between the vehicle and IoT devices either inside or outside the vehicle.
- Vehicle-to-Maintenance (V2M) communication is the wireless exchange of information between the vehicle and the vehicle condition responsible (automotive manufacturer or repair shop), including vehicle condition monitoring, predictive maintenance notification or alerts.
- Vehicle-to-Users (V2U) communication is the wired/wireless exchange of information between the vehicle and its current user, including situational details.
- Vehicle-to-Owner (V2O) communication is the wireless exchange of information between vehicles and its owner. Use cases may be vehicle rental, fleet management, freight tracking, etc.

The convergence of enhanced automated/autonomous vehicles, IoT and AI applications are accelerating the implementation of V2X concept and the move to mobility as a service (MaaS) and tier-one automotive companies, large technology companies and technology start-ups active involved in V2X, addressing first safety, security and privacy use cases to accelerate user acceptance and innovation. The overall interactions are covered under the name of V2X and consists of the following [1, 13]:

- The communication and sensing interactions between the autonomous vehicle and the dynamically changing environment.
- The communication and sensing interactions between the vehicle and its static environment.
- The communication and sensing interactions with different service providers.
- The communications with the owners, users, mobility service providers.

There are two key technologies considered for intelligent transportation systems (ITS), namely ITS-G5 and C-V2X, which are based on different design principles and radio interfaces [1, 13, 14]. However, the higher layers (above the PHY/MAC radio layers) can mainly share the same protocol stack. The two technologies are primarily intended for driver assistance warnings rather than autonomous driving but contribute to extending the line-of-sight limited operation of sensors such as cameras, RADARs and LiDARs.

ITS-G5 is defined by ETSI, and its radio air interface is based on IEEE 802.11p (DSRC in the US), which is an approved amendment of the Wi-Fi standard to add wireless access in vehicular environments (WAVE). ITS-G5 works independently of cellular networks, it supports V2V and V2I

low latency short-range communication in the 5.9 GHz frequency band and uses orthogonal frequency-division multiplexing (OFDM) and a carrier sense multiple access (CSMA) based protocol in the MAC layer. ITS-G5 facilitates high reliability under high vehicle speed mobility conditions. Enhancements towards more advanced services such as autonomous driving are addressed by the IEEE 802.11 Next Generation V2X Study Group.

C-V2X is specified by 3GPP and is realised as LTE-V2X (3GPP rel. 14/15) for short- and long-range communication. The short-range mode can work independently of cellular networks, supports V2V, V2I and V2P communication, uses direct side-link communication over PC5 interface, uses orthogonal frequency-division multiplexing (OFDM) in the 5.9GHz frequency band, and its MAC layer is based on semi-persistent scheduling allowing deterministic sharing of the medium among multiple stations in a distributed manner. The long-range mode is cellular mobile network-dependent and supports V2N communication, i.e. up-/down-link communication between vehicles and base stations in a cellular LTE network over Uu interface. The next release 5G NR-V2X (5G New Radio V2X, rel. 16) addresses improvements such as lower latency, increased reliable communication, and higher data rates to support autonomous driving. 5G NR-V2X will complement LTE-V2X, i.e. not replace but co-exist with LTE-V2X.

LTE-V2X short-range mode and ITS-G5 are substitutes, but LTE-V2X has been shown in recent tests to have a superior performance in range/link-budget (reliability) [14]. However, ITS-G5 is not an equivalent replacement for LTE-V2X for providing C-ITS priority services. ITS-G5 provides different performance compared to LTE-V2X in direct side-link short-range communications and does not support long-range communications. The current, ITS-G5 cannot achieve the level of implicit compatibility between LTE-V2X and 5G-V2X, due to the different technological and design principles in the specifications of IEEE 802.11p (ITS-G5) and 3GPP C-V2X (LTE-V2X/5G-V2X). LTE-V2X is the natural precursor to 5G NR-V2X from the perspectives of the design and industrial ecosystem. The combination of these two V2X technologies can allow for the most cost-effective deployment of C-ITS services in EU [14].

A vehicle with automated features must establish interactions with different domains that are interlinked with one or more operational design domains like the use cases established in the AUTOPILOT project [1], namely the Automated valet parking, Highway pilot, Platooning, Urban driving, and vehicle sharing use cases. In this context for enhanced automated/autonomous vehicle applications, four connectivity domains are

defined as essential connectivity building blocks of the IoT ecosystem in the AUTOPILOT project, namely V2V, V2P, V2D, and V2I. The IoT ecosystem relies on the interaction among the vehicles, the VRUs like pedestrians, a variety of devices and the infrastructure; to improve traffic management by increased efficiency, security and safety. Intelligent sensors and actuators in the vehicles, roads and traffic control infrastructures collect a variety of information to serve enhanced automated driving. These require robust sensors, actuators, and communication solutions, which can communicate with the control systems while considering the timing, safety and security constraints. Redundancy and parallel systems are required in all safety and security-critical applications. It is also worth mentioning that power saving mode, for example, for sensors and actuators, can be a barrier to real-time information. For battery-powered equipment, it will be a trade-off between power consumption and communication latency.

To mitigate the risks for the autonomous driving systems and infrastructures, security should be implemented at all layers and security policies should be defined following international standards and best practices. This can be achieved using existing frameworks like the ISA IEC 62443 [16].

6.2.2 Vehicle-to-Vehicle Domain

Vehicle-to-Vehicle (V2V) communication is defined as the wireless exchange of information (data) between vehicles. V2V communication facilitates the transfer of information and early warnings/control to ensure traffic safety, avoid traffic congestion, improve traffic flow and environment, etc. Interconnectivity between vehicles plays an important role in autonomous driving. High-speed environments and reliable real-time information are important issues for the V2V ad-hoc communication network, also referred to as VANETs (vehicular ad-hoc networks) or IVC (inter-vehicle communication) [11]. Examples of relevant standards are ETSI ITS-G5, IEEE 802.11p, IEEE 1609, and SAE J2735.

In the AUTOPILOT project at the French pilot site [1, 12], V2V communication is used in a platooning use case. This communication is made over ETSI ITS-G5 (IEEE 802.11 OCB) to allow the exchange of information between the vehicles forming the platoon. This information will be used to place the vehicles according to the others. The goal is to ensure that the platoon is not broken and that all vehicles are capable at any time to cross an intersection, for example. All the relevant information about the platoon is displayed to the driver on the embedded screen.

In the AUTOPILOT's Dutch pilot site, V2V communication is established via ITS-G5 connections and additionally a ultra-wide band (UWB) connection. An alternative approach for V2V information exchange is via IoT technology, using a MEC based local cloud service that forwards messages coming from one vehicle to another. In the AUTOPILOT's Spanish pilot site, V2V communication is performed by using the IoT in-vehicle platform system. To verify the impact of the fully IoT communication system, this V2V communication is achieved through the infrastructure and using standard oneM2M messages. These messages wrap the defined data models that allow IoT communication with the vehicle. Therefore, if a vehicle needs to send its information to other vehicles, that one will upload the corresponding message to the cloud, which later will be available for any other connected vehicle.

In AUTOPILOT's Italian pilot site, V2V communication is managed by an in-vehicle platform that implements an almost full ETSI stack. The main exchanged V2V messages are cooperative awareness messages (CAM). This information is used to provide a detailed look at the surroundings of the automated vehicle. CAM messages notify the information sensed by the in-vehicle sensors to the vehicles in the transmission range. This information is used by the automated driving data fusion algorithm to make decisions for both highway and urban driving use case scenarios. In the AUTOPILOT's Finnish pilot site, the vehicle is equipped with 4G/LTE communications. The vehicle ETSI ITS-G5 station transmits CAM messages regularly, and the vehicle position is also sent to the IoT platform, for use by other services.

6.2.3 Vehicle-to-Pedestrian Domain

Every year, many vulnerable road users (VRUs) are seriously injured or killed in accidents. Improved connectivity solutions can contribute to reducing the number of these fatalities thanks to an effective warning system for the involved actors. Vehicle-to-Pedestrian (V2P) connectivity is a field of research that studies the communications between vehicles and pedestrians. In the broadest sense, it typically considers bicyclists and motorcyclists, children in strollers, mobility-impaired people with wheelchairs, etc. However, these may also be classified as vehicles in V2V connectivity, if for example the communication unit is bicycle equipped and not used as wearables, mobile phones, etc. The goal of the V2P connectivity is to detect a pedestrian or more generally a VRU and notify information useful to avoid accidents.

The more intuitive device to warn pedestrians is through a smartphone or even a smartwatch, due to its increasing computational power, the availability

of wireless connection and its widespread availability. Today's incumbent standard for vehicular communication is ETSI ITS-G5 that is based on the IEEE 802.11p amendment of Wi-Fi standard. Unfortunately, while Wi-Fi is supported by most smartphones, IEEE 802.11p is not implemented in commercial products yet [1, 12]. In 2014 Qualcomm and Honda, published a paper that describes a real implementation of this idea [2]. The prototype is made with a smartphone equipped with a Qualcomm Wi-Fi solution. As reported in the original paper: "The design goal was to provide an always-on, highly accurate and low latency pedestrian collision warning system, without introducing significant hardware or processing overhead to the smartphone". The paper states that good performances can be achieved, although some problems still need to be solved. Among the others, the accuracy of the position is given by the internal GNSS receiver of the smartphone, the congestion of the wireless medium and the certification of communications and application performances. Indeed, the certification procedure changes a lot depending on whether the application is considered as a supplemental alert or as a complete safety-critical warning system. A more recent prototype, created by Bosch, addresses motorcyclists is shown a video on YouTube [3]. An alternative approach is to exploit the cellular communication channel, owing to its complete availability on mobile devices. Waiting for the complete definition of LTE-V2X and 5G, several papers explored this idea showing good performances. In "Cellular-based vehicle to pedestrian (V2P) adaptive communication for collision avoidance" presented in 2014 [4], this approach is theoretically described, also taking into account the road-safety system in terms of energy consumption on the smartphone. In other papers, LTE communications are used, together with Wi-Fi, to exploit the advantages of both channels, i.e. the more extended communication range of LTE and the low delays of Wi-Fi direct communication. A further example is a study on the use of a pure Wi-Fi solution in "Vehicle to pedestrian communications for protection of vulnerable road users" presented in 2014 [5], which demonstrates the possibility of effectively using such a channel for safety purposes.

A different vision is to use different radio systems, with a dedicated transmitting device carried out by the VRUs. The system can be used to compute the distance and the position of the users without the need of a GNSS device and the related issues (e.g. accuracy in urban areas). One of the most important works in this sense is done in the Ko-TAG project (Security for vulnerable road users through Ko-Tag) [6], which uses an RFID-like approach.

In the AUTOPILOT project's Dutch pilot site [1, 12], a smartphone application is developed which connects to the Huawei OceanConnect IoT platform and the oneM2M platform. This smartphone application uses Global Positioning System (GPS) localisation to localise the VRUs in the area. This information is used to inform the vehicle of a possible VRU on the road where the vehicle is also driving. The vehicle must adapt its speed accordingly. Also, the other way around, the vehicle is sending its location to the smartphone using oneM2M, in order to warn the VRUs of an automated driving vehicle approaching. ITS-G5 beacons are used, in addition to the smartphone, to correlate the data transmitted from the smartphone with the location transmitted from the ITS-G5 beacons.

Finally, a Wi-Fi sniffer is used to detect surrounding Wi-Fi enabled devices, which can be used to detect crowdedness by detection of pedestrians and cyclists in the area, using their smartphone or other devices as trackers. While Wi-Fi detection applies to smartphones in the vicinity based on Wi-Fi sensing range (i.e. about 30 meters in outdoor scenarios), filtering mechanisms based on received signal strength indication (RSSI) levels may be used to detect only pedestrians closer to the vehicle. Due to the relatively low position accuracy utilising this technology, the output (number of devices detected and location of detection, logged by GPS) will only be used to map a crowdedness mapping of the area and not to individually position VRUs with smartphones. This information will then be used to inform other automated driving vehicles on how many VRUs are on a certain road, so they can adequately decide to take the less crowded routes.

6.2.4 Vehicle-to-Device Domain

In the AUTOPILOT project's French pilot site, the car/vehicle-sharing use case relies on a mobile application that allows the user to unlock and start one's vehicle. The system consists of an onboard unit that communicates with the mobile app via Bluetooth Low Energy (BLE). An embedded interface is also developed to display information about the vehicle to the driver, via an Android tablet that communicates with the vehicle through a serial and an Ethernet link. The serial link is used to communicate with low- level network in the vehicle and display failures, etc. The Ethernet one is used to communicate with the automated driving units and, for example, to guide the driver during the switch between manual and autonomous driving and autonomous and manual driving. During the car/vehicle-sharing use case, this interface displays its position on a map to the user. This position comes from

the vehicle GPS through the Ethernet link. It also displays an alert when the vehicle enters a zone where the autonomous driving is allowed and when the vehicle is approaching the end of this zone. In the vehicle rebalancing use case, this interface is used to display the state of each vehicle in convoy.

In the AUTOPILOT's Dutch pilot site, V2D connectivity is used in platooning and automated valet parking use cases. In the platooning use case, the drivers are notified in their vehicle by a platoon manager service about the platoon status and related information. It uses an existing screen on the dashboard, which was modified for this purpose. Additionally, the lead driver of the platoon is informed about speed and lane advice via an Android on a dedicated smartphone. In the automated valet parking (AVP) use case, the vehicle communicates with an Android smartphone via an IoT platform using a 5G/LTE communication network. The AVP application running on the smartphone receives information such as vehicle state (e.g. current vehicle position, current AVP action and phase) and can send commands like "park" or "collect" to the vehicle. The data to be exchanged over the IoT platform has been defined in detail by the DMAG (data modelling activity group).

In AUTOPILOT's Italian pilot site, the vehicular IoT bridge should enable bidirectional semantic-full communications between vehicles and application entities both in-vehicle and in roadside infrastructure nodes. The bridge contains a processing unit able to manage all communication interfaces; an IEEE 802.15.4 wireless interface, an OBD/CAN interface, the IEEE 802.11p (ETSI ITS-G5) transceiver and the 4G modem for cellular communication. At the network layer, the bridge should be able to address 6LoWPAN destinations (to talk with the onboard WSN) and to address other C-ITS station using the GeoNetworking protocol. From outside, the bridge should be addressable as an IP node. The bridge should, at least, handle at the transport layer UDP (User Datagram Protocol) and BTP (Basic Transport Protocol) [2] and, at the application layer, CoAP communications. It also requires a bridge to abstract all the onboard generated data. This involves the abstraction of all the data that are shared on the OBD/CAN network. Therefore, it should be able to read the main messages in accordance with OBDII standards and to aggregate them with the information coming from a wireless sensor network. In the Italian pilot site use cases, the IoT bridge is an OBU developed so that it can manage several different devices (V2D): it will manage the connection to a tablet that will be used as HMI and as a sensor for vibration data. The OBU will also interface with an inertial measurement unit (IMU) via CAN and with a 6LoWPAN dedicated vibration sensor.

Moreover, to segregate the OBD/CAN from the V2X and sensors network traffic a secure gateway is implemented onboard preventing that undesired communication can happen between non-safety critical onboard zones and safety-critical onboard zones.

6.2.5 Vehicle-to-Infrastructure Domain

Within the platooning use case in the city centre of Versailles at the AUTOPILOT's French pilot site, the platoon must pass through two complicated crossroads. To do so, it is necessary to have V2I communication. When the platoon is approaching, the complicated intersection, the RSU detects the lead vehicle and passes the message on to the traffic light controller for it to change its phase in order to give priority to the platoon. The traffic lights interrupt their usual phase and switch specific traffic lights to the correct green/red combination so that the platoon can cross safely. Once the RSU has communicated with the cloud through the oneM2M server, the OBU is informed on whether the platoon can continue following its route. Once the platoon has gone past the junction, it goes back into its classic functioning mode. The traffic assist architecture for platooning is illustrated in Figure 6.2.

In the AUTOPILOT's Dutch pilot site, V2I connectivity is used in the highway pilot, platooning and automated valet parking use cases. Concerning

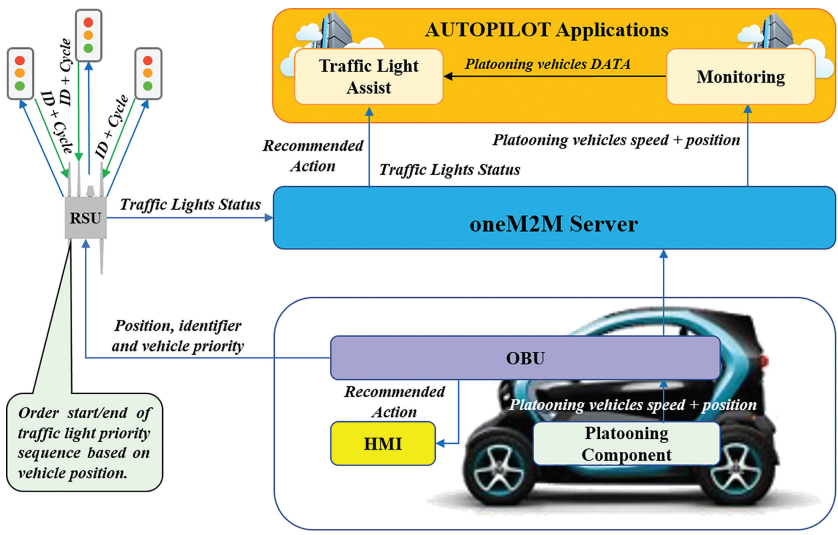

Figure 6.2 Traffic light assist architecture for platooning in complicated crossroads, (example from AUTOPILOT French pilot site) [1, 12].

the highway pilot use case, all exchanges to and from the vehicles go through the infrastructure. There are four major components of the system: detection (of anomalies by leading ego vehicles), reporting (of anomalies to the cloud), validation (or learning of hazards presence) and information (for the control of following vehicles). However, only the reporting and information components rely on V2I communication:

- For reporting, the vehicle communicates with the cloud with MQTT and HTTP over a 4G connection.
- For information, the vehicle communicates with the map provider with Web Socket and HTTP over a 4G connection.

The platooning use case uses V2I communication in the following different ways:

- Broadcasting CAM messages via ITS-G5 that are intercepted by the instrumented facility along the highway to support vehicle detection.
- Exchanging platoon status information with the cloud-based platoon manager service that involves IoT (oneM2M) and cellular (commercial 4G) technology.
- Publishing data to and retrieving data from an IoT-enabled (oneM2M) local dynamic map service deployed at the roadside. This concerns data that can be used to increase the environmental perception of IoT connected vehicles (platoon vehicles and other vehicles). The communication channel is realised through the Hi-5 pre-5G network, which provides coverage over a part of the road through a base station.
- Status information of four traffic light controllers controlled by RSUs; one on each successive junction on the road are received by the MQTT clients. The data in binary format is converted to JSON format with the ASN.1 decoder and published to the respective containers on the oneM2M platform. The binary data is also published to the oneM2M MQTT broker. All services and vehicles subscribed to this service can pick up this data.

The automated valet parking (AVP) use case:

- Parking spot occupancy and obstacle detection: The AVP use case features a stationary roadside camera and the micro aerial vehicle (MAV) as infrastructure devices. The MAV and the camera detect free parking spots and obstacles and send this information to the vehicle via the AVP parking management service (PMS) application. The vehicle communicates with the infrastructure devices using the IoT platform over the cellular network connectivity (e.g. 5G/LTE).

- The MAV detects the free parking spots and obstacle, processes the data and publishes the parking spot and obstacle status information to the IBM Watson IoT platform. The parking management service application, as an IoT application, registered by the Watson IoT platform, receives this data over MQTT and publishes it to the AVP vehicle.
- Roadside stationary camera: The traffic manager application is providing parking spot status and obstacle status update information, and deep learning algorithms send out parking spot status and obstacle status (along the access road to the parking lot). These algorithms are running in the servers and use an advanced message queuing protocol to communicate with the parking spot entity, which then publishes them to the containers' resources in the oneM2M platform. The data are updated to a Watson-specific format and published. The vehicle subscribed to this information gets these updates from the oneM2M platform. The data in the Watson-specific format is subscribed by an interworking proxy, which then forwards it to the IBM Watson platform. The vehicle or the parking management service application receives these data from Watson IoT platform over MQTT. For evaluation purposes, the parking spot entity also forwards the data directly to the IBM Watson platform. The data flow diagram is shown in Figure 6.3. The AVP data models follow the SENSORIS and DATEX data models, which are currently being standardised (for AUTOPILOT community) in the data modelling activity group (DMAG).

In the AUTOPILOT's Italian pilot site, V2I connectivity is managed using two different channels. The first one is the classic DSRC, used to exchange decentralised environmental notification messages (DENMs) with the RSUs and SPaT/MAP messages with the traffic lights. The second channel is LTE, mainly used to send information to the oneM2M platform. V2I connectivity is used in the highway, urban and highway driving use cases, and the DENMs are used to notify alert sensed by the IoT devices. More in details:

- Highway driving use case – For puddle detection, some dedicated 6LoWPAN sensors will detect a puddle. The sensors are connected to an RSU that sends the information directly to the surrounding vehicles using a DENM message. The same information is sent by the RSU to the oneM2M platform (via the cellular network) and then, through the cloud, it is validated from the Traffic Control Centre and sent back to the relevant RSUs and to the approaching vehicles, using both the LTE and the ETSI ITS-G5 channels. The information is sent in the

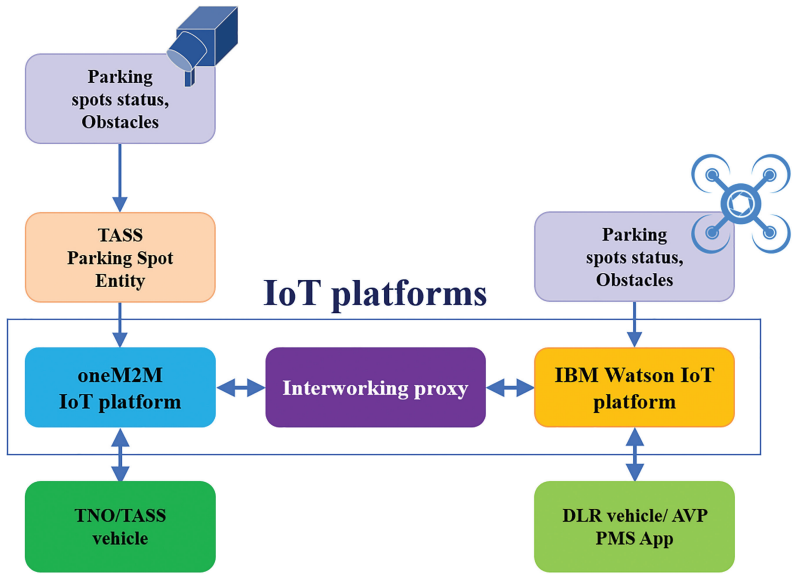

Figure 6.3 Interaction between the AVP devices and the IoT platforms [1, 12].

form of a different speed limit for the portion of highway affected by the puddles. In this way, both short and long-range communication are covered. As a further option, also NB-IoT water sensors are used: in this case, the information about the water level is transmitted straight to the oneM2M platform via a cellular network and then consumed from the applications that generate the alert messages. As for road works' warning, a notification is sent from the Traffic Control Centre to the oneM2M platform and then consumed by both the RSU, to notify the vehicles via ETSI ITS-G5, and the e-Horizon cloud application that dynamically updates the maps onboard the vehicles. The road works can be fixed or mobile.

- Urban driving use case – For pedestrian red-light violation, the pedestrians are detected thanks to a smart camera. The information is combined with the status of the pedestrian lights, and in case of violation, a message is sent using a DENM notification. The message is also sent to the oneM2M platform. For fallen bicycle detection, a bicycle is equipped with an IoT in-vehicle platform. This device will be equipped with sensors that permit to detect when the bicycle has fallen. This information is automatically sent via DENM by the bicycle. If the message is received by an RSU, this will be sent to the oneM2M platform.

- Highway and urban driving use cases – For pothole detection, the in-vehicle platform will act as a "virtual sensor" for vibration. The information can be taken by a 6LoWPAN sensor, a smartphone/tablet or an inertial measurement unit (IMU). The "virtual sensor" can work with only one source of information or combines different sources. When a pothole is detected, a message is sent to the oneM2M platform where it becomes available for subsequent usage by all the other vehicles. Additionally, the OBU reports to the oneM2M platform also an idea about the status of the road surface depending on the data coming from the sensors.

V2I communications are used to report relevant information coming from IoT to the oneM2M platform. These data are then used to give useful feedback to the autonomous driving function.

In the AUTOPILOT's Spanish pilot site, the V2I connectivity is supported with both cellular network connectivity and Wi-Fi. Through these channels, the bidirectional IoT communication will be performed, sending and receiving messages following the oneM2M standard in the urban driving and automated valet parking use cases.

Urban driving use case:

- Traffic Lights: In the pilot site, the different involved traffic lights will be connected to RSUs. These RSUs are monitoring the status of the traffic lights and publishing it to the IoT cloud platform (IBM Watson). These statuses are obtained by the in-vehicle IoT platform through an urban server, which will be providing and filtering this information to any connected vehicle.
- Vulnerable Road Users (VSUs): In order to detect VRUs, a smart camera is used, located in the surroundings of the road. This camera detects any pedestrian located in a relevant area and sends a VRU event message to the IoT cloud platform (IBM Watson). Afterwards, this information is collected by the mentioned urban server, which will provide and filter it to any connected vehicle.
- Hazards: In order to obtain the different hazard events that might occur, the control management system of the public authorities is used. By using a module that obtains the different hazard events and translates them to IoT messages, publishing them to the Watson IoT platform, these hazards are available to any vehicle connected to the same urban server.

Automated valet parking (AVP) use case:

- Drop-off and pick-up: A parking management system is developed. This parking management system can forward the user's command of pick-up and drop-off to the vehicle. Also, this system can detect VRUs that afterwards would be published to the IoT platform in the same way that it is done for the urban driving use case. The in-vehicle platform can then receive these commands and VRU events adapting its behaviour.

V2I communications are used to report relevant information coming from the IoT platform. This data is then used to give useful feedback to the autonomous driving functions.

In the AUTOPILOT's Finnish pilot site, V2I connectivity is supported with cellular 4G/LTE communications. In urban driving and automated valet parking use cases, communication is as follows:

Urban driving use case:

- Traffic Lights: Real-time information on signal state and the next phase is available both through cellular communications, through connection to the traffic light operator's server.
- Vulnerable road users (VRUs): In order to detect VRUs, a smart camera is used, which is installed at a mobile RSU. This camera will detect pedestrians and cyclists located in a relevant area and send a VRU event message to the IoT cloud platform. From there, the information will be made available to the vehicle.

Automated valet parking (AVP) use case:

- Traffic cameras, installed at the mobile RSU, monitor the parking area and detect objects and pedestrians either at the parking spaces or on the potential vehicle paths, and send the information to the IoT platform.

6.3 Automated Driving Use-Cases and Applications

In the AUTOPILOT project, five different use cases are developed and implemented in two or more of the pilot sites established in the project. An overview of the pilot sites and their respective use cases (denoted "+") are given in Table 6.1 [1, 12].

This includes connectivity with IoT devices, connectivity between vehicles, infrastructure and other sensors to enhance automated driving capabilities and technology that allows vehicles to monitor the state and availability of different services. As for the in-vehicle functions, three main groups of sensor systems such as camera-, RADAR- and LiDAR-based systems, together

Table 6.1 Pilot sites and use cases in the AUTOPILOT project [1, 12]

Pilot Sites vs. Use Cases	France (Versailles)	Italy (Livorno-Florence)	The Netherlands (Brainport)	Spain (Vigo)	Finland (Tampere)
Automated Valet Parking (AVP)	–	–	+	+	+
Highway Pilot	–	+	+	–	–
Platooning	+	–	+	–	–
Urban Driving	+	+	+	+	+
Car/vehicle Sharing	+	–	+	–	–

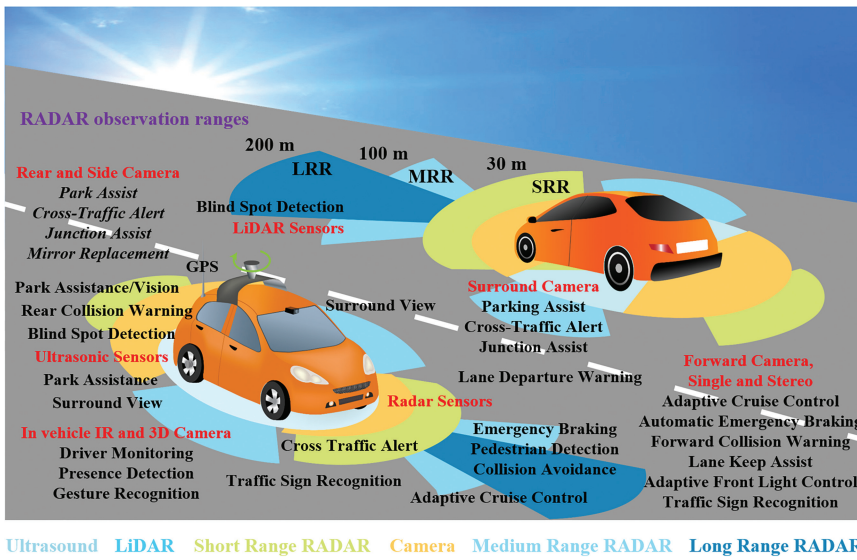

Figure 6.4 RADAR observation ranges, sensors, actuators and functions [7].

with ultrasonic sensors, are used for autonomous driving, as illustrated in Figure 6.4.

6.3.1 Automated Valet Parking

The aim of the automated valet parking (AVP) use case is to demonstrate how this functionality can benefit from different information sources, other than the onboard sensors, accessed via the principle of the IoT like parking cameras. Through the use of IoT, the IoT platform can monitor and/or

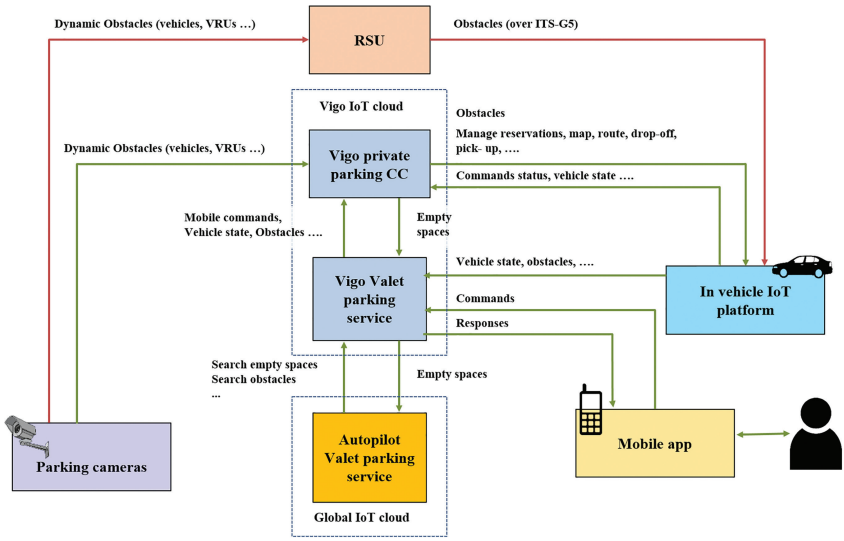

Figure 6.5 Automated valet parking (AVP) execution view, (example from the AUTOPILOT Spanish pilot site) [1, 12].

coordinate traffic on the parking lot and do efficient route planning based on real-time available traffic information. Hence, the IoT platform will exchange information about the dynamic and static obstacles in the parking lot and/or the route to be followed by the vehicle using the information provided by the parking cameras. The AVP use case has two main scenarios:

- Autonomous parking of the vehicle (drop-off scenario), after the driver, has left the vehicle at the drop-off point, that can be located near the entrance of a parking area.
- Autonomous collection of the vehicle (pick-up scenario), when the driver wants to leave the site, he/she will request the vehicle to return itself to the collection point, using, for example, a smartphone application.

In Figure 6.5, which is an execution view from the Spanish pilot site, the IoT devices and the functions that will be supported using the IoT platform are described. The following list is a detailed proposal of devices and functions to support the valet parking use case:

Private parking control centre:

- Informs when a parking spot is free or not.
- Manages reservations.

- Validates vehicle access.
- Manages maps and vehicle routes.

User's mobile device:

- Requests parking slots.
- Manages pick-up and drop-off events.

Smart cameras:

- Publish detected events (e.g. pedestrians or other objects on the parking place).

Connected automated driving (CAD) vehicle:

- Validates that the access to the vehicle is provided to the authorised driver.
- Informs when the vehicle is ready to move unmanned to the destination (parking place or collect point), e.g. when the driver has moved out of the proximity of the vehicle or has locked the doors.
- Manages pick-up and drop-off events and Navigation to the destination, following a route either determined by the IoT platform, while avoiding obstacles detected by either the vehicle sensors or the IoT platform.
- Informs when the vehicle goes into a low power consumption mode.
- Informs when an obstacle is detected.
- Informs about vehicle sensors values and position.

Interior parking areas are very controlled scenarios where the main challenges are the corners without visibility. IoT parking cameras can provide information on these blind spots, allowing the AD function to increase the SAE automation level from 3 to 4 [1, 12].

At the Dutch pilot site, the AVP use case story starts with the vehicle being manually driven to the drop-off point. After arriving there, the user activates the AVP function (e.g. by in-vehicle interface or smartphone app) and exits the vehicle. Services on the IoT platform determine an obstacle-free route to an available parking position based on information from IoT devices. The vehicle autonomously drives to the dedicated parking position. IoT devices involved in the use case are:

- Permanently installed cameras on the parking area that can detect free parking spots and obstacles.
- A micro aerial vehicle (MAV) that can provide information about free parking spots and obstacles, for areas the cameras do not cover.
- IoT-enabled vehicles with their own sensors.

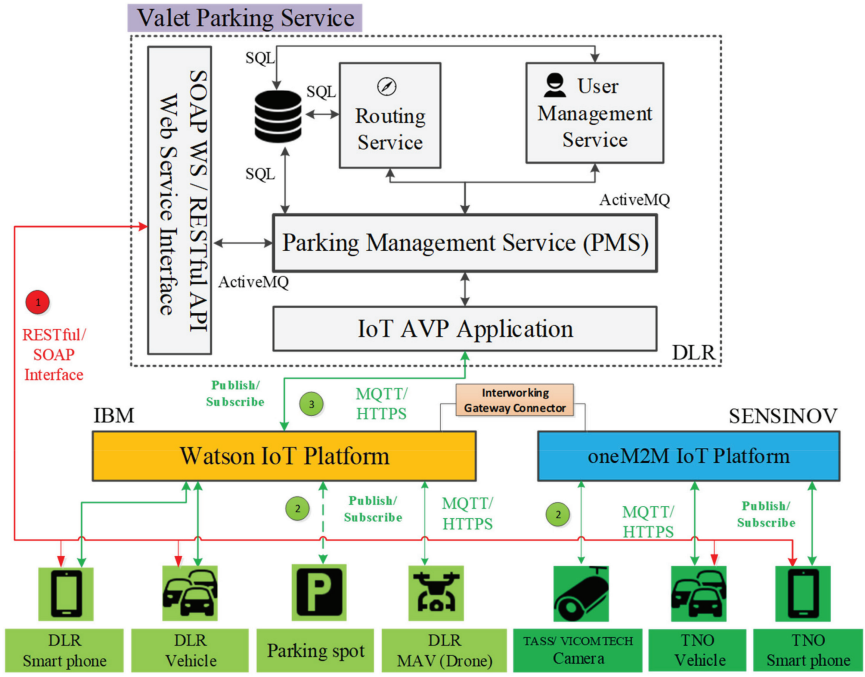

Figure 6.6 Automated valet parking (AVP) use case architecture, (example from the AUTOPILOT Dutch pilot site) [1, 12].

The primary goal of the IoT usage is, therefore, to gain an improved environment model that can possibly increase the efficiency and safety of the use case. Figure 6.6 depicts an overview of the IoT architecture of the AVP use case as deployed in the Dutch pilot site. Two IoT platforms from Watson IBM and oneM2M are used by the AVP, and the interoperability between the two platforms is realised through the bidirectional interworking connector that has been implemented for this purpose.

6.3.2 Highway Pilot Use Case

For the detection component of the Dutch pilot site system, three sensors in the vehicle are relied upon: a LiDAR, a front camera and an inertial measurement unit (IMU). An extra camera supports the use case for lane detection but is not directly involved in hazard detection. The LiDAR data is processed by a specifically developed algorithm, focusing on speed bump detection. The front camera data is processed by a specifically developed algorithm,

focusing on potholes. The IMU data is processed by a specifically developed algorithm, capable of detecting anomalies without specific classification.

For the information component of the system, one actuator relies upon the active cruise control (ACC) unit. Moreover, turning lights are controlled to support lane changes scenario. The way all these are interconnected is illustrated in Figure 6.7.

It is worth noting that the raw data from sensors are indeed passed directly to the runtime environment where the real-time detection algorithms runs. However, everything else is coordinated through an in-vehicle IoT platform (here an MQTT Broker) that ensures the coordination between the results from all other software modules. In addition to the IoT devices within vehicles, the use case also takes advantage of a roadside camera that monitors the road for anomalies too (e.g. static objects like fallen cargo). The detection from this camera is passed through onto the oneM2M IoT platform.

The use case carried out in the Italian pilot site involves vehicles with IoT enhanced automated driving (AD) functions, driving on a "smart" highway. The test vehicles are equipped with an onboard IoT open vehicular platform enabling IoT triggered AD functions, like speed adaptation, lane change, and lane-keeping. Some vehicles also have special sensors, such as an IoT-based pothole detector.

The "smart" highway is a highway where a pervasive IoT ICT system is deployed based on a network of roadside sensors or other sources capable of collecting information and making it available to cloud-based applications. In the use cases, connected vehicles and the traffic control centre (TCC) also have an important role. For safety reasons, the connected vehicles precede and follow the AD vehicle driving in convoy.

The goal is to show how the combined use of IoT and C-ITS can mitigate the risk of accident for an AD vehicle when at a certain point, the road becomes dangerous because of the two kinds of hazardous events: Wet road (puddle) and road works. In the following, the functions of the different IoT devices are described.

6.3.2.1 Hazard on the roadway (puddle)

Puddle IoT sensors:

- In the Italian pilot site, two kinds of such sensors are deployed, using different communication technologies: 6LowPAN and NB-IoT. They continuously monitor the highway in critical locations sending two kinds of signals; a low-frequency heartbeat and a high-frequency alert triggered by the rising of the water level.

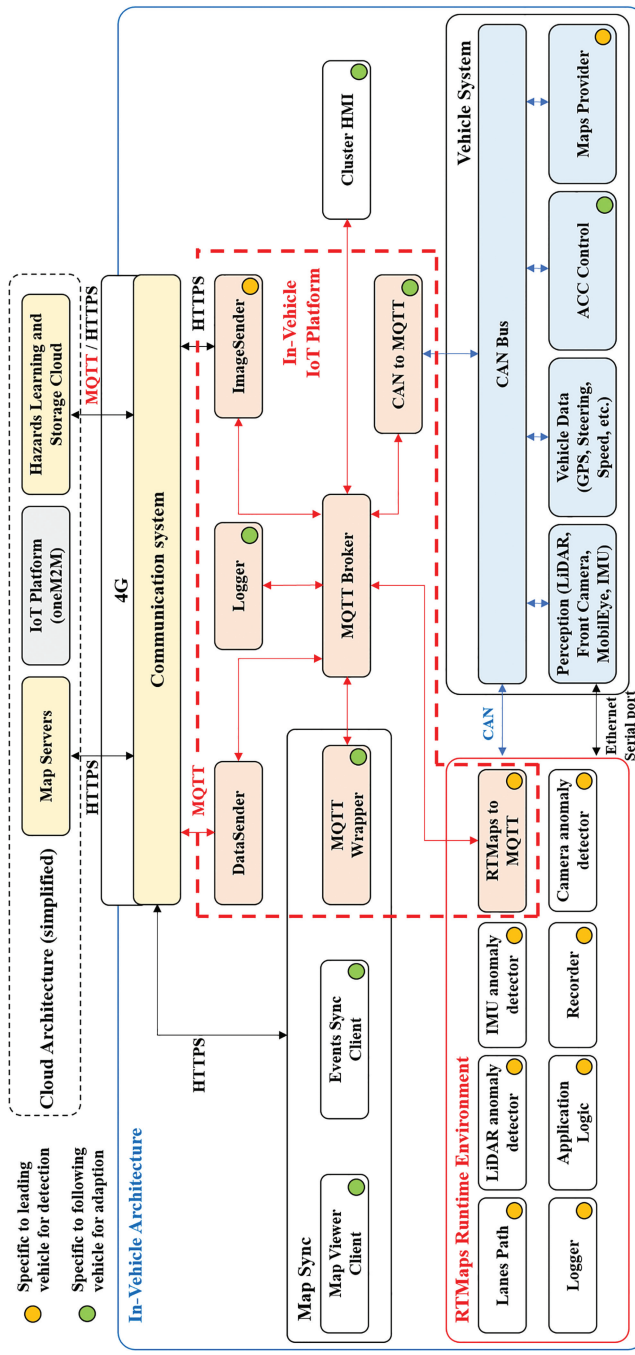

Figure 6.7 SW and HW IoT architecture, (example from the AUTOPILOT Dutch pilot site) [1, 12].

- The 6loWPAN puddle sensors send the messages to the roadside ITS-Station by means of CoAP.
- The NB-IoT puddle sensor sends the message straight to the oneM2M platform using the LTE cellular network and CoAP protocol, as well.

Roadside ITS station:

- Roadside ITS station is a programmable gateway with multi-access technologies (notably 6LowPAN, ETSI ITS G5, LTE, and Ethernet). It is an RSU, compliant with ISO/TC204 WG16 standards, able to exchange information over different networks, using different protocols, including the IoT ones.
- The RSU always listens to the 6loWPAN sensors and sends the measurement to the oneM2M IoT platform of the pilot site with a certain frequency.
- When a hazard occurs, the RSU broadcasts a DENM with the lowest quality level of the information (i.e. not yet validated by the TCC), toward both the approaching vehicles via the ITS-G5 network and the oneM2M platform via LTE cellular network.
- Furthermore, the RSU publishes on the oneM2M platform the CAMs collected from the vehicles in the ITS-G5 communication range.

The traffic control centre (TCC):

- The TCC implements a DATEX II node that is allowed to supply information from the whole highway network. The TCC is also responsible for managing ITS on the oneM2M platform of the Italian pilot site. Two kinds of services are provided leveraging the subscription to the oneM2M platform: hazard validation and DENM forwarding. It also publishes to the oneM2M platform the relevant traffic information from the DATEX II node, to be consumed by the highway infotainment service (FI-PI-LI App).
- When a hazard like flooding on the road occurs, the TCC is notified by the subscription to the oneM2M platform. After assessing the severity of the danger, it validates the hazard and broadcasts a DENM with the highest quality level of the information (i.e. validated by the TCC) to the RSUs along the highway, using the cabled LAN.
- The TCC subscribes to the CAMs of the vehicles published by the RSUs on the oneM2M platform. The information is combined with the Bluetooth and Wi-Fi transit data loggers to perform the travel time analysis and live overview on the TCC video wall.

- The TCC subscribes to the AD vehicle's sensor data on the oneM2M platform in order to provide ITS services to the users of the highway.

The automated driving (AD) vehicle:

- The AD vehicle broadcasts CAMs over the IEEE 802.11 OCB (ETSI ITS-G5) network; at the same time, the AD vehicle publishes data from its sensors to the oneM2M platform.
- The AD vehicle is approaching the hazard on the road; the in-vehicle application (Connected e-Horizon (CeH)) subscribes to the alert from the oneM2M platform.
- The in-vehicle IoT platform combines the information obtained by the CeH with that obtained by DENM via the IEEE 802.11 OCB (ETSI ITS-G5) network and then feeds the appropriate autonomous functions that perform either the necessary adaptation of the driving style in a smooth way, if sufficiently in advance.
- In a case when a vehicle is close to the hazard and for some reason (i.e. the warning from the IoT services was not received, or the warning was received just by the safety channels of ITS-G5 (DSRC), etc.), an emergency braking is needed, and this event is registered by the in-vehicle application and sent to the oneM2M IoT platform of the pilot site.
- At the same time, the cloud monitors the performance of the vehicle, checks that the in-vehicle application feeds the appropriate autonomous functions, and sends a notification to the in-vehicle HMI.

Connected vehicles:

- The connected vehicles lead and follow the AD vehicle; they continuously broadcast CAMs over the ETSI ITS-G5 (IEEE 802.11 OCB) network; at the same time, they publish its sensor's data the oneM2M platform.
- The connected vehicles are approaching the hazard on the road; the in-vehicle IoT platform receives the information from both the RSU along the track and the oneM2M IoT platform.
- The in-vehicle application pre-alerts the driver about the hazard using the information obtained by the oneM2M IoT platform of the pilot site and by the DENM.

An overview of the demonstration storyboard is shown in Figure 6.8: IoT sensors placed along with to the highway monitor continuously the presence of puddles and if a warning condition has been detected, send an alert to the

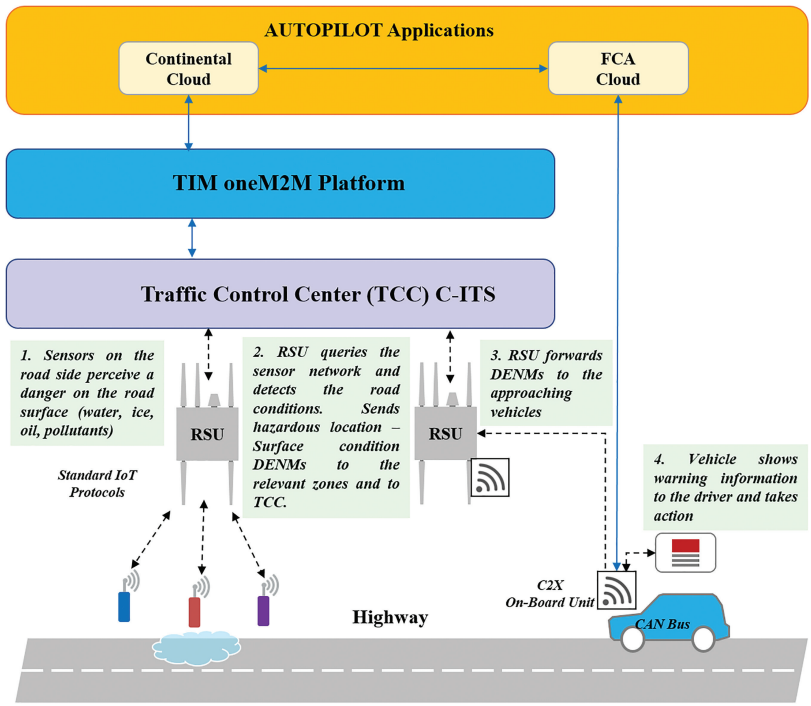

Figure 6.8 Hazard on the roadway (puddle) execution view, (example from the AUTOPILOT Italian pilot site) [1, 12].

RSU that broadcasts this information to vehicles (DENM) and to the TCC. It validates the alert, forwards the DENM message to farther away RSUs and feeds the IoT oneM2M cloud platform with alert related data.

The information on the presence of puddles generates a temporary update of the speed limit in the interested area, which is transmitted from the cloud to the CeH installed inside the prototypes. The in-vehicle application feeds the appropriate autonomous functions that perform a smooth speed adaptation (IoT-enabled speed adaptation for AD vehicle) in combination with information obtained from DENM. In consequence, IoT technology assists the rising of the SAE automation level from 3 to 4 [1, 12].

6.3.2.2 Roadworks warning by traffic control centre (TCC)

A roadworks event is planned by traffic/road operators, and a temporary speed limit is associated with the event. Two IoT-assisted AD manoeuvres are expected:

- The AD vehicle has to reduce its speed approaching the roadworks area, travel at the temporary speed limitation and increase the speed again at the end of the roadwork area.
- The AD vehicle has to stay on the current lane without any human steering action. Moreover, in the presence of a lane closed due to roadworks, it has to perform a lane change and avoid the obstacle.

An overview of the demonstration storyboard is shown in Figure 6.9:

- A sensor node is attached to the road works trailer and announces the presence of roadway works to an RSU.
- Then the RSU triggers DENM messages, broadcasting information about available lanes, speed limits, geometry, alternative routes, etc.
- The TCC broadcasts the DENM messages to farther away RSUs. At the same time, the TCC feeds the oneM2M platform with roadworks related data.

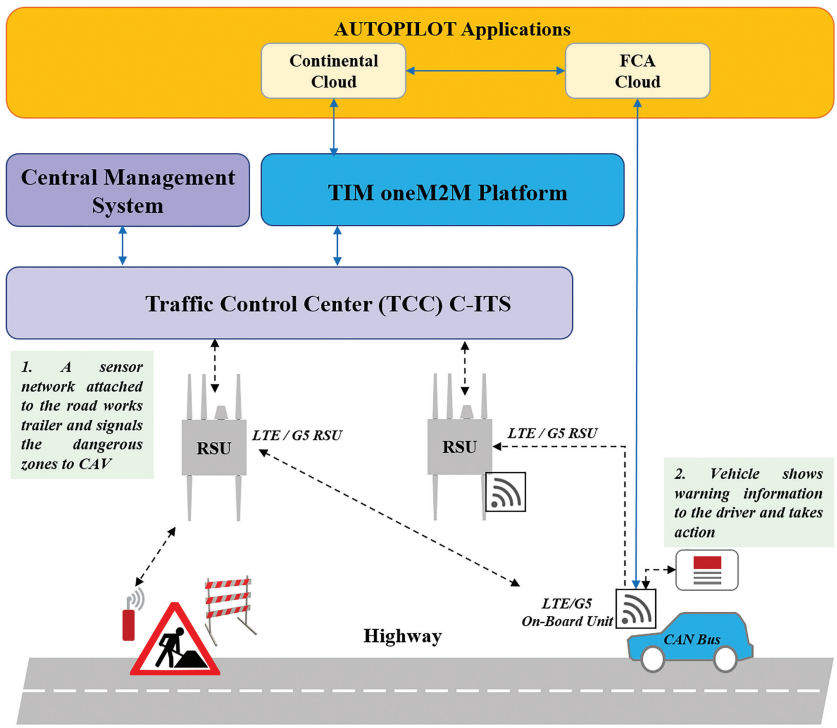

Figure 6.9 Roadworks warning by traffic control centre (TCC) execution view, (example from the AUTOPILOT Italian pilot site) [1, 12].

- Then the information is consumed by the CeH application and transmitted to the cloud as a modified dynamic speed limit that considers the generated dynamic event.
- The cloud immediately notifies to the prototype vehicles the updated information for the onboard CeH device. Thus the in-vehicle application feeds the appropriate autonomous functions that perform the necessary adaptation of the driving style in combination with information obtained from DENM. A notification/warning can be generated through the in-vehicle HMI.

Expected benefits; IoT can provide to the AD vehicle information in advance on the presence of obstacles, roadworks or other vehicles in the rear blind spot. With that information, the in-vehicle application can instantiate both smooth IoT-enabled speed adaptation and lane-change manoeuvres. In such a way, IoT technology assists the rising of the automation level from 3 to 4 [1, 12].

6.3.3 Platooning Use Case

The platooning use case of the French pilot site is part of the vehicle rebalancing business case and is closely linked to the fleet management system that indicates which vehicles have to be transferred from one station to another. The added value of the IoT in the platooning use case is illustrated in the following aspects of mission planning, and traffic light assist:

Mission planning:

- Choose the leading vehicle and its start/end stations according to data collected via IoT objects (e.g. the position of the operator, the charging level of the vehicle, etc.).
- Choose the follower vehicles, the start/end station and their order in the platoon according to data collected via IoT sensors in each vehicle and in the parking spots.

Traffic light assist:

- Suggest a reference speed to the operator in order to minimise the waiting time (red light) at each intersection that counts with a traffic light along the entire itinerary. (The traffic assist architecture for platooning is already illustrated in Figure 6.2 as an example from the French pilot site and the V2I domain).

The main scope in the Dutch pilot site is to show how increased flexibility in platoon navigation and manoeuvring capabilities can be realised, and how

it can benefit from the use of IoT technology. For instance, platoon forming is done under the control of a platoon manager service that calculates the estimated time of arrival and rendezvous point of platoon vehicles based on the actual positions and speeds of those vehicles.. An additional function of the service is to guide the platoon after successful formation. Guidance involves speed and lane advice to the lead vehicle, based on the traffic situation on the road ahead. For example, the platoon service receives regulatory information from the road operator (max speed and lane access/or closure) and takes data from the IoT platform (oneM2M) concerning vehicle traffic conditions and traffic light status data. In order to minimise the probability of platoon break-up, the platoon service provides specific speed advice. After (an unlikely) break-up of the platoon, the service will support reformation of the platoon. The platooning use case utilises various communication channels (V2V and V2I). V2V concerns operational driving of the Cooperative Adaptive Cruise Control (CACC) while the bidirectional V2I channels are mainly used for exchange of data related to tactical driving (such as lane or speed choice). Relevant IoT data are the road operator originated info, the actual traffic state data (from road-side surveillance cameras), platoon state data and traffic light data. Logging takes place on the vehicle (vehicle state and control) and on the IoT platform.

The execution view of the systems and processes involved during the platoon formation stage gives some insight into the system architecture implemented for platooning. The intended procedures in Figure 6.10 are:

- Traveller steps into the vehicle and starts the vehicle-sharing application.
- Traveller defines whether he/she wants to be leading or following in platoon.
- Traveller defines the destination.
- Vehicle sharing application already knows about existing platoons and can match.
- Vehicle sharing app gives route to the Watson IoT platform, which sends it to the oneM2M IoT platform.
- Traveller presses the vehicle GUI to put the vehicle in platoon formation mode.
- Platoon service receives a message from the vehicle that it wants to platoon.
- Platoon service application receives a message from the vehicle-sharing app that matches has been made.

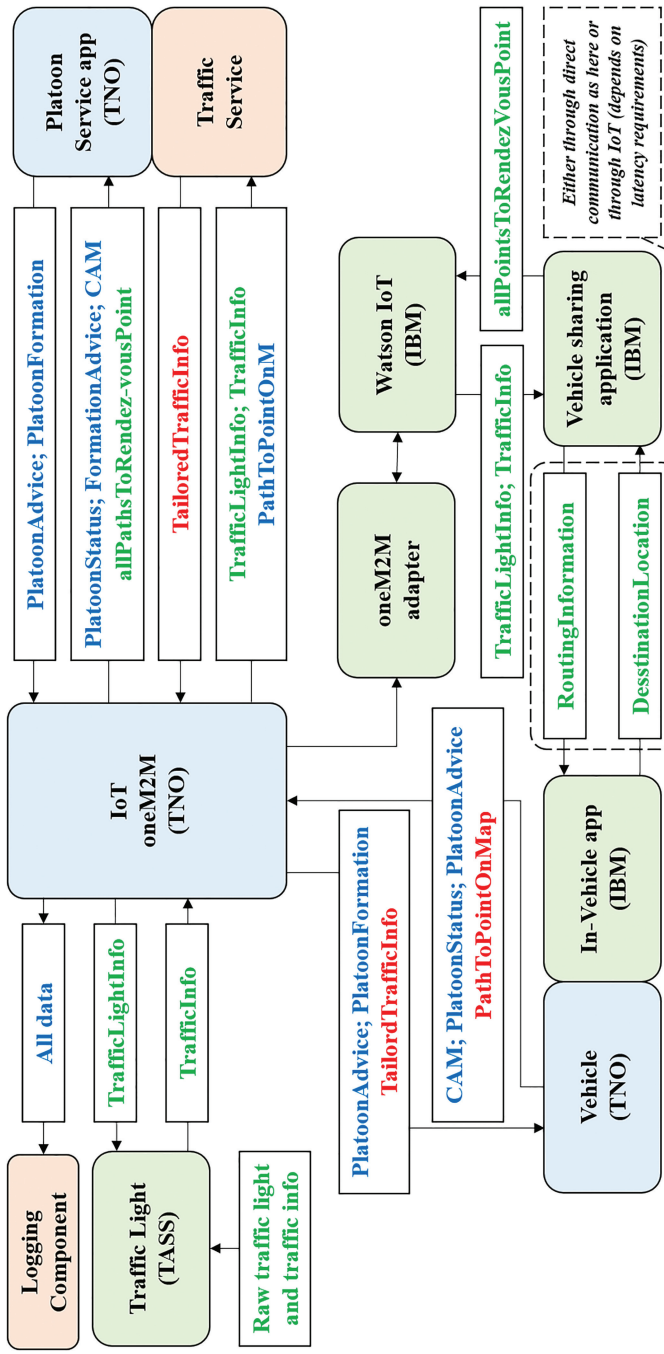

Figure 6.10 Platooning use case execution view of platoon formation (example from the Dutch pilot site) [1, 12].

- Platoon service application gives route(s) to the planner; fill platoon formation message with info from the planner and send to vehicles.
- Vehicle receives a platoon formation message containing platoon ID and planner information.

The platoon service listens to the cloud-based Traffic Manager application, which delivers regulatory road information. The traffic operator can update the traffic management info such as speed limits, lane status, etc., using the GUI and publishes this information to a respective container in oneM2M. The operator can also publish road map information (usually static) wherever there is any change to the otherwise static map. The platooning vehicles subscribed to these containers in oneM2M get these updates and adapt their driving accordingly.

6.3.4 Urban Driving Use Case

Urban driving assisted by IoT has the main objective to support connected, and automated driving (CAD) functions through the extension of the CeH of an automated vehicle. The vehicle can process data from external sources that enrich those provided by its own sensors (Camera, LiDAR, RADAR, etc.). In Figure 6.11, which is an execution view from the Spanish pilot site, the IoT devices and the functions that will be supported using the IoT platform are

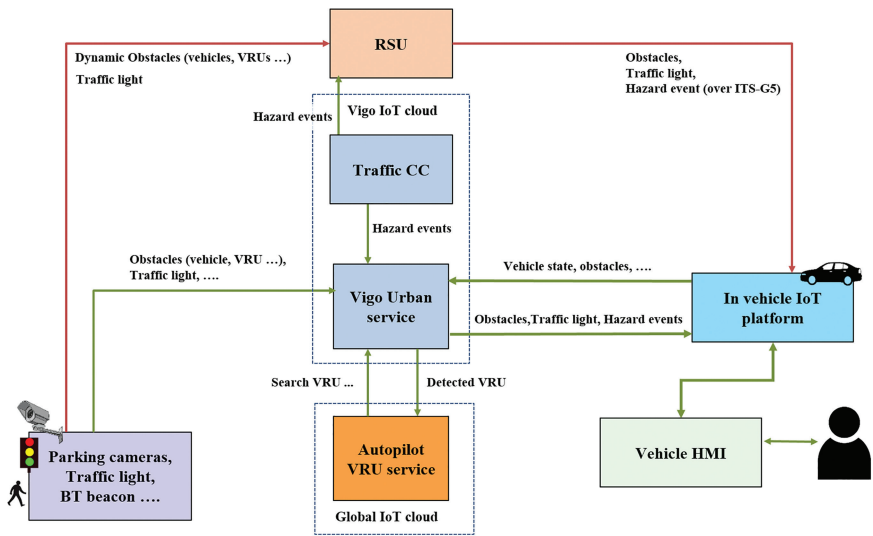

Figure 6.11 Urban driving execution view, (example from AUTOPILOT Spanish pilot site) [1, 12].

described. The following list is a detailed proposal of devices and functions to support the urban driving use case:

- Traffic control centre: Informs when there is a hazard on the road (e.g. accident, traffic jam, road work warning).
- Traffic light: Informs about the traffic light status and time to change.
- Smart cameras: Publish detected events (e.g. pedestrians or other objects on the intersection).
- Connected AD vehicle: Informs when an obstacle is detected, and about vehicle sensors values and position.

Considering all the information provided by IoT devices, the CAD systems will adapt their behaviour accordingly. The complexity of urban scenarios makes it essential to have as much redundancy information as possible. IoT platform provides data about the traffic lights and road events through 3G/4G. Furthermore, the frequency with which the IoT platform sends the data is higher than other advanced V2X communication. For the case of VRUs, the information received by IoT complements the data from the AD sensors, so it provides more reliable and accurate results. There are other objects that could not be detected if there were no IoT services (IoT camera or sensor information from other vehicles). As a result, IoT technology allows for increasing the SAE automation level from 3 to 4 [1, 12].

The urban driving use cases concern IoT-assisted speed adaptation in the common urban scenario, considering traffic light, presence of bicycles, pedestrians and other vehicles. An Italian pilot site overview of the execution is shown in Figure 6.12, including pedestrian detection with a camera, connected bicycles, and potholes detection:

Pedestrian detection with a camera:

- An AD vehicle is approaching an intersection regulated by a "smart" traffic light.
- A smart camera detects a pedestrian or an obstacle on the lane. The information is processed locally and notified to the RSU via IoT protocols. The stereo-camera used for the implementation can even provide information about the position of the VRU or obstacle with a good confidence degree. Moreover, a connected traffic light sends to the RSU via SPaT/MAP messages information about the time to green/red.
- The RSU receives the information transmitted by both devices (smart camera and traffic light), fuses the data and sends it by DENM messages to all the interested actors on the roads.

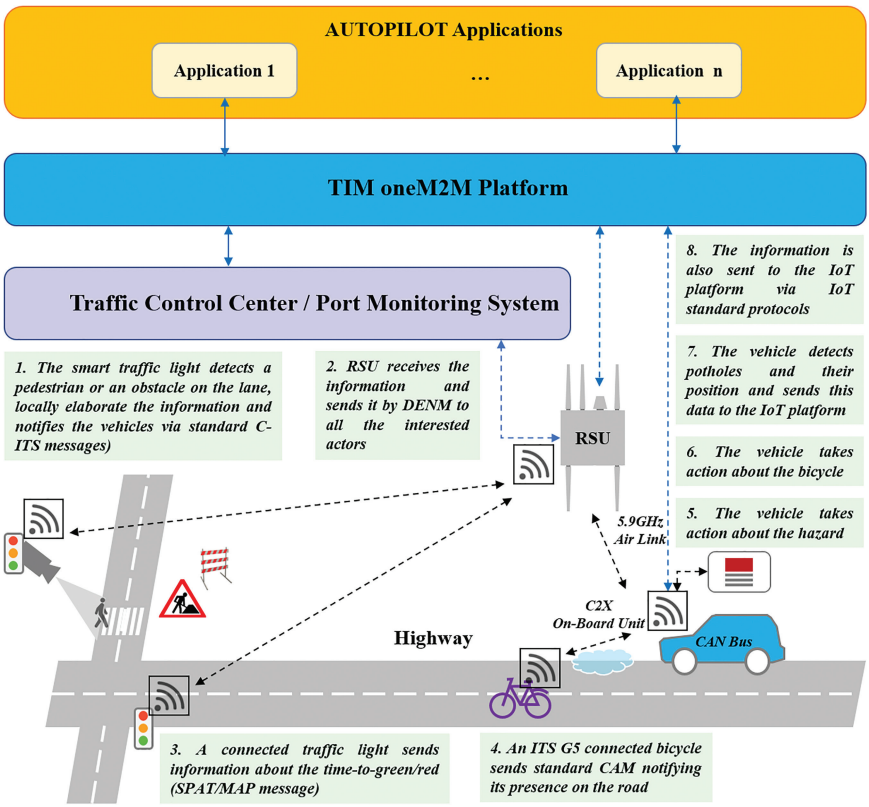

Figure 6.12 Urban driving execution view, (examples from AUTOPILOT Italian pilot site) [1, 12].

- The OBU of the AD vehicle receives the information and smoothly adapts the speed to the situation. The detection of VRUs and the traffic light status is also displayed on the HMI of the vehicle.
- The information is also sent to the oneM2M platform and can be retrieved by other vehicles in the same area via cloud applications.
- At the same time, the area monitoring centre consumes the information from the oneM2M platform and displays a new advisory speed limit for the interested area to avoid possible problems.

Connected bicycle:

- An AD vehicle is moving in an urban scenario with other road users, including a connected bicycle.

- The connected bicycle is equipped with battery-powered communication modules and dropout sensors: currently, it sends CAM messages to other vehicles and to the infrastructure.
- At a certain point, the bicyclist falls while the AD vehicle is approaching and a DENM is triggered.
- The AD vehicle, informed by IoT of the dangerous situation, smoothly decreases its speed and stops before reaching the accident area.
- The information is also sent to the oneM2M platform and can be retrieved by other vehicles in the same area via cloud applications.
- At the same time, the area monitoring centre consumes the information from the oneM2M platform and displays a new advisory speed limit for the interested area to avoid possible problems.

Potholes detection:

- A wireless vibrations sensor installed on the vehicle collect the data of the raw signal accelerations on the three axes and notifies to the OBU, via 6LowPAN or MQTT protocol, the occurrence of a vibrational shock above a certain level (threshold), due to a pothole presence on the road.
- The OBU combines this information with other data coming from the CAN bus (speed, odometer, etc.) and GPS and sends this data to the oneM2M IoT platform, by using MQTT and/or HTTP as application protocols.
- An upcoming AD vehicle consumes the information and can arrange its speed accordingly.

In such complex scenario, the IoT inputs to AD functions are many: IoT information about the traffic light phase and remaining time can be used from AD vehicles to adapt their speed in order to cross the intersection with green traffic light; and if not possible, to safety stop at the traffic light or queue behind other vehicles. Moreover, a smart camera on the test site can provide information on pedestrian traffic light violation. AD vehicles can use this information to stop at the traffic light even if the traffic light on its side is green. IoT enabled speed adaptation for AD vehicle is also related to the bicycle presence and if a fallen bicycle is detected, and to the road conditions. What is more, in this scenario, the IoT technology enhances the rising of the automation level from 3 to 4 [1, 12].

6.3.5 Car/Vehicle Sharing Use Case

A car/vehicle sharing service is intended as a service to enable different customers to make use of a fleet of vehicles (either self-driving or not) which

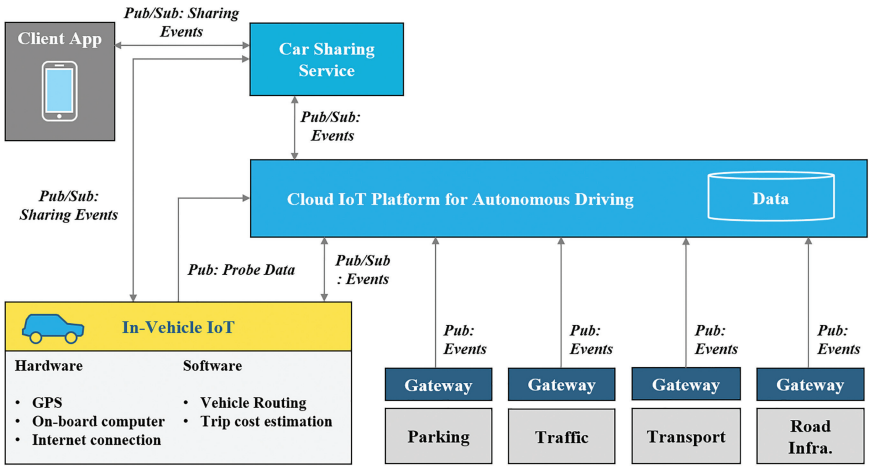

Figure 6.13 Vehicle sharing use case architecture (example from the Dutch pilot site) [1, 12].

is shared amongst them. Vehicle sharing can be interpreted as a service that finds the closest available vehicle and assigns it to a single customer or drives the closest available vehicle to the requesting customer. Vehicle sharing can also be intended as ridesharing when multiple customers that possibly have different origins and destinations share a part of the ride on a common vehicle (either self-driving or by driving it themselves). Finally, vehicle-sharing services can also be thought of as services that allow customers to specify pick-up and drop-off time-windows to increase flexibility and planning.

Figure 6.13 shows the target architecture for the vehicle-sharing use case at the Dutch pilot site. The focus here is on the interaction between the various vehicle-sharing actors and components and the open IoT platform common services, represented as one box.

The users should book vehicles and manage (modify, cancel, etc.) their bookings using the central vehicle-sharing service through a mobile or desktop application, referred to as the client app. The proposed architecture requires that shared vehicles should be equipped with the necessary hardware and software to:

- Communicate their probe data (GPS location, speed, etc.) to the open IoT platform common services and the vehicle-sharing service.
- Compute optimum routes and their costs (distance, energy consumption, etc.) given an assigned destination. These may be fully implemented inside the vehicle itself or may be delegated to external web services.

IoT enabled devices and vehicles of the IoT ecosystem should publish relevant events (traffic, accidents, weather, parking spot availability, etc.) on the open IoT platform. In order for the vehicle-sharing service and shared vehicles to be notified about events that may affect their planned trips, they should subscribe to the open IoT platform for relevant events. The open IoT platform should be responsible for collecting data from the various IoT devices, storing them and communicating the relevant pieces of data (events) to subscribers.

6.4 IoT Devices and Platforms Integration

IoT devices for autonomous driving applications are deployed through IoT platforms that offer integrated services where the IoT devices interact and exchange information. The integration of IoT devices into IoT end-to-end platforms provides the hardware, software, connectivity, security and device management tools to handle the different IoT devices used in the different use cases across the AUTOPILOT project's pilot sites. Different sections provide information on how some of the integration is implemented presenting the managed integrations, device management, cloud connection, cellular modem, etc., to manage and monitor the IoT devices in different use cases. Table 6.2 gives an overview of the communication infrastructure in the AUTOPILOT project [1, 13]. Fields denoted "+" means that the communication technology is implemented in the respective use case in one or more of the pilot sites.

6.4.1 French Pilot Site in Versailles

The oneM2M standard defines two mechanisms to integrate oneM2M and non-oneM2M IoT devices into the IoT platform:

- Integration of oneM2M devices: The IoT devices are called application dedicated nodes (ADN) and can interact with the oneM2M platform directly via the Mca, one of the oneM2M standard interfaces. The IoT devices send requests and receive notification using the oneM2M RESTful API.
- Integration of non-oneM2M devices: The oneM2M standard is highly extensible and allows the integration of non-oneM2M devices and applications, regardless of their vendor or provider. A dedicated software component called Interworking Proxy Entity (IPE) shall be developed and deployed for this purpose. The IPE provides interworking between the oneM2M platform and specific IoT device technologies or protocols.

Table 6.2 Communication technologies in the AUTOPILOT project [1, 13]

Use Cases vs. Technologies	Urban Driving	Automated Valet Parking	Highway Pilot	Platooning	Car/ Vehicle Sharing
Long Range Wireless Communication Networks:					
3GPP 4G (LTE)	+	+	+	+	+
3GPP 4.5G (LTE advanced)	+	−	−	+	+
IoT Wireless Communication Technologies:					
IEEE 802.15.4	+	−	+	−	−
IEEE 802.11	+	+	−	+	+
IETF 6LoWPAN/LP-WAN	+	−	+	+	+
LoRaWAN	+	−	−	+	+
Bluetooth/BLE	+	+	−	+	+
RFID	+	−	−	+	+
3GPP NB-IoT	−	−	+	−	−
Intelligent Transport Systems wireless technologies:					
ETSI ITS G5	+	+	+	+	+
IEEE 802.11-OCB	+	+	+	+	+
LTE Cellular-V2X-Release14	+	−	+	−	−
IP Communication:					
IP-V4 TCP/UDP	+	+	+	+	+
IP-V6 TCP/UDP	+	−	−	+	−
IoT Protocols:					
DDS	+	+	−	−	−
MQTT	+	+	+	+	+
oneM2M standard	+	+	+	+	+
Facilities, Transport and Application Protocols:					
ETSI CAM	+	+	+	+	+
ETSI DENM	+	+	+	+	+
ETSI SPaT	+	+	−	−	−
ETSI MAP	+	−	−	−	−
CEN/TS 16157 DATEX II	−	−	+	−	−
DIASER NF P 99-071-1 G3	−	−	−	+	−

Figure 6.14 illustrates the main components and interactions of the AUTOPILOT's French pilot site. The connectivity within the vehicle is handled by the vehicle connectivity module (VCM) developed.

Vehicle remote control data is not exposed to the IoT platform. It is pushed to the OEM platform (via the VEDECOM Broker) using a separate interface available on the vehicle. In addition, a separate communication

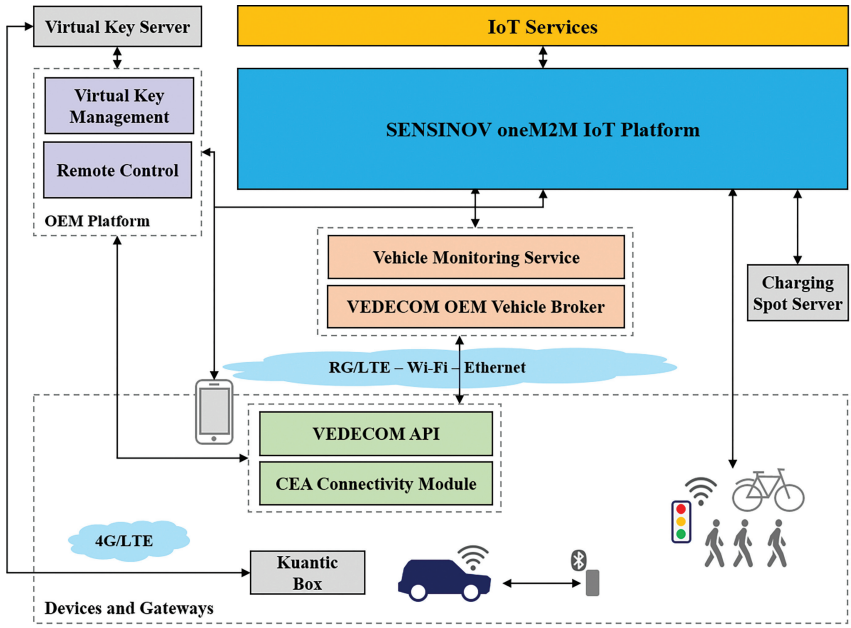

Figure 6.14 AUTOPILOT's French pilot site IoT platform integration [1].

channel for virtual key management is established between the Kuantic server, deployed on the cloud, and the Kuantic box, deployed on the vehicle.

Vehicle monitoring data is exposed to the OEM vehicle Broker using the API service available on the vehicle. Data is pushed to the IoT platform via an IPE to make it available for high-level IoT services using a generic data model and Mca the oneM2M Mca interface.

Other IoT devices, including traffic lights, bicycles, charging spots, passengers' devices are considered as oneM2M-enabled devices and will interact with the IoT Platform using Mca interface.

6.4.2 Dutch Pilot Site in Brainport

There are several use cases implemented and rolled out on the AUTOPILOT's Dutch pilot site. The case implementations are being developed by various project partners using different IoT platforms and technologies:

- oneM2M interoperability integration platform provided by Sensinov.
- FIWARE IoT Broker [17].
- Watson IoT platform.
- Huawei IoT platform.

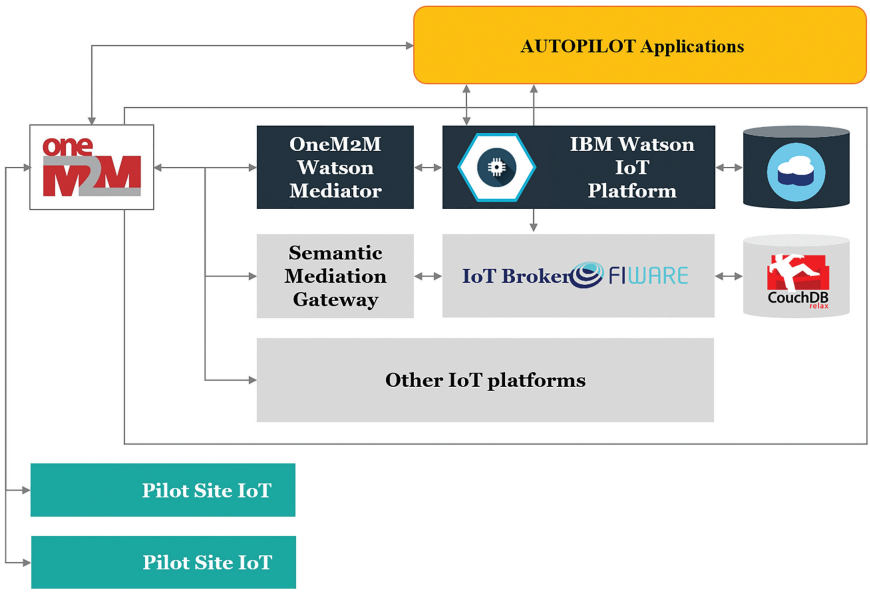

Figure 6.15 AUTOPILOT's Dutch pilot site IoT platform integration [1, 12].

Since the platforms generally perform similar tasks and provide comparable interfaces (e.g. device management, discovery, message brokers, etc.), it has been a challenging task to make all components work together. Moreover, the pilot site devices can connect to one of the platforms, i.e. the platforms are able to discover the devices and communicate with them. The goal was to make the platforms and devices interoperable, and Figure 6.15 illustrates the integration between the platforms and devices in the AUTOPILOT's Dutch pilot site:

- AUTOPILOT applications that implement the use cases.
- An oneM2M platform that all devices connect to by default to "hide" the complexity of the communications between the platforms and applications.
- A set of IoT platforms that should either be able to communicate with the oneM2M platform or implement support to the oneM2M communication protocols by itself.
- The IoT devices connected to the oneM2M platform of the pilot site.

In this scenario, there are two platforms involved in the communications from the bottom up to the top; from the device to the oneM2M interoperability platform, then to the target IoT platform and finally, an application that deals

with the device, and vice versa. Another scenario is that the devices connect directly to the target IoT platform (e.g. Watson IoT platform) to reduce the burden of the interoperability between the platforms. This may be useful if one knows that messages from the device will be consumed only by one IoT platform. In this case, there is no need to build a hierarchy of the platforms and pass the messages emitted by the device through the full stack. The drawback of this approach is that the interoperability platform does not know all the connected devices. To address this problem, an announcement process may be introduced. When a device is connecting to an IoT platform, this platform makes an announcement to the interoperability platform to convey that a new device is connected to a given IoT platform, and if somebody wants to consume data from the device via the interoperability platform, it must lookup for the device and message at this IoT platform.

The various platforms and applications are interfaced, as depicted in Figure 6.16. FIWARE focuses on a common data model and powerful interfaces for searching and finding information in IoT. FIWARE is using the OMA Next Generation Service Interface (NGSI) data model as the common information model of IoT-based systems and the protocol for communication. NGSI-9 and NGSI-10 are HTTP-based protocols that support JSON and XML formats for data. Let us shortly describe these two interfaces.

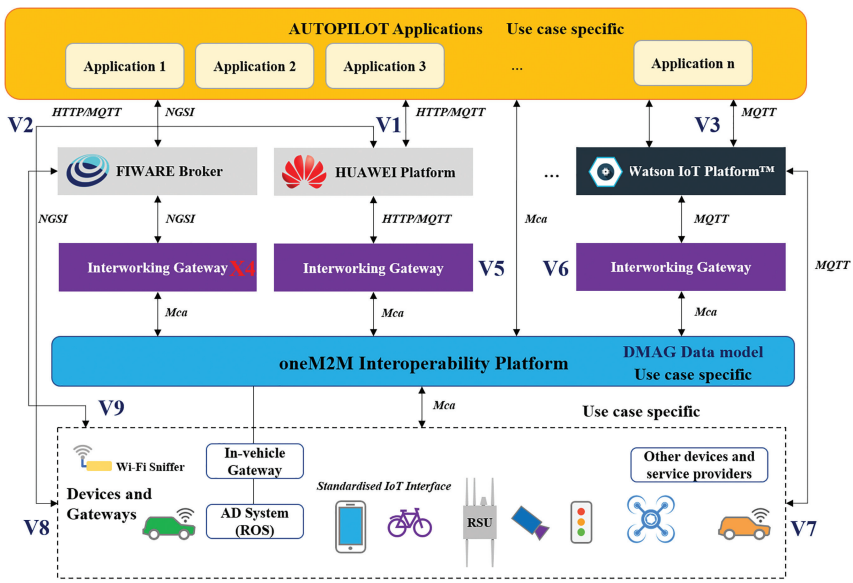

Figure 6.16 The platform interfaces in AUTOPILOT's Dutch pilot site [1, 12].

- NGSI-9 is used to manage the availability of context entity. A system component can register the availability of context information, and later on, the other system component can issue either discover or subscribe messages to find out the registered new context information. Detailed specifications can be found in the FIWARE NGSI-9 Open RESTful API Specification [9].
- NGSI-10: is used to enable the context data transfer between data producers and data consumers. NGSI10 has a query, update, subscribe and notify context operations for providing context values. A context broker is necessary for establishing data flow between different resources as well as consumers or providers. Detailed specifications can be found in the FIWARE NGSI-10 Open RESTful API Specification [10].

The micro aerial vehicle (MAV) and its ground station computer act as one single IoT device in the AVP use case. The communication between the MAV and the ground station is based on a local IEEE 802.11n Wi-Fi connection that guarantees high-data bandwidth and continuous local availability. Small Open Mesh OM2P routers are used on both sides. The ground station computer connects to the Watson IoT platform via 4G/5G. The Huawei OceanConnect IoT platform is an open ecosystem built on IoT, cloud computing and Big Data technologies. It provides over 170 open APIs and serial agents that enable application integration, simplifies and accelerate device access, guarantees network connection and realises the seamless connection between upstream and downstream products for Huawei partners. The used communication protocols are MQTT and HTTP. Applications requiring access to the Huawei OceanConnect IoT Platform need to be authenticated first. Once an application is successfully authenticated, it may perform the following actions:

- Collect device data from the IoT connection management platform using either an active query or data subscription.
- Issue commands to a specified sensor through the IoT connection management platform.
- Issue rules to the IoT connection management platform, allowing response events and commands to be triggered based on the rules.
- Subscribe to device information (events) from the platform.

6.4.3 Italian Pilot Site in Livorno-Florence

At the AUTOPILOT's Italian pilot site, the IoT devices are integrated into the IoT oneM2M platform according to the oneM2M standard, as illustrated in Figure 6.17:

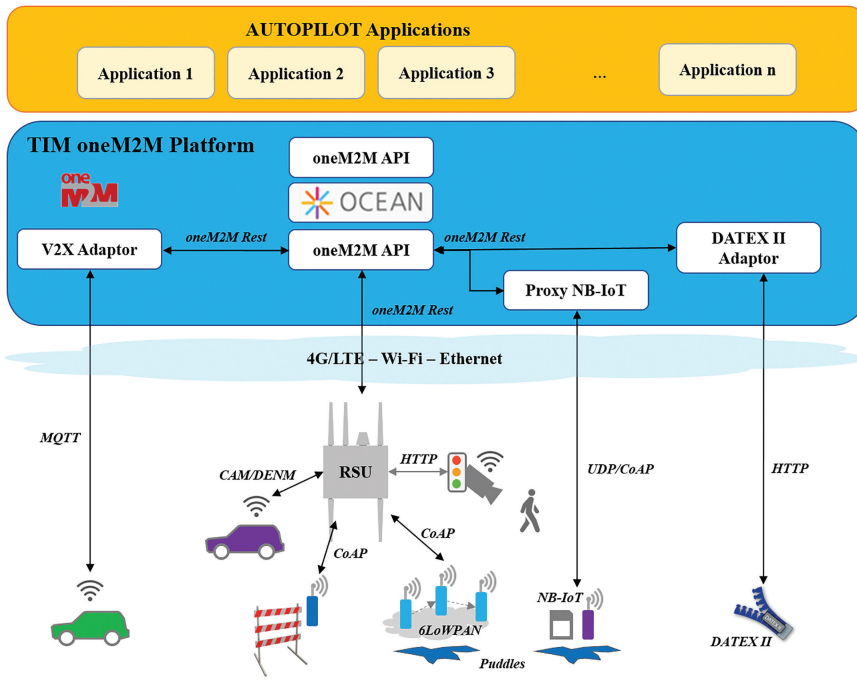

Figure 6.17 AUTOPILOT's Italian pilot site IoT device integration [1, 12].

- IoT oneM2M platform: A federated model where several heterogeneous IoT platforms are interconnected. A central IoT platform includes various modules: big data management and storage, real-time and batch analytics, security and privacy, semantics, etc. Interoperability between the central IoT platform and the pilot site IoT platforms is addressed in this platform.
- In-vehicle IoT platform: An in-vehicle component that provides communication with the cloud IoT platform and the interfaces to other in-vehicle components.

The in-vehicle software architecture for the IoT platform integration is illustrated in Figure 6.18. In this scheme, it is possible to represent the IoT in-vehicle platform and also the interconnections between this container with other onboard sensors in the host vehicle and the cloud system and/or other vehicles and RSUs.

The IoT in-vehicle platform is composed by a quad-core ARM processor. The platform runs an optimised version of Linux and provides

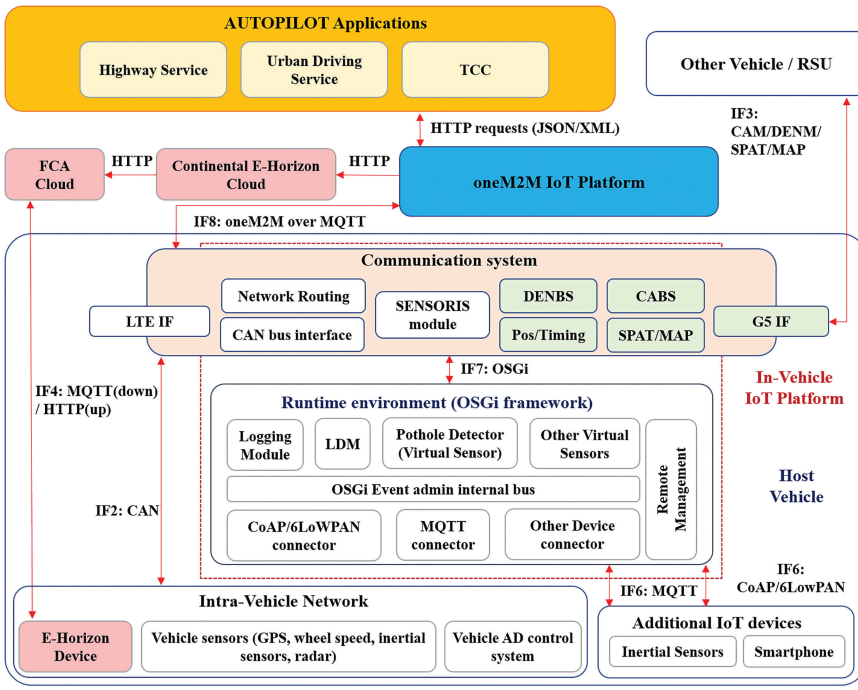

Figure 6.18 AUTOPILOT's Italian pilot site software architecture for OBU IoT platform integration [1, 12].

several interfaces like IEEE ETSI ITS-G5, Wi-Fi, Bluetooth, Ethernet, CAN, 6LoWPAN, and LTE. The board implements CAM, DENM and SPaT/MAP standards with the possibility to send messages both over ETSI G5 and LTE channels. The board will manage the lane level computation of the surrounding vehicles' position. Finally, it mounts a GNSS (Galileo + GPS) receiver that is used for positioning and synchronisation. The unit can synchronise other hosts (within 10 ms) using the NTP standard or other protocols. The IoT in-vehicle platform is modular software including application container and communication system, which are deployed on the OBU. The runtime environment part of the OBU is composed of several software modules.

The functionality of the remote management is implemented by software, which allows configuring the platform by adding/removing bundles, introducing the idea of remote monitoring and control of external application based on an OSGi platform. Through the event admin internal bus, the connectors have the same communication interface to the bundles, which they interfaced in the

application container. The application container also encases the functionality of data management, with the modules of local dynamic maps (LDM) and the pothole detector. LDM is a database that achieves integrated management of map and vehicle information (functional requirement of context awareness). It contains information on real-world and conceptual objects that have an influence on the traffic flow. The bundle of the pothole detector represents the implementation of the pothole detection algorithm. It is based on data fusion techniques in order to implement the concept of "virtual sensors". This module collects data from multiple sensors on the vehicle (IoT in-vehicle components or OEM in-vehicle components), processes the various data and sends the results of this elaboration to the cloud oneM2M platform, RSUs or other vehicles via the communication system.

Regarding the IoT device adaptation, the target is to support different IoT communication protocols with the devices. The IoT connectors showed in Figure 6.18 are used to integrate with 6LoWPAN data coming from additional IoT devices (i.e. inertial sensors), which are used by edge applications on the OBU (CoAP/6LoWPAN connector). They are also used to integrate with MQTT protocol data coming from additional IoT devices (e.g. smartphone), which are used by edge applications on the OBU (MQTT connector).

The communication system part of the OBU manages different high-level capabilities. The module CAN bus interface reads data coming from the CAN bus and decodes important data coming from the in-vehicle sensors that are sent directly to the oneM2M platform or used by edge applications on the OBU. The module Pos-Timing reads the positioning data and timing information through the GPS hardware module to set the position on CAM and DENM messages. CABS and DENBS modules take data from the CAN bus, position and time from Pos-Timing and create a CAM/DEN message as described in the proper ETSI standard [8]. They also receive CAM/DEN messages coming from other vehicles and save them on the LDM. The SPaT/MAP messages in the communication system are generated from a traffic light, and SPaT/MAP module decodes them, saving the relevant information in the LDM for further use. SPaT/MAP offers a potential channel for detailed information exchange between traffic systems and road users.

The capability of message routing is assigned to network routing, which manages the connectivity of all the in-vehicle modules that need network connectivity. Moreover, it manages the channels where CAM and DENM messages are sent. In the OBU, they can be transmitted on the ETSI G5 radio channel and/or on the cellular way towards the oneM2M platform or for debugging.

As far as the interoperability part is concerned, it should be considered that the in-vehicle IoT platform should work with heterogeneous devices, technologies, applications, without additional effort from the application or service developer. OEM-specific components relate to components such as actuators for power steering and brakes, inputs to gearbox or vehicle sensors needed for the normal vehicle functions (MAP, MAF, ABS, etc.). Software modules implementing drivers to virtualise such OEM-specific components into vehicle IoT platform are needed, so as to satisfy the OEM systems communication functionality. The OBU can also exchange data with additional IoT devices such as inertial sensors or the motion sensors of, for example, the smartphone. These data are interfaced with the IoT in-vehicle platform using CoAP/6LoWPAN or MQTT protocols as already described, and better implement the concept of "virtual sensors" added to pothole detection.

In order to have a complete vision of Italian pilot site architecture, external components should also be mentioned. The AUTOPILOT applications interface the IoT platform and implement the AUTOPILOT functions in the cloud. Each application communicates with the vehicle via the IoT platform. An application can also comprise a component that runs in the vehicle platform. These components can be either an IoT application or an in-vehicle application, depending on the level of integration with the IoT platform. The IoT platform implements the IoT functions at the cloud or edge level. It also comprises other vehicles and roadside elements.

For example, in the use case of urban driving, a smart traffic light detects a pedestrian or an obstacle on the lane. The information is processed locally and notified to the RSU using the IoT protocols to the vehicles via standard C-ITS messages. Moreover, a connected traffic light sends information about the time to green/red (SPaT/MAP messages). The RSU receives the information, fuses the data and sends it by DENM to all the interested actors on the roads. The information from RSUs and OBUs is also sent to the IoT data platform via IoT standard protocols, and it can then be processed by the area monitoring centre for real-time risk assessment and safety services.

Figure 6.19 illustrates the RSU software architecture for IoT platform integration. The peculiarity given by the modularity and configurability of the designed software, it is possible to customise it depending on the context in which it is inserted (i.e. OBU or RSU IoT platform). In this case, the runtime environment contains a bundle related to pedestrian detection. The module Jaywalking Detector represents the implementation of the algorithm that notifies this event when a pedestrian crosses the strip while the traffic light is red. In these conditions, the IoT platform of RSU is interfaced with a

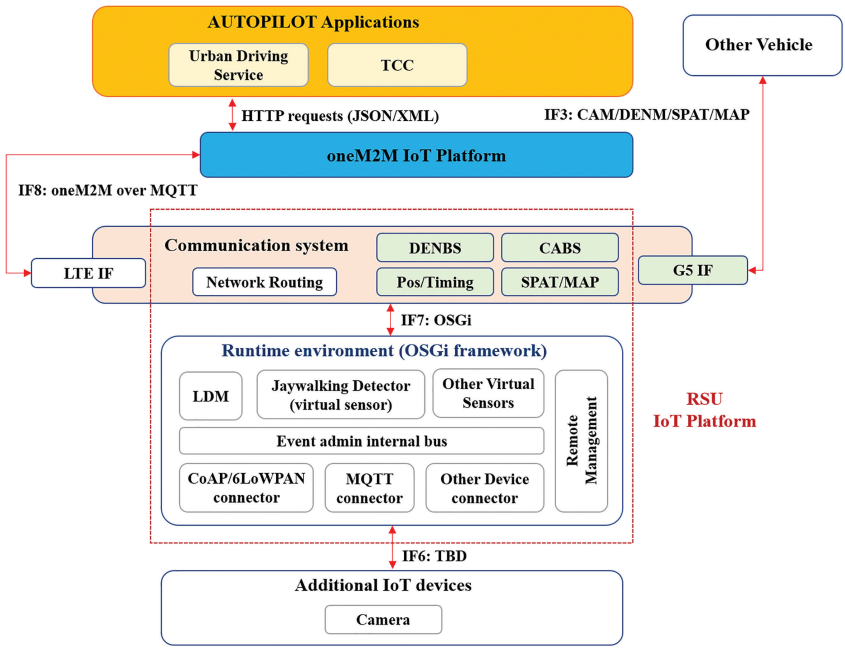

Figure 6.19 AUTOPILOT's Italian pilot site software architecture for RSU IoT platform integration [1, 12].

camera that may register the wrong crossing of pedestrians and send data to the IoT platform. In this bundle, the data are elaborated and the notification of "detected jaywalking pedestrian" is sent to oneM2M IoT platform exploiting HTTP request (JSON, XML) via oneM2M protocol, or to other vehicles using the CAM/DENM/SPaT/MAP interfaces.

6.4.4 Spanish Pilot Site in Vigo

AUTOPILOT's Spanish pilot site is composed of three main IoT platforms, as illustrated in Figure 6.20:

- IoT platform: A federated model where several heterogeneous IoT platforms are interconnected. A central IoT platform includes various modules like big data management and storage real-time and batch analytics, security and privacy, semantics, etc. Interoperability between the central IoT platform and the pilot site IoT platforms is addressed in this platform.
- In-vehicle IoT platform: An in-vehicle component that provides communication with the cloud IoT platform and the interfaces to other in-vehicle components.

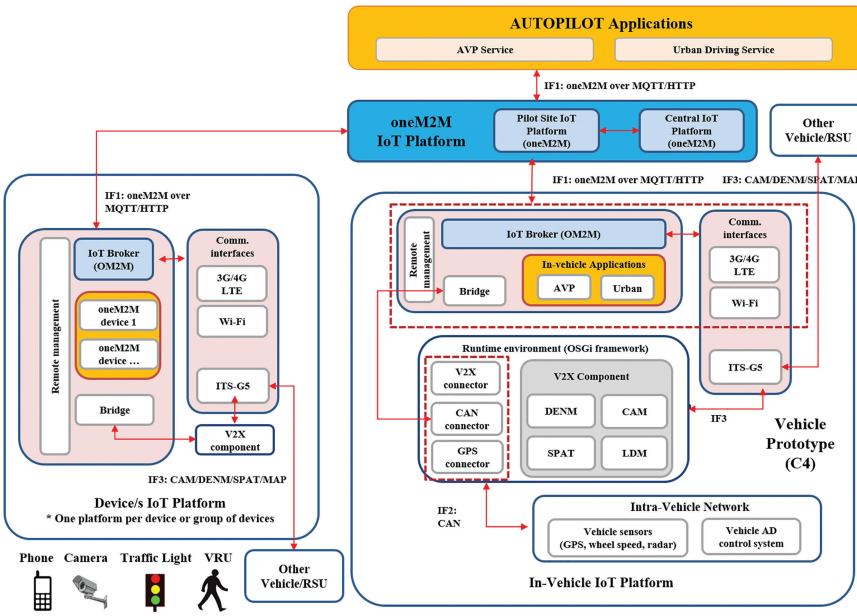

Figure 6.20 AUTOPILOT's Spanish pilot site IoT platform integration [1, 12].

- Devices IoT platform: The devices can be new devices or existing devices adapted to become IoT devices able to be integrated into the IoT ecosystem.

The in-vehicle platform and device platform software components are described in Figure 6.20. The more important software components are:

Communication interfaces: The component responsible for providing connectivity to the device.

- The supported interfaces are cellular (3G/4G LTE), Wi-Fi and ITS-G5 wireless interface.

IoT Module: This module translates the information that comes from the different devices into oneM2M messages and translates oneM2M message into understandable information for the vehicle.

- IoT Broker: OM2M based ASN-CSE (oneM2M) that acts as an IoT gateway. It provides the HTTP and MQTT connectivity to the cloud IoT platform.
- Bridge: Responsible for translating all the information from the vehicle into oneM2M and for publishing and providing any needed methods to obtain this data.

- IoT Applications: Responsible for the interaction with the physical devices in order to provide the full functionality expected in the use cases.

Runtime environment: OSGi framework that contains the stack that enables the V2X communication.

- V2X Component: Contains several modules that are able to process data coming from V2X communication through ITS-G5. The component provides the encoding/decoding for the SPaT/MAP, CAM and DENM messages. Includes the connectors that give access to the IoT module.

6.4.5 Finnish Pilot Site in Tampere

Figure 6.21 illustrates the communication architecture of the AUTOPILOT's Finnish pilot site, including the two use cases; automated valet parking and urban driving. For both use cases, the same infrastructure is used; the prototype vehicles and a traffic camera installed on the mobile RSU. The data of the traffic camera are processed locally, and information on objects is transmitted to the IoT platform. Both the vehicle and the mobile RSU internal network are

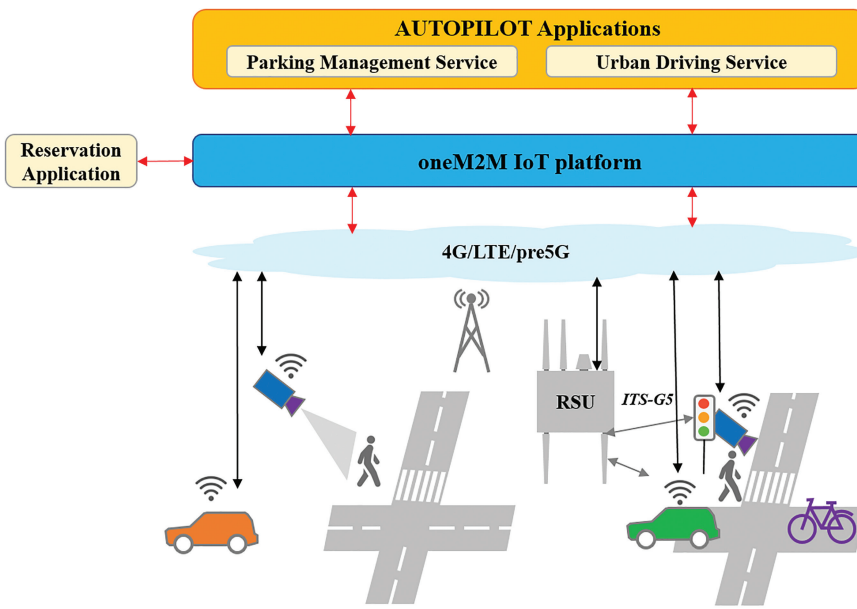

Figure 6.21 AUTOPILOT's Finnish pilot site communication architecture overview.

based on the data distribution service (DDS) network. Information exchanged between the vehicles, RSU and the services, like the parking management service, is based on MQTT and is being sent to an open oneM2M IoT platform. Communication between vehicle, mobile RSU and the IoT platform uses available mobile commercial network (4G/LTE) or a Pre-5G innovation platform, which is installed in the city of Tampere. Vehicles receive signal phase information from traffic lights also from the traffic light operator's server over MQTT. Services for parking management and for management of the urban driving use case are developed and integrated with the IoT platform.

Figure 6.22 illustrates the IoT platform architecture integration of the Finnish pilot site and is composed as follows:

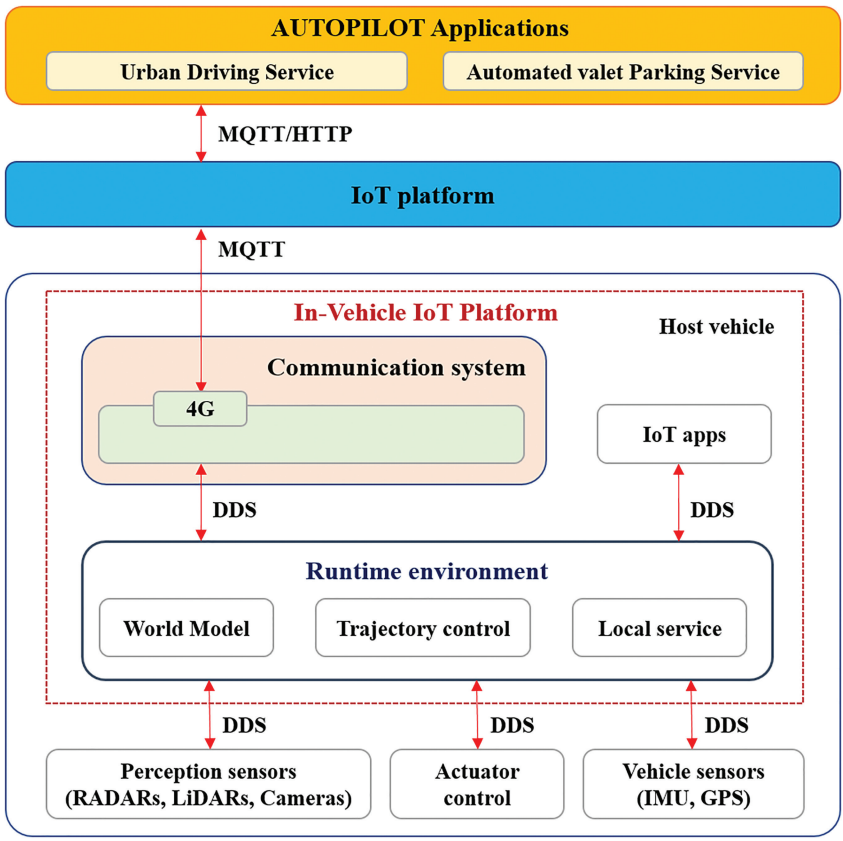

Figure 6.22 AUTOPILOT's Finnish pilot site IoT platform integration [1, 12].

- An open IoT platform for connecting the different devices based on oneM2M. The main purpose of the IoT platform is to act as a broker.
- The in-vehicle IoT platform provides communication with the IoT platform, and with the different devices and applications in the vehicle. Data is exchanged between the different applications using data distribution service (DDS).
- The mobile roadside unit has a similar architecture as the vehicle unit. The mobile roadside unit processes the information from the traffic camera and makes this information available through the IoT platform to the vehicle and the parking management system. The system also has a storage process for assuring that all data needed for evaluation are made available.
- In addition, there is a connection to the traffic light server. Information on the traffic signal phases is available in real-time over the cellular network as MQTT messages.

6.5 Conclusion

The IoT technologies used in different AUTOPILOT use cases have demonstrated that it is possible to support automated/autonomous driving functions as defined by SAE levels and IoT technologies and platforms embedded in vehicles and infrastructure, enhancing the automated/autonomous driving functions. There are five different IoT platforms used for collecting, exchanging and processing the data from the IoT devices in the different use cases in the different pilot sites presented:

- FIWARE IoT Broker.
- IBM Watson IoT platform.
- HUAWEI OceanConnect IoT platform.
- Telecom Italia (TIM) oneM2M IoT platform.
- Sensinov oneM2M platform.

The integration of IoT technologies and platforms is adapted to the infrastructure of the pilot sites. The use cases map the AUTOPILOT architecture, and the IoT technologies are integrated into different architecture components and interfaced/connected to the infrastructure of each pilot site. The IoT technologies used were adapted to the autonomous driving function requirements in terms of speed of access (latency), availability and range (covered area).

The vehicles used in the different AUTOPILOT use cases starts at level 2 with internal systems that take care of the different aspects of driving, such

as steering, acceleration and braking. The driver is able to intervene if any part of the vehicle system fails. Examples of level 2 include use cases helping vehicles to stay in lanes and self-parking features, with more than one advanced driver assistance system (ADAS) aspect. Tesla's Autopilot and Nissan's ProPilot are examples of level 2, as the vehicles can automatically keep you in the right lane on the road and keep you at a safe distance from the vehicle in front when in a traffic jam.

The results from the AUTOPILOT projects show that the IoT devices and technologies can support the autonomous driving functions in use cases such as urban driving/vehicles rebalancing, highway driving and automated valet parking.

Acknowledgements

The work presented in this chapter has been supported by the European Commission within the European Union's Horizon 2020 research and innovation programme funding, project AUTOPILOT [1] under Grant Agreement No. 731993. Special thanks to all involved project partners, whose names do not appear on the author list, but who also contribute significantly to the development and testing of the automated driving applications presented in this chapter at various pilot sites.

References

[1] The AUTOPILOT project – Automated driving progressed by Internet of Things, online at: https://autopilot-project.eu/

[2] X. Wu et al., "Cars Talk to Phones: A DSRC Based Vehicle-Pedestrian Safety System," 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), Vancouver, BC, 2014, pp. 1–7.

[3] Bosch Motorcycle-to-vehicle communication, online at: https://www.youtube.com/watch?v=BXXlodI9gO0

[4] M. Bagheri, M. Siekkinen and J. K. Nurminen, "Cellular-based vehicle to pedestrian (V2P) adaptive communication for collision avoidance," 2014 International Conference on Connected Vehicles and Expo (ICCVE), Vienna, 2014, pp. 450–456.

[5] J. J. Anaya, P. Merdrignac, O. Shagdar, F. Nashashibi and J. E. Naranjo, "Vehicle to pedestrian communications for protection of vulnerable

road users," 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, MI, 2014, pp. 1037–1042.

[6] The Ko-TAG project, online at: https://www.iis.fraunhofer.de/en/ff/lv/lok/proj/kotag.html

[7] M.S. Greco. Automotive Radar. IEEE Radar Conference, Atlanta, May 2012.

[8] O. Vermesan and J. Bacquet (Eds.). Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution, ISBN: 978-87-93609-10-5, River Publishers, Gistrup, 2017.

[9] "FI-WARE NGSI-9 Open RESTful API Specification", FIWARE Forge, 2017, online at: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-9_Open_RESTful_API_Specification

[10] "FI-WARE NGSI-10 Open RESTful API Specification", FIWARE Forge, 2017, online at: https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_NGSI-10_Open_RESTful_API_Specification

[11] Handbook to the IoT Large-Scale pilots Programme, online at: https://wiki.european-iot-pilots.eu/index.php?title=HANDBOOK_TO_THE_IOT_LARGE-SCALE_PILOTS_PROGRAMME

[12] The AUTOPILOT project – Automated driving progressed by Internet of Things. Report on development and integration of IoT devices into IoT ecosystem. D2.4, July 2018.

[13] The AUTOPILOT project – Automated driving progressed by Internet of Things. Final specification of communication system for IoT enhanced AD. D1.8, June 2019, online at: https://autopilot-project.eu/deliverables/

[14] Alliance for Internet of Things Innovation (AIOTI), IoT Relation and Impact on 5G, (Rel. 2.0). AIOTI WG03 – IoT Standardisation. February 2019.

[15] Intelligent Connectivity, GSMA Report, 2018, online at: https://www.gsma.com/IC/wp-content/uploads/2018/09/21494-MWC-Americas-report.pdf

[16] The AUTOPILOT project – Automated driving progressed by Internet of Things. Final specification of Security and Privacy for IoT-enhanced AD. D1.10, June 2019.

[17] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng and E. Kovacs, "A Standard-Based Open Source IoT Platform: FIWARE," in IEEE Internet of Things Magazine, vol. 2, no. 3, pp. 12–18, September 2019.