C-MobILE

Accelerating C-ITS Mobility Innovation and deployment in Europe

D3.3 Low-level implementation ready architecture

Status	Final
Main authors	Deniz Kadiogullari (htw saar) Manuel Fünfrocken (htw saar) Jacint Castells (Applus+ IDIADA) Priyanka Karkhanis (TU/e) Saurab Rajkarnikar (TU/e) Yanja Dajsuren (TU/e) Robbin Blokpoel (DYNNIQ) Danny Vroeman (TCN) Jacco van de Sluis (TNO) Patrick Hoffman (MAPTM) Geert Vanstraelen (MACQ) Areti Kotis (CERTH)
Work Package	WP3 – Architecture and system design
Task	T3.3 – Service design and T3.4 – Architecture for implementation
Dissemination level	Public
Issue date	29/06/2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723311

Project coordination

Mr. Marcos Pillado Quintas

Applus+ IDIADA

PO Box 20 Santa Oliva

43710, L'Albornar, Tarragona

Spain

Telephone: +34 977 18 93 60

E-mail: marcos.pillado@idiada.com

Revision and history sheet

Version	Date	Authors	Summary of changes	Status
0.1	15/04/2018	Deniz Kadiogullari	Creation of ToC	Prepared
0.11	16/04/2018	Manuel Fünfrocken	Updated of ToC	Prepared
0.11	17/04/2018	Areti Kotsi	Contriubutes ARC-IT diagrams	Contribution
0.2	26/04/2018	Deniz Kadiogullari	Added description for access protocols	Contribution
0.21	30/04/2018	Deniz Kadiogullari	Added description for SVW	Contribution
0.22	30/04/2018	Deniz Kadiogullari	Added description for FI	Contribution
0.23	30/04/2018	Deniz Kadiogullari	Added description for MAI	Contribution
0.24	03/05/2018	Jacco van de Sluis	Added description for EBL	Contribution
0.25	04/05/2018	Saurab Rajkarnikar	Added description for GLOSA	Contribution
0.26	04/05/2018	Saurab Rajkarnikar	Added description for SSVW	Contribution
0.27	04/05/2018	Saurab Rajkarnikar	Added description for RWW	Contribution
0.28	07/05/2018	Danny Vroeman	Added description for CTP	Contribution
0.29	07/05/2018	Danny Vroeman	Added description for TLP	Contribution
0.30	08/05/2018	Deniz Kadiogullari	Revised CTP	Revise
0.31	09/05/2018	Robbin Blokpoel	Added description for RHW	Contribution
0.32	11/05/2018	Meena Krishnamurthi	Added description for MPA	Contribution
0.33	11/05/2018	Deniz Kadiogullari	Added description for RTM	Contribution
0.33	11/05/2018	Danny Vroeman	Revised RTM	Revise
0.33	14/05/2018	Jacint Castells	Revised SVW, RWW	Revise
0.34	14/05/2018	Geert Vanstraelen	Added description for WSP	Contribution
0.35	14/05/2018	Robbin Blokpoel	Added description for GP	Contribution
0.36	14/05/2018	Robbin Blokpoel	Added description for MPA	Contribution
0.37	14/05/2018	Deniz Kadiogullari	Addede description for C-MobILE Services	Contribution
0.38	14/05/2018	Deniz Kadiogullari	Added description for MTTA	Contribution
0.39	14/05/2018	Jacco van de Sluis	Added description for CACC	Contribution
0.39	14/05/2018	Jacint Castells	Review document	Review
0.39	14/05/2018	Manos Nestoras	Review document	Review
0.39	14/05/2018	Pauline Baudens	Review document	Review
0.39	14/05/2018	Geert Vanstraelen	Review document	Review
0.39	14/05/2018	Charlotte Fléchon	Review document	Review
0.39	15/05/2018	Deniz Kadiogullari	Revised RTM	Revise
0.40	15/05/2018	Jacint Castells	Added description for UPA	Contribution
0.41	15/05/2018	Jacint Castells	Added description for IVS	Contribution
0.42	15/05/2018	Jacint Castells	Added description for EVW	Contribution
0.43	15/05/2018	Danny Vroeman	Added description for BSD	Contribution
0.44	16/05/2018	Jacint Castells	Added description for PVD	Contribution

0.44	19/05/2018	Jacint Castells	Revised BSD	Revise
0.44	21/05/2018	Areti Kotsi	Review document	Review
0.44	22/05/2018	Meena Krishnamurthi	Review document	Review
0.45	24/05/2018	Meena Krishnamurthi	Added description for Network & Transport protocols	Contribution
0.46	24/05/2018	Meena Krishnamurthi	Added description for Management	Contribution
0.46	24/05/2018	Geert Vanstraelen	Revised BSD	Revise
0.46	25/05/2018	Patrick Hofman	Review document	Review
0.46	26/05/2018	Deniz Kadiogullari	Revised WSP	Revise
0.47	26/05/2018	Patrick Hofman	Added description for Interoperability	Contribution
0.50	28/05/2018	Manuel Fünfrocken	Review document	Review
0.80	31/05/2018	Saurab Rajkarnikar Yanja Dajsuren	Added description for Interoperability	Contribution
0.81	20/06/2018	Yanja Dajsuren	Review document	Review
0.82	20/06/2018	Geert Vanstraelen	Review document	Review
0.83	20/06/2018	Manuel Fünfrocken	Review document	Review
0.84	21/06/2018	Deniz Kadiogullari Manuel Fünfrocken Yanja Dajsuren	Added Conclusion	Contribution
0.9	22/06/2018	Deniz Kadiogullari	Finalize document	Revise
1.0	22/06/2018	Manuel Fünfrocken	Corrections	Revise
1.1	28/06/2018	Marcos Pillado Quintas	Corrections	Revise
1.2	28/06/2018	Manuel Fünfrocken	Final revise. Finished for publication.	Published

Table of Contents

Figures

Tables

Abbreviations

Abbreviation	Definition
3G	3rd generation of mobile telecommunications technology
4G	4th generation of mobile telecommunications technology
AAA	Authorization and Accounting
ASS	Application Specific Support
ADAS	Advanced Driver Assisted Systems
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
Archimate©	An open and independent modelling language for enterprise Architecture
ASN.1	Abstract Syntax Notation No.1
AU	Application Unit (in IRS or IVS)
B2X/X2B	Business-to-X,X=Business (B), Consumer (C) or Government (G)
BCN	Barcelona
BDD	Block Definition Diagram
BLE	Bluetooth Low Energy
BO	Back-Office
BSA	Basic Set of Applications
BTP	Basic Transport Protocol
C2C	Car-to-Car respectively vehicle-to-vehicle Communication; information exchange between vehicles using ETSI G5; the term is now replaced by „V2V“
C2I	Car-to-Infrastructure respectively vehicle-to-infrastructure Communication; information exchange between vehicles and infrastructure using ETSI G5; the term is now replaced by „V2I“
C2X/Car2X	Car-2-X Communication (generic term: X is either infrastructure or car); including communication between vehicles as well as between vehicles and infrastructure; the term is now replaced by „V2x“
CA	Certification Authority
CACC	Cooperative Adaptive Cruise Control
C-AD	Connected-Automated Driving
CAM	Co-operative Awareness Message
CAN bus	Controller Area Network bus
CBA	Cost Benefit Analysis
CBF	Contention Based Forwarding (Geo Broadcast)
CCU	Communication and Control Unit (in IRS or IVS)
CEN	Comité Européen de Normalisation; English: European Committee for Standardization
CIS	Central ITS Subsystem
C-ITS	Cooperative Intelligent Transport Systems
CMD	Cooperative Mobility Device
C-MobILE	Accelerating C-ITS Mobility Innovation and depLoyment in Europe
CONVERGE	Communication Network Vehicle Road Global Extension
CP	Communication Provider
DAB	Digital audio broadcasting
DATEXII	Second generation of a standard for the exchange of traffic related data which can be used by all actors in the traffic sector (www.datex2.eu).
DCC	Distributed Congestion Control
DENM	Decentralized Environmental Notification Message
DIS	Data Interchange Server
DITCM	Dutch ITS Test site for Cooperative Mobility
DoA	Description of action
DP	Data Provider
DS	Deployment Site
DSL	Deployment Site Leader
EA	Enterprise Architect [software]
EC	European Commission
EM	Exploitation Manager
EOBD	European On-Board Diagnostics
ETSI	European Telecommunications Standards Institute

ETSI G5	G5 (Wi-Fi) communication standard for vehicular communication, standardized by ETSI in standard ETSI ES 202 663
ETSI ITS G5	ETSI term for „IEEE 802.11p"
ETSI ITS-G5A	ITS Frequency band 5,875GHz to 5,905GHz dedicated for safety related applications
EV	Electrical Vehicle
FESTA	FESTA (Field opErational teSt supporT Action) is a shared methodological framework to carry out field operation tests (FOTs) and may serve as a handbook for the deployment of C-ITS service bundles and their impact assessment.
FOT	Field Operational Test. Is a study undertaken to evaluate a function, or functions, under normal operating conditions in environments typically encountered by the host vehicle(s) using quasi-experimental methods.
GA	Grant Agreement or General Assembly
G-ASS	General Application Specific Support
GEOM-C	GeoMessaging Client
GEOM-S	GeoMessaging Server
GLOSA	Green Light Optimal Speed Advisory
GN	GeoNetworking
GPS	Global Positioning System
HMI	Human Machine Interface
IA	Innovation Action
IBD	Internal Block Diagram
ICS	ITS Central Station
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information System
IM	Innovation Manager
INS	Intersection Safety
IP(v4/6)	Internet Protocol, version 4 or 6
IPTS	Intelligent Pedestrians Traffic Signal
IRP	Intermodal Route Planner
IRS	ITS Roadside Station
ISO	International Organization for Standardization
ITS	Intelligent Transport System
ITSC	Intelligent Transport System Communications
ITS-G5	ITS at 5 GHz frequency band
ITS-S	Intelligent Transport System Station
IVERA	Management protocol for traffic light controllers in the Netherlands
IVS	ITS Vehicle Station respectively any Mobile ITS Node (e.g. Smartphone)
KoM	Kick-off meeting
KPI	Key Performance Indicators
LAN	Local Area Network
LDM	Local Dynamic Map
LHW	Local Hazard Warning
LIDAR	Laser Imagining Detection and Ranging
LOS	Level of Service
LTE	Long Term Evolution (4G)
MAC	Media Access Control
MIB	Management Information Base
MNO	Mobile Network Operator
MoM	Minutes of meeting
OBD	On-Board Diagnostics
OBU	On-board Unit
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
PC	Project Coordinator
PHY	Physical layer
PI	Performance Indicators
PID	Personal Information Devices (e.g. smart phone)
PKI	Public Key Infrastructure
PTW	Powered Two Wheelers
PVD	Probe Vehicle Data
pWLAN	Acronym for ITS G5 (IEEE 802.11p)
QoS	Quality of Service
RAS	Roadside Actuation System

RDS - TMC	Radio Data System – Traffic Message Channel
RHW	Road Hazard Warning
RIS	Roadside Intelligent transport Sub-system
RLVW	Red Light Violation Warning
RS	Roadside System
RSS	Roadside Sensor System
RSU	Roadside Unit
RWW	Roadworks Warning
SC	Steering Committee
SCADA	Supervisory control and data acquisition
SD	Service Directory
SDK	Software Development Kit
SDM	Strategic Deployment Manager
SEC	Security
SHB	Single Hop Broadcasting
SP	Service Provider
SPAT	Signal Phase and Timing
SPES	Service Provider Exchange System
SysML	Systems Modelling Language
TC/TCC	Traffic (Control) Centre
TCP	Transmission Control Protocol
TIS	Traffic Information System
TLC	Traffic Light Controller
TMS	Traffic Management System
TMT	Technical Management Team
TOPO	Topology Message
TPC	Transmit power control
TPEG	Transport Protocol Experts Group
TRC	Transmit rate control
TRL	Technical Readiness Level
TS	Technical Specification; usually deployed as „ETSI TS uniqueID“
UC	Use Case
UDP	User Datagram Protocol
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System (3G)
US	User Story
UTC	Coordinated Universal Time
V2I	Vehicle - to - infrastructure
V2V	Vehicle - to - Vehicle
V2X	Vehicle - to - X (generic term: X is either infrastructure or vehicle)
VDP	Visually Disabled Pedestrian
VEE	Vehicle Electrical & Electronic System
VIS	Vehicle Intelligent transport Sub-system
VRU	Vulnerable Road User
VRUITS	improving the safety and mobility of Vulnerable Road Users by ITS applications
WLAN	Wireless LAN
WP	Work Package
WPL	Work Package Leader
WWW	World Wide Web

Executive Summary

In the past years, there has been tremendous progress in the field of intelligent transport systems; several successful cooperative mobility have proven potential benefits of cooperative systems in increasing both energy efficiency and safety for specific transport modes. However, the large variety of cooperative applications have been designed for different goals, stakeholders or specific settings / environments and have been developed on a silo-based approach and deployed independently from each other, serving however, at higher level, similar goals and functionalities for the end-user. Scalability, IT-security, decentralization and operator openness are some of the most important properties that a technical and commercial successful solution must provide.

C-MobILE aims to stimulate / push existing and new deployment sites towards large-scale, real-life C-ITS deployments interoperable across Europe. Well-defined operational procedures will lead to decentralized and dynamic coupling of systems, services and stakeholders across national and organizational borders in an open, but secure C-ITS ecosystem, based on different access technologies, the usage of which is transparent for service providers and seamless and continuous for the end-users across different transport modes, environments and countries.

As part of C-MobILE project, Task 3.4 “Low-level implementation-ready architecture” comprises the following sub-tasks:

- Identify services based on initial CBA and business models from WP2, the reference and concrete
- architectures, existing best practices and experiences gathered in previous projects.
- Define services based on the reference architecture (from Task 3.1) and the systems interfaces and role model defined in the concrete architecture.
- Verify that relevant parts of the architecture are specified in detail for the services operation.
- Harmonize architecture with updated requirements received from WP2 and input from WP5.
- Specify architecture in detail, so that interoperable implementations are possible, e.g. definition of data types, parametrisation of algorithms
- Highlight proprietary interfaces, e.g. for traffic infrastructure, and communicate them to WP6 and Task 4.4.

The final result of these sub-tasks is the current document D3.3 “Low-level implementation architecture”, where the reference architecture refined to medium-level, concrete architecture is described following the C-ITS architecture framework presented in the D3.1 “Reference Architecture”. Given the fact that the concrete architecture is an extension of the reference architecture plus some important input from WP2 and WP5 work, this deliverable presents three specific viewpoints of the architecture that will be further used in the Deployment Sites’ adaptation, implementation and deployment of the C-MobILE systems.

1. Introduction

1.1. Objective

Task 3.3 "Service Design" and T3.4 "Architecture for implementation" aims at detail the concrete-level architecture. The main objective is to define a low-level architecture for all deployed services from which site specific technical architectures can be derived.

The result of Task 3.3 and Task 3.4, D3.3 "Low. -level implementation-ready architecture" will focus on the description of various services at a low-level. This document describes the components and interfaces between the components defined in D3.2 "Mid-level architecture". The goal of the low-level architecture is to provide a detailed implementation architecture for the different services in C-MobILE based on the concrete-level architecture provided in D3.2.

The low-level definitions include the involved components, protocol capabilities, and datatypes.

1.2. Intended audience

This document is intended to provide a low-level understanding of the architecture developed in C-MobILE. It is targeted mainly at technical people related to the definition and implementation of the architecture or parts thereof. Whilst in principal of interest for most of the C-ITS stakeholders this document is specifically targeted to architecture stakeholders such as system/software architects, software designers, software developer, technicians, and technical managers. Furthermore, it is intended to give system designers a good definition of the interaction between systems and devices within C-MobILE.

1.3. Approach

The C-ITS architecture framework has six core viewpoints: Context, Functional, Information, Physical, Communication, and Implementation. These viewpoints are defined based on the existing literature and ITS reference architectures. We believe that this set of viewpoints enable structured architectural descriptions for the C-ITS. In this document the different viewpoints are described using SysML BDD/IBD and other diagrams format to provide a clear and complete description of the system.

1.4. Document structure

This document is organized as follows:

/ **Chapter 2 Overview high-level reference architecture**: this chapter provides information of ITS architecture from past and ongoing project as well as the high-level reference architecture created in D3.1 High-level reference architecture. This content is included in this deliverable to have a valid reference for the new content.

/ **Chapter 3 Current C-ITS deployed infrastructure:** describes the current status of C-ITS deployment in the eight deployment sites. The description includes the existing architectures, giving a high-level description of the existing system and devices. These descriptions also include a brief description of the planned deployments within the C-MobILE project.

/ **Chapter 4 Concrete Architecture:** description of the C-MobILE concrete architecture. The section is divided in parts, which provide different viewpoints.

/ **Chapter 5 Implementation Architecture:** description of the C-MobILE services. This section contains the communication and information viewpoint.

2. Overview high-level reference architecture

2.1. Architectures from previous/ongoing projects

2.1.1. Existing Reference Architectures

Cooperative Intelligent Transportation Systems (C-ITS) are currently under intense development. Several previous projects have already been done regarding C-ITS, which have developed different architectures depending on the needs that the project wanted to cover or the technology that was being used. In C-MobILE, an infrastructure that is able to facilitate large-scale deployment must be developed. This means that the defined infrastructure must support various technologies (e.g., cellular and 802.11p), a wide range of users, while maintaining sustainability and seamless operation within the deployment sites. In order to make this possible, state-of the art solutions will be re-used, creating new solutions only when previous architectures do not meet our needs. In this section of the document, different projects related to C-ITS in Europe are presented. Out of those, the previously defined building blocks, which may be suitable for the C-MobILE project, have been extracted.

2.1.1.1. DITCM

DITCM is a Dutch program that had the aim to accelerate the deployment at large scale of C-ITS and Connected-Automated Driving (C-AD) and carried out from 2014 to 2015. To achieve this smart roads and smart cars need to work together. The challenges are the mix of old and new systems, evolving technology (moving target) and unpredictable human behaviour. DITCM is a cooperation between Connekt and AutomotiveNL.

In 2014, DITCM initiated a project with the objective to develop a reference architecture that can be used as a basis for future ITS deployment projects in The Netherlands [48]. The ITS architecture consists of a system architecture and a description of the business aspects of an eco-system with stakeholders from public and private parties in a Dutch context. The reference architecture was built based on the existing architectures from past and running C-ITS projects in The Netherlands (such as Shockwave Traffic Jams A58, Praktijkproef Amsterdam, ITS Corridor, MOBiNET, and VRUITS. Figure 1 presents a physical view of the DITCM reference architecture. It captures the decomposition of sub-systems and their dependencies in detail and in C-MobILE architecture this would be captured in the physical view of the concrete architecture.

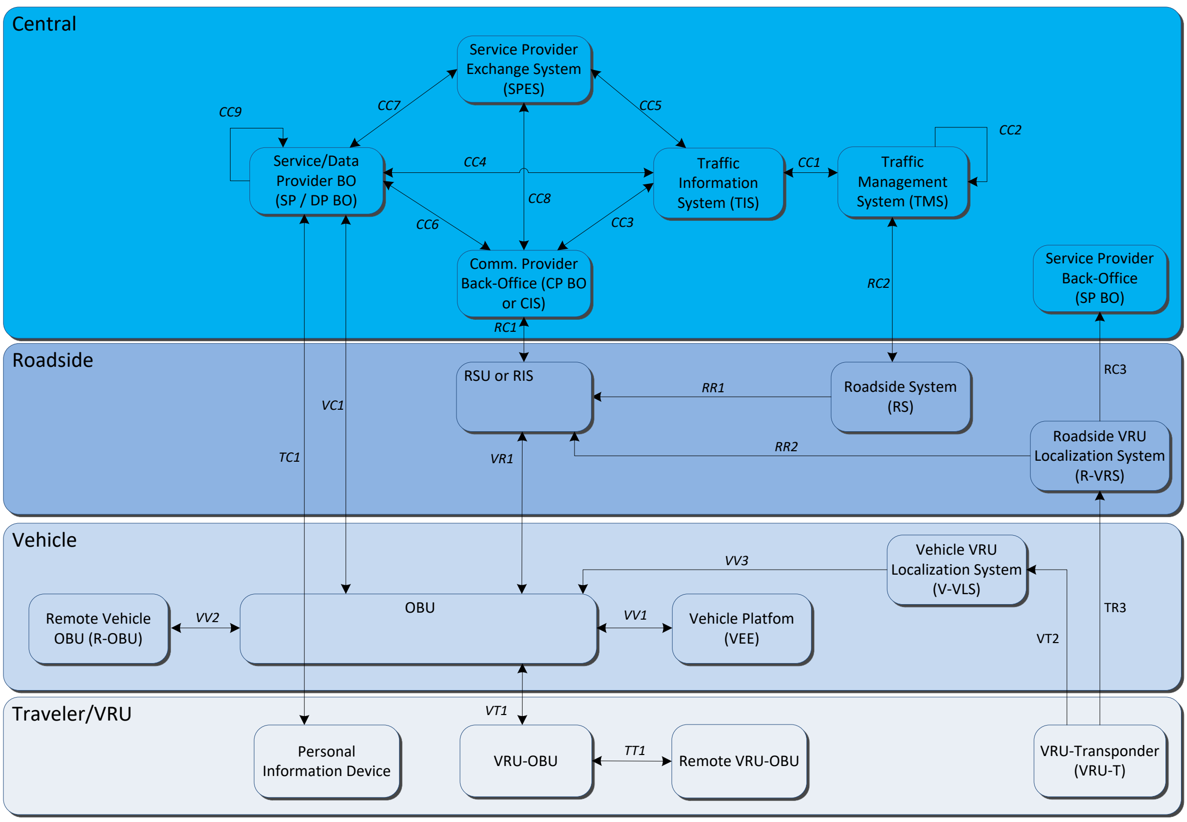


Figure 1: The NL Reference Architecture (physical view with sub-systems, Level 2) [48]

2.1.1.2. CONVERGE

The German research project CONVERGE [34], performed from 2012 to 2015, created an ITS architecture which was heavily focused on interoperability and economic viability. This architecture, called Car2X Systems Network was intended to be scalable, decentral, secure and not dependent on an operator, thus being resilient to change of the partaking organizations.

The CONVERGE architecture was separated in four major structural layers: the governance layer, the backend layer, the communication network layer and the ITS mobile stations.

The **governance layer** contains entities, which are necessary for contracts, regulations, and general supervision of the network. Most of those entities are not pure technical, but represent 'real-world' institutions. During the project, it was identified, that a kind of 'management board', called C2X Initialization Body, is needed, which will define the rules under which the different parties will work together.

The **backend layer** contains all entities, which are normally placed on servers, e.g. in enterprise networks or 'the cloud'. The most prominent entity is the Service Provider, which is an abstract entity implemented by every party providing a service in the system. Most notably, the layer also contains a system to geo-reference user nodes through multiple communication networks, without the need to make the user nodes known to the Service Providers, the so-called GeoMessaging Proxy.

The **communication networks layer** contains several different communication networks, linking backend entities to mobile stations. In CONVERGE, cellular communication and networks of ITS G5 roadside stations have been used, but the architecture is not limited to those.

The **ITS mobile stations layer** contains user related ITS stations, like vehicles or smartphones. The CONVERGE architecture didn't made any assumptions on the internal structure of those stations, but specified some external interfaces, to define how those stations interact with the other entities of the architecture. The architecture is shown Figure 2.

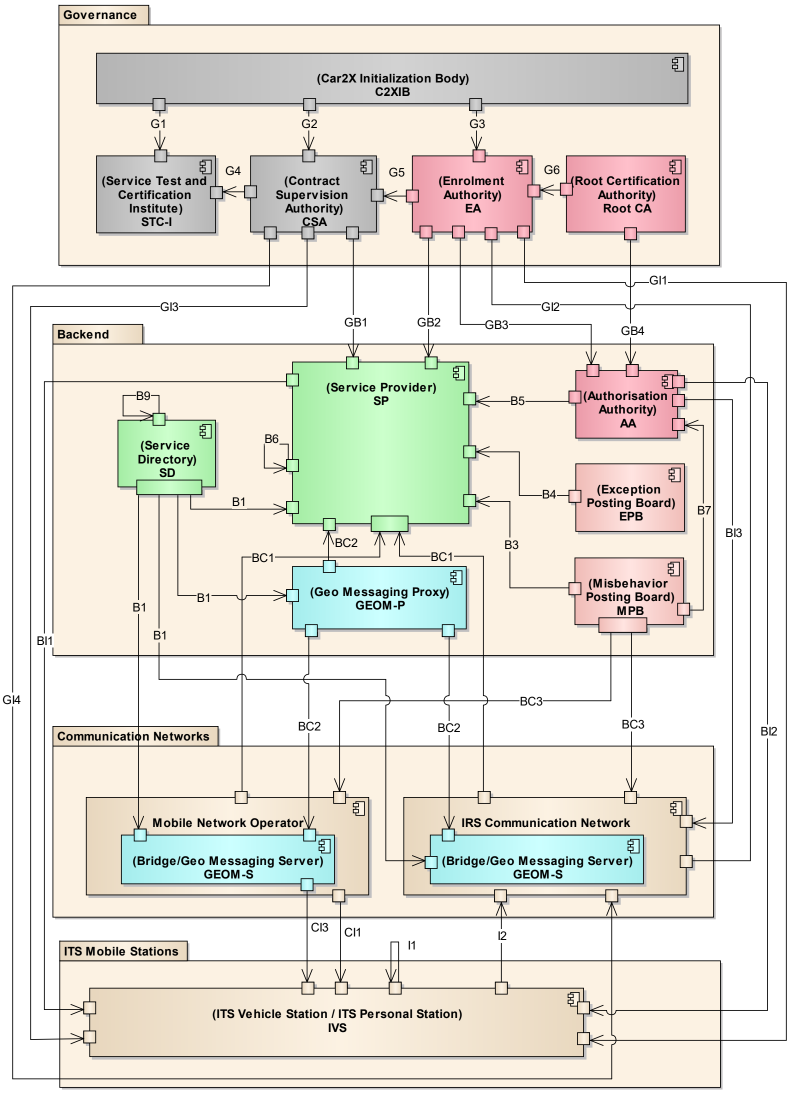


Figure 2: The CONVERGE architecture [44]

Besides those components, CONVERGE described some overarching concepts, needed in the architecture. Those were, for example: GeoMessaging over different networks, provider independent service directory, pseudonymous service usage and message topic aware communication via the GeoNetworking mentioned above. Most notably, CONVERGE focused on the absence of ‘single-points of failure’ regarding the implementation of the architecture. For example, the system does not relay on a single GeoMessaging Proxy to be present, but all Service Providers also provide this proxy functionality, thus creating a distributed proxy. By doing this, it is ensured, that a proxy is present, if at least one Service Provider is present.

2.1.1.3. COMPASS4D

The European project Compass4D focused on three services aiming to increase safety and comfort for drivers by: 1) reducing the number and severity of road accidents, 2) optimising the vehicle speed at intersections, and 3) possibly avoiding queues and traffic jams. The three services were Energy Efficient Intersection Service (EEIS), Road Hazard Warning (RHW), and Red Light Violation Warning (RLVW) [1]. Regarding the Compass4D architecture, the basic idea was to use as many concepts, standards and background from previous projects (COSMO, FREILOT, DRIVEC2X, ECOMOVE, COVEL) as possible, in order to define a consolidated and interoperable architecture for all Compass4D pilot sites. The reference architecture identified three main sub-systems, which were used by all pilot sites, while the architecture of the OBU and RSU followed the ETSI ITS station architecture as specified in ETSI ITS [2]. The three sub-systems were: 1) OBU, the unit responsible for handling ETSI G5 communication with the RSUs/OBUs or cellular communication (LTE) with the BO, and the driver, 2) RSU, fixed units at the side of the road (e.g. traffic lights), equipped with ETSI G5 communication facilities, 3) BO, consisting in two sub-components, TMC and POMS, in charge of the traffic control and the operation of the pilot sites. The following picture provides an overview of the reference architecture, where the focus was only on facilities and applications layers of the ETSI ITS station architecture [3].

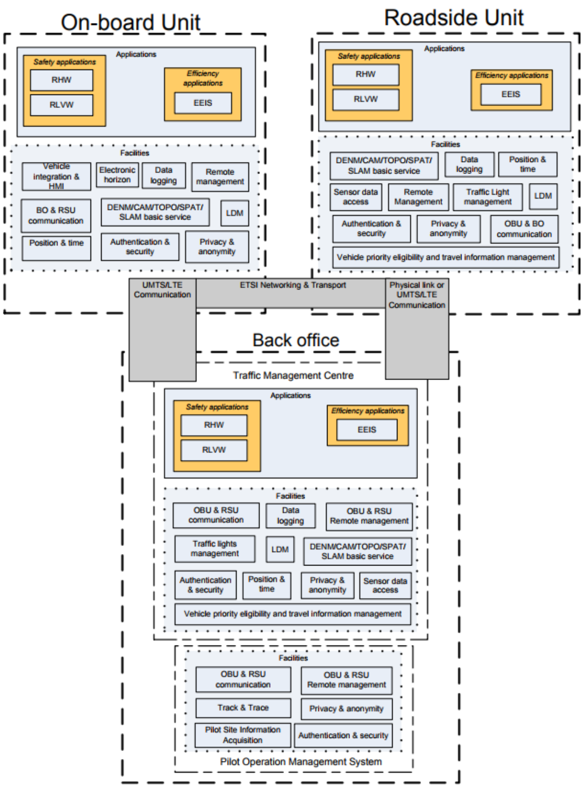


Figure 3: Compass4D Reference Architecture overview

2.1.1.4. MOBiNET

MOBiNET was a collaborative project, performed from 2012-11-01 to 2017-06-30, that aimed at simplifying the Europe-wide deployment of transport and mobility services by creating an “Internet of Mobility” in which transport users’ requests match Service Providers’ offers, and promotes openness, harmonisation, interoperability, and quality. It aimed to develop, deploy, and operate the technical and organisational foundations of an open, multi-vendor platform for Europe-wide transport and mobility services.

The key objective of the project is the simplification of the overall process of bringing together mobility service offerings and demand in a common market place. The open platform provides the required “glue” functionality to let Service Providers easily compose their services based on available data or other business-to-business (B2B) services, and to deliver their services to end users. End users will be enabled to easily discover and use these services. During MOBiNET project, ten example services had been identified that can be enhanced by a MOBiNET like platform. Besides these services, there were eight pilot sites EU-wide involved within the project: Aalborg, Helmond, Helsinki, London, Torino, Trikala, Trondheim, and Vigo. Each pilot site hosts one or multiple of the above-mentioned services. [32]

The figures below depict the components and tools as well the conceptual architecture of MOBiNET.

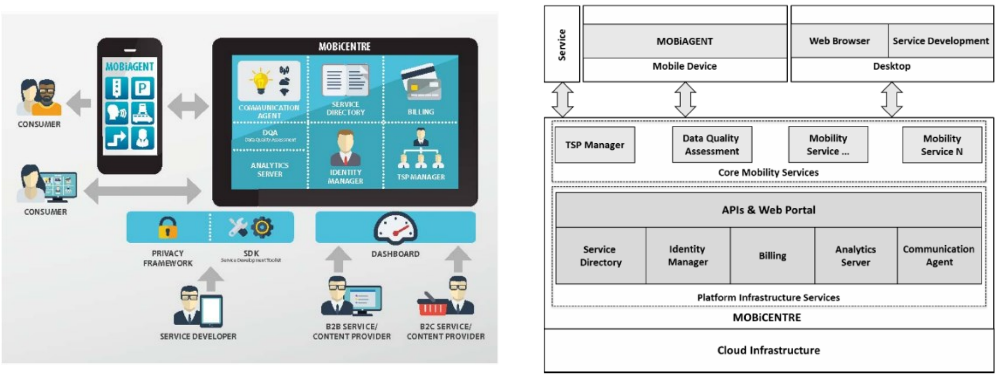


Figure 4: Component and tools [33] and Conceptual architecture of MOBiNET [32]

Key MOBiNET innovations aimed to address the barriers of cooperative system-enabled service deployment, including the lack of harmonised service interfaces, availability of communication means, inaccessibility and incompatibility of transport-related data, fragmentation of end user subscription and payment services, and proprietary technologies in end user devices.

In this view, the architecture and its components create a new ecosystem for drivers, users and providers of transport services. It offers solutions for users including one click access to a one-stop shop for context-aware mobility services, pan-European roaming & coverage, integrated user accounts for transport services throughout Europe and traveller assistance tools for service roaming and virtual ticketing. For road and traffic operators, publishing traffic and travel information to all users, attract new customers and save costs. For the data and services providers, it allows to deliver services to any kind of compliant customer device, directory of all mobility-related data and services and service/data trading without one-to-one negotiation using the automated mechanisms for service orchestration. For developers, it provides an opportunity to develop a broad range of mobility Apps. These activities are further supported by a service development kit. [32][33]

2.1.1.5. NordicWay

The proposed action, NordicWay, is a pre-deployment pilot of Cooperative Intelligent Transport Systems (C-ITS) services in four countries (Finland, Sweden, Norway and Denmark) which will be followed by wide-scale deployment and potentially to be scaled up to Europe. NordicWay has the potential to improve safety, efficiency, and comfort of mobility and connect road transport with other modes. NordicWay is the first large-scale pilot using cellular communication (3G and LTE/4G) for C-ITS. This access network will be covered in the future by LTE/4G and later by 5G, and no specific investments in the infrastructure will be needed. It offers continuous interoperable services to the users with roaming between different mobile networks and cross-border, offering C-ITS services across all participating countries. NordicWay puts emphasis on building a sustainable business model on the large investment of the public sector on the priority services of the ITS Directive. NordicWay is fully based on European standards and will act as the last mile between C-ITS research and development and wide-scale deployment [19][3].

The NordicWay architecture uses a message queuing approach to transfer messages between the different actors, such as Service Providers, OEMs (Original Equipment Manufacturers, means car makers here), and Traffic Message Centers. A driver, resp. smartphone user, only communicates with a Service Provider/OEM cloud, which in turn communicates with other clouds, which belong to both other Service Providers/OEMs and national Traffic Clouds. Messages between these actors are relayed through the NordicWay Interchange Node, which distributes them to the actors, which have subscribed to the messages.

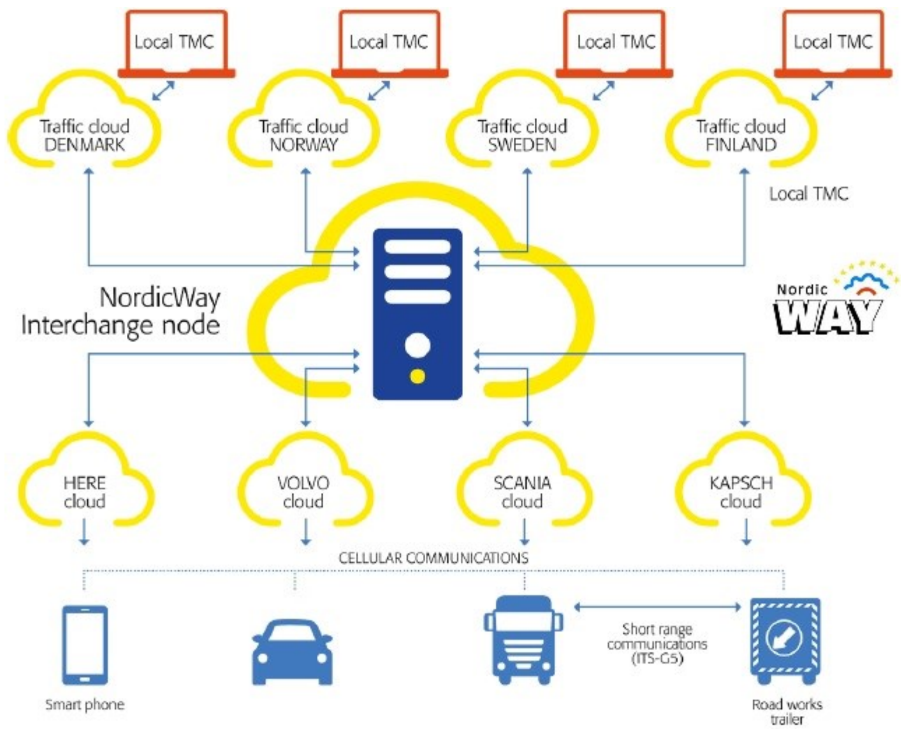


Figure 5: Nordic Way architecture

The NordicWay interchange uses a publish-subscribe AMQP (v1.0) queuing system for distributing messages between connected actors. In this system, all actors take on the role of either a producer or a consumer. A single actor can also be both a producer and a subscriber at the same time.

The data model for exchanged data is based on DATEX II version 2.3 level A with level B extensions. This means that nodes that support exchange of messages, which are conformant with this model, will be interoperable with respect to data exchange in NordicWay. The data definitions for DATEX II will be implemented as XML schemas, and the serialization format for DATEX II messages will be XML.

2.1.1.6. US ITS

The CVRIA (Connected Vehicle Implementation Architecture) Team, led by the ITS Joint Program Office, is comprised of the National ITS Architecture Team (led by Iteris), the Standards Program Technical Support Services Team (led by Booz Allen Hamilton) and the Policy Team (ITS JPO Policy Program and the Volpe National Transportation Systems Center). CVRIA is being developed as the basis for identifying the key interfaces across the connected vehicle environment, supporting this way further analysis for the identification and prioritization of standards' development activities. The approach taken to develop the CVRIA includes a number of source documents as inputs, such as Concepts of Operation (ConOps) documents from connected vehicle applications, Operational Concepts, the Core System ConOps, existing standards, the existing National ITS Architecture and the Core System architecture, as well as the existing International and Domestic standards. The development of the System Architecture was based on the fundamentals of ISO/IEC/IEEE 42010:2011 standard, including steps to define, data, messages, and the full environment in which the stakeholder concerns are satisfied. "CVRIA aims to become a "framework" for developers, standards organizations, and implementers to all use as a common frame of reference for developing the eventual systems"[4].

The four Views comprising CVRIA are described below [4]:

/ Enterprise: This view describes the relationships between organizations and the roles those organizations play within the connected vehicle environment. Here, the emphasis is given to the set of Enterprise Objects, which interact to exchange information, manage and operate systems beyond the scope of one organization. The Enterprise View includes relationships and interactions between the Enterprise Objects, as well as significant elements for the delivery of services, defined as Resources. The relationships between Enterprise Objects and between Enterprise Objects and Resources are determined by Roles (e.g., owns, operates, develops, etc.). Between Enterprise Objects there can also be Coordination in the form of an agreement or contract, in order to achieve the common purposes necessary to implement and carry-out a connected vehicle application.

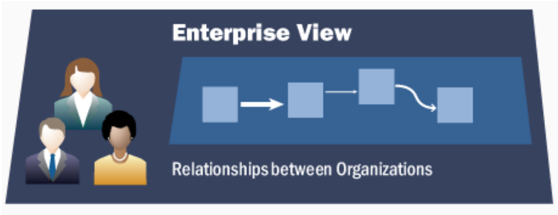


Figure 6: CVRIA Enterprise View

/ Functional: The Functional View addresses the analysis of abstract functional elements and their logical interactions. Here CVRIA is depicted as a set of hierarchically organized Processes (activities and functions), which trace to a set of Requirements derived from the connected vehicle source documents. The data flows between processes and the data stores, where data may reside for longer periods, are all defined in a Data Dictionary. The Process, or Function, is defined by a set of actions performed by this element to achieve an objective or to support actions of another Process. This typically involve data collection, data transformation, data generation, data generation or processing in performing those actions.

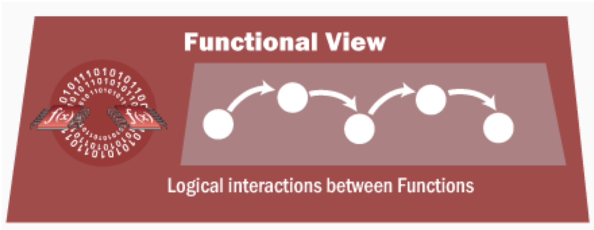


Figure 7: CVRIA Functional View

/ Physical: The Physical view describes the connections between Physical Objects within the connected vehicle environment. CVRIA is depicted as a set of integrated Physical Objects, which interact and exchange information to support the connected vehicle applications. Physical Objects represent the major physical components of the connected vehicle environment, including Application Objects that define more specifically the functionality and interfaces required to support a particular application. Information Flows depict the exchange of information that occurs between Physical Objects and Application Objects, which are identified by Triples. The Triples include the source and destination Physical Objects and the Information Flow that is exchanged. Each Application Object is linked to the Functional View and to the Enterprise view.

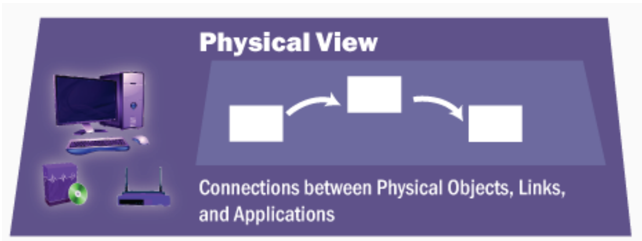


Figure 8: CVRIA Physical View

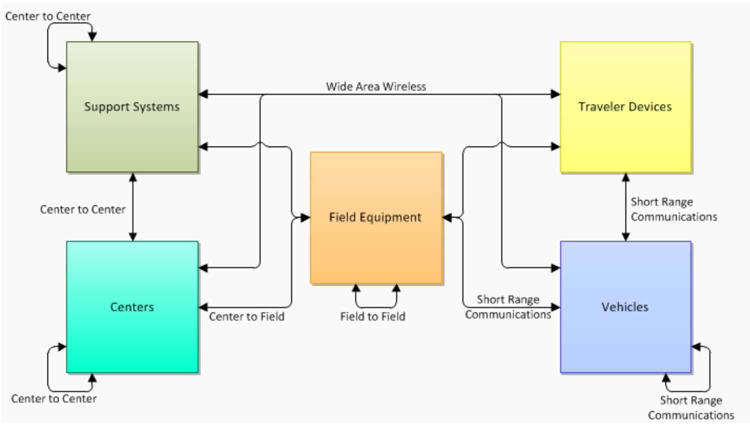


Figure 9: CVRIA Physical View - Interactions between systems

/ The Communications View describes the communications protocols necessary to provide interoperability between the Physical Objects. The CVRIA NITSA Communications Model and Communications Profiles are based on the Open System Interconnection (OSI) Model, the NTCIP Framework, and DSRC/WAVE Implementation Guide.

Figure 10: CVRIA Communications View

The 8 layers of the CVRIA NITSA Communications Model are described below:

1. ITS Application Information Layer: The ITS Application information layer standards specify the structure, meaning, and control exchange of information between two end points.
2. Application Layer: The application layer standards define the rules and procedures for exchanging encoded data.
3. Presentation Layer: The presentation layer standards define the rules for representing the bits and bytes of information content to be transferred.
4. Session Layer: The session layer provides the mechanism for opening, closing and managing a dialogue between application processes. Sessions may be asynchronous as in paired requests and responses (information exchanges), asynchronous as in an unsolicited publication of information, and may require acknowledgement or receipt or not.
5. Transport Layer: The transport layer standards define the rules and procedures for exchanging application data between endpoints on a network.
6. Network Layer: The network layer standards define the routing, message disassembly/re-assembly and network management functions.
7. Data Link Layer: The data link layer standards define the rules and procedures for exchanging data between two adjacent devices over some communications media.
8. Physical Layer: The physical layer is a general term used to describe the numerous signalling standards within this layer, typically developed for specific communications media and industry needs.

2.1.2. Related C-ITS Projects

Related projects and their architectural aspects e.g. quality requirements and functional structure models are described in short below.

2.1.2.1. C-The-Difference

C-The Difference pilot project has been elaborated on the basis of a shared vision developed and adopted by the consortium partners representing demand and supply sides who have been committed for the last 10 years to bring C-ITS (Cooperative Intelligent Transport Systems) to the market through intensive efforts and long lasting investments in the development and deployment of C-ITS services. This group of pioneers are strong believers in the capacity of C-ITS services to bring efficient and cost-effective solutions to address urban mobility problems with respect to traffic efficiency, safety, and impact on the environment.

Success in implementation and long run provision of C-ITS services rely on five golden rules that need to be addressed in a coordinated and integrated way:

/ Inter-operability: Thanks to adoption of international standards, C-ITS services are fully inter-operable and continuity of services can be guaranteed independently from geographical location, C-ITS Service Provider and C-ITS system suppliers

/ Sustainability: Key actors from public and private sectors involved in the C-ITS service chain are engaged in a long-term cooperation to create added value to all users in their daily mobility, to develop viable business models, to raise awareness on C-ITS benefits, to build European-wide C-ITS market and to contribute to economic growth.

/ Scalability: A deployment scenario can be customized according to user needs, urban transport and mobility policies, existing infrastructure, and financial capacity. Thanks to scalable architecture, implementation can start with a first package of C-ITS services that deliver quick benefits with respect to urban mobility priorities and can be further developed in a modular approach by means of additional services and/or extended geographical coverage and/or an increasing number of users with minimum additional costs. Combined use of G5 and 3G/4G communication technologies contribute to speeding up the penetration rate of several C-ITS services.

/ Replicability: C-ITS services are not restricted to a small number of front-runner cities. All cities can benefit from experience of early adopters by means of effective knowledge sharing to facilitate decision making in initial C-ITS investment and to accelerate deployment of customized C-ITS solutions.

/ Reliability: Cities can rely on sound evidence of C-ITS benefits to take decisions on C-ITS service implementation that can be integrated within existing transport and mobility infrastructure. Cities can invest in confidence in a portfolio of C-ITS services based on mature and cost-effective technologies, and open and standardized architecture enabling high quality service provision and capacity to integrate new features.

Objectives of C-The-Difference are the following:

/ Deliver comprehensive and integrated impact assessment by means of enhanced evaluation methodology and up to 18 months operation of C-ITS services package.

/ Bridge the gap between most advanced C-ITS implementations in urban environment and large-scale deployment and operations by targeting professionals responsible for urban transport planning and operations, policy makers and decision makers.

/ Convince European cities to invest in mature and proven C-ITS solutions by fostering and replication through City Twinning Program.

/ C-The-Difference offers the following key innovative solutions:

/ A traffic app allowing you to adapt your driving depending on the infrastructures and the different road events that might occur. Deployed and functional on Bordeaux urban area, it can be downloaded in the app stores.

/ Green light priority with SSM/SRM functionality for direction dependent priority calls. Unlike older projects like Compass4D, it is possible to request priority for a specific turn direction. This improves the effectiveness for the prioritized vehicle and traffic flow for other vehicles.

/ Extended emergency vehicle warning with indication of the direction of the vehicle on the HMI.

2.1.2.2. SCOOP@F phase 2

SCOOP@F is a C-ITS pilot deployment project, intending to connect approximately 3000 vehicles with 2000 kilometres of roads. It consists of 5 pilot sites, Ile-de-France, "East Corridor" between Paris and Strasbourg, Brittany, Bordeaux and Isère, and is composed of SCOOP@F Part 1, 2014-2015, and SCOOP@F Part 2, 2016-2018. SCOOP@F Part 2 includes the validations of C-ITS services in open roads, cross border tests with other EU Member States and development of a hybrid communication solution (3G-4G/ITS G5) [5]. The architecture of the SCOOP@F project is presented in terms of network architecture its integration in the road operators' networks. Regarding the physical architecture, the servers and equipment needed for operation include PKI servers, to manage the different certificates, road operator servers and OBUs. The communications between RSUs and OBU are in: GeoNetworking for exchanges of CAM and DENM messages, IPv6 for OBU exchanges with the PKI, and IPv4 for RSUs exchanges with the PKI [6].

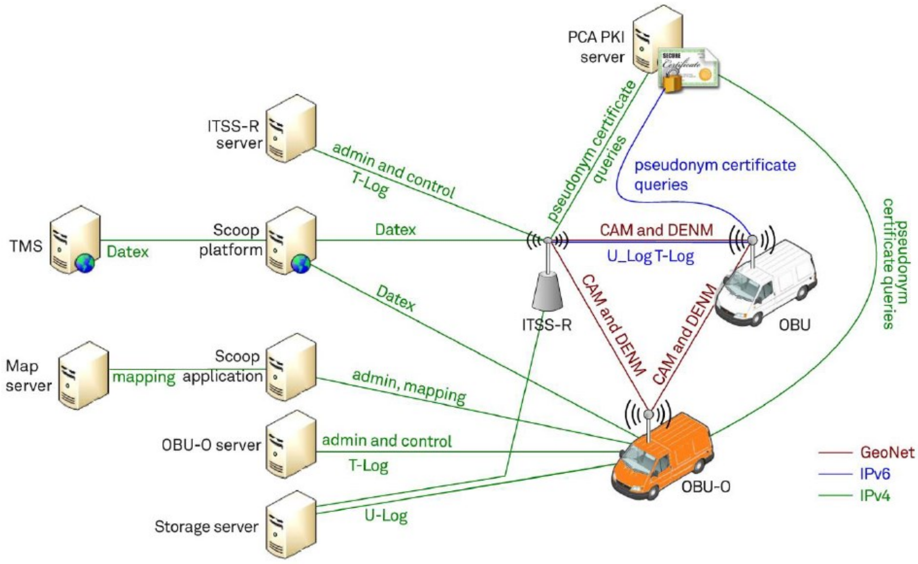


Figure 11: Summary schema of exchanges

The Scoop@F architecture must fit into the existing networks of traffic operators, presented schematically as follows [6]:

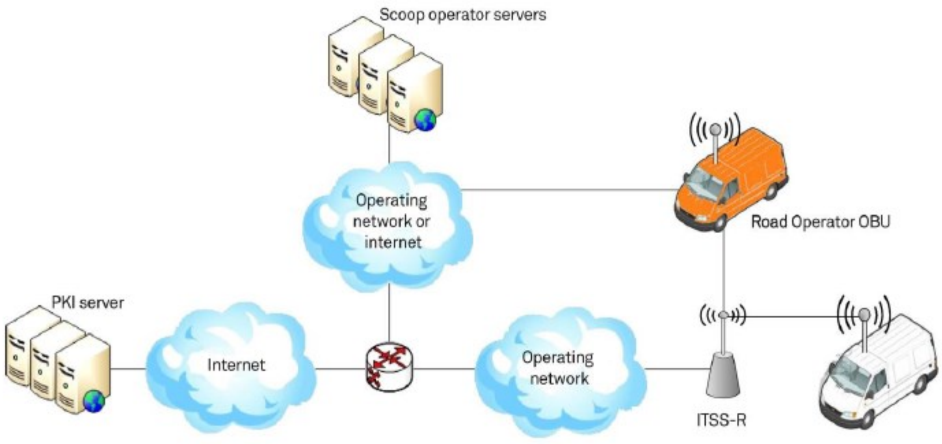


Figure 12: General integration schema

2.1.2.3. InterCor

InterCor constitutes an action, which aims to streamline C-ITS implementation in 4 member states linking the different national initiatives towards a harmonized strategic rollout and common specification. C-ITS pilot sites to communicate data through cellular and/or ITS G5 networks will be installed in approximately 968 km along the Netherlands, Belgium, UK, and France, for operation and evaluation of C-ITS services. InterCor will focus on the deployment of "Day-1" services as recommended by EC "C-ITS Platform" such as Road works warning, Green Light Optimized Speed Advisory, In-Vehicle-Signage and Probe vehicle data. Furthermore, an additional use case dedicated to transport of goods (MultiModalCargoTransportationOptimization) will also be deployed in several countries in order to integrate logistics and C-ITS services but also to test interoperability between countries. The action is part of the C-Roads platform, which is a platform of Member States working on the deployment of C-ITS services. Cross-border tests will also be conducted with other C-Roads Member States [24].

2.1.2.4. C-Roads

C-Roads [42] is a platform of Member States working on the deployment of C-ITS services. C-ITS pilot sites will be installed across the EU for testing and later operation of "Day-1" applications as recommended by EC "C-ITS platform". Member States will invest in their infrastructure, while the industry will test components and services. Technical and organisational issues will be tackled by the C-Roads platform to ensure interoperability and harmonisation of C-ITS between pilots.

The project runs from February 2016 until December 2020 and is cofounded by the Connecting Europe Facility (CEF).

The services C-Roads wants to implement are:

- Slow or stationary vehicle(s) and traffic ahead warning
- RWW: Road Works Warning
- Weather Conditions
- Emergency Vehicle Approaching
- OHLN Other Hazardous (Location) Notifications
- IVS: In-Vehicle Signage
- In-Vehicle Speed Limits
- Signal Violation / Intersection Safety
- GLOSA: Green Light Optimal Speed Advisory
- Probe Vehicle Data
- Shockwave Damping

C-Roads published a first deliverable "Harmonised C-ITS Specifications for Europe" for the RWW, IVS, OHLN and GLOSA services.

The Focus is on ITS-G5 communication (ETSI ITS G5) and Hybrid communication with a security mechanism.

2.1.2.5. CITRUS

CITRUS [35] stands for C-ITS for Trucks. It is a Belgian project, which will run from October 2016 until September 2019, that aims to improve road safety and reduce CO2 emissions of truck traffic. CITRUS is cofounded by the Connecting Europe Facility TRANSPORT.

The project builds a companion mobile app for truck drivers tested with 300 truck drivers. The services are based on existing 3G/4G communication in combination with geographical messaging technologies. ITS-G5 is envisaged.

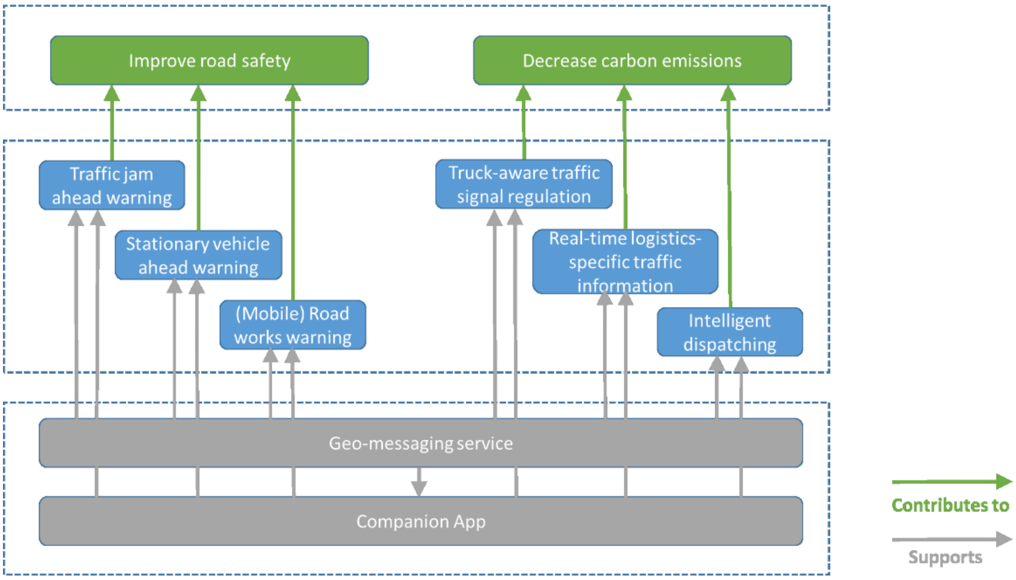


Figure 13: CITRUS architecture

The Day-1 services are:

- / Traffic jam ahead warning
- / Stationary vehicle ahead warning
- / (Mobile) Road works ahead warning
- / Truck-aware traffic signal regulation (GLOSA)

Day-1.5 services are:

- / Real-time logistics-specific traffic information
- / Intelligent dispatching

The project concentrates on the principal highways in Flanders and semi-motorways near Halle where the Colruyt distribution center is located [35] [50].

2.1.2.6. VRUITS

The EU-funded VRUITS project, which started in 2013, aims at actively integrating the “human” element in the ITS approach by focusing on needs of all relevant stakeholder groups, in order to improve traffic safety and the general mobility of vulnerable road users (VRUs) [7]. The VRUITS architecture supports the following ITS applications [8]:

- / Intelligent Pedestrians Traffic Signal
- / Intersection Safety
- / Powered Two Wheelers (PTW) Oncoming vehicle info system
- / Vulnerable Road User (VRU) Beacon System
- / Roadside Pedestrian Presence
- / Bicycle to car communication
- / Green wave for cyclists

This VRUITS reference architecture, used to develop sub-systems and elements for C-ITS applications for VRUs, is through [8]:

- The physical architecture, which is a high-level description of the physical ITS sub-systems used by VRUs, Vehicles, Roadside and Central layer, together with high-level description of the communication/interaction between these sub-systems.
- The Functional architecture, which describes the functional elements within the sub-systems in the VRU, Vehicle, Roadside, and Central layer.
- The Communication architecture, which describes the type of communication and networks used between the functional elements of the physical sub-systems.

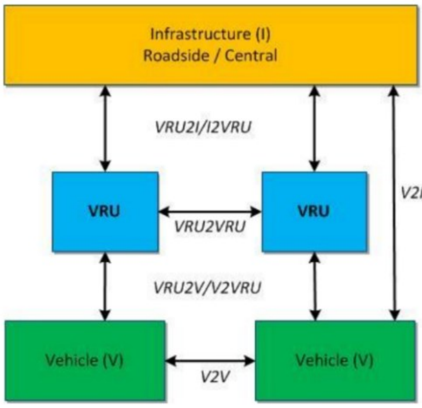


Figure 14: Physical architecture for C-ITS applications with Vulnerable Road Users

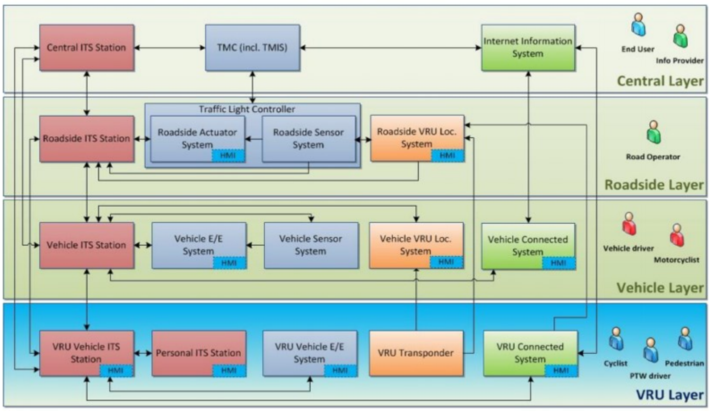


Figure 15: Functional Architecture for C-ITS with Vulnerable Road Users

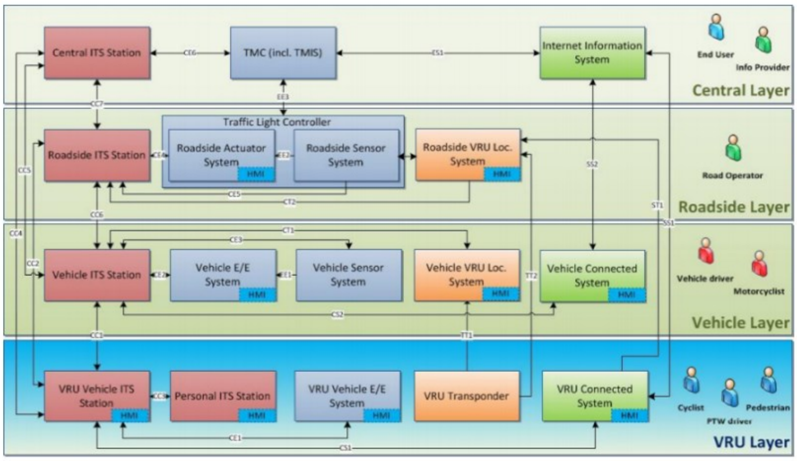


Figure 16: Functional architecture with marked interfaces

2.1.2.7. iKoPa

The German project iKoPA (Integrated cooperating platform for automated electric vehicles)[36] is a continuation project of CONVERGE. It was started in 2016 and will run until the end of 2018. It focuses on the enhancement of the CONVERGE architecture described above. It will integrate DAB+ as a communication network, assess the usefulness of the architecture for electric mobility and validate the conformity of the architecture with the requirements created by the General Data Protection Regulation (Regulation (EU) 2016/679)[37] coming into effect on 2018-05-25.

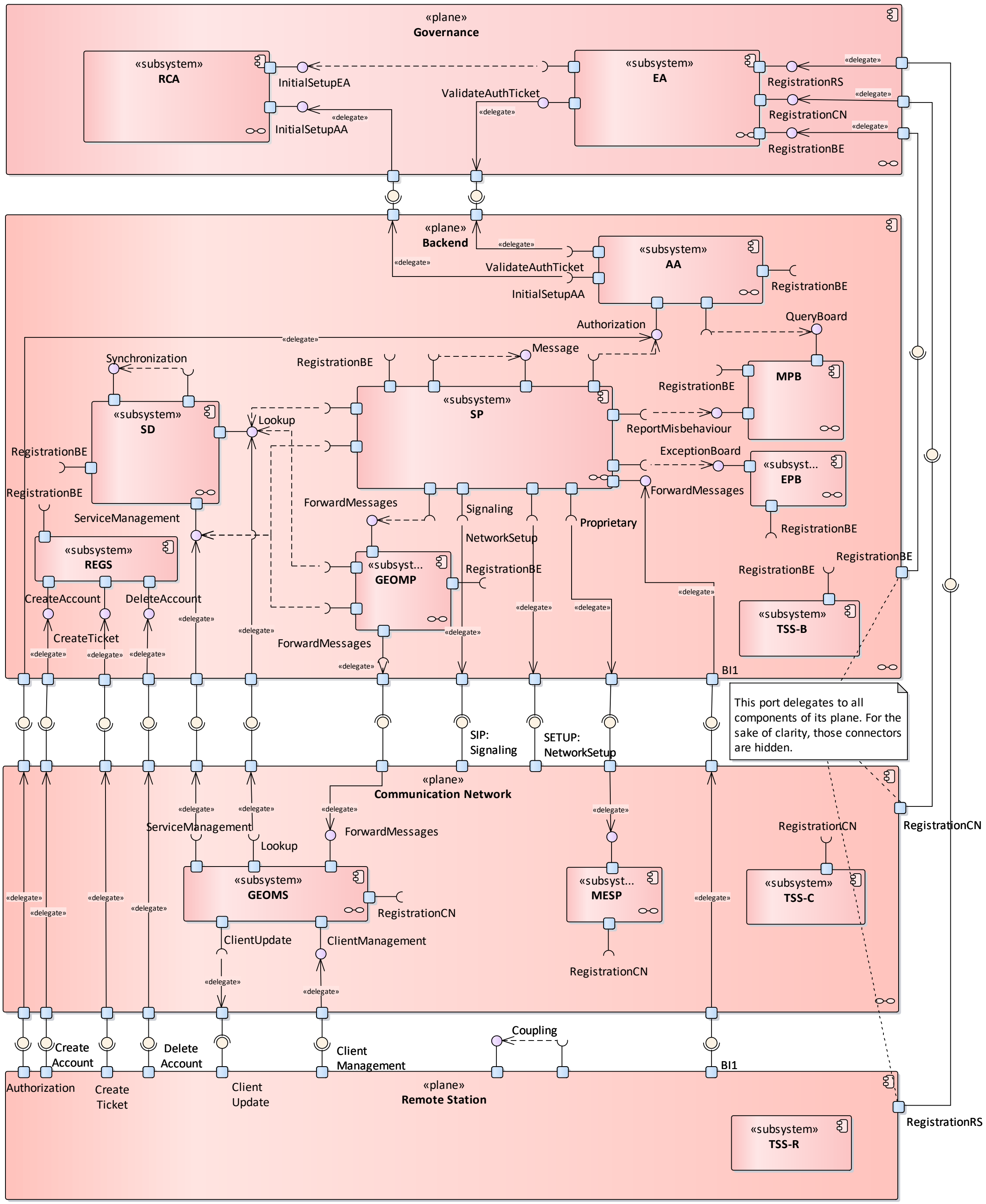


Figure 17: The iKoPA architecture [43]

The basic architecture is very similar to the Car2X Systems Network designed by CONVERGE. However, interfaces have been enhanced and described more independently. In addition, new entities have been introduced, like the Registration Server. This entity decouples the registration process from the service usage, so that a Service Provider is not able to determine the identity of its users.

2.1.2.8. Talking Traffic

The goal of Talking Traffic [38] is C-ITS deployment. It is a collaboration between the Dutch Ministry of Infrastructure and the Environment, regional and local authorities and (inter)national companies [51].

The use cases are In-vehicle signage, Road hazard warning, Priority at traffic lights, Traffic lights info, Flow optimization and In-vehicle parking info.

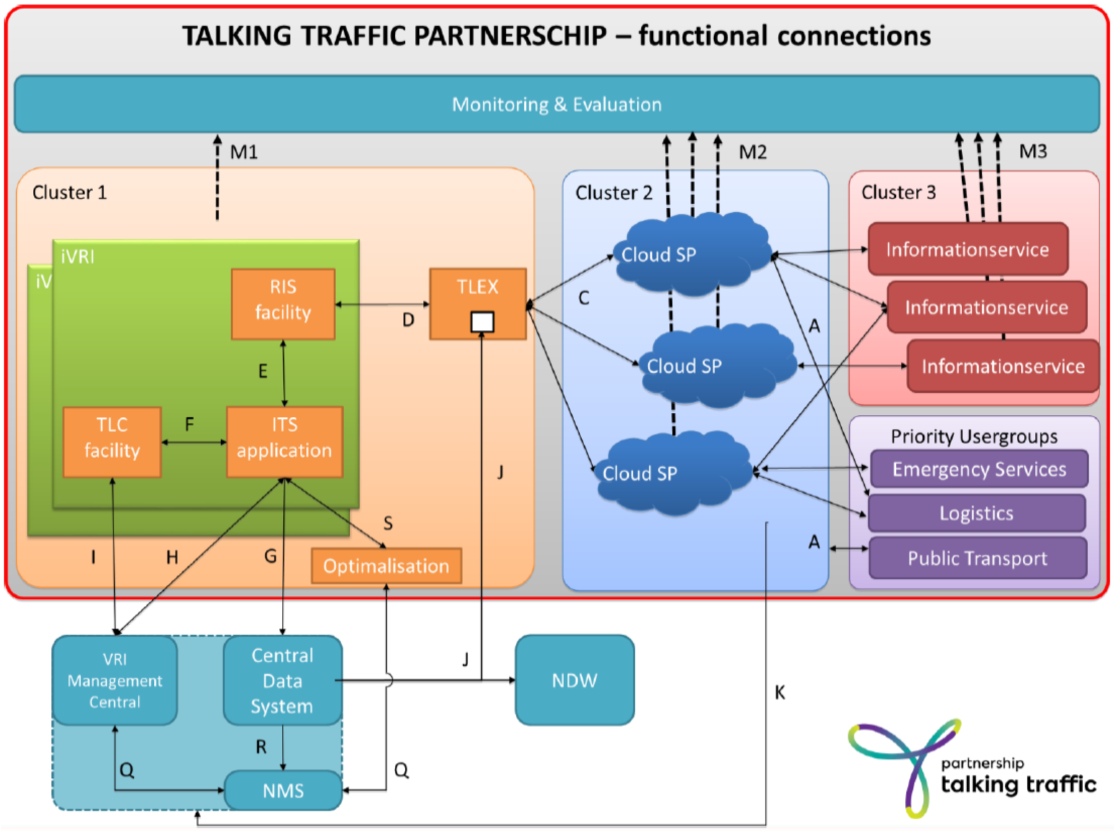


Figure 18: Talking traffic architecture [38]

2.1.2.9. C-ITS Corridor

German, Dutch and Austrian highway operators, in cooperation with partners from the automotive industry, have launched the gradual deployment of Cooperative Systems. This allows the exchange of traffic-related information among vehicles and between vehicles and the roadside infrastructure. In June 2013, the national transport ministries of Germany, the Netherlands and Austria signed a Memorandum of Understanding (MoU), which marked the start of Cooperative Systems[39]. The ministries agreed:

/ to develop a common launch/rollout timetable for the implementation of the first cooperative applications on highways

/ to define common conventions that ensure a harmonized interface with vehicles in the three countries

/ to implement roadside facilities for the first collaborative applications.

A highway corridor, extending from Rotterdam (Netherlands), via Frankfurt/ M. (Germany) to Vienna (Austria), was chosen as the route for the first deployment - the so-called C-ITS Corridor [39].

The Netherlands, Germany, and Austria have agreed upon the introduction of two cooperative services: (1) roadworks warning and (2) improved traffic management by vehicle data. They are part of the “Day 1” services defined by the Amsterdam Group. Both applications have been selected because of their present relevance, as there are still many accidents related to roadworks, and with regard to the further dissemination of C-ITS technology. In both cases, communication from the vehicle and infrastructure is established via short-range communication (Wifi 802.11p, 5.9GHz) or the cellular network (3G, 4G). Both initial applications increase road safety and provide the basis for an improved traffic flow. Thanks to the collaboration of the automotive industry, service providers, and road operators, cooperative ITS systems will be directly experienced by the road user and are useful for everyone [39].

2.1.2.10. ECo-AT

ECo-AT (European Corridor – Austrian Testbed for Cooperative Systems) is the Austrian project to create harmonised and standardised cooperative ITS applications jointly with partners in Germany and the Netherlands. The project is led by the Austrian motorway operator ASFINAG and the consortium consists of Kapsch TrafficCom AG, Siemens AG Österreich, SWARCO AG, High Tech Marketing, Volvo Technology AB, ITS Vienna Region, FTW (Forschungszentrum Telekommunikation Wien) and BASt (Bundesanstalt für Straßenwesen). Within the next years C-ITS shall be developed for being applied in the Cooperative ITS Corridor Rotterdam – Frankfurt/M. – Wien. This happens in close cooperation between the EU-member states Netherlands, Germany and Austria, who have signed a Memorandum of Understanding. Austria has established itself as constructive implementation pioneer of C-ITS applications within the European Union – not least because of the project Testfeld Telematik. The next steps towards pan-European deployment in the European C-ITS Corridor from the Netherlands via Germany to Austria will be prepared and developed within the project ECo-AT for the Austrian section[25].

2.1.2.11. CODECS

The Coordination and Support Action COoperative ITS DEployment Coordination Support (CODECS) supports the European Commission and the manifold stakeholders involved in C-ITS deployment in finding strategic and technical policy solutions and processes for a consolidated C-ITS roll-out. CODECS serves as hub for transparent information and knowledge transfer on function approaches, experiences and lessons-learned by stakeholders active in the initial deployment. To ensure European-wide seamless (cross-border) interoperability and end-user experiences, CODECS develops a harmonised standards profile supporting a growing amount of C-ITS services. To address key organisational and technology related issues, CODECS will derive a strategic common road map from preferences of the involved stakeholders, giving direction for innovation, testing, standardisation, and deployment beyond Day One. CODECS also supports future C-ITS common deployment by achieving a clear understanding on policies, roles, and responsibilities. CODECS does convey these insights to the C-ITS deployment platform initiated by the European Commission and to the Amsterdam Group [26].

2.1.2.12. AUTOCITS

The aim of the Study is to contribute to the deployment of C-ITS in Europe by enhancing interoperability for autonomous vehicles as well as to boost the role of C-ITS as catalyst for the implementation of autonomous driving. Pilots will be implemented in 3 major Core Urban nodes (Paris, Madrid, Lisbon) located along the Core network Atlantic Corridor in 3 different Member States. The Action consists of Analysis and design, Pilots deployment and assessment, Dissemination and communication as well as Project Management and Coordination. The three pilots will test and evaluate C-ITS services for autonomous vehicles under the applicable traffic regulation, study its extension to other European countries and contribute to the C-Roads and C-ITS platform as well as to other European standards organizations [27].

2.1.2.13. CITRUS

The Action takes place in Belgium and studies the technical and economic viability of a companion mobile app for truck drivers. It envisages the development of the app as well as a pilot deployment and testing involving around 300 truck drivers. The app will provide some services relating to “Day 1 services” as identified by the C-ITS platform, like giving safety related warnings or advice as regards speed, routing, and other information. Services deployed will be based on a cellular C-ITS approach in combination with geographical messaging technologies. The project will contribute to improve road safety and reduces CO2 emissions of truck traffic [28].

2.1.2.14. PROSPECT

PROSPECT will significantly improve the effectiveness of active VRU safety systems compared to those currently on the market. This will be achieved in two complementary ways, first by expanded scope of VRU scenarios addressed and second by improved overall system performance (earlier and more robust detection of VRUs, proactive situation analysis, and fast actuators combined with new intervention strategies for collision avoidance). PROSPECT targets five key objectives [29]:

- Better understanding of relevant VRU scenarios
- Improved VRU sensing and situational analysis
- Advanced HMI and vehicle control strategies
- Four vehicle demonstrators, a mobile driving simulator and a realistic bicycle dummy demonstrator
- Testing in realistic traffic scenarios and user acceptance study.

The consortium includes the majority of European OEMs (Audi, BMW, DAIMLER, TME and Volvo Cars) currently offering AEB systems for VRU. They are keen to introduce the next generation systems into the market. BOSCH and CONTI will contribute with next generation components and intervention concepts. Video algorithms will be developed by UoA and DAIMLER. Driver interaction aspects (HMI) are considered by UoN and IFSTTAR. Euro NCAP test labs (IDIADA, BAST, TNO) will define and validate test procedures and propose standardization to Euro NCAP and UN-ECE. Accident research will be performed by Chalmers, VTI and BME, based on major in-depth accident databases (GIDAS and IGLAD) and complemented by East Europe data. The work will be done in cooperation with experts in Japan (JARI, NTSEL) and the US (VTTI, UMTRI, NHTSA) [29].

2.1.2.15. XCYCLE

The XCYCLE [49] project will contribute to innovative and efficient advanced safety measures to reduce the number of accidents, often of high severity, involving cyclists in interaction with motorised vehicles. The XCYCLE Project has started on June 1st, 2015 and its activities will be completed by November 2018. The project is developing [30]:

/ Technologies that improve active and passive detection of cyclists

/ Systems informing both drivers and cyclists of a hazard at junctions

/ Effective methods of presenting information in vehicles and on-site

/ Cooperation systems aimed at reducing collisions with cyclists.

Two relevant use cases will be bicycle interaction with large vehicles and cars at intersections and immediate or extended green traffic light for cyclists approaching traffic signals. An in-vehicle detection system and a system of threat mitigation and risk avoidance by traffic signals will be developed. The components developed and built up will be systematically integrated, implemented, and verified. A new large-scale research infrastructure in the city of Braunschweig (Germany) and a second test mobile platform will be used as test site. A demo bicycle with a cooperative technology will be developed and tested as well. A user-centred approach will be adopted. Behavioural evaluation will part of the whole process: attentional responses using eye tracking data; evaluation of human-machine interface; acceptance and willingness to pay. In the cost-benefit analysis, behavioural changes will be translated into estimated crashes and casualties avoided [30].

2.1.2.16. SOLRED

The overall objective of the action is to test a new Integrated Fuel and Fleet Management System, the so-called C-ITS Telemat, which enables the automatic real time calculation of the smartest route plan and the automatic estimation, authorisation and payment of the refuelling needed to complete a planned route. Moreover, the system provides the heavy duty vehicles (HDV) drivers and fleet managers with useful notifications concerning maintenance scheduling, eco/safety driving, traffic issues as well as information on the estimated fuel consumption vis-a-vis the real one[31].

The testing of this system will be done through a monitoring network, which will involve approximately 53 Repsol service stations along the Spanish part of the Atlantic and Mediterranean core network Corridors. This C-ITS Telemat is expected to contribute to road safety by avoiding accidents and fuel thefts and fraud, but also will assist in improving traffic flows, and reducing fuel consumption, congestion, and environmental impacts. In particular, this new technology is expected to reduce fuel fraud by 5% and fuel consumption by 3% as compared with the previous ITS Telemat technology used by Repsol service stations [31].

2.2. High-level reference architecture description

2.2.1. C-ITS Architecture Framework

2.2.1.1. Architecture Framework

An architecture framework is one of the widely-applied approaches used in software/system architecting of complex systems. The architecture frameworks facilitate communication and cooperation between different stakeholders during architecting and building complex systems such as C-ITS. Many different stakeholders with their interweaving concerns require a systematic approach for addressing complexity and full lifecycle of the system. Example representations of widely applied architecture frameworks include Kruchten's 4+1 View Model, TOGAF, and Zachman framework. 4+1 is developed by Kruchten as a generic architecture framework for describing the architecture of software-intensive systems based on the use of multiple, concurrent views [15]. TOGAF provides a practical and industry standardized approach for designing an enterprise architecture [16]. Zachman framework is used for modelling an enterprise's information infrastructure from six perspectives [17].

According to the ISO/IEC/IEEE 42010:2011 standard, an architecture framework establishes a common practice for creating, interpreting, analysing and using architecture descriptions within a particular domain of application or stakeholder community [12]. As a well-defined architecture framework is considered to be an important part of any architecture description [13], we define an architecture framework for the C-ITS domain. To put architecture framework and architecture description concepts in context, we extend the conceptual model of the ISO/IEC/IEEE 42010 architecture framework as illustrated in

Figure 19. Without the common C-ITS architecture framework, different categorizations and ad-hoc notations are used in the existing C-ITS reference architectures. The C-ITS domain covers not only software/system engineering field, but also traffic engineering, civil engineering, information technology etc., which require a unified definition of architecture framework for the C-ITS domain.

The conceptual model of *architecture framework* is highlighted in blue and the relationships of architecture description concepts are added to the original standard diagram. As illustrated, an *architecture description* helps the stakeholders using a set of Architecture Views and models. An *Architecture View* conforms to a *viewpoint* which addresses stakeholder concerns and can be shaped by a number of perspectives. The *perspective* defines concerns that guide architectural decision making to help ensure that the resulting architecture quality characteristics considered by the perspective [14].

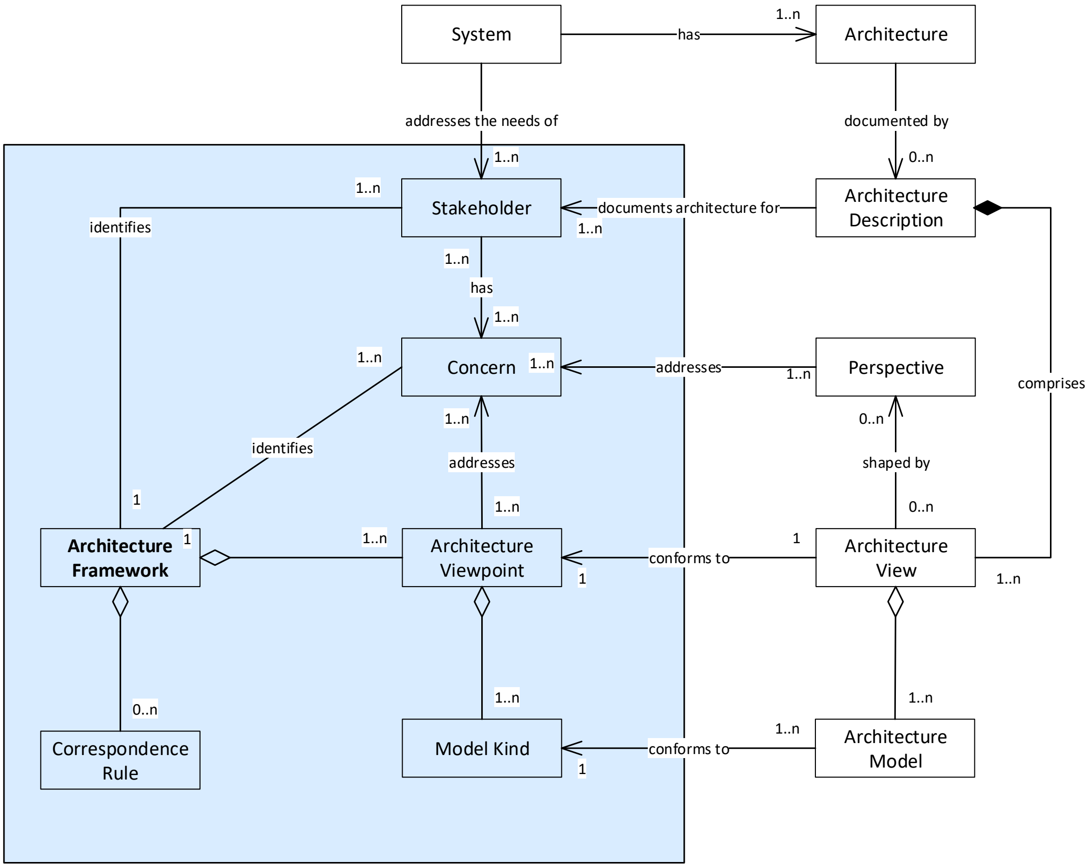


Figure 19: Architecture framework in context

To enable systematic architecture description of C-ITS, the ISO/IEC/IEEE42010:2011 is used to define the C-ITS architecture framework. As described in the definition of an architecture framework, the C-ITS architecture framework specifies stakeholders, their concerns, viewpoints, model kinds, and correspondence rules. In addition, architecture perspectives related to C-MobILE project will be addressed. C-ITS architects can use an architecture framework to represent the C-ITS reference architecture, concrete, implementation and deployment site architectures.

2.2.1.1.1. C-ITS stakeholders and Concerns

A stakeholder is an individual, team, or organization holding concerns for the system such as architect, designer, user, and authority [12]. A concern is any interest in the system such as functionality, structure, behaviour, and interoperability [12]. The C-ITS addresses the needs of following stakeholders.

Stakeholder	Description	Concerns
End-User		
Driver	The real final individual user of the (private or commercial) road network and a service [DITCM] using a motorized vehicle.	/ Functionality / Dependability / Interoperability / Security (Privacy) / Maintainability / Cost
PTW	Individual user using a motorbike, electric bicycle.	/ Functionality / Dependability / Interoperability / Security (Privacy) / Maintainability

		/ Cost
Cyclist	VRU[1] using a bicycle.	/ Functionality / Security (Privacy) / Maintainability / Cost
Pedestrian	VRU, on foot.	/ Functionality / Security (Privacy) / Maintainability / Cost
Visually Disabled Pedestrian (VDP)	Disabled road user [VRUITS].	/ Functionality / Usability (Ease of use) / Security (Privacy) / Maintainability / Cost
Non-Motorized Vehicle User	Users in non-automated vehicles (wheelchairs, buggies, prams).	/ Functionality / Usability (Ease of use) / Security (Privacy) / Maintainability / Cost
Traveller	Individual user that may travel with more than one type of transportation means and uses a C-ITS service.	/ Functionality / Usability (Ease of use) / Dependability / Security (Privacy) / Maintainability / Cost
Fleet Operator	Manages a number of vehicles such as buses, emergency vehicles, trucks or taxi cars [DITCM].	/ Functionality / Usability (Ease of use) / Reliability / Maintainability
Road Works Operator	Road side recovery (tow trucks), Utilities (road sweepers, dustcarts), road works, forensics, etc.	/ Functionality / Dependability / Interoperability / Security (Authenticity) / Maintainability / Cost
Technological Provider		
Original Equipment Manufacturer (OEM)	Manufacturer and suppliers for cars, trucks, trailers, caravans, commercial vehicles, etc.	/ Functionality / Maintainability / Security (privacy) / Interoperability

[1] Any kind of vulnerable road user

		/ Cost
Telecom/Mobile Network Operator	• Network Operators • Infrastructure providers • Connected device and appliance manufacturers • Broadcast	/ Functionality / Maintainability / Security (privacy) / Interoperability / Cost
Maps, Navigation and Data Provider	• Map makers • Parking data providers • Real-time traffic info providers • Commercial information services • Data aggregators/analytics consultants	/ Functionality / Maintainability / Security (privacy) / Interoperability / Cost
C-ITS Service Provider	A private-sector entity which facilitates the C-ITS service by either setting up the required infrastructure in the absence of public infrastructure or the creation and upkeep of software in the absence of public software.	/ Functionality / Maintainability / Security (privacy) / Interoperability / Cost
Parking operator or Parking Service Provider	Can be both a Service Provider arranging reservation and/or payment in a parking space operated by itself or by a 3rd party. Can also be a traditional parking operator that does not facilitate C-ITS (e.g. payment with cash/bank card only)	/ Functionality / Maintainability / Security (privacy) / Interoperability / Cost
Public Transport Operator	Operates a fleet of public transport vehicles, trams, trains or other.	/ Functionality / Maintainability / Security (privacy) / Usability (Ease of use) / Reliability / Interoperability / Cost
Legal Authority		
Road Operator and **National/ Local Authority**	-Planners -Traffic management -infrastructure owners (tunnels, bridges) -maintainers - Local	/ Functionality / Maintainability / Security (privacy) / Interoperability / Usability (Ease of use) / Reliability / Cost
City or Municipality	Cities and municipalities.	/ Functionality / Maintainability / Security (privacy) / Interoperability / Usability (Ease of use) / Reliability

		/ Cost
European Commission	Providing vision & legal environment.	/ Functionality / Security (privacy) / Interoperability
Policy Advisor, **Consultancy,** **Public-Private Partnership**	Provide advice and consultancy for matters regarding policies and vision e.g. ERTICO [53], IRU [54], and FIA [55].	/ Functionality / Security (privacy) / Interoperability

Table 1: C-MobILE stakeholders and their concerns

2.2.1.2. Architecture Viewpoints and Views

In this section, we propose a set of six core viewpoints as part of the C-ITS architecture framework: Enterprise, Functional, Information, Implementation, Physical, and Communication. The relationships between views created using these viewpoints are shown in Figure 20. These viewpoints are defined based on the existing literature especially definitions from [14] and ITS reference architectures discussed in the previous sections. We believe that this set of viewpoints enable structured architectural descriptions for the C-ITS systems.

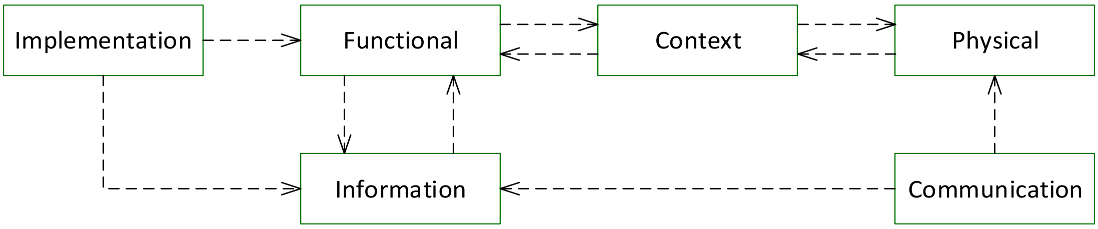


Figure 20: Relationships between C-ITS Architecture Views

Viewpoint	Definition	Respective View
Context	Describes the relationships, dependencies, and interactions between the system and its environment (people, systems, external entities interacting with the system).	A *context view* helps the system's stakeholders to understand system's responsibilities and how it relates to its organization.
Functional	Describes the system's runtime functional elements, their responsibilities, interfaces, and primary interactions.	A *functional view* helps the system's stakeholders understand the system structures and has an impact on the system's quality properties.
Communication	Describes the communications (e.g. interfaces, communication protocols) between different sub-systems deployed on different hardware environment.	A *communication view* supports stakeholders involved in defining/enabling communication between systems.
Information	Describes how the architecture stores, manages, and distributes data and information.	An *information view* provides high-level view of static data structure and information flow to users, developers, testers, and maintainers.
Implementation	Describes the implementation for realizing functionality into real life software systems.	An *implementation view* supports stakeholders involved in building, testing, maintaining, and enhancing the system.
Physical	Describes the physical environment where the system will be deployed and the dependencies that the system has on elements of it.	A *physical view* supports stakeholders involved in deploying, testing, and maintaining the system by capturing the hardware environment that the system needs, The technical environment requirements for each element, and the mapping of software elements to the runtime environment that will execute them.

Table 2: Viewpoint Definition

As the result of the architecture analysis and reverse architecting process, we identified that the DITCM reference architecture covers all the C-MobILE pre-selected services except the “Bundle1: urban efficiency” services. We have extracted the reference architecture from existing reference architectures, which was consistent with the DITCM reference architecture. Therefore, the C-MobILE reference architecture is adopted from the DITCM reference architecture with the additional changes to enable the Bundle 1 services for urban efficiency. The architecture descriptions have three levels, each one refining the previous one: Reference, Concrete, Implementation, and deployment site Architectures. To put the architecture framework and architecture description concepts in context, C-MobILE extends the conceptual model of the ISO/IEC/IEEE 42010 international standard for architecture descriptions of systems and software [12] and uses the proposed concept of architecture perspective for shaping the architecture views [14].

In the sections 2.2.2 to 2.2.7, we present the details for each viewpoint with a guideline to follow when extending the models for each view.

2.2.1.3. Architectural Perspectives

We use architectural perspectives to ensure that our architecture exhibit key software quality characteristics as illustrated in

Figure 19. In this section, we identify the key perspectives for large scale demonstration of C-ITS systems. The identified perspectives can be applied to the views. Additional quality characteristics and perspectives may be added in the descriptions of concrete and implementation architectures.

Perspectives								
		Interoperability	Security	Performance	Usability	Reliability	Availability	Adaptability
Views	Context						x	x
	Functional	Identify interoperable functions & Apply locate tactic	Identify vulnerable functions & Apply security policies	x	x			x
	Information	Determine syntax and semantics of data models to be exchanged	Information security (access control, access classes, object-level security) & Apply Information integrity constraints		x	x		x
	Implementation		Provide guidelines & constraints to developers to ensure security policy	x				x
	Physical	Mapping of software to hardware should take communication interoperability and other quality attributes into account	System’s packaging & deployment environment and hardware choices	x	x	x		
	Communication	Resource management needs to be investigated	ETSI security entity & Interface security	x				x

Table 3: Applying Perspectives to C-ITS Views

Architectural perspectives are used to formalize and guide the process of evaluating and reviewing the architectural models to ensure that the architecture satisfies the required quality characteristics and to select architectural tactics when it does not.

Perspectives								
Views		Interoperability	Security	Performance	Usability	Reliability	Availability	Adaptability
	Context						x	x
	Functional	Identify interoperable functions & Apply locate tactic	Identify vulnerable functions & Apply security policies	x	x			x
	Information	Determine syntax and semantics of data models to be exchanged	Information security (access control, access classes, object-level security) & Apply Information integrity constraints		x	x		x
	Implementation		Provide guidelines & constraints to developers to ensure security policy	x				x
	Physical	Mapping of software to hardware should take communication interoperability and other quality attributes into account	System's packaging & deployment environment and hardware choices	x	x	x		
	Communication	Resource management needs to be investigated	ETSI security entity & Interface security	x				x

Table 3 and summarize below the definitions of each perspective which are based on the international ISO/IEC 25010 standard [18].

/ Security is degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization.

/ Performance efficiency is performance relative to the amount of resources used under stated conditions.

/ Usability is degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

/ Reliability is degree to which a system, product or component performs specified functions under specified conditions for a specified period.

/ Availability is degree to which a system, product or component is operational and accessible when required for use.

- Adaptability is degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.

We also provide architectural tactics for the interoperability and security perspectives so that they could be of use as an inspiration for elaborating the relevant tactics for the concrete, implementation, and deployment site architectures. Defining the perspectives for C-MobILE architecture definition and eventually large-scale demonstration of C-ITS systems would help avoid expensive changes in the later stages of development, therefore need to be further elaborated in D3.2 and D3.4 when quality attributes are further elicited and prioritized.

2.2.1.3.1. Interoperability Perspective

One of the main objectives of C-MobILE is large-scale, real-life C-ITS deployments interoperable across Europe. Interoperability is degree to which two or more systems, products or components can exchange information and use the information that has been exchanged [18]. This definition implies both syntactic and semantic interoperability meaning the ability to exchange data but also the ability to correctly interpret the data that is being exchanged [14]. Below we highlight the main tactics to ensure interoperability between C-ITS services:

- In the functional view, it is determined which system responsibilities need to be interoperable with other systems. In addition, the locate tactic can be used to enable service discovery. A *service* can be located by type of service, name, location or other attributes to be found at runtime. MobiNET uses the 'discover service' tactic to enable interoperability between services. Orchestrate and tailor interface tactics [14] can be used to enable interoperability as well.
- In information view, the syntax and semantics of the main data models that need to be exchanged are determined. The syntax and semantics of the data models need to be consistent with the interoperable systems. If they data models are confidential, the proper transformations need to be made.
- Physical view addresses the mapping of software to hardware components/systems. The components that interact with external systems need to be ensured to have the proper communication and should take other quality attributes e.g. performance, availability and security into account.
- Communication view should cover resource management e.g. ensuring the interoperation with another system does not exhaust critical system resources. Resource load for the communication requirements remains acceptable. In addition, binding time to both known and unknown external systems need to be acceptable as well.

2.2.1.3.2. Security Perspective

For C-ITS, security is an essential part of the system design, therefore applying security perspective across multiple viewpoints will ensure the security across the C-ITS. Below it is elaborated how security perspective affects each view [14] and how main security principles could be leveraged as architectural tactics for ensuring security for C-ITS:

- In the functional view, it is identified which functional elements need to be protected. On the other hand, security policies may impact the functional structure as well. A security policy defines the set of security-related constraints that the system should be able to enforce.
- In the information view, it is identified which (sensitive) data needs to be protected. Information models can be modified as a result of security design. Information access policy in terms of different types of principles the system has (e.g. administrators, users, public authority) and for different type of information (vehicle information – e.g. location and speed, device information), and different type of access each group requires (e.g. only view the information, change it, share it, delete it). Information integrity constraints must be defined and determined if the communicated data needs to be signed or encrypted.
- In the implementation view, guidelines and constraints need to be provided to the developers to enable security policies. A security policy for the implementation view needs to define how the execution of certain sensitive system operations (e.g. system shutdown) will be controlled.
- In the physical view, it is identified which elements need to be packaged and deployed into one system as a result of security design. Security design has also impact on the system's deployment environment and hardware choices.
- In the communication view, the security entity of the ETSI communication reference architecture is applied. The security entity provides security services to the OSI communication protocol stack, to the security entity and to the management entity [2]. Its overview is shown in Figure 21.

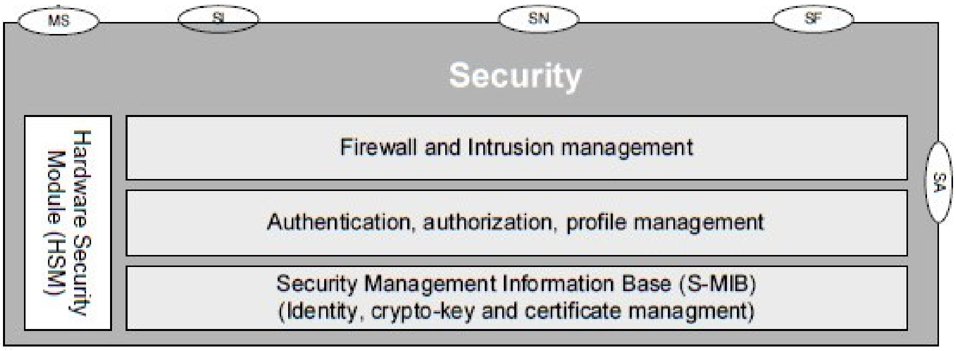


Figure 21: Security entity of the ETSI communication reference architecture [2]

In addition, the design choice needs to be made if a communication channel has to be secured e.g. by using TLS defined.

2.2.1.4. Architectural Representation

We propose to use Systems Modelling Language (SysML) diagram types to for architectural notations of the C-ITS architectures. The SysML is a general purpose modelling language for engineering systems and consists of structure diagram, requirement diagram, and behaviour diagram types as shown in Figure 22 [47].

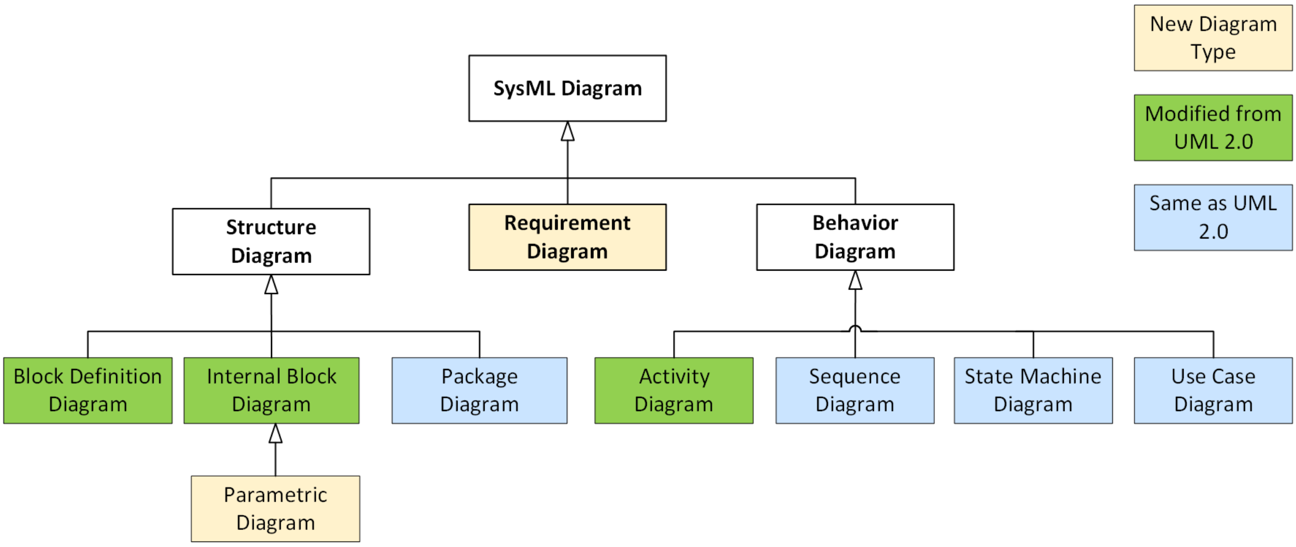


Figure 22: SysML Diagram Types

The SysML diagram types for each architectural viewpoint will be briefly presented in the later sections.

2.2.2. Context Viewpoint

2.2.2.1. Definition

The context viewpoint describes the relationships, dependencies, and interactions between the system and its environment (e.g. people, systems and external entities) [14]. The context view conforms to the context viewpoint and helps system's stakeholders (e.g. system/software architects, designers, developer and users) understand the system context.

An architect usually needs to include a definition of the system's context as part of their architectural description. The reasons for this include:

- the system context simply not being included in the requirements gathering exercise;
- a system context being loosely defined by requirements analysts, but at a level of detail which means that the architect needs to add significantly to it; and

/ the system/software architect needing to reference elements of the system context elsewhere in the architectural description, so making it desirable for this information to be part of the architectural description and under the control of the architect.

2.2.2.2. Stakeholders and Concerns

All systems exist in some larger environment, be it a department, an organisation's IT environment, a mobile communications system or even a virtual world. The context view aims to answer questions about this environment and specifically the technical relationships that the system being designed has with the various elements of this wider environment. The concerns that a context view addresses discussed below.

/ **System Scope and Responsibilities**

This concern defines system scope briefly and lists a high-level list of the systems' main responsibilities. The system requirements are elicited as part of the requirements analysis; thus this concern does not need to include complete requirements. In addition, some functional exclusion could be highlighted for clarity.

/ **Identity and Responsibilities of External Entities**

The key information that the context view must define is the set of external entities that the current system interacts with in some way, the reason for the interaction and the responsibilities that the external entities are assumed to fulfil in the context of this relationship. It is important to make sure that external entities that the system has irregular or occasional interactions with (e.g. systems that are only polled for data at the end of each month) are defined just as carefully as those which the system interacts with continually. Similarly, it is important to consider and carefully define external entities that rely on this system as well as those that this system relies on (it is very easy to worry about what we need while rather neglecting what others are expecting from us!) Also make sure that different types of external entities are considered, including systems supplying or consuming data, systems called as services, systems that call us as services, physical entities such as reports and files and human actors who need to interact with this system.

/ **External Interdependencies and Connections**

There are sometimes inter-dependencies between external entities that the system interacts with. An example could be where two systems have a data dependency between them that means that new data should always be sent to one of the systems, and acknowledged, before related data is sent to the other. These dependencies may be subtle and must be identified as part of this process.

/ **Expected External Interactions**

Having defined the external entities, the next concern is to decide or discover the nature of the connections with them. Connections can vary widely, from high volume messaging or RPC connections, through batch-oriented file or database interfaces, to manual connections involving human interaction or even document scanning. Some connections may need to be secured; some may need to implement very specific protocols. Defining and agreeing the fundamental characteristics of each connection allows the architect to start thinking about their practical implications and helps to identify gaps in knowledge and potential problems.

2.2.2.3. Context View

The context view conforms to the context viewpoint. SysML Block Definition Diagram (BDD) is identified as suitable modelling notation for capturing the context viewpoint. SysML Use Case diagram can be used to show the usage of a system. For the reference architecture, the use case diagram is too early to be defined, since the use case list is still being defined.

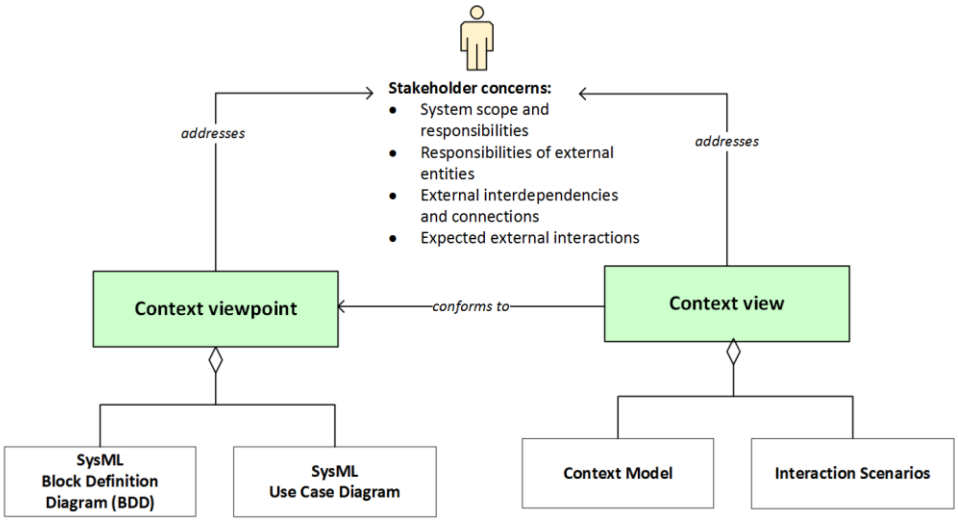


Figure 23: Context viewpoint and view

As illustrated in Figure 23, we define the context model to address the stakeholder concerns on the system scope and responsibilities, interdependencies and interactions.

2.2.2.4. Model kinds

SysML Block Definition Diagram and Use Case Diagram can be used for representing the context models. The context diagram is the key model within a context view, placing the system in its environment by relating it to the external actors that it interacts with via explicit relationships that represent the connections to and from it. A context diagram is usually quite simple and contains elements of the following types:

- System – the system being designed, which is treated as a “black box” with its internal structure hidden.
- External Entities – systems, people, groups and other entities that the system interacts with.
- Connections – the interfaces, protocols, and connectors that link the external entities and the system being designed or utilized.

2.2.2.4.1. Context Model

The notations that we commonly see used for context diagrams are SysML Block Definition Diagram. C-MobILE consists of five main systems which is depicted as black box and corresponding actors’ connections with those systems is shown in Figure 24 below.

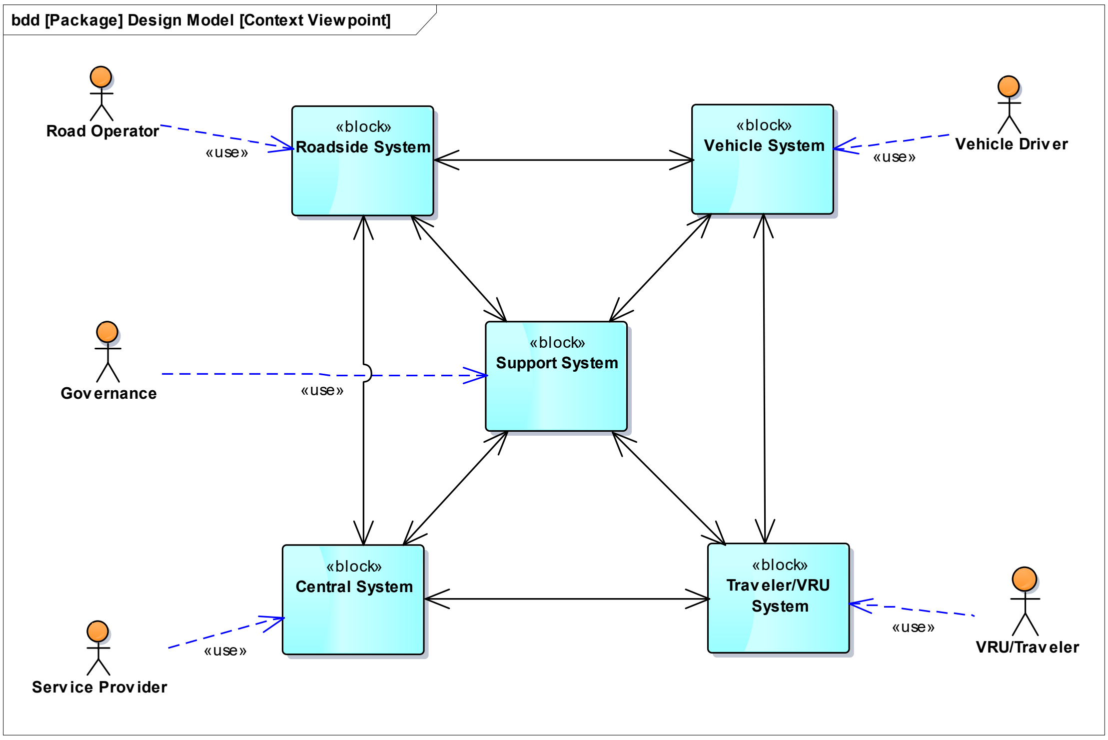


Figure 24: Context model

These five main systems of the C-MobILE architecture are aligned with the five layers of the DITCM reference architecture [48]:

- *Support System*: Comprise of sub-systems performing various tasks e.g.: governance, test and certification management, security and credentials management.
- *Central System*: Comprise of sub-systems to support connected vehicles, field and mobile devices. The sub-systems can be aggregated together or geographical or functionally distributed.
- *Roadside System*: Comprise of sub-systems which covers the ITS infrastructure on or along physical road infrastructure, e.g.: roadside units, signal/lane control etc.
- *Vehicle System*: Comprise of sub-systems which are integrated within vehicle such on-board systems (advanced driver assistance / safety systems, navigation, remote data collection or information).
- *Traveller/VRU System*: Comprise of both personal devices (e.g.: mobile devices, navigations devices) and specific systems connected to vehicles of VRU's (e.g.: tags).

(Human) actors are treated as external entities that interact with the systems:

- *Vehicle Driver*: An actor driving in a vehicle. The vehicle is a motorized vehicle (car, bus, truck) and not a vehicle of a vulnerable road user (bike, moped, motor). An actor in this category is directly concerned with Vehicle System as shown in Figure 24 through various vehicle related interfaces like : OBU , HMI etc.
- *Vulnerable Road User*: A VRU is a human actor like a pedestrian, cyclist or PTW driver; A motorcyclist is also an example of a PTW and is treated as a vulnerable road user in specific road hazard situations with other cars. An actor in this category is directly concerned with Traveller/VRU System as shown in Figure 24 through various interfaces like HMI, tablet, mobile, etc.
- *Road Operator*: An actor responsible for the traffic management of a road network. An actor under this category is directly concerned with Roadside System through various communication channels and is responsible for collecting and evaluating data related to roadside information.
- *Service Provider*: An actor (organization) supplying services to one or more customers. Customers are either other organizations, including government (B2B / B2G / G2B / G2G) or end users (B2C / G2C). An actor under this category is directly concerned with Central System which also is responsible providing various services. Typical examples of a Service Provider are a Navigation Provider as a Service Provider providing navigation services to end users or organizations or a Traffic Information Provider as a Service Provider that provides road traffic related information, like traffic jams, incidents, road works warning etc.
- *Governance*: An actor under this category is directly concerned with Support System whose responsibility is to support various other sub-systems such as legal authorities, test and certification management, security and credentials management etc.

2.2.2.4.2. Interaction Scenarios

The expected interactions between the system and the external entities can be described in the context diagram to identify design constraints and un-elicited requirements. When the system usage is unclear or conflicting requirements are identified, it can be useful to make interaction scenarios. SysML Use Case Diagram can be used to give a visual overview of the functionalities provided by a system in terms of actors, their goals (i.e. use cases), and any dependencies among the use case.

2.2.2.5. Correspondence rules

The context viewpoint has correspondences with functional and physical viewpoints as highlighted in Figure 25.

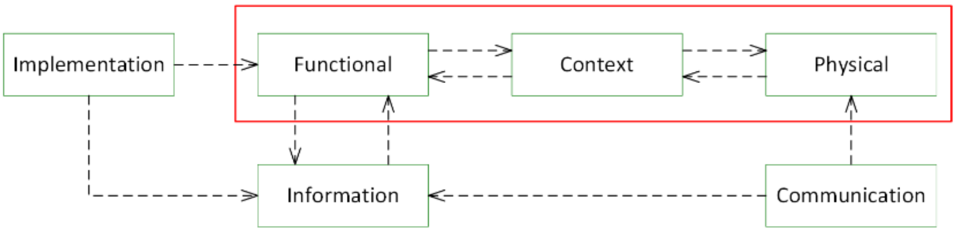


Figure 25: Correspondences for the Context Viewpoint

Functional and physical viewpoints have conformance correspondence to the context viewpoint.

2.2.3. Functional Viewpoint

2.2.3.1. Definition

We define the concepts for the functional viewpoints, which can be used for modelling functional structures for different type of architectures. Functional viewpoint describes the system's runtime functional elements, their responsibilities, interfaces, and primary interactions. The functional view conforms to the functional viewpoint, helps the system's stakeholders understand the system structures, and has an impact on the system's quality properties.

2.2.3.2. Stakeholders and concerns

All stakeholders (particularly system architects, developers and integrators) use the functional viewpoint as it is usually easy to understand and describes the system's functional structure. The functional viewpoint addresses the following concerns of the stakeholders.

/ Functional capabilities:

Functional capabilities describe the functionality that the system is required to provide. In the Architecture Viewpoint for the reference architecture, it defines what the system will explicitly do. The set of functional and quality requirements will be used to define the functionality.

/ External interfaces:

External interfaces address the interactions between systems e.g. based on data/control flow or events. A system can send or receive data either because of an internal state change or a state change in another system. A system can send or receive a request to perform a task or notify that something has been occurred. In the functional view of the reference architecture, high-level generic interfaces are described. The interface syntax and semantics in further detail will be described in the concrete and implementation architectures.

/ Internal structure:

A system can be further decomposed into sub-systems or components to meet its requirements. Its decomposition has an impact on the quality attributes e.g. on security, scalability, reliability, and availability. Therefore, the definition of the internal structure should be taken both functional and quality requirements into account. In the functional view of the reference architecture, a system is further decomposed into sub-systems, which can be further decomposed into functional components in concrete/implementation architectures.

2.2.3.3. Functional view

As presented in Section 2.2.1.2, an architecture description includes one Architecture View for each Architecture Viewpoint. Thus, the functional view conforms to the Functional Viewpoint. SysML Block Definition Diagram and Internal Block Definition Diagram are identified as suitable modelling notations for capturing the functional viewpoint.

As illustrated in Figure 26, we define *functional structure model* to address the stakeholder concerns for functional capabilities and external interfaces and *functional internal structure model* to address the internal structure of the element. SysML BDD and IBD can be both used to model the functional structure and the internal structure.

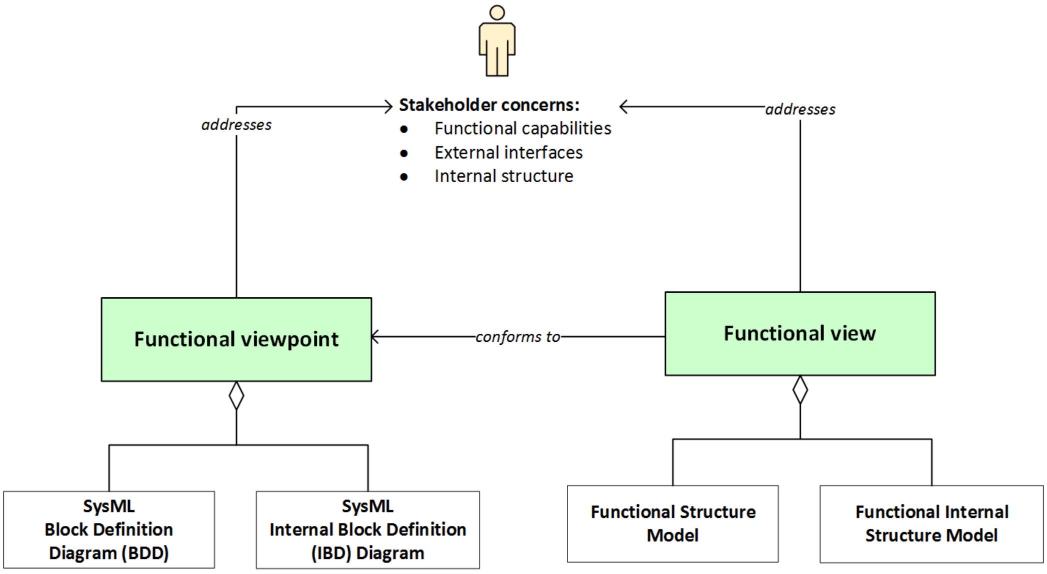


Figure 26. Functional viewpoint and view

The structure of a system is captured in functional structure models using SysML BDD by categorizing into systems and decomposing a system into sub-systems. A system defines the functionality and functional data flow interfaces between systems that are required to support a particular ITS application.

2.2.3.4. Model Kinds

Below we describe SysML block definition diagram and internal block diagram, which are used for capturing the models for functional structure and internal structure of the system. The Block Definition Diagram and Internal Block Diagram are part of the structure diagram.

2.2.3.4.1. Functional Structure Modelling

The SysML Block Definition Diagram provides a black box representation of a system block. In SysML, BDD is the replacement of the UML 2.0 class diagram by replacing classes with blocks, which can be of any type including software, hardware. For representing the functional structure model, blocks, their contents and relationships are shown using the BDD.

The following BDD concepts are used for modelling the functional structure of the block/system:

- Block is a modular unit of system structure that encapsulates its contents [47] which we use to represent a system in the context of C-ITS reference architecture. A system is further decomposed into sub-systems or functional components. A block can both provide and require Interfaces for both information and physical flows.
- A relationship between blocks can be represented by a composition (“has a” relationship) with a solid diamond or a reference with an open diamond.
- The flow port is a new definition from SysML. It represents what can go through a block in and/or out (e.g. data, energy), which will be of use in concrete and implementation architectures.

Functional viewpoint describes the system’s runtime functional elements, their responsibilities, interfaces, and primary interactions. The functional view conforms to the functional viewpoint, helps the system’s stakeholders understand the system structures, and has an impact on the system’s quality properties. The system structure is captured in functional models using SysML block definition diagram (BDD) and by categorizing into systems and decomposing a system into sub-systems. A system defines the functionality and functional data flow interfaces between systems that are required to support a particular ITS application. Information flows depict the exchange of information between sub-systems. Figure 27 shows the high-level functional architectural model for the C-MobILE applications.

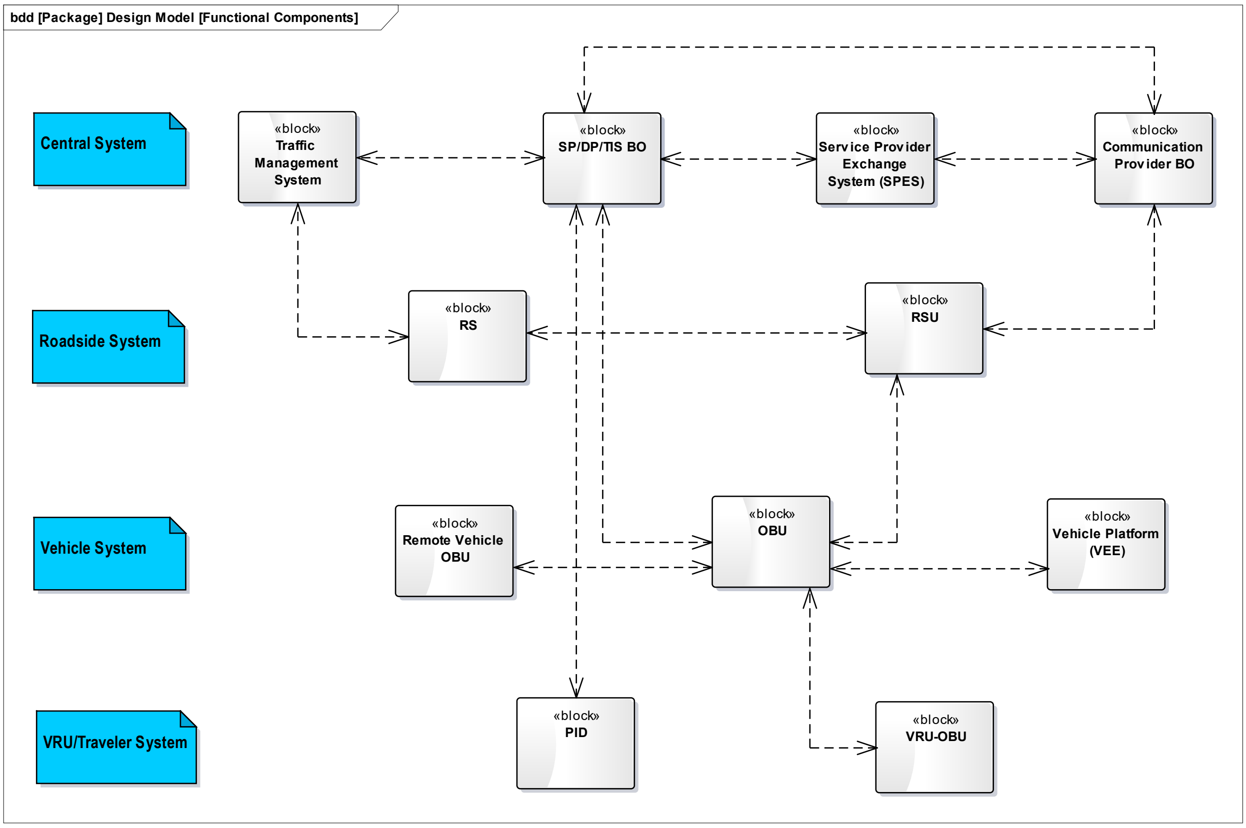


Figure 27: High-level functional model of the C-ITS systems for C-MobILE

The main functions of the systems are sensing, communication, situation monitoring and assessment, and acting and trust management. The hierarchic decomposition of these functions is based on geometrical and temporal scale of information and information abstraction. Cardinality (multiple entities with the same functionality) of the system is supported and dependent on physical limitations of sensors and actuators and heterogeneity of goals.

2.2.3.4.1.1. Central System

In Figure 28, the highest-level functional structure of the Central System is illustrated. The Central System consists of the following main sub-systems which will be further refined in the concrete architecture by defining its functional components and interfaces between them: TMS, SP/DP/TIS, CP, SPES and IIS.

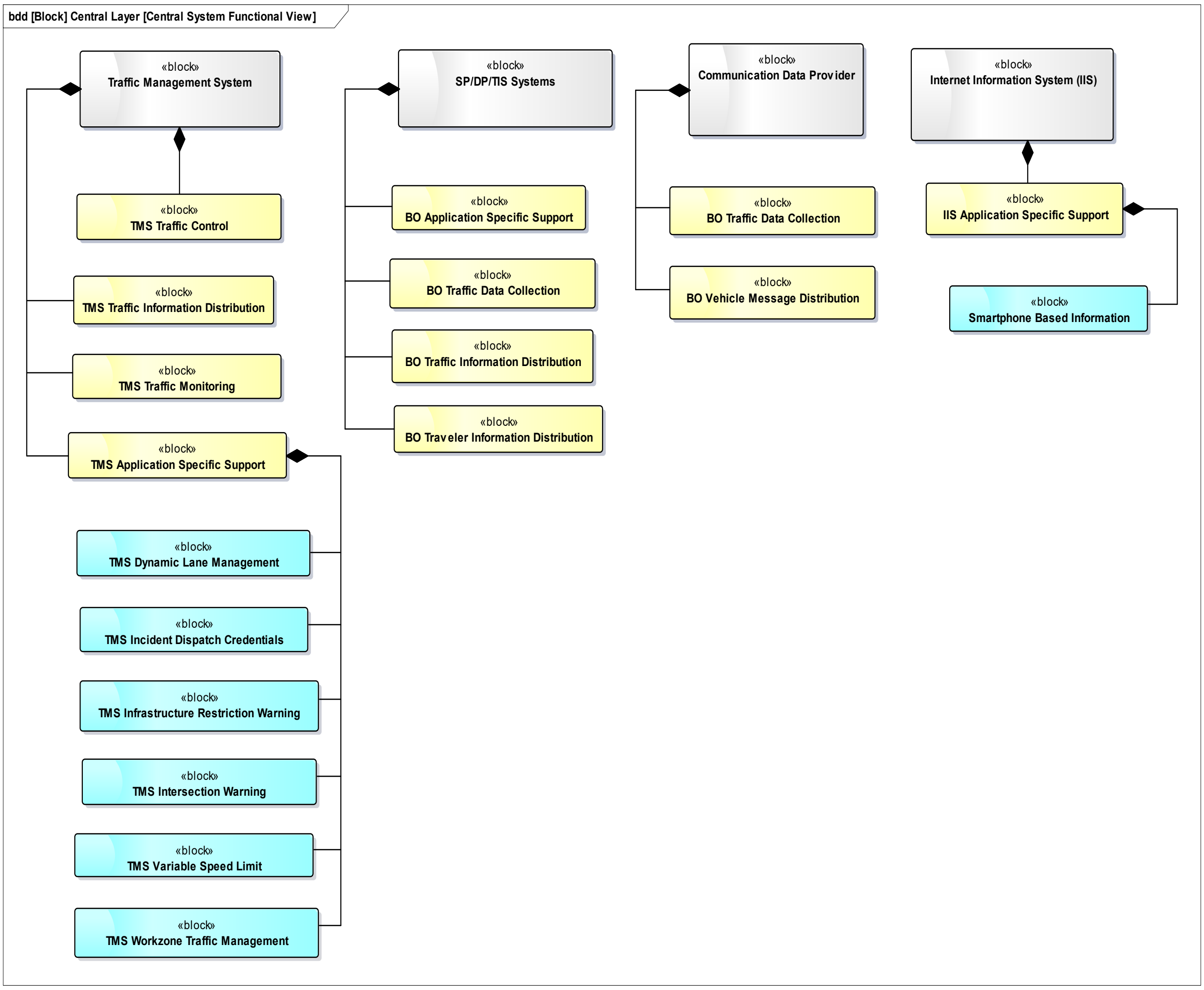


Figure 28: High-level functional model of the Central System

System	Subsystem	C-MobILE Application	Description
TMS	TMS Traffic Monitoring	Road Works Warning, Road Hazard Warning	Remotely monitors traffic sensors and surveillance equipment (cameras), and collects, processes and stores the collected traffic data.
	TMS Traffic Control	Green Light Optimal Speed Advisory (GLOSA)	Controls driver information system field equipment including dynamic message signs, managing dissemination of driver information through these systems
	TMS Traffic Information Distribution	Navigation related services	Disseminates traffic and road conditions, dynamic speed limits, closure and detour information, incident information, driver advisories, and other traffic-related data to other centres, the media, and driver information systems
	TMS Intersection Safety	Signal violation warning Warning system for pedestrian	Controls and monitors Roadside Units (RSUs) that support stop sign, red light, and pedestrian crossing violations. Configures the RSUs for the current intersection geometry and traffic signal control equipment at the intersection
	TMS In-Vehicle Signing Management	In-Vehicle signage	Sign information that may include static regulatory, service, and directional sign information as well as variable information such as traffic and road conditions can be

			provided to the RSU, which uses short range communications to send the information to in-vehicle equipment
SP/DP/TIS	Back-Office (BO) Traffic Data Collection	Probe Vehicle Data	Current traffic information and other real-time transportation information are collected from several sources like TMS, and connected vehicles
	BO Traffic Information Distribution	Navigation related services	Disseminates traffic and road conditions, closure and detour information, incident information, driver advisories, and other traffic-related data to other centers and the media (e.g. radio, Service Providers).
	BO Traveller Information Distribution	Navigation related services	Disseminates traveller information including event information, transit information, parking information and weather information.
	BO Application Specific Support	Motorway/Urban Parking	Disseminates traveller information including urban and motorway parking information.
Communication Provider	BO Traffic Data Collection (from RSU Traffic and situation monitoring)	V2I applications with RSU	Current traffic flow information and other real-time information are collected from equipped cooperative vehicles passing the roadside station of the communication provider.
	BO Vehicle Message Distribution	I2V applications with RSU	Receives information including traffic and road conditions, incident information, maintenance and construction information, event information, transit information, parking information, and weather information.
SPES	Service Directory (SD)		Provides basis capabilities to manage and search service descriptions
	Identity Manager (IM)		Provides capabilities to manage common identities and to handle all security and privacy related concerns
	Billing		Support system that handles all financial transactions and provides a neutral instance which monitors the transactions between different parties.
IIS	IIS Application Specific	V2I, VRU specific services	A VRU or Vehicle Connected System can request for specific information or send information to the IIS

Table 4: Central Sub-systems Functional Descriptions

2.2.3.4.1.2. Roadside System

In Figure 29, the highest-level functional structure of the Roadside System is illustrated. The Roadside System consists of the following main sub-systems which will be further refined in the concrete architecture by defining its functional components and interfaces between them: Roadside and Roadside Units.

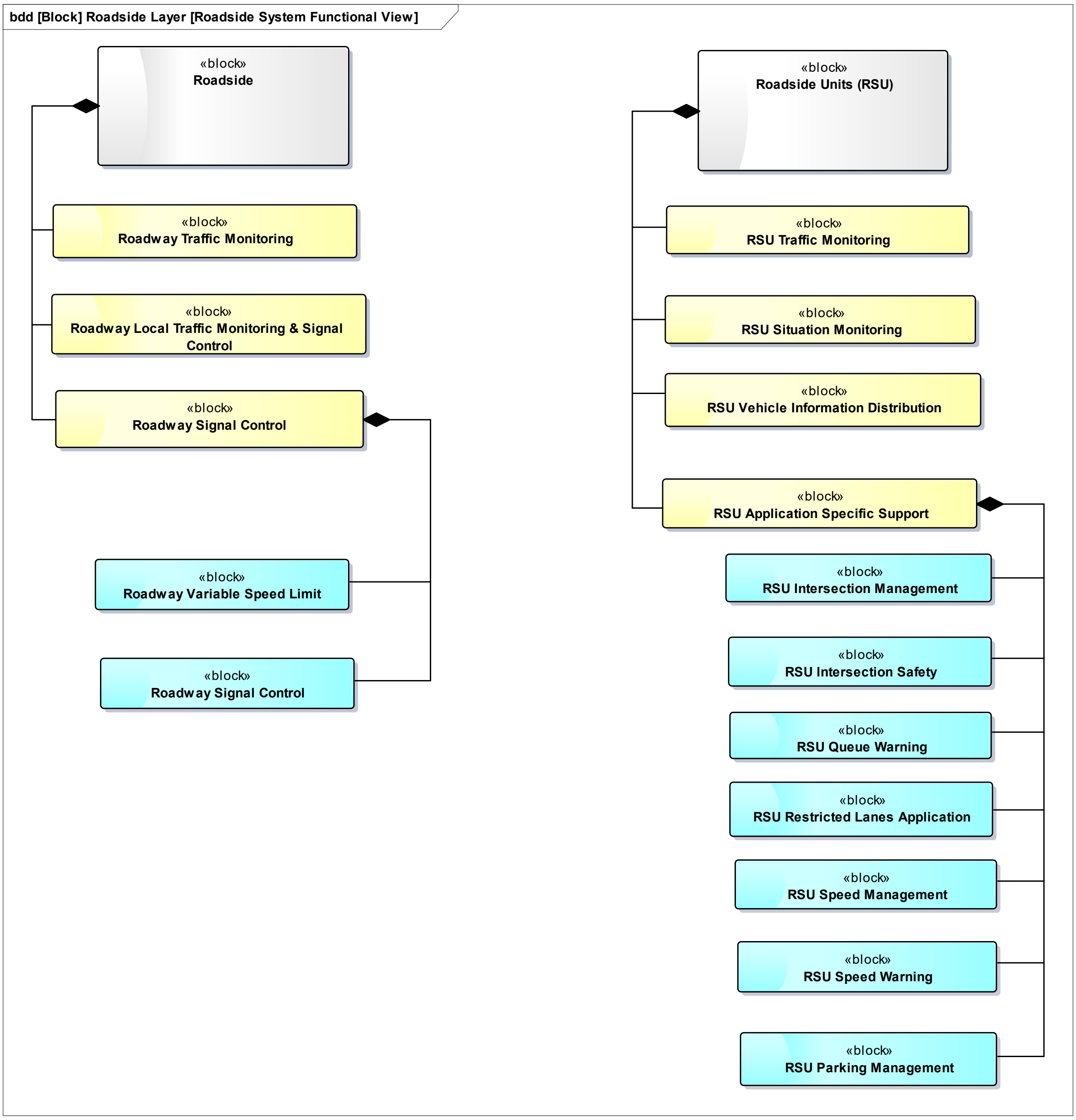


Figure 29: High-level functional model of the Roadside System

System	Subsystem	C-MobILE Application	Description
RSU	RSU Traffic Monitoring	V2I applications via V2V monitoring	Vehicle V2V safety messages that are shared between connected vehicles and distils this data into traffic flow measures that can be used to manage the network in combination with or in lieu of traffic data collected by infrastructure-based sensors. Also supports incident detection by monitoring for changes in speed and vehicle control events that indicate a potential incident
	RSU Situation Monitoring	Probe Vehicle Data	This object collects current status information from local field devices including intersection status, sensor data, and signage data, providing complete, configurable monitoring of the situation for the local transportation system in the vicinity of the RSU.
	RSU Vehicle Message Distribution	I2V applications with RSU	Receives information from the CP BO. Location-specific or situation-relevant information is sent to short range communications transceivers at the roadside

	RSU Intersection Management		It communicates with approaching vehicles and ITS infrastructure (e.g., the traffic signal controller) to enhance traffic signal operations.
	RSU Intersection Safety	Signal Violation Warning, Warning system for pedestrian	It communicates with approaching vehicles and ITS infrastructure to alert and warn drivers of potential stop sign, red light, and pedestrian crossing conflicts or violations.
	RSU Queue Warning	V2I communications	It monitors connected vehicles to identify and monitor queues in real-time and provides information to vehicles about upcoming queues, including downstream queues that are reported by the Traffic Management System
	RSU Speed Management	Slow or Stationary Vehicle Warning, Motorcycle approaching indication	Provides infrastructure information including road grade, roadway geometry, road weather information, and current speed limits to assist vehicles in maintaining safe speeds and headways.
	RSU Speed Warning		This application object works in conjunction with the 'Roadway Speed Monitoring and Warning' application object, which uses traditional ITS field equipment to warn non-equipped vehicles.
	RSU Parking Management	Urban/Motorway Parking	Monitors the basic safety messages generated by connected vehicles to detect vehicles parking and maintain and report spaces that are occupied by connected vehicles.
RS	Roadway Traffic Monitoring	Incident warning , Traffic Jam ahead	Monitors traffic conditions using fixed equipment such as loop detectors and cameras.
	Roadway Signal Control	GLOSA, In-Vehicle Signage	Monitor and control signalized intersections/ramps and dynamic roadway signs
	Roadway local traffic monitoring and control distribution	GLOSA, In-Vehicle Signage	Receive information from the Roadway Traffic Monitoring and send this information via a RSU to vehicles or BO systems.

Table 5: Roadside Sub-systems Functional Description

2.2.3.4.1.3. Vehicle System

In Figure 30, the highest-level functional structure of the Vehicle System is illustrated. The Vehicle System consists of the following main sub-systems which will be further refined in the concrete architecture by defining its functional components and interfaces between them: Vehicle Electrical & Electronic System and On-Board Unit.

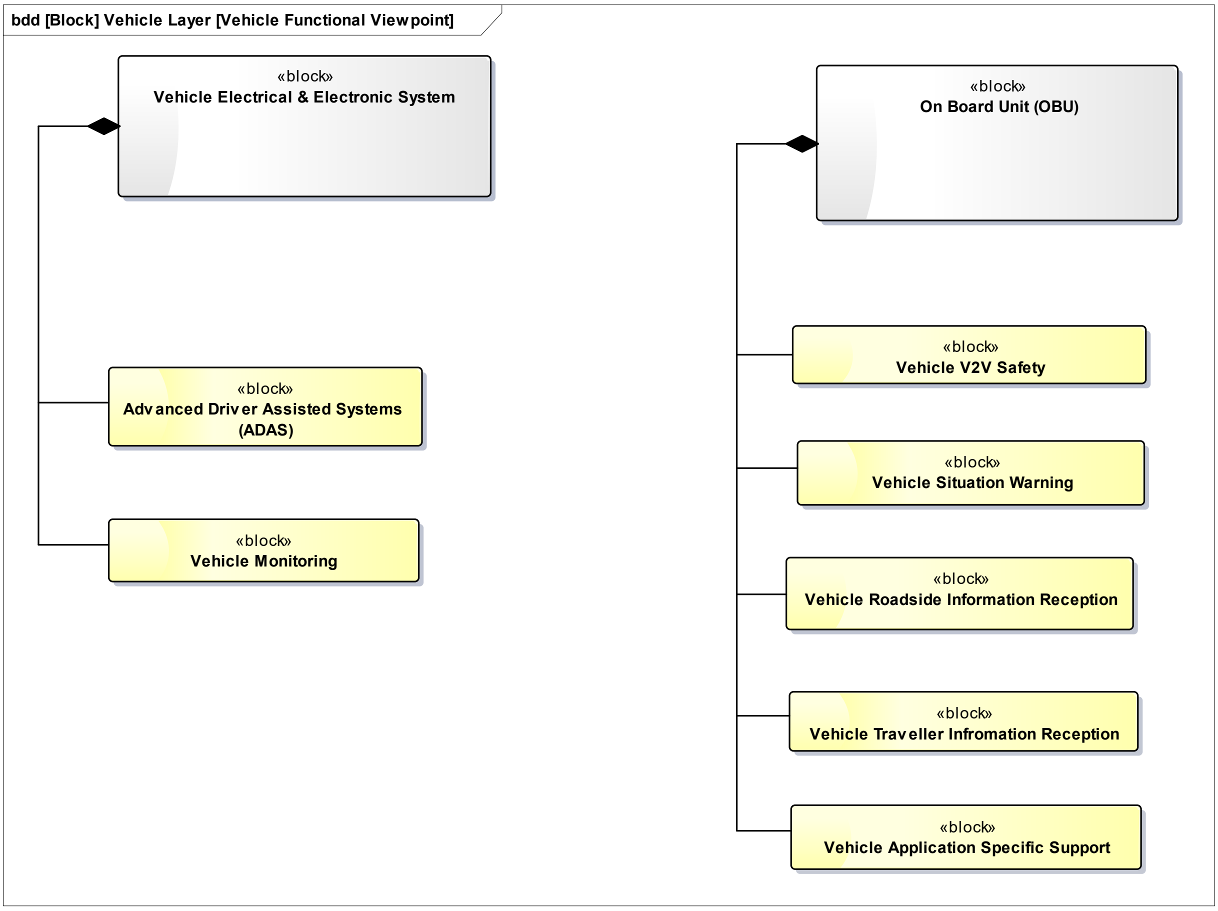


Figure 30: Vehicle functionality decomposition

System	Subsystem	C-MobILE Application	Description
OBU/ RV-OBU	Vehicle V2V Safety	Road Works Warning, Road Hazard Warning, Emergency Vehicle Warning	Exchange current vehicle location and motion information with other vehicles in the vicinity. The information is used to calculate vehicle paths, and warns the driver when the potential for an impending collision is detected.
	Vehicle Situation Monitoring		Collect traffic data and environmental situation data from on-board sensors and systems related to environmental conditions and sends the collected data to the infrastructure (V2I) as the vehicle travels.
	Vehicle Roadside Information Reception	I2V applications with RSU	Information presented may include fixed sign information, traffic control device status (e.g., signal phase and timing data), advisory and detour information, warnings of adverse road and weather conditions, travel times, and other driver information.
	Vehicle Traveller Information Reception	I2V applications with SP BO Motorway/Urban Parking	General traveller information including traffic and road conditions, incident information, maintenance and construction information, event information, transit information, parking information, weather information, and broadcast alerts.
	Vehicle Application Specific Support	Cooperative cruise control	Representation of the functionality required in the vehicle to execute a specific application e.g. cooperative adaptive cruise control, rerouting etc.
Vehicle Electrical and Electronic system (VEE)	Advanced Driver Assisted Systems (ADAS)	Cruise control	Vendor-specific assistance systems to increase safety and comfort of the driver. Examples are lane departure warning, automatic emergency brake, and advanced cruise control.
	Vehicle Monitoring		Access to vehicle-specific sensor and actuator information systems of the vehicle

Table 6: Vehicle Sub-systems Functional Description

2.2.3.4.1.4. Traveller/VRU System

In Figure 31, the highest-level functional structure of the Traveller/VRU System is illustrated. The Traveller/VRU System consists of the following main sub-systems which will be further refined in the concrete architecture by defining its functional components and interfaces between them: Personal Information Devices.

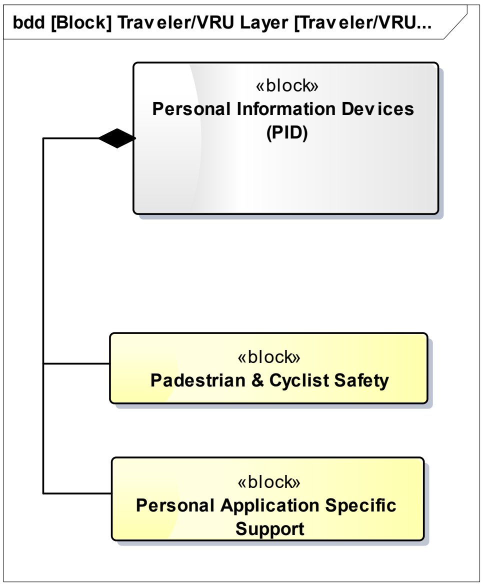


Figure 31: Block Definition Diagram for VRU Functions

System	Subsystem	C-MobILE Application	Description
PID	Personal Pedestrian and Cyclist Safety	All VRU applications	Providing pedestrian and cyclist location information to the infrastructure that can be used to avoid collisions involving pedestrians/cyclists.
	Personal Application Specific Support	Navigation related applications	Personal Interactive Traveller Information provides traffic information, road conditions, transit information, yellow pages (traveller services) information, special event information, and other traveller information that is specifically tailored based on the traveller's request and/or previously submitted traveller profile information.

Table 7: Traveller/VRU Sub-systems Functional Description

2.2.3.4.2. Functional Internal Structure Modelling

The SysML Internal Block Definition Diagram provides an internal or white box representation of a system block. UML 2.0 composite structure diagram, the SysML IBD redefines the composite structure diagram by supporting blocks and flow ports. BDD can be used in combination with IBD i.e. functional structure of the system is represented as trees of modular systems/sub-systems, which further refined into the representation of final assembly of all blocks/systems. Blocks that can be further decomposed into IBD, are called composite blocks.

The following IBD concepts are used for modelling the internal structure of a block/system:

/ BDD composite blocks are further decomposed into sub-systems or functional components (which are usually called in IBD as *parts*). Block or system that is further decomposed into sub-systems or functional components are connected via standard ports with exposed interfaces and/or flow ports.

/ The item flow is a new definition from SysML as well. It represents the things that flow between blocks/systems and/or sub-systems across their connectors, which will be of use in implementation architecture.

2.2.3.5. Correspondence rules

The functional viewpoint has correspondences with context, implementation, and information viewpoints as illustrated in Figure 32.

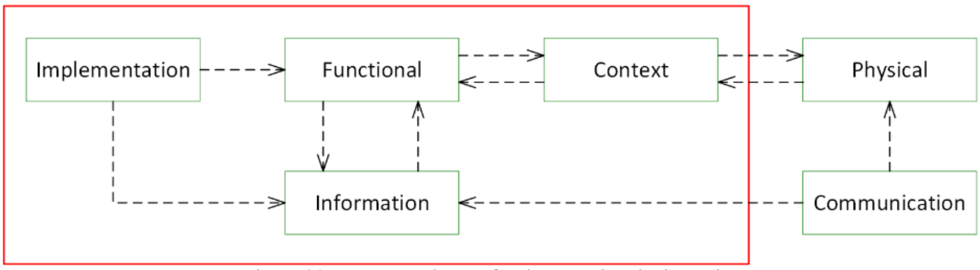


Figure 32: Correspondences for the Functional Viewpoint

Functional viewpoint refines the context, information, and implementation viewpoints needs to conform to the functional viewpoint.

2.2.4. Communication Viewpoint

2.2.4.1. Definition

Communication viewpoint describes the mode of communication through network interfaces and communication protocols between different systems deployed on different hardware environment. The communication view supports stakeholders involved in defining/enabling communication between systems and shows the interfaces between systems and sub-systems. The communication architecture for C-MobILE conforms to the general communications reference architecture defined in ETSI EN 302 665 which is illustrated in Figure 35.

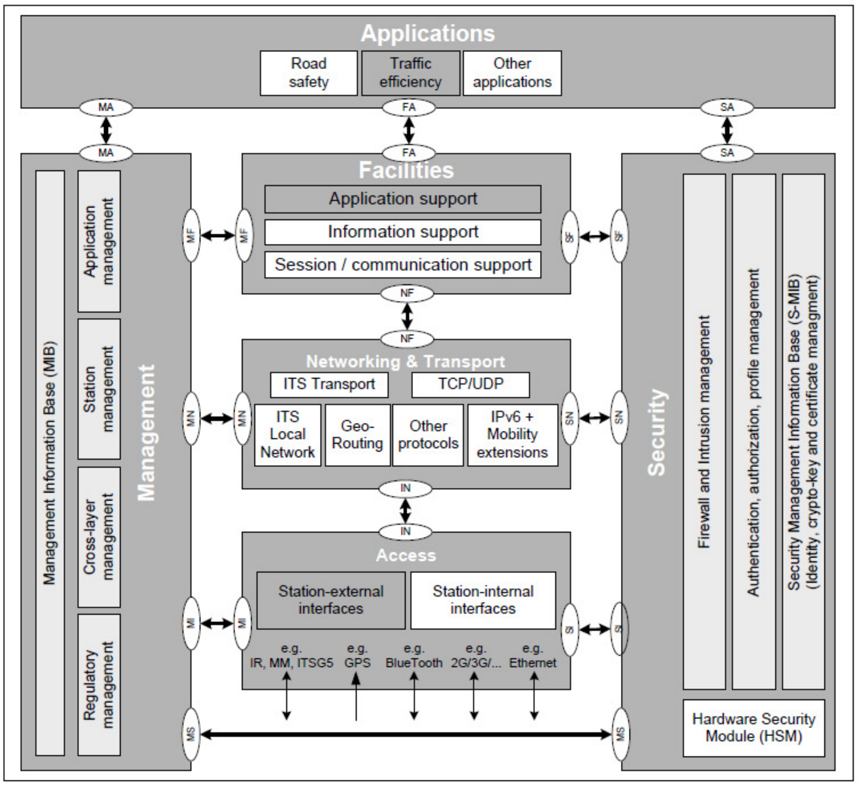


Figure 33: ITS station reference architecture [2]

The reference communication architecture for C-ITS stations consists of four main functional domains namely applications, facilities, network & transport, and access and two support domains (security and management) [2]. This reference communication architecture is valid for all ITS systems, i.e. OBU, RSU and BO systems which are respectively named vehicle ITS, roadside ITS and central ITS in the ETSI definitions.

The ETSI communication reference architecture defines six generic entities [2]:

9. Applications (re)present the ITS-S applications making use of the ITS-S services to connect to one or more other ITS-S applications. An association of two or more complementary ITS-S applications constitutes an ITS application which provides an ITS service to a user of ITS.

10. Facilities represents ITSC's communication specifications at OSI layers 5, 6 and 7, e.g. cooperative awareness basic service (for CAM, ETSI EN 302 637-2), decentralized environmental notification basic service (for DENM, ETSI EN 302 637-2) and location dynamic map (LDM, ETSI EN 302 895).
11. Networking & transport represents ITSC's communication specifications at OSI layers 3 and 4, e.g. GeoNetworking, IPv6 over GeoNetworking and IPv6 with mobility extensions. To connect to systems via other protocols (e.g. IPv4) a gateway is needed.
12. Access represents ITSC's communication specifications at OSI layers 1 and 2, e.g. on 5.9 GHz spectrum usage, Decentralized Congestion Control (DCC) and coexistence of ITS and EFC (CEN DSRC) services in the 5.8 GHz and 5.9 GHz bands.
13. Management responsible for managing communications in the ITS station. This entity grants access to the Management Information Base (MIB).
14. Security provides security services to the OSI communication protocol stack, to the security entity and to the management entity. "Security" can also be considered as a specific part of the management entity.

2.2.4.2. Stakeholders and Concerns

Most of the stakeholders have some level of interest in communication viewpoint however system architects, data modellers, network administrators, network managers, hardware managers, integrators are the main stakeholders. Concerns of these stakeholders are shown below Figure 34.

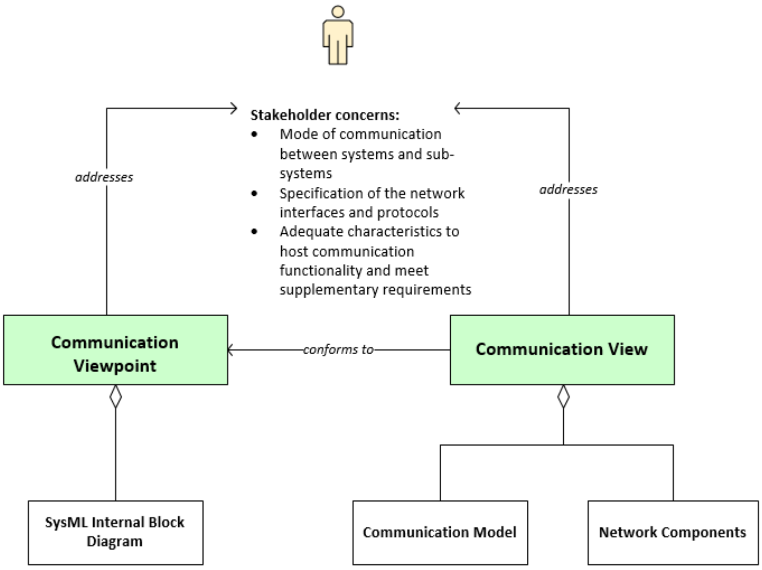


Figure 34: Communication Viewpoint and View

2.2.4.3. Communication View

In real-world deployments, the functional systems at one of the four layers (i.e. VRU, vehicle, roadside or central layer), can be deployed in one physical box. However, in case the involved functional systems are deployed in separate physical elements a communication network is needed to interconnect the functional systems. A communication network is needed for the communication between systems at the different layers as well.

The Communication Viewpoint can be mapped to the ISO's Open System Interconnection model as shown in Figure 35 below.

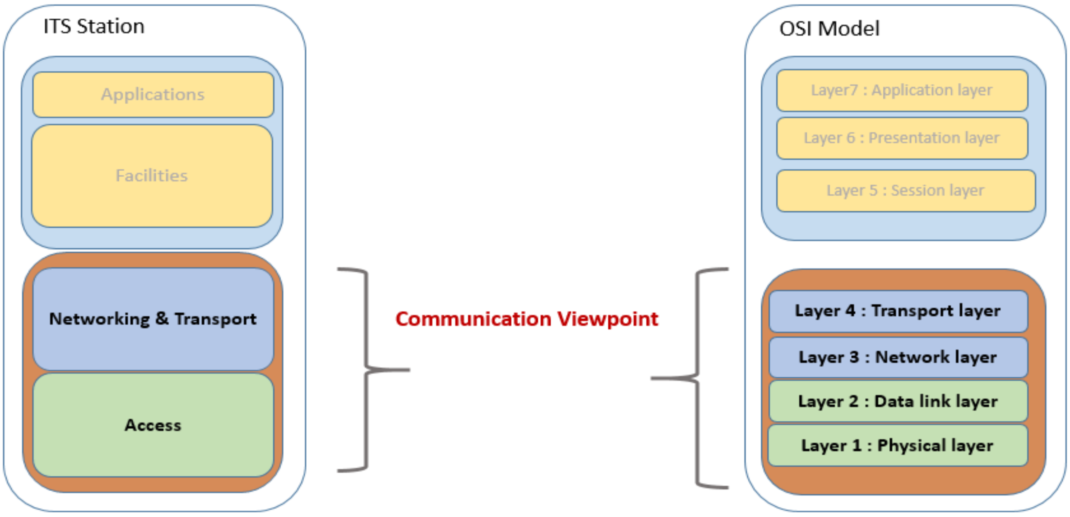


Figure 35: Communication viewpoint mapping of ITS Station and OSI Model

The following networks are identified from communication viewpoint perspective by considering VRUITS architecture [8]:

/ Cooperative ad-hoc networks: best suited for cooperative applications. ITS-G5 with GeoNetworking is used in these networks for VRU2VRU, VRU2V/VRU2I and V2IVRU/I2VRU communication to exchange CAM, DENM and other C-ITS defined messages between cooperative systems.

/ In-vehicle networks for cars and VRU vehicles like PTW three types are defined:

/ Car-specific networks. A serial bus is currently used in the automotive industry to allow microcontrollers and devices to communicate with each other within a car without a host computer. This type of network can be based on CAN, MOST or FlexRay. CAN (Controller Area Network) is one (out of five) message-based protocols within OBD-II and is standardized at the lower layers (physical, data link, transfer layer). Recent network protocols like MOST (Media Oriented Systems Transport) is a high-speed multimedia network technology optimized by the automotive industry which can be used for applications insider or outside the car and FlexRay as successor for CAN. However, FlexRay is not yet widely adopted. EOBD is an EU standard providing diagnostic and reporting capabilities, based on OBD-II (On-Board Diagnostics, release II).

/ VRU-vehicle specific networks. For motorcycles and for other VRU-specific vehicles like mopeds and eBikes such networks with (partly) standardized interfaces are not yet available. Motorcycle vendors also have a proprietary implementation of an OBD-II type of network. Another example of a VRU-vehicle specific network is EnergyBus. It is an open standard for integration of and communication between electric components of light electric vehicles based on DC. The EnergyBus specification is published through the EnergyBus Association, based in Germany.

/ In-vehicle IP networks. This IP network is used to interconnect in-vehicle systems for advanced driver assistance, comfort, and infotainment features. This network is used to connect devices (e.g. smartphone, communication unit) that contain one or more systems like VRU-VIS, VRU CS with HMI. This type of IP-based network can use widespread lower layer technologies like Wi-Fi, Bluetooth as lower layer protocols. Automotive Ethernet is a more recent industry standard for in-car IP networks, developed by the OPEN (one-pair ether-net) alliance special interest group (SIG). Powered VRU-vehicles like eBikes with on-board computers have USB interfaces to connect external systems, (e.g. a smartphone for charging or an external diagnostics system for battery health monitoring) or to an external computer to read in-formation on trips (distance, average speed, etc.). These device-to-device network connections (based on USB or Bluetooth) could be used to connect different systems on powered VRU-vehicles.

/ Public mobile data networks. VRU systems and in-vehicle systems can be connected to central systems via public mobile data networks. These networks are IP-based and use different mobile radio access technologies like GPRS, UMTS, and LTE. ITS systems are mainly the only users on these networks, and mobile operators own these networks and licenses and are responsible for performance and capacity.

/ Other networks:

/ Internet. The central systems in the architecture can be connected via a public IP network.

/ Private IP networks: At the roadside layer, the systems are mostly connected via private IP networks, including the connections to central TMC.

/ Other short-range wireless networks: systems at the different layers can be connected via other short-range wireless technologies like RF, Bluetooth, BLE or Wi-Fi. IP can be used to exchange information. In some cases, only the wireless MAC identifier and signal strength are used to identify and locate a user. In addition, Bluetooth, BLE, and Wi-Fi can be used to exchange information between components installed in the VRU vehicle and nomadic devices.

2.2.4.4. Model kinds and Models

Communication model is considered which shows the mode of communication in terms of network interfaces and protocols. SysML Internal Block Diagram is considered to model the structure of these interfaces and protocols as well as the connection between different networks which will be included during Concrete Architecture D3.2

2.2.4.5. Correspondence rules

The context viewpoint has correspondences with information and physical viewpoints as highlighted in Figure 36.

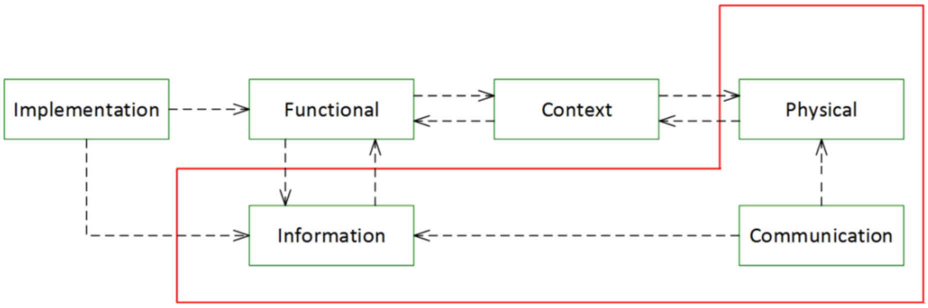


Figure 36: Correspondences for the Communication Viewpoint

Physical and information viewpoints have conformance correspondence to the Communication viewpoint.

2.2.5. Information Viewpoint

2.2.5.1. Definition

The information viewpoint and view at architectural level help define how the systems will store, manage, manipulate, and distribute information [14]. The information view provides high-level view of static data structure and information flow to users, developers, testers, and maintainers. In this section, the main stakeholder concerns, model kinds and models such as data flow (information exchange, protocol message types) are explained.

2.2.5.2. Stakeholders and Concerns

Although most of the stakeholders have some level of interest in the information viewpoint, users, architects, data modellers, developers, and integrators are the main stakeholders. The information viewpoint addresses the following list of stakeholder concerns.

/ Information structure and content:

It is important to define the structure and content of the information that C-ITS manages. An architect needs to define it at early stage in alignment with the system’s functionality independent of where and how it would be located.

/ Data flow:

The most important data flows need to be considered during the architecture definition. The importance can be decided based on the system’s primary responsibilities or its impact on system quality. Data flow can be considered in both functional and information viewpoints.

/ Data lifecycle:

The lifecycle of data is another important concern. It is about the transitions that data items go through in response to external events – transitioning from creation, changes to deletion.

2.2.5.3. Information View

The most important data structures and flows need to be considered during the architecture definition. For this purpose, information viewpoint and its respective view are of use. As depicted in Figure 37, we propose the *information structure model* to address the information structure and its content, *data flow model* to address data flow, and data lifecycle model to address data lifecycle concerns.

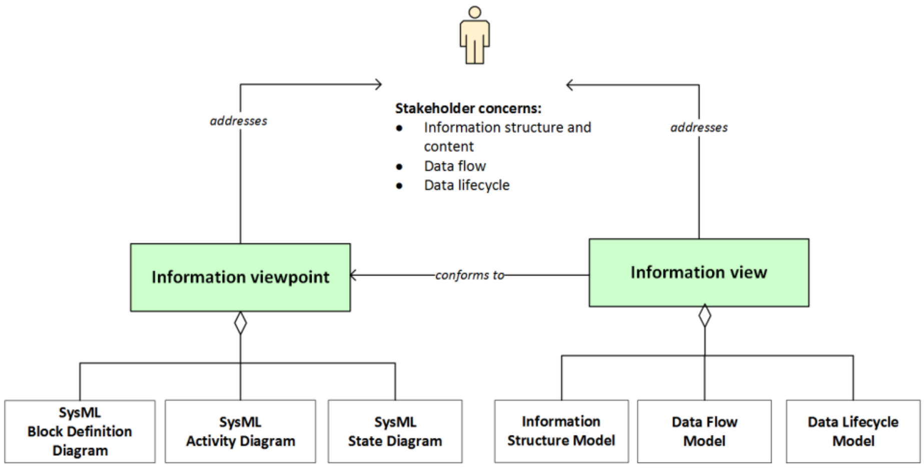


Figure 37: Information viewpoint and view

SysML Block Definition Diagram, activity diagram, and state diagram can be used respectively as a modeling diagram for the information structure, data flow, and data lifecycle models.

Information viewpoint describes how the architecture stores, manages, and distributes data and information. The information view provides high-level view of static data structure and information flow to users, developers, testers, and maintainers. In this section, the data flow (information exchange, protocol message types) is explained.

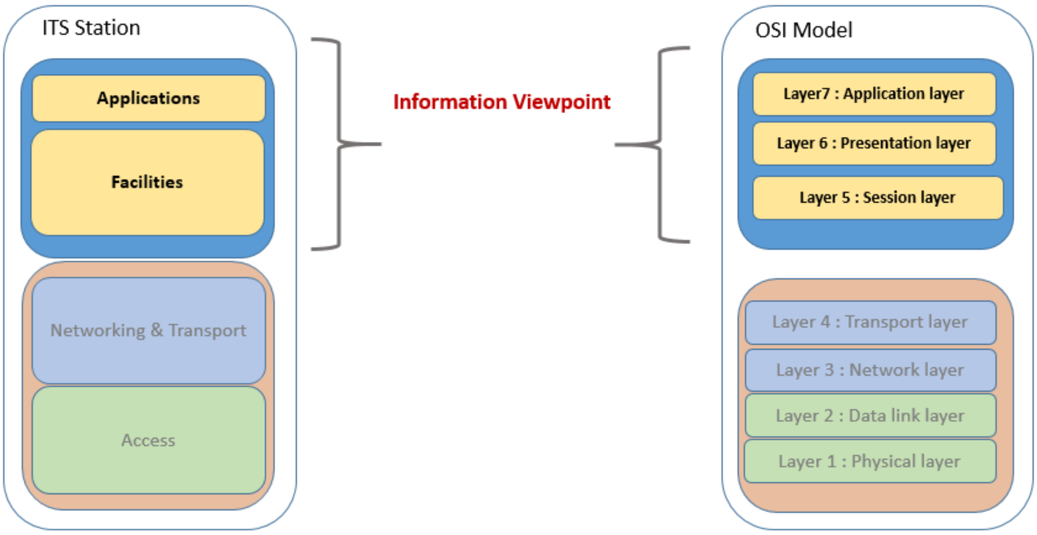


Figure 38: Information viewpoint mapping between ITS station and OSI model.

Following generic exchange message types have been identified from various existing ITS architectures mainly referring to VRUITS architecture [8], which will be utilized communicating between two systems:

- CAM:
  - ETSI has defined the CAM message to inform vehicle status in V2X applications. The CAM message has been specified for ITS-G5 communications, in which vehicles and roadside units make a risk assessment based on the location and speed of vehicles in the safety zone round the vehicle.

> Vehicles transmit already data, equivalent to the data contained in CAM-messages, on position, speed, and other sensor information to the OEM or Service Provider cloud, which analyses data and provides services to vehicles and customers, e.g. traffic information based on probe vehicle data, and slippery road information.

- DENM: Road Side Units communicate with On-Board Units in vehicles using ITS-G5 standardised communications. DENM (ETSI EN 302 637-3 V1.2.2) is used for this purpose.
- DATEX II: DATEX II (version 2.3) messages can be used for the communication between Service Providers, and between Service Providers and Traffic Data Providers.
- TOPO: Messages are sent from a roadside unit to a vehicle to inform the vehicle about the geometry of an intersection. Message format is inherited from the SAE J2735 DSRC standard.
- SPAT: Message broadcasted by Roadside Units (RSU) to provide current signal status (colour) by lane and when the status is expected to change [45]
- LDM: The basic functionality of the LDM is to provide a repository of information for facilities and applications. Facilities such as the CA and DEN basic services can store information into the LDM. Applications can retrieve information from and store information into the LDM [40]

The data flow is explained for the different types of systems and between the systems at VRU, vehicle, roadside, and central system:

- Cooperative ITS systems: Different message types are defined within ETSI TC ITS that can be used for cooperative applications with VRUs. For the specific use cases in this document, the relevant message sets are CAM and DENM. Within CAM the container message sets for PTW, bicycles and pedestrians are not defined in ETSI EN 302 637-2. In addition, other infrastructure-related message sets that are still work-in-progress within ETSI/CEN/ISO are needed. Such messages are for example MAP on Road Topology and Signalling Phase and Timing on signalized intersections (e.g. for INS and IPTS), In-Vehicle Information messages on road signs (IVI, e.g. for GWC) and Cooperative Perception Messages (CPM, e.g. as defined by the Ko-FAS project to broadcast information on detected vulnerable road users to other road users).
- Tag-based systems: tag-based systems can use different technologies for VRU localization relative to their own position, via wireless communication. The tags used in the system contain IDs to distinguish a VRU or VRU type.
- Smartphone based systems: For smartphone-based applications, information can be exchanged via widely used web-based protocols like SOAP/XML. Special description files are needed per application to describe the information elements for the specific application. Information for VRU-specific applications should preferably be distributed via open data, e.g. on locations for IPTS, GWC trajectories etc.

2.2.5.4. Model kinds and Models

As illustrated in Figure 37 the information view consists of Information Structure Model, Data Flow Model, and Data Lifecycle Model, which can be represented using SysML Block Definition Diagram (BDD), Activity Diagram, and State Diagram respectively.

2.2.5.4.1. Information Structure Model

Information structure models capture the important data elements and their relationships. Entity-relationship modeling (ER model) is broadly used in data analysis. It composes of entity types and defines their relationships. Besides the ER model, SysML Block Definition Diagram (BDD) can be used for the notation of information structure. The SysML BDD is described in Section 2.2.3.4.1. The information structure model should remain high-level and with less detailed information.

2.2.5.4.2. Data Flow Model

Data flow models capture the dynamic movement of information or data between system elements and the outside world. It represents the information or data flow between system elements and their directions. Besides the information interface, it needs to capture, flow direction, information scope, volumetric information, the means via which information or data is exchanged (transfer of flat files or real-time exchange of XML messages) [14]. The definition of the data flow model should conform to the interface definitions and function invocations of the functional view.

Data flow can be represented using SysML activity diagrams.

SysML activity diagram captures the overall flow of activities or actions.

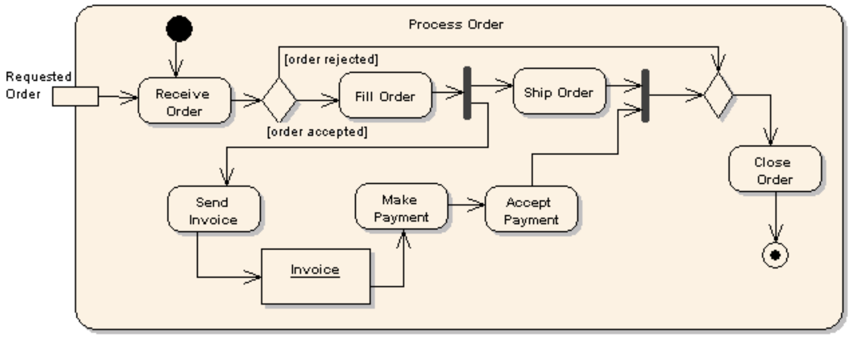


Figure 39: Example activity representation

Figure 39 illustrates an example activity diagram in SysML notation. The main concepts are described below:

- Actions are represented by rounded rectangles e.g. “Receive Order”;
- Decisions represented by diamonds;
- The start (split) or end (join) of concurrent activities are represented by bars;
- The initial node or start of the workflow is represented in a black circle;
- Final node or end is represented by an encircled black circle.
- Arrows running from the start towards the end represent the order in which activities happen.

Besides the SysML activity diagrams, Gane and Sarson or SSADM data flow diagrams can be used to represent information or data flow models.

The data flow within the different systems is described below:

- **VRU**: at the VRU system the next interfaces are identified
  - VRU-VIS to VRU Vehicle E/E system: For cars and trucks, the CAN-bus (Controller Area Network) interface with EOBD (European On-Board Diagnostics) protocol is used to retrieve status information from the car. For PTW or (electrical) bicycles, no CAN-based interface and protocol has been defined as of today. Interfaces like Blue-tooth and USB are widely available to connect devices, and proprietary EOBD-based protocols can be used to exchange status information retrieved from vehicle sensors e.g. on bicycles or PTW on wheel rotations, steering angle etc. This information is needed to get accurate information on speed, acceleration and direction, together with object state (stop, start, ride, turn).
  - VRU-VIS to VRU-CS: A VRU-VIS can be connected to a VRU-CS (smartphone) to use the HMI of the smartphone. Some of the technologies as described below for vehicles (CE2) can be used to connect a VRU-VIS to an external HMI of a smartphone.
- **Vehicle**: at the vehicle system the next interfaces are identified:
  - VIS to Vehicle E/E system: The VIS to VEE interface is used in three ways i.e. i) to retrieve information from the VEE on e.g. actual speed, acceleration and exterior lights on/off, ii) to send information on collision risk and request for actuation (e.g. for autonomous emergency braking) and iii) to send information to the in-car HMI. For i) and ii) EOBD with vendor-specific extensions can be used. For iii) the following non-exhaustive list of technologies can be used to connect a VIS to an external HMI:
    - MirrorLink: a technology that bridges the mobile phone and the car. It allows specially written apps running on the phone to be displayed on the car's head unit, where the user can interact with them.
    - iPod Out: Apple supports iPod Out for Apple devices, which allows selected applications to output analogue video to the head unit.
    - HTML5: web technology allows presenting a HMI through the head unit or mobile device, while the application is executed at the VIS.
    - Simple UI Protocol: instead of replicating the complete HMI. The head unit provides simple UI elements, which external applications can use.
- **Roadside**: at the roadside system the next interfaces are identified:
  - RIS to TLC: The RIS to TLC interface is needed by a RIS to retrieve dynamic information on traffic state or intersection state. Today, no EU standards exist to exchange data from a TLC to external systems like a RIS. In the Netherlands, the IVERA protocol was developed (www.ivera.nl) to ex-change information between TLC and TMC of different vendors. This protocol

can be reused as interface between RIS and TLC to exchange information on intersection state. In Germany, a similar protocol was developed by OCIT (www.ocit.org).

> RIS to Roadside VLS: A roadside VLS system can send information on detected VRUs to a RIS. The interface is system-specific.

/ **Central**: at the central system the next interfaces are identified:

> CIS to TMC: A TMC with TMIS can be used as central distribution point on all traffic and road state information, i.e. the actual status of flow/speed/travel times and measures, warnings and status of traffic signs. The information could be exchanged by DATEX2 protocol.

> TMC to IIS: A similar interface as between CIS and TMC can be used between TMC and IIS since similar information of the TMC/TMIS can be sent to the IIS. Also requests to a specific TLC (extended green time) from the IIS can be sent via a central TMC to a specific TLC. Proprietary message formats are available today to send these types of message requests (e.g. IVERA in the Netherlands or OCIT in Germany).

> TMC to TLC: Dynamic information from RSS or RAS systems at TLCs or other roadside systems can be exchanged to other systems like CIS or IIS a central TMC.

> TMC to DIS: Proprietary protocols for DIS (Data Interchange Server) can be used to exchange traffic information and road state for interoperability between cross borders. The service allows applications to publish events about logistics entities to which other part subscribe to. The format for message transport is AMQP, although the subscription and publication protocols are at a higher (REST) level. The message payload is any message format that sender/receiver agree.

2.2.5.4.3. Data Lifecycle Model

Data or information lifecycle models are used to analyze the way information or data values change over time [14]. SysML state diagram can be used to model the data lifecycle model by capturing the state transition of system element in response to external stimuli.

State diagrams represent the life-cycle behavior of a SysML block in terms of its states and transitions. The transitions that data items undergo in response to external events (from creating data through updating it to deleting the data) can be represented in state diagrams after the functional requirements are elicited.

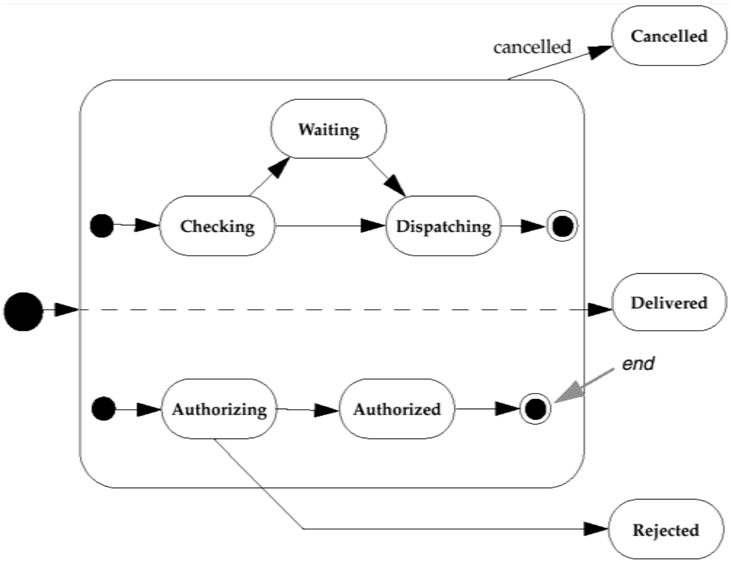


Figure 40: Example state diagram [41]

SysML state diagram has the following main concepts, which are shown in an example diagram Figure 40

/ State is captured in a rounded rectangle or circle. It is a significant condition in the life of a SysML block.

/ The initial node or start of the state diagram is represented in a black circle;

/ Final node or end is represented by an encircled black circle.

/ Concurrency is expressed by an orthogonal state.

2.2.5.5. Correspondence rules

The information viewpoint has correspondences with functional viewpoint as highlighted in Figure 41 Information viewpoint conforms to the Functional viewpoint and vice versa.

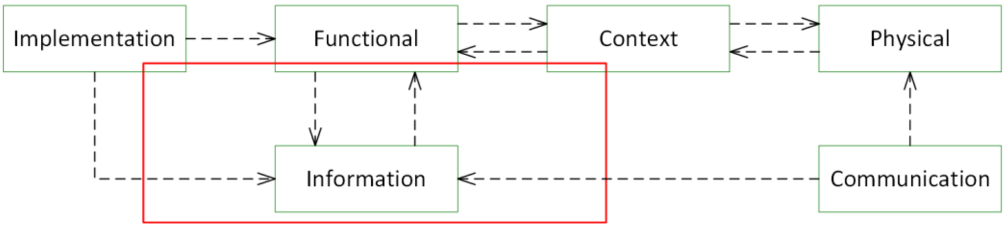


Figure 41: Correspondences for the information viewpoint

The implementation and communication viewpoints conform to the information viewpoint. The definition of the information models is iterative thus requires close interactions with the functional viewpoint.

2.2.6. Physical Viewpoint

2.2.6.1. Definition

The physical view depicts the system from a system engineer's point of view. It is concerned with the topology of sub-systems at each respective domain of interest, as well as the physical connections between these sub-systems to support the C-ITS applications implemented in the different C-MobILE deployment sites. Sub-systems include functional components that define more specifically the functionality and interfaces that are required to support a particular connected vehicle application.

2.2.6.2. Stakeholders and Concerns

Although most of the stakeholders have some level of interest in the Physical Viewpoint, users, architects, system maintainers, OEM (Original Equipment Manufacturer) are the main stakeholders. The physical viewpoint addresses the stakeholders' concerns which are mentioned in below Figure 42.

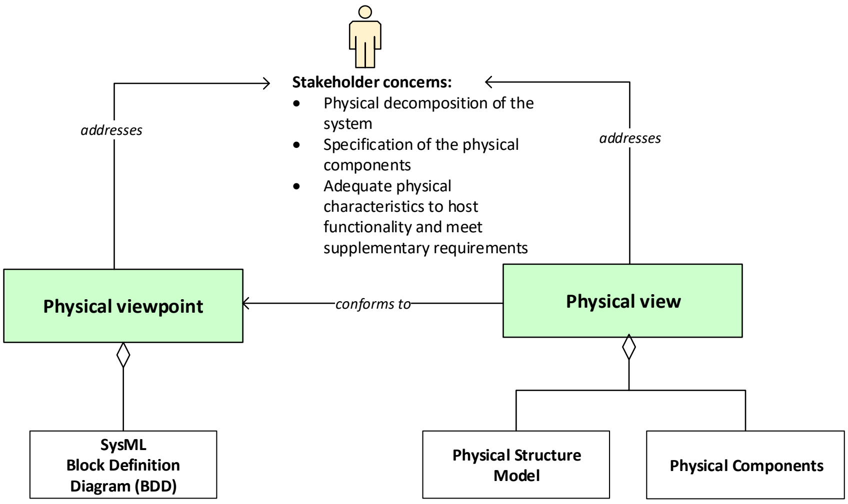


Figure 42: Physical viewpoint and view

SysML Block Definition Diagram can be used as a modelling diagram to depict physical components involved in C-MobILE.

2.2.6.3. Model kinds and Models

As illustrated in Figure 42, the Physical View consists of Physical Structure Model which can be represented using SysML Block Definition Diagram (BDD).

2.2.6.3.1. Physical Structure Model

The Physical structure is based on best common practice in previous ITS projects such as [48] i.e. a split in five main physical layers for Vehicle, Roadside, Central (or Back-Office), Traveller/VRU System and Support System. These layers are termed as system such as Central System for as similar set of sub-systems are grouped together performing similar set of functionalities for C-ITS.

The physical structure is divided in five 'Systems as shown in Figure 43

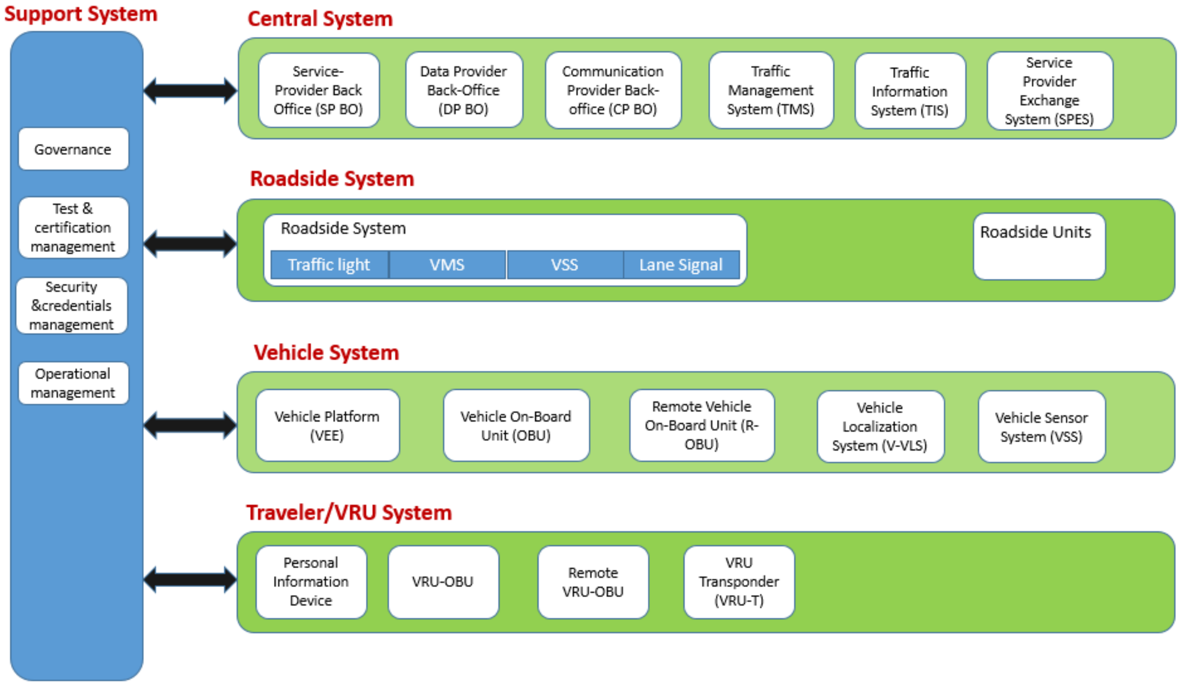


Figure 43: High-level physical structure

Besides the High-level physical model, SysML Block Definition Diagram (BDD) can be used for the notation of physical structure where each main system and its sub-systems are depicted in terms of Blocks.

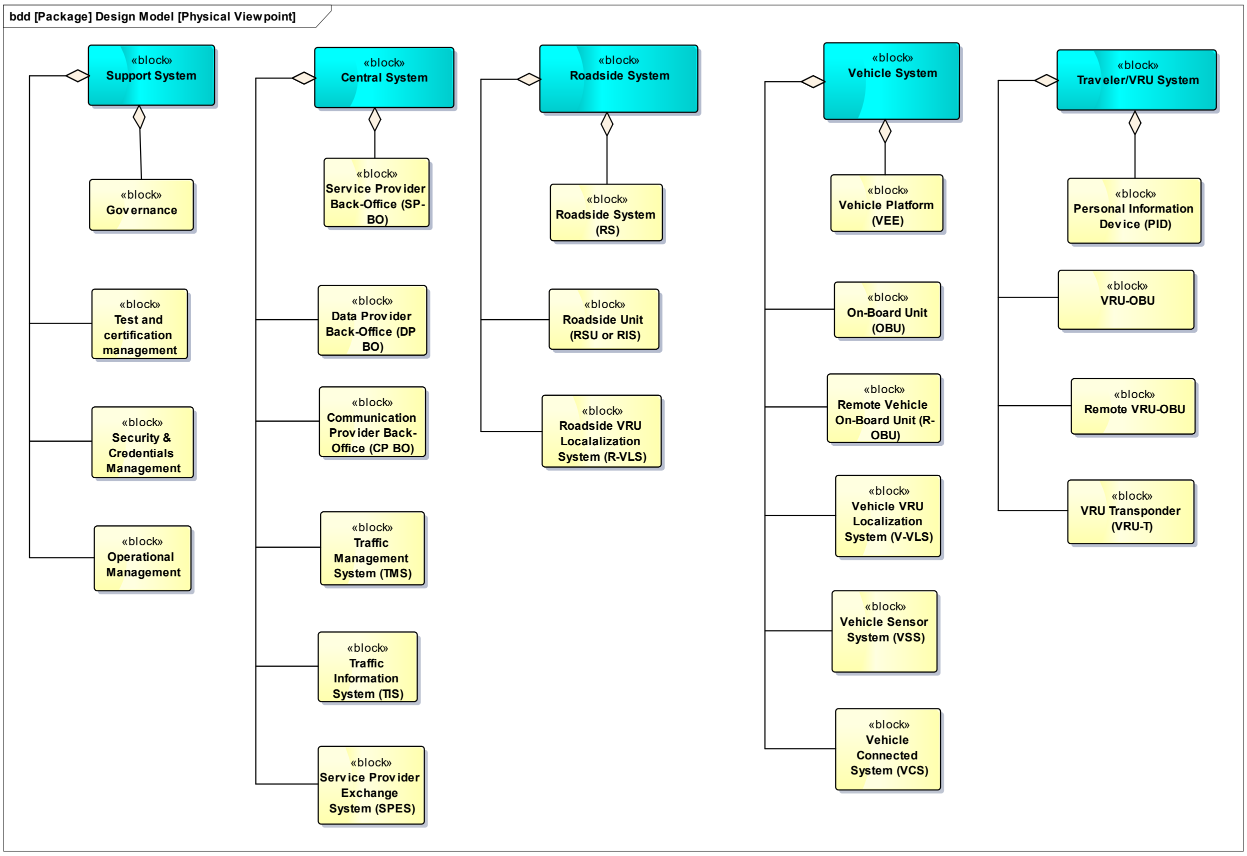


Figure 44: Block Definition Diagram for Physical Viewpoint

The description of each sub-system are described below

2.2.6.3.1.1. Central System

The Central System comprises those sub-systems that support connected vehicles, field, and mobile devices and perform management and administration functions. The sub-systems in this system are typically virtual systems that can be aggregated together or geographical or functions distributed

Following are the systems mainly involved at Central system:

- Traffic Management System (TMS): A TMS is the functional back-office system of the responsible road operator to enforce legal actions on urban or high-way road sections or intersections based on real-time traffic data from loops, cameras, speed sensors, etc. or actions by traffic controllers. The real-time data that flows from the Traffic Info System is integrated and processed by the TMS (e.g. for incident detection), and may result in traffic measures (e.g. traffic routing, dynamic speed limits) with the goal of improving safety and traffic flow. Cloud servers can be deployed across borders to enable interoperability such as Ericsson Interchange server of Nordic Way Architecture and AEON server of Co-GISTICS
- Traffic Information System (TIS): A Traffic Information System is the functional back-office system of a road operator to collect and process real time traffic data from traffic data systems (e.g. roadside sensor systems (loops, cameras) or connected vehicles) and to distribute real-time and/or aggregated information on traffic state (speed, flow and travel times) or road state to TMS or external systems like a SP BO. In practice several distributed TIS from different road operators can be interconnected to a central TIS (e.g. from NDW), which provides aggregated information for the Netherlands.
- Service Provider Back-Office (SP BO): A generic back-office system of a Service Provider used for the specific services of the SP to connected drivers or end-users to inform end users or other SP BO systems from providers. A SP BO can be used to support personal information services for, e.g. navigation or traffic information applications on OBU/PID. A SP BO can also be used to gather floating car data from OBU/PID;
- Data Provider Back-Office (DP BO): A Data Provider BO system is a data system that collects and fuses floating car data and real-time traffic data from roadside sensor systems to increase insight in actual and expected traffic state (e.g. on traffic jams). The DS also distributes enriched (aggregated) information on traffic state (speed, flow and travel times) to Service Providers.
- Communication Provider Back-Office (CP BO) or Central ITS System (CIS): A generic back-office system of a communication provider used for access at several communication systems from other BO systems (like SP BO, TMS,TIS etc.) to send and receive ITS information to/from vehicles or other road users.

- Service Provider Exchange System (SPES): an e-Market ('broker') system for discovery and exchange of ITS (end-user) services and ITS communication services; the SPES can support functions like service discovery, service authentication, authorization, accounting (AAA) and billing.
- Data Interchange Server (DIS): Cloud based server specifically to solve interoperability concerns by interconnecting data from cross-border providing data, information, materiel, and services to, and accept the same from, other systems…and to use the data, information, material and services so exchanged to enable them to operate effectively together.

Other back-office systems can also be located at this layer depending on the type of application. One example is a Fleet and Freight Management System which provides the capability for commercial drivers and fleet-freight managers to receive real-time routing information and access databases containing vehicle and/or freight equipment locations as well as carrier, vehicle, freight equipment and driver information. Fleet and Freight Management Centre also provide the capability for fleet managers to monitor the safety and security of their commercial vehicle drivers and fleet.

2.2.6.3.1.2. Roadside System

It covers the ITS infrastructure on or along the physical road infrastructure, e.g. surveillance or control devices (signal/lane control, ramp meters, or systems to supply information to connected vehicles.

In the roadside (or field) area, the following sub-systems are defined:

- Roadside System (RS): Different types of existing roadside systems are identified:
  - Roadside Substation (RSS): a system deployed along highways and includes sensors (loops), control logic, and actuators. The system can run as a stand-alone closed loop system i.e. run standalone local traffic control functions (e.g. traffic jam tail detection and warning via Variable Message Signs) or can be controlled by the TMS.
  - Traffic Light Controller (TLC): a TLC is a specific type of roadside system. It includes the input from loop detectors or other sensors, a control logic, and the actuation of the traffic lights. A TLC can be run as a stand-alone closed-loop traffic control system. A TLC can also be controlled by a central TMs, e.g. in green wave applications between different TLC's. A TLC is deployed on urban road or can be deployed at highway access roads for access control.
- Roadside Unit (RSU) or Roadside ITS System (RIS): A RSU/RIS is a cooperative roadside communication system responsible for the two-way communication functionality at a part of a road network (typically an intersection or a road section of 500m – 1km). This physical object is responsible for implementing communication functionality in the roadside system and optionally also application functions. A RSU/RIS is included in the ITS reference architecture standardized by ETSI ITS. A RSU/RIS can be part of the roadside communication network with distributed radio units, and centralized functions in the Communication Provider Back-Office.

2.2.6.3.1.3. Vehicle System

In the vehicle area the following sub-systems are defined:

- Vehicle Platform or Vehicle E/E system (VEE): The Vehicle Electrical and Electronic system (E/E) system includes all in-car sensors (speed, lights, etc.) and actuators (brake, etc.). The Vehicle Electrical and Electronic system provides sensor information (e.g. speed) from a vehicle to an external C-ITS system and optionally enables the control/actuation (e.g. speed control) of that vehicle by an external system. The Vehicle E/E must include safety measures to ensure the safe operation of the vehicle, independent of the interaction between the Vehicle E/E and external sub-systems. A further differentiation can be made per vehicle type, e.g. emergency vehicle, commercial vehicle or (public) transport/transit vehicle.
- Vehicle On-board Unit (OBU) or Vehicle ITS Station (VIS): An on-board unit is a sub-system attached to a car and needed for driver assisted applications to inform / advise a driver via a HMI. The OBU provides the vehicle-based processing, storage, and communications functions necessary to support connected vehicle operations. The radio(s) supporting V2V and V2I communications are a key component of the Vehicle OBU. Four different types of implementations are represented by the Vehicle OBU:
  - Vehicle Awareness Device – This is an aftermarket electronic device, installed in a vehicle without connection to vehicle systems and is only capable of sending the basic safety message over short-range communications. Vehicle awareness devices do not generate warnings.
  - Aftermarket Device – This is an aftermarket electronic device, installed in a vehicle, and capable of sending and receiving messages over a wireless communications link. The self-contained device includes GPS, runs connected vehicle applications, and includes an integrated driver interface that issues audible or visual warnings, alerts, and guidance to the driver of the vehicle;
  - Retrofit Device – This is an electronic device installed in vehicles by an authorized Service Provider, at a service facility after the vehicle has completed the manufacturing process (retrofit). This type of device provides two-way communications and is connected to a vehicle data bus to integrate the device with other on-board systems. Depending on implementation, the device may include an integrated driver interface and GPS or integrate with modules on the vehicle bus that provides these services.

> Integrated System – This is a system of one or more electronic devices integrated into vehicles during vehicle production. The Integrated System is connected to proprietary data busses to share information with other on-board systems. The Integrated System may include many control modules.

In retrofit and integrated implementations, the Vehicle OBU interfaces to other on-board systems through a vehicle bus (e.g., CAN), represented as the Vehicle Platform, this interface provides access to on-board sensors, monitoring and control systems, and information systems that support connected vehicle applications. The vehicle bus may also be the source for GPS location and time, and the access point for the vehicle's driver-vehicle interface. Self-contained devices include an integrated GPS and driver interface that supports direct visual, audible, or haptic interaction with the driver. The Vehicle OBU includes the functions and interfaces that support connected vehicle applications for passenger cars and trucks. Many of these applications (e.g., V2V Safety applications) apply to all vehicle types including personal automobiles, commercial vehicles, emergency vehicles, transit vehicles, and maintenance vehicles. The Vehicle OBU is used to model the common interfaces and functions that apply to all of these vehicle types, i.e. also commercial, public transport or emergency vehicles.

/ Remote Vehicle OBU (R-OBU): Remote Vehicle OBUs represents other vehicles that are communicating with the host vehicle. The host vehicle onboard unit, represented by the Vehicle OBU physical object, sends information to, and receives information from the Remote Vehicle OBUs to model all vehicle V2V communications.

2.2.6.3.1.4. Traveller/VRU System

At the traveller / VRU system the following sub-systems are defined:

/ Personal Information Device (PID): A personal information device is typically a smart phone or personal navigation device used by an end-user. The PID provides the capability for travellers to receive formatted traveller information wherever they are. Capabilities include traveller information, trip planning, and route guidance. It provides travellers with the capability to receive route planning from the infrastructure at home, at work, or on-route using personal devices that may be linked with connected vehicle on-board equipment. A PID might include the communication functionality of a Personal ITS station, as specified in ETSI ITS specifications;

/ VRU Vehicle OBU (VRU-OBU): an on-board unit is a sub-system attached to a VRU vehicle (e.g. moped, electric bike) and needed for VRU assisted applications to inform / advise a driver via a HMI.

/ Remote VRU OBU (R-VRU-OBU): Remote VRU Vehicle OBUs represent other VRU vehicles that are communicating with the host VRU vehicle. The host VRU vehicle on-board unit, represented by the VRU-OBU physical object, sends information to, and receives information from the Remote Vehicle OBUs to model all VRU related V2V communications.

/ VRU Transponder (VRU-T): A V RU transponder is part of a tag-based communication system. A transponder can be active (=with own battery, sending data at constant time intervals), semi-passive (with own battery, sending message at request of an interrogator) or passive tag/chip (without own battery, responding to interrogator request). The tags communicate with an external interrogator, called VRU Localization System, which can be integrated in a vehicle (car, bus, truck) or in a roadside system:

> Vehicle VRU Localization System (V-VLS): A VRU Localization System is part of a tag-based communication system.

> Roadside VRU Localization System (R-VLS): A VRU Localization System is part of a tag-based communication system. The VRU transponder carried by a VRU, is an active (=with own battery) or passive tag/chip that can respond on an interrogation signal (trigger) from the VRU Localization System. A VRU Localization System can be integrated in, e.g., a Traffic Light to detect the presence of a specific user, e.g. a person with a disability.

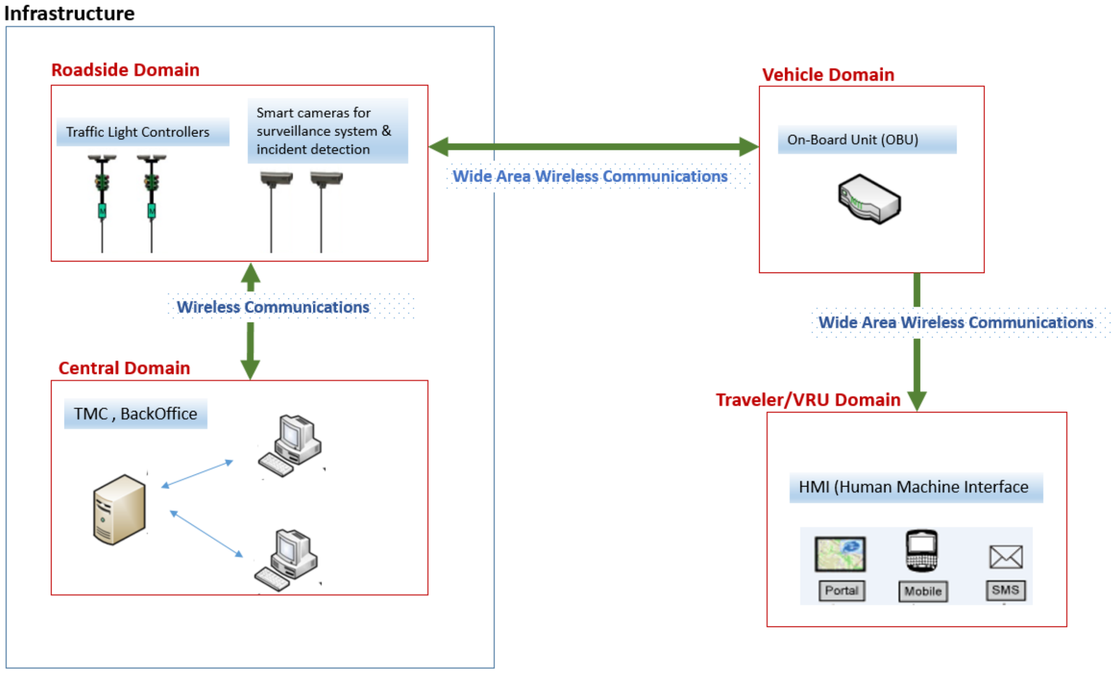


Figure 45: Connections between physical components of C-MobILE

2.2.6.4. Correspondence rules

The Physical Viewpoint has direct correspondence with Context Viewpoint. Communication Viewpoint conforms to Physical Viewpoint in terms of communication interfaces and protocols between physical components.

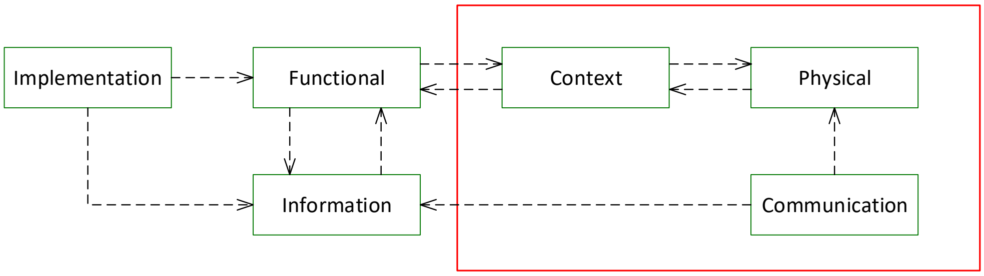


Figure 46: Correspondences for the Physical Viewpoint

2.2.7. Implementation Viewpoint

The implementation viewpoint captures the design and implementation details of the C-ITS functional architecture by realizing the functionality into software and hardware components. The C-MobILE reference architecture focuses more on an abstract level independent of design and implementation details.

Main stakeholders for the implementation viewpoint are end user, system/software architect, designer, and tester. Their key concerns are implementation of functional components into software and hardware components, optimal resource utilization, allocation, performance estimation, security etc. The implementation views may consist of application software view, function allocation view, and execution platform view.

For describing the application software view, SysML BDD and IBD can be used. Allocation table of software components to hardware components can be used for the function allocation view. For execution platform view, SysML BDD and activity diagrams can be used.

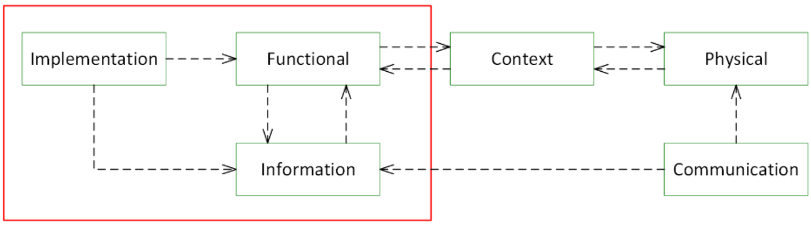


Figure 47: Correspondences for the Implementation viewpoint

As highlighted in Figure 47, the implementation viewpoint has *realization* correspondence to the functional and information viewpoints. It means *n-to-m mappings* by realization relationships between entities in the implementation viewpoint and entities in the functional and information viewpoints.

The implementation viewpoint is out of the scope of this report, however, having the initial definition of the implementation viewpoint and its respective views will ensure the consistency between the architectures and the software/hardware development of the C-ITS services for the deployment sites. Therefore, the implementation viewpoint and its respective views will be elaborated further in the WP3 T3.3 deliverables.

3. Current C-ITS deployed infrastructures

3.1. Architecture Barcelona

The city of Barcelona and its metropolis currently suffers constant traffic jams and congestions. The high density of the population together with these congestions generates big environmental concerns. Barcelona sees C-ITS as a possibility to mitigate these problems and is currently working on deploying C-ITS services aimed at increasing safety, reducing congestion and solving the environmental issues.

3.1.1. Deployed Services

Barcelona has been participating in several projects aiming to deploy smart mobility services although it is the first time that the city is chosen as a C-ITS deployment site in co-founded European projects.

Currently there are no C-ITS services deployed although the city sees C-MobILE as a great opportunity to uptake this technology. However, there are service providers that offer relevant data such as Road Hazard Warning, Road Works Warning and Mode & trip time advice.

The next table shows the services that are planned to be deployed and its penetration rate.

Service	Communication	User-equipment	Users
Road work warning	Cellular	Smartphone	200 vehicles
Road hazard warning	Cellular	Smartphone	200 vehicles
Emergency vehicle warning	Cellular	User smartphone	200 Vehicles
	Cellular	EV 3/4G	1 fire truck
Signal violation warning	Cellular	Smartphone	200 Vehicles
Warning system for pedestrian	Cellular	Smartphone	175 pedestrians
Green priority	Cellular	Smartphone	1 fire truck
GLOSA	Cellular	Smartphone	1 fire truck
Cooperative traffic light for pedestrian	Cellular	Smartphone	175 pedestrians
Flexible infrastructure	Cellular	Smartphone	200 Vehicles
In vehicle signage	Cellular	Smartphone	200 Vehicles
Mode and trip time advice	Cellular	Smartphone	200 Vehicles
Probe Vehicle Data	Cellular	Smartphone	200 Vehicles

Table 8: Planned C-ITS services in Barcelona

3.1.2. Covered Area

Barcelona is willing to deploy C-ITS services in the entire city ring road, in the accesses of the northern part of the city and in some specific roads and intersections of the inner city.

C-ITS area	User extension
/ 35 Intersections / 45 Km (inter-) urban roads 66 traffic panels at 20 km roads	Target: 200 cars, 1 emergency vehicle, 100 motorcycles, 175 pedestrians, 25 cyclists, 6000 shared bicycles

3.1.3. Architecture

The Barcelona Deployment City is mainly focused on the cellular communications for serving the C-ITS services. Currently there is no ETSI ITS G5 infrastructure and there is no short-term deployment plan for this technology, therefore all C-ITS services will use cellular communications. The high-level site architecture depicted in the following figure shows the elements running in this city in order to offer cellular-based services to all kind of end-users.

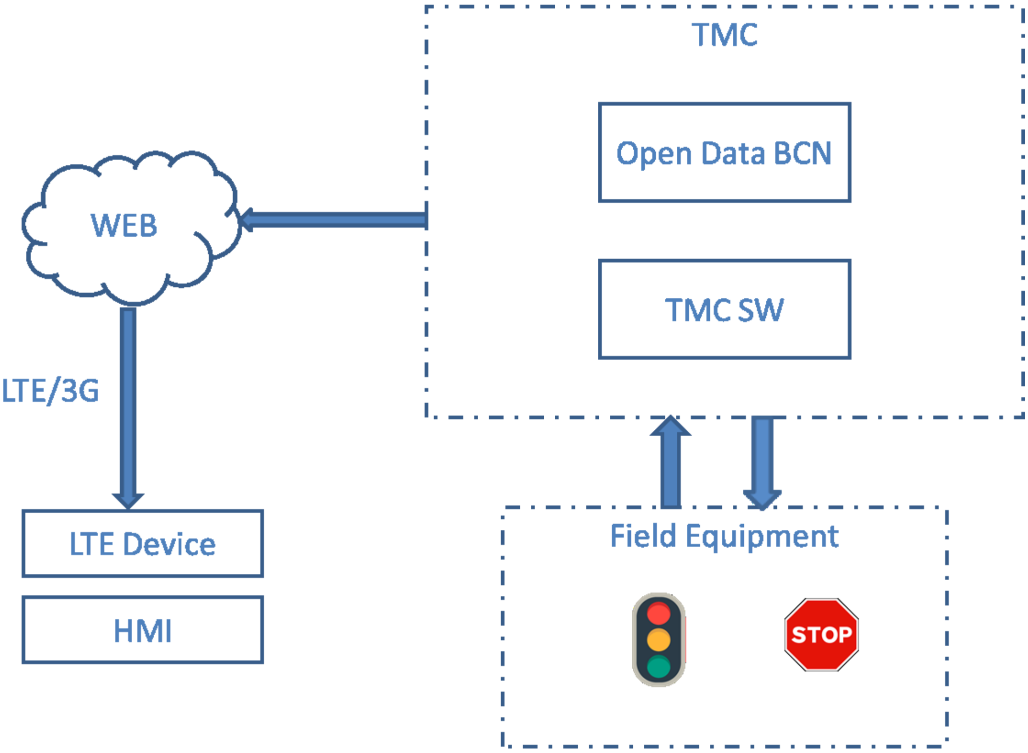


Figure 48: Generic architecture for Barcelona

3.1.3.1. Central Systems

In this section of the document, the different systems represented in the previous figure present in the deployment site are explained providing information of their function as well as the interaction between them.

3.1.3.1.1. Open Data BCN

Open data BCN is a movement promoted by public administrations in Barcelona with the main objective of making the most of available public resources, exposing the information generated or guarded by public bodies, allowing their access and reuse for the common good and for the benefit of individuals and entities interested.

This public information, of great potential value, can be relative to any topic, statistical data, results of studies or analysis, information on public services, etc.-. Companies, researchers, other public institutions or the general public can make use of the information resources for any purpose, maximizing the economic and social possibilities: promoting transparency in management, improving services to citizens, generation of business activities and social impact, in search of efficiency in governance.

Open Data BCN is part of the strategy of Barcelona Digital City, fostering a plural digital economy and developing a new model of urban innovation based on the transformation and digital innovation of the public sector and the involvement among companies, administrations, the world academic, organizations, communities and people, with a clear public and citizen leadership.

All public information managed by municipal public entities is publicly exposed by default. Through the data catalogue, metadata associated with the published resources are exposed, which classify and describe data sets with descriptive and technical information. Among the data sets available in Open Data BCN are data such as bicycle lanes, information on available parking slots, road works, incidents, available public transport, loading and unloading areas, car sharing services, charging points for electric vehicles, traffic incidents, transit status, etc.

The Open Data Portal of the Barcelona city council has been developed with a mixed installation of Drupal and CKAN on Ubuntu. The installed version of Drupal is 7.52 (with php 5.6) and CKAN 2.6.0.

It is basically a REST web service where users can retrieve the information in JSON, XML or csv formats.

Hardware	Web server with Ubuntu
Relevant services	RWW, RHW, MTTA, EVW
Communication flows	RHW/RWW: DENM over LTE to the HMI and CAM over LTE to TMC SW MTTA: XML/JSON over LTE to the HMI/Smartphones

	EVW: CAM over LTE to the TMC from the Emergency Vehicle, DENM over LTE to the HMI of the Vehicles

3.1.3.1.2. TMC

C-ITS services will be implemented with the use of two existing traffic management centres, one responsible for the city of Barcelona and one for the northern access to the city.

The traffic management centres are based in SCADA (Supervisory control and data acquisition) which is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery. The real-time control logic is performed by networked modules which connect to the field sensors, traffic lights, dynamic panels and actuators.

3.1.3.1.3. Vehicle Systems

The OBU is an LTE enabled device (smartphone) with direct communication with the server through the web service. There are two types of vehicles listed below:

3.1.3.1.3.1. User Vehicles

Hardware	Android Smartphone
Relevant services	Road work warning Road hazard warning Emergency vehicle warning
Communication flows	CAM and DENM over Cellular network (LTE/3G) to/from the TMC SW

3.1.3.1.3.2. Emergency Vehicles

The emergency vehicles will have 3G OBUs which regularly update its position to the local web server.

There is an existing deployment which provides an estimation of the location of the firetrucks. This system will be improved so that an OBU with cellular communications is able to provide an accurate and real-time position of the emergency vehicles.

Hardware	Android Smartphone
Relevant Services	Emergency vehicle warning
Communication flows	CAM over Cellular network (LTE/3G) to the TMC SW

3.1.3.1.4. VRU/Pedestrian Systems

Hardware	Android Smartphone
Compatible services	MTTA
Communication flows	CAM and DENM over Cellular network (LTE/3G) to/from the TMC SW

3.1.4. Stakeholders' partnership

Barcelona is a complex deployment city that requires some strategic and key partners and associated partners in order to implement, deploy, operate and evaluate the C-ITS services. The complete list is the following:

Partners:

- Barcelona City Council: Public authority provides the necessary means and connections to implement, deploy and successfully test the services in the city of Barcelona. It manages data providers. Provides access to emergency vehicles.
- IDIADA: In charge of development. Operates the Operational Web Server.

- RACC: Has an active set of users willing to use the developed C-ITS services. Allows reaching end-users for large-scale deployment.
- Piaggio: Has an active set of PTW users willing to use the developed C-ITS services. Supports the development of C-ITS services targeting PTW users.
- IMI: Supports the Barcelona City Council on providing the necessary means and connections to deploy the services in the city of Barcelona.

Associated:

- Ferrovial: Is a multinational company involved in the design, construction, financing, operation and maintenance of transport, urban and services infrastructure.
- AMB: Territorial entity operating on the principle of metropolitan municipality composed of Barcelona and 35 adjacent municipalities around the city.
- SABA: is an industrial operator of reference in the development of solutions in the field of urban mobility specialized in parking management.
- DGT Spain: is the government department that is responsible for the Spanish transport network.

3.2. Architecture Bilbao

The city of Bilbao currently suffers constant traffic jams and congestions due to its 345,000 habitants and economic activity. These factors create several traffic, economic and environmental challenges which must be faced in order to increase the economic growth of the city in a more sustainable and innovative manner. Considering the importance and benefits of the C-ITS technologies in previous projects (CO-CITIES, CO-GISTICS and CIMEC), the city of Bilbao works in cooperation with different stakeholders to achieve the commitment of investing in C-ITS technologies, improving the impact and benefits of C-ITS technologies and mitigating environmental and driving safety issues.

3.2.1. Deployed Services

Bilbao currently implements the following services: (1) On-street Urban Parking availability.

- Urban Parking service is provided through an App on the Smartphone that currently provides the drivers with information of the available parking locations in 12 different zones throughout the city.
- Road Work Warning data is published in the Open Data Catalogue at Bilbao's website; however, it is not implemented as cooperative service.

Using smartphones, the users of C-ITS technologies can receive necessary data through cellular communication between devices.

Service	Communication	User-equipment	Users
Rest time Management	TBD	TBD	TBD
Motorway parking availability	Cellular	Smartphone / Tablet	2,000 approximately
Urban parking availability	Cellular/Wi-Fi	Smartphone	1,000 – 1,500
Road work warning	Cellular	Smartphone	TBD
Road hazard warning	Cellular	Smartphone	TBD
Blind Spot detection	Cellular/Wi-Fi	Smartphone	20,000 – 25,000

3.2.2. Covered Area

Currently, Bilbao is deploying C-ITS services in several neighbourhoods of the city which cover most area of the entire city.

C-ITS area	User extension
/ 180 Truck parking, 1000 street parking / 30 intersections with Wi-Fi / 20 km roads with CCTV camera / 15 km roads with variable messaging panels	Existing: 0 trucks, 0 shared bikes and 100 cars Target: 150 shared bicycles (20000 users), 2000 trucks, 1500 cars, 152 urban buses

As mentioned before, the currently deployed services in Bilbao use the cellular network. Users' smartphones obtain data to inform the user with the requested information about the zone in which the user is located.

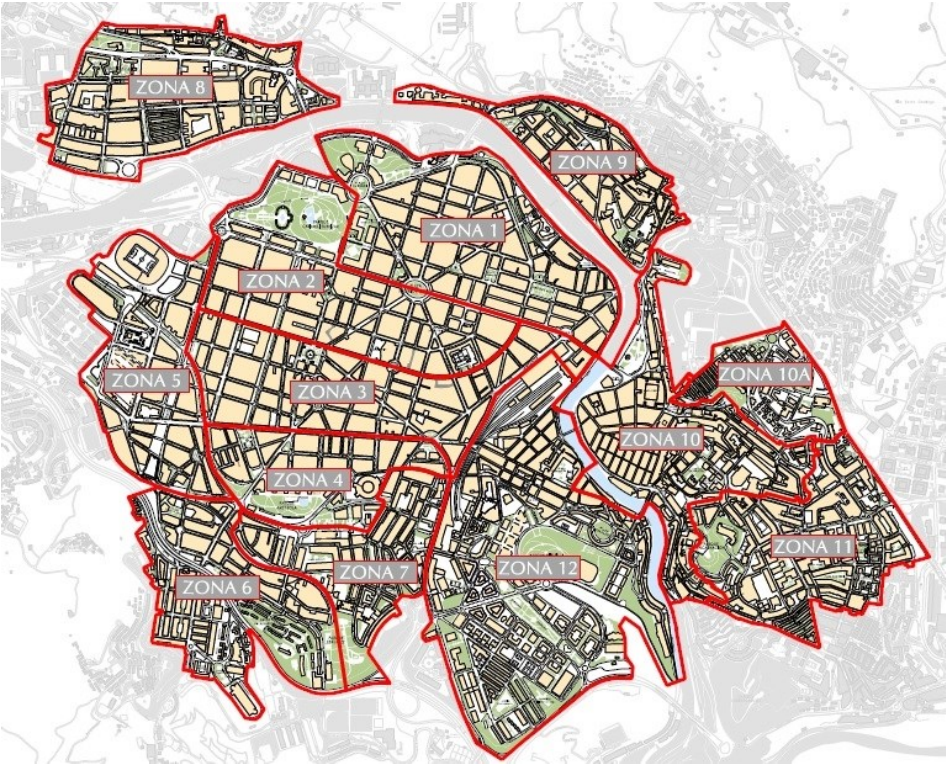


Figure 48: Extent of the covered area in Bilbao divided in 12 different zones

3.2.3. Architecture

The deployment of C-ITS services in Bilbao is based on cellular/Wi-Fi communications. The high-level site architecture depicted in the figure below shows the elements running in the city in order to offer cellular-based services to the end-users.

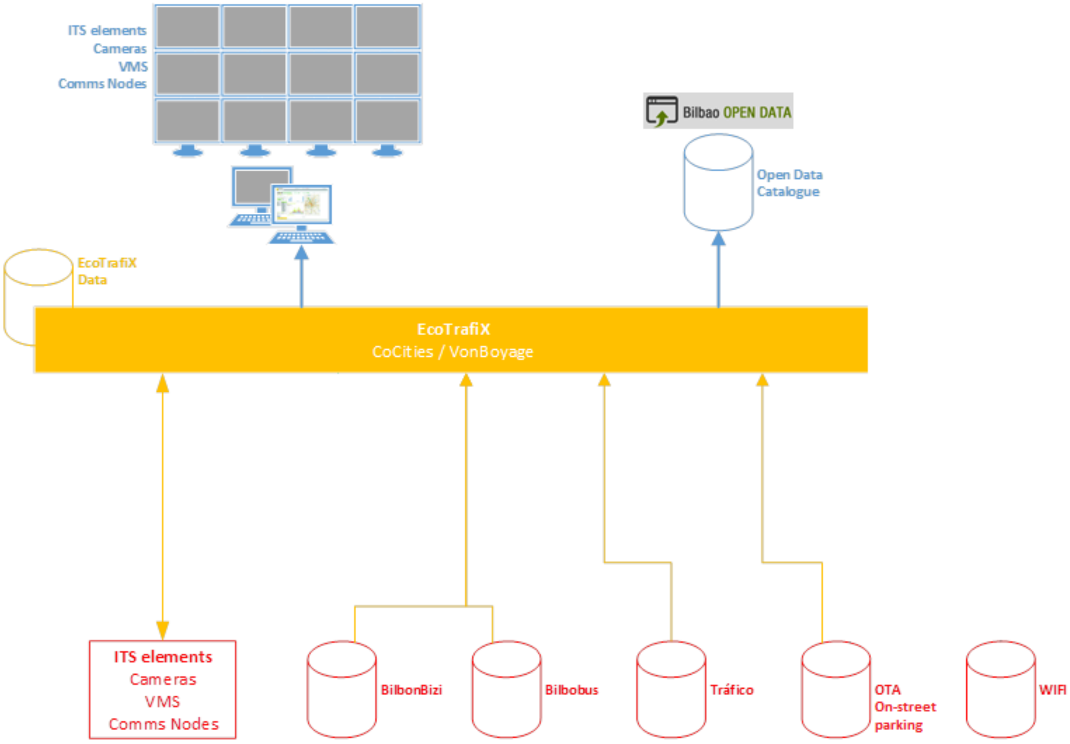


Figure 49: Scheme of Bilbao's high-level architecture

3.2.3.1. Central Systems

In this section of the document, the different systems (deployed in the deployment site) represented in Figure 49 above are explained providing information of their function as well as the interaction between them.

3.2.3.2. Open Data Platform / Operational Web Server

There are two open data platforms installed in City Council premises. They are the following:

- Co-Cities: based on the data model as defined in the e-Motion FP7 project and on the interfaces defined in both In-Time and CoCities FP7 projects, it is a WFS service supplying information about traffic, parking and public transportation.
- BonVoyage: developed within a H2020 project, it supplies very similar information to that of the CoCities interface, but using DatexII and SIRI/NeTeX standards.

It is installed in a fully virtualized environment using VMware technologies and provides the following data services:

- Traffic:
  - Static topology of the streets network in the city.
  - Dynamic information about events such as roadworks.
- Public transportation:
  - Static topology of the bus lines, including the stops, lines, routes, etc…
  - Theoretical timelines.
  - Real time waiting times in each stop.
- Parking:
  - Static information about all off-street parking lots.
  - Static information about all on-street parking zones and stretches.
  - Real time information about the status of each parking lot, zone and stretch, including the occupation level (not ready yet for on-street parking, but planned to be available soon).

3.2.3.3. TMC

This platform serves as the core of most of the ITS systems and provides the following functionalities:

- It automates the launching and execution of action plans as triggered by events.
- It lets the operators control ITS elements such as dynamic message panels, cameras as well as monitoring the status of the communication network and other field elements such as red light cameras.
- It constantly gathers information from several databases and external web service interfaces, integrating it into a unified data model and feeding the open data platform with it.

The platform is installed in a fully virtualized environment using VMware technologies.

3.2.3.4. ITS Elements

Regarding field ITS elements, there are the following:

- About 75 video cameras of different types and resolutions, all of them controllable from the EcoTrafix platform.
- Several signalling gantries to provide information to drivers. Those gantries can also be controlled from EcoTrafiX.
- Several dynamic message panels to provide information to both drivers and pedestrians.

3.2.3.5. Other systems: Bilbonbizi, Bilbobus, On-street parking, municipal Wi-Fi

Currently, the city bus service (Bilbobus) provides information in real time about its status thanks to an operation assistance system. The information then is gathered by the Municipal City Platform and fed to the open data platform.

On top of that, all the off-street parking lots may send real time information about their status and occupation level to the Municipal City platform over a web services interface.

Regarding the on-street parking, the Municipal platform is designed to read the status of every zone and stretch from the City Council databases where that information is to be written to by the company operating the on-street service sometime in the near future.

3.2.3.6. Other items

The city of Bilbao contains the following Roadside Systems.

- 120 Communication nodes.
- Seven Red Light Cameras.
- Currently there is a restricted area entrance but there are 28 to be developed within the next year.

3.2.3.7. Vehicle Systems

In Bilbao, the drivers and VRUs use a smartphone in order to receive information from the Local Operational Web Server and the Open Data server related to the different services. However, will not only receive but send information of their location to the Open Data server to keep the server updated of the position of this kind of vehicles.

Two types of vehicles are presented in the Deployment city of Bilbao, the user vehicles, and the public transport buses.

3.2.3.8. User Vehicles

Hardware	Android Smartphone
Relevant services	Urban parking availability Motorway parking availability

In Bilbao, the user vehicles will be considered those that use the Urban Parking Availability and Motorway Parking Availability services. Therefore, vans and trucks form this group.

3.2.3.9. Public Buses: BilboBus

Hardware	Android Smartphone
Relevant Services	Blind Spot Detection / Warning System

As explained before, the city bus service (Bilbobus) provides information in real time about its status, and then, the information is gathered by the Municipal City Platform and fed to the open data platform.

3.2.3.10. VRU/Pedestrian Systems

Hardware	Android Smartphone
Compatible services	Road hazard warning Blind spot detection / warning

VRU (cyclist) will receive guidance and information about what is happening in Bilbao. They will use their smartphone to get information about buses location so they can be warned. This situation is expected to happen at several blind spots defined through the city. Moreover, the VRUs will also receive warning messages when there is a road hazard.

3.2.4. Communications schema

In this section, the different communication schema (depending on the use case) that Bilbao will implement is shown. In the figures below, the communication schema for the "Motorway Parking Availability", "Blind Spot / Warning Message Detection" and "Urban Parking Availability" are represented.

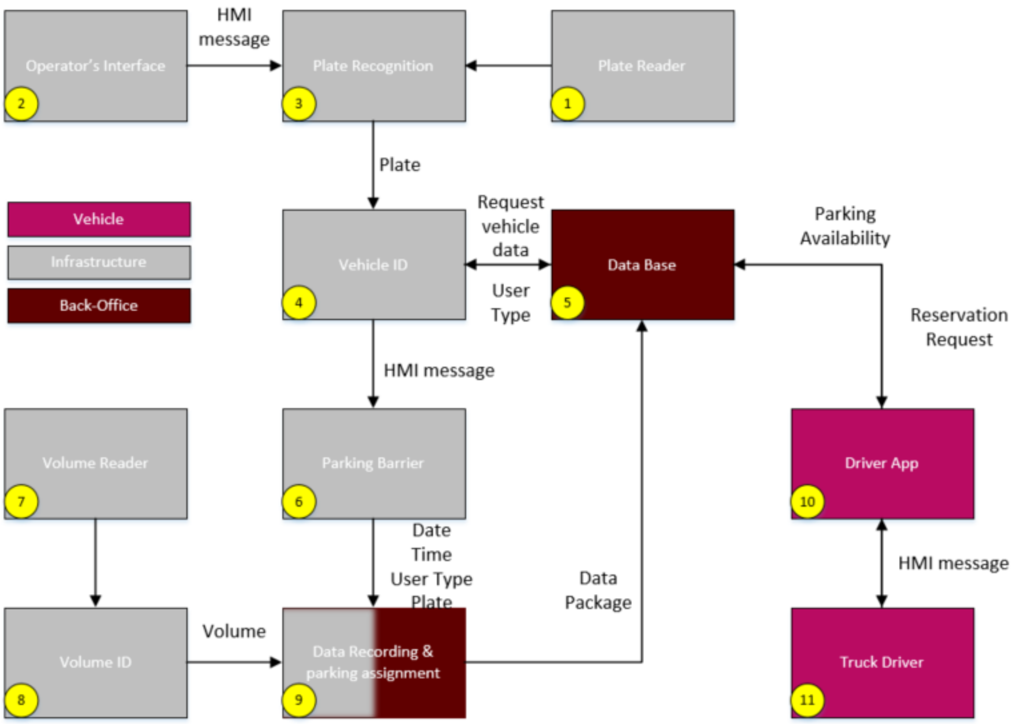


Figure 50: Motorway Parking Availability Communications Schema

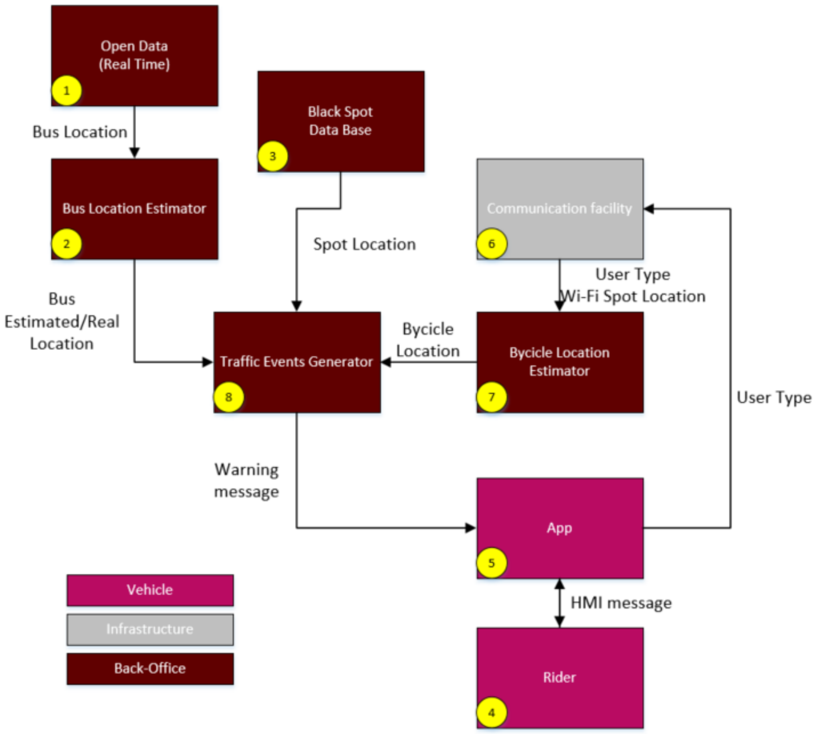


Figure 51: Blind Spot Detection Communications Schema

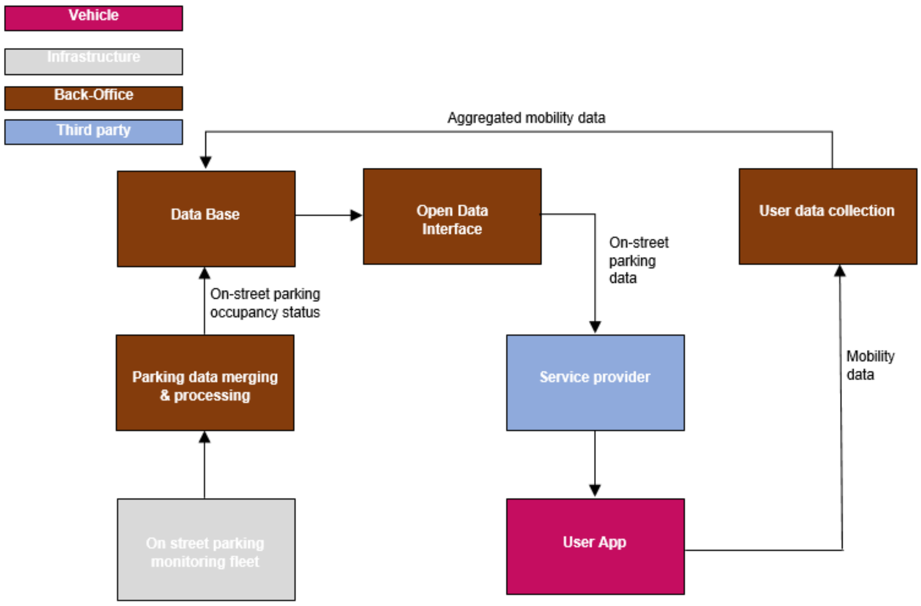


Figure 52: On-Street Urban Parking Availability Communications Schema

The previous communication schemas Figure 51 and Figure 52will be based on cellular communication systems.

3.2.5. Stakeholders' partnership

Bilbao is a complex deployment city that requires some strategic and key partners and associated partners in order to implement, deploy, operate and evaluate the C-ITS services. The complete list for C-MobILE project is the following:

Partners:

/ Bilbao City Council: Public authority provides the necessary means and connections to implement, deploy and successfully test the services in the city of Bilbao. It manages data providers.

/ CEIT: This is Bilbao's deployment site leader, and it is involved in MPA and BSD services.

/ Gertek: Responsible of designing UPA services Apps and the APIs related with the communications between Bilbao council's applications and back-office.

/ Kapsch: This Enterprise manages the information of the back-office related with UPA services.

/ MLC: This Cluster is the responsible of spreading the news about the project.

Associated:

/ Azkar: Interested in the development of the "load" and truck parking deployment and applications.

/ DGT Spain: The government's department that is responsible for the Spanish transport network.

/ San Sebastian City: Interested in the development and status of C-MobILE in Bilbao.

/ Dbus (Pubic bus service provider): Analyses the associated services to the bus public transport.

/ CTVI (parking service provider in motorways): This Company is the owner of the truck parking used for the MPA application development.

3.3. Architecture Bordeaux

The city of Bordeaux, its metropolis and the ring road suffer constant traffic jams and congestions. This is due to heavy truck traffic, higher and higher density of the population, lack of bridges and delay in sufficient road infrastructure. C-ITS is considered as one of the solutions by the 2 authorities managing the roads in the Bordeaux area for congestions but also for safety. For that reason Bordeaux is highly active in several European projects permitting the deployment of C-ITS infrastructure and services. Scoop for safety use cases on the ring road using ITS G5, C-The Difference for deployment of several use cases in Bordeaux and on the ring road using cellular and G5 communication, C-Roads for the deployment of additional use cases in Bordeaux and on the ring road and finally C-Mobile. C-Mobile will permit the deployment of additional use cases but also make all the deployments interoperable so that a user has access to all the C-ITS services deployed.

3.3.1. Deployed services

Bordeaux currently implements Urban parking, Road Work Warning, Road Hazard Warning, Emergency Vehicle Warning, Signal violation warning, GLOSA and In Vehicle Signage. The penetration of C-ITS in Bordeaux city is of 780 users using a smartphone to obtain information from the infrastructure. Communications between devices are essentially done via cellular technology as this is the technology that allows a faster user base expansion. Nonetheless IEEE 802.11p deployment is also available in certain areas of Bordeaux for specific use cases.

Service	Communication	User-equipment	Users
Urban parking	Cellular	Smartphone	780 vehicles
Road work warning	Cellular	Smartphone	780 vehicles
Road work warning	IEEE 802.11p	OBU + integrated system	4 vehicles
Road work warning	IEEE 802.11p	OBU + smartphone	3 vehicles
Road work warning	IEEE 802.11p	ITS roadside station (Scoop)	24 RSUs
Road hazard warning	Cellular	Smartphone	780 vehicles
Road hazard warning	IEEE 802.11p	OBU + integrated system	4 vehicles
Road hazard warning	IEEE 802.11p	OBU + smartphone	3 vehicles
Road work warning	IEEE 802.11p	ITS roadside station (Scoop)	24 RSUs
Emergency vehicle warning	IEEE 802.11p	User smartphone	3 Vehicles
	IEEE 802.11p	EV OBU	6 firetrucks
	IEEE 802.11p	ITS roadside station (Scoop)	13 RSUs
Signal violation warning	Cellular	Smartphone	780 vehicles
GLOSA	IEEE 802.11p	In vehicle OBU	3 vehicles
	IEEE 802.11p	ITS roadside station	13 IRS
GLOSA	Cellular	Smartphone	780 vehicles
In vehicle signage	Cellular	Smartphone	780 vehicles

Table 9: Bordeaux deployed services status

3.3.2. Covered area

Currently, Bordeaux is deploying C-ITS services in the entire urban part of Bordeaux Metropolis and on the ring road around Bordeaux.

C-ITS area	User extension
/ 1 350 Intersections in urban Bordeaux / 33 Km on the ring road	Existing: 780 cars, 6 emergency vehicles Target: +2000 cars, 20 emergency vehicles, 200 pedestrians

Table 10: Covered Area Bordeaux

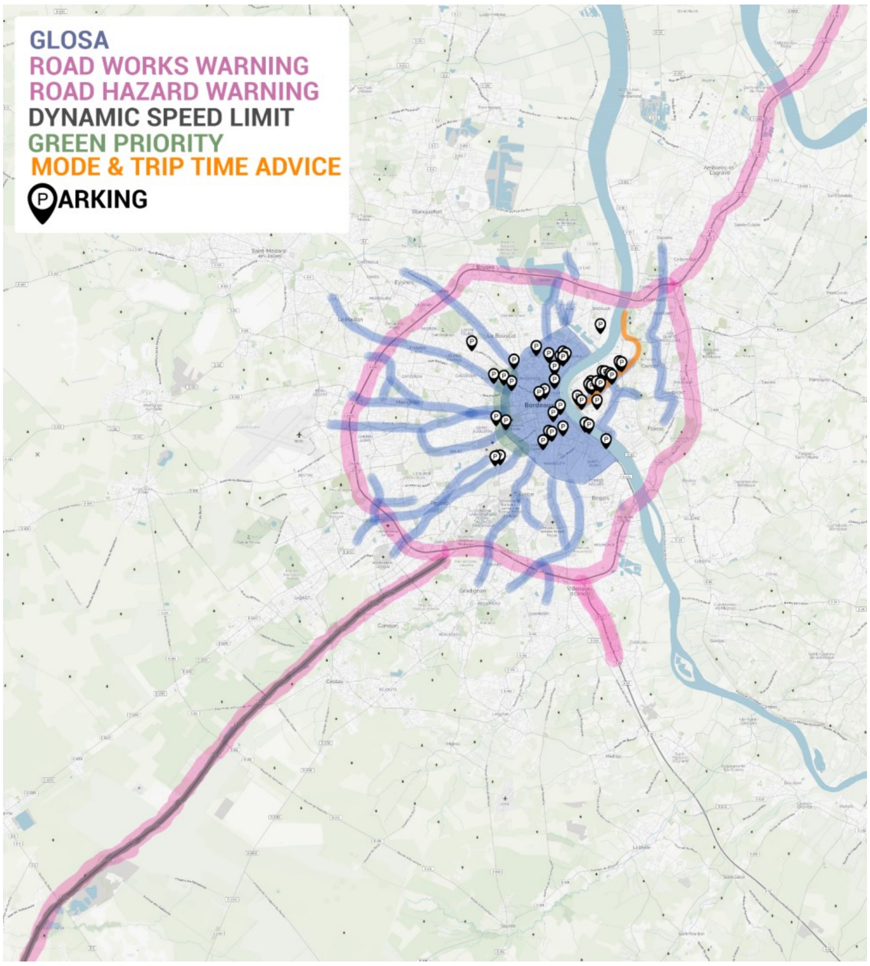


Figure 53: Service deployment per road

The urban area of Bordeaux is entirely covered by cellular communication and provides GLOSA, IVS, Road Works Warning and Red Light Violation. The urban deployment is completed by an ITS G5 road essentially used for emergency vehicles management. The ring road is equipped with 24 RSUs through the Scoop project. The goal in C-Mobile is to propose interoperability between the 2 deployments.

3.3.3. Architecture

The following high-level architecture is valid in Bordeaux where ITS G5 and cellular communication are used for the deployment of C-ITS use cases.

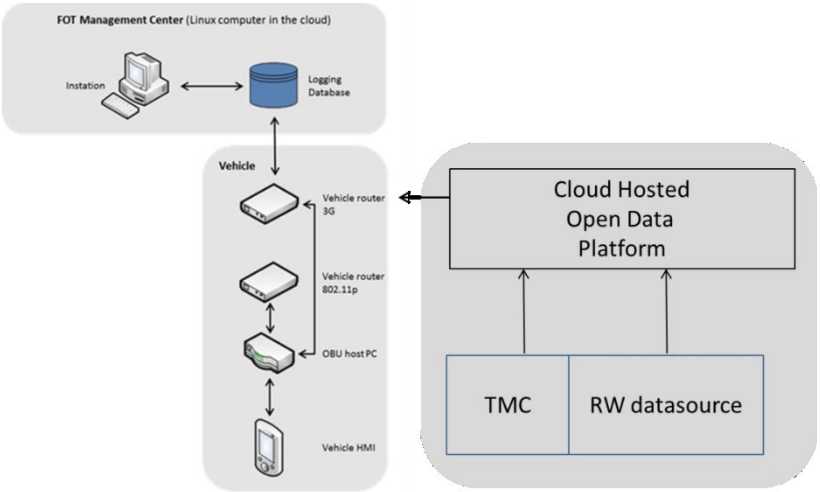


Table 11: High-level architecture in Bordeaux

3.3.3.1. Central Systems

3.3.3.1.1. Open Data Platform of Bordeaux Metropolis

Hardware	Open data server
Relevant services	RWW
Communication flows	Internal format

3.3.3.1.2. Open Data Platform of City of Bordeaux

Hardware	Open data server
Relevant services	30 km/h zones, school areas
Communication flows	Internal format

3.3.3.1.3. Traffic Light TMC

Hardware	Gertrude Server
Relevant services	GLOSA, Green Priority
Communication flows	Internal format

3.3.3.1.4. Ring road TMC

Hardware	TIPI French national TMC
Relevant services	RWW, RHW, IVS
Communication flows	DATEX2

3.3.3.2. Road Side Systems

3.3.3.2.1. Ring-road Road Side Units

Hardware	Road Side Units provided by the Scoop project

Relevant services	RWW, RHW
Communication flows	CAM and DENM over ITS G5

3.3.3.2.2. Urban Road Side Units

Hardware	Road Side Units Scoop compatible
Relevant services	GLOSA, Emergency vehicle approaching, green priority
Communication flows	CAM, SPATEM, MAPEM

3.3.3.3. Vehicle Systems

3.3.3.3.1. User Vehicles without ITS G5

Hardware	Android Smartphone
Relevant services	All services
Communication flows	All data necessary for use cases over cellular network to/from the web server

3.3.3.3.2. User Vehicles with ITS G5

Hardware	Android Smartphone/ integrated HMI + OBU
Relevant services	RWW/RHW
Communication flows	CAM and DENM over ITS G5

3.3.3.3.3. Emergency Vehicles

Hardware	OBU
Relevant Services	Emergency vehicle warning
Communication flows	CAM over ITS G5

3.3.4. Communications schema

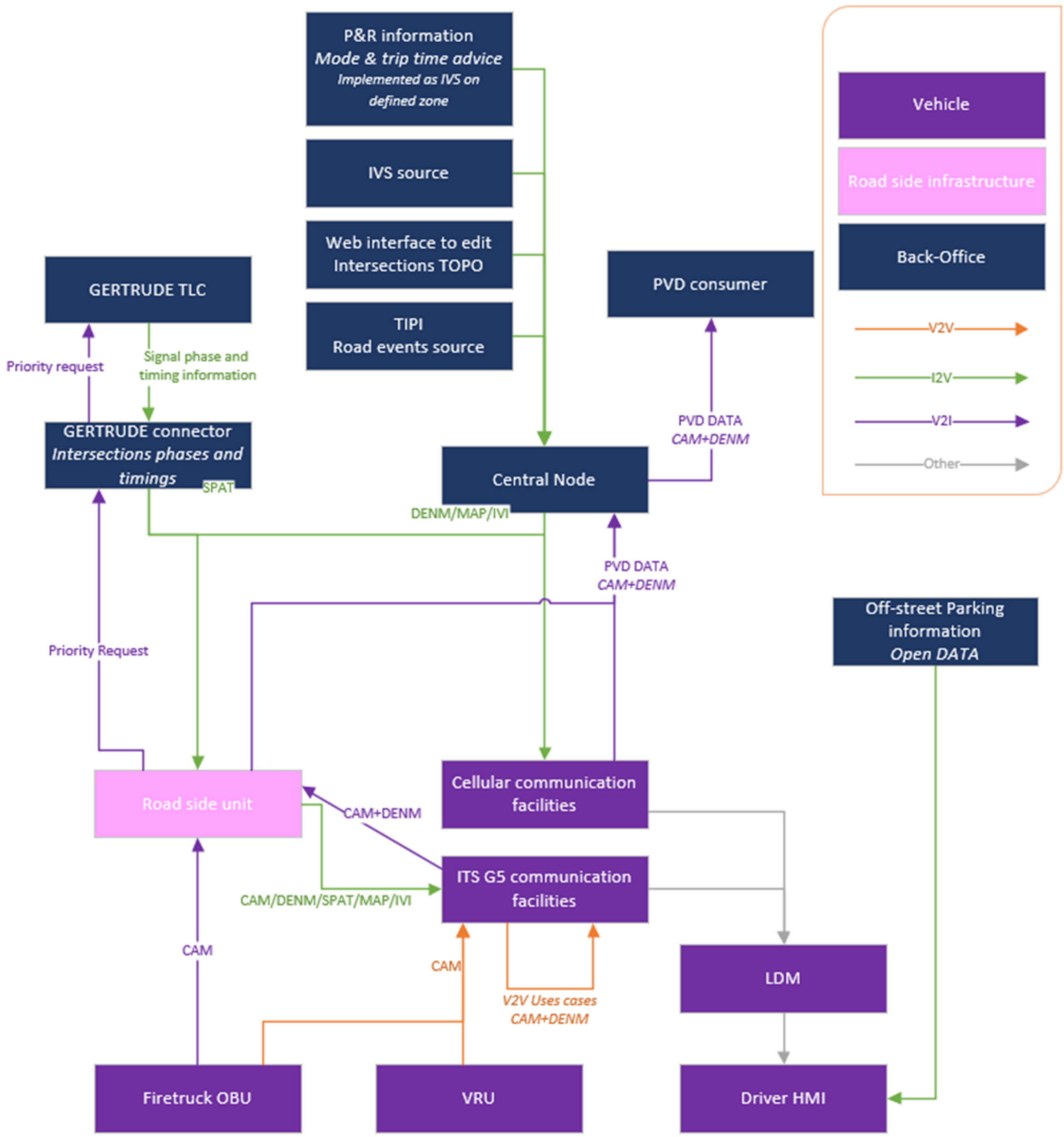


Figure 54: Example of architecture and communication schema

3.3.5. Stakeholders' partnership

Bordeaux deployment site has few partners but many associated partners which have the major role of helping to reach a full scale deployment of C-ITS services. In the near future, other key entities working in Scoop and C-Roads will join this list in order to collaborate and make all deployments compatible and interoperable.

Partners:

- NeoGLS: Deployment site leader and responsible of the development, deployment and management of the C-Mobile services
- Gertrude: Provider of the centralized system which manages the traffic lights of Bordeaux. Provide data for GLOSA and other use cases

Associated:

- / Bordeaux Metropolis: Manages mobility for the Bordeaux deployment site and accepts and follows the deployment of C-Mobile use cases
- / Automobile Club Sud-Ouest: Association responsible of private drivers which will disseminate C-Mobile to its members
- / Kedge Business School: University which will propose the C-Mobile services to their staff and students
- / Université de Bordeaux : University which will propose the C-Mobile services to their staff and students
- / Peugeot Citroen
- / Fédération Nationale du Transport Routier : Association of truck companies which will disseminate C-Mobile to its members in order to find companies which will participate

3.4. Architecture Copenhagen

The city of Copenhagen has the ambition to be CO_2 neutral by 2025. Copenhagen sees C-ITS as a vital part to achieve its ambitious goals. GLOSA and green light priority are key services for reducing emissions. The city has been successful in stimulating bicycle use, which reflects in a modal share far above the European average. This high share results in problems such as congestion on cycle paths, but also opens opportunities to launch services targeted at them.

3.4.1. Deployed services

Copenhagen services are listed in the table below.

Service	Communication	User-equipment	Users
Road work warning	Cellular	Smartphone*	TBD
Road hazard warning	Cellular	Smartphone*	TBD
Warning system for pedestrian	IEEE 802.11p	In vehicle OBU	TBD
Green priority	IEEE 802.11p	In vehicle OBU	87 busses, 2 hybrid vehicles, 47 trucks.
GLOSA	IEEE 802.11p	In vehicle OBU	87 busses, 2 hybrid vehicles, 47 trucks
	IEEE 802.11p	ITS roadside station	49 RSUs
	Cellular	Smartphone IoS	49 RSUs
	Cellular	Smartphone Android	49 RSUs + 11 ImFlow TLCs (Valby)
Cooperative traffic light for pedestrian (also bike)	Cellular	Smartphone IoS	60 cyclists

* Road Works and Road Hazard warning can also be received by OBU when central DENM is copied to RSU.

3.4.2. Covered area

C-ITS area	User extension
/ 49 Intersections / 17.3 Km (inter-) urban roads	Existing: 134 busses and trucks, 2 hybrid vehicles, TBD Users of GreenCatch. TBD bike users of CatchGreen. Target: +200 cars, 100 motorcycles, 175 pedestrians, 25 cyclists, 6000 shared bicycles

Half of the secondary ring road of the City of Copenhagen will be a C-ITS corridor using the implementations from previous implementations in the Folehavn and Compass4D projects and the current ITS Copenhagen project.

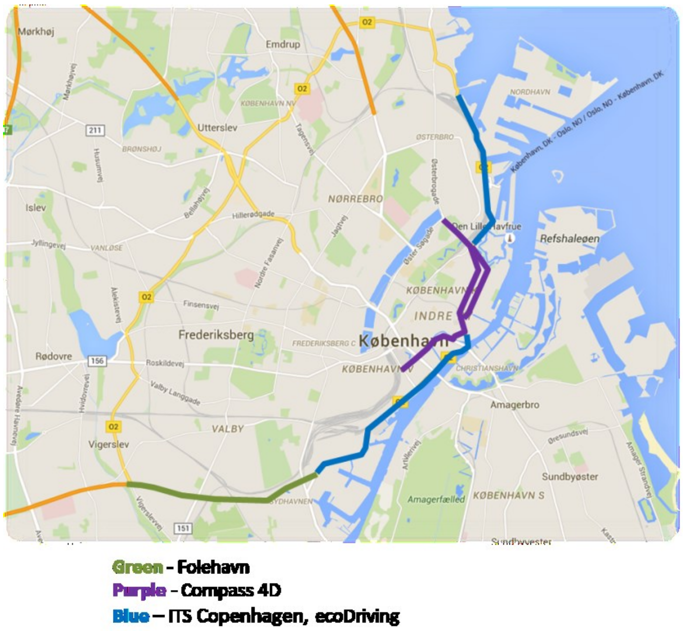


Figure 55: C-ITS corridors in Copenhagen

Along this corridor both regular (ITS-G5 based) and cloud-based (cellular 3G/4G based) ecoDriving will be operational.

On-Board Units	136
Roadside Units	49
User devices	TBD

The Copenhagen Deployment City uses hybrid communications for serving the C-ITS services. Both 802.11p and connected communications are supported. The current high-level site architecture depicted in the following figure shows the elements running in this city in order to offer its services to all kind of end-users.

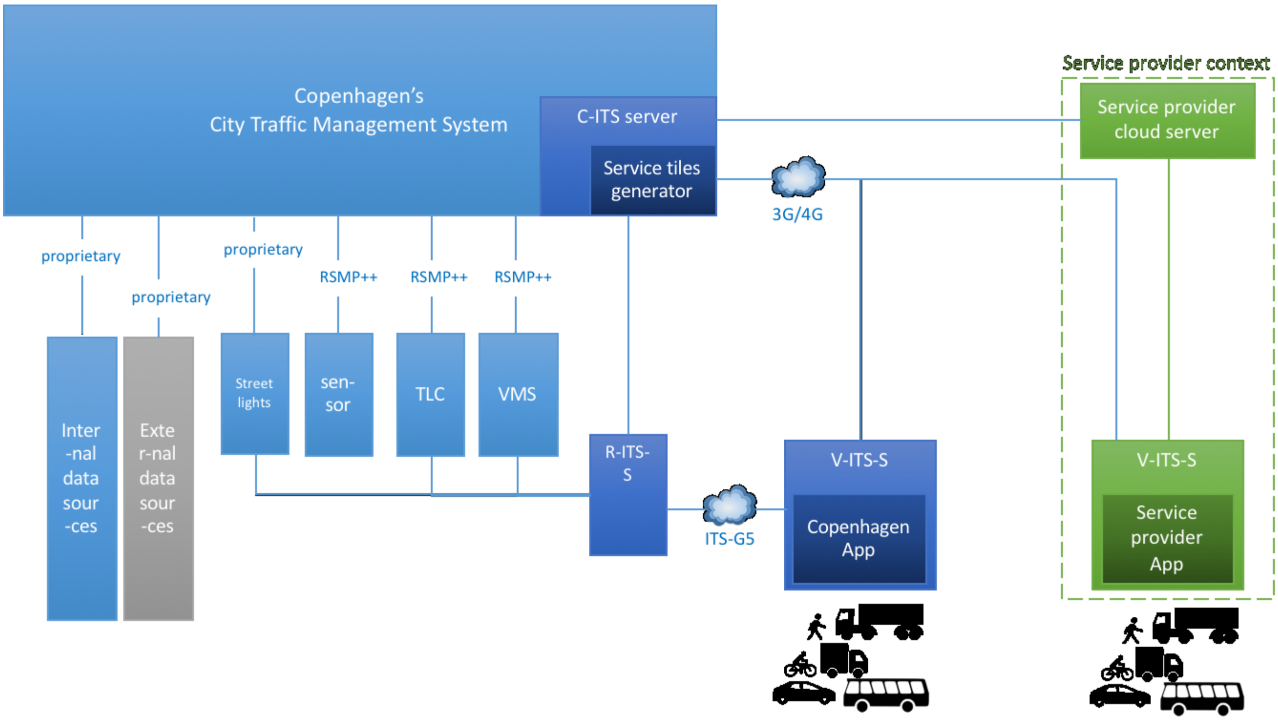


Figure 56: Current Copenhagen architecture

During C-MobILE, the architecture will be opened further to allow multiple vendors to host a GeoMessaging service in the form of a cloud broker. The C-MobILE architecture for Copenhagen is shown in Figure 57.

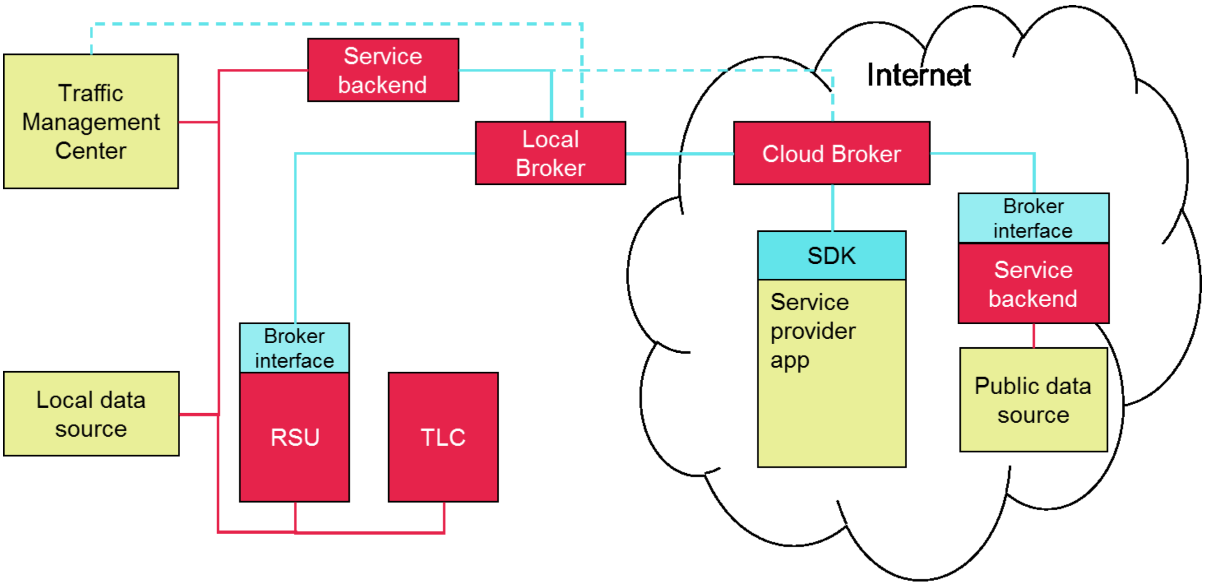


Figure 57: C-MobILE future architecture for Copenhagen

In Figure 57 the local protocols are indicated with a red line, while C-MobILE standardized interfaces have a blue line. An important consideration is that these messages use SAE J2735 standardized messages and are the same as used for IEEE 802.11p/G5. For Copenhagen this concretely means the RSUs can directly forward their MAP and SPaT messages to the broker, because they already encode them for G5. For traffic light controllers without RSU it is still possible to add a “service backend” behind the KK firewall that translates RSMP+ data into MAP and SPaT messages. The local data is collected into a local broker for two reasons; the first is firewalling and security. Having the local broker means the RSUs don’t need individual connections to the internet, only the local broker requires this. Secondly, not all central services need a direct connection to the RSU, saving data and processing power locally. The brokers in C-MobILE have open standards and their implementation is even open source. The City Traffic Management System (CTMS) will still use RSMP+ to get the data from the TLCs. Roadworks and Road Hazard warning have an open data source that is currently connected to the CTMS. This data is also available on the internet and can therefore be fed into C-MobILE using a service backend in the internet as is depicted on the right side of the figure for “public data source”.

3.4.2.1. Central Systems

In this section of the document, the different systems represented in the previous figure present in the deployment site are explained providing information of their function as well as the interaction between them.

3.4.2.1.1. Open Data Platform / Operational Web Server

Copenhagen has a publicly available server with various kinds of data. This can be found at data.kk.dk. Interesting for C-MobILE is that data about roadworks and road hazard should be available on this site as well.

Hardware	Host/Server
Relevant services	RWW, RHW
Communication flows	GeoJSON and CSV.

3.4.2.1.2. TMC

In the current Copenhagen architecture bicycles are connected through the CTMS for route advice and other services.

Hardware	Host/Server
Relevant services	Cooperative traffic light for pedestrian (also bike)
Communication flows	DATEX2 to the Cloud Hosted Open Data Platform

3.4.2.2. Roadside Systems

The previously described corridors have 49 intersections equipped with RSUs. These currently deliver MAP, SPaT and DENM through IEEE 802.11p communications and receive CAM messages of nearby vehicles. This combination enables GLOSA and green light priority. Both are dependent on the Traffic Light Controller that should have time to green information available and support green priority requests. Both can be supported only on a subset of signal groups. The 11 intersections in the Valby area running ImFlow controllers will be connected in the cloud only, because there is no roadside unit present.

3.4.2.3. Vehicle Systems

In Copenhagen the drivers will receive a split set-up in terms of an OBU, FlowRadar and an app on a mobile device. Within the C-Mobile trails it is envisioned that 30 OBU are available within Copenhagen.

3.4.2.3.1. User Vehicles / Trucks / Busses

Hardware	OBU
Relevant services	GLOSA Green priority Warning system for pedestrians RoadWorks/RoadHazard warning
Communication flows	MAP, SPaT, CAM and DENM over IEEE 802.11p

Hardware	iOS / Android Smartphone
Relevant Services	GLOSA Roadworks/hazard warning
Communication flows	MAP, SPaT and DENM over IEEE 802.11p & Cellular network (3G)

3.4.2.4. Bicycle/Pedestrian Systems

The GreenCatch app has been designed for multimodal usage. As such also Bicyclist can use the GreenCatch app to get the information biking towards the traffic lights in terms of green and red lights.

Hardware	iOS smartphone
Compatible services	Cooperative traffic light for Bicyclist (also pedestrians, still need to decide on actual solution)
Communication flows	MAP, SPAT and DENM over cellular network (3/4G).

3.4.3. Communications schema

In Figure 58 the communications among the architectural systems is shown. The messages used are CAM/SPAT/MAP and some proprietary solution among some components.

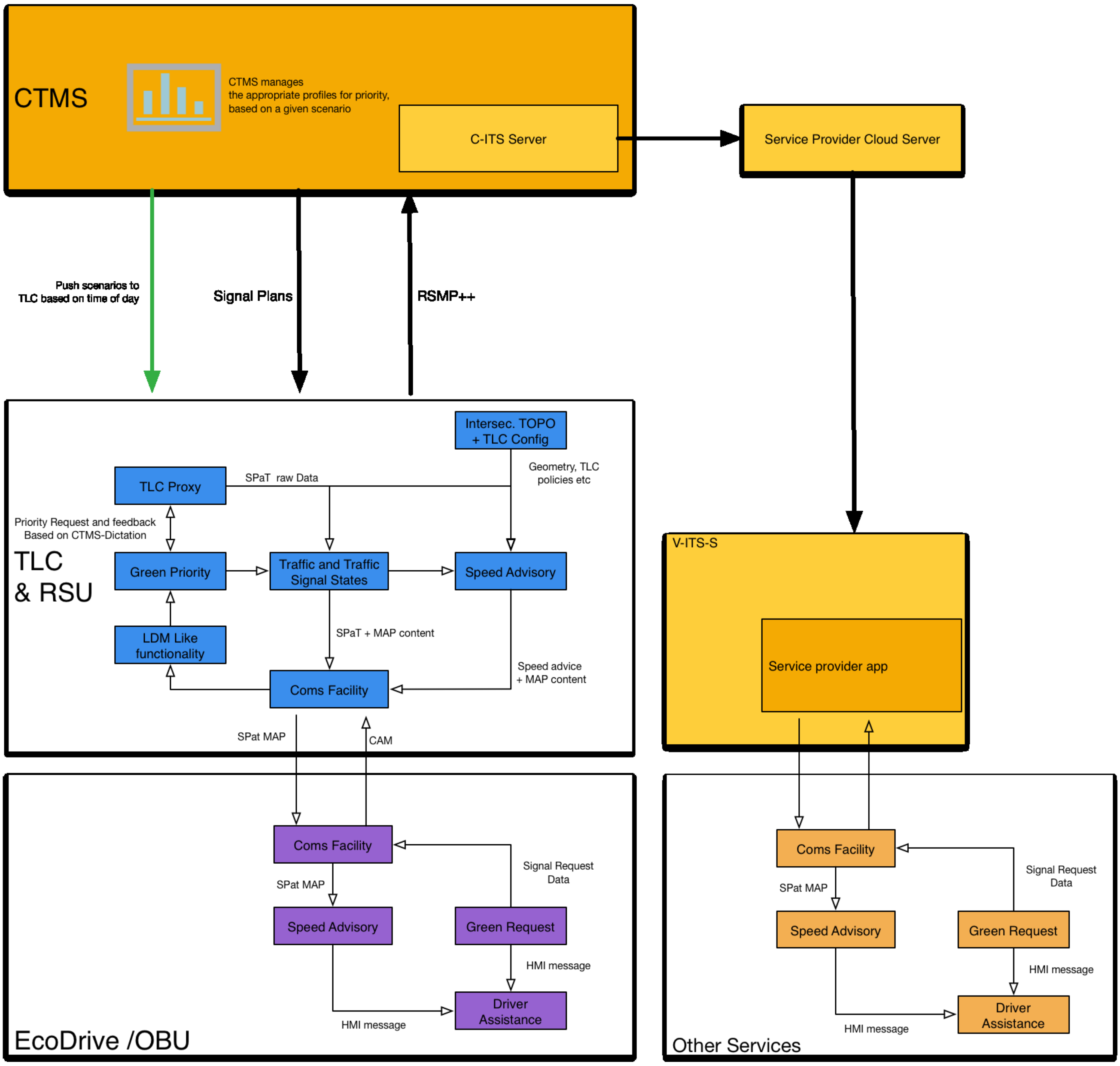


Figure 58: Example of communication schema

3.4.4. Stakeholders' partnership

Copenhagen is a complex deployment city that requires some strategic and key partners and associated partners in order to implement, deploy, operate and evaluate the C-ITS services. The complete list is the following:

Partners:

- Copenhagen City Council: Public authority provides the necessary means and connections to implement, deploy and successfully test the services in the city of Copenhagen. It manages the road network and from that role decides under which conditions a service is allowed. The cities CTMS (Central Traffic Management System) is the central management platform for controlling the various services for the traffic management network. It also provides the gateway for service providers to get access to the on street equipment. The city also has a wide network to make contacts for associated partners and user recruitment.
- Dynniq: Responsible for road works warning, road hazard warning, green priority and GLOSA. Details for warning system for pedestrian and cooperative traffic light for pedestrian/bicycle are still to be agreed.
- Technolution: As a technology partner for the city of Copenhagen Technolution is responsible for delivering and maintaining the CTMS and the delivery of the multimodal GreenCatch application.
- Other C-MobILE partners: Due to interoperability between test sites in C-MobILE any service provider with an app can use the data available and let its users benefit from the services offered.

Associated:

- / The association of Copenhagen Truck Drivers.
- / Copenhagen Public Bus Service Provider.
- / Danish Pedestrian Federation.
- / Copenhagen cyclist association

3.5. Architecture Newcastle

Situated in Tyne and Wear, in the north-east of England, Newcastle has a population of approximately 295,000, within a wider metropolitan area of approximately 1 million. This area has significant issues with congestion at peak times and consequent issues with air quality. Newcastle City Council is the lead authority for the Tyne and Wear Urban Traffic Management Control (UTMC), which includes Gateshead, North and South Tyneside and the City of Sunderland as well as the city of Newcastle.

The city has a good mode share of public transport. However, the bus service often suffers delays at peak times and this reduces the attractiveness of these services.

In addition to this, there are reported delays for emergency service vehicles and freight and taxi vehicles, which impede their effectiveness and the competitiveness of the city.

The city wishes to be at the forefront of innovative transport investment and see C-ITS services as one part of this wider jigsaw of innovation. Working with academic partners, including Newcastle University Faculty of Science, Agriculture and Engineering and the Newcastle Urban Observatory we wish to complete the circle through policy making, implementation, monitoring and evaluation.

3.5.1. Deployed services

Newcastle currently implements Road Work Warning, Green Priority, GLOSA, Road Work/Hazard Warning and Blind Spot Detection/Vulnerable Road User Warning.

The penetration of C-ITS

Service	Communication	User-equipment	Users
Road work warning	Cellular	Smartphone/HMI	13 Ambulances
Road hazard warning	Cellular	Smartphone/HMI	13 Ambulances
Green priority	IEEE 802.11p	In vehicle OBU	13 Ambulances
Green Priority	IEEE 802.11p	ITS Roadside Unit	39 RSUs
GLOSA	IEEE 802.11p	In Vehicle OBU	13 Ambulances
	IEEE 802.11p	ITS Roadside Unit	39 RSUs
Blind Spot detection	Cellular	Standalone	35 Buses

3.5.2. Covered area

Newcastle has deployed C-ITS architecture on 2 radial corridors to the City Centre:

C-ITS area	User extension
/ 39 Intersections / 7 Km urban roads	<u>Existing</u>: 13 Ambulances, 2 shared cars, 50 cyclists <u>Target</u>: 35 Buses, Up to 10 Taxis, Up to 10 Freight vehicles

These corridors are shown in yellow above.

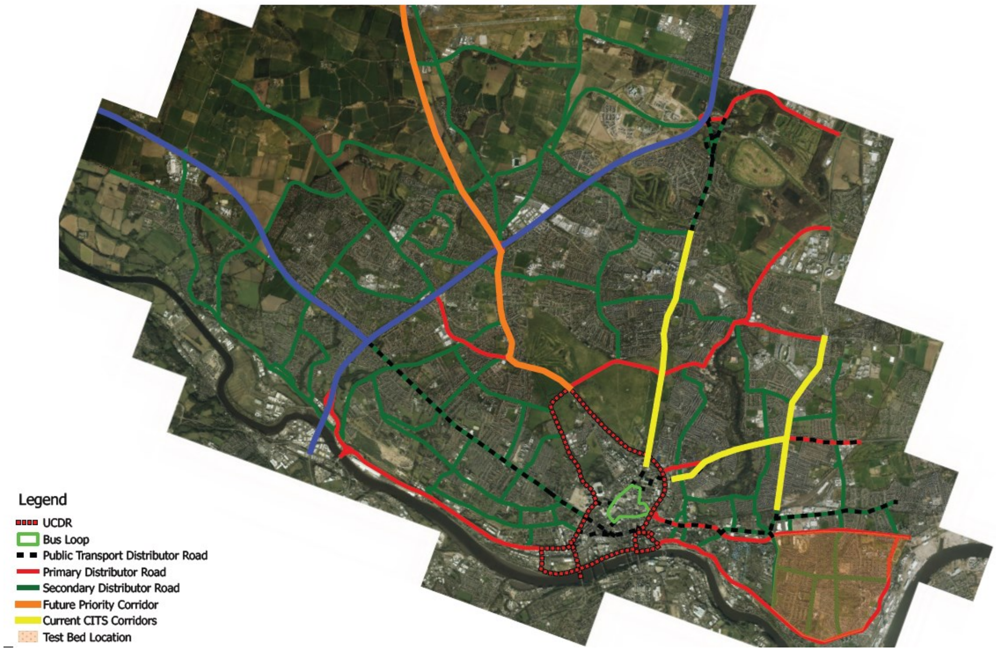


Figure 59: Newcastle C-ITS deployment area

3.5.3. Architecture

The high-level site architecture depicted in the following figure shows the elements running in this city in order to offer cellular-based services to all kind of end-users.

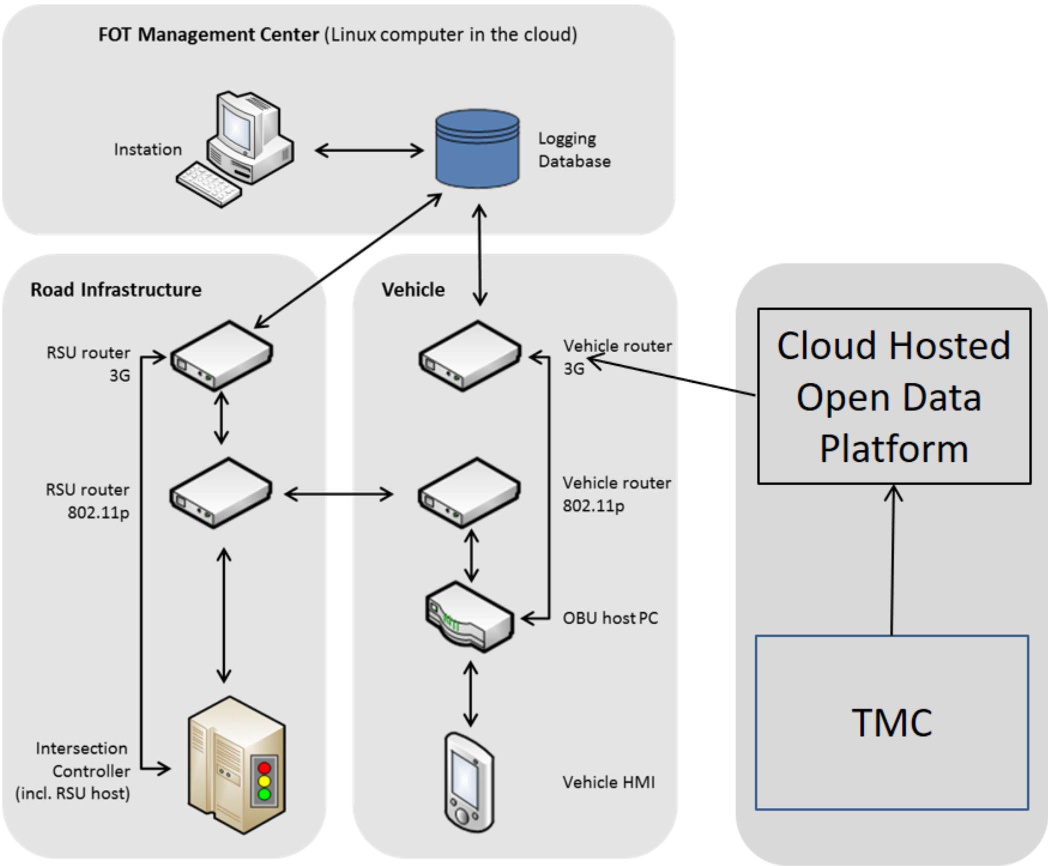


Figure 60: Architecture in Newcastle

3.5.3.1. Central Systems

In this section of the document, the different systems represented in Figure 60 present in the deployment site are explained providing information of their function as well as the interaction between them.

The hardware architecture is shown in the figure above. One back-office (instation) is used, which will be realised as a LINUX computer in the Internet cloud. This computer will be connected via 3G (UMTS) communication. The instation communicates with both sub-systems, the road-side and vehicle one. On this LINUX computer a spatial PostGis database will be installed to store the logging data for further evaluation.

The RSU host (application computer) is fully integrated in the intersection controller. The controller is connected with a 3G and IEEE 802.11p-capable router via Ethernet.

The in-vehicle systems consist of a 3G router, an IEEE 802.11p-capable router, the OBU host PC to run the services on, and an HMI.

3.5.3.2. Interface IEEE 802.11p WLAN

The Scalance Communication Unit supplied by Siemens implements the protocol IEEE 802.11p (ITS G5) amendment for ITS applications to the IEEE 802.11 Wi-Fi standards. The 802.11p amendment provides low-latency data exchange capabilities by removing the need to wait for the usual Wi-Fi association and authentication procedures to complete.

The UDP interface of the Scalance Communication Unit allows configuration of the transmission and reception of the 5.9 GHZ air interface, including configuration and status information of the Scalance. An attached device such as a pc may register itself via UDP communication with the Scalance Communication Unit for forwarding of received messages from the neighbouring ITS G5 devices over the air. A detailed specification of the interface is given in the Siemens internal document “V2X Device user interface” (Version 05_00_01).

3.5.3.3. Interface Instation

This system element provides connectivity to the instation for data-logging, monitoring and firmware upgrade.

A data structure for the Newcastle deployment site can be seen in the following figure:

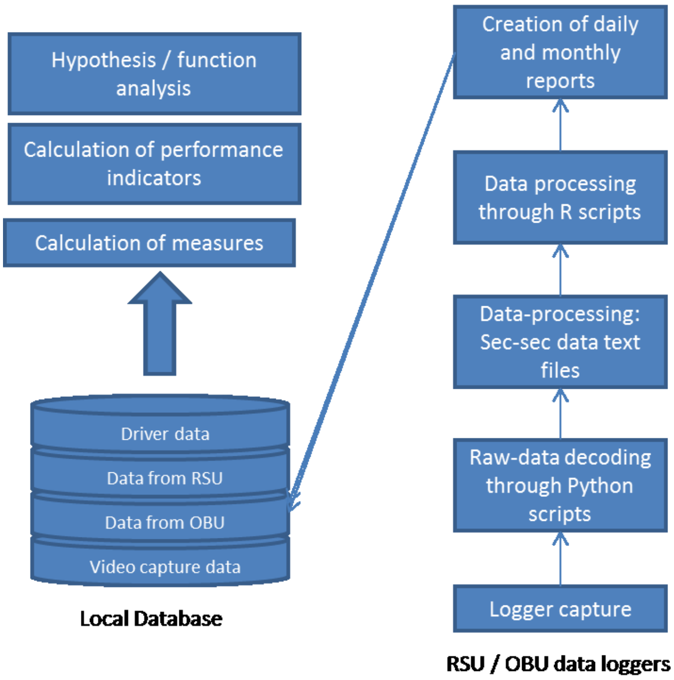


Figure 61: Logging Information Flow

3.5.3.4. Vehicle Systems

A total of 13 vehicles have been equipped in Newcastle thus far, 11 non-emergency vehicles from the North East Ambulance Service (NEAS) and 2 electric vehicles from Newcastle University. Work is currently ongoing to equip 35 express buses.

Each vehicle is fitted with an antenna, OBU and HMI.

Figure 62: Vehicle Installation Architecture

NEAS vehicles have the OBU mounted in an existing equipment box and Newcastle University vehicles will utilise a separate storage compartment within the boot of the electric vehicle.

In all cases the driver is responsible for the mounting of the OBU.

Tyne and Wear TMC staff is responsible for all firmware and software updates to both HMI and OBU.

3.5.3.4.1. Ambulance Vehicles

Hardware	Android Smartphone (HMI), OBU
Relevant services	Road work warning Road hazard warning GLOSA Green Priority
Communication flows	CAM and DENM over Cellular network (3G) to/from the web server

3.5.3.4.2. Bus Vehicles

Hardware	Android Smartphone (HMI), OBU

Relevant Services	Road work warning Road hazard warning GLOSA Green Priority Vulnerable road user warning (cyclist)
Communication flows	CAM and DENM over Cellular network (3G) to/from the web server; RFID from VRU system tag

3.5.3.5. VRU/Pedestrian Systems

Hardware	Cyclealert tag
Compatible services	Vulnerable Road User Warning
Communication flows	RFID when moving to Bus sensor

3.5.4. Communications schema

The Newcastle deployment site consists of 39 locations equipped with Siemens UK controllers and (at most sites) associated DUSC OMUs (Dial-up strategic control Outstation Monitoring Units).

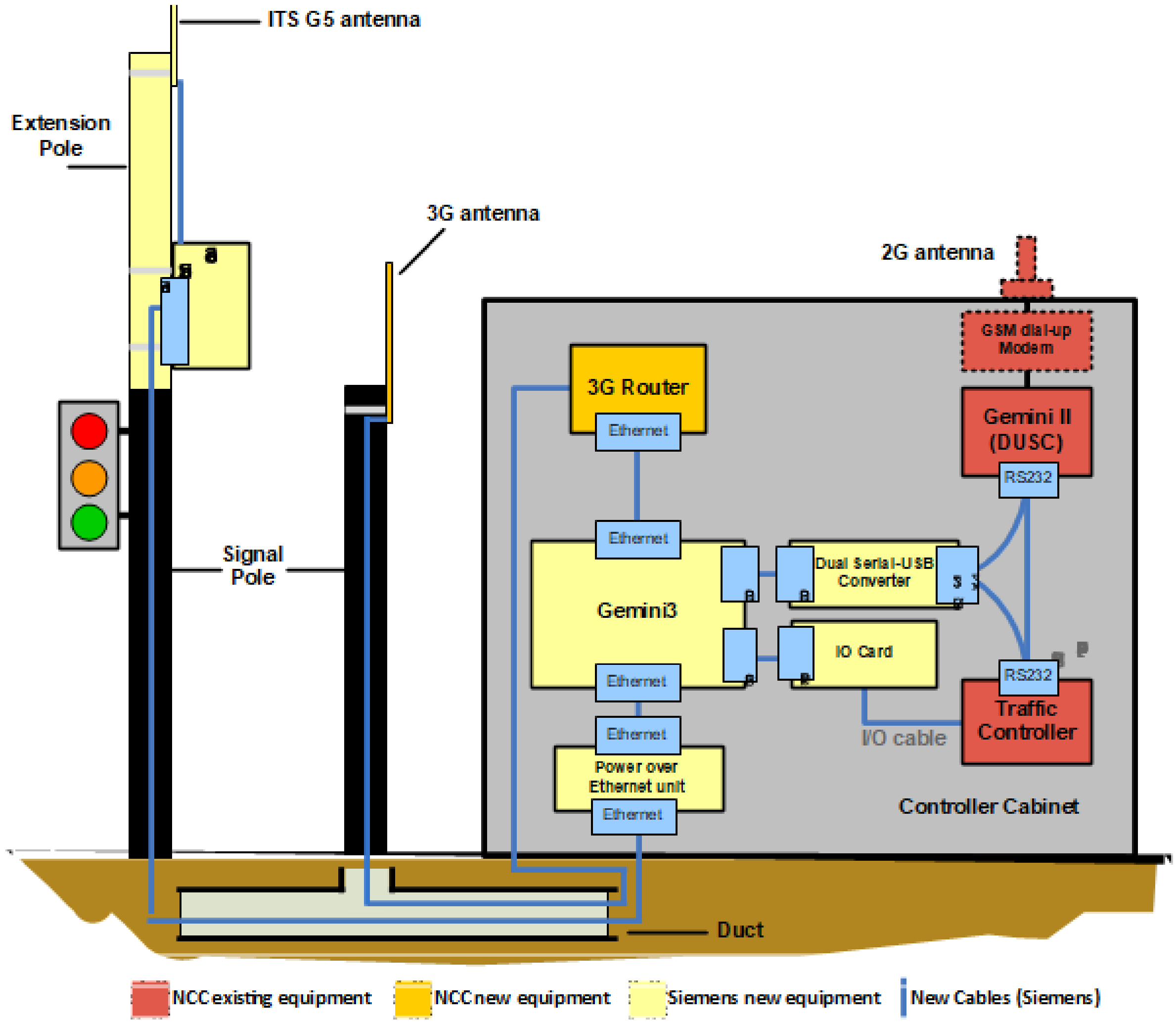


Figure 63: The roadside infrastructure sub-system.

The Gemini3 processor unit monitors Stage (similar to European "Phase") force and confirm information on the serial link between Traffic Controller and DUSC OMU unit to predict Signal Phase and Time information. Where the OMU is not present the serial interface must be configured via TLC configuration.

The ITS Services application runs on the Gemini3 unit and processes both SPaT information and cooperative system messages received by the Scalance Communication Unit.

Requests for EEIS priority received from vehicles equipped with OBUs are processed by the ITS application and if accepted result in activation of a Traffic Controller IO input (controller configuration will be adapted to correctly process these inputs).

Logging, firmware update and maintenance will be performed over the 3G communication link.

The following design decisions have been taken:

The Scalance Communication Unit shall be connected with the TC via Ethernet. The Scalance does not create messages itself, but only formats the messages it receives for transmission.

ITS Services is started by the TC Proxy as a separate Linux process and therefore does not execute unless / until the TC Proxy has been started by the program framework GVP.

ITS Services is written in C/C++ and uses POSIX calls (those supported by the Linux OS).

/ The ITS Services process streams logging messages to its standard output. TC Proxy monitors this output and interprets the received messages to determine where the associated data is to be sent. The logging messages are sent then to the Logging Instation via a 3G wireless link. ITS Services has no knowledge of the 3G communications.

/ ITS Services will make use of the GVP System Log facility to record faults, notification, warning and info level information. To distinguish between logging data destined for the Logging Instation and GVP System Log messages the ITS Services process prefixes messages with an identifier. Messages destined for the System Log require further resolution in terms of a category i.e. fault, notification, warning or information.

/ TC Proxy monitors the correct operation of ITS Services, restarting the process if abnormal operation is detected. A heartbeat message is used for this type of monitoring that can be sent periodically.

/ ITS Services uses a Local Dynamic Map (LDM). The static data element of the LDM is generated manually. ITS Services accesses this file from the file system during start-up.

The following figure shows the system architecture of the road-side subsystem in Newcastle:

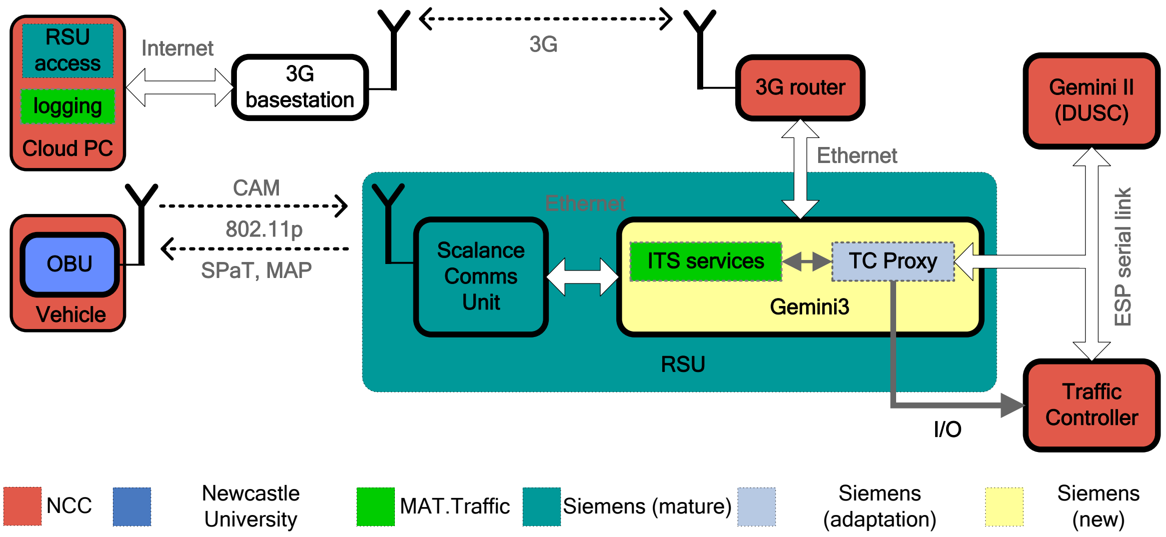


Figure 64: System architecture of the road-side subsystem in Newcastle.

The Gemini3 unit sniffs Stage (Signal Group) force and confirm information on the ESP serial link between Traffic Controller and the Gemini2 unit to predict Signal Phase and Time information.

The ITS application written by MAT.TRAFFIC runs on the Gemini3 unit and processes both SPaT information and cooperative system messages received by the Scalance ITS G5 Radio.

Requests for priority received from vehicles equipped with OBUs are processed by the ITS application and if accepted result in activation of a Traffic Controller IO input (the Controller configuration will be adapted to correctly process these inputs).

Logging, firmware update and maintenance will be performed over the 3G communication link.

Flows of data are illustrated below:

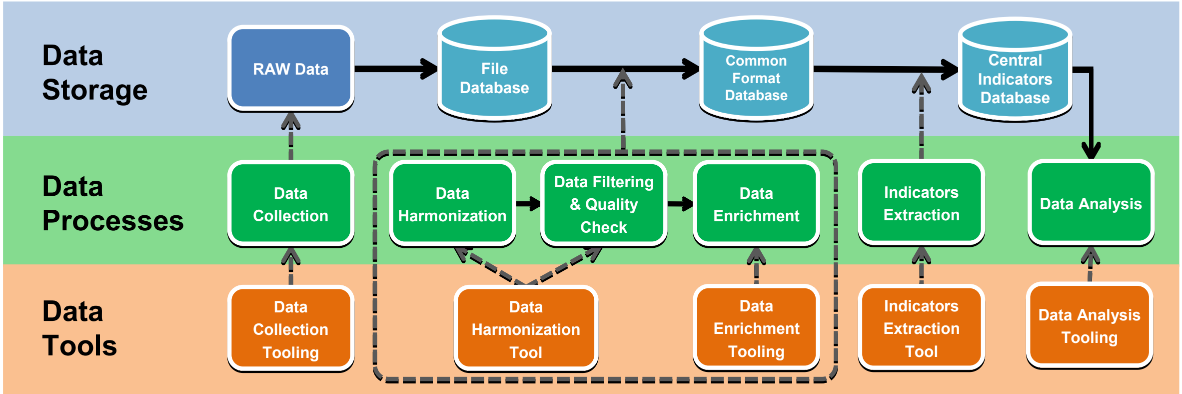


Figure 65: Newcastle Communication flows of Data

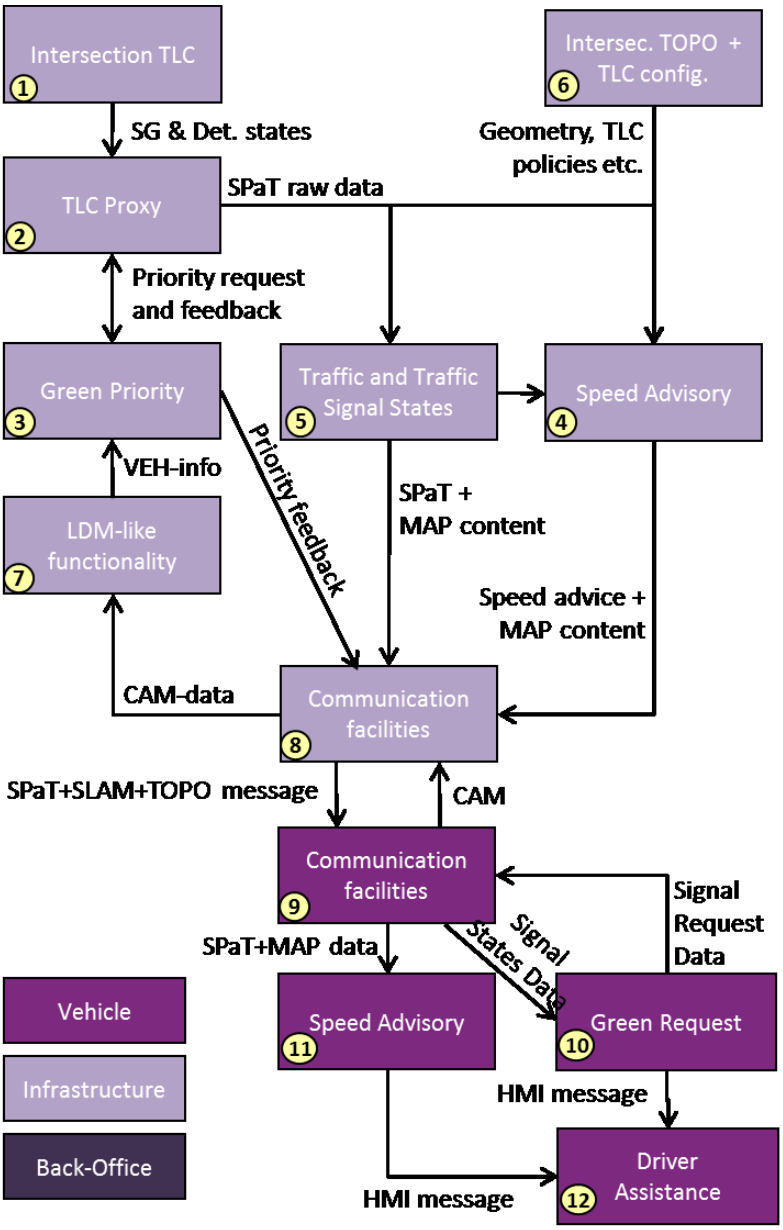


Figure 66: Newcastle Communications Schema (originally from Compass4D)

3.5.5. Stakeholders' partnership

Newcastle as a deployment site has a number of partners who are involved in the delivery of the work.

Partners:

- Newcastle City Council – Local Authority and responsible legally for the management of roads within the city. Manages the project and provides an interface between local partners.
- Tyne and Wear Urban Traffic Management Centre (UTMC or TMC) – Responsible for the technical back-office of the majority of systems involved in the work. Responsible for ensuring the smooth flow of traffic on roads within the wider sub-region (population 1 million). In charge of cloud hosted open data platform. UTMC employees are also employees of Newcastle City Council.
- Newcastle University – Full partner of C-MobILE project. Also assists Newcastle City Council in the provision of evaluation services for the data generated by the Newcastle deployment site. Has 2 OBUs for testing on Newcastle University vehicles
- North East Ambulance Service – Has active set of OBUs used in Compass4D, willing to use the developed C-ITS services.
- Arriva Buses (Deutsche Bahn) – Has a set of users (express buses) willing to use the C-ITS services developed to aid reliability of express bus services into the city
- NODA Taxis - Has a set of users (taxi drivers) willing to use the C-ITS services developed to aid reliability of taxi services in off peak hours into the city centre
- Greggs (Freight) -Has a set of users (freight drivers) willing to use the C-ITS services developed to aid reliability of service deliveries in off peak hours

Associated:

- Highways England: Responsible for the maintenance of strategic roads within the UK
- North East Freight Partnership: Representative body for the freight industry within the North East
- Siemens: Developer of the Road Side Units and the majority of traffic services infrastructure in the North East
- Dynniq: Developer of the On-Board Units

3.6. Architecture North Brabant

Important highways for transport between the harbour of Rotterdam, through Venlo to Germany are running through North-Brabant. Besides, these high-ways are also crowded with commuting traffic between the large cities Tilburg, Eindhoven, and Venlo as well as between the south of the Netherlands and the more densely populated west part of the Netherlands. Further, in the Netherlands cycling is also a popular way of commuting, especially within the cities. Due to the traffic being mixed in the cities, cyclists and pedestrians are at risk of being hit by a vehicle, despite the entire infrastructure. The highways as well as the large cities in North-Brabant, like Helmond, Eindhoven and Tilburg, suffer from traffic jams and congestions. Besides the economic loss, the citizens suffer from polluted air. North-Brabant sees C-ITS as a possibility to mitigate these problems, and therefor built several deployment sites where C-ITS services aimed at increasing safety, mitigating congestion, and/or reducing environmental issues can be tested. The deployment sites in North-Brabant are shown in Figure 67. Helmond in specific has a large share of ongoing traffic due to the A270 highway continues through the city centre as N270 connecting Eindhoven, Helmond, Deurne and Venray. Because there is also a high share of heavy goods traffic, the air quality is of special attention. Therefore, Helmond has already started investing and cooperating in many C-ITS projects since 2006 with green priority for trucks as the main service. This report provides information on the current status of the North-Brabant deployment site.

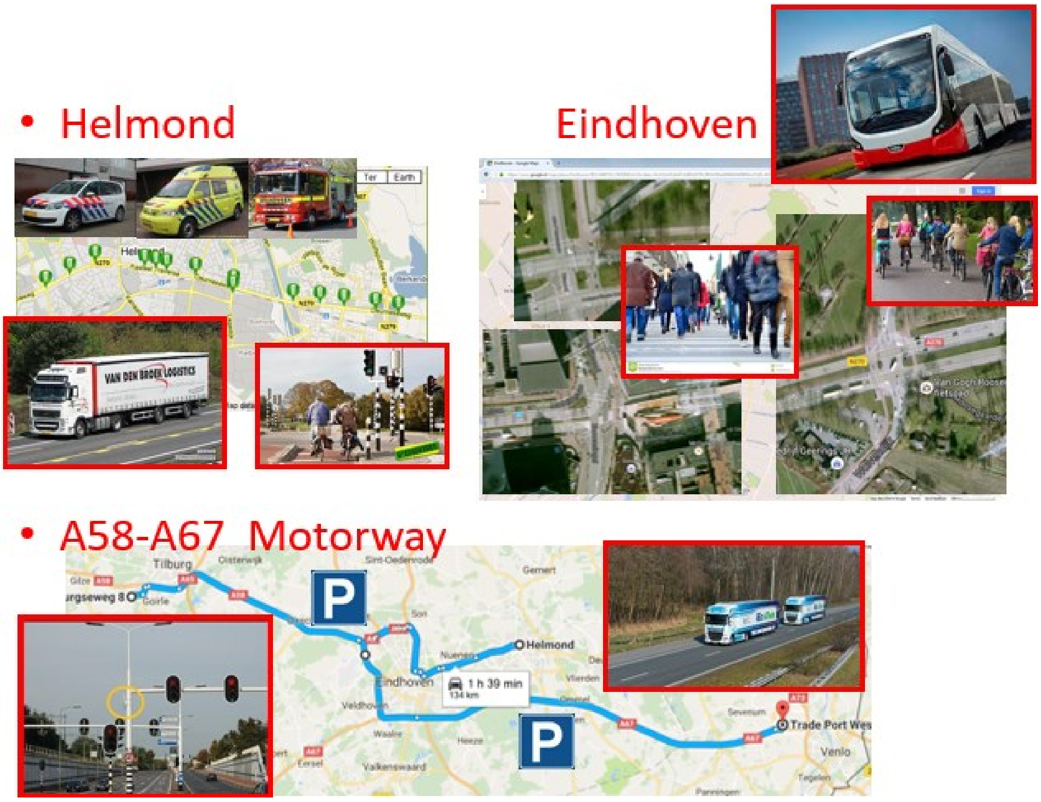


Figure 67: North-Brabant deployment sites locations

Next table provides an overview and high-level description of the current services in the North-Brabant deployment site. The services that will not be deployed in North-Brabant are not included in this table. Some services are new and have currently no installed base and therefore have dashes in the communication, user-equipment and users cells.

<table>
<tr><th colspan="2">Service</th><th>Communication</th><th>User-equipment</th><th>Users</th></tr>
<tr><td colspan="2">Rest time Management</td><td>Cellular</td><td>Smartphone</td><td>Truck drivers</td></tr>
<tr><td colspan="2">Motorway parking availability</td><td>Cellular</td><td>Smartphone</td><td>Truck drivers</td></tr>
<tr><td colspan="2">Road works warning</td><td>G5</td><td>OBU</td><td>Trucks and Emergency Vehicles</td></tr>
<tr><td colspan="2">Road hazard warning</td><td>G5</td><td>OBU</td><td>Trucks and Emergency Vehicles</td></tr>
<tr><td colspan="2">Emergency vehicle warning</td><td>G5</td><td>OBU</td><td>Emergency Vehicles</td></tr>
<tr><td colspan="2">Signal violation warning</td><td>G5</td><td>OBU</td><td>Trucks and Emergency Vehicles</td></tr>
<tr><td colspan="2">Warning system for pedestrians</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
<tr><td colspan="2">Green priority</td><td>G5</td><td>OBU</td><td>Trucks and Emergency Vehicles</td></tr>
<tr><td colspan="2">Green light optimal speed advise (GLOSA)</td><td>G5 + cellular</td><td>OBU and/or smartphone</td><td>Trucks and Emergency Vehicles (cellular/smartphone is experimental MOBiNET system without active users)</td></tr>
<tr><td colspan="2">Cooperative traffic light for VRU</td><td>Cellular</td><td>Smartphone</td><td>Selected group of elderly pedestrians and recruited cyclists</td></tr>
<tr><td colspan="2">Urban Cooperative Adaptive Cruise Control (U-CACC)</td><td>ITS-G5 for V2V, currently no I2V</td><td>OBU</td><td>Min. 2 vehicles (platoon)</td></tr>
<tr><td colspan="2">Truck Platooning</td><td>ITS-G5 for V2V, currently no I2V</td><td>OBU</td><td>Min. 2 trucks (platoon)</td></tr>
<tr><td rowspan="2">Motorcycle approaching indication</td><td>V2V</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
<tr><td>V2I</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
<tr><td colspan="2">Blind Spot detection</td><td>TBD</td><td>TBD</td><td>TBD</td></tr>
</table>

	TBD	TBD	TBD

Table 12: Overview and high-level description of the services deployed

3.6.1. Covered area

Currently, North-Brabant is deploying C-ITS services at the main roads or ring, and some intersections in Helmond, and the highway between Eindhoven and Venlo.

C-ITS area	Users
/ 27 Dynniq Intersections / 20 Dynniq km (inter-) urban roads	Trucks, emergency vehicles (fire brigade), and 26 VRU's

Most of the services currently deployed in North-Brabant use ITS-G5, but can be easily upgraded to be available on the cellular network as well. The smartphones obtain the data from the ICS (ITS Central Station) and regularly send position updates. GLOSA has already been deployed using cellular communication, but this was an experimental implementation for MOBiNET, which never had external users other than testers/developers.

On-Board Units	103
Roadside Units	27 x Dynniq
User devices	26 Smartphones for VRU's

For the Highway deployment site, C-MobILE is in contact with the InterCor project coordinating the highway developments in The Netherlands. The RSUs currently deployed are not under control of the C-MobILE consortium, but also don't need to be. On IEEE 802.11p, the standards are currently clear and any C-MobILE OBU can receive and use the messages disseminated here. There is cooperation for the Cloud-based solutions of this test site. The Dutch Traffic Datawarehouse (NDW) will publish all available data for the RWW, RHW and IVI on an open interface. C-MobILE will connect to this interface to also offer this service through the cloud. Details about conversion of geo-references and encoding of the messages still have to be worked out.

Figure 68: Helmond urban deployment site, main road and intersections

The CrossWalk and CrossCycle services in Tilburg improve safety and comfort for VRUs. CrossWalk is intended for pedestrians that need more time to cross an intersection. This can be due to disability, but also school teachers can use it to cross with their entire class. The pedestrian has to install an app and only needs to activate it before the start of the trip. No interaction is required with the smartphone during the trip. The app publishes CAM messages in the cloud server when in the proximity of the intersection. This data is fused with the local detection data and used to extend the green phase for a safe crossing. CrossCycle works similarly, but is used for comfort of cyclists. They also don't need to interact with their phone during the trip. The app will inform the traffic light controller through the cloud server of their pending arrival at the intersection. This information will be used to switch the light to green quicker for the cyclists. It can also help detect the number of cyclists arriving, giving higher priority when larger groups are present.

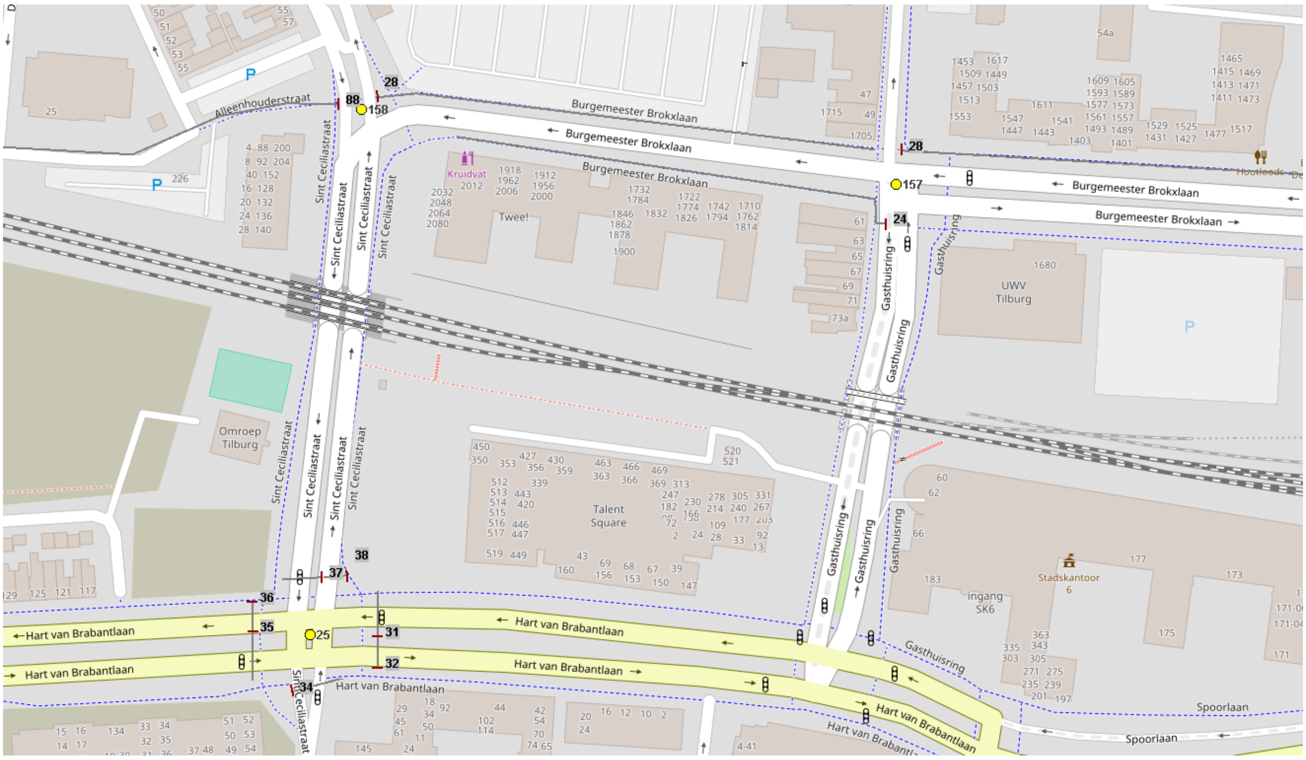


Figure 69: CrossWalk at intersection 25 and CrossCycle at 157 and 158 in Tilburg

3.6.2. Architecture

The North-Brabant Deployment site is mainly focused on the cellular communications for serving the C-ITS services. The high-level architecture in North Brabant is depicted in Figure 70. This picture shows the elements running in the deployment site in order to offer cellular-based services to all kind of end-users.

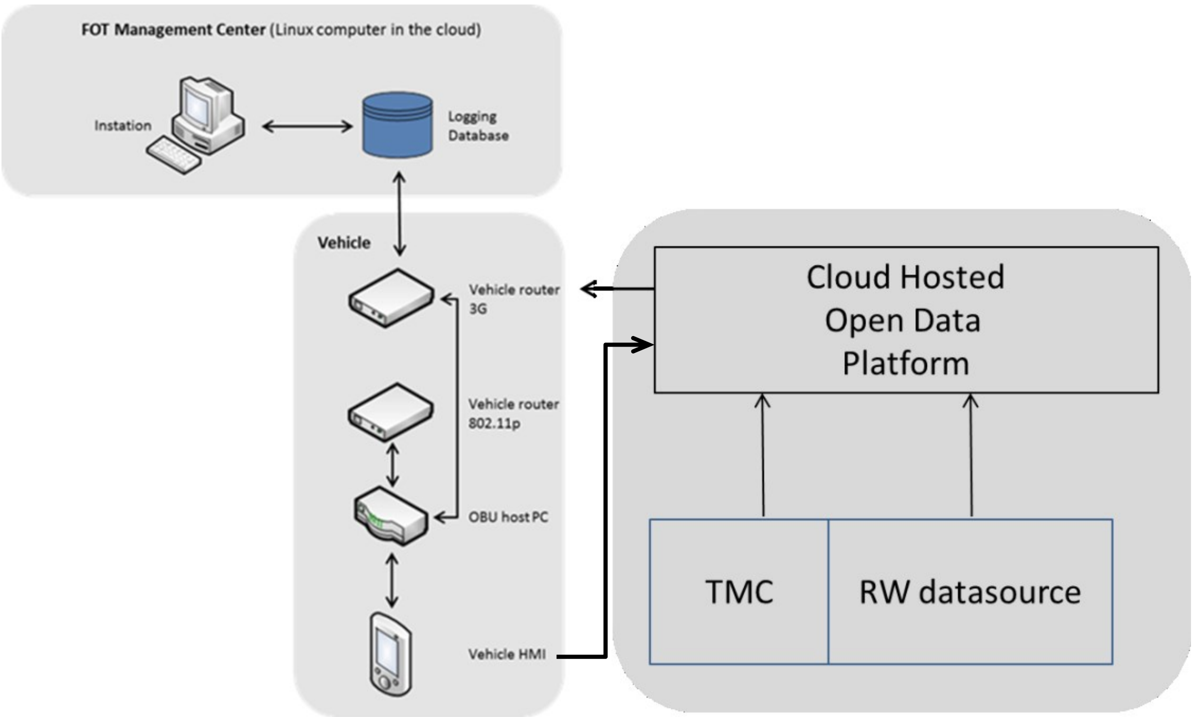


Figure 70: High-level vehicle-centric architecture of the North-Brabant Deployment site.

Figure 71 shows the high-level architecture for the North-Brabant test site from an infrastructure point of view. OBUs connect directly to the RSU using ITS-G5. Some services are very time-critical and can only be provided using this direct communication. This is the case for pedestrian warning, blind spot detection and CACC services, Smartphone users connect through the Communication Manager and Communication Agent in the MOBiNET architecture. Services like the roadworks and hazard warning and in-vehicle signage would use the service provider block at the top of the figure, since all blue MOBiNET blocks have internet connectivity and their data is available in a publicly accessible data source. GLOSA, emergency vehicle warning and green light priority use direct connections with the RSUs through a VPN connection to share the information via cellular communication. A traffic light controller without RSU can connect through a separate backend in the city's back office, but this was not deployed in North-Brabant (only in Trondheim for MOBiNET).

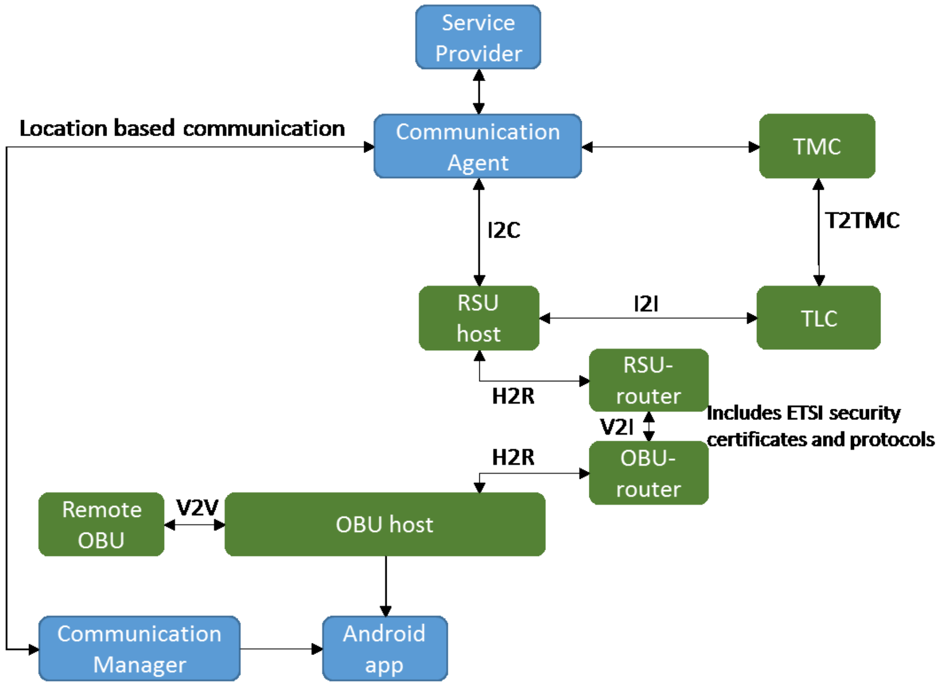


Figure 71: High-level roadside centric architecture

Rest time and parking applications use unicast between service backend and smartphone; these services do not require any architecture for managing communications other than already existing internet facilities. Similarly, the motorcycle approach warning and CACC are pure ITS-G5 V2V and only use the Compass4D part of the architecture.

The cooperative traffic light for VRU uses an improved version of the Communication Agent/Manager. The Communication agent is still at the TMC level, but the communication manager can be included in an Android app in the form of an SDK.

3.6.2.1. Central Systems

In this section, the different systems represented in the previous figures, present in the deployment site, are explained providing information of their function as well as the interaction between them.

3.6.2.1.1. Open Data Platform / Operational Web Server

The Cloud hosted platform of the NDW keeps a live tracking of all road concerns, including the position of road works and other relevant road hazards. At the same time, it generates the corresponding ETS ITS-G5 messages according to the situations detected.

Hardware	Host/Server
Relevant services	RWW, RHW, IVS
Communication flows	DATEX2 information feed

3.6.2.1.2. TMC

Hardware	Host/Server
Relevant services	Cooperative traffic light pedestrians

Communication flows	CAM from VRU via TMC to RSU/TLC.

3.6.2.2. Roadside Systems

As already described in the architecture of Compass4D, the RSU is connected to the TLC to acquire signal status and timing information. GLOSA, red light violation warning and green priority services run on the RSU and use the information from the TLC to encode MAP/SPaT and DENM information. For red light violation the CAM messages of the vehicles are used to evaluate if a vehicle is (about to) violate the red light. There is also an interface to accept the CAM messages from the TMC level for the cooperative traffic light for VRU service.

3.6.2.3. Vehicle Systems

At the North-Brabant deployment site the drivers and VRUs use a smartphone in order to receive information from the Local Operational Web Server related to traffic and road hazards.

The smartphone provides regular updates of their location (using a geo-fencing) to keep the web server updated of the position of the vehicles.

3.6.2.3.1. Emergency Vehicles

Hardware	OBU
Service	Green priority
Communication flows	CAM and DENM over Cellular network (3G) to/from the web server

The emergency vehicles have 3G OBUs which regularly update its position to the local web server.

3.6.2.3.2. Trucks

Hardware	OBU
Compatible services	Green light priority, GLOSA, emergency vehicle warning, red light violation warning
Communication flows	TBD

3.6.2.3.3. VRU/Pedestrian Systems

Hardware	Android Smartphone
Compatible services	Cooperative traffic light for VRU
Communication flows	CAM over Cellular network (3G) via TMC to RSU/TLC

3.6.3. Stakeholders' partnership

The North-Brabant Deployment site has strategic partners, development partners, and some third parties for the implementation, deployment, operation and evaluation of the C-ITS services. The complete list is as follows:

Strategic partners:

/ Tilburg City Council: Public authority; providing the necessary means and connections to implement, deploy and successfully test the services in the city of Tilburg and the highway A58, and manging data providers.

/ Eindhoven City Council: Public authority; providing the necessary means and connections to implement, deploy and successfully test the services in the region of Eindhoven, and managing data providers.

/ Helmond City Council: Public authority providing the necessary means and connections to implement, deploy and successfully test the services in the city of Helmond and the highway A270, and managing data providers, and providing access to emergency vehicles.

Development partners:

/ Dynniq: C-ITS system provider

/ Planning Transport Verkehr AG: Truck navigation services

/ Macq SA: VRU protection systems; providing camera's and development of image processing algorithms

/ TU/e: Technical university; developing architectures for mobility

/ TNO: Organisation for applied scientific research; developing and deploying U-CACC and Truck Platooning

/ V-tron BV: Research and development for mobility; developing apps for C-ITS services

Third parties:

/ Astrata Europe BV: Fleet manager provider

/ DAF Trucks: Truck manufacturer (provide trucks for Truck Platooning)

/ Technolution BV: Traffic Systems

/ Fire brigade Helmond: Allow C-ITS to be installed on emergency vehicle

3.7. Architecture Thessaloniki

The deployment city of Thessaloniki faces specific urban transport challenges. These challenges are associated to traffic congestion confrontation, road transport efficiency increase, multimodal & cooperative traffic management, traffic induced environmental impacts reduction, and sustainable economic growth & innovation. Having acknowledged the importance and benefits of the C-ITS technologies, the city's stakeholders in cooperation with research and innovation institutes have been engaged and have invested early on in a significant number of innovation initiatives and projects, such as Compass4D and CO-GISTICS. The commitment to the continuation of related C-ITS services provision is achieved within the C-Mobile C-ITS services deployment, aiming to increase road safety, mobility and accessibility for all road users.

3.7.1. Deployed services

Thessaloniki implements GLOSA and Road Hazard Warning. GLOSA is provided through a dedicated App, which has been integrated in the taxi fleet dispatching App. The service provides speed advice based on traffic light status, the vehicle's position, and speed. The aim is for taxi drivers to minimise the number of stops at equipped signalised intersections (especially when traffic density is moderate) along Tsimiski Street (main arterial road).

Road Hazard Warning is implemented along the Peripheral Ring Road of Thessaloniki (peri-urban highway). The event detection and management system of the Peripheral Ring Road is comprised of incident detection cameras and VMSs installed in 2008, as well as a network of Bluetooth detectors installed in 2014.

The provision of the services is based on both short-range and long-range communication protocols (G5 and LTE). The penetration of the C-ITS services in Thessaloniki was of 600 taxi drivers, during the Compass4D pilot operation period. The daily average number of drivers circulating was 152, during the first few weeks, rising up later to 178.

Service	Communication	User-equipment	Users
Road hazard warning	G5 and LTE	PDA/ Smartphone	600 taxi drivers
GLOSA		In vehicle OBU	4 taxis equipped

3.7.2. Covered area

Currently, Thessaloniki is deploying C-ITS services along the Peripheral Ring Road and along Tsimiski Street, a main arterial road of the inner city.

C-ITS area	User extension
/ 12 Intersections (14 traffic lights) along Tsimiski Street / 5 VMSs along the Peripheral Ring Road – 13 km / 7 RSUs	Existing: 600 taxis Target: +6500 cars, 300 pedestrians

Figure 72: Extent of the covered area in Thessaloniki

3.7.3. Architecture

The Thessaloniki architecture is currently focused on long range (LTE) and short range (G5) communications for serving the C-ITS services. The high-level site architecture, depicted in the following figure, shows the elements running in the city, in order to offer LTE/ G5-based services to the end-users.

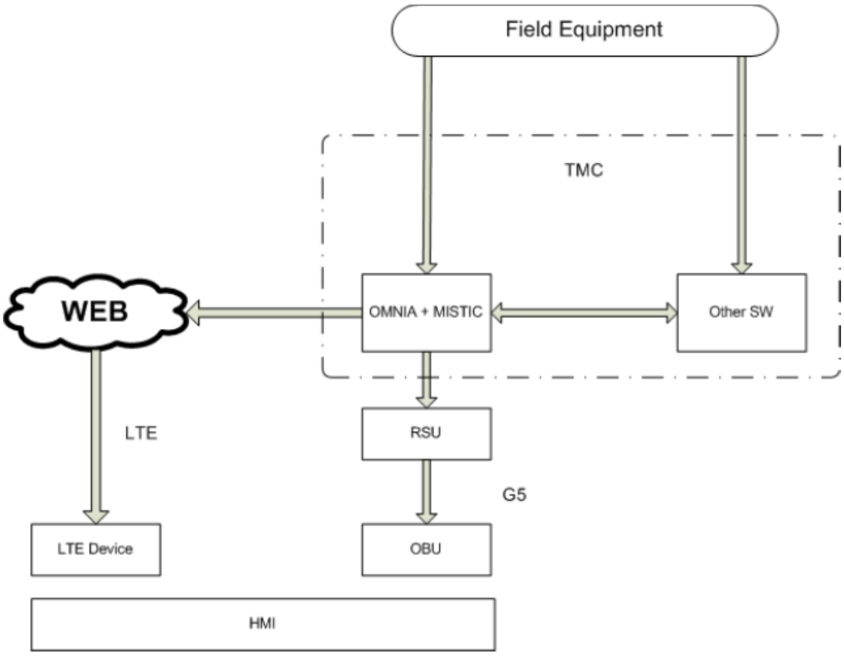


Figure 73: Generic architecture of Thessaloniki

3.7.3.1. Central Systems

In this section of the document, the different systems represented in the previous figure, present in the deployment site, are explained providing information of their function, as well as the interaction between them.

3.7.3.1.1. Open Data Platform / Operational Web Server

The operational web server used in Thessaloniki is Microsoft IIS Microsoft-HTTPAPI/2.0. The web service is xml based restful web service. The xml response is parsed according to the SURFACE VEHICLE STANDARD [57], in order to retrieve the useful information. This is currently done by a proprietary web service implemented by OMNIA/ UTOPIA of SWARCO.

OMNIA and MISTIC applications are used for the creation and exchange of the cooperative messages of both services (Green Light Optimal Speed Advisory and RHW). The cooperative messages are generated by SWARCO-MIZAR equipment and communicate directly with OMNIA for the Green Light Optimal Speed Advisory and through the existing communications network of the Region of Central Macedonia (RCM) for the RHW service.

Hardware	Web server Microsoft IIS Microsoft-HTTPAPI/2.0
Relevant services	GLOSA, RHW
Communication flows	GLOSA: SPAT and TOPO over LTE to the HMI, and CAM over LTE to the TMC RHW: DENM over G5 to RSU, OBU and HMI, and CAM over G5 to OBU, RSU, TMS

3.7.3.1.2. TMC

The GLOSA and Road Hazard Warning services are implemented with the use of the two existing traffic management centres of the RCM, one responsible for Tsimiski Street and one for the Peripheral Ring Road of Thessaloniki.

The OMNIA platform installed for the traffic management of Tsimiski Street provides a common interface for all traffic management related systems of the centre of Thessaloniki. The system is composed of:

- 12 traffic controllers along Tsimiski
- 1 surveillance camera
- 5 AUTOSCOPE cameras
- 29 traffic detection units and
- 5 VMSs located at the main gates of the city centre.

UTOPIA, a distributed adaptive traffic control system, is used for traffic lights management. The local management of the 12 intersections (14 traffic lights) is executed by SPOT at each traffic controller. The system provides real-time monitoring of the traffic conditions as well as signal phase optimization along Tsimiski Street. Furthermore, the system is supported by MISTIC, a platform dedicated to the validation, normalization and synchronization of traffic data. The TMC is connected to the field equipment through optic fibre.

The event detection and management system of the Peripheral Ring Road of Thessaloniki provides information to travellers related to incidents along the road through 5 VMSs. Incidents are detected through Automatic Incident Detection algorithms using 22 cameras and include:

- Fallen Object
- Inverse Direction
- Pedestrian
- Stopped Vehicle
- Under speed.

All the field equipment is connected to the TMC through 3 Wi-Fi points, while local connections are done by optic fibre and Wi-Fi.

Hardware	Host/Server
Relevant services	GLOSA, RHW
Communication flows	GLOSA: SPAT and TOPO over LTE from the TMC to the HMI RHW: DENM over G5 from the TMC to the RSU

3.7.3.2. Roadside Systems

Regarding RHW, the current automatic incident detection system of the Peripheral Ring Road is a Traficon solution integrated into the Networks platform (by Delcan). The incident detection management is based on AID cameras, CCTV cameras and radar traffic sensors. The incidents are inserted in Networks and monitored by TMC operators. TMC operators use MISTIC as an incident management application, which generates the information (DENM messages) to be displayed, and transmits it through the RSUs. The OBUs receive the DENM messages through the RSUs.

The interfaces for the RSUs are:

- RSU with TMC (back office); the RSU communicates directly with OMNIA using a proprietary protocol.
- RSU with OBU; standardized messages as mentioned above.

3.7.3.3. Vehicle Systems

Regarding RHW, OBUs receive the DENM messages from the RSUs through G5 and transmit them to the smart devices. OBUs transmit as well the CAM messages to the RSUs through G5. The OBUs is interfaced with the RSUs. If the OBU is an LTE-enabled device then there is direct communication with the server through the web service. The OBU interface is present only in the case of an OBU being installed in the vehicle along with the smartphone device.

3.7.3.3.1. Taxis

Both services (GLOSA and RHW) were tested in Thessaloniki from November 2014 to August 2015. The services were tested using a fleet of taxis, about 600 drivers using GLOSA and 4 vehicles equipped with G5-enabled OBUs.

Hardware	OBU
Compatible services	RHW
Communication flows	DENM and CAM over G5

3.7.4. Communications schema

The following figure shows the typical architecture for GLOSA, including the communications among the elements. The messages used are SPAT, TOPO and CAM.

The web service contains updated (every second) SPAT and TOPO messages for all the intersections along Tsimiski Street.

The smart device downloads the messages from the web service and estimates the speed advice based on the current position (GPS), the current speed (GPS based), the distance to the traffic light (TOPO) and the time to green/red (SPAT and TOPO).

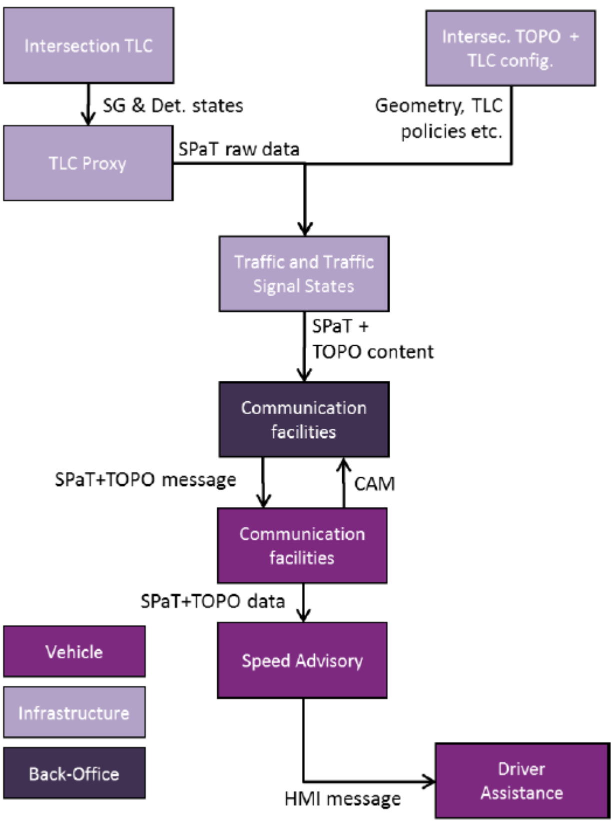


Figure 74: Typical architecture for GLOSA

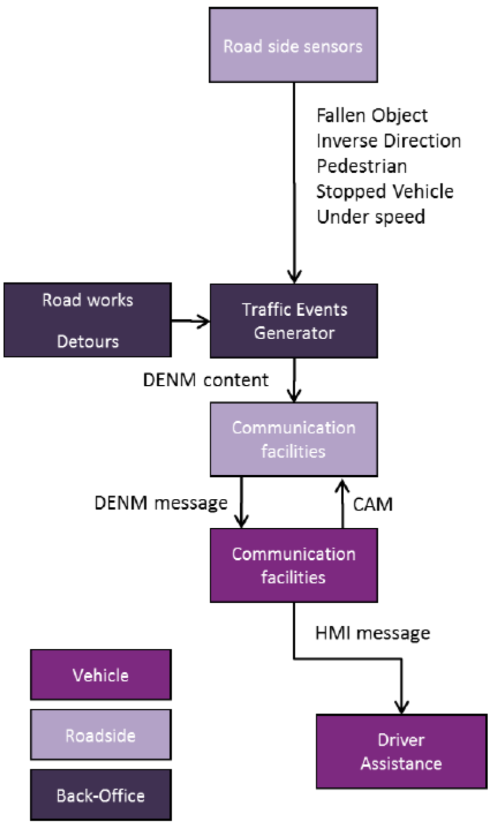


Figure 75: Typical architecture for RHW

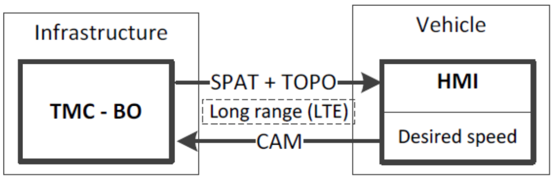


Figure 76: Data flow for GLOSA

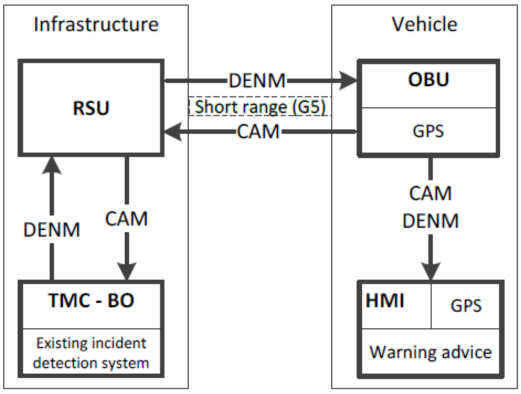


Figure 77: Data flow for RHW

The typical architecture for RHW is presented in the following figure, where communications among the elements are depicted as well. The messages used are DENM and CAM.

DENM are generated by the MISTIC and then transmitted to the RSUs. Smart devices receive the DENM through the OBUs (which receive the DENM through the RSUs).

3.7.5. Stakeholders' partnership

For the C-ITS services deployment in Thessaloniki, a significant number of key partners and associated partners are engaged in the implementation, operation and evaluation of the C-ITS services. The complete list is the following:

Partners:

- Region of Central Macedonia (RCM): Public authority, contributing in the large-scale deployment of the C-ITS services, by being engaged in the identification of the replication capabilities for the Thessaloniki deployment city, in the C-ITS services' demonstration and integration, as well as in communication and dissemination activities. RCM is responsible for the operation of the two TMCs (Tsimiski Street and Peripheral Ring Road of Thessaloniki) in the city of Thessaloniki and for the operation of the GLOSA and RHW services (with the support of the technology providers).
- Centre for Research and Technology Hellas (CERTH-HIT): Research institute contributing in coordination and management, identification of C-ITS services' requirements, architecture and systems design, large-scale deployment, validation and impact assessment. CERTH-HIT is the main responsible for activities concerning the deployment site of Thessaloniki, such as deployment site adaptation, C-ITS services implementation and integration.
- Infotrip (INF): Company providing infomobility services and ITS solutions, service provider for the deployment site of Thessaloniki.
- TrafficTech (TRAF): Company operating in the field of road traffic management, service provider for the deployment site of Thessaloniki.
- Taxiway (TXW): Taxi Transportation Company in Thessaloniki, providing the taxi fleet (vehicles and drivers) to take part in the C-ITS services demonstration.

Associated:

- Aristotle University of Thessaloniki (AUTH): The Laboratory of Transport Planning, Traffic and Highway Engineering will take part in activities associated to deployment site demonstrations, contributing in the large-scale sustainable deployment of the C-ITS services.
- Ministry of Transport (YME): The Hellenic Ministry of Infrastructure, Transport and Networks will fully support the C-ITS services deployment, by taking part in activities regarding the provision of advice on the project work and the creation of synergies with other relevant C-ITS deployments and relevant initiatives.

3.8. Architecture Vigo

Vigo city with around 300.000 habitants and frenetic activity due to its diversified economy (international seaport, important automotive sector, commercial areas, etc.), provides a daily traffic flow within its metropolitan area of more than 480.000 people with a relevant presence of freight traffic, what means an appropriate location to deploy and test new complementary services, as C-ITS, that help to increase driving safety level and solve environmental issues.

Vigo city wants to take advantage of experience gathered in previous C-ITS related projects (e.g. COMPASS4D, CO-GISTICS, etc.) and aims to both extend the catalogue of C-ITS services and make them available by using both G5 and cellular communication technologies.

3.8.1. Deployed services

Vigo city is currently providing Road Works Warning, Road Hazard Warning (Traffic Jam Ahead Warning and Stationary Vehicle Warning), Emergency Vehicle Warning, Signal Violation Warning (Red Light Negation Warning), Green Priority (for Emergency Vehicles) and GLOSA (Time to Green).

Service	Communication	User-equipment	Users
Road work warning	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All
Road hazard warning	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All
Emergency vehicle warning	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All
Signal violation warning	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All
Green priority	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	Emergency Vehicles
GLOSA	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All
Slow or stationary vehicle warning	IEEE 802.11p	OBU + SMARTPHONE (HMI purpose)	All

3.8.2. Covered area

Vigo urban area where C-ITS services are currently deployed is consisting of routes that cross the entire city centre connecting two of the main entrances to the city (AP9 and A55 highways) and also covering seaport and automotive industry road accesses (50 intersections)

Complementing this urban coverage, sections of Spanish A52, A55 and AP9 motorways and highways close to Vigo - including city entrances- are also equipped with G5 Road Side Units (100 Km)

C-ITS area	User extension
/ 50 Intersections	Target for C-MOBILE: 20 trucks, 10 buses, 30 proprietary vehicles, 5 emergency vehicles, 10 motorcycles and pedestrians.

As previously commented, current provision of C-ITS services is done by using G5 based RSU (50), obtaining traffic information from Traffic Management Center of Vigo City and depending Traffic Light Controllers (proprietary communication protocol).

Messages transmitted by RSUs can be received and processed by any G5 OBU able to manage CAM, DENM, MAPEM and SPATEM ETSI messages.

Main goal within C-MOBILE project is to extend the catalogue of C-ITS services and to enlarge provision by using cellular communication.

Figure 78: Vigo C-ITS corridor

3.8.3. Architecture

C-ITS deployment in Vigo is currently based on ITS G5 technology.

Architecture supporting this deployment comes from previous C-ITS related projects and is depicted in Figure 79 and explained within next subsections.

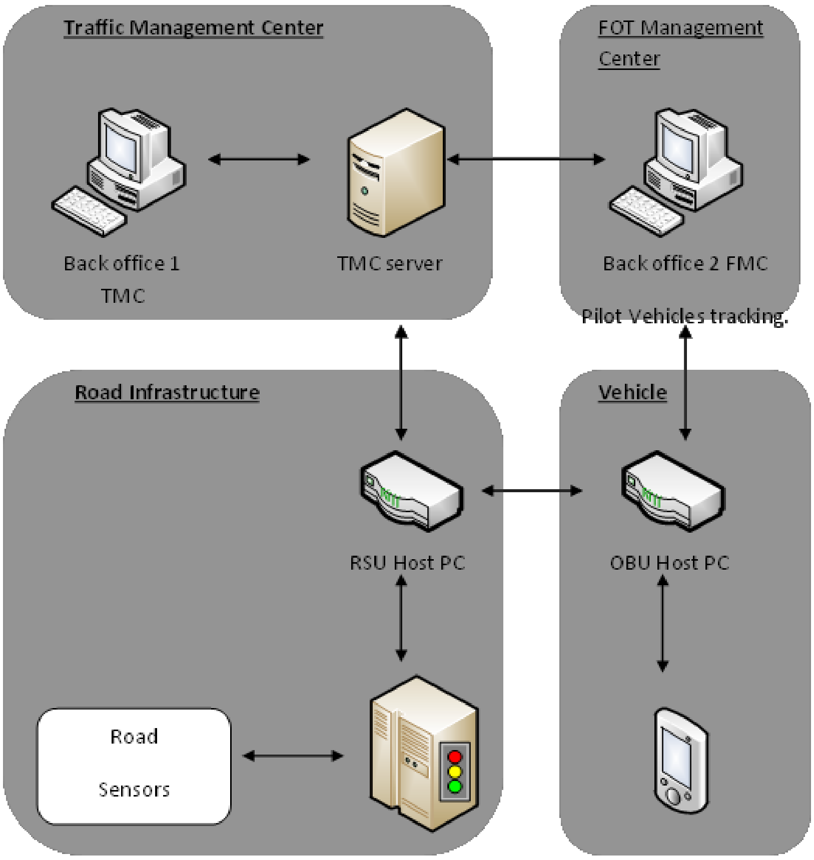


Figure 79: Vigo C-ITS (G5 based) architecture

As commented in previous sections, one of the goals within this project is to enlarge provision of C-ITS services by using cellular communication. For that, architecture agreed within C-MOBILE will be used as reference taking into account related existing standards and current available cellular technologies.

3.8.3.1. Central Systems

In this section of the document, the different systems represented in the previous figure are explained providing information of their function as well as the interaction between them.

3.8.3.1.1. Traffic Management Centre

Managed by ESYCSA, Vigo city contractor for urban mobility management, TMC controls infrastructure and has access to Traffic Light Controllers (TLC), road side sensors, CCTV cameras and RSUs deployed along all urban area

It also generates info concerning Road Works Warning and Road Hazard Warning

Hardware	Back office server
Relevant services	Infrastructure management/ RWW, RHW info related generation
Communication flows	To road sensors, proprietary protocols over private network To FOT management Centre, proprietary protocols over Internet VPN

3.8.3.1.2. FOT management Centre

Managed by CTAG, it centralizes pilot management by collecting data from TMC and vehicles.

Hardware	Back office server
Relevant services	Pilot management (logs collection, RSUs remote checks, …)
Communication flows	To TMC, proprietary protocols over Internet VPN To vehicles (for logs collection purposes), Cellular connection

3.8.3.2. Roadside Systems

Main roadside systems are: TLC, road side sensors (inductive loops) and RSUS. Both TLC and road side sensors, controlled and managed by TMC, provide their information to RSUs and TMC using proprietary protocols in such a way that RSU can generate next ETSI ITS messages to be sent via G5 link:

- CAM Cooperative Awareness Message
- DENM Decentralized Environmental Notification Message
- SPaTEM for Signal Phase and Timing message
- MAPEM for intersection topology

C-ITS services currently supported: Road Works Warning, Road Hazard Warning(Traffic Jam Ahead Warning and Stationary Vehicle Warning), Emergency Vehicle Warning, Signal Violation Warning(Red Light Negation Warning), Green Priority(for Emergency Vehicles) and GLOSA (Time to Green),

3.8.3.3. Vehicle Systems

Vehicle systems should consist of a G5 OBU together with some appropriate device to display info corresponding to message processing. When enlarging C-ITS coverage by using cellular technology, if due to whatever reason just this communication link is used, a nomadic device is forecasted to be just needed (e.g. smartphone)

3.8.4. Communications schema

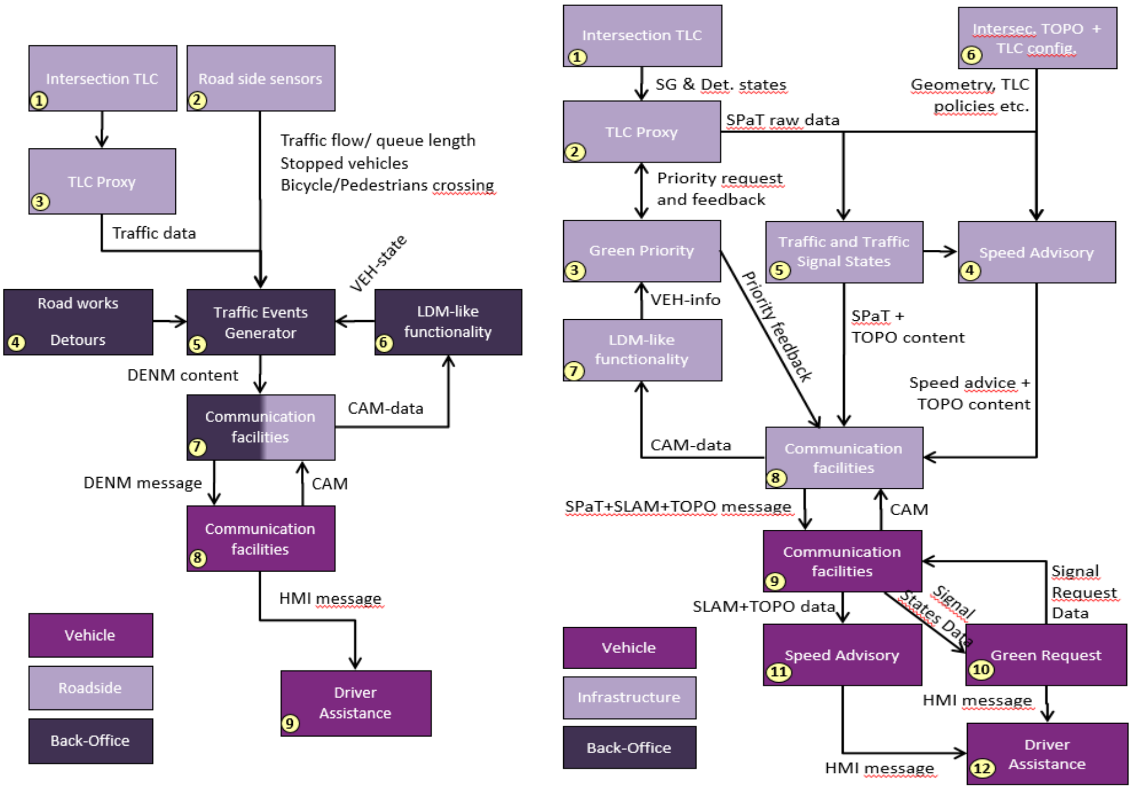


Figure 80: Communication schemas for DENM and SPATEM/MAPEM-based services

3.8.5. Stakeholders' partnership

Within C-Mobile, as in previous projects, Vigo city counts on two main partners to implement, deploy, operate and evaluate the C-ITS services and also with associated partners collaborating to success with this initiative.

Partners:

- Vigo City Council: Public authority that provides the necessary means and connections to implement, deploy and successfully test the services in the city of Vigo. It manages data providers (ESYCSA, TMC operator) and provides access to deploy C-ITS services in emergency vehicles.
- CTAG: Galician Automotive Technological Centre is the entity in charge of implementation, deployment, operation and evaluation of C-ITS services in Vigo city. FOT Management Operator.

Associated:

- VITRASA: Vigo public transport company provides access to C-ITS deployment in urban buses.
- CEAGA: Galician Automotive Enterprises Cluster. Provides access to C-ITS deployment in freight vehicles sector.
- Radiotaxi Vigo association provides access to C-ITS deployment in taxi sector.

Also DGT Spain, government department that is responsible for the Spanish transport network, supports this initiative.

4. Concrete Architecture

The concrete architecture is defined taking the reference architecture (Figure 27) as a basis and paying special attention to the current deployed architectures in the eight Deployment Sites of C-MobILE. One of the real challenges of C-MobILE is ending up with a large-scale long-term deployment on cities with different C-ITS experience, and this variety needs to be addressed by the architecture to be able to adapt the current architectures, independently on their status, as well as make the introduction to the C-ITS world to new cities as easy as possible.

The C-MobILE architecture follows the methodology applied for the reference architecture and, therefore, is developed in three consecutive phases (reference, concrete and implementation) over six different viewpoints (context, functional, communication, information, implementation and physical). The second phase, also known as the concrete architecture definition, focuses the work on four over those six viewpoints, in order to stablish a concrete step towards the interoperability, security, availability and adaptability perspectives. The main target is to deliver specific points that will be deeply elaborated in the architecture for implementation, which will be carried out in the Task 3.4 of C-MobILE. Therefore, during the lifetime of this Task 3.2, multiple work flows have been assigned to work in parallel in order to define the Context, Functional, Communications and Physical viewpoints. However, not all the viewpoints have been developed at the same level of depth, as the further tasks of C-MobILE need a very well defined functional viewpoint to ease the work over other implementation-related viewpoints such as the Information and Communication ones.

This implies that the concrete architecture needs to pay special attention to the Functional viewpoint not only for further work, but also for showing the Deployment Sites how the architecture will look like in an early phase, so they can fine tune and validate the proposed architecture. Indeed, one of the biggest mistakes is to define a C-ITS architecture without listening the cities or regions it is going to be deployed.

The reference architecture deliverable (D3.1) describes the viewpoints in detail, comprising a definition of the viewpoint, which stakeholders are related and the model kinds that are used to develop such viewpoint. The deliverable D3.2 is a continuation of this previous work and is focused on offering more details about the models initially shown in D3.1.

4.1. Context Viewpoint

For concrete architecture, the context viewpoint describes the relationships, dependencies, and interactions between the system and its environment (e.g. people, systems and external entities) more in detail derived from reference architecture context viewpoint. As mentioned in D3.1 [61], the context view conforms to the context viewpoint and help system's stakeholders (e.g. system/software architects, designers, developer and users) understand the system context. Stakeholders and concerns are similar to what was defined for Reference Architecture. The reference architecture can also be found in the section 2.2 of this document.

As already stated in D3.1, the C-MobILE architecture follows a methodology based on model kinds using BDDs and IBDs diagrams. The context view conforms to the context viewpoint. SysML Block Definition Diagram (BDD) is identified as suitable modelling notation for capturing the context viewpoint for concrete architecture. SysML Use Case diagram can be used to show the usage of a system which will be refined later based on requirements during implementation phase.

The notations that we commonly see used for context diagrams are SysML Block Definition Diagram for concrete architecture. As defined in reference architecture, C-MobILE consists of five main systems which is now further disseminated into sub-systems depicted as black box and corresponding actor's roles with those sub-systems is captured in concrete architecture. Actors and their respective roles have been further categorized based on their individual tasks towards the specific sub-system or system.

For better readability we have designed context diagrams for each System: Support, Central, Roadside, Vehicle, and VRU/Traveller separately and the main diagram showing all the connections and interactions between all actors and their respective systems and sub-systems, as shown in the general diagram (Figure 86).

4.1.1. Support System

Comprise of sub-systems performing various tasks e.g.: governance, test and certification management, security and credentials management which is describe in Figure 81.

Following actors have been identified interacting with support system:

- Governance: an actor that is directly concerned with Support System whose responsibility is to support various other sub-systems such as legal authorities, test and certification management, security and credentials management etc.
- Legal Authorities: the governmental body that provides and mandates laws and regulations that will be used by the C-ITS implementation for safe use of infrastructure.
- Certificate Authority Administrator: the entity that issues digital certificates for safe and secure transfer of data through the C-ITS infrastructure. They will also be responsible for the certificates that will be used for secure registration of the infrastructure, service providers and end-users and also secure payments.

Following sub-systems identified comprising support system

- Security & Credentials Management: a system containing the data store or a database that is used to store credentials, root certificates and SSL certificates in a secure manner.

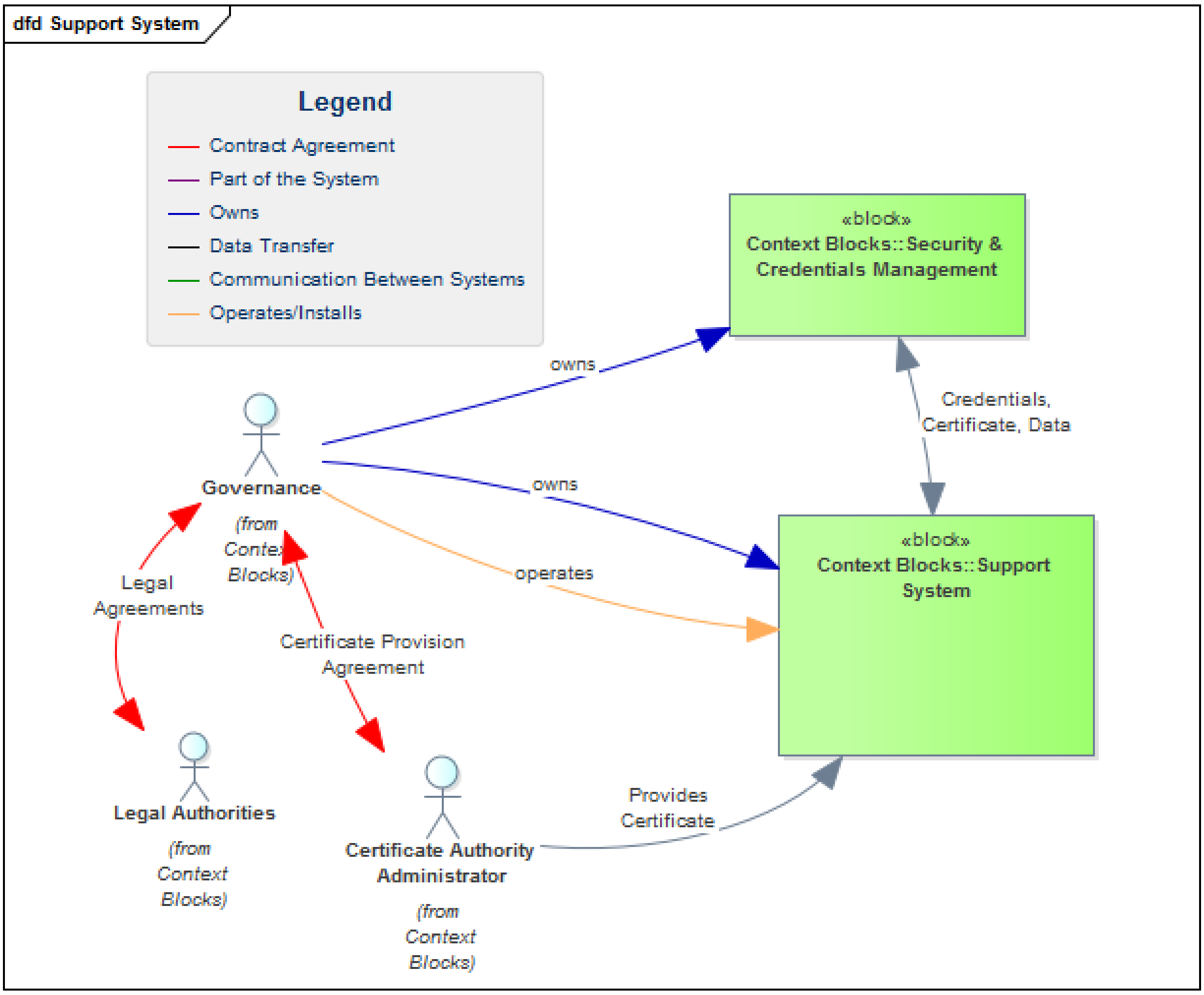


Figure 81: Context diagram of the Support System

4.1.2. Central System

Comprise of sub-systems to support connected vehicles, field and mobile devices. The sub-systems can be aggregated together or geographical or functionally distributed which is described in Figure 82.

Following actors are identified

- Service Providers:
  - Parking Site Provider: an entity that owns parking facilities and provides them for vehicles/trucks.
  - Navigation Data Provider: an entity provides the data used for navigation vehicles with its
  - Weather Information Provider: an entity provides weather and climate information and warning of hazardous weather including thunderstorms, flooding, etc.
  - Information Provider: an entity that provides information that may include data or control information to the recipient. The information provided depends on agreement made.
- Deployment Site Owner: the city council or the body that implements C-ITS in their roads;
- Financial Authority: the organization that owns the financial gateway that the C-ITS network uses for payments.
- Traffic Manager: the body responsible for management of traffic in a deployment site and also the owner of the Traffic Management System for the deployment site.
- Traffic Operations Personnel: the people that operate a Traffic Management System who interact with traffic control systems, surveillance systems and other systems related to the TMS.

Following sub-systems are identified within Central System and the definitions of those are defined in physical viewpoint of reference architecture:

- Service Provider BO: Individual service providers (Parking Site Provider, Navigation Data Provider, Weather Info Provider, Information Provider, etc.) will be the actors that communicate through the Service Provider BO, which will be owned by the Deployment Site Owner through the Central System.
- Traffic Management System (TMS): The Traffic Manager, a part of the Deployment Site, owns the Traffic Management System which will be operated by Traffic Operations Personnel in agreement with the Traffic Manager.
- SPES: A Financial Authority will process payment using the financial gateway through the SPES which will be owned by the Deployment Site Owner through the Central System.
- Financial Gateway: a company or organization that handles electronic fund transfer requests and performs the transfer of funds from the user to the service provider or general C-ITS providers that will be owned by a Financial Authority.
- Central Data Storage: the data store or the database that can be used to store information about the service providers and the information that they provide. These can also be used to store a list of which service is being used by which end-user and payment status if present. This would be owned by the Deployment Site Owner and residing the central system.

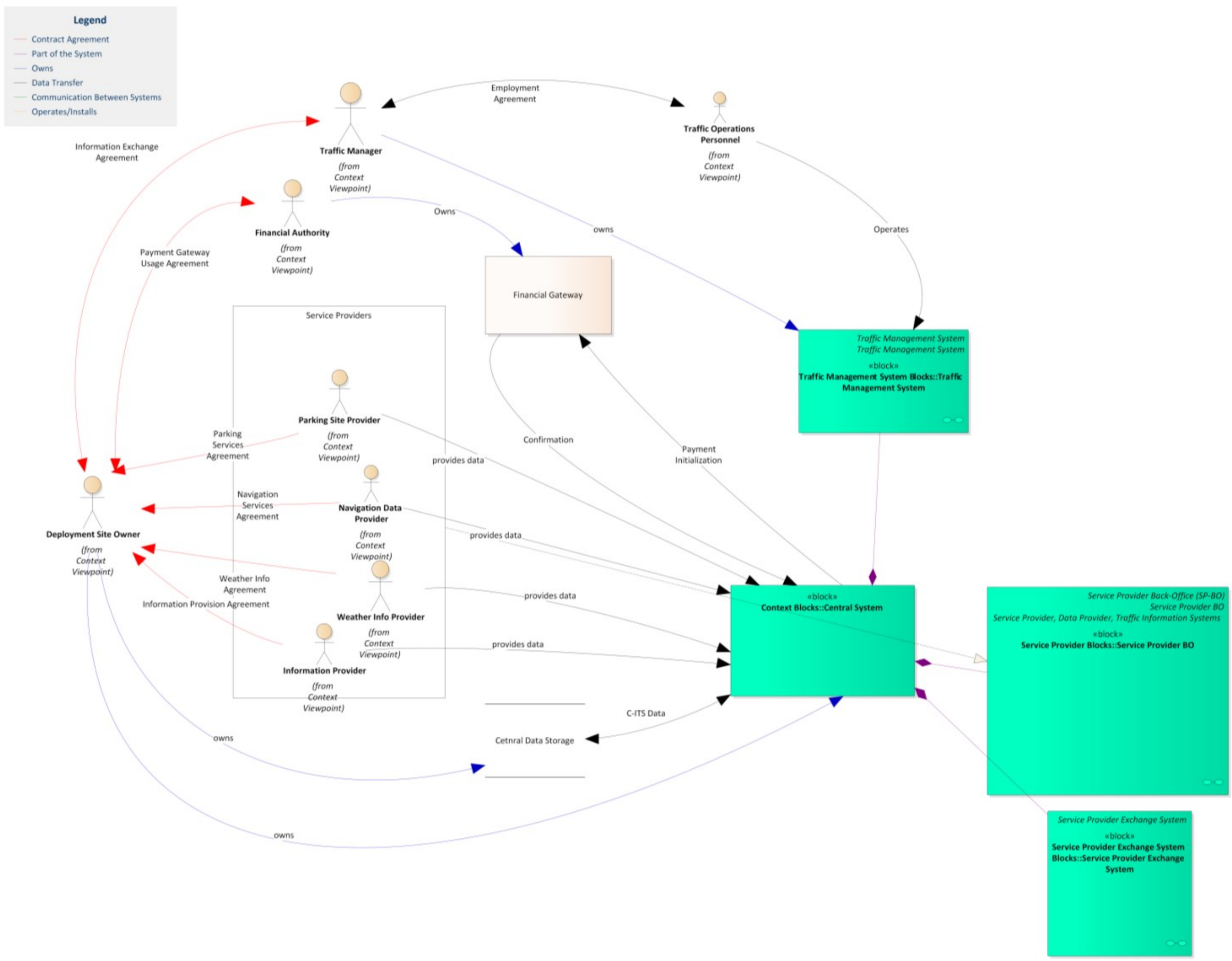


Figure 82: Context diagram of the Central System

4.1.3. Roadside System

Comprise of sub-systems which covers the ITS infrastructure on or along physical road infrastructure, e.g.: roadside units, signal/lane control, etc. describe in Figure 83.

Following actors are identified for roadside system:

/ Information Provider: the owner of an entity that provides information that may include data or control information to the recipient. The information provided depends on agreement made.

/ Parking Site Provider: the owner of the parking site that provides data and a space for vehicles/trucks to park.

/ Roadway Owner: the owner of the roadway that is connected using C-MobILE. It can be the city or the neighbourhood.

/ Roadside System Owner: the owner of Roadside System equipment that represents the ITS equipment distributed on and along the roadways the monitors, controls and manages the roadway.

/ Road Operator: the entity that has an agreement with the Roadside System Owner to operate and manage the Roadside System equipment that is deployed on the roadway.

Following sub-systems are identified within roadside system and are defined in detail in physical viewpoint section of reference architecture:

/ Roadside System: These will be owned by a Roadside System Owner that will deploy them in agreement with the Roadway Owner and will be operated by the Road Operator.

/ Roadside Unit: These will be operated by the Roadway operator and owned by the roadside owner.

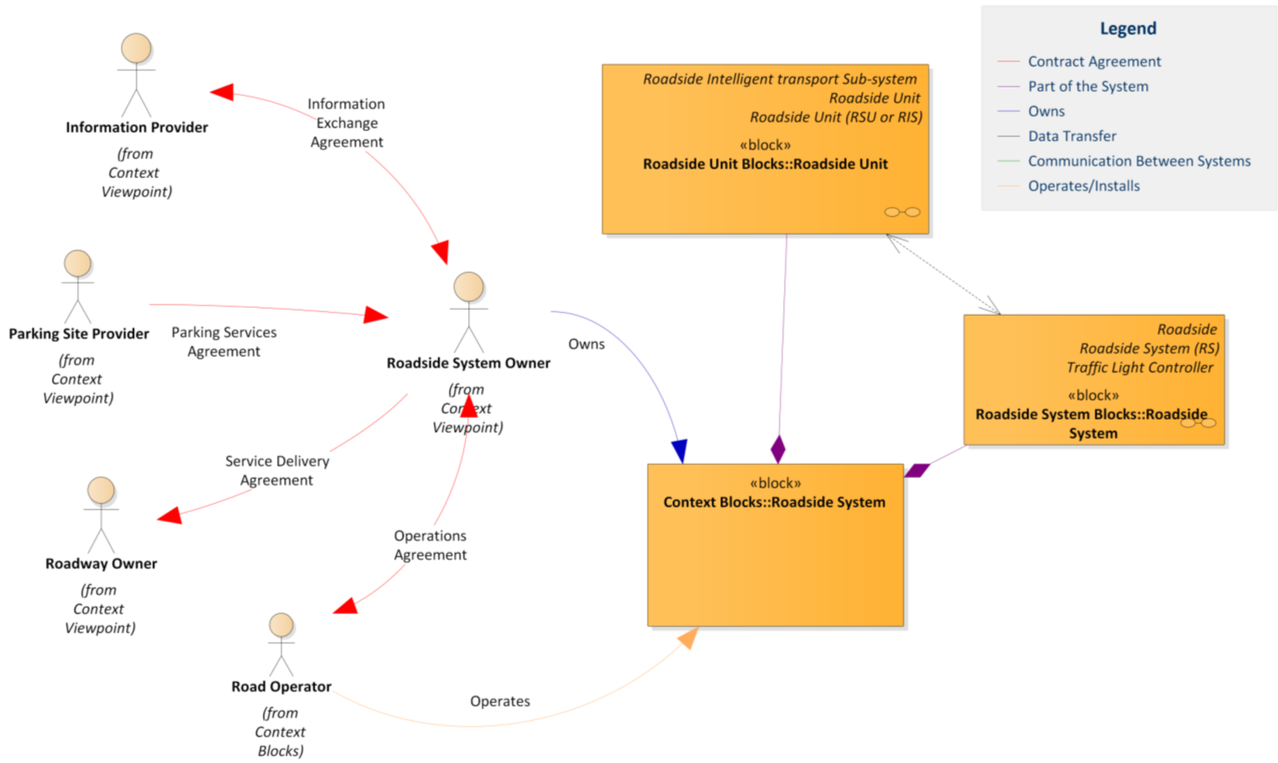


Figure 83: Context diagram of the Roadside System

4.1.4. Vehicle System

Comprise of sub-systems which are integrated within vehicle such on-board systems (advanced driver assistance / safety systems, navigation, remote data collection or information) as described in Figure 84.

Following actors are identified for vehicle system:

/ Vehicle Driver: the person that operates a vehicle on the roadway. These can be operators of private, commercial or emergency vehicles.

/ Map Provider: the entity that provides map databases and systems that use those databases to the Vehicle Manufacturer who installs the system in the Vehicle OBU. They may represent a third-party provider or an internal organization that produces map data.

/ Automated Assist OEM: the entity that develops and provides automated assist systems to the Vehicle Manufacturer who install it in the Vehicle.

/ Vehicle Manufacturer: the entity that is responsible for the manufacturing of the vehicle (private, commercial, emergency) and also the installation of the OBU and the VEE system according to contractual agreements with other OEMs.

Following sub-systems are identified within vehicle system and are defined in detail in physical viewpoint section of reference architecture:

/ On-Board Unit: These will be owned by the Vehicle Driver through the Vehicle and will be installed by the Vehicle Manufacturer in accordance with agreement with other OEMs like the Map Provider

/ VEE: These will be owned by the Vehicle Driver through the Vehicle and will be installed by the Vehicle Manufacturer in accordance with agreement with other OEMs like the Automated Assist OEM.

/ Map System: the system that uses the map stored in the database of the Vehicle and installed in the VEE system of the Vehicle. It can send map data to other systems in the vehicle when requested and also update the Map data through an interface.

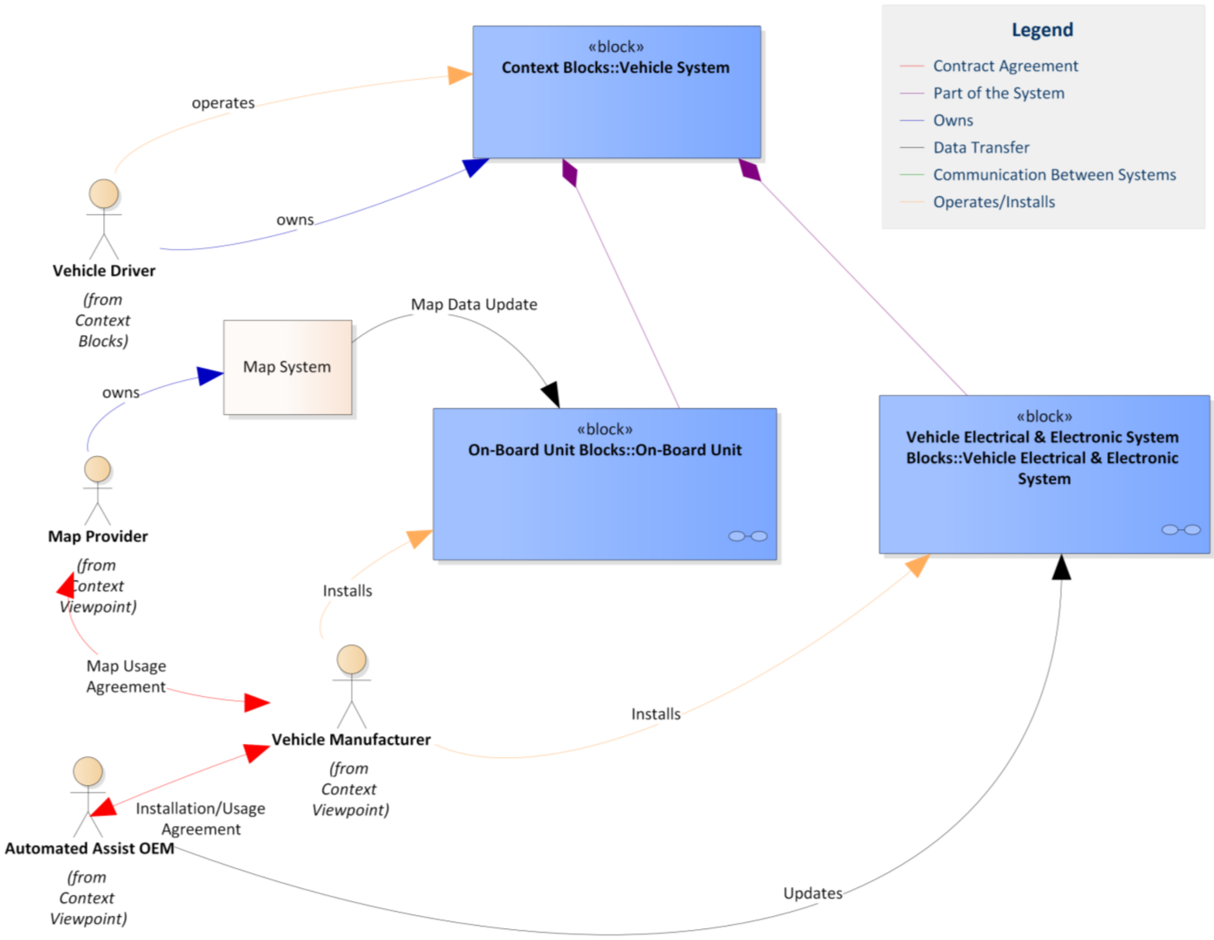


Figure 84: Context diagram of the Vehicle System

4.1.5. VRU/Traveller System

Comprise of both personal devices (e.g.: mobile devices, navigations devices) and specific systems connected to vehicles of VRU's (e.g.: tags) as described in Figure 85.

Following actors are identified:

/ VRU (Vulnerable Road User): a human actor like a pedestrian or a cyclist. These can also include people on skateboards, skate scooters and hover boards.

/ Traveller: any individual that uses transportation services and is roaming. These are separate from Vehicle owners as they will be interacting with the C-ITS installation using their PIDs. They receive information related to trip planning and route guidance including route planning from infrastructure.

Following sub-systems are identified and are defined in detail in physical viewpoint section of reference architecture:

/ Personal Information Devices (PIDs): These will be owned and operated by Traveller/VRUs through an application.

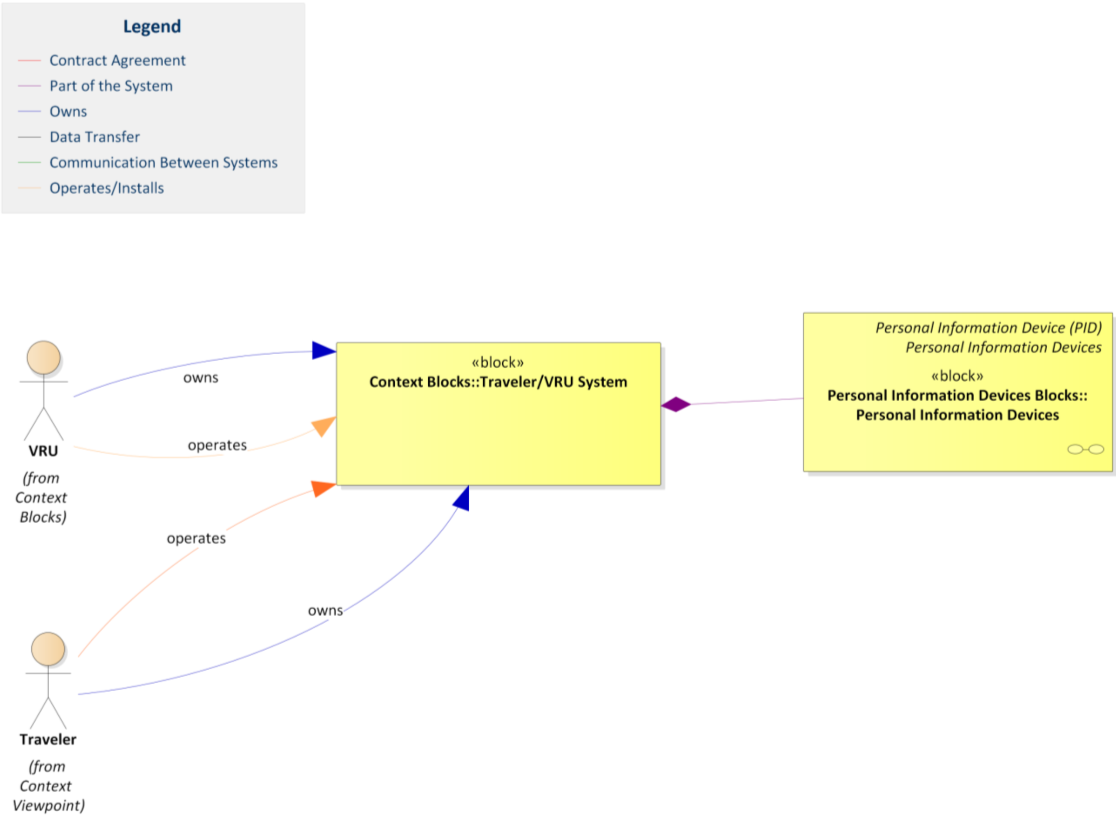


Figure 85: Context diagram of the VRU/Traveller System

4.1.6. Overall Context Diagram

Following diagram defines the overall interactions between actors and their respective sub-systems for C-MobILE.

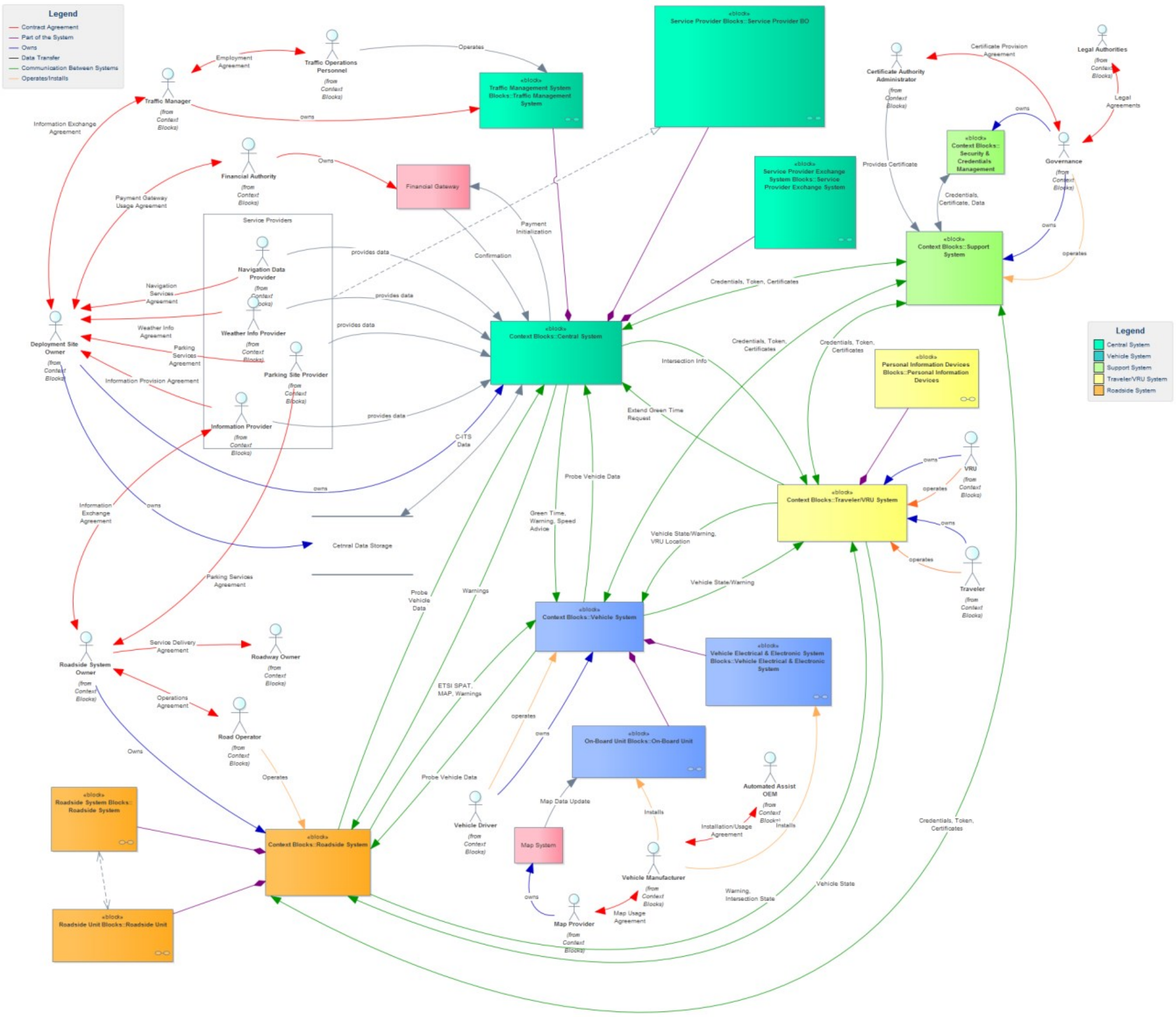


Figure 86: General Context diagram

4.2. Functional Viewpoint

The functional viewpoint, as stated in the deliverable D3.1 [61], is captured by suitable modelling notations such as SysML Block Definition Diagram (BDD) and Internal Block Definition Diagram (IDB). They are used for capturing the models for functional structure and internal structure of the system, respectively.

The D3.1 presented a high-level functional model for C-MobILE (Figure 87), in form of a SysML BDD, which has been deeply analysed to be extended and detailed in such a way that all internal functionalities of the defined blocks are covered and provided.

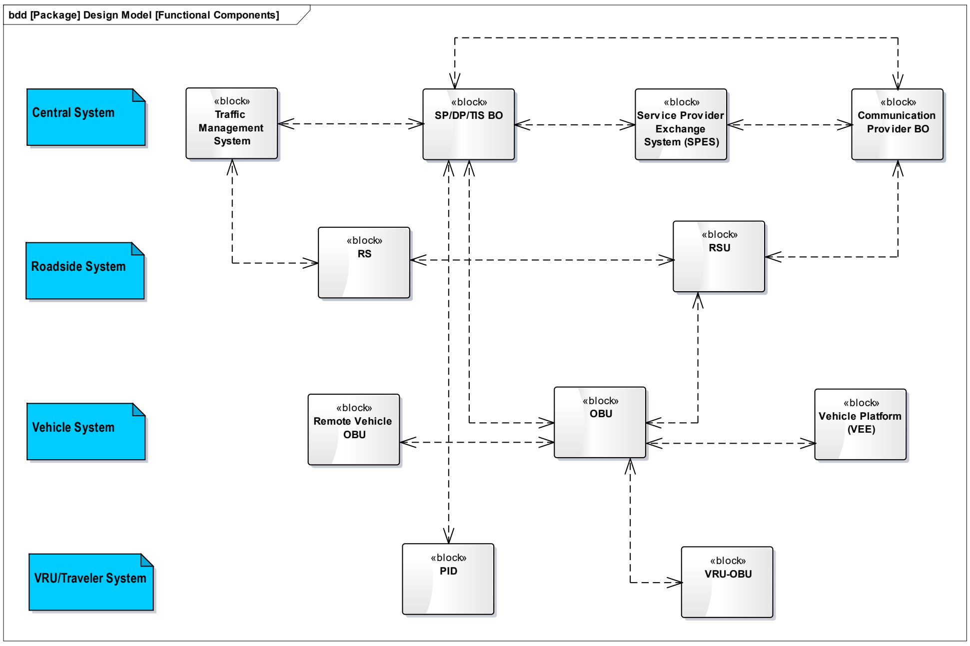


Figure 87: High-level functional model of the C-ITS systems for C-MobILE

The final result of the extended functional model (SysML BDD) is the one shown in the Figure 88, which represents all the detected links among the blocks of the different layers.

After a huge work over the reference architecture, the following activities have been performed and resulted in the complete functional architecture illustrated above:

- Identification of missing blocks and concepts from the functional reference architecture. For such work, the following information has been used:
  - Information related to the current architecture of the Deployment Sites
  - Technical requirements from Task 2.2 of C-MobILE [60], including security, privacy and hybrid communications.
- Determination of the internal structure/functionalities of the main blocks of the architecture.
- Determination of the interfaces connecting internal and external blocks to cover the functionalities.

Figure 88 represents the complete view of the concrete architecture, which will be analysed step by step, system by system in the following sections.

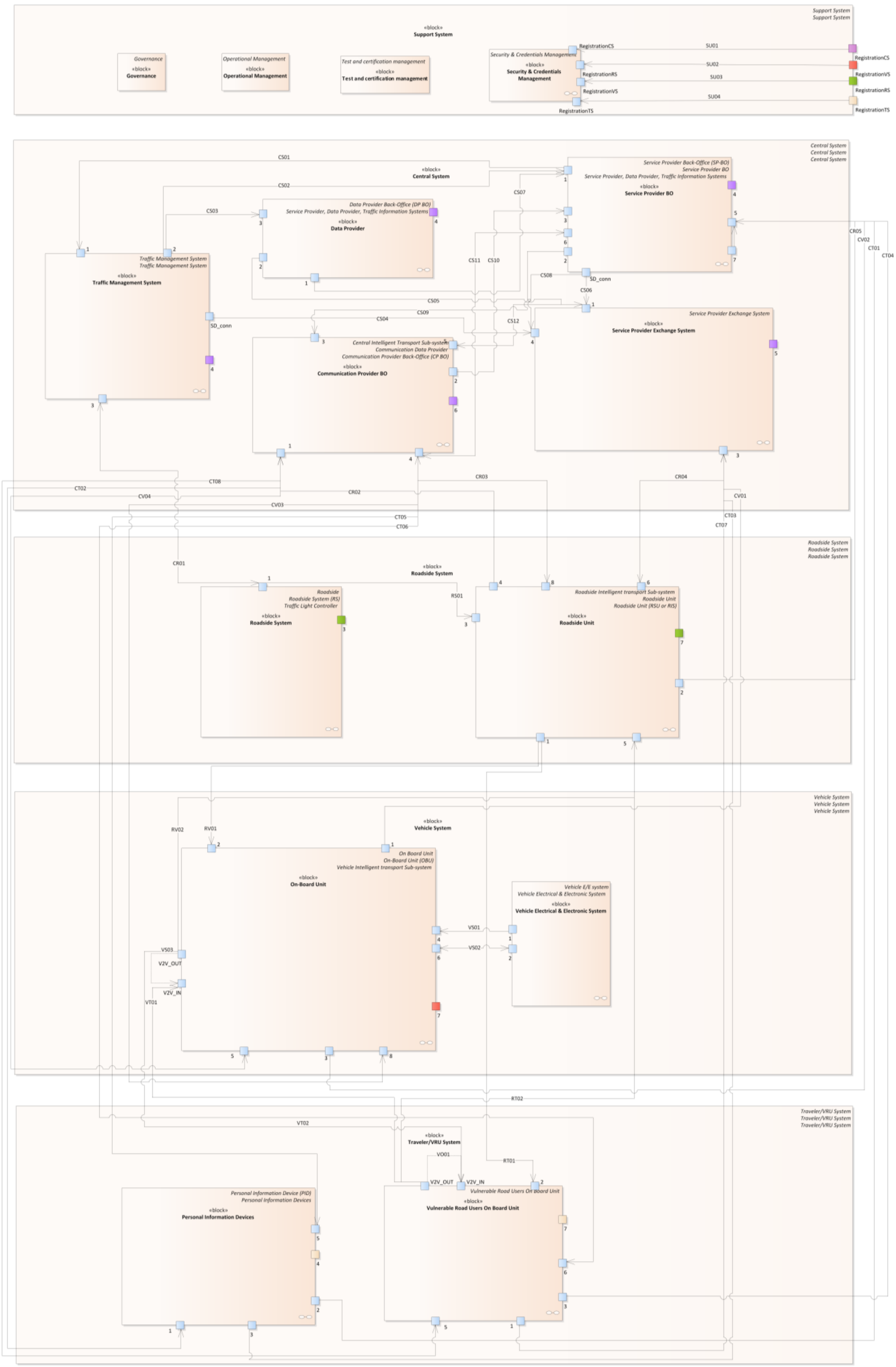

Support System
«block»
Support System
Governance
«block»
Governance
Operational Management
«block»
Operational Management
Test and certification management
«block»
Test and certification management
Security & Credentials Management
«block»
Security & Credentials Management
RegistrationCS
RegistrationRS
RegistrationVS
RegistrationTS
SU01
SU02
SU03
SU04
Central System
«block»
Central System
Service Provider Back-Office (SP-BO)
Service Provider BO
Service Provider, Data Provider, Traffic Information Systems
«block»
Service Provider BO
Data Provider Back-Office (DP BO)
Service Provider, Data Provider, Traffic Information Systems
«block»
Data Provider
Traffic Management System
«block»
Traffic Management System
Central Intelligent Transport Sub-system
Communication Data Provider
Communication Provider Back-Office (CP BO)
«block»
Communication Provider BO
Service Provider Exchange System
«block»
Service Provider Exchange System
SD_conn
Roadside System
«block»
Roadside System
Roadside
Roadside System (RS)
Traffic Light Controller
Roadside Intelligent transport Sub-system
Roadside Unit
Roadside Unit (RSU or RIS)
«block»
Roadside Unit
Vehicle System
«block»
Vehicle System
On Board Unit
On-Board Unit (OBU)
Vehicle Intelligent transport Sub-system
«block»
On-Board Unit
Vehicle E/E system
Vehicle Electrical & Electronic System
«block»
Vehicle Electrical & Electronic System
V2V_OUT
V2V_IN
Traveler/VRU System
«block»
Traveler/VRU System
Personal Information Device (PID)
Personal Information Devices
«block»
Personal Information Devices
Vulnerable Road Users On board Unit
«block»
Vulnerable Road Users On Board Unit

Figure 88: C-MobILE Concrete Architecture functional viewpoint

In order to present all of the material created for this viewpoint, every layer/system is going to be taken to pieces and each relevant piece is going to be described in detail. Therefore, the IDB diagrams of the internal blocks of every layer will be presented and detailed, which contain the internal blocks of a system and the links between them. The lists of links present in a diagram are described in the “Internal communication description” sections of each system, where the following information is available:

- **Link Name**: uniquely identifies a link in the diagram. Generated from a contraction of the block name and a number.
- **Direction:** describes the type of communication between the blocks
  - **B**: The links is bidirectional, information flows in both directions.
  - **D**: The link is directional, information flows in one direction. The direction in which the information flows can be seen in the diagram
- **Description**: provides information of the type of data present in the link.

Moreover, within this task a set of blocks covering a single certain functional concepts have been identified. The 4.2.6 section presents these concepts, which are the User Management, the GeoMessaging and the Service Directory.

4.2.1. Support System

The Support System contains all sub-systems to support the overall system e.g. governance, test and certification management and security and credentials management.

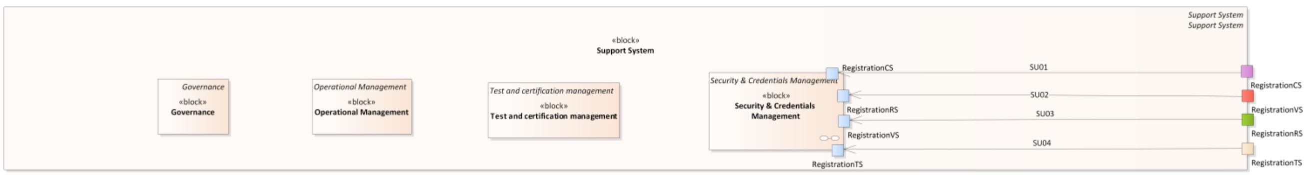


Figure 89: IBD functional diagram of the Support System

Internal Block	Description
Governance	A system from policy makers for regulations & enforcement of the ITS system of environment / safety measures;
Operational Management	A system for operational processes like fault, performance and configuration management of the sub-systems.
Test and certification management	A system for registration of tested and certified communication systems for ITS (safety) applications;
Security & Credentials Management	A high-level aggregate representation of the systems that enable trusted communications between mobile devices, roadside devices and centres, and protect data from unauthorized access. This sub-system will be implemented as an interconnected system of support applications that enable the secure distribution, use, and revocation of trust;

4.2.1.1. Internal communication description

Link Name	Direction	Descriptions
SU01	D	This link is used for certificate request and provision/generation from Central System entities.
SU02	D	This link is used for certificate request and provision/generation from Roadside System entities.
SU03	D	This link is used for certificate request and provision/generation from Vehicle System entities.
SU04	D	This link is used for certificate request and provision/generation from Traveller/VRU System entities.

4.2.1.2. Internal blocks structure

4.2.1.2.1. Security & Credentials Management

The Security & Credentials Management block is a high-level aggregated representation of the systems that enable trusted communications between mobile devices, roadside devices and centers, and protect data from unauthorized access. It contains two independent trust systems, one used for vehicle-to-x communication (V2X) and one for other, IP based communications. The V2X communication is based on the ETSI resp. EU C-ITS security model, whereas the trust system for other communications is based on x.509 certificates.

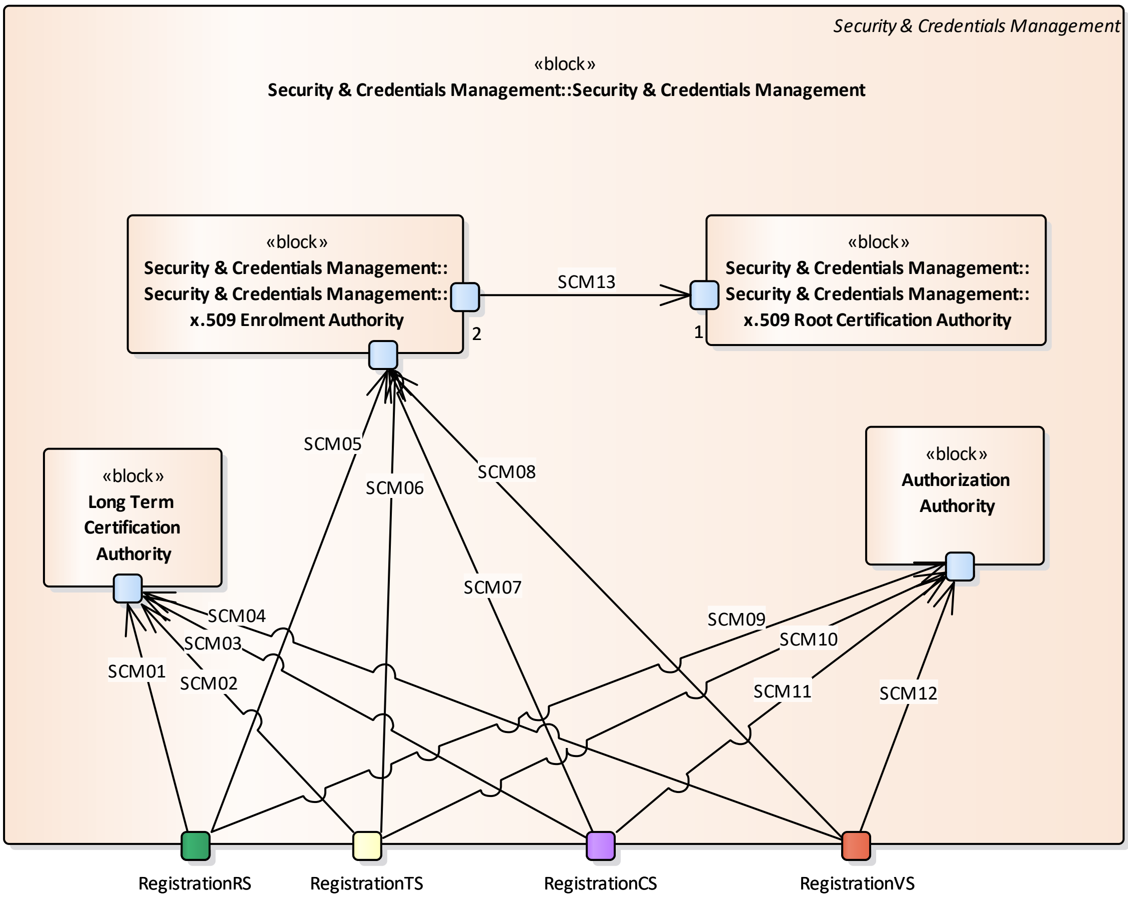


Figure 90: IBD functional diagram of the Security & credentials Management

Internal Block	Description
Long Term Certification Authority	The LTCA is an Enrolment Authority. It is in charge of providing Enrolment Credentials (EC) to ITS Stations (ITS-S). The LTCA is the Enrolment Authority, which issues Enrolment Credentials to ITS vehicle stations, and will most probably be operated by the respective vehicle or vehicle-equipment Manufacturers. The Car-2-Car Communication Consortium (C2C-CC) term for this kind of Enrolment Authority is Long Term Certification Authority (LTCA). The Enrolment Credentials issued by this LTCA are called Long Term Certificates (LTC) by the C2C-CC.
Authorization Authority	An Authorization Authority (AA) is in charge of issuing Authorization Tickets (AT) to ITS-S for use within ETSI ITS G5. There are different implementations of AA's involved: The AA, which issues AT's to IVS. This one is operated by the respective IVS manufacturer. The C2C-CC term for that kind of AA is Pseudonym CA (PCA). The C2C-CC term for AT is Pseudonym Certificate (PC), because of the pseudonymous nature of this certificate.

	The AA, which issues AT's to IRS. This one is probably operated by the Roadside Network operator. These do not have to be pseudonymous and frequently changed like the PCs above. The CONVERGE project introduced a Service Provider CA (SP CA) that will offer service specific AT to ITS-Central Stations for service specific use. (This is covered by the Registration Server in C-MobILE.)
x.509 Enrolment Authority	This entity provides long-term certificates. These certificates are used to uniquely identify participants. They are never used directly for communication or service usage. Instead, they are used to obtain pseudonymous tickets (e.g. for ETSI ITS G5) or pseudonymous x.509 certificates for service usage. The x.509 Enrolment Authority is analogous to the "Long-Term Certification Authority" but for x.509 certificates.
x.509 Root Certification Authority	The Root Certification Authority acts as a trust anchor for one or more Enrolment authorities as well as Registration Server. The certificate of the Root CA needs either to be installed on every participant, or there need to be an additional trust anchor, e.g. the European Trust List Manager of the C-ITS EU Trust Model.

4.2.1.2.1.1. Internal communication description

Link Name	Direction	Descriptions
SCM01	D	Used by roadside equipment to obtain a Long Term Certificate to use ETSI ITS G5.
SCM02	D	Used by traffic management systems/equipment to obtain a Long Term Certificate to use ETSI ITS G5.
SCM03	D	Used by central systems/equipment, e.g. Service Provider BO, to obtain a Long Term Certificate to use ETSI ITS G5.
SCM04	D	Used by vehicle equipment, to obtain a Long Term Certificate to use ETSI ITS G5.
SCM05	D	Used by roadside equipment to obtain a Long Term x.509 Certificate to use TLS.
SCM06	D	Used by traffic management systems/equipment to obtain a Long Term x.509 Certificate to use TLS.
SCM07	D	Used by central systems/equipment, e.g. Service Provider BO, to obtain a Long Term x.509 Certificate to use TLS.
SCM08	D	Used by vehicle equipment, to obtain a Long Term x.509 Certificate to use TLS.
SCM09	D	Used by legitimate roadside ITS stations to query the AA to obtain sets of "Authorization Tickets"/"Pseudonym certificates". Legitimate stations are stations, which want to use ETSI ITS G5 and are in possession of a Long Term Certificate.
SCM10	D	Used by legitimate traffic management systems/equipment ITS stations to query the AA to obtain sets of "Authorization Tickets"/"Pseudonym certificates". Legitimate stations are stations, which want to use ETSI ITS G5 and are in possession of a Long Term Certificate.
SCM11	D	Used by legitimate central systems/equipment ITS stations to query the AA to obtain sets of "Authorization Tickets"/"Pseudonym certificates". Legitimate stations are stations, which want to use ETSI ITS G5 and are in possession of a Long Term Certificate.
SCM12	D	Used by legitimate vehicle equipment ITS stations to query the AA to obtain sets of "Authorization Tickets"/"Pseudonym certificates". Legitimate stations are stations, which want to use ETSI ITS G5 and are in possession of a Long Term Certificate.
SCM13	D	Used by the x.509 Enrolment Authority to obtain certificate signed by Root-CA. This certificate is used to sign the long-term certificates created by the Enrolment Authority.

4.2.2. Central System

The Central System comprised all the sub-systems which aim to support connected vehicles, field and mobile devices and to perform management and administration functions. The sub-systems in this layer are typically virtual systems that can be aggregated together or geographical or functions distributed.

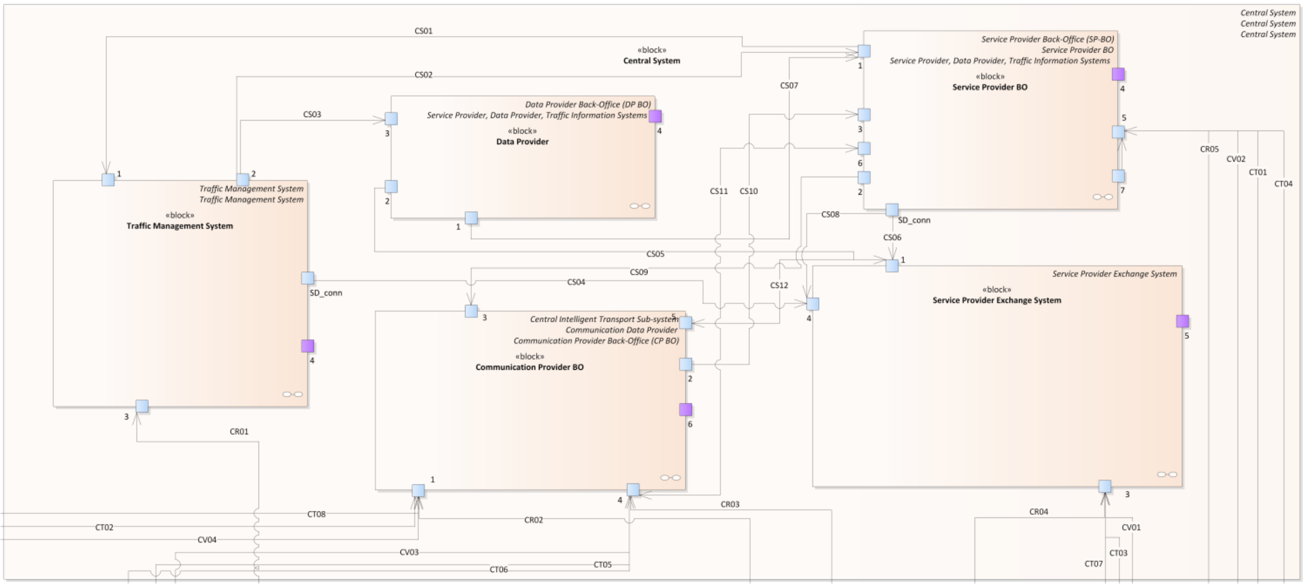


Figure 91: IBD functional diagram of the Central System

Internal Block	Description
Time Management System (TMS)	A TMS is the functional back-office system of the responsible road operator to enforce legal actions on urban or high-way road sections or intersections based on real-time traffic data from loops, cameras, speed sensors, etc. or actions by traffic controllers. The real-time data that flows from the Traffic Info System is integrated and processed by the TMS (e.g. for incident detection), and may result in traffic measures (e.g. traffic routing, dynamic speed limits) with the goal of improving safety and traffic flow.
Data Provider (DP)	A Data Provider BO system is a data system that collects and fuses floating car data and real-time traffic data from roadside sensor systems to increase insight in actual and expected traffic state (e.g. on traffic jams). The DS also distributes enriched (aggregated) information on traffic state (speed, flow and travel times) to service providers.
Communication Provider Back-Office (CP BO)	A generic back-office system of a communication provider used for access at several communication layers from other BO systems (like SP BO, TMS, TIS etc.) to send and receive ITS information to/from vehicles or other users.
Service Provider Exchange System (SPES)	It is an e-Market ('broker') system for discovery and exchange of ITS (end-user) services and ITS communication services; the SPES can support functions like service discovery, service authentication, authorization, accounting (AAA) and billing.
Service Provider Back-Office (SP BO)	A generic back-office system of a service provider used for the specific services of the SP to connected drivers or end-users to inform end users or other SP BO systems from providers. A SP BO can be used to support personal information services for, e.g. navigation or traffic information applications on OBU/PID. A SP BO can also be used to gather floating car data from OBU/PID;

4.2.2.1. Internal communication description

Link Name	Direction	Descriptions
CS01	D	This link is used by the Service Provider Back-Office to pass specific application-related information (e.g. priority requests, EV location data, etc.) to the TMS, which can use them to react accordingly.
CS02	D	The Traffic Management System provides access of collected data to the Service Provider Back-Office through this link.

CS03	D	The Traffic Management System provides access of collected data to the Data Provider through this link.
CS04	D	Link used form the TMS to the Service Provider Exchange System to query the Entries of the Service Directory.
CS05	D	This link is used by the Data Provider to perform management and lookup operations on the Service Directory.
CS06	D	This link is used by the Service Provider Back-Office for management purposes e.g. create/modify/delete entries in the SD, initiate transactions, etc.
CS07	D	The Data Provider is using this link to provide data to the Service Provider BO.
CS08	D	This link is used by the Service Provider Back-Office to query the Entries of the Service Directory.
CS09	D	The Service Provider BO sends the messages to be disseminated to the vehicles and Travellers using this link. The Communication Provider Back-Office is the receiver of this information as it is capable of reaching the end-users.
CS10	B	The data received and collected (vehicles' information) from the RSUs and PIDs will be sent to the Service Provider BO using this link.
CS11	B	GeoMessages received by the GEOM-S from the field devices (RSU, OBU, PID and VRU-OBUs) go through this link to reach the SP-BO, where they can be processed. It also allows managing the registration of the GEOM-Client of the SP BO.
CT01	D	Direct communication from the PID to the Service Provider BO to initially register with a new GEOM-Server.
CT02	B	This link is used for sending and receiving travellers' information to/from Communication Provider Back-Office.
CT04	D	Direct communication from the VRU OBU to the Service Provider BO to initially register with a new GEOM-Server.
CT05	B	This link is used by a PID to use GeoMessaging-related communication with the GEOM-S.
CT06	B	This link is used by a VRU OBU to use GeoMessaging-related communication with the GEOM-Server.
CT07	D	This link is used by a VRU On-Board Unit to get access to the Identity Manager (e.g. certificate signing, etc.).
CT08	B	This link is used to receive messages regarding the Travellers from the SP BOs
CV01	D	This link is used to communicate the OBU with the Identity Manager sub-block, in the SPES block. It is mainly used to get pseudonymous certificates and to register the OBU with the Registration Server.
CV02	D	Direct communication from the OBU to the Service Provider BO to initially register with a new GEOM-Server.
CV03	B	This link is used by the OBU to use GeoMessaging-related communication with the GEOM-S.
CV04	B	This link us used by a OBU to receive messages regarding the Travellers from the SP BOs
CR01	B	Link that connects the TMS to the Roadside Systems. It is used to exchange traffic lights and road sensor information to the TMS and send signalling modification requests and dynamic roadway signs information to the Roadside System (e.g. Green Priority)..
CR02	D	The Application Specific Support sub-block of the RSU receives the event messages to be disseminated to the vehicles using this link.
CR03	B	This link is used by a RSU to use GeoMessaging-related communication with the GEOM-S.
CR04	B	The RSU obtain pseudonyms and communicate with the RS through this link.
CR05	D	Direct communication from the RSU to the Service Provider BO to initially register with a new GEOM-Server.

4.2.2.2. Internal blocks structure

4.2.2.2.1. Communication Provider Back-Office (CP BO)

The Communication Provider Back-Office (BO) is a system of a communication provider used for access to several communication layers. It connects with other BO and roadside systems (like SP BO, TMS, etc.) on the infrastructure side, but also sends and receives ITS information to/from vehicles or other road users.

There are three functional sub-blocks, which can be provided by different companies. These sub-blocks and their interfaces are described in more detail in the following sections.

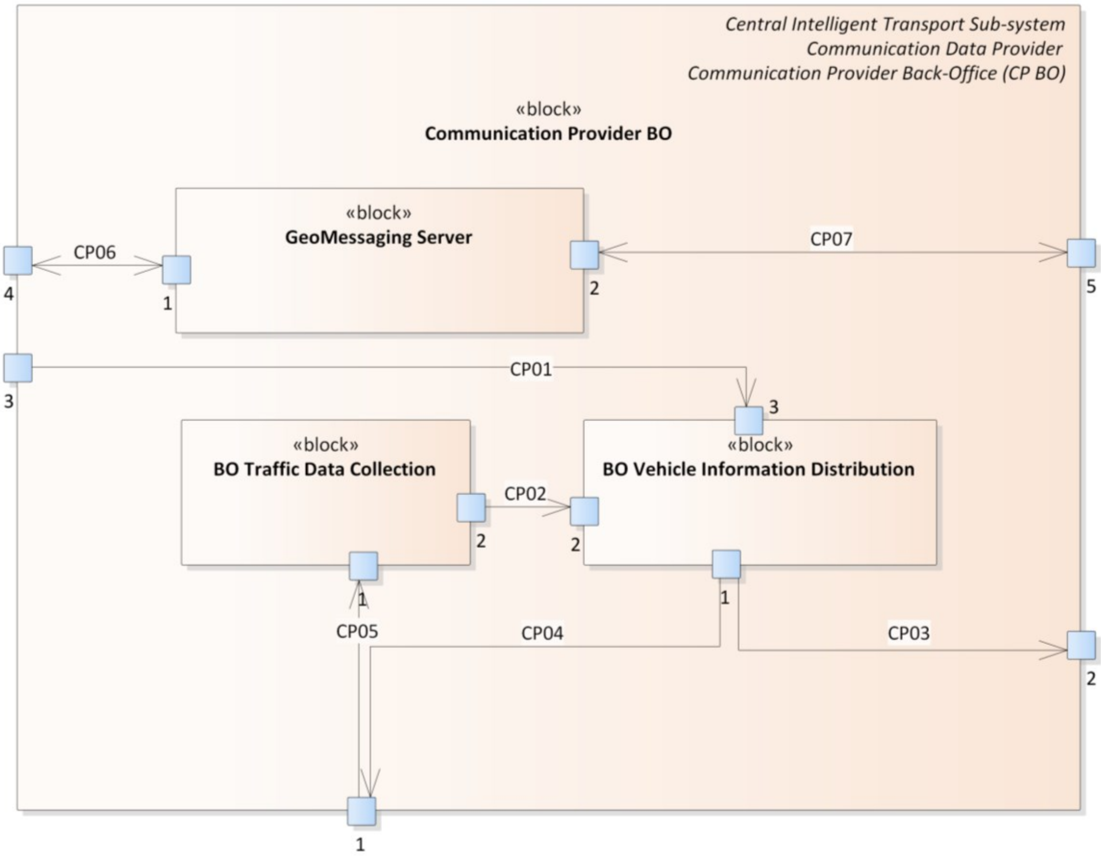


Figure 92: IBD functional diagram of the Communication Provider BO

Internal Block	Description
GeoMessaging Server	GeoMessaging enables location based communication. This way, road users in Copenhagen will not receive data for Barcelona. The communication can be bi-directional. The easiest example is the MAPEM/SPaTEM data for the GLOSA service, the data of a particular intersection only needs to be sent to road users in the vicinity. The other way around, Signal Request Messages for green priority and CAM for probe vehicle data can be forwarded only to back offices and road side systems that supervise a certain area.
BO Vehicle Information Distribution	Collects information about road and traffic conditions from various sources and distributes it to road users. The information can be distributed directly using unicast or through GeoMessaging depending on the service. Another possibility is to disseminate through local RSUs connected to GeoMessaging.
BO Traffic Data Collection	Collects traffic flow and other real-time information either directly from road users or through RSUs. The data is shared with other systems for instance in case the TDC is a probe vehicle data service provider.

4.2.2.2.1.1. Internal communication description

Number	Direction	Description

CP01	D	Information from SPs that has to be distributed to road users travel through this link to reach the Distribution sub-block.
CP02	D	Link to send the collected information from the vehicle to the Vehicle Information Distribution sub-block. This information can be sent to the Service Provider Back-Office using the link CP03 or sent to another type of end-users using the link CP04.
CP03	D	Connects the CP BO with the SP BO in order to deliver collected vehicles' messages.
CP04	D	Link that represents the dissemination of messages to the field devices (RSU, OBU, VRU OBU, PID)
CP05	D	Through this link the vehicles' messages enter this block and are collected.
CP06	B	Link that allows the GEOM-S to exchange information with the GEOM-Cs presents in the OBU, PID, VRU OBU RSU and SP BO. It is used for both authentication and data flows. The latter uses MQTT protocol and has a special topic structure to enable efficient geo-casting and geo-reception.
CP07	B	The GEOM-S uses this link to perform management and lookup queries to the SD. Metadata about the contents of the GeoMessaging server is available in the service directory. Therefore, the information needs to be synchronized. Optionally, for paid services, the billing data is also exchanged over this interface.

4.2.2.2.2. Service Provider Exchange System (SPES)

The Service Provider Exchange System (SPES) provides the functionality of an e-Market ('broker') system for discovery and exchange ITS (end-user) services and ITS communication services; the SPES can support functions like service discovery, service authentication, authorization and accounting (AAA), as well as_billing for support the business models detected within the project.

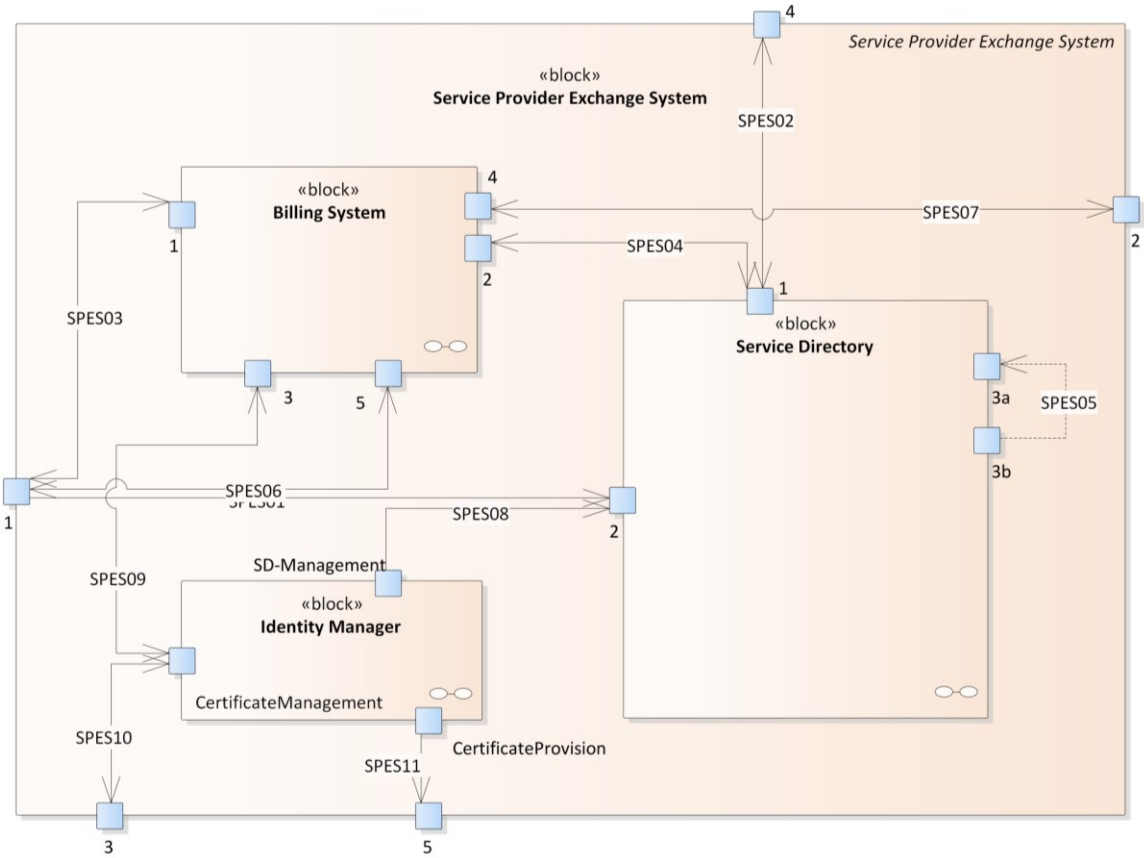


Figure 93: IBD functional diagram of the Service Provider Exchange System

Internal Block	Description
Billing System	Support system that handles all financial transactions and provides a neutral instance which monitors the transactions between different parties.

Identity Manager	Provides capabilities to manage common identities and to handle all security and privacy related concerns.
Service Directory	The Service Directory contains a listing of the services available in the network. Special extensions will feature specific concepts of certain technologies, like DAB and TPEG, to include them fully into the Service Directory concept.

4.2.2.2.2.1. Internal communication description

Link Name	Direction	Descriptions
SPES01	D	It allows many other entities to interact with the Service Directory (SD) over the Management Interface, e.g. Inscribing the modules to the Service Directory, create and delete Entries/Services to the SD Database.
SPES02	B	This link provides access to the SD Lookup Interface. The interface offers the possibility to query Entries from the SD.
SPES03	B	This link is used to enable the communication between Service Provider and Billing System. Therefore this link allows many management operations such as initiating payments creating and modifying subscriptions.
SPES04	B	Over this link billing details for a specific service get queried by the Billing System.
SPES05	D	This Link is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance.
SPES06	B	All bills and invoices generated after a transaction are sent back to the end-user over this link. It also allows to retrieving passed transaction details.
SPES07	B	This is a generic link in order to communicate with external payment entities/systems in order to perform the transactions with the corresponding Financial Centres (e.g. PayPal, direct bank transactions, etc.)
SPES08	D	This link is used to communicate with the Service Directory (SD). This is necessary, as each Registration Server (Identity Management) is listed in the SD, so that possible clients can find it. Over this connection, the entries of specific Registration Servers are created and managed.
SPES09	B	The Billing System uses this link to connect with the Identity Manager in order to validate/authenticate the users, their permissions and other security information that can make the transactions safer.
SPES10	B	This link is used by the Management Client (mainly) to manage the user certificates. The IDM signs and return it to the User Management Client to have a valid identification.
SPES11	D	This link describes the connection to the X.509 Root Certification Authority. It is needed to request a signed certificate which is used to validate the trust of a user.

4.2.2.2.2.2. Internal blocks structure

4.2.2.2.2.2.1 Billing System

The Billing System handles all the financial transactions within C-MobILE. It also provides a neutral instance which monitors the transactions between different parties. It allows the use of third party paying sites as well as one time and recurring payments. The Billing System is comprised in the Service Provider Exchange System. This Billing System is a primitive version that only covers two of the business models identified in C-MobILE. Further work on this module will be elaborated in future tasks.

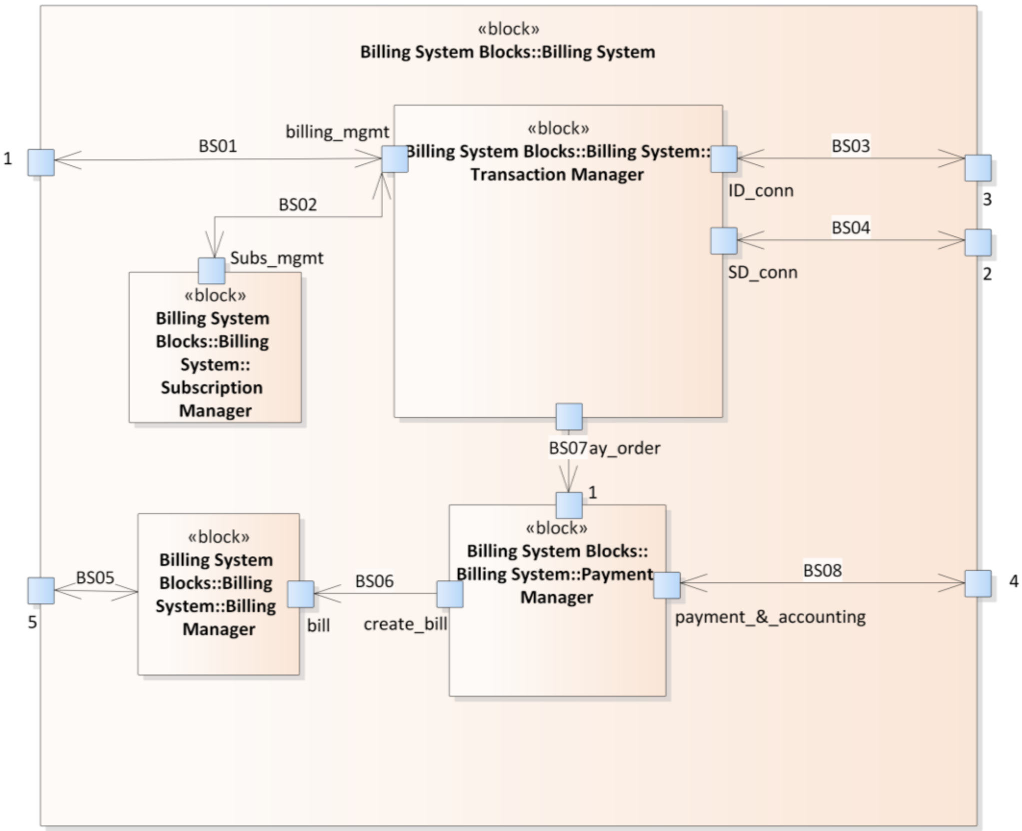


Figure 94: IBD functional diagram of the Billing System

Internal Block	Description
Transaction Manager	Manager of the Billing System. It governs/manages the transaction from the very beginning and passes the needed information to complete the transaction to the Payment Manager.
Subscription Manager	It manages the payment subscriptions and initiates transaction when needed.
Billing Manager	It is in charge of generating the bills/invoices from received transaction details.
Payment Manager	It manages the communication with the External Payment Systems and the corresponding Transaction tokens and payment status messages.

4.2.2.2.2.2.1.1 Internal communication description

Link Name	Direction	Description
BS01	B	Communication with the Service Provider to initiate payments and manage transaction subscriptions (i.e. create/modify/delete subscriptions).
BS02	B	Allows initiating periodic transactions and to create/modify/delete subscriptions for periodic payments.
BS03	B	Communicates the Transaction Manager with the Identity Manager. It allows checking the user permissions and getting the user billing details, as well as registering the Billing System to the C-MobILE architecture.
BS04	B	Communicates the Transaction manager with the Service Directory. It provides the billing details, including the amount to pay, provider payment details, etc. from the Service Provider.
BS05	B	Link that allows transferring the invoices from the Billing Managers to the end-users and also used to get invoices and details from passed transactions.
BS06	D	Used to transfer the bill or invoice corresponding to a transaction from the Payment Manager to the Billing manager.
BS07	B	Initiates the final phase of the transaction by passing the transaction details to complete the payment.

BS08	B	Interface with trusted external payment methods such as PayPal, Bank API, etc.

4.2.2.2.2.2.2 Identity Manager

The Identity Manager (IDM) provides the capabilities necessary to manage pseudonyms and to handle privacy related concerns. It is an essential part in the C-MobILE privacy concept, as it provides a possibility to distribute pseudonymous service certificates to users, after checking their long-term certificate.

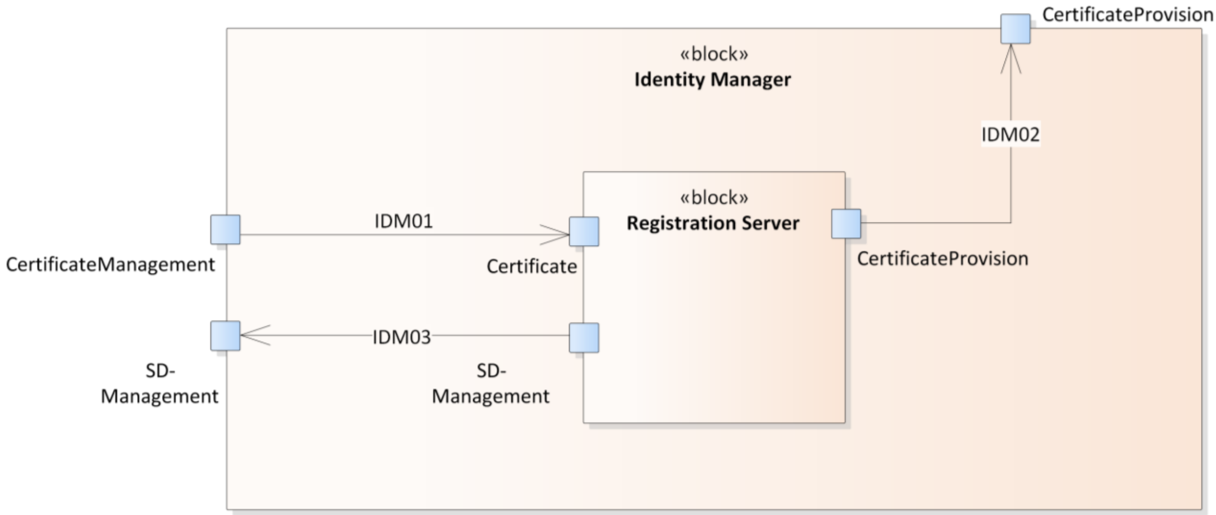


Figure 95: IDB functional diagram of the Identity Manager

Internal Block	Description
Registration Server	The Registration Server (RS) is the core element of the Identity Manager. It provides a link from Pseudonymous Service Certificates to long-Term Certificates/Pseudonymous of users. This makes it possible in the event of a lawful intervention to identify a specific user, whereas it is impossible for Service Providers or other architectural entities to identify a specific user based on the pseudonymous service certificate alone. There will most probably be multiple implementations of the Registration Server.

4.2.2.2.2.2.2.1 Internal communication description

Link Name	Direction	Description
IDM01	B	This link is used by clients of the IM/RS. They use it to send in their pseudonymous service certificates as well as a proof that they are in possession of a long-term certificate. The RS will, after it verified the proof, send back a pseudonymous service certificate, signed with his private key, as well as his public certificate including the certificate chain, so clients can use this information as authorization tokens for other services.
IDM02	B	This link is used by RS to obtain a signed certificate from the x.509 Root-CA to sign the pseudonymous service certificates with. This is done to establish a chain of trust, so that clients do not need to verify the trust into each individual RS, but can trust the central Root-CA instead.
IDM03	D	This link is used to communicate with the Service Directory (SD). This is necessary, as each Registration Server (RS) is listed in the SD, so that possible clients can find it. Over this connection, the entries of specific RS's are created and managed.

4.2.2.2.2.2.3 Service Directory

The Service Directory contains a listing of the services available in the network. Special extensions will feature specific concepts of certain technologies, like DAB and TPEG, to include them fully into the Service Directory concept.

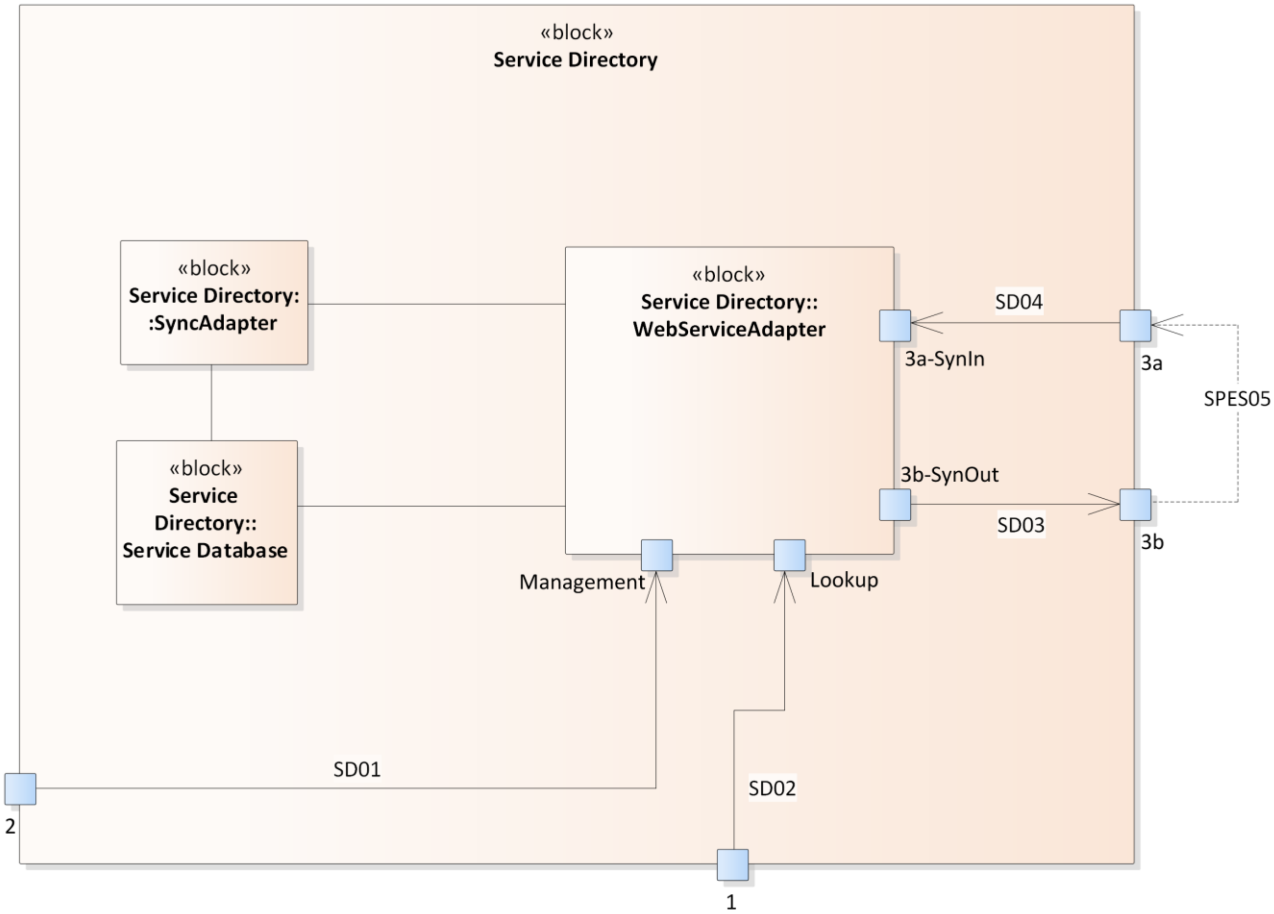


Figure 96: IBD functional diagram of the Service Provider

Internal Block	Description
WebServiceAdapter	The WebServiceAdapter adapts the ServiceDatabase to the WebService interface.
SyncAdapter	This adapter implements the synchronization facilities of the ServiceDirectory.
Service Database	This database contains a listing of all ServiceEntries known to the ServiceDirectory.

4.2.2.2.2.2.3.1 Internal communication description

Link Name	Direction	Descriptions
SD01	D	This link is needed by many other entities to interact with the Service Directory (SD) over the Management Interface, e.g. Inscribing the modules to the Service Directory, create and delete Entries/Services to the SD Database
SD02	D	This link provides access to the SD Lookup Interface. The interface offers the possibility to query Entries from the SD.
SD03	D	This link is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance.
SD04	D	This link is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance.
SD05	D	This link is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance.

4.2.2.2.3. Service Provider Back-Office (SP BO)

The Service Provider Back-Office (SP BO) is a generic back-office system of a service provider used to manage and send messages from/to end users and data providers for the specific services. A SP BO can be used to support personal information services for, e.g. navigation or traffic information applications on OBU/PID, as well as to gather floating car data from connected vehicles and end-users' devices.

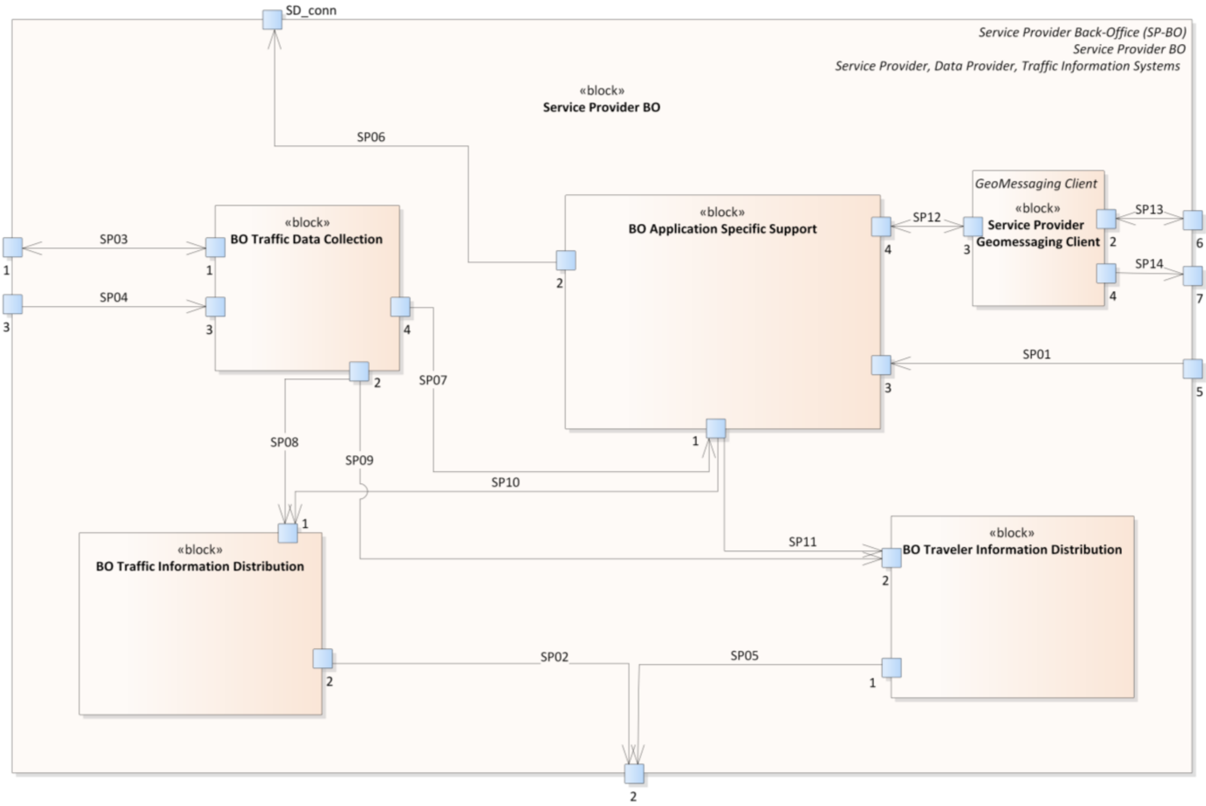


Figure 97: IBD functional diagram of the Service Provider Back-Office

Internal Block	Description
BO Traffic Data Collection	Current traffic information and other real-time transportation information are collected from several sources like TMS and connected vehicles/devices. It decides whether this information needs to be treated by the internal locks or needs to be forwarded to external blocks.
BO Application Specific Support	This block is in charge of treating the messages coming from the different data sources by the corresponding application/service. If the application decides that a piece of information needs to be delivered to a user or a set of users, it contacts the distribution block to reach the proper users. At the same time, it manages the GEOM management data coming from the field equipment (RSU, OBU, PID and VRU OBU) in order register for the first time and determine the communication details between the GEOM-C and the proper GEOM-S.
BO Traffic Information Distribution	Disseminates traffic and road conditions, closure and detour information, incident information, driver advisories, and other traffic-related data to the vehicles, as well as to other centres and the media (e.g. radio, Service Providers) if needed.
BO Traveller Information Distribution	Disseminates traveller information including event information, transit information, parking information and weather information to the cellular-based devices and VRUs.
Service Provider GeoMessaging Client	Allows the Service Provider to contact the GeoMessaging Servers in order to exchange geo-referenced messages.

4.2.2.2.3.1. Internal communication description

Link Name	Direction	Descriptions
SP01	D	Incoming management data comes from this port. This data is mainly comprised by registration requests to the GEOM system. The SP BO returns key information that allows the registered entities (RSU, OBU, PID and VRU OBU) to use the GeoMessaging system.
SP02	D	Used to send the traffic information from the distribution block to lower layers in order to reach the vehicles.
SP03	B	Through this connection, relevant road and traffic information coming from the TMS and Data Providers reaches the BO Traffic Data Collector. The incoming information could be related to several services like RWW, RHW, GLOSA or IVS. On the other hand, this link also returns to the TMS: Application Specific Support block to forward special information such as priority requests or Emergency Vehicles location data.
SP04	D	This link contains data coming from the vehicles which has nothing to do with the GeoMessaging, e.g. floating data, priority requests, etc. The information is passed to the collector that will decide whether it needs to pass it to the BO Application Specific Support, or to external blocks such as the TMS.
SP05	D	Used to send relevant information from the distribution block to lower layers in order to reach the travellers.
SP06	D	Offers an connection to perform management and lookup operations to the Service Directory, which allows the SP BO to check the services permissions, particular GEOM information of the services, etc.
SP07	D	This link is used for sending the collected information to the BO Application Specific Support.
SP08	D	Allows the BO Traffic Data Collector to disseminate specific information to the vehicles.
SP09	D	Allows the BO Traffic Data Collector to disseminate specific information to the travellers.
SP10	D	Allows the BO Application Specific Support to disseminate specific information to the vehicles.
SP11	D	Allows the BO Application Specific Support to disseminate specific information to the travellers.
SP12	B	Used to send GeoMessages to the SPO:GEOM-C in order to reach the GEOM-S and deliver them. It also allows to other way around to receive GeoMessages send by the field entities.
SP13	D	Used for exchanging GeoMessages between the SPBO:GEOM-C and the GEOM-Servers.
SP14	D	Allows the SP BO with GeoMessaging to communicate with other instances of "GeoMessaging SP BO" implementations to register them.

4.2.2.2.4. Data Provider

A Data Provider system is a data system that collects and fuses floating car data and real-time traffic data from roadside sensor systems to increase insight in actual and expected traffic state (e.g. on traffic jams). The DP also distributes enriched (aggregated) information on traffic state (speed, flow and travel times) to Service Provider BOs.

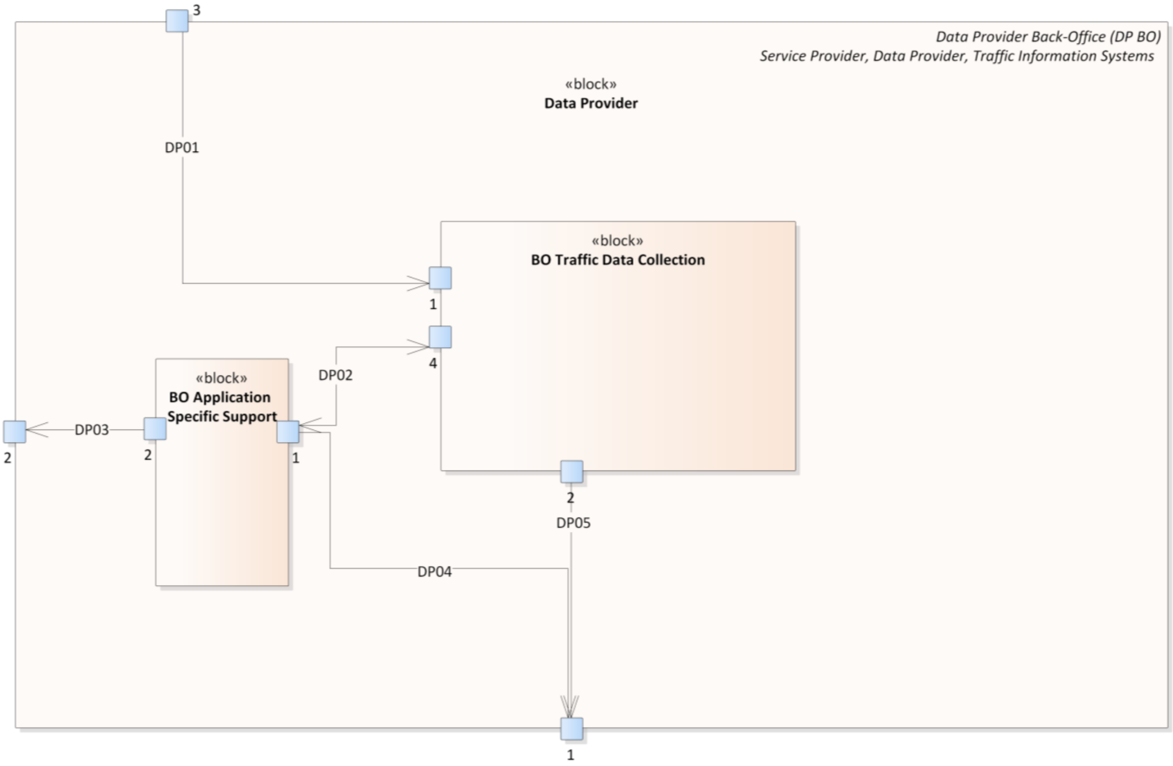


Figure 98: IBD functional diagram of the Data Provider Back-Office

Internal Block	Description
BO Traffic Data Collection	Current traffic information and other real-time transportation information are collected from several sources like TMS, Roadside Systems and open databases
BO Application Specific Support	It manages application-specific data and is capable of contacting the SD.

4.2.2.2.4.1. Internal communication description

Link Name	Direction	Descriptions
DP01	D	This link is used to receive traffic data information from TMS or Open Databases and store them in the BO Traffic Data Collection.
DP02	B	This link connects the BO Application Specific Support with the BO Traffic Data Collection. This is needed to receive application-specific information in the BO TDC to distribute them to Vehicle and Traveller systems.
DP03	D	This link is used to lookup (query) information about the provided services.
DP04	D	This link is used to provide application-specific information, e.g. parking to the SP BO.
DP05	D	The collected traffic data information will be distributed to SP BO over this link.

4.2.2.2.5. Traffic Management System (TMS)

A TMS is the functional back-office system of the responsible road operator to enforce legal actions on urban or high-way road sections or intersections based on real-time traffic data from loops, cameras, speed sensors, etc. or actions by traffic controllers. The real-time data that flows from the Traffic Info System is integrated and processed by the TMS (e.g. for incident detection), and may result in traffic measures (e.g. traffic routing, dynamic speed limits) with the goal of improving safety and traffic flow.

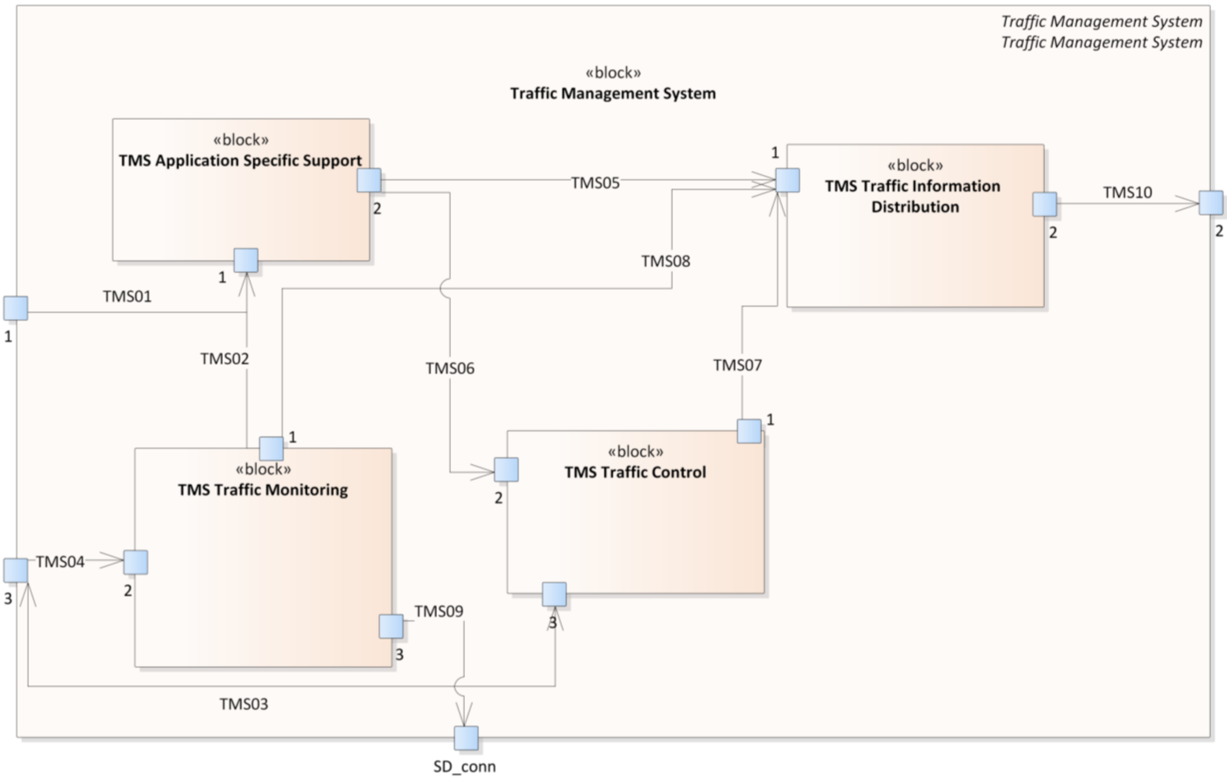


Figure 99: IBD functional diagram of the Traffic Management System

Internal Block	Description
TMS Application Specific Support	Block designed for implementing specific functionalities of certain C-MobILE services if required, e.g. Green Priority, EVW, etc.
TMS Traffic Control	Controls driver information system field equipment including dynamic message signs, managing dissemination of driver information through these systems
TMS Traffic Information Distribution	Sends traffic and road conditions, dynamic speed limits, closure and detour information, incident information, driver advisories, and other traffic-related data to the Data Providers and Service Providers BO.
TMS Traffic Monitoring	Remotely monitors traffic sensors and surveillance equipment (cameras), and collects, processes and stores the collected traffic data.

4.2.2.2.5.1. Internal communication description

Link Name	Direction	Description
TMS01	D	For certain services, contains generic request/information, e.g. green priority request, emergency vehicle location, data, etc., from the SP BO and DP.
TMS02	D	Link used to pass specific information from the Roadside Systems to the Application Specific Support.
TMS03	B	It contains control/requests of the signalized intersection/ramps and dynamic roadway signs. These requests go to the Roadway local traffic monitoring and control distribution, which forwards it to the Roadway signal control (of the RS). This link is also used to receive control information from the Roadside System, i.e., status data from the Roadway local traffic monitoring and control distribution.
TMS04	D	This link is also used to receive information from the Roadside System, i.e., monitored information from the Roadway local traffic monitoring and control distribution.
TMS05	D	Link used by the Application Specific Support sub-block to send messages that need to be distributed.

TMS06	D	Link used by the Application Specific Support sub-block to send detected requests to the TMS Traffic Control.
TMS07	D	Provides information related to the phase and time of the streetlights as well as other information related to dynamic signs to the distribution sub-block.
TMS08	D	Provides the information (traffic density, road condition, accidents, etc.) obtained by cameras, induction loops and other traffic sensor to TMS Traffic Information Distribution.
TMS09	D	It allows performing lookup queries to the Service Directory.
TMS10	D	Provides access of collected data and generated messages in the TMS to the SP BO and SP. This data is further processed and sent to the end-users if needed.

4.2.3. Roadside System

The Roadside Systems covers the ITS infrastructure on or along the physical road infrastructure, e.g. surveillance or control devices (signal/lane control, ramp meters, or systems to supply information to connected vehicles or to the TMSs. The Roadside layer contains the following sub-blocks:

- The Roadside System (RS) is in charge of gathering data from sensors and traffic equipment controllers and distributes it. The block is further described in 4.2.3.2.1
- The Roadside Unit (RSU) has dual functionality. It is the first contact point for exchanging C—ITS messages from the vehicles/OBUs to the infrastructure and vice versa, as both RSU and OBU are communicating via IEEE 802.11p protocol, while the RSU is connected to the infrastructure permanently. The block is further described in 4.2.3.2.2

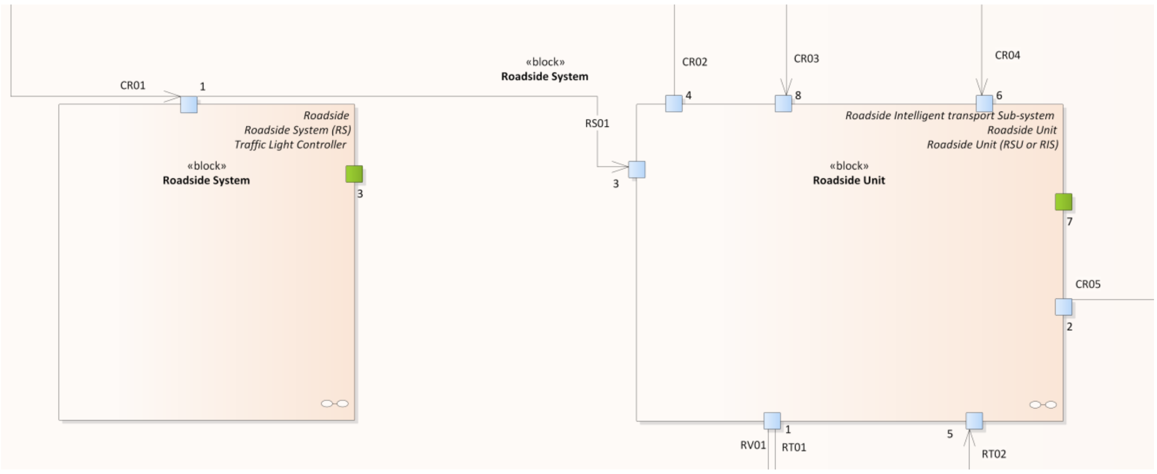


Figure 100: Functional diagram of the Roadside Layer

Internal Block	Description
Roadside System	Different types of existing roadside systems are identified. This Roadside Systems include possible sensor and controllers deployed in the roadside. The information of which is sent to the RSUs and the TMS to be processes and used by the C-MobILE services. A detailed description of this block can be found in 4.2.3.2.
Roadside Unit	A RSU is a cooperative roadside communication system responsible for the two-way communication functionality in a section of the road network. More detail in 4.2.3.2.2

4.2.3.1. Internal communication description

Link Name	Direction	Description
CR01	B	Communication between the RS and the TMS. The main functionality is to pass roadside information (sensors, traffic lights phase, traffic controller status, etc.) to the Traffic Management System. At the same time, the TMS can send requests to the RS, e.g. traffic lights phase change, etc., using this link.

RS01	D	Used to send information to the RSU that needs to be forwarded to the vehicles or to the SP BO, depending on the service and the current situation. Contains warnings and green time from the Roadside System to be disseminated to the vehicles and intersection status, sensor data, signage data that may be of interest to the Service Provider Back-Office.
RV01	D	Used by the RSU to communicate over the air interface (802.11p) with other traffic participants, like vehicles/OBUs and VRU OBUs.
CR02	D	Receives the event messages to be sent to the vehicles (using the link RV01) from the Communication Provider BO in the Central System.
RT02	D	Receives all messages broadcasted by the vehicles with their dynamic information as well as traffic, environmental and emissions data from passing vehicles.
CR04	B	Used by the RSU to obtain pseudonyms and communicate with Registration Server to be part of the C-MobILE architecture.
CR03	B	Communication to exchange GeoMessaging messages to a GEOM-S.
SU3 (RS)	D	RS management of the certificates with the Support System.
SU3 (RSU)	D	RSU management of the certificates with the Support System.

4.2.3.2. Internal blocks structure

4.2.3.2.1. Roadside System

Different types of existing roadside systems are identified:

- Roadside Substation (RSS): a system deployed along highways and includes sensors (loops), control logic and actuators. The system can run as a stand-alone closed loop system i.e., it runs standalone local traffic control functions (e.g. traffic jam tail detection and warning via Variable Message Signs) or can be controlled by the TMS;
- Traffic Light Controller (TLC): a TLC is a specific type of roadside system. It includes the input from loop detectors or other sensors, control logic, and the actuation of the traffic lights. A TLC can be run as a stand-alone closed-loop traffic control system. A TLC can also be controlled by a central TMs, e.g. in green wave applications between different TLC's. A TLC is deployed on urban road or can be deployed at highway access roads for access control;

The IBD of the Roadside System can be seen in Figure 101.

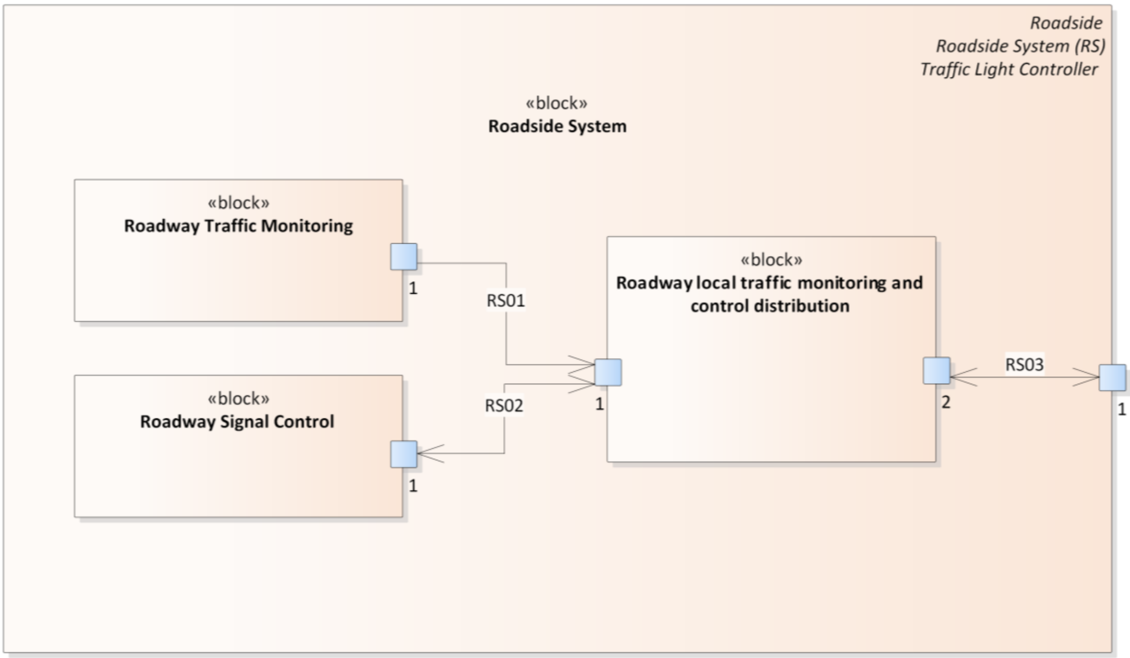


Figure 101: IBD functional diagram of the Roadside System

Internal Block	Description
Roadway Traffic Monitoring	Monitors traffic conditions (number of vehicles on the road, if there is traffic jam or not, etc.) using fixed equipment such as loop detectors and cameras.
Roadway Signal Control	It monitors and controls signalized intersections/ ramps and dynamic roadway signs. Roadway variable speed limits, field equipment, physical overhead lane signs, roadway signal control, traffic signal controllers, signal heads, detectors, other ancillary equipment.
Roadway local traffic monitoring and control distribution	Receive information from the Roadway Traffic Monitoring and Roadway Signal Control in order to send this information to the Traffic Management System or to the vehicles via a RSU. It is also able to forward received control requests from the TMS to the Roadway Signal Control.

4.2.3.2.1.1. Internal communication description

Link Name	Direction	Description
RS01	D	Provides traffic information to be distributed to the central systems (TMS) and RSUs.
RS02	B	The Roadway Signal Control sub-block is able to monitor some traffic information (loop detections, cameras, etc.). The information gathered is send to the Roadway Local Traffic Monitoring and Control Distribution using this link. The Roadway local traffic monitoring and control distribution also forwards the input received from the TMS to the Roadway Signal Control through this interface.
RS03	B	This links has multiple functionalities: / Destination TMS: used to send information to the central layer in order to process the gathered information and generate the corresponding events that will reach the users. / Destination RSU: used to send information to the RSU to forward the information to the vehicles. / Source TMS: used to forward the control orders to the Roadway Signal Control.

4.2.3.2.2. Roadside Unit

Roadside Unit (RSU) or Roadside ITS System (RIS): A RSU/RIS is a cooperative roadside communication system responsible for the two-way communication functionality at a part of a road network (typically an intersection or a road section of 500m – 1km). This block is responsible for implementing communication functionality in the roadside layer and optionally application functions. A RSU/RIS is included in the ITS reference architecture standardised by ETSI ITS. A RSU/RIS can be part of the roadside communication network with distributed radio units, and centralized functions in the Communication Provider Back-Office.

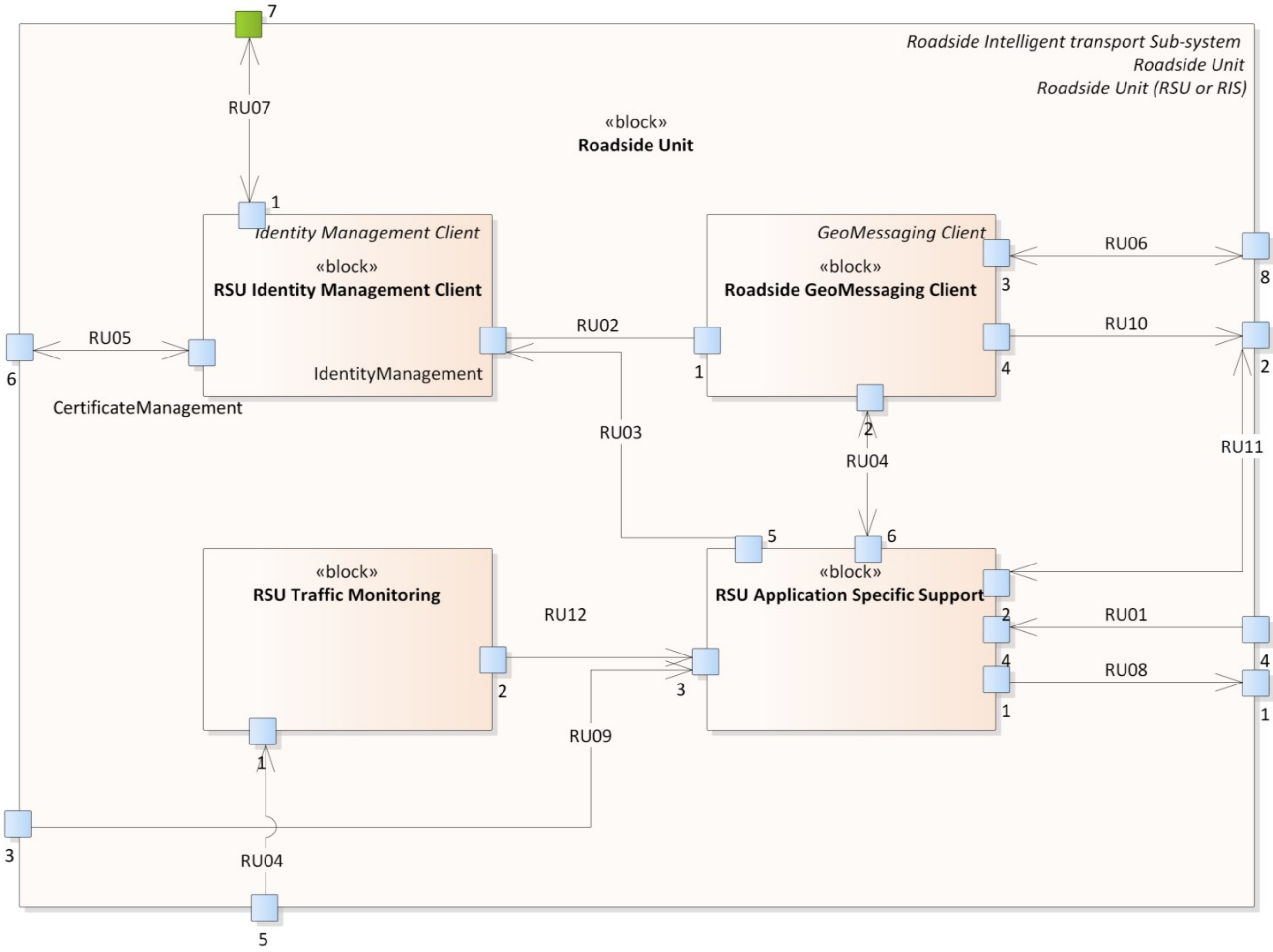


Figure 102: IBD functional diagram of the Roadside Unit

Internal Block	Description
Roadside GeoMessaging Client	This module communicates with the GEOM-Server in order to send and receive geo-referenced messages. It also communicates with the Identity Management Client providing pseudonymous certificates to use GeoMessaging services.
RSU Traffic Monitoring	Vehicle V2V safety messages that are shared between connected vehicles and distils this data into traffic flow measures that can be used to manage the network in combination with or in lieu of traffic data collected by infrastructure-based sensors. Also supports incident detection by monitoring for changes in speed and vehicle control events that indicate a potential incident
RSU Application Specific Support	It is the central sub-block of the RSU, which manages the identity, multiple types of messages/data and could be capable of implementing certain services/applications as well, e.g. RSU Intersection Management, Intersection Safety, Queue Warning, Speed Management, Speed Warning, Parking Management, etc. In general, besides the management functionality, this block collects current status information from local field devices including intersection status, sensor data, and signage data, providing complete, configurable monitoring of the situation for the local transportation system in the vicinity of the RSU. From all this information, location-specific or situation-relevant information is sent to short-range communications transceivers to reach the users.
RSU Identity Management Client (IM-C)	This module is a specialization of the Identity Management Client which for vehicles. It manages the identity and privacy of the RSU in terms of pseudonymous requests, certification and registration.

4.2.3.2.2.1. Internal communication description

Link Name	Direction	Description
RU01	D	Link used to receive the event messages to be sent to the vehicles from the Communication Provider BO in the Central System.
RU02	B	The IM-C provides pseudonymous certificates for the GEOM-C to allow the RSU to use GeoMessaging.
RU03	D	Allows requesting identities/pseudonyms to the IM-C in order to register the RSU to the C-MobILE System
RU04	D	Link used to receive all messages broadcasted by the vehicles/OBUs and VRU OBUs.
RU05	B	Via this link, the communication to the Identity Management functionality is performed. It is used to get pseudonymous certificates and to register the RSU to the Registration Server.
RU06	D	Link used to exchange GeoMessages with the GEOM-S located at the CP BO.
RU07	B	The IM-C communicates with the Support System to get certificates from the RootCA using this link.
RU08	D	It is used to disseminates messages (gathered from the BO and Roadside Systems or generated in the RSU) to the vehicles
RU09	D	This object collects current status information from local field devices including intersection status, sensor data, and signage data, providing complete, configurable monitoring of the situation for the local transportation system in the vicinity of the RSU.
RU10	D	The GEOM-C of the RSU communicates with a Service Provider BO to initially register with a GeoMessaging Server.
RU11	B	The RSU Application Specific Support can communicate with one or more SP-BO's which provides backend functionality for the applications using this link.
RU12	D	The information coming from the Roadside System is gathered in the RSU Situation Monitoring and sent to the Application Specific Support sub-lock, where this information is processed and some actions are taken.

4.2.4. Vehicle System

The Vehicle System is a set of sub-systems, which are integrated within the vehicles and Powered Two-Wheelers (PTWs). It consists of the following main sub-systems:

- On-Board Unit: The OBU represents the communications functionality of a vehicle, being able to exchange information with other IEEE 802.11p-compatible devices, such as RSUs and other OBUs/vehicles, as well as treat the received information and reach accordingly. It consists of the Vehicle V2V Safety sub-block, the Vehicle Roadside Information Reception sub-block, the Vehicle Traveller Information Reception sub-block and the Vehicle Application Specific Support sub-block. Those sub-blocks are further explained below.
- Vehicle Electrical & Electronic System: This block represents the sensors and automated systems of the vehicles, in case they are available. It consists of the Advance Driver Assisted System sub-block and the Vehicle Monitoring sub-block, which are further explained below.

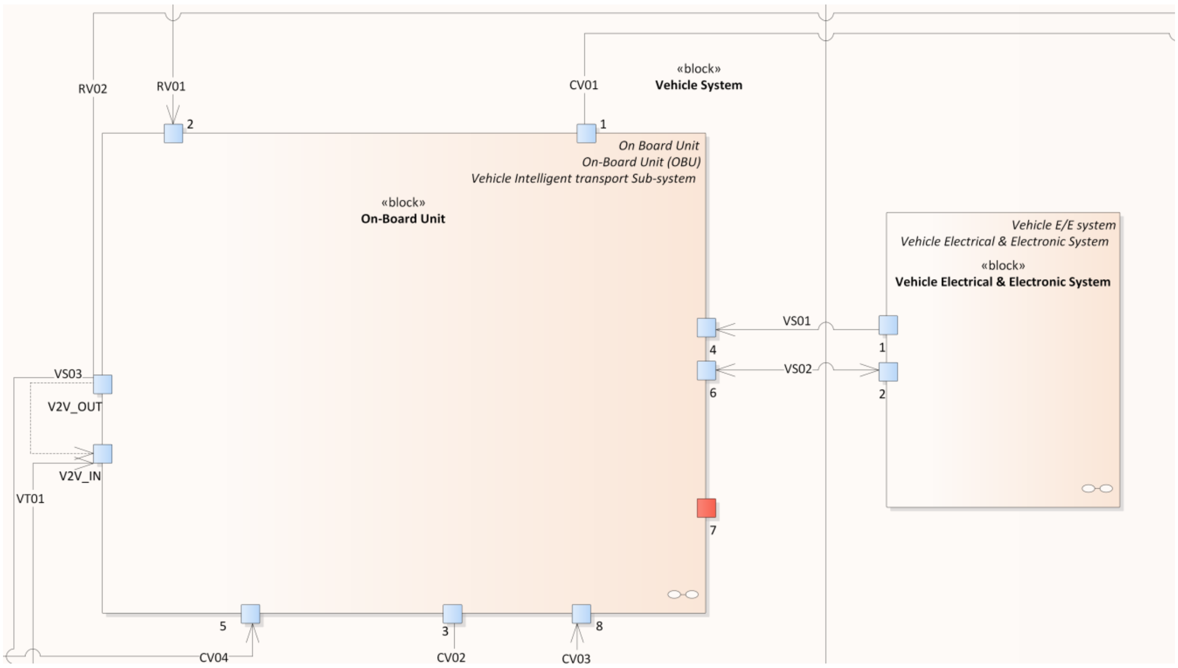


Figure 103: IBD functional diagram of the Vehicle System

Internal Block	Description
On-Board Unit (OBU)	An on-board unit is a sub-system attached to a car and needed for driver assisted applications to inform a driver via a HMI. The OBU provides the vehicle-based processing, storage, and communications functions necessary to support connected vehicle operations. The radio(s) supporting V2V and V2I communications are a key component of the Vehicle OBU.
Vehicle Electrical & Electronic System (VEE)	The Vehicle Electrical and Electronic system includes all in-car sensors (speed, lights, etc.) and actuators (brake, etc.). The Vehicle Electrical and Electronic system provides sensor information (e.g. speed) from a vehicle to an external C-ITS system and optionally enables the control/actuation (e.g. speed control) of that vehicle by an external system. The Vehicle E/E must include safety measures to ensure the safe operation of the vehicle, independent of the interaction between the Vehicle Electrical & Electronics System and external sub-systems. A further differentiation can be made per vehicle type, e.g. emergency vehicle, commercial vehicle or (public) transport/transit vehicle.

4.2.4.1. Internal communication description

Link Name	Direction	Description
CV01	D	This link is used to communicate the OBU with the Identity Manager sub-block, in the SPES block. It is mainly used to get pseudonymous certificates and to register the OBU with the Registration Server.
CV02	D	This link is used to communicate with the BO Application Specific Support located at the Service Provider BO. It might be used for several purposes e.g. request and validate user and service with the service certificate.
CV03	B	This link is used to communicate with the Communication Provider Back-Office module in order to exchange GeoMessages with the GEOM-Server.
RV01	D	This link represents the reception of event messages sent by the RSU to the vehicle.
VS01	D	This link is used internally by the on-board unit to collect and process data and environmental situation data from on-board sensors to detect certain situations.
VS02	B	It is used to manage/order actions to the ADAS system (if enabled) in the Vehicle Electrical & Electronic System, as well as gather some relevant data from this ADAS system. It can be used for specific use cases where the vehicles behave autonomously in a certain way.
V2V_IN	D	This link is used to receive messages over IEEE 802.11p (Vehicle State/Warning CAM/DENM) from other Vehicle On-Board Units (represented as a dashed loop connector in the diagram) or VRU-OBU devices. The reception of the messages from the RSU is represented by the interface RV01.

V2V_OUT	D	This link is used to send messages over IEEE 802.11p (Vehicle State/Warning CAM/DENM) to other Vehicle On-Board Units, VRU-OBU and RSU devices.

4.2.4.2. Internal blocks structure

4.2.4.2.1. On-Board Unit

As mentioned above, an on-board unit is a sub-system attached to a car that support driver assisted applications to inform a driver. The OBU provides the vehicle-based processing, storage, and communications functions necessary to support connected vehicle operations supporting V2V and V2I communications.

The On-Board Unit consists of the following main sub-systems:

- Vehicle System GeoMessaging Client: This Block takes over the functionality of a GeoMessaging Client. It communicates with the central layer whenever the vehicle changes its location related to the predefined map tiles.
- Vehicle Identity Management Client: This block is a specialization of the Identity Management Client, which is used inside vehicles.
- Vehicle V2V Safety System: This block exchange current vehicle location and motion information with other vehicles in the vicinity. The information is used to calculate vehicle paths, and warns the driver when the potential for an impending collision is detected.
- Vehicle Roadside Information Reception: This block is used by I2V applications with RSU. Information presented may include fixed sign information, traffic control device status (e.g., signal phase and timing data), advisory and detour information, warnings of adverse road and weather conditions, travel times, and other driver information.
- Vehicle Traveller Information Reception: This block is used by I2V applications with SP BO. It receives general traveller information including traffic and road conditions, incident information, maintenance and construction information, event information, transit information, parking information, weather information, and broadcast alerts.
- Vehicle Application Specific Support: Representation of the functionality required in the vehicle to execute a specific application e.g. cooperative adaptive cruise control, rerouting etc. In addition, this contains the vehicle-site part of distributed applications, e.g. rest-time-management.

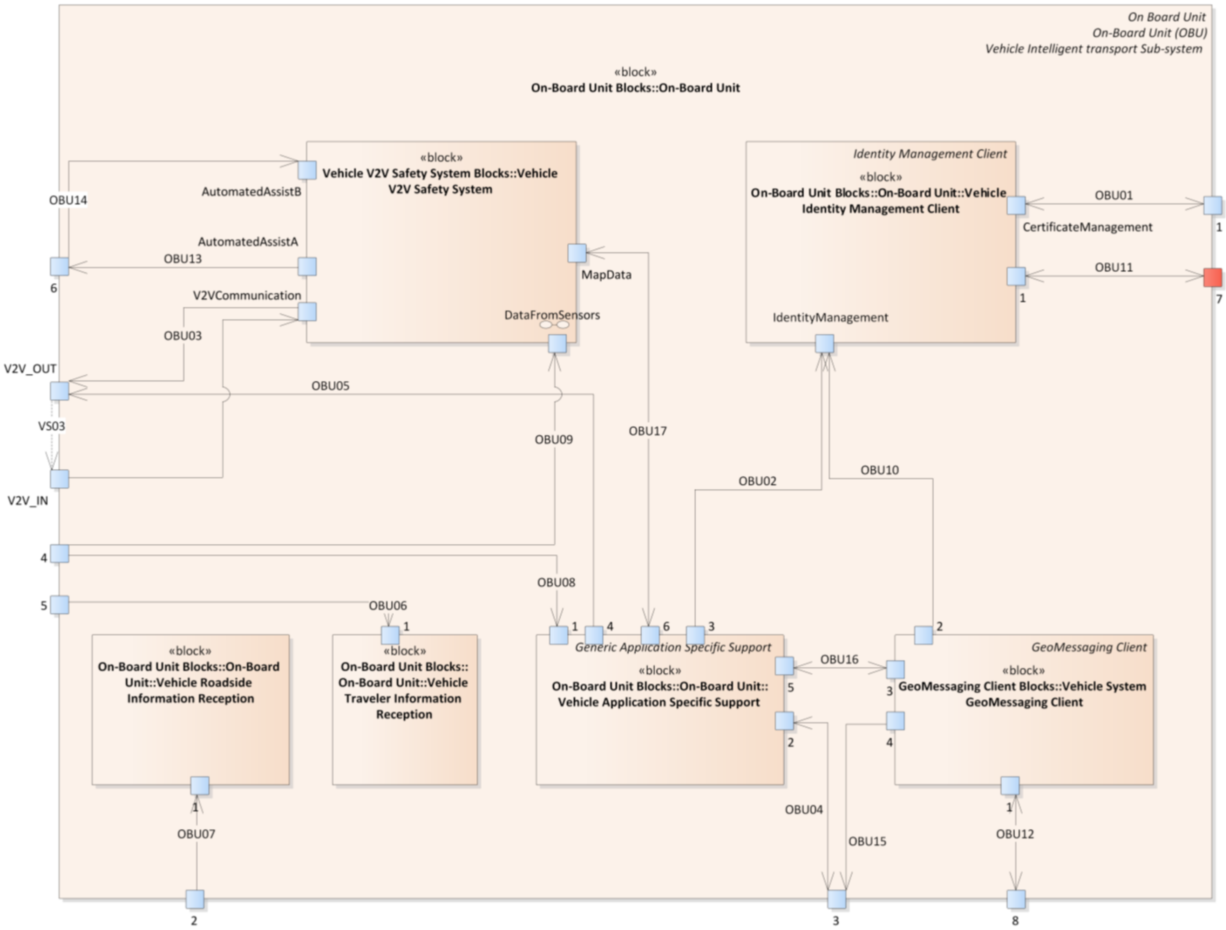


Figure 104: IBD functional diagram of the On-Board Unit

Internal Block	Description
Vehicle System GeoMessaging Client	This module mainly communicates with the GeoMessaging Server located in the CP BO in order to exchange GeoMessages whenever needed.
Vehicle Identity Management Client	This module is a specialization of the Identity Management Client which for vehicles. It manages the identity and privacy of the OBU in terms of pseudonymous requests, certification and registration.
Vehicle V2V Safety System	This module exchange current vehicle location and motion information with other vehicles in the vicinity. The information is used to calculate vehicle paths, and warns the driver when the potential for an impending collision is detected.
Vehicle Roadside Information Reception	This module receives data from the RSU. Information presented may include fixed sign information, traffic control device status (e.g., signal phase and timing data), advisory and detour information, warnings of adverse road and weather conditions, travel times, and other driver information.
Vehicle Traveller Information Reception	This module receives traveller-related messages from the Service Provider through the CP BO.
Vehicle Application Specific Support	This is the module that manages all the application-related information. It is the central sub-block of the OBU in terms of management and processing of information, which send orders to the other sub-blocks in order to provide all the functionalities of the OBU.

4.2.4.2.1.1. Internal communication description

Link Name	Direction	Description

OBU01	B	This link is used to communicate with the Identity Manager sub-block located at the Service Provider Exchange System for identity management purposes, e.g. registering to the system and getting pseudonymous credentials.
OBU02	D	This link is used by the Vehicle Application Specific Support to order a credentials request to the Identity Management Client.
OBU04	B	Bi-directional link to exchange information between the OBU and a Service Provider BO, e.g. Probe Vehicle Data.
OBU05	D	Allows the Application Specific Support sub-block to send messages to other IEEE 802.11p-capable devices related to a certain application.
OBU06	D	Through this link, the CP BO can reach the OBU to transfer traveller-related messages.
OBU07	D	It is used to receive broadcast event messages from RSUs.
OBU08	D	Allows gathering the sensors information from the VEE and reach the Application Specific Support sub-block, where they are processed by the applications that require to.
OBU09	D	Allows gathering the sensors information from the VEE and reach the V2V Safety System sub-block, where they are processed to detect specific situations.
OBU10	D	This link is used by the GEOM-C to requests pseudonymous certificates to use GeoMessaging Services.
OBU11	B	This link is mainly use d to forward and perform the real requests of the pseudonymous certificate to the Security & Credentials Management block of the Support system.
V2V_OUT	D	Used to broadcast messages using IEEE 802.11p protocol. Expected receivers are RSUs, other OBUs and VRU OBUs.
V2V_IN	D	V2V Safety System and Application Specific Support sub-blocks use this link to receive the messages sent by other OBUs and VRU OBUs. The messages from the RSUs go through the OBU07 link.
OBU12	B	Communicates the GOEM-C to the GEOM-S to be able to send and receive GeoMessages.
OBU13	D	It allows performing requests/orders to the ADAS system of the VEE
OBU14	D	It is used by the V2V Safety System as a control link to know the status of the ADAS system.
OBU17	B	MapData: Communication channel that requests map data if present from the Vehicle Application Specific Support. It is assumed that the OEM has installed a Map service in the OBU of the vehicle.

4.2.4.2.1.2. Internal Block structure

4.2.4.2.1.2.1 Vehicle V2V Safety System

Vehicle V2V Safety is the functionality to exchange current vehicle location and motion/dynamic information with other vehicles in the vicinity and the infrastructure. The information is used to calculate vehicle paths and warns the driver when the potential for an impending collision is detected.

If available, map data is used to filter and interpret the relative location and motion of vehicles in the vicinity. Information from on-board sensors (e.g., radars and image processing) is also used, if available, in combination with the V2V communications to detect non-equipped vehicles and fuse with connected vehicle data. This object represents a broad range of implementations ranging from basic Vehicle Awareness Devices that only broadcast vehicle location and motion and provide no driver warnings to advanced integrated safety systems that may, in addition to warning the driver, provide collision warning information to support automated control functions that can support control intervention.

This function also includes vehicle control events that indicate a potential incident or other hazardous location warning extracted from on-board sensors (e.g. emergency brake light, slippery road, slow vehicle etc.)

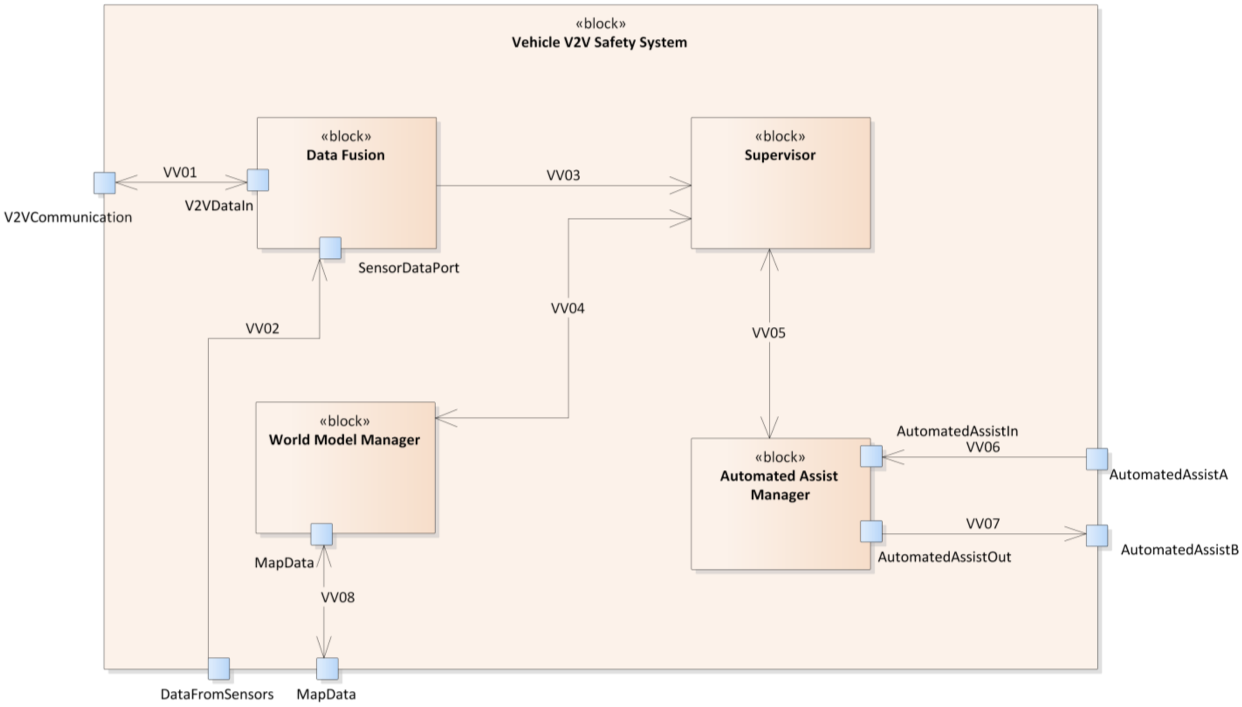


Figure 105: IBD functional diagram of the Vehicle V2V Safety System

4.2.4.2.1.2.1.1 Internal Blocks structure

Internal Block	Description
Supervisor	The Supervisor makes the decisions and generates the instructions for the driver or an automated assist device to follow to avoid collision. The supervisor processes the aggregated data together with a world model/map data (if present) and provides appropriate instructions to the vehicle driver or the automated assistance systems. The instructions can include change in speed, lane, direction, etc. according to the data received from other vehicles and the current state of the vehicle.
Data Fusion	The Data Fusion block aggregates, merges, and processes data received from another vehicle via the V2V Communication Interface and the Data from the sensors present in the vehicle, which is sent to the V2V Safety System Supervisor for further processing.
World Model Manager	This World Model Manager checks, receives and can store a map data from a Map model that may be added by the OEM in the OBU of the vehicle.
Automated Assist Manager	The Automated Assist Manager translates the instructions provided by the supervisor to appropriate commands for the automated assist system to adhere to (if automated assist is present).

4.2.4.2.1.2.1.2 Internal communication description

Link Name	Direction	Descriptions
VV01	B	This link acts as the interface where V2V Communication can be received by the vehicle or sent by the Vehicle to other vehicles.
VV02	D	This link provides an interface for the receipt of data from sensors that can be the be speed of the vehicle, the direction the vehicle is traveling, the location of the vehicle (from camera or LIDAR), etc.
VV03	D	This link is used by the Data Fusion to transfer the value that is combined from the data received from V2V Communication and the sensors.
VV04	B	This link is used as a check and to receive the world model from the map data provided in the OBU.
VV05	B	This link is used by the Supervisor to send the instructions to the Automated Assist Manager to be translated into appropriate commands.
VV06	D	This link acts as an interface that receives confirmation of automated assist presence and the automated assist system type.
VV07	D	This Link acts as an interface that sends check for presence of automated assist and the appropriate commands required by the automated assist system, if automated assist present.

VV08	B	This Link acts as an interface that receives map data from the OBU's Vehicle Application Specific Support system, if map data is present or has a new map data.

4.2.4.2.2. Vehicle Electrical & Electronic System

The Vehicle Electrical and Electronic system (E/E) includes all in-car sensors (speed, lights, etc.) and actuators (brake, etc.). The Vehicle Electrical and Electronic system provides sensor information (e.g. speed) from a vehicle to an external C-ITS system and optionally enables the control/actuation (e.g. speed control) of the vehicle based on information received from external systems. The Vehicle E/E must include safety measures to ensure the safe operation of the vehicle, independent of the interaction between the Vehicle E/E and external sub-systems. A further differentiation can be made per vehicle type, e.g. emergency vehicle, commercial vehicle or (public) transport/transit vehicle.

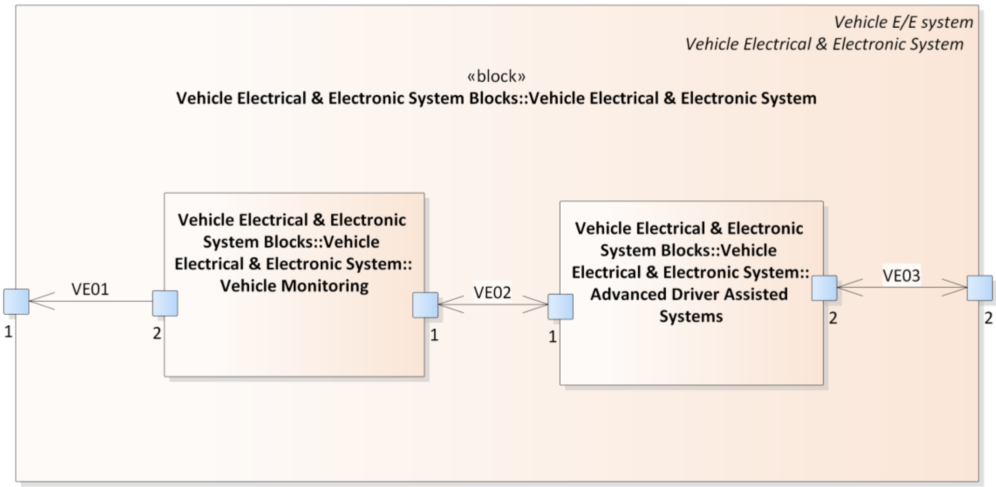


Figure 106: IBD functional diagram of the Vehicle Electrical & Electronic System

Internal Block	Description
Vehicle Monitoring	Provides access to vehicle-specific sensor and actuator information systems of the vehicle.
Advanced Driver Assisted System	Vendor-specific assistance systems to increase safety and comfort of the driver. Examples are lane departure warning, automatic emergency brake, and adaptive cruise control.

4.2.4.2.2.1. Internal communication description

Link Name	Direction	Description
VE01	D	Link to provide access of the vehicle sensors to the OBU.
VE02	B	Bi-directional link to exchange information between the ADAS systems and the Vehicle Monitoring sub-blocks.
VE03	B	Interface that allows interacting with the ADAS systems from the OBU, e.g. to order certain actions or know the status of the systems.

4.2.5. Traveller/VRU System

The VRU/Traveller System relates to the systems at vulnerable road users level. It consists of the following main sub-systems

- Personal Information Device (PID): A personal information device is typically a smart phone or personal navigation device used by an end-user. The PID provides the capability for travellers to receive formatted traveller information wherever they are. Capabilities include traveller information, trip planning, and route guidance. It provides travellers with the capability to receive route planning from the infrastructure at home, at work, or on-route using personal devices that may be linked with connected vehicle on-board equipment. A PID might include the communication functionality of a Personal ITS station, as specified in ETSI ITS specifications.

/ Vulnerable Road Users On-Board Unit (VRU-OBU): An on-board unit is a sub-system attached to a VRU vehicle (e.g. moped, electric bike) and needed for VRU assisted applications to inform / advise a driver via a HMI.

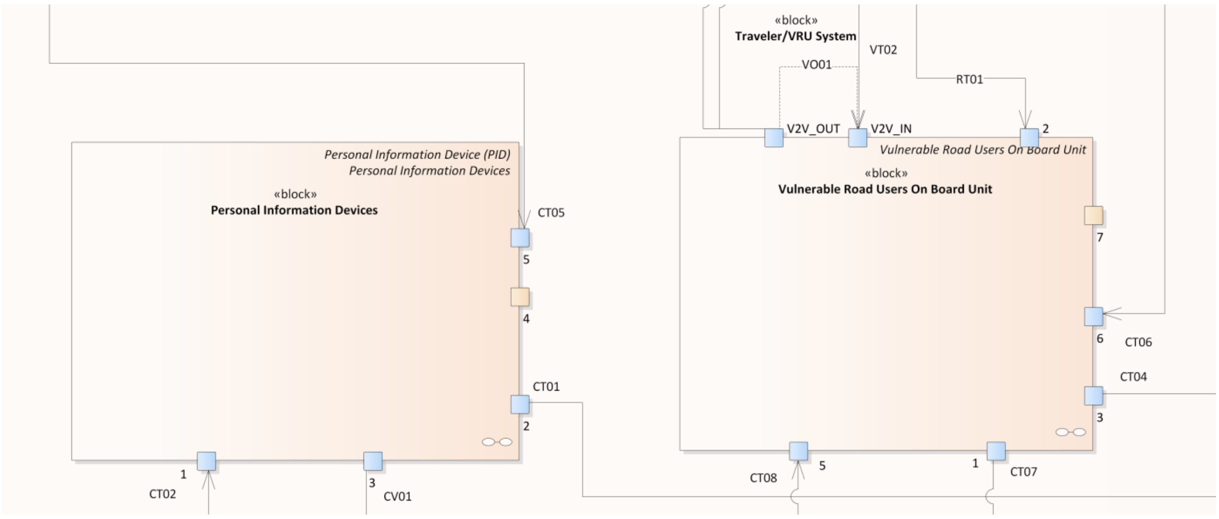


Figure 107: Functional view of the Traveller/VRU System

Internal Block	Description
Personal Information Device (PID)	As stated above, a personal information device is typically a smart phone or personal navigation device used by an end-user. The PID provides the capability for travellers to receive formatted traveller information wherever they are. Capabilities include traveller information, trip planning, and route guidance. It provides travellers with the capability to receive route planning from the infrastructure at home, at work, or on-route using personal devices that may be linked with connected vehicle on-board equipment. A PID might include the communication functionality of a Personal ITS station, as specified in ETSI ITS specifications.
Vulnerable Road Users On-Board Unit (VRU OBU)	A VRU On-Board Unit is a system attached to a VRU vehicle (e.g. moped, electric bike) and needed for VRU assisted applications to inform/advise a user via a HMI. It is equivalent to the Vehicle OBU for vulnerable road users.

4.2.5.1. Internal communication description

Link Name	Direction	Description
CT01	D	Link used by the PID to contact the SP BO in order to perform an initial registration to the GEOM system as well as interact with the SP BO
CT02	B	Link used to send and receive C-ITS messages between the BO and the PID
CT03	D	The PID requests the signature of the certificate to the Identity Manager using this link
CT04	D	Communicates the VRU OBU with the Service Provider BO in order to perform an initial registration of the device to the GEOM system.
CT05	B	It represents the GeoMessaging communication among the PIDs and the GEOM-Ss
CT06	D	It represents the GeoMessaging communication among the VRU OBUs and the GEOM-Ss
CT07	D	The VRU OBU requests the signature of the certificate to the Identity Manager using this link
CT08	B	Link used to send and receive C-ITS messages between the BO and the VRU OBU.
RT01	D	Link used for representing the reception of the messages sent by the RSUs by the VRU OBU.
RT02	D	Output link representing the transmission of 802.11p messages from the VRU OBU to the RSUs.
VT01	D	Input link representing the transmission of messages over IEEE 802.11p from the VRU OBU to the vehicles/OBUs.
VT02	D	Output link representing the transmission of messages over IEEE 802.11p from the vehicles/OBUs to the VRU OBU.

VO01	D	It represents the communication with other VRU OBU messages using IEEE 802.11p protocol.

4.2.5.2. Internal blocks structure

4.2.5.2.1. Personal Information Device (PID)

As mentioned above, a personal information device is usually a smart phone or PND (Personal Navigation Device) used by an end-user. The Personal Information Device provides the capability for travellers to receive formatted traveller information wherever they are. Capabilities include traveller information, trip planning, and route guidance. It provides travellers with the capability to receive route planning from the infrastructure at home, at work, or on-route using personal devices that may be linked with connected vehicle on-board equipment. A PID might include the communication functionality of a Personal ITS station, as specified in ETSI ITS specifications.

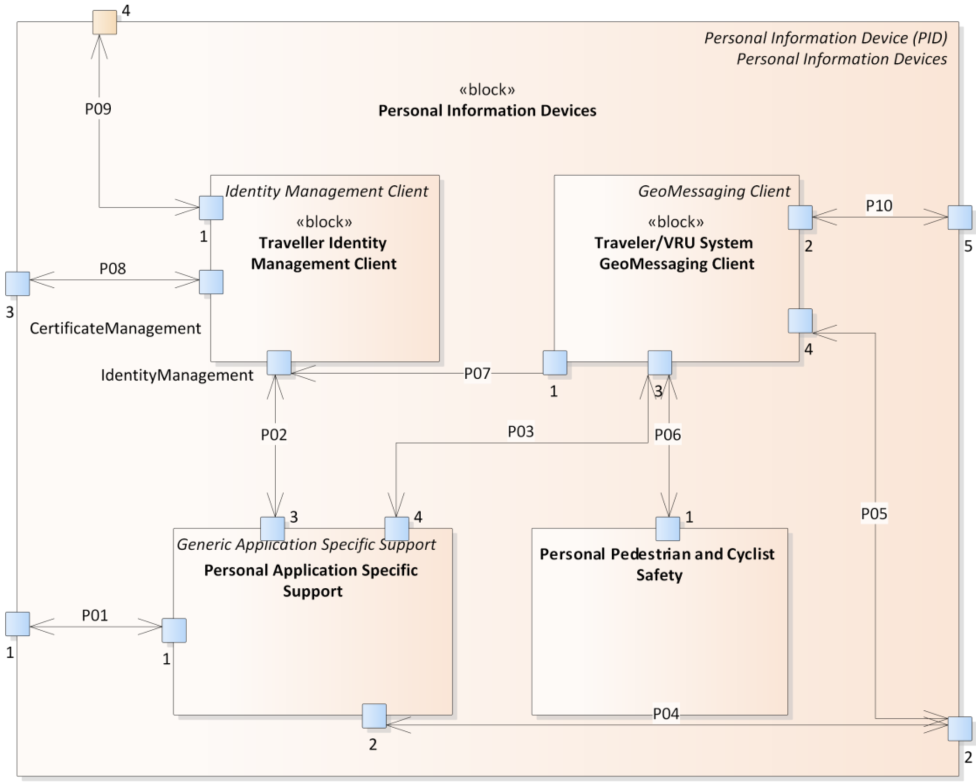


Figure 108: IBD functional diagram of the Personal Information Device

The Personal Information Device consists of the following main sub-systems:

- Traveller Identity Management Client: This is a specialization of the Identity Management Client which is used inside traveller/VRU devices.
- Personal Application Specific Support: This module provides traffic information, road conditions, transit information, yellow pages (traveller services) information, special event information, and other traveller information that is specifically tailored based on the traveller's request and/or previously submitted traveller profile information.
- Personal Pedestrian and Cyclist Safety: This module provides pedestrian and cyclist location information to the infrastructure that can be used to avoid collisions involving pedestrians/cyclists.
- Traveller/VRU System GeoMessaging Client: This module covers the functionality of the GeoMessaging Client which is responsible for updating his position/tile to the GeoMessaging server in order to keep track of the traveller/VRU location.

Internal Block	Description
Traveller/VRU System GeoMessaging Client	This module communicates with the GEOM-Server in order to exchange GeoMessages.
Traveller Identity Management Client	This module is a specialization of the Identity Management Client which is used inside traveller/VRUs. It communicates with the Service Provider Exchange System where the Identity Manager is located.

Personal Application Specific Support	This is the module that manages all the application-related information. It is the central sub-block of the PID in terms of management and processing of information, which send orders to the other sub-blocks in order to provide all the functionalities of the PID.
Personal Pedestrian and Cyclist Safety	Providing pedestrian and cyclist location information to the infrastructure that can be used to avoid collisions involving those kinds of VRUs.

4.2.5.2.1.1. Internal communication description

Link Name	Direction	Description
P01	B	This link is used by the Personal Application Specific Support of the PID for sending and receiving traveller/VRU information from/to the Back Office.
P02	B	This link is used internally by the Personal Information Device to communicate between the Personal Application Specific Support and the Traveller Identity Management to e.g. request pseudonyms.
P03	B	This link is used to communicate the Application Specific Support and the GEOM-Client to manage the received and ready-to-send GeoMessages.
P04	B	Link used by the PID:ASS to contact the SP BO
P05	B	Link used by the PID:GEOM-C to contact the SP BO in order to perform an initial registration to the GEOM system as well as interact with the SP BO
P06	B	This link is used to communicate the Pedestrian and Cyclist Safety module and the GEOM-Client to manage the received and ready-to-send GeoMessages.
P07	D	The GEOM-C uses this link to requests an identity to the Traveller Identity Management Client, who provides pseudonymous certificates to be able to use GeoMessaging services.
P08	B	This link is used for getting the pseudonym certificate signed by the Identity Management of the BO.
P09	B	This link is used between the Support System and the Traveller Identity Management Client to e.g. Communication with X.509 Enrolment Authority.
P10	B	This link is used to communicate the GEOM-Client and the GEOM-Server to send/receive geo-referenced messages.

4.2.5.3. Vulnerable Road Users On-Board Unit (VRU OBU)

The VRU OBU presents the same functionalities as the OBU for the vehicles. The OBU functional IDB model can be found in section 4.2.4.2.1. There may be some interfaces that are unused in the VRU case, such as those involving sensor data but it would depend on the Deployment Site.

4.2.6. Functional concepts

Within Task 3.2 some extraction work on the “concepts” has been carried out. The “concepts” are those functionalities that are not represented by a single block, but a set of blocks interacting each other for a certain purpose.

4.2.6.1. GeoMessaging

The GeoMessaging (GEOM) corresponds to a very particular way to route messages based on the location information of the possible receivers. The system exchanges geo-referenced data in order to get a general view of the users’ location, which is used to determine what entities the system needs to send the information to.

There are several solutions of GeoMessaging in the literature, but the C-MobILE approach is a well-known tile-based solution that makes the whole architecture efficient for hybrid communications. The architecture comprises two types of entities that enable the GeoMessaging, the GEOM-Server and the GEOM-Client. Both can be multiple, and can be seen as a distributed network of functional blocks providing the GEOM service whenever the GEOM-C are, keeping the architecture cross-border and seamless among the eight Deployment Sites of the C-MobILE project.

The internal blocks of the GeoMessaging-Server are shown in the figure below. Interface 1, for clients to connect and 5.

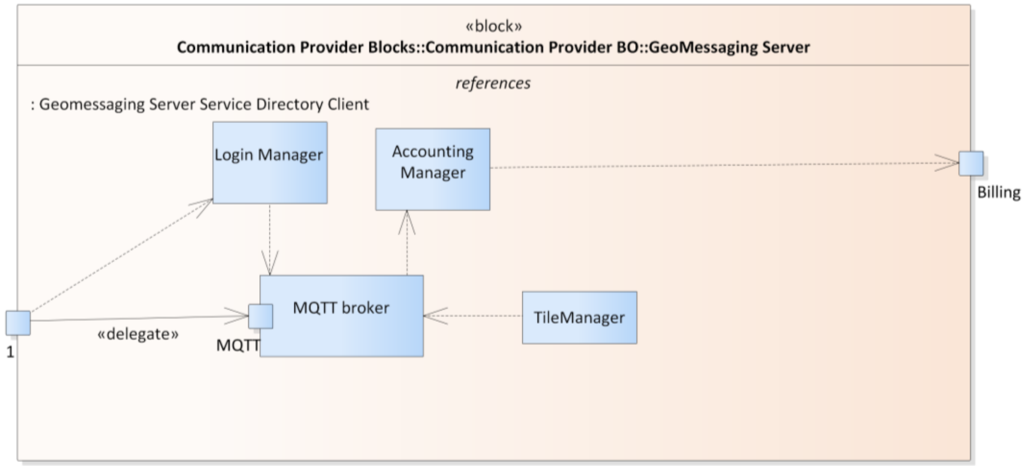


Figure 109: IBD functional diagram of the GeoMessaging Server

Internal Block	Description
Login Manager	The login manager is responsible for the verification of certificates and setting the proper access rights. Connections are set up using TLS and the service provider directing the user to the GeoMessaging server supplies together with the end-user signed pseudonymous certificates for this login.
MQTT broker	This is the core of the GeoMessaging server, it is a broker that supports location based communication through its topic structure. Information that is published has to contain location information, while clients should subscribe to topics based on their geographical area of interest. The topic structure is further explained below this table.
TileManager	The tile manager reads new messages that are published and checks their location. Based on this location, the applicable geographic tiles are calculated. References to the data are then inserted in the topic structure for those applicable tiles. This way the data only has to be uploaded onto one topic, while the tiles get small references. Lastly, the TileManager is also responsible for removing references to outdated messages.
Accounting Manager	The accounting manager has a list that links clientID's of connected end users and their corresponding service providers. These service providers will get a bill for the aggregated data usage by their clients. Since clients log in with a pseudonym and are free to log out and relog with a different pseudonym, the privacy is guaranteed at this level.

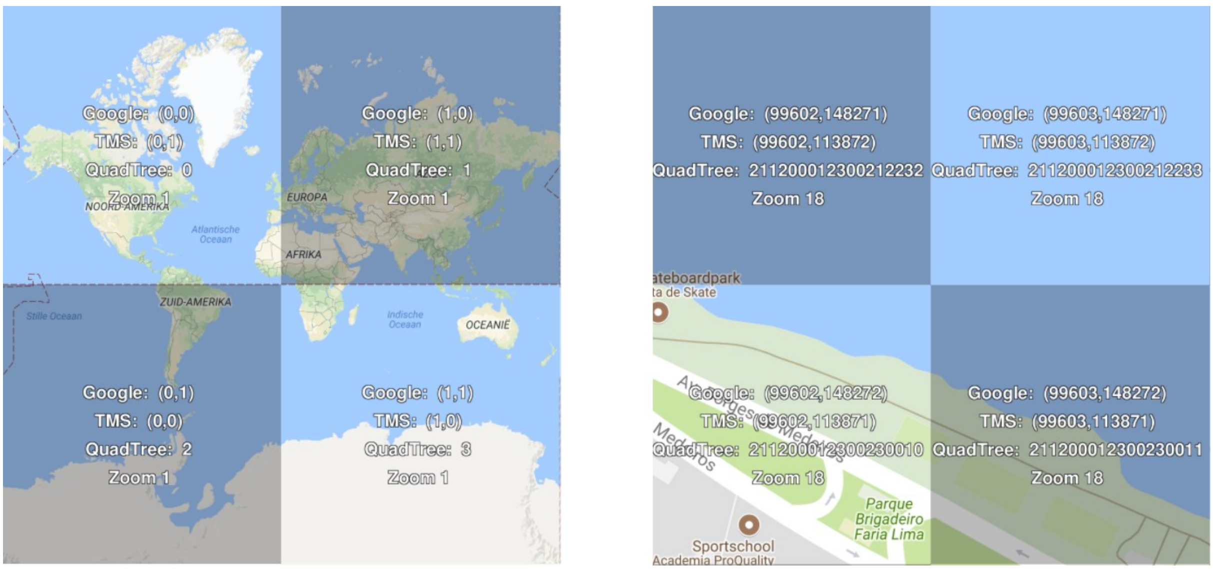


Figure 110: Tiling concept, with zoom level 1 on the left and zoom level 18 on the right

Both the MQTT broker and the TileManager depend on the topic structure inside the broker. Therefore, this structure is further described here. The first part is the tiling concept. Unlike previous solutions, the tile edges are no longer exchanged between the vehicle and the broker, but use the Google XYZ standard as described in [58]. This enables any system to calculate the relevant geographic tiles for its current location. Figure 92 shows the level 1 tiles on the left, the first level divides the world in 4 squares. For level 2 each level 1 tile is again divided into 4 squares, and so on. The right side of the figure shows level 18 tiles. Because of the Mercator projection used for the map, the size of a tile differs with the latitude. The closer to the poles, the smaller the tiles. For intersection specific ITS applications, the level 18 is a good trade-off between having enough granularity to avoid receiving irrelevant messages and not having to update the tile subscriptions too often. This results in a tile size of 65m in Oulu, which is at 65 degrees latitude. At the equator, the tile size is 154m. For road hazard warnings related to weather, a lower level tile with larger size can be used.

There are two ways of referencing the map tiles, an (x,y) coordinate or the quadtree. The latter is chosen for the C-MobILE system, because it allows structures that span multiple zoom levels. In Figure 92, both methods are printed inside the tile. As can be seen, all tiles on the right start with a "2" in the quadtree, which indicate that the tile is inside the quadtree tile "2" in the level 1 view on the left. This is correct because the right side shows a part of Rio de Janeiro in Brazil, which is in the southwest quadrant of the earth (22 degrees south and 43 west).

The schematic topic structure is presented in Figure 111. For example, if a road user wants to receive all data for the bottom-right level 18 tile of Figure 92, a subscription to the following topic should be made:

/tiles/2/1/1/2/0/0/0/1/2/3/0/0/2/3/0/0/1/1/#

By using the wildcard "#" at a lower level, a user can effectively subscribe to a level 15 tile as follows: */tiles/2/1/1/2/0/0/0/1/2/3/0/0/2/3/0/#*

The publisher, however, still has to publish on all individual tiles unless it knows all clients are listening on a specific level. When a message is relevant on an area equal to the size of a level 15 tile, this does not mean that the data will be copied to $4^3 = 64$ tiles. This is where the "sources" element of the topic structure comes in. It enables the data source to publish as a data source following the "country/region/…" part of the structure. The TileManager reads the message and places a reference on those 64 tiles and not the actual data. The reference can in theory contain any topic structure for the actual data, but it is recommended to follow the following example, where a reference to MAP/SPaT is given on a level 18 tile:

Topic: /tiles/2/1/1/2/0/0/0/1/2/3/0/0/2/3/0/0/1/1/sources/intersections/RSU701

Message body: /nl/helmond/intersections/RSU701/

This structure allows for easy identification of the data source when managing the broker. Since the actual data follows the same standardized messages as for DSRC, the actual data is published with a topic containing "asn1uper", as this is the encoding mechanism used for those messages. When the user receives the message of the data source from its tile subscription, it should then add a subscription to the following data topic:

"*nl/helmond/intersections/RSU701/#*"

Through which DSRC messages will be received on these two topics for a GLOSA service:

"*nl/helmond/intersections/RSU701/asn1uper/map*"

"*nl/helmond/intersections/RSU701/asn1uper/spat*"

The other way around, vehicles can publish for example CAM and SRM messages to the broker for services that require actions at the infrastructure side. Service specific guidelines should be made at which tile level and which messages a certain service uses.

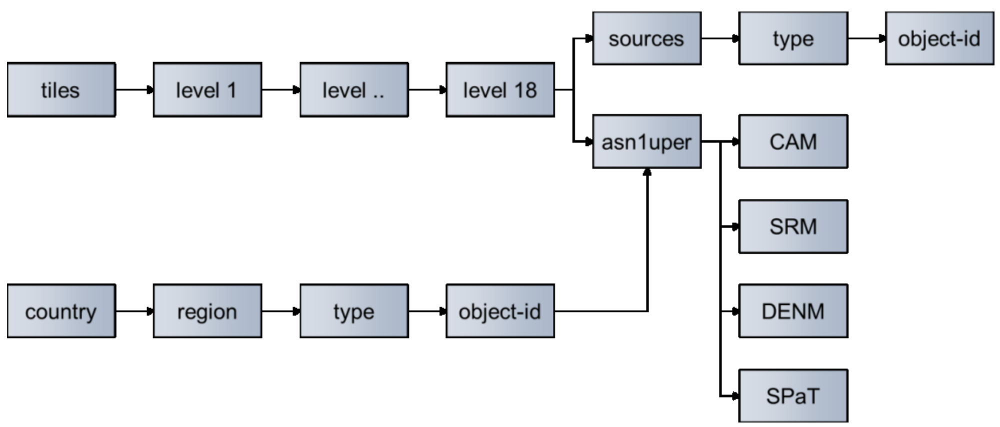


Figure 111: Schematic representation of topic structure

4.2.6.1.1. GeoMessaging sequence diagrams

The login procedure shown in Figure 112 starts between a GeoMessaging client (for example an end-user) and its service provider, which is responsible for providing both Identity Management and a Registration Server. The identity management is not necessarily from the service provider to enable models as often seen on the internet where you can for example login to a forum using LinkedIn or your Google account. Therefore, the first step is that the Identity Management and the Registration Server need to establish a long-term relationship. Once this is done the first step is that the Client requests a pseudonym at the Identity Management, this is generated using the private key of which the public counterpart is known by the registration server thanks to the long-term relationship. After that, the Registration Server receives this pseudonymous certificate, adds the access rights of the individual user and signs it with its own private key. This is returned to Identity Management and then returned to the Client. The certificate also contains information about the DNS name to reach the GeoMessaging Server.

Having the pseudonymous certificate signed by the Identity Manager ensures that the Client is a real existing user, having it signed by the Registration Server ensures that the associated Service Provider is going to pay for the data usage. Neither of those, no the combination of both gives the GeoMessaging Server information about the real identity of the Client. Both signatures are verified by the Login Manager of the GeoMessaging Server after a login request. When both signatures are correct, the access rights for the *ClientID* are set to the broker and a mapping is added between *ClientID* and Service Provider for accounting.

After these steps the data flow can start, which is further described in the sequence diagrams for the data publishing and reception. Once the connection is logged out or otherwise lost, the accounting manager will collect the statistics and adds it to the aggregated bill for the Service provider.

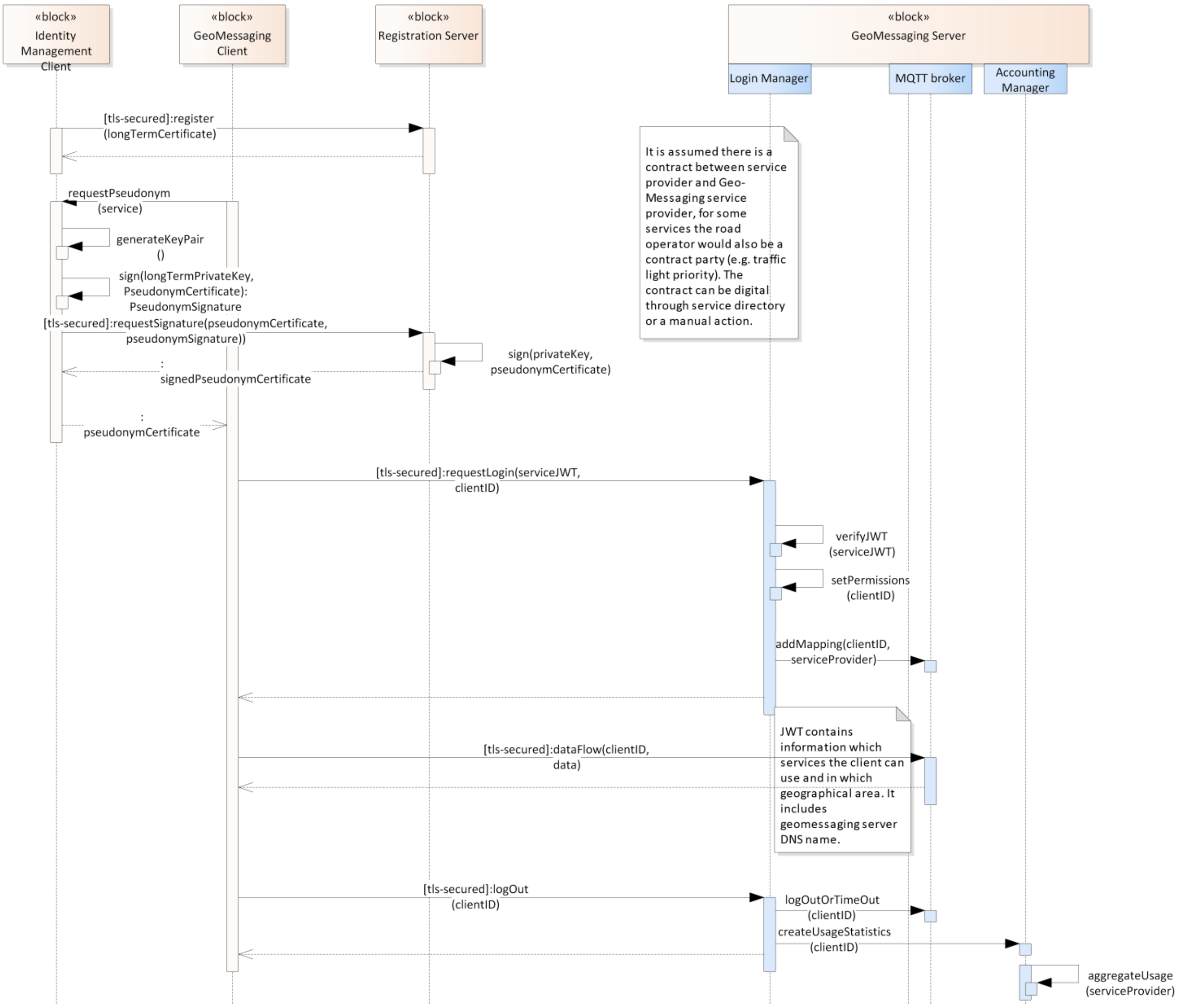


Figure 112: GeoMessaging login sequence diagram

The process of publishing data is shown in Figure 113. Both data source and data sink are GeoMessaging clients. The data source could for example be a Road Hazard Warning service, while the client could be an end-user with a smart phone app. The RHW service publishes a DENM in the broker and immediately when this is done it is forwarded to the subscribers. These subscribers were referred to this topic due to the structure described in 4.2.6.1. A special kind of GeoMessaging Client is another broker that could be the link between a central broker in the cloud and a set of local clients in a VPN. Technically this works the same as any other client, but functionally it is important to be aware of this option. Since not all messages are updates of previous messages that already have the geographical references set and all interested clients subscribed, some messages are forwarded to the Tile Manager. These messages should have a geographical reference inside that specifies to which location they apply and are typically retained as well. The tile manager interprets them and generates new references when needed.

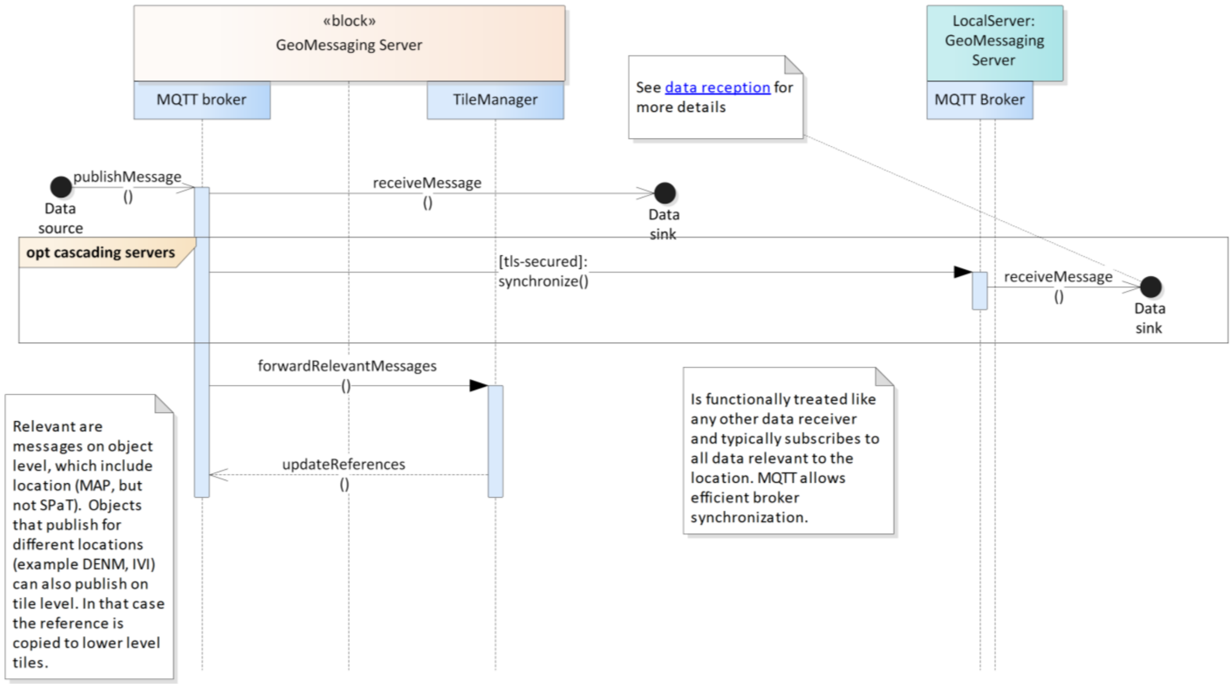


Figure 113: GeoMessaging data publishing

This diagram about data reception focusses on geographically moving end-user devices. They receive regular updates from a positioning sensor from which the tile number can be determined. Static GeoMessaging Clients can skip this step and simply use a configuration file. When this calculation results in a new tile, the subscriptions on the tile level are updated as previously described in 4.2.6.1. This returns a list of objects from the broker that is linked to that tile. If there are new objects in this list, then the object subscriptions have to be updated as well. For example if a vehicle changes tiles and is therefore not anymore in range of intersection A, but is now in range of intersection B, the object references in the new tile will only contain intersection B. The next step for the client is to unsubscribe from intersection A and subscribe to messages from intersection B.

Asynchronous of this tile and object reference update procedures, the data that is published on the tiles and subscribed objects, will be flowing to the client. It can therefore happen that a single message from intersection A still arrives while the vehicle just entered the new tile, but before the client unsubscribed. This is not a problem because the client will simply read and consider irrelevant. It's just preferable to keep the amount of irrelevant data to a minimum for scalability and data subscription fees of the end-user.

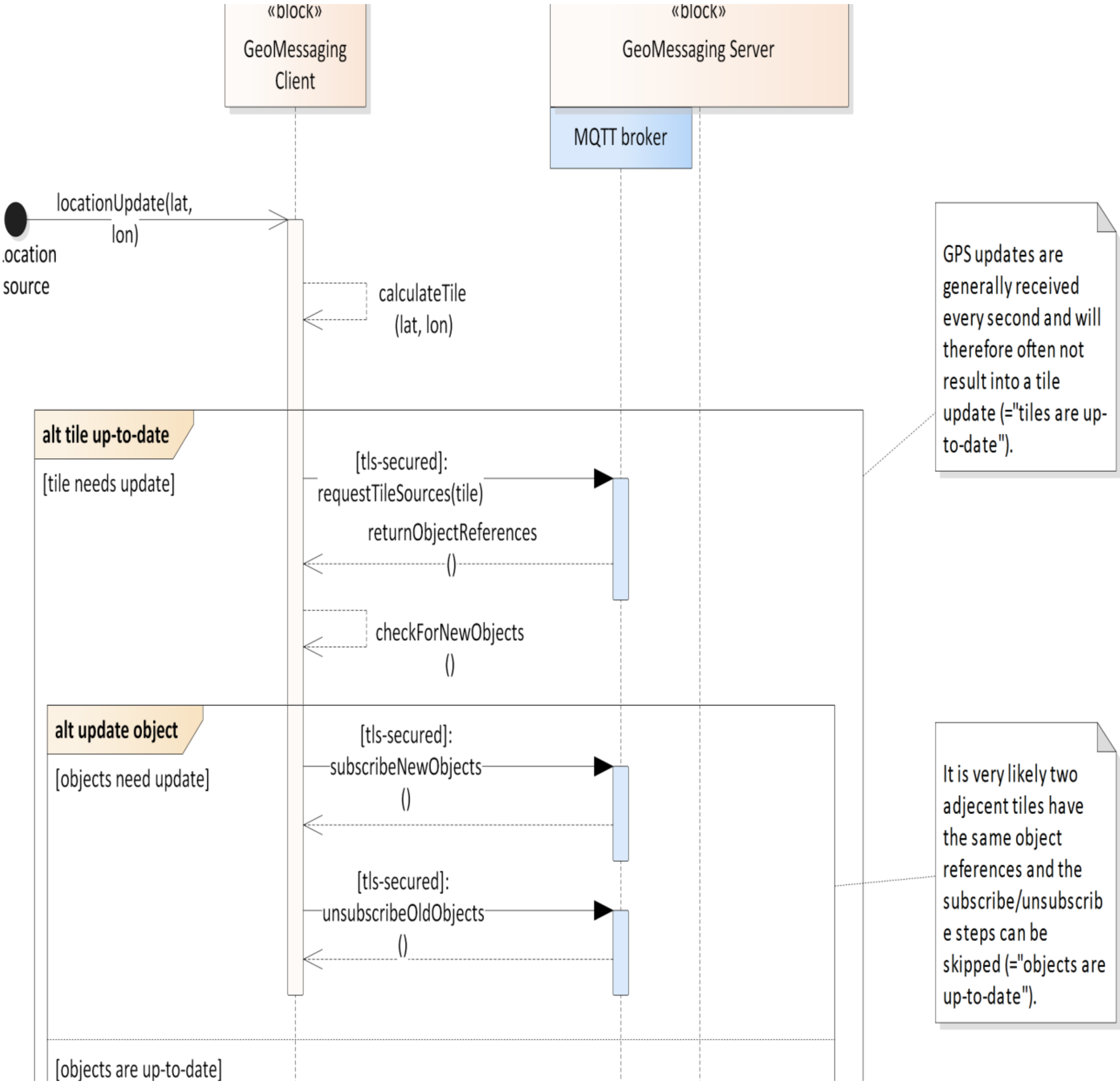


Figure 114: GeoMessaging data reception

4.2.6.2. User Management

The User Management concept defines how service users are handled in C-MobILE. It does not specify, under which conditions users might be added to the system or when they might be excluded. It specifies how users are authorized at various entities in C-MobILE.

The user management in C-MobILE uses standardized mechanisms, but combines them in such a way, that the privacy of the users is maximized. However, more advanced and complex privacy enhancing techniques, like ABC4Trust have not been deployed, as they have been considered not mature enough to provide a reliable operation.

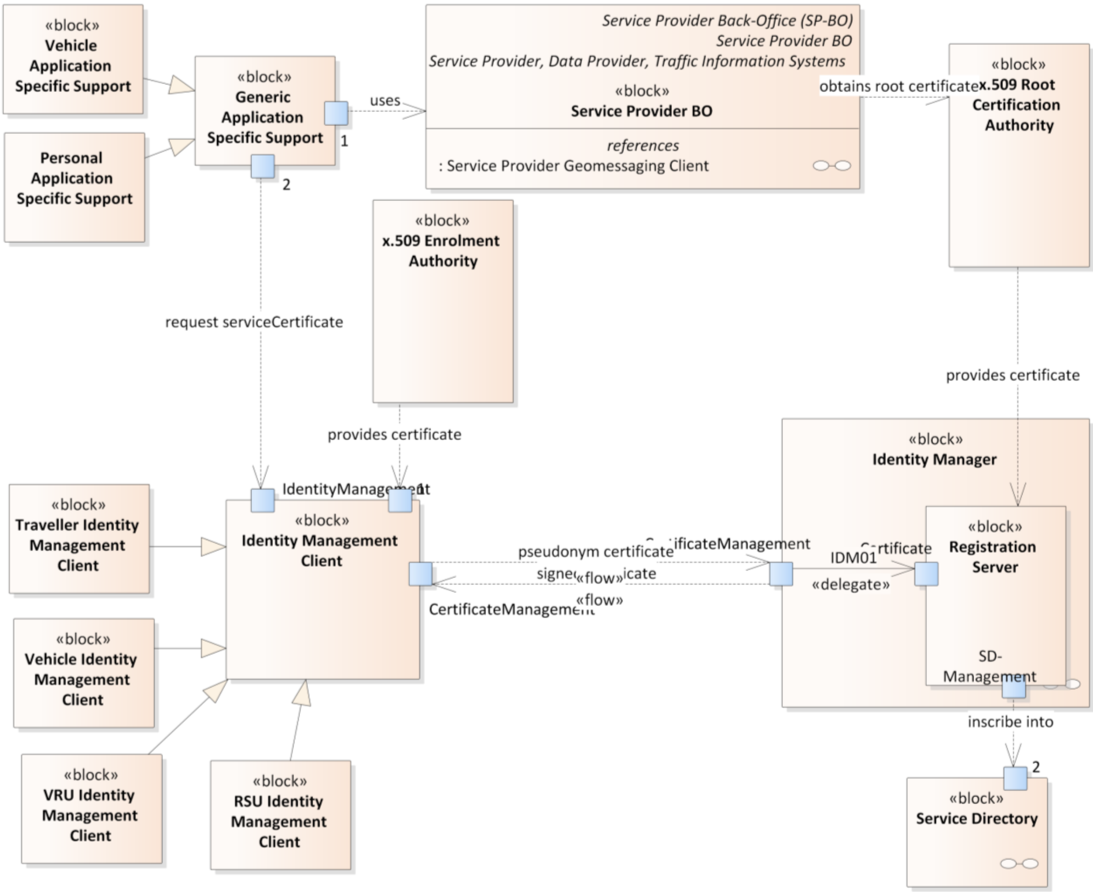


Figure 115: User Management Context

The diagram show above gives an overview of the entities involved in user management. The core elements are the Registration Server (REGS), the Identity Management Client (IMC), the Service Provider BO (SP-BO), the x.509 Enrolment Authority and the x.509 Root Certification Authority (x.509 Root-CA). The x.509 Enrolment Authority and x.509 Root-CA are used as trust anchors, and allow the identification of valid users of the system. The Registration Server is used as an intermediary between clients and Service Provider BO, thus enabling the possibility of pseudonymous service usage. The IMC is a client functionality, which handles the registration processes for various applications.

The concept allows pseudonymous service usage. This means, that the Service Provider of a Service is not able to (easily) get knowledge of the real identity of a service user, even if the Service Provider has access to multiple services, which are used by a user. Furthermore, no entity besides the client knows which services the client is using. Especially the Registration Server or x.509 Enrolment Authority does not know which services are consumed by the client.

However, this concept does not prevent tracking of the user by other means, i.e. installation of cookies, device fingerprinting, or profiling via IP-addresses. To prevent such attempts to spoof the privacy of users, additional means are necessary.

As can be seen in the above diagram, the various user entities of the architecture, like VRU devices or vehicle devices, contain specific implementations of the IMC. Those are tailored to the environment available on those devices, but their behaviour to the other entities is always the same, so we only consider a generic IMC in the following. The same is true for the Generic Application Specific Support (G-ASS). This is a generic block, which represents the client side implementation of the application, which tries to use a service.

As can be seen in the above diagram, the Registration Server has also a connection to the Service Directory. This is necessary, as each Registration Server is also inscribed in the directory, so clients can find new servers.

4.2.6.2.1. Initial user registration

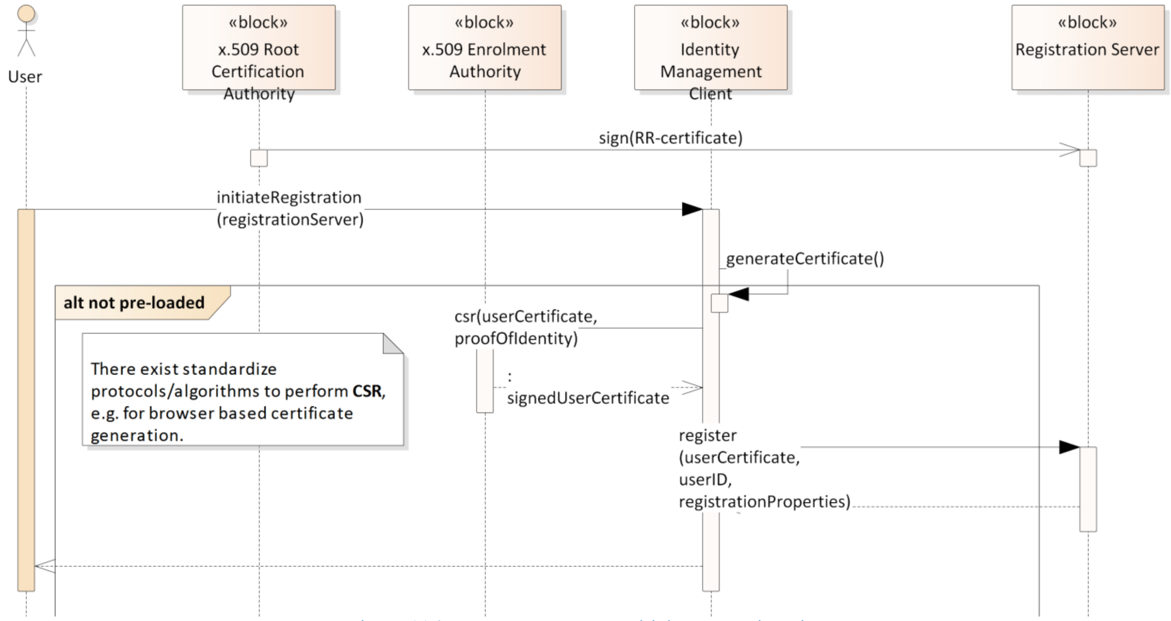


Figure 116: User Management: Initial User Registration

A user, which joins the system for the first time needs to obtain a long-term x.509 certificate, called *userCertificate*. This certificate is used, to proof that the holding entity is a valid user of the system. In addition, it is linked to the real identity of a user, so it can be used to depseudonymize a user in the case of a legal investigation.

To obtain a *userCertificate*, the user device generates a key pair, containing a private and a public key. The pubic key is send as part of a certificate-signing request (CSR) to the x.509 Enrolment Authority, together with a proof of identity ("*csr()*" call in the diagram above). How this proof of identity is implemented, is dependent on the Enrolment Authority. This authority will then sign the certificate, ensuring to other entities that the holder of this certificate is a valid user.

The private key never leaves the user device and is stored in secure storage, e.g. in a hardware security module.

This *userCertificate*, is send to the Registration Server, together with additional properties and *userID* ("*register()*" signal in the above diagram). The details of the properties and the *userID* are dependent of the Registration Server. The Registration Server stores the *userCertificate* and links it with the *userID*. Afterwards, the Registration Server can, if legally challenged to do so, indicate which *userCertificate* is associated with a given *userID*. This information can then be used to get the real identity of the user from the x.509 Enrolment Authority. However, the Registration Server has no information of the real identity of the user.

All communication is in addition secured by TLS, using the TLS certificates of either x.509 Enrolment Authority or the Registration Server.

4.2.6.2.2. Service usage

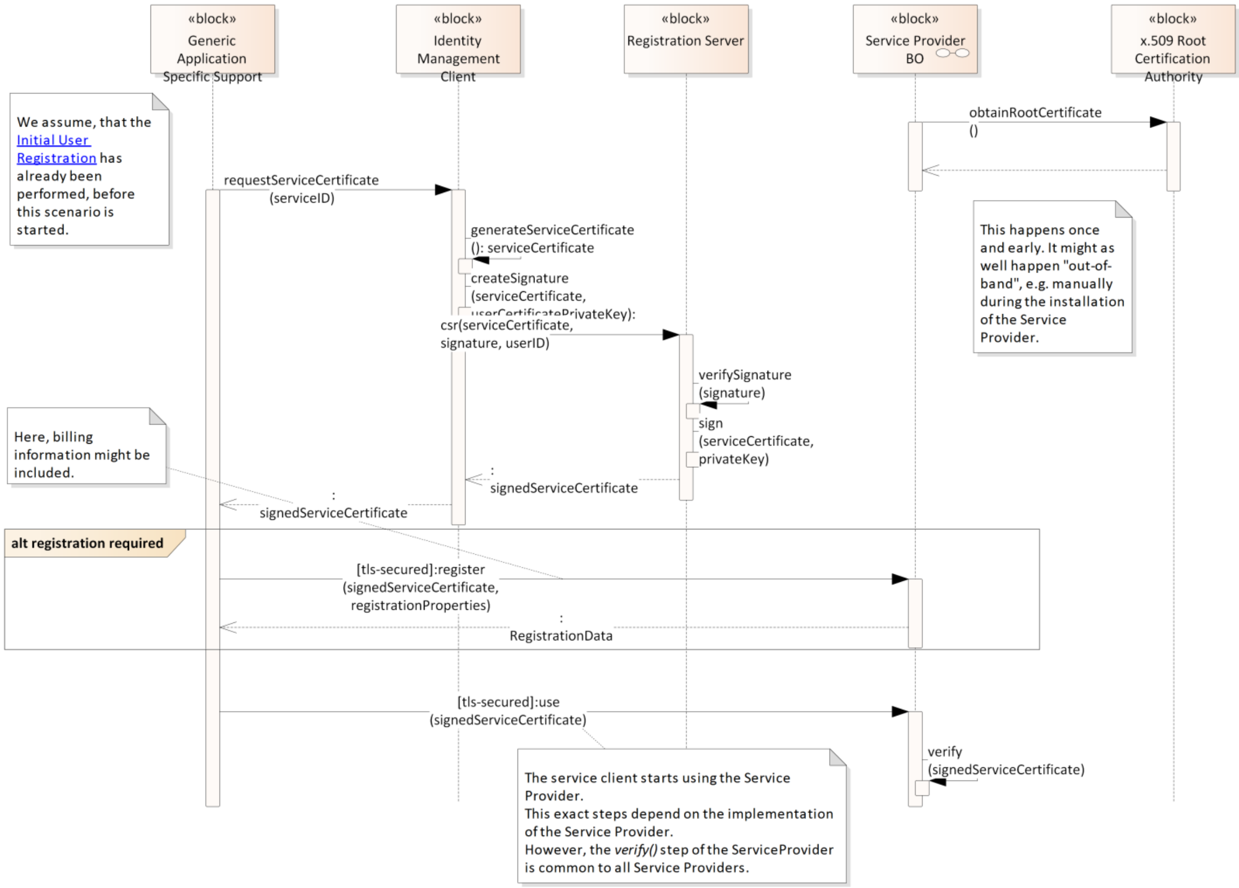


Figure 117: User Management Service Usage

If an application, in the above diagram represented by the Generic Application Specific Support (G-ASS), wants to use a service, it requested a pseudonym for the specific services. According to the C-MobILE requirements, pseudonyms for services are never shared between services and it is used exactly one pseudonym for each service. This means, that a client will use the same pseudonym for each invocation of a service.

The IMC will check if a pseudonym for this service has already been created. If this is the case, it is returned immediately. (This step is not shown in the diagram above.)

If no pseudonym is available, the process of generating on is started. For this, the IMC will generate a new key pair. In the next step, a signature based on the newly generated certificate and the *userCertificate* is generated. It is important, that this signature is not attached to the *serviceCertificate*, as this would tie the certificate to the *userCertificate* which would make it possible to link the two later on. The *serviceCertificate* is send together with the signature and the *userID* to the Registration Server. The RS can verify with the previously stored *userCertificate*, that the signature for this *serviceCertificate* has been made by the holder of the private key, associated with the *userCertificate*/*userID*. Thus, the creator of the *serviceCertificate* is a valid user. The Registration Server now signs the *serviceCertificate* and returns it. This step proofs to other entities, that the Registration Server, which has signed the certificate, knows the *userCertificate* of the original user, in case legal action against that user is necessary. However, as no information of the desired service has been added to the certificate, the RS does not know which service the user wants to use.

The IMC stores the returned *serviceCertificate* in its internal storage and links it with the *serviceID*, initially given to him by the G-ASS. Afterwards the IMC returns the *serviceCertificate* to the G-ASS. The certificate can now be used to authorize the user to the service. When doing this, the service can see, which Registration Server holds the registration of the given user and he can identify if the user uses the service in the future, but he does not know the real identity of the user.

If the G-ASS needs to proof its identity, it can request the certificate from the IMC or request, e.g. a signature of payload with the private key of the *serviceCertificate*. The private keys associated with the certificates never leave the IMC and shall be stored in secure storage.

4.2.6.2.3. Involved blocks

This is a short description of the blocks involved in this concept. Please refer to the sections of the various blocks for details.

Involved Block	Description
Identity Management Client	The Identity Management Client is a functional entity, which handles the identity management on an architectural element. It processes the real and pseudonymous identities and provides other blocks with access to the identities they need. In parallel, it blocks unauthorized access to identities.
Registration Server	The Registration Server is an entity, which contains the relation of a long-term certificate and multiple pseudonyms of a user. Its purpose is to provide a possibility to de-anonymize a user in case of lawful intervention. IT does this by linking the pseudonym to a long-term certificate, which can be linked to a real identity by the Long-Term Certificate Authority. By signing pseudonymous certificates for the user registered within the Registration Server, the server certifies that he is able to correlate the certificate with the real identity of a user. However, the Registration Server does not know where these certificates are used and other entities do not have the possibilities to cross-reference the certificates to a real identity.
x.509 Enrolment Authority	This entity provides long-term certificates. These certificates are used to uniquely identify participants. They are never used directly for communication or service usage. Instead, they are used to obtain pseudonymous tickets (e.g. for ETSI ITS G5) or pseudonymous x.509 certificates for service usage. The x.509 Enrolment Authority is analogous to the "Long-Term Certification Authority" but for x.509 certificates.
x.509 Root Certification Authority	The Root Certification Authority acts as a trust anchor for one or more Enrolment authorities as well as Registration Server. The certificate of the Root CA needs either to be installed on every participant, or there need to be an additional trust anchor, e.g. the European Trust List Manager of the C-ITS EU Trust Model.
Generic Application Specific Support	This is a generic block, which describes the client part of a service, e.g. an end user application via which the user accesses the Service Provider BO. There exist specific implementations of this block for each station/entity type. This general block is used as a simplification, where the specific type of ASS is not of relevance.
Service Provider BO	A generic back-office system of a service provider used for the specific services of the SP to connected drivers or end-users to inform end users or other SP BO systems from providers. A SP BO can be used to support personal information services for, e.g. navigation or traffic information applications on OBU/PID. A SP BO can also be used to gather floating car data from OBU/PID.
Service Directory	The Service Directory contains a listing of the services available in the network.

4.2.6.3. Service Directory

Available and certified Services have to be published to make their service offer available to possible service consumers. Such publication is accomplished using the Service Directory (SD). This allows Service Providers to provide information, so called service-entries (SE). Participants of the C-MobILE network can then look up the entries in the SD to search for services that match defined criteria. [34]

4.2.6.3.1. Interfaces

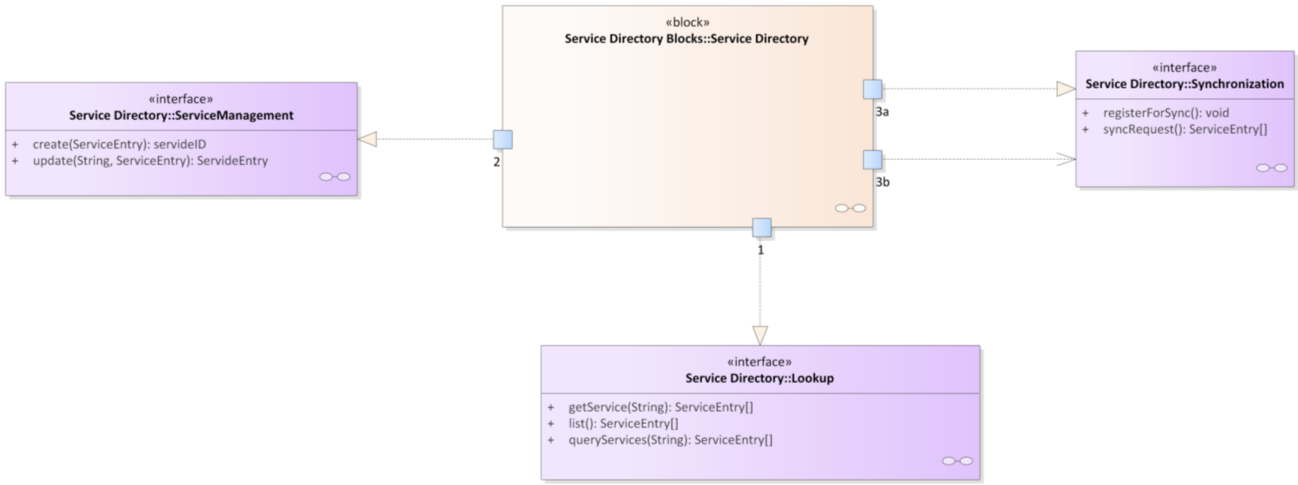


Figure 118: Service Directory Interfaces

The Service Directory provides three interfaces, which realize the functionality to create, manage, and query SEs as well as the synchronization between multiple Service Directories. The first interface, *ServiceManagement*, provides the possibility to manage SEs. The *create()* method expects a SE Object. This Object includes all needed information about the offered service. It is signed with JSON Web Token [59] to protect its integrity. The sequence how the method is working can be seen in Figure 119: Management methods. When the Service Provider needs to change details of his published service, he needs to perform an update to the stored SE. The *update()* method expects the *serviceID* as well as the updated SE Object. This method can also be seen in Figure 119: Management methods. Deleting of Services is handled via expiration periods. If a Service Provider wants to delete this service entry, he will set an appropriate expiration date. If this date is reached, the Service Directory will remove the Service Entry. To find and provide the stored entries the Lookup interface is needed. The interface provides three methods. The *getService()* method, which expects a *serviceID* as String, provides selection of a single Entry. When more than one Entry should be queried the *queryServices()* method is called. This Method gets a filter-expression, which is used to select SE's. This is needed for clients who are looking for a special kind of service. The *list()* method is used to query every SE stored in the Service Directory.

The Service Directories constitutes as single, logical entity. However, in a real world implementation, there will be multiple instance of the Service Directory, e.g. to distribute load. Different instances of the SD use the Synchronization interface to synchronize each other, so every client gets the same view to the Service Directory. The exact details will be described in D3.3.

4.2.6.3.2. Management

The SD Entry Client represents every entity which interacts with ServiceManagement interface of the Service Directory. Those entities are Data Provider, GeoMessaging Server and the Service Provider.

The Figure 119 shows the sequences of the methods provided by the interface. The first alternative shows how a SE is created. The SD Entry Client will create and sign a new SE and sends this information through a TLS-secured way to the Service Directory to publish the new service. The second alternative shows how a SE gets updated which simply differ in the first call and the last alternative shows that the deletion of a service can be done by update the entry with an expiration date.

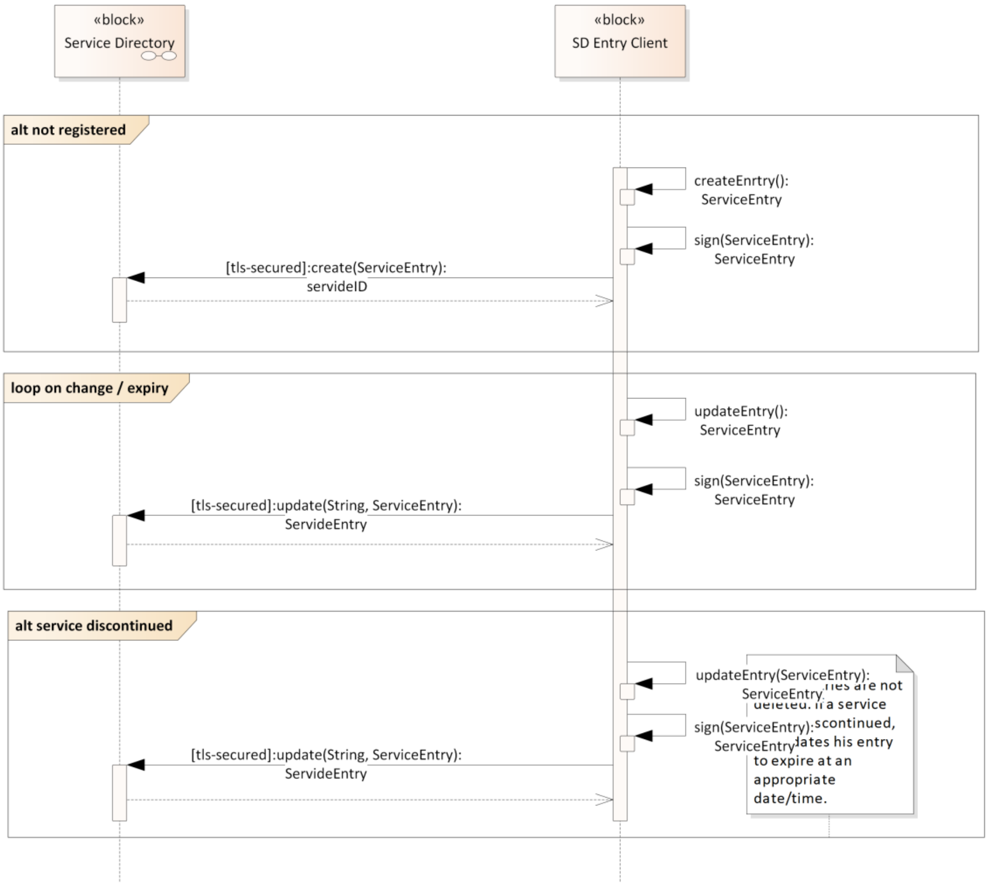


Figure 119: Management methods sequence diagram

4.2.6.3.3. Lookup

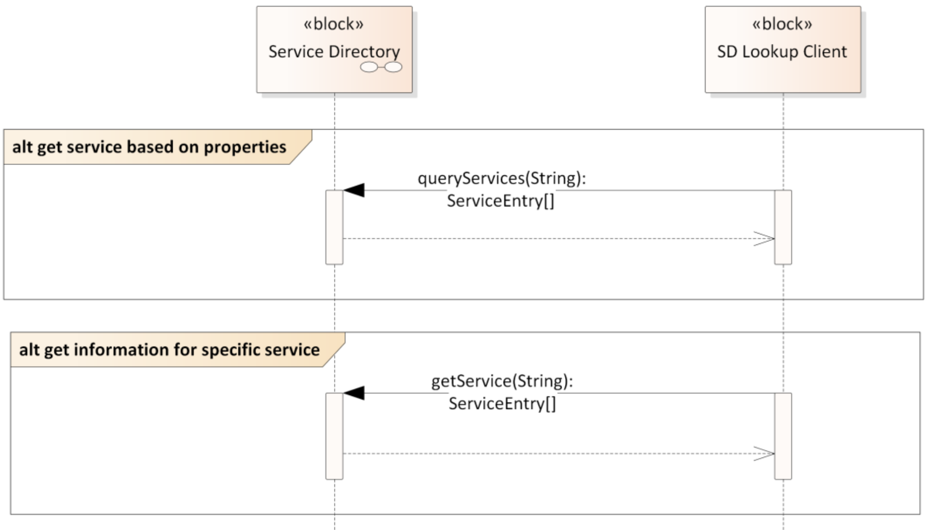


Figure 120: Lookup methods sequence diagram

The SD Lookup Client can be part of a Personal Information Device, Vehicle, TMS Traffic Monitoring as well as a GeoMessaging Client. The response to a received lookup request is a list of matching SEs. Service Lookup may address a closed set of services or may be open. An example for open lookup may be ‘give me all traffic data services’. A lookup for a closed set is ‘give me service with ID *HM_TrafficData001*’.

It doesn’t matter if many or a specific service is requested, the return value of the functions will always be a list of SEs.

4.3. Physical viewpoint

The physical view depicts the system from a system engineer's point of view. It is concerned with the topology of sub-systems at each respective domain of interest, as well as the physical connections between these sub-systems to support the C-ITS applications implemented in the different C-MobILE deployment sites. For the concrete architecture, the sub-systems defined at reference architecture are further disseminated to the respective components participating in performing specific functionalities.

The physical view consists of a physical Structure Model that is represented using SysML Block Definition Diagrams (BDD). The Physical structure is based on best common practice in previous ITS projects such as [48] i.e. the split in five main physical layers for Vehicle, Roadside, Central (or Back Office), Traveller/VRU System and Support System as already shown above. These systems and their sub-systems are categorized into the further physical entities satisfying specific functionalities. The refined physical structure is shown below in Figure 121.

The sub-systems have already been defined and described in the other architecture viewpoints above. Following, these sub-systems are further categorized into set of systems based on their specific functionalities and task. For the concrete architecture, we are concentrating on listing the generic physical entities involved in those sub-systems.

The following diagram shows the physical entities involved in Central System and Roadside System. The blocks are then described in detail in the following sections.

Figure 121: Physical view BDD diagram of the C-MobILE architecture

4.3.1. Central System

/ Traffic Management System (TMS): A TMS is responsible for various tasks and functionalities such as integrating and processing real-time data that flows from Traffic Information System, resulting in traffic measures with the goal of improving safety and traffic flow. Various sub-systems can be involved as a part of the TMS to perform these various tasks. Following sub-systems are identified for concrete architecture.

> Monitoring System: A system that monitors and controls various systems related to Traffic Management. These systems are specific according to the application specific functions.

> Reporting System: A system that passes information that has been processed by the TMS to other TMS's or RSU's for dissemination.

> Alerting and Advisory System: A system that provides alerts, advisories and other information that is relevant to transportation systems. This can include general assessments and incident awareness information.

> Traffic Regulatory Authority System: A back-office system to enforce legal actions on urban or high-way road sections or intersections based on real time traffic data from loops, cameras, speed sensors, etc.

/ Traffic Information System (TIS): A TIS is responsible to distribute real-time and/or aggregated information on traffic state (speed, flow and travel times) or road state to TMS or SP BO. In practice, several distributed TIS from different road operators can be interconnected to a central TIS. The following sub-systems of TIS have been identified:

> Broadcasting System: A system that provides an interface for the TIS to distribute data to other systems.

- Service Provider Back-Office (SP BO): A functional back office supporting personal information services e.g. navigation or traffic information applications on OBU/PID. Following sub systems are identified:
  - Media: This system provides traffic reports, travel conditions and other transportation related services to the public through radio, TV and other media.
- Data Provider Back-Office (DP BO): A functional back-office responsible to collect and fuse floating car data and real-time traffic data as well as distributing aggregated information on traffic state to SP BO.
- Communication Provider Back-Office: A functional back office responsible for accessing several communication systems from other BO systems like SP BO, TMS, TIS etc. Following sub-systems are identified:
  - Geo-Messaging Server: This is a server in the CP BO which is responsible for serving Geo-Messages based on the location information of the possible receivers.
  - Geo-Messaging Storage: This is a storage system for the Geo-Messaging feature in the CP BO where data is stored in a tile-based solution (more information in section 4.2.6.1 about the GeoMessaging concept).
- Service Provider Exchange System (SPES): A functional back office responsible for discovery and exchanging ITS end user services. It contains functions like service discovery, service authentication, and authorization, accounting and billing concepts, which have been described above. In addition to them, the following sub systems are identified:
  - Payment System: The payment systems host the payment manager which communicates with the external payment systems/financial gateway. It aids in creating a bill and other accounting.
- Central Data Storage System: A system that houses the data store or the database that can be used to store information about the service providers and the information that they provide.

4.3.2. Roadside System

Apart from Roadside Substation and Traffic Light Controller as describe above, the following sub-systems are identified for Roadside System and Roadside Unit:

- Roadside System:
  - Parking Management System: This system provides an interfaces to manage and monitor the parking spots that are connected to the C-MobILE C-ITS infrastructure.
  - Roadway Signal: These are systems that provides interface to display signs that is used to provide drivers with information on lane usage, speed advisory/limits of the lane, closure, etc.
  - Physical Overhead Lane Signs: This is a physical display sign place mostly on highways that display information about the lane it is stationed over.
  - ITS Roadway Equipment: These is the ITS equipment that is deployed along the roadway that is used to monitor and control traffic and the roadway itself.
  - Loop Detectors/Cameras: These are sensors and cameras that are deployed along the roadway to monitor traffic movement on the roadway.
  - Roadside Maintenance Equipment: This is the equipment that is used to deploy, test, monitor, debug and maintain the Roadside Units and ITS Roadway Equipment.
- Roadside Unit:
  - Location and Time Data Source: These provide accurate position information with a GPS receivers being the most common implementation for roadside units and connected vehicles.
  - Connected Vehicle Roadside Equipment: These are systems that are used to send messages to and receive messages from nearby vehicles using wireless connectivity (G5).

Following diagram shows the physical entities involved for Vehicle System, Traveller/VRU System and Support System.

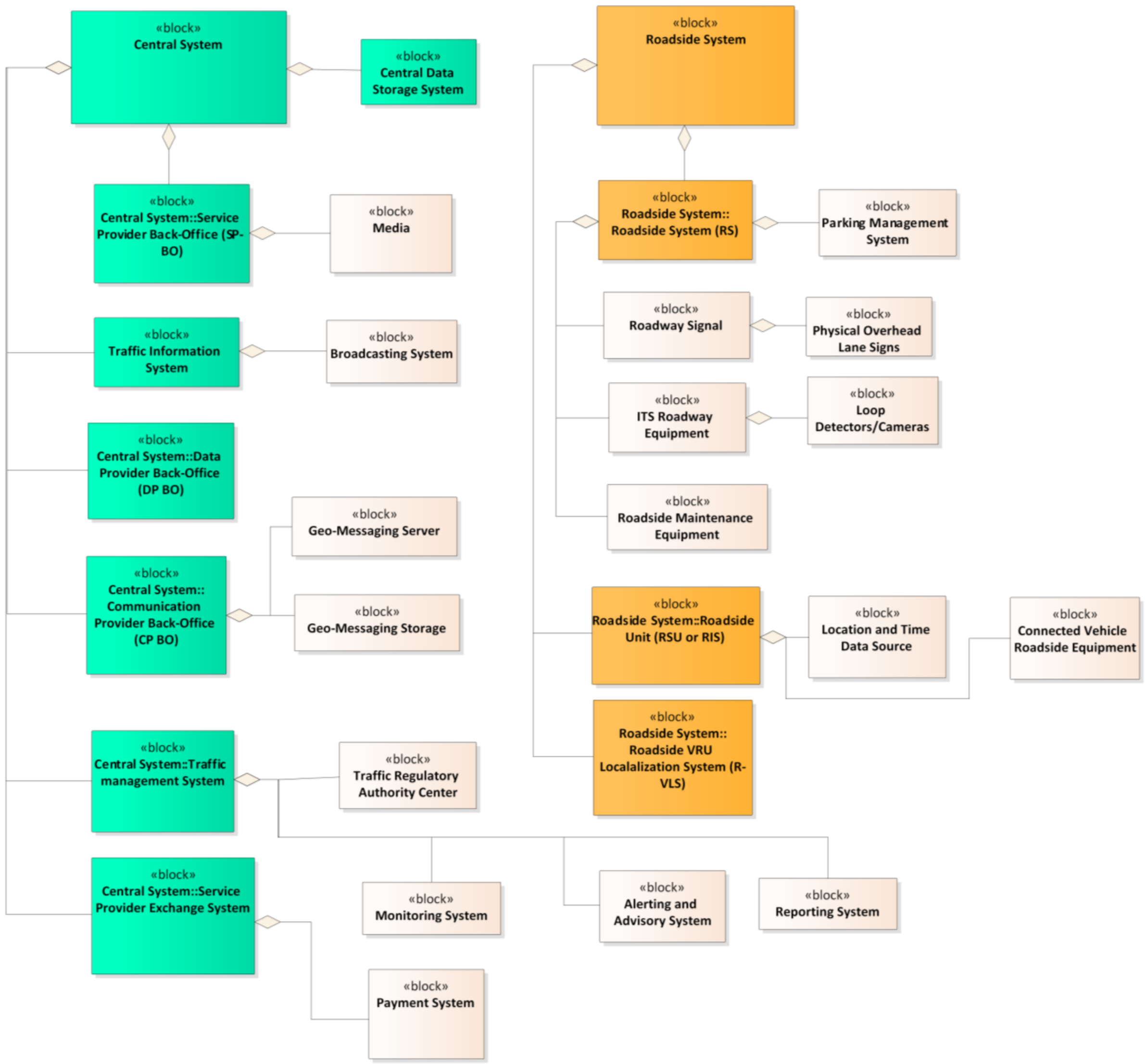


Figure 122: Physical view BDD diagram of the Central and Roadside systems

4.3.3. Vehicle System

Following sub-systems are identified as a part of Vehicle System depicted in Figure 123:

/ Vehicle Platform or Vehicle E/E system: The Vehicle Electrical and Electronic (E/E) system responsible for safety measures to ensure safe operation of the vehicle independent of the interaction between the Vehicle E/E and external sub-systems. Following systems are identified as a part of VEE:

> In-car sensors: VEE system includes all in-car sensors (speed, lights, etc.) which provide sensor information from a vehicle to an external C-ITS system.

> Actuators: VEE optionally enables the control/actuation (e.g. speed control) of vehicle by an external system to ensure safety operation.

> Advanced Driver Assisted Systems: Mainly responsible for cruise control capabilities.

/ On-Board Unit: An OBU is attached to a car and needed for driver assisted applications to inform or advise a driver via a HMI. Following systems are identified as a part of OBU:

> Vehicle OBU: These are the OBUs present in most vehicles with generic capabilities that apply to private vehicles, trucks and all other forms of vehicles.

> Map Update System: This is a system that can be used to update the map stored in the Vehicle's OBU by the Vehicle Manufacturer. This will be performed in accordance with the agreement with a map provider.

> Human Machine Interface (HMI): HMI is used to inform or advise the driver through vehicle assisted application or the vehicle OBU about various warnings or messages.

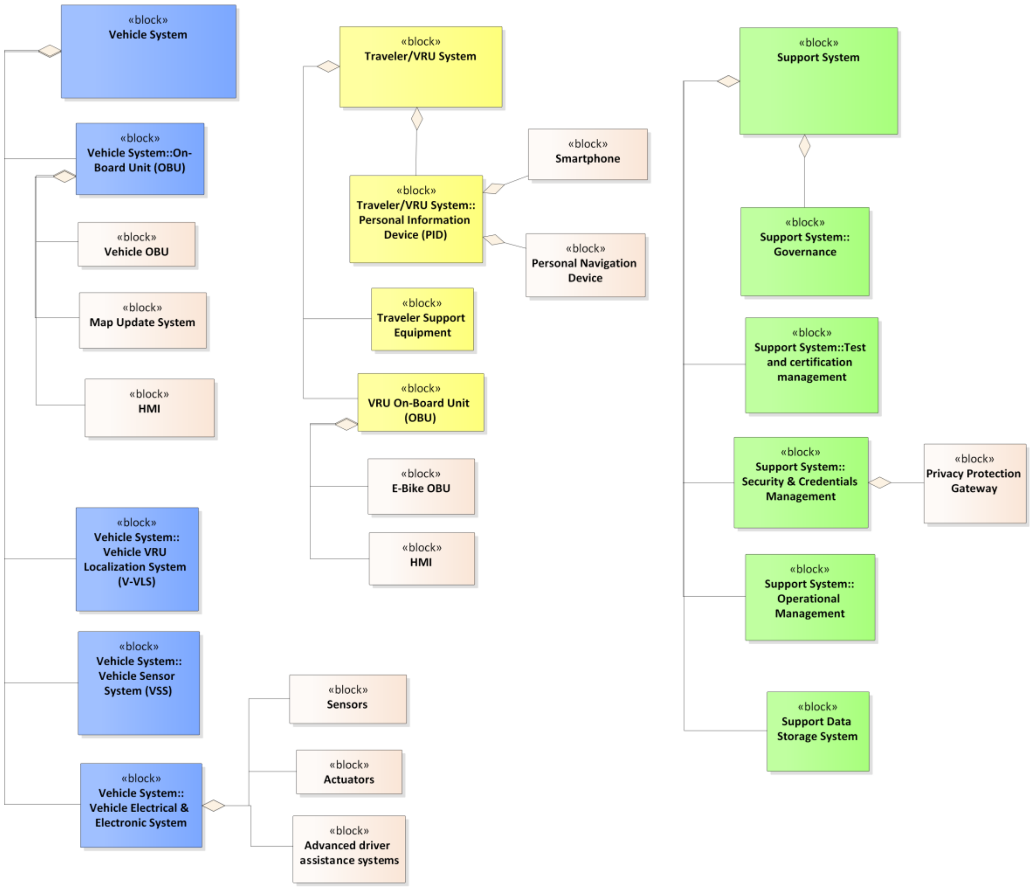


Figure 123: Physical view BDD diagram of the Vehicle, Traveller/VRU and Support systems

4.3.4. Traveller/VRU System

Following sub-systems are identified as a part of traveller/VRU System depicted in Figure 123:

/ Personal Information Device

> Smartphone: A personal information device owned by an end user

> Personal Navigation Device: Navigation device such as TomTom used by an end-user

/ Traveller Support Equipment: This equipment provides traveller information according the specifics provided by the traveller. It can provide personalized route plans and guidance. This can act as a substitute for a PID if the traveller hasn't connected their PID to the C-ITS network and can be placed in pit stops such as gas stations, restaurants, etc.

/ VRU On-Board Unit (OBU):

> E-Bike OBU: These are OBUs that are installed on E-Bikes that contain information about the battery levels and other specifics to an E-Bike together with functionalities that support efficient, safe and convenient travel.

> Human Machine Interface (HMI): HMI is used to inform or advise driver through VRU assisted applications

4.3.5. Support System

Following sub-systems are identified as a part of Support System depicted in Figure 123:

/ Governance: This sub-system is a placeholder system, as it is not a technical system. In general, it contains all the organizations, entities, and policies necessary to operate the system.

- Test and certification management: This sub-system is a placeholder system, as it is not a technical system. In accordance with the rules created by the Governance block, there might be different tests or certifications necessary for all or some of the entities of the system e.g. like the CE certification for electric equipment or regular financial audits for banks.
- Security & Credentials Management
  - Privacy Protection Gateway: These are support system that obscures the network identifiers of mobile devices. This will help secure the network and keep the information of the VRU/Travellers safe.
- Support Data Storage System: A system that houses the data store or a database that is used to store credentials, root certificates and SSL certificates in a secure manner.

4.4. Communication Viewpoint

This content can be found in section 5.2.

4.5. Information Viewpoint

This is part of the section 5 and the content can be found in Appendix A.

4.6. Implementation viewpoint

This is described through the section 5.

5. Implementation Architecture

5.1.1. Interoperability in Related Projects

Cooperative Intelligent Transportation Systems (C-ITS) are currently under intense development. Several previous projects have already been done regarding C-ITS, which have developed different interoperability solutions. In C-MobILE an infrastructure that is able to facilitate interoperability between deployment sites has been developed. In order to make this possible, state of the art solutions is re-used. In this section of the document different projects related to C-ITS interoperability in Europe are presented. Out of those the solutions suitable for C-MobILE have been extracted.

5.1.1.1. C-Roads

C-Roads [70] is a platform of European member states working on the deployment of C-ITS services. C-ITS pilot sites will be installed across the EU for testing and later operation of "Day-1" applications as recommended by EC "C-ITS platform"[77]. Member states will invest in their infrastructure, while the industry will test components and services. Technical and organisational issues will be tackled by the C-Roads platform to ensure interoperability and harmonisation of C-ITS between pilots. Individual experts from pilots work together in Working Groups (WG) to prepare proposals and recommendations regarding specification of services to achieve the goal of the implementation of interoperable end-user services.

In C-Roads, Working Group 2, Technical Aspects, Task Force 3, Infrastructure Communication, the main purpose is to ensure interoperability between RSUs and OBUs (I2V & V2I) via ITS-G5. In this task force the profiles of the day-1 infrastructure-to-vehicles services Roadworks Warning (RWW), Other Hazardous Location Notifications (OHLN), In Vehicle Signage (IVS), Traffic Light Manoeuvres & Road and Lane Topology (TSM & RLT), Coexistence (ITS-G5 – CEN-DSRC) and Shock-Wave-Damping (SWD) via ITS-G5 have been developed [71] [72].

5.1.1.2. CONVERGE

The German research project CONVERGE [68], performed from 2012 to 2015, created an ITS architecture which was heavily focused on interoperability and economic viability. This architecture, called Car2X Systems Network was intended to be scalable, decentral, secure and not dependent on a single operator, thus being resilient to change of the partaking organizations.

As a hybrid communication system, CONVERGE has developed a system which includes cellular as well as ITS-G5 communication technologies and also different mobile network operators. Figure 124 displays an example of this hybrid communication system.

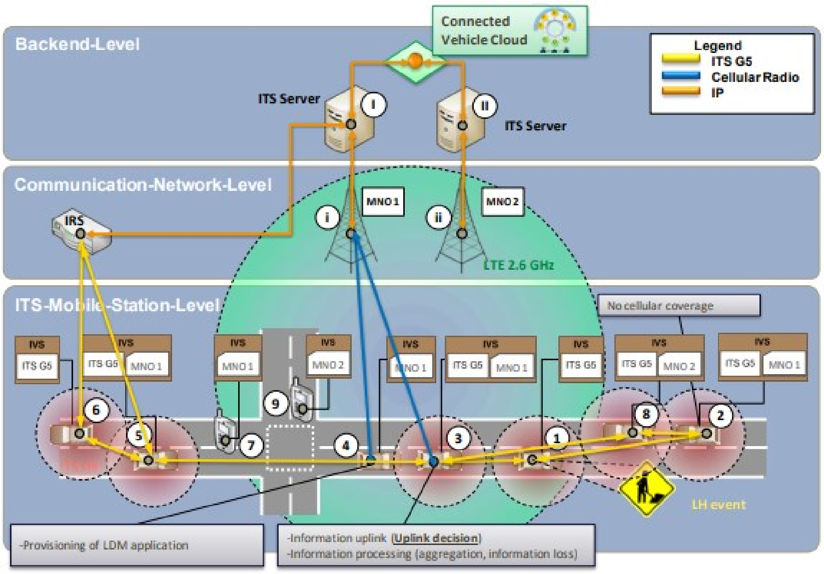


Figure 124: Example of a hybrid communication system

5.1.1.3. InterCor

InterCor (Interoperable Corridors) [24] constitutes an action, which aims to streamline C-ITS implementation in four member states linking the different national initiatives towards a harmonized strategic rollout and common specification. C-ITS pilot sites to communicate data through cellular and/or ITS G5 networks will be installed on approximately 968 km in the Netherlands, Belgium, UK, and France, for operation and evaluation of C-ITS services. InterCor will focus on the deployment of "Day-1" services as recommended by EC "C-ITS Platform" such as Road works warning, Green Light Optimized Speed Advisory, In-Vehicle-Signage and Probe vehicle data.

In InterCor three interfaces have been defined to support cross-border interoperability [24]. The first interface (IF1) is the ITS-G5 interface between road side units (RSU) and on board units (OBU). For this interface harmonized profiles have been developed for Road Works Warning (RWW) and In Vehicle Signage (IVS). Regarding GLOSA InterCor adapted the Dutch SPAT and MAP profiles [73] and regarding Probe Vehicle Data InterCor agreed to use the CAM Standard.

The second interface (IF2) is an interface between back offices in the countries to exchange relevant information for the services IVS, RWW and GLOSA via cellular network. With back offices meaning at least one central back office where all data, needed for the services that have been deployed in that country, will be collected. This could be a back office of a service provider, data provider or traffic management centre. By developing an interface between those back offices information will be available for foreign service providers.

The third interface (IF3) is the interface between back offices and devices of end-users via cellular network. This interface is needed to bring the services to the end-users and is therefore complementary to interface two.

These three interfaces have been visualized in Figure 125.

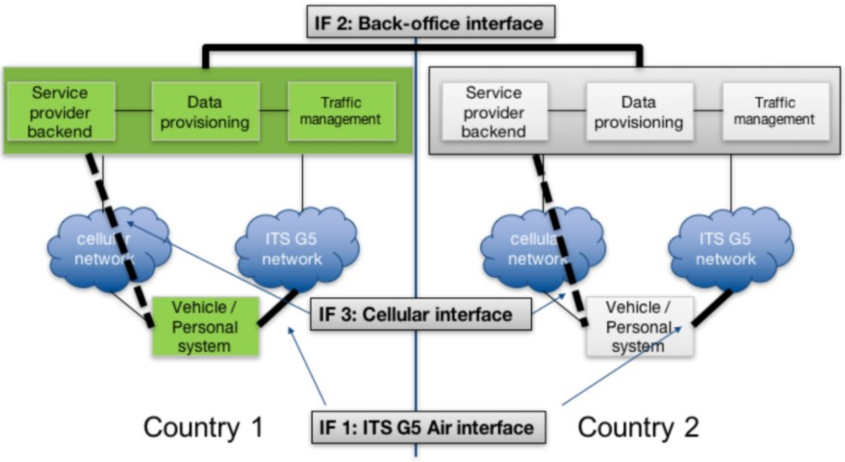


Figure 125: Interoperability diagram for cellular and ITS-G5 communication [69]

IF2

Based on the requirements defined in InterCor it should be possible to support flexible, real-time exchange of many messages from different sources to multiple destinations and it should be possible to filter messages on several criteria, such as type of message, validity in tome and geographical information. The best way to support these requirements is by using a message queue protocol and messaging system. In InterCor two message queue protocols have been considered:

- AMQP. NordicWay (described in chapter 5.1.1.4) combines AMQP with simplified and extended DATEX-II based messages.
- MQTT. Talking Traffic (described in chapter 5.1.1.5) uses MQTT with ASN.1 encoded, standardized messages, such as CAM, DENM, MAP, SPAT, IVI.

Because of the reliability and interoperability of the AMQP protocol, but mainly because of the use of AMQP in NordicWay and therefore a (possible) easier European wide implementation in InterCor it has been decided to use the AMQP protocol (specifically AMQP 0.9.1) for interface 2.

5.1.1.4. NordicWay

The proposed action, NordicWay, is a pre-deployment pilot of Cooperative Intelligent Transport Systems (C-ITS) services in four countries (Finland, Sweden, Norway and Denmark) which will be followed by wide-scale deployment and potentially to be scaled up to Europe. NordicWay has the potential to improve safety, efficiency, and comfort of mobility and connect road transport with other modes. NordicWay is the first large-scale pilot using cellular communication (3G and LTE/4G) for C-ITS. This access network will be covered in the future by LTE/4G and later by 5G, and no specific investments in the infrastructure will be needed. It offers continuous interoperable services to the users with roaming between different mobile networks and cross-border, offering C-ITS services across all participating countries. NordicWay puts emphasis on building a sustainable business model on the large investment of the public sector on the priority services of the ITS Directive. NordicWay is fully based on European standards and will act as the last mile between C-ITS research and development and wide-scale deployment [19][3].

The NordicWay architecture (see Figure 126) uses a message queuing approach to transfer messages between the different actors, such as Service Providers, OEMs (Original Equipment Manufacturers, meaning car makers), and Traffic Message Centers. A driver, resp. smartphone user, only communicates with a Service Provider/OEM cloud, which in turn communicates with other clouds, which belong to both other Service Providers/OEMs and national Traffic Clouds. Messages between these actors are relayed through the NordicWay Interchange Node, which distributes them to the actors, which have subscribed to the messages.

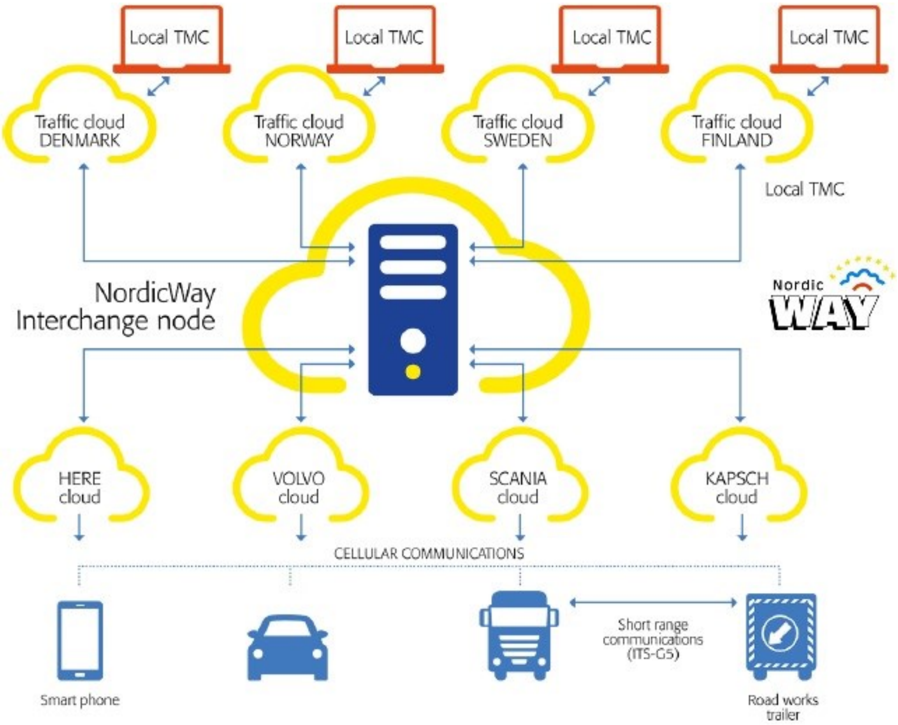


Figure 126: Nordic Way architecture

The NordicWay interchange node uses a publish-subscribe AMQP (v1.0) queuing system to distribute messages between connected actors. In this system, all actors take the role of either a producer or a consumer. A single actor can also be both a producer and a subscriber at the same time.

The data model for exchanged data is based on DATEX II version 2.3 level A with level B extensions. This means that nodes that support exchange of messages, which are conformant with this model, will be interoperable with respect to data exchange in NordicWay. The data definitions for DATEX II will be implemented as XML schemas, and the serialization format for DATEX II messages will be XML

5.1.1.5. Talking Traffic

The goal of Talking Traffic [38] is C-ITS deployment. It is a collaboration between the Dutch Ministry of Infrastructure and the Environment, regional and local authorities and (inter)national companies [51]. For interoperability the architecture used for deployment of use cases involving traffic lights is interesting. This architecture (see Figure 127) is divided in three clusters:

/ Cluster 1

> Cluster 1 is the gate to and from real time traffic light information. In this Cluster a Traffic Light Exchange (TLEX) component has been developed, which is a central component with interfaces to all intelligent traffic lights. The TLEX provides to Cluster 2 traffic light information in SPAT, MAP, CAM and the TLEX receives priority requests from Cluster 2 and provide Cluster 2 feedback whether the request is accepted or not.

/ Cluster 2

> Cluster 2 has access to the information provided by Cluster 1. They can enrich this traffic light information with other data and provide this data to Cluster 3. Cluster 2 also has a relation with other services, such as priority services for emergency vehicles. Cluster 2 receives priority requests from priority services and sends these requests to the TLEX. Cluster 2 receives feedback from the TLEX if the request is accepted or not and Cluster 2 provides Cluster 3 with the answer of the TLEX.

/ Cluster 3

> In Cluster 3 the use cases will be developed, based on the information provided by Cluster 2.

The relation between all Clusters is a business to business relation, meaning that foreign service providers (Cluster 3) are able to receive traffic light information of all intelligent traffic lights in The Netherlands and therefore they can provide traffic light use cases to their end-users not only in their home country, but also in The Netherlands.

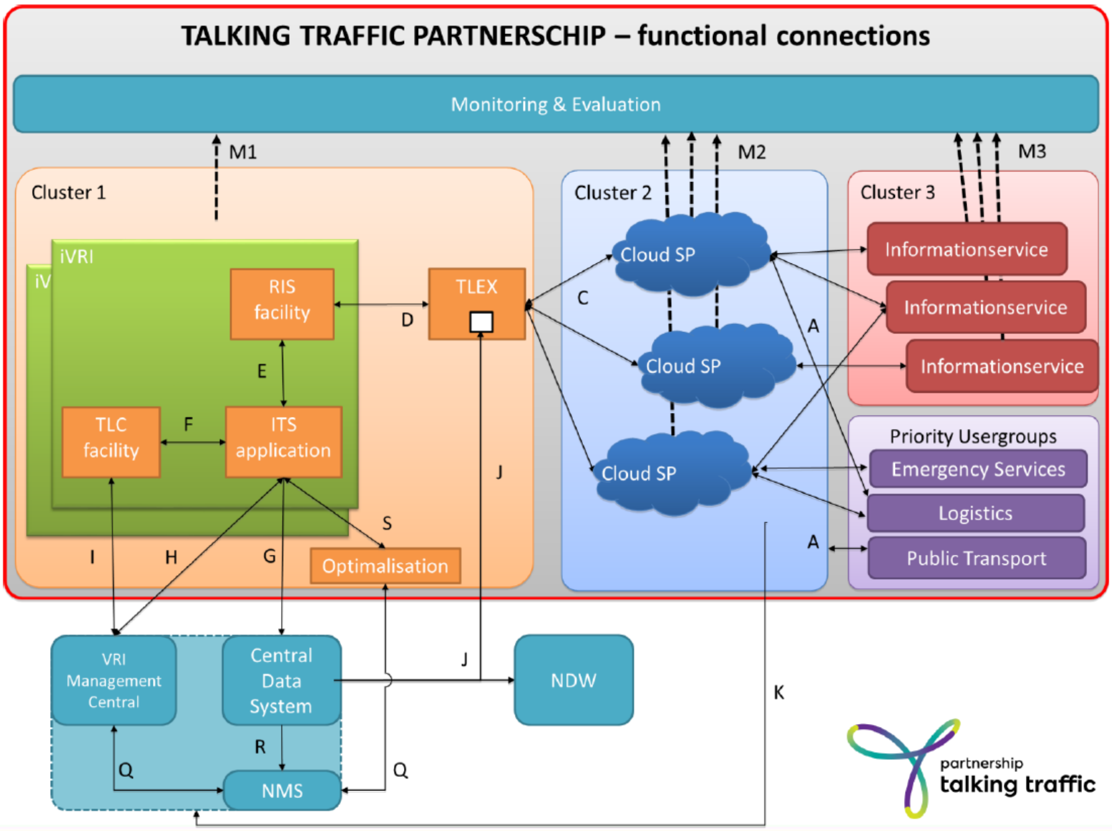


Figure 127: Talking traffic architecture [38]

5.1.1.6. Other Related Projects

On the 23rd of May 2018, ERTICO organized a "Workshop on the Interoperability of Services" at Brussels, Belgium. In the workshop, together with members from C-MobILE, the members of the following projects were involved.

- NeMo: Hyper-Network for electro Mobility or NeMo aims to make electro mobility more attractive and facilitate its mass adoption in the road transport sector. It is developing interoperability in charging and other electric vehicle services in Europe. It is creating an open cloud marketplace to connect existing services and create new business opportunities. [2]
- MOBiNET: See section 2.1.1.4.
- eMI3: eMI3 is a project that is under the umbrells of ERTICO – ITS Europe and is an open interest group. Its overall object is to harmonize the ICT data definities, formats, interfaces and exchange mechanisms to create and/or enhance eMobility ICT standards.[3]
- MaaS Alliance: Mobility as a Service (MaaS) Alliance is a public-private partnership. It is the integration of various forms of transport services into a single mobility service accessible on demand. MaaS Alliance plans to make MaaS the best value proposition to the consumers by helping them meet their mobility needs and solve the inconvenient parts of individual journeys as well as the entire system of mobility services. [4]
- AEOLIX: Architecture for EurOpean Logistics Information eXchange (AEOLIX) project is a European project that plans to establish a cloud-based collaborative logistics ecosystem for managing information pipelines that support logistics decision making to address issues with current logistics-related data stores, information channels, information management systems and data mining facilities.[5]

---

2 https://nemo-emobility.eu/

3 http://emi3group.com/

4 https://maas-alliance.eu/

5 https://ec.europa.eu/inea/en/horizon-2020/projects/h2020-transport/aeolix

- SAFE STRIP: SAFE STRIP is a Europe based project that plans to introduce a technology that will embed C-ITS applications in existing road infrastructure. They plan to implement solutions to address equipped vehicles (intelligent vehicles with on board sensors and C-ITS) as well as one to address non-equipped vehicles. [6]
- Concorda: Connected Corridor for Driving Automation (CONCORDA) project has test sites in the Netherlands, Belgium, Germany, France and Spain. Their main objective is to assess the performance of hybrid communication systems, combining 802.11p and LTE connectivity, under real traffic situations. That plan to contribute to the preparation of European motorways for automated driving and high density truck platooning.[7]
- AUTOPILOT: The AUTOPILOT consortium plan to test IoT enabled autonomous driving cars in real conditions at six permanent large scale pilot sites in Finland, France, Italy, the Netherlands, South Korea and Spain. They plan to make data from autonomous cars available to the Internet-of-Things.[8]

In the workshop, services from the participating projects that require interoperability or are important in terms of interoperability were recognized and discussed. A first view on (common) services was drafted with each workshop participant asked to complete the related project column as much as possible. The services related to C-MobILE are discussed in section 5.1.2.

In the workshop, the need to have a document repository or a collaboration platform available to store the result documents, support on-line discussions and publish meeting schedules was expressed. The participants agreed to a follow-up conference call before the end of June as a status review and to finalize the organization for a follow-workshop during the ITS World Congress in Copenhagen.

5.1.2. Interoperability in C-MobILE

Since it is expected that the service architectures of the ITS systems in the C-MobILE deployment cities are significantly different, interoperability of services will be realized on the level of specifying as less as possible interfaces to guarantee interoperability.

Out of 20 C-MobILE services, we identified the following six services that would need interoperability:

15. Road Works Warning (RWW),
16. Road Hazard Warning (RHW),
17. Emergency Vehicle Warning (EVW),
18. Green Priority (GP),
19. Green Light Optimal Speed Advisory (GLOSA), and
20. Probe Vehicle Data (PVD).

Among these, most of the services that can require interoperability are planned to be deployed in at least seven out of the eight deployment sites with RWW and RHW scheduled to be deployed in all eight deployment sites. As of last year, we see among the eight deployment sites, Vigo and Newcastle do not have any concern or have completely solved the issue of interoperability for their GLOSA services. In North Brabant only details need to be solved, whereas Bordeaux and Bilbao have concepts defined with only partial implementation. Copenhagen and Thessaloniki have problems and use-cases identified but have not completely covered them yet, while Barcelona has not addressed the interoperability concerns. The table in Figure 128 shows the state as collected during the architecture creating phase in 2017.

Deployment Sites	Level	Services
Barcelona	5	Green Priority
Bilbao	3	Urban Parking Availability
Bordeaux	3	In general
Copenhagen	4	GLOSA
Newcastle	1	GLOSA
North Brabant	2	Emergency Vehicle Warning
Thessaloniki	4	GLOSA

Figure 128: Current Interoperability Status at Deployment Sites

Description	Level
No concern/Fully solved	1
Only details need to be solved	2
Concepts defined, but only partially implemented	3
Problems/Use-cases identified but not totally covered	4
Major concerns/ not addressed yet	5

Figure 129: Index for Figure 128

[6] https://ec.europa.eu/inea/en/horizon-2020/projects/h2020-transport/safety/safe-strip

[7] https://connectedautomateddriving.eu/project/concorda/

[8] http://autopilot-project.eu

Some interoperability issues that have been identified for C-MobILE deployment sites are:

- Low harmonization and interoperability between system and services due to fragmented and proprietary solutions (NBR)
- The configuration of one or more deployment sites does not allow for all adaptions (or service extensions) to support C-Mobile (BOR)
- Data requirements for impact assessment do not fit existing capacity in the deployment site (DLR)
- Competing industry standards, challenging to align with respect to the Traffic Management System and the Traffic Light System
- Future services to be interoperable, cannot specify how protocol/technology will evolve in the future

One way the interoperability issues have been addressed is by defining the infrastructures for the deployment sites. ITS-G5 as well as cellular communication will be used for operation of the services. For ITS-G5, interoperability will be realized by harmonizing messages send over radio between RSU's and OBU's. In the case of cellular communication, it is more difficult because service providers in city X should have information available needed for services in city Y. In that case service providers X needs also to develop services that are available in other (foreign) cities, despite having these services in their own country/city.

5.1.2.1. Interoperability methods

Interoperability for the users is provided in different ways in C-MobILE. First, every service, which uses geo-references messages, can use the Geomessaging to have a type of "roaming" functionality. Second, services, which rely on a cellular connection, can use the "IF2" from Intercor to exchange data between service providers. In both cases, the user gets the same data, without the need for adaptions when he is travelling outside his home location. Those concepts are described in more detail below.

5.1.2.1.1. Cellular for Application Interface.

Regarding the cellular path more components are involved, specifically components of different cities having an interface to disseminate the information needed for the services. For example, city 1 has to provide traffic light information to service providers in order to make the GLOSA service available to the end-user. It should not matter if the end-user lives in this city or not, the service should work anyway.

In InterCor this interface has been identified as interface 2 (IF2) and an interface definition of IF2 for the services Road Works Warning (RWW), In Vehicle Signage (IVS) and Green Light Optimal Speed Advisory (GLOSA) has been described. This IF2 is an interface between back offices (see Figure 125) in the countries to exchange relevant information for the services IVS, RWW and GLOSA via cellular network. A back office is at least one central (country) back office where all data will be collected that is needed for the services that have been deployed in that country. This could be a back office of a service provider, data provider or traffic management centre/road authority where relevant information for the services will be collected and/or provided. By developing an interface between that back offices' information will be available for foreign service providers. More detailed information about IF2 is written in milestone 4 [69].

5.1.2.1.2. ITS G5 or 802.11p for Infrastructure.

Regarding the specifications for ITS-G5 communication C-MobILE will adapt the profiles of the day-1 infrastructure-to-vehicles services Roadworks Warning (RWW), Other Hazardous Location Notifications (OHLN), In Vehicle Signage (IVS), Traffic Light Manoeuvres & Road and Lane Topology (TSM & RLT), Coexistence (ITS-G5 – CEN-DSRC) and Shock-Wave-Damping (SWD) developed in C-Roads [71] [72] for the purpose of harmonizing services and therefore taking care of interoperability. After all C-Roads is a platform of Member States working on the deployment of harmonized and interoperable C-ITS services in Europe. The relevant ETSI ITS standards and profiles are highlighted in the following communication viewpoints of the various services below.

5.1.2.1.3. IF2 for inter-back office communication

Intercor has specificied IF2 for real-time C-ITS related messages between back offices. It is based on the AMQP standard v0.9.1. The specifications target the exchange of (standardized) MAPEM, SPATEM, IVI and DENM messages to support the services RWW, IVS, and GLOSA, but can easily be extended with other messages for other services. Messages are tagged with metadata that describe the type and version of the message, the originator and the geographical relevant area. Clients can subscribe to these messages and can specify its own filters based on these properties. This allows for a lightweight server implementation, as the full filtering is done based on the standard AMQP filtering mechanisms and can be specified and modified in real-time by the clients without any (management) involvement from the server side.

All messages are expected to be according to the Intercor profiles (which are integerated in the C-Roads specifications), and encoded in ASN.1 format, identical to the messages being exchanged via ITS-G5 (IF1 specifications in Intercor). The IF2 specifications, however, do not rely on the actual content or encoding of the messages.

A (backward compatible) update of the specification is foreseen in 2019, extending the specifcations with security aspects and additional services. [78]

5.1.2.1.4. Data Formats

For communication between systems/infrastructures **DATEX II** will be used for information exchange between Traffic Management Services, Traffic Information Services, Servie Providers, and all the actors involved in traffic and travel information sector. For further details and specifications, see Appendix 8.1.6.2.

MAPEM – MAPEM is a data format that is used to represent the topology/geometry of a set of lanes or area. For more details, see Appendix 8.1.5.7.

SPATEM – SPATEM is a data format that is used to represent the status of a set of traffic lights usually placed in the same geographical area and is usually sent together with MAPEM message for accurare representation of the traffic lights and the topology of lanes and roads where they are relevant. For more details, see Appendix 8.1.5.8.

ETSI CAM is a data format that is used to provide cooperative awareness within road traffic. See Appendix 8.1.5.4 for further details.

ETSI DENM – DENM message is disseminated to ITS services that are located in a geographic area through direct V2V or V2I communications. See Appendix 8.1.5.5.

In the below table, the related parties selected five of the services for interoperability (from the six that we had initially selected). They are as below:

Table 13: Services for interoperability

Service	Protocols or Data Standards	Related Projects
Green Light Optimal Speed Advce (GLOSA)	SPaT MAP MQTT, SNMP/TLS	Concorda, InterCor, MOBiNET, AutoPilot
Road Works Warning	ETSI DENM/CAM MQTT, SNMP/TLS	InterCor, Concorda, SAFE STRIP
Emergency Vehicle Warning	ETSI DENM/CAM MQTT, SNMP/TLS	Concorda
Warning System for Pedestrian	ETSI DENM/CAM, SPaT	SAFE STRIP
Green Prioroty	ETSI CAM, SPaT, SSM, SRM	

Standardization bodies

To standardize our definitions and address interoperability, we will be liaising with ETS, CEN/ISO and IEEE and develop a methodology and tools to check the standards compliancy. Also, we will need to add GDPR as a part of the standardized exercise as there can be different level of privacy from service providers in terms of interoperability and there are not any technical protocols defined to communication for privacy.

5.2. Communication Viewpoint of C-MobILE Services

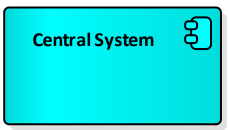
The following sections describe per service which components are involved, how they are related and which protocols should be used between entities. This information is provided as table. Therefore, for every connection, the protocols are described and additionally, the messages and datatypes are referenced for a specific flow. Some of them are not further specified as they will be developed in more detail during the project. Those details will be part of the D5.1 document.

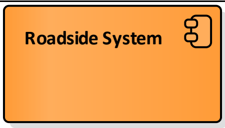
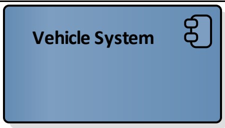
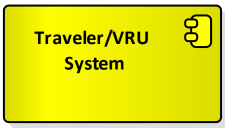
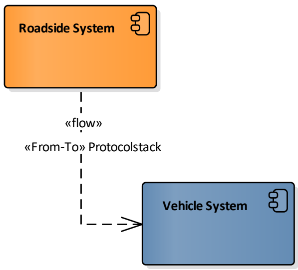
The first column of the protocol table describes the name of the flow which is also shown in the diagrams. Second and third column represent the source and destination entity. Then the fourth column is divided into multiple columns for the different protocol layer. The last one contains a reference to the used datatype for this connection.

To have a better overview of the diagrams, the components are color-coded. The meaning of the different color is listed in

Table 14. Connections or relations between components present an information flow, which are described in the table as well.

Table 14: Component diagram description

	Central System covers back office systems e.g. Service Provider Back Office or Communication Provider Back Office. All back office systems are colored in turquoise for the following sections.

	Roadside System is the layer which includes mostly a Roadside System and Roadside Unit. Roadside System means a generic entity, e.g. Traffic controller. These kind of components are colored in orange.
	The Vehicle System is colored blue and covers the ON Board Unit and Vehicle Electrical and Electronic System.
	Traveler containing the Personal Information Device and a OBU for VRUs. For the diagrams the color yellow is used.
	The information flows between entities are described as a dotted arrow from source entity to destination. Every flow is labeled with an element with the stereotype <<From-To>> which represent an Enterprise Architect Element, containing diagrams and other elements about protocols and datatypes. For this document this information is excluded and put into tables and figures.

5.2.1. Rest-Time management

Rest time management supports managing the working hours of drivers engaged in the transport of goods and passengers by road. The process is regulated by policies, laws or regulations (e.g., EU regulation (EC) No 561/2006) that lay down the rules on driving times, breaks and rest periods for the drivers.

This service enables truck drivers to make a safer journey by assisting rest time management through the provision of information on parking availability, at a relevant frequency.[74]

5.2.1.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 130.

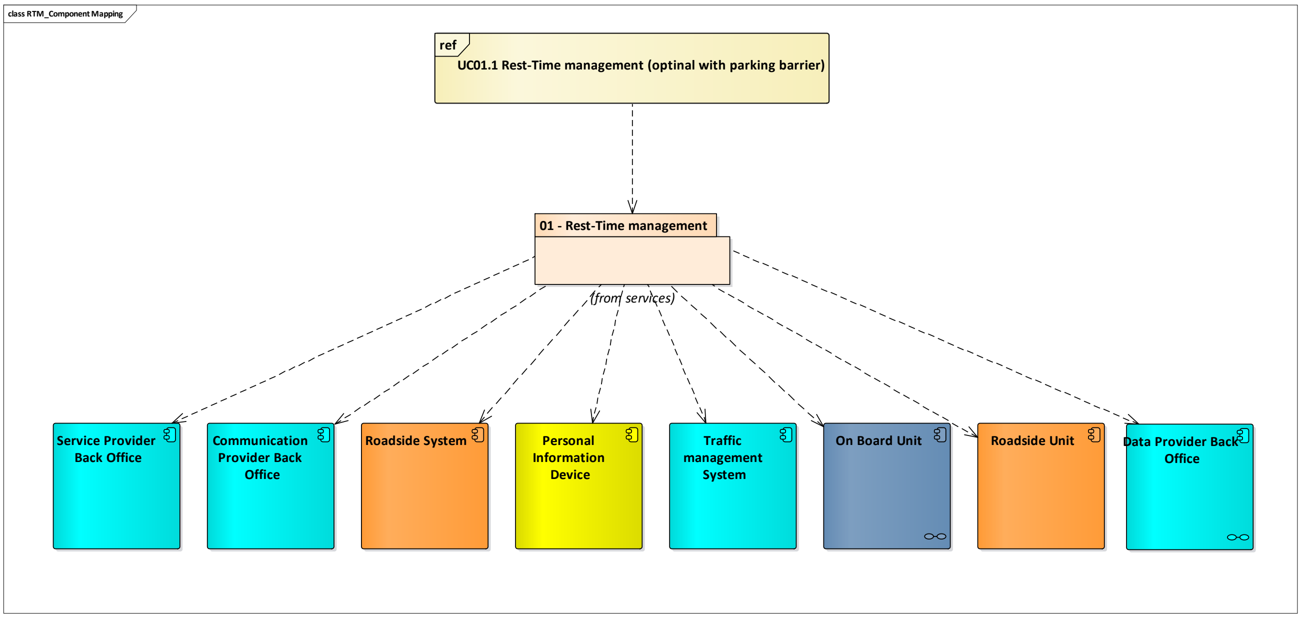


Figure 130: Rest-Time management - Components involved in service

To implement this service, the following components are necessary.

/ Service Provider Back Office (see section 4.2.2.2.3 for details.)

/ Communication Provider Back Office (See section 4.2.2.2.1 for details)

/ Roadside System (see section 4.2.3.2.1 for details.)

/ Personal Information Device (see section 4.2.5.2.1 for details.)

/ Traffic Management System (See section 4.2.2.2.5 for details)

/ On Board Unit (see section 4.2.4.2.1 for details.)

/ Roadside Unit (see section 4.2.3.2.2 for details.)

/ Data Provider Back Office (see section 4.2.2.2.4 for details.)

The relations between those components are described in the section 5.2.1.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in the ARC-IT diagram on which this service is based. This are in particular:

/ S01 Rest Time Management as shown in Appendix A

5.2.1.2. Component Connections

The following section describes the relations between the various components. In Figure 131 all the involved components and the connections between them are listed for all use cases of the service.

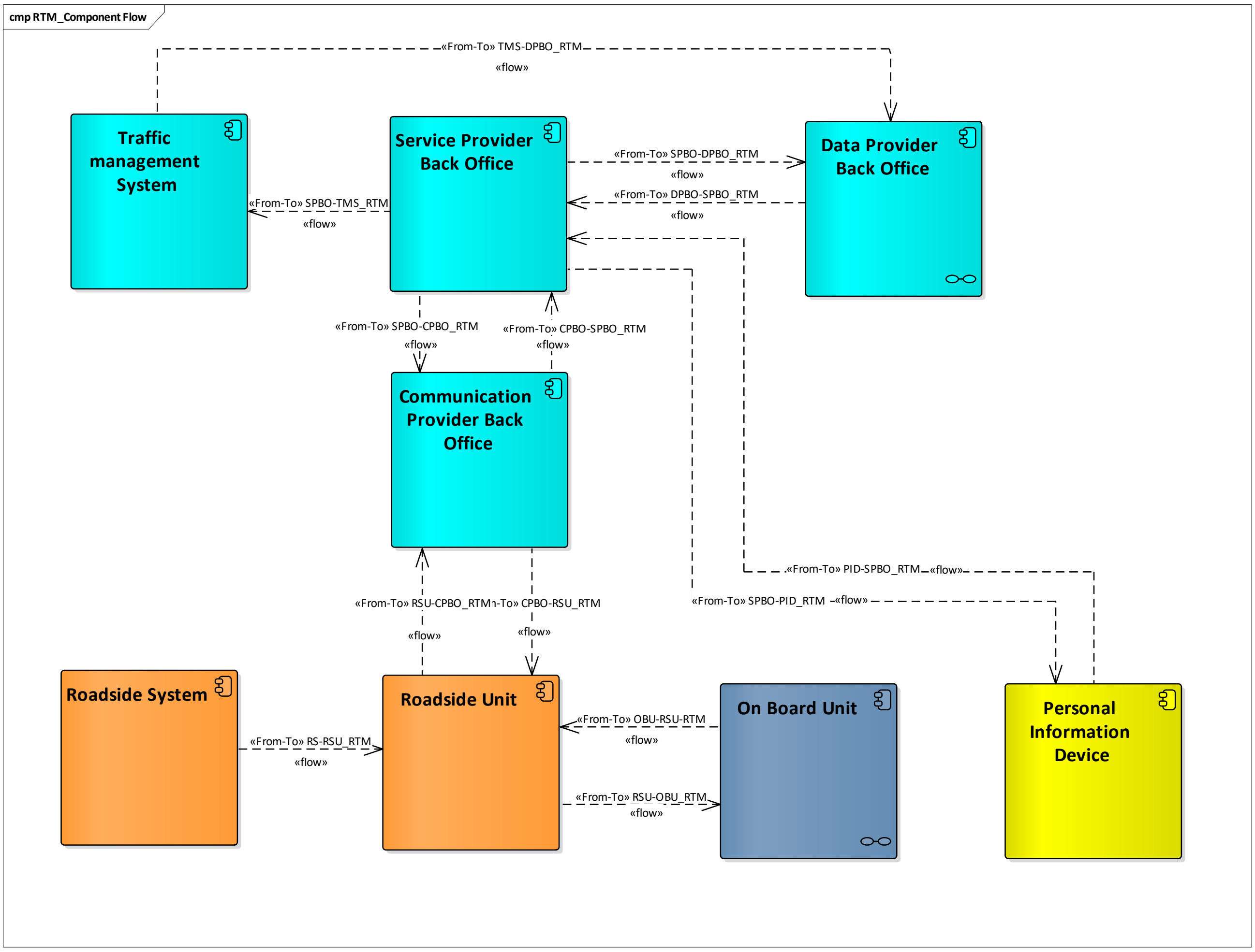


Figure 131: Rest-Time management – Components and communication flows

The **Service Provider Back Office (SPBO)** uses the information received from the **Data Provider Back Office (DPBO)**, which can also include information from the **Traffic Management System (TMS)**, to provide parking information to the Vehicle **On Board Units (OBU)** and **Personal Information Devices (PID)**. The Information about free parking lots could be collected by a **Roadside System (RS)** which pushs the information through the **Roadside Unit (RSU)** and **Communication Provider Back Office (CPBO)** to the **Service Provider**.

Table 15: Rest-Time management - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
TMS-DPBO_RTM	TMS	DPBO	HTTPS	JSON	TCP, IPv4, IPv6				Not defined yet
CPBO-TMS_RTM	CPBO	TMS	HTTPS	JSON	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_RTM	SPBO	CPBO	HTTPS	JSON	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
CPBO-SPBO_RTM	CPBO	SPBO	HTTPS	JSON	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
RSU-CPBO_RTM	RSU	CPBO	Supplier		TCP, IPv4, IPv6				
RS-RSU_RTM	RS	RSU	Supplier						
RSU-RS_RTM	RISRSU	RS	Supplier						
RSU-OBU_RTM	RSU	OBU		TBD	GeoNetworking	ETSI ITS G5			
OBU-RSU_RTM	OBU	RSU		ETSI ITS CAM	GeoNetworking	ETSI ITS G5			
SPBO-PID_RTM	SPBO	PID	HTTPS	JSON	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
PID-SPBO_RTM	PID	SPBO	HTTPS	JSON	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
SPBO-DPBO_RTM	SPBO	DPBO	HTTPS	AMQP	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet
DPBO-SPBO_RTM	DPBO	SPBO	HTTPS	AMQP	TCP, IPv4, IPv6	Generic Access	SNMP	TLS	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.2. Motorway parking availability

The use case is meant to inform truck drivers on available truck parking spaces and extra information on parking spaces. This information can bring more comfort and security by helping the truck driver manage his/her driving times and rest periods.

The objective of the use case is to provide to truck drivers information on parking spaces. Information provided are [74]:

/ the location of parking lots

/ the number of their available spaces. If not known, information provided is just “full” or “free”.

/ Vehicle Types permitted to be parked

/ Services provided in the parking lot, and associated rates

/ If the parking is secured or not

5.2.2.1. Involved Components

This section presents the components involved in the Motorway Parking Availability service. Furthermore, it lists the various sequence diagrams, which were created to describe the service. The base of the service description is the component diagram, as shown below in Figure 132.

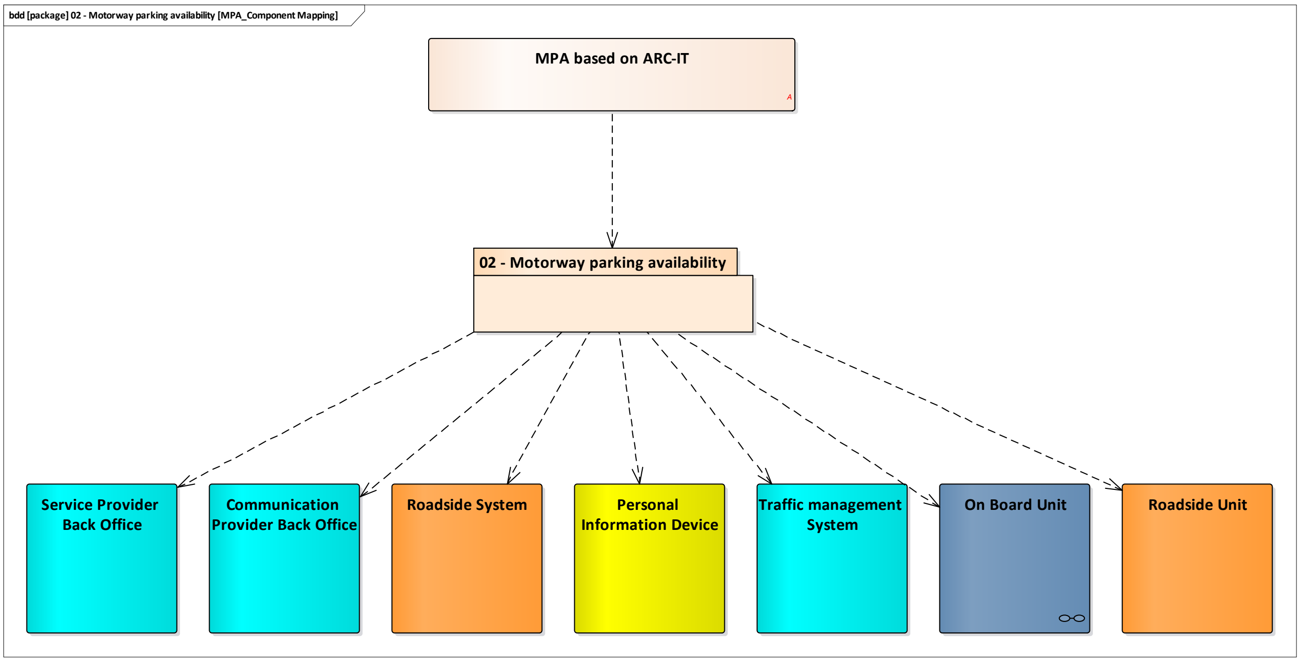


Figure 132:MPA - Components involved in the Motorway Parking Availability service

To implement this service, the following components are necessary:

/ Service Provider Back Office (see section 4.2.2.2.3 for details.)

/ Communication Provider Back Office (see section 4.2.2.2.1 for details.)

/ Roadside System (see section 4.2.3.2.1 for details.)

/ Personal Information Device (see section 4.2.5.2.1 for details.)

/ Traffic Management System (See section 4.2.2.2.5 for details)

/ On Board Unit (see section 4.2.4.2.1 for details.)

/ Roadside Unit (see section 4.2.3.2.2 for details.)

The relations between these components are described below, in the section 5.2.2.2. The general functionality of the components, as well as more detailed interactions among them, are further described in UML Sequence Diagrams, including the different use-cases of the service. More specifically, the use-cases are:

- Information on parking lots location, availability and services via internet (see Appendix A).
- Information on parking lots location, availability and services via I2V (see Appendix A).
- Information about a truck parking space released by a user (see Appendix A).
- Reservation of a truck parking space released by a user (see Appendix A).
- Guide the truck in the port (terminal or truck parking) (see Appendix A).

5.2.2.2. Component Connections

The following section describes the relations between the several components. Figure 133 presents all the involved components and the connections between them, including all the use cases of the service.

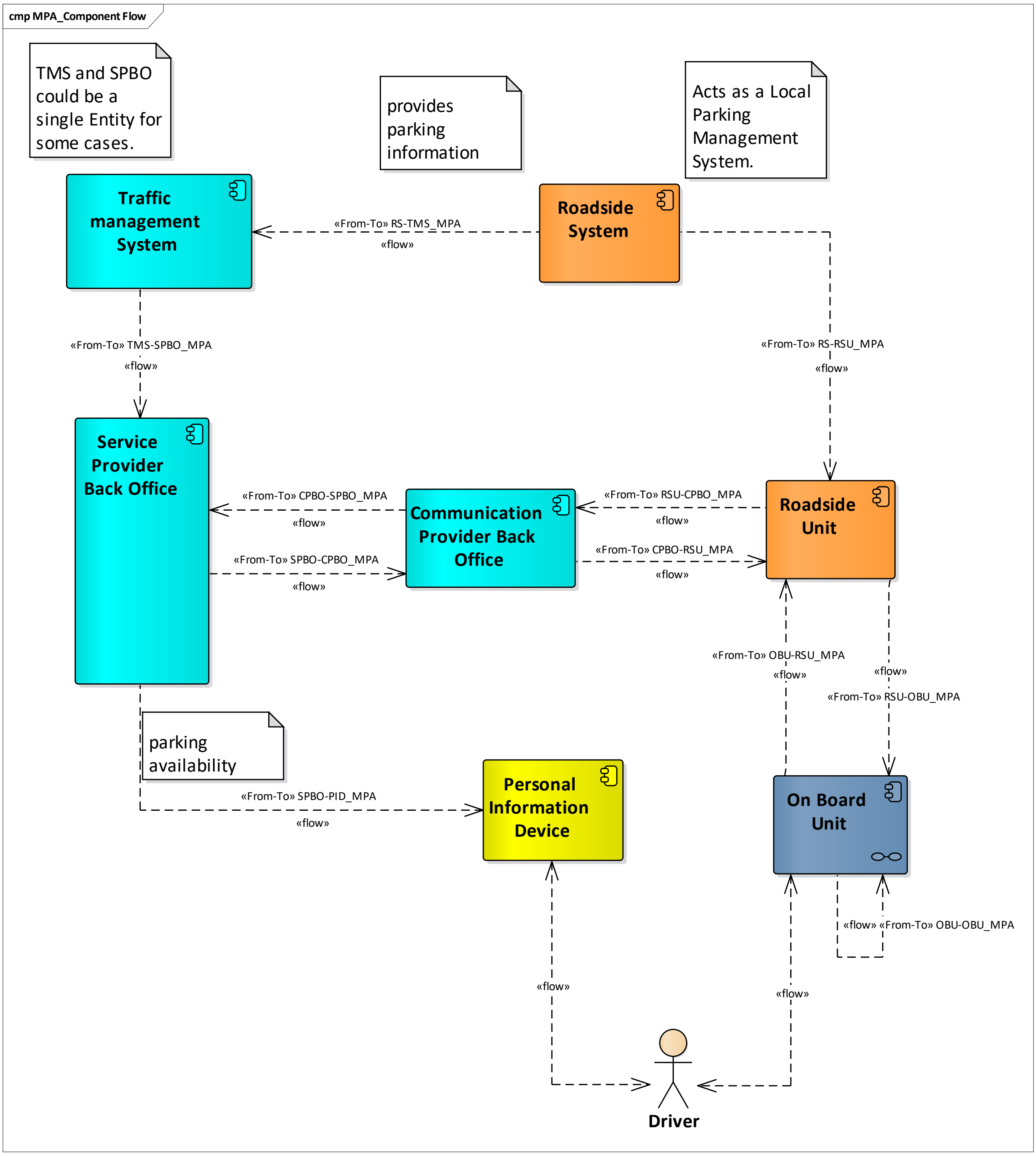


Figure 133: Motorway Parking Availability – Components and communication flows

The **Roadside System (RS)** uses **RS-TMS_MPA** connection to send parking information to the **Traffic Management System (TMS)**, which is forwarded to the **Service Provider Back Office (SPBO),** via the **TMS-SPBO_MPA** connection. In case of using the **Personal Information Device (PID)** for the service, then **SPBO** uses the **SPBO-PID_MPA** connection to send the parking availability information to the **PID**. In case of using the **On-Board Unit (OBU)**for the service, the **CPBO** uses the **SPBO-CPBO_MPA** connection to send the parking availability information to the **Roadside Unit (RSU)** or the **RS** sends the information directly to the **RSU**, which in turn forwards the information to the **OBU** via the **RSU-OBU_MPA** connection.

In the **Cooperative Communication** use case, the **OBU** uses the **OBU-OBU_MPA** connection to broadcast parking spot lookup information, in order to indicate that a vehicle is looking for a parking availability or parking spot availability/ release information to provide other vehicles with parking spot availability. This information is forwarded to the **RSU** via **OBU-RSU** connection, which in turn is forwarded to the **CPBO** via **RSU-CPBO_MPA** connection. This information is then forwarded to **SPBO** via **CPBO-SPBO_MPA** connection and then forwarded to the **TMS** via **SPBO-TMS_MPA** connection.

Table 16: Motorway Parking Availability - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
RS-TMS_MPA	RS	TMS	HTTPS	TBD	IPv4, IPv6, TCP	Generic Access	TBD	TLS	Not defined yet
RS-RSU-MPA	RS	RSU	HTTPS	ETSI ITS MAPEM	IPv4, IPv6, TCP	Generic Access	TBD	ETIS ITS Security, TLS	Not defined yet
SPBO-TMS_MPA	SPBO	TMS	HTTPS	TBD	IPv4, IPv6, TCP	Generic Access	TBD	TLS	Not defined yet
SPBO-CPBO_MPA	SPBO	CPBO	-	ETSI ITS MAPEM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	ETIS ITS Security, TLS	Not defined yet
SPBO-PID_MPA	SPBO	PID	HTTPS	TBD	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	TBD	ETIS ITS Security, TLS	Not defined yet
CPBO-SPBO_MPA	CPBO	SPBO	-	ETSI ITS MAPEM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	ETIS ITS Security, TLS	Not defined yet
CPBO-RSU_MPA	CPBO	RSU	-	ETSI ITS MAPEM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	ETIS ITS Security, TLS	Not defined yet
RSU_CPBO_MPA	RSU	CPBO	-	ETSI ITS MAPEM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	ETIS ITS Security, TLS	Not defined yet
RSU-OBU_MPA	RSU	OBU	-	ETSI ITS MAPEM	GeoNetworking	ETSI ITS-G5	TBD	ETIS ITS Security	Not defined yet
OBU_RSU	OBU	RSU	-	ETSI ITS MAPEM	GeoNetworking	ETSI ITS-G5	TBD	ETIS ITS Security	Not defined yet
OBU-OBU_MPA	OBU	OBU	-	ETSI ITS MAPEM	GeoNetworking	ETSI ITS-G5	TBD	ETIS ITS Security	Not defined yet
TMS-SPBO_MPA	TMS	SPBO	-	AMQP	IPv4, IPv6, TCP	Generic Access	TBD	TLS	Not defined yet
RS-TMS_MPA	RS	TMS	-	TBD	IPv4, IPv6	Generic Access	TBD	TBD	Not defined yet

The table above shows the protocols which should be used for the respective layer. The list may also contain alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.3. Urban parking availability

UPA provides parking availability information and guidance for drivers to make informed choices about available parking places. This service aims to reduce congestion, time loss, pollution, and stress caused by cruising for parking.

Information on urban parking availability is aimed to provide efficiency benefits to drivers and help to reduce emissions and congestions on urban areas by reducing the time spent searching for parking. [74]

5.2.3.1. Involved Components

This section presents, the components involved in the Urban Parking Availability service. Furthermore, it lists the various sequence diagrams, which were created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 134.

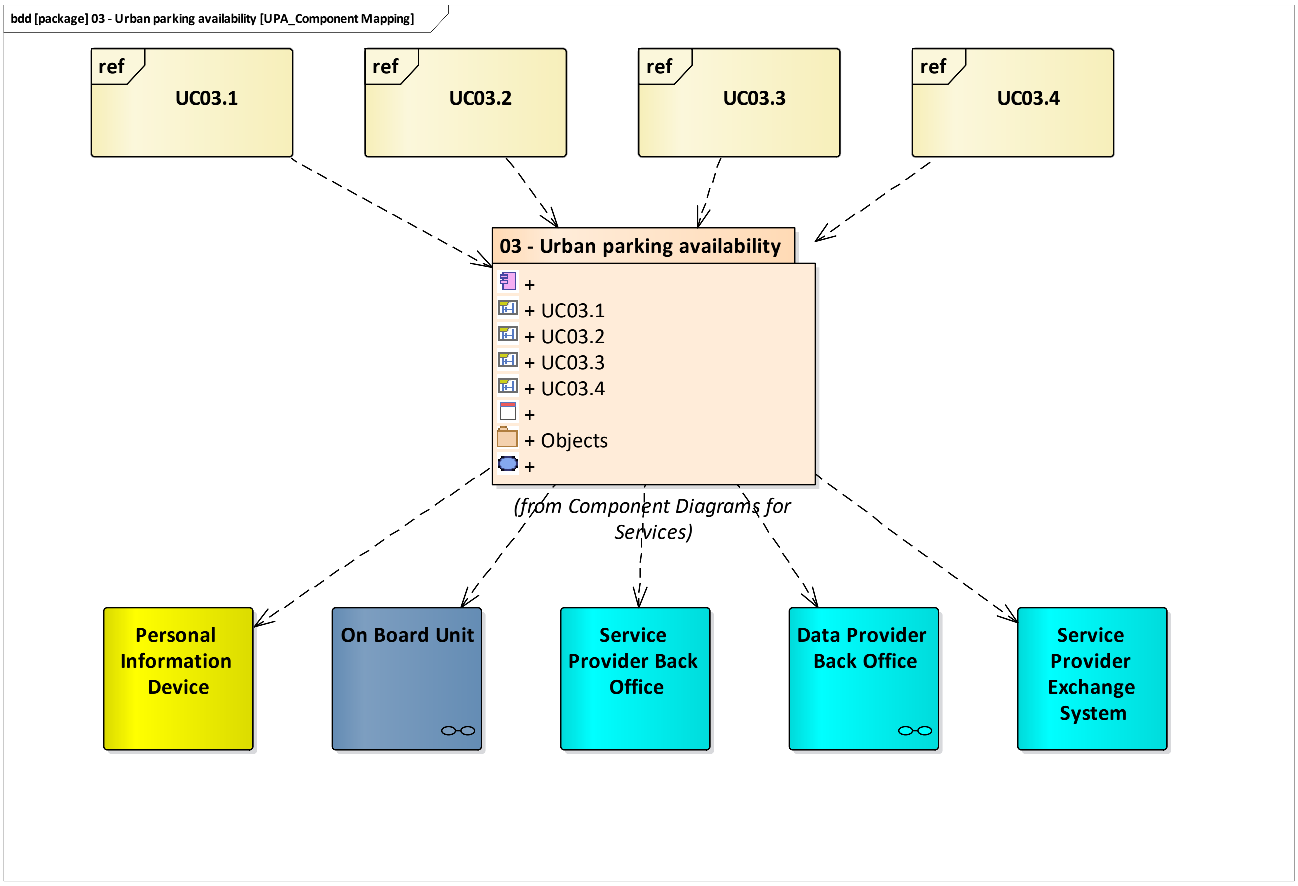


Figure 134: UPA service's component mapping diagram

Urban parking availability is described with four (4) use cases addressing a wide variety of vehicles and users. The main objective is to provide parking information and reservation information to the drivers restricted to urban areas. The four use cases are:

- UC03.1 “Information about a vehicle parking space released by a user”. (Appendix A)
- UC03.2 “Reservation of a vehicle parking space released by a user”. (Appendix A)
- UC03.3 “Information about on-street parking availability for urban freight (loading zones)”. (Appendix A)
- UC03.4 “Information about on-street parking availability for private car drivers”. (Appendix A)

The first two use cases are described using cooperative communication (Vehicle-to-Vehicle) while the last two use cases are addressed for cellular communication (connected approach).

Therefore, depending on the communication method used, the architecture for each use case as well as the relations among the components would vary. Moreover, certain particular functionalities of the use cases allowing special operations/actions from the user side may need extra connections. In general, the architecture components needed to operate the UPA service are the following:

- / Personal Information Device (see section 4.2.5.2.1 for details.)
- / On Board Unit (see section 4.2.4.2.1 for details.)
- / Service Provider Back Office (see section 4.2.2.2.3 for details.)
- / Data Provider Back Office (see section 4.2.2.2.4 for details.)
- / Service Provider Exchange Systems (see section 4.2.3.2.2 for details.)

The following section "Component Connections" describes the flows among the architecture components. The general functionality of the components, as well as more detailed interactions among them are further described in UML Sequence Diagrams, including the different use-cases of the service.

5.2.3.2. Component Connections

The following section describes the relations between the several components. Figure 135 presents all the involved components and the connections between them, including all use cases of the service.

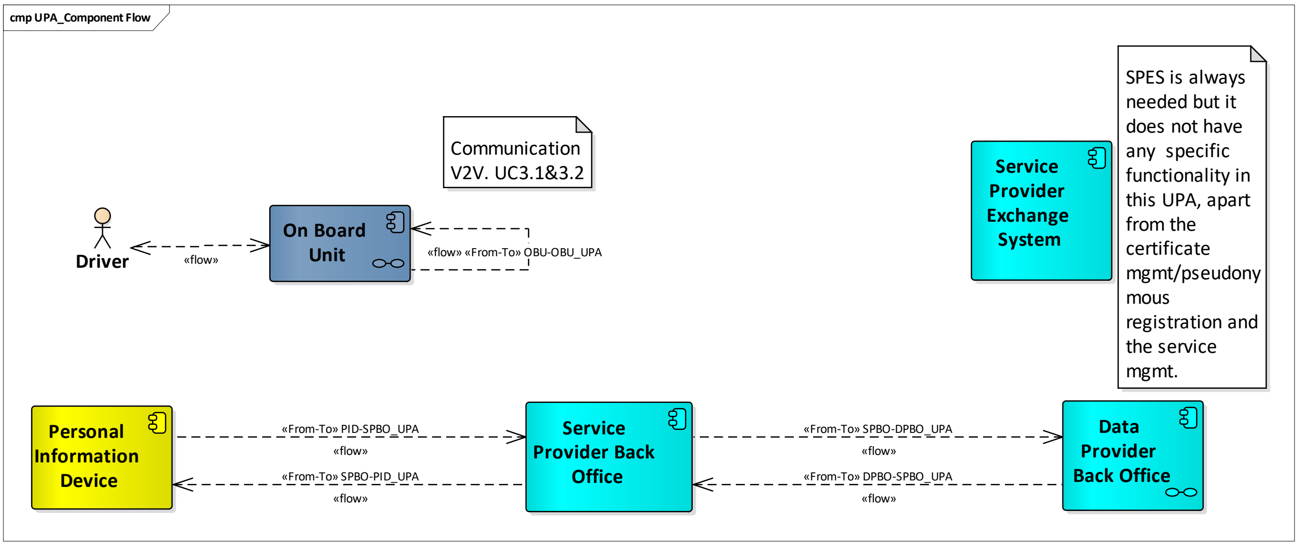


Figure 135: UPA service's components and communication flows

As in many other V2V services, a loop flow IN and OUT of the On-Board Unit (OBU) represents a V2V communication, indicating that broadcast and/or unicast information is disseminated using the IEEE 802.11p protocol so other OBU can receive it. Therefore, in the case of the **cooperative communication (IEEE 802.11p)** use cases (UC03.1 and UC03.2), the **On Board Unit (OBU)** uses the **OBU-OBU_UPA** relation to broadcast parking spot lookup information, to indicate that a vehicle is looking for a parking possibility. The receiving OBUs can use the same interface to inform the searching vehicle about the releasing of a parking spot via unicast, as an answer to the lookup, if a vehicle is about to leave a parking spot. Optionally, in UC03.2, a reservation message is also sent using the same connection, to inform the leaving **OBU** that another vehicle will take over the parking spot.

In the **Connected Communication** use cases (UC03.3 and UC03.4), the **Personal Information Device (PID)** uses the **PID-SPBO_UPA** to request information about loading zones from the **Service Provider Back Office (SPBO)**, which forwards the request to the **Data Provider Back Office (DPBO)** over the **SPBO-DPBO_UPA** connection and receives that information over the **DPBO_SPBO_UPA**. Then, the SPBO can provide the parking information to the **PID** over the **SPBO_PID_UPA**.

Table 17: Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
SPBO-DPBO_UPA	SP BO	DP BO	HTTP	SPDP, TTI(TPEG2), JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-PID_UPA	SP BO	PID	HTTP	SPDP, TTI(TPEG2), JSON	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS	Not defined yet
PID-SPBO_UPA	PID	SP BO	HTTP	SPDP, TTI(TPEG2), JSON	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS	Not defined yet
DPBO-SPBO_UPA	DP BO	SP BO	HTTP	DATEX, XML, JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
OBU-OBU_UPA	OBU	OBU	ETSI ITS BSA	SPDP, TTI(TPEG2), JSON	GeoNetworking	ETSI ITS-G5	Tpeg2-mmc	ETIS ITS Security, TPEG2-LTE	Not defined yet

The table above shows the protocols which should be used for the respective layer. The list may also contain alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols is listed in Will futher described in WP 5.

Appendix B.

The protocol layers used follow the protocol stack as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.4. Road works warning

The Service is providing in-vehicle information and warnings about road works, changes to the road layout and applicable driving regulations. Road works usually affect the road layout, driving regulations, etc. Despite dedicated signage prior to road work zones, such changed conditions frequently come as a surprise to vehicle drivers. This may lead to increased risk and sometimes even accidents, both for road users and workers.

The objectives of this service are more attentive driving while approaching and passing a work zone by providing in-vehicle information and warnings about road works, changes to the road layout and applicable driving regulations. [74]

5.2.4.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 136.

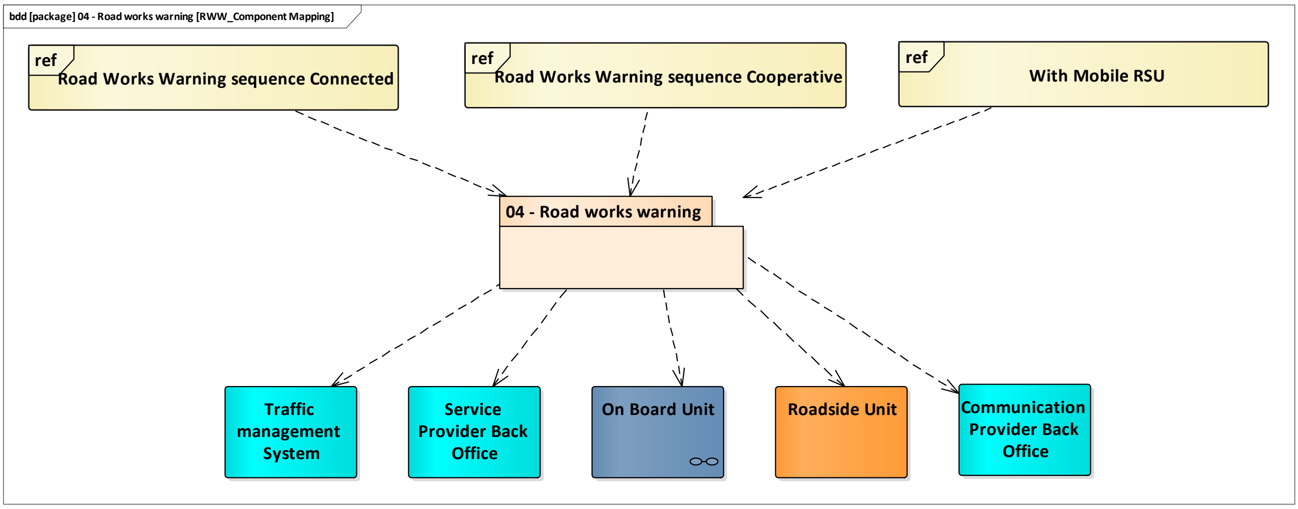


Figure 136: Road Works Warning - Components involved in service

To implement this service, the following components are necessary.

- / Traffic Management System (See section 4.2.2.2.5 for details)
- / Service Provider Back Office (see section 4.2.2.2.3 for details.)
- / On Board Unit (see section 4.2.4.2.1 for details.)
- / Roadside Unit (see section 4.2.3.2.2 for details.)
- / Communication Provider Back Office (see section 4.2.2.2.1 for details.)

The relations between those components is described in the section 5.2.4.1, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- / “Road Works Warning Sequence Connected” as shown in section 7.1.4.1.1
- / “Road Works Warning Sequence Cooperative” as shown in section 7.1.4.1.2
- / “With Mobile RSU” as shown in section 7.1.4.1.3

5.2.4.2. Component Connections

The following section describes the relations between the several components. In Figure 137 all the involved components and the connections between them are listed for all use cases of the service.

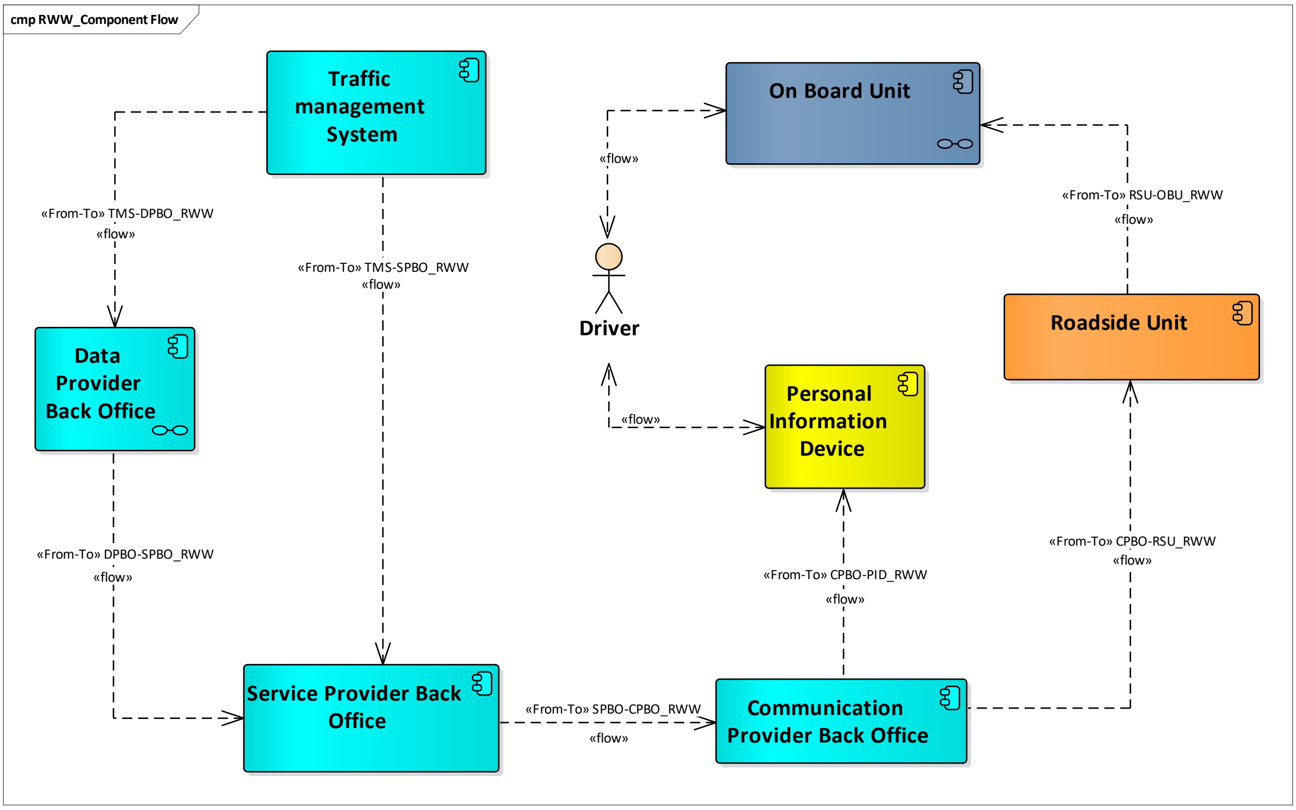


Figure 137: Road Works Warning – Components and communication flows

In the **Road Works Warning Sequence Connected** and **Road Works Warning Sequence Cooperative** scenarios, the **Traffic Management System (TMS)** either uses the **TMS-DBPO_RWW** connection to broadcast an update on roadworks to **Data Provider Back Office (DPBO)** (which in turn uses the **DPBO-SPBO_RWW** connection to update the same to **Service Provider Back Office (SPBO)**), or the **TMS-SPBO_RWW** connection to broadcast the update on roadworks directly to the **SPBO**. The **SPBO** the forwards the update to the **Communication Provider Back Office (CPBO)** over the **SPBO-CPBO_RWW** connection. Then, in **Road Works Warning Sequence Connected** scenario, the **CPBO** forwards the message directly to the **Personal Information Device (PID)** for the user to view over the **CPBO-PID_RWW** connection, whereas in the **Road Works Warning Sequence Cooperative** scenario, the **CPBO** uses the **CPBO-RSU_RWW** connection to forward the message to the **Roadside Unit (RSU)** that in turn forwards the message to the **On Board Unit (OBU)** via the **RSU-OBU_RWW** connection, where the user can see it on the **OBU**.

In the **With Mobile RSU** scenario, a **Mobile RSU** (basically a road work vehicle stationed downstream from the location where the road works is occurring) transmits the update on roadworks directly to the **OBU** via the RSU-**OBU_RWW** connection.

Table 18: Road Works Warning - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
TMS-DPBO_RWW	TMS	DPBO	DATEX II		IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
TMS-SPBO_RWW	TMS	SPBO	DATEX II	Local	IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
DPBO-SPBO_RWW	DPBO	SPBO	-	AMQP	IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_RWW	SPBO	CPBO		ETSI ITS CAM	IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Figure 183
CPBO-PID_RWW	CPBO	PID	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	ETSI ITS-S Security Architecture, TLS	Figure 184
CPBO-RSU_RWW	CPBO	RSU	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	ETSI ITS-S Security Architecture , TLS	Figure 185
RSU-OBU_RWW	RSU	OBU	-	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5		ETSI ITS-S Security Architecture	Figure 186

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.5. Road hazard warning

The road hazard warning service aims to inform the drivers in a timely manner of upcoming, and possibly dangerous events and locations. This allows drivers to be better prepared for the upcoming hazards and make necessary adjustments and manoeuvres in advance. (This is also known as "Hazardous location notification" (ETSI, 2009) or 'Road hazard signalling').

The objectives are enabling vehicle drivers to be better prepared for upcoming hazards by providing timely in-vehicle driving assistance information on hazardous locations downstream of the current position and in the driving direction of the vehicle. [74]

5.2.5.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 138.

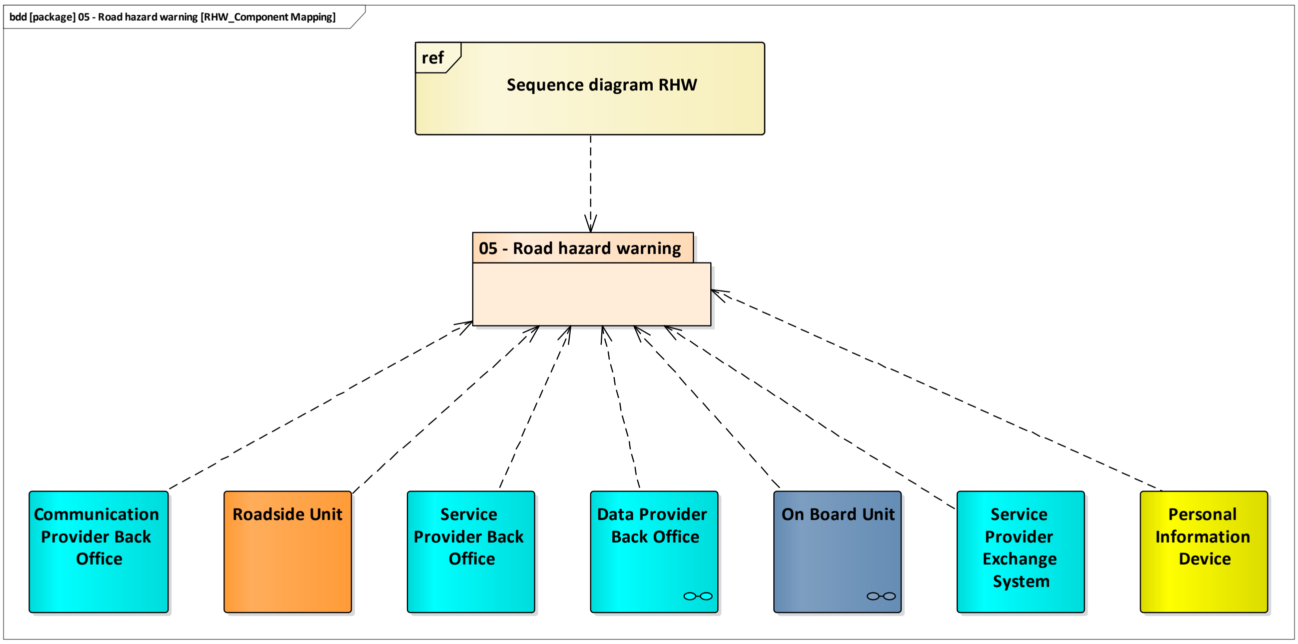


Figure 138: Road Works Warning - Components involved in service

To implement this service, the following components are necessary or optional:

- Communication Provider Back Office (see section 4.2.2.2.1 for details.)
- Roadside Unit, optional required for 802.11p communication only (see section 4.2.3.2.2 for details.)
- Service Provider Back Office (see section 4.2.2.2.3 for details.)
- Data Provider Back Office (see section 4.2.2.2.4 for details.)
- On Board Unit, optional required for 802.11p communication only (see section 4.2.4.2.1 for details.)
- Service Provider Exchange Systems, optional, services could connect manually as well (see section 4.2.3.2.2 for details.)
- Personal Information Device (see section 4.2.5.2.1 for details.)

The relations between those components is described in the section 5.2.5.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in Sequence Diagrams for the different use-cases on which this service is based and can be found in Figure 187.

5.2.5.2. Component Connections

The following section describes the relations between the components. In Figure 139 all the involved components and the connections between them are listed for all use cases of the service.

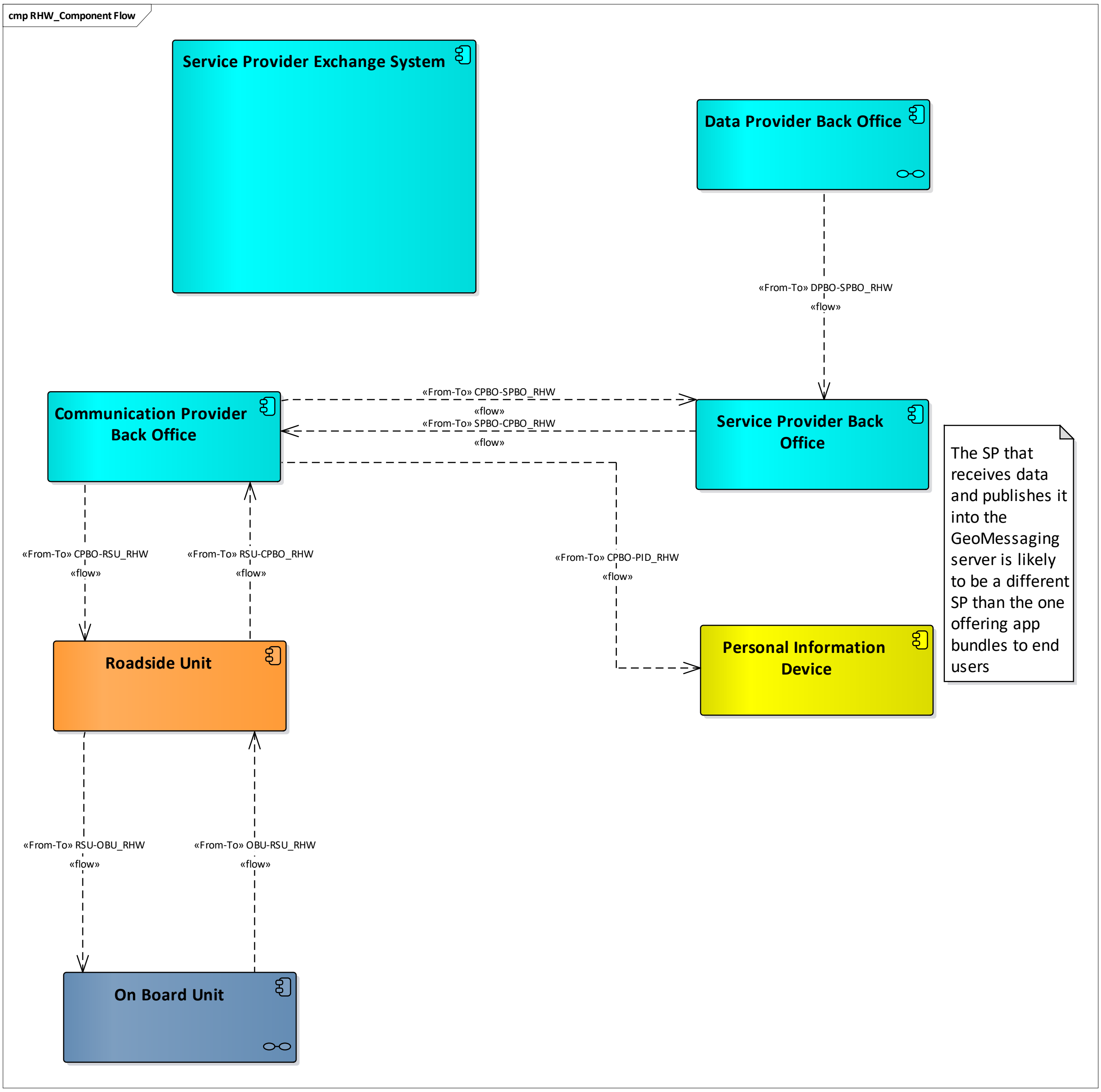


Figure 139: Road Hazard Warning – Components and communication flows

The sequence diagram in Figure 187 describes the communication flow in more detail. This diagram gives a good summary. The information originates at the **Data Provider Back Office (DPBO)**, which could be a **Traffic Management system (TMS)**, but also a data sharing platform when information is crowdsourced by a community as is common for road hazards. The **Service Provider Back Office (SPBO)** then reads this data and transforms it to C-MobILE standards, which means encapsulating the information in DENM messages. One of the main challenges here is the location references as data providers often use road names instead of geographical coordinates as reference. The **SPBO** pushes the data into the **CPBO**. At this point there are two possible paths, either the information gets directly forwarded to **Personal Information Devices (PIDs)** in the relevant area, or 802.11p communication is used. In the latter case a **Road Side Unit (RSU)** in the relevant area receives the information and broadcasts the messages. These messages will be picked up by **On Board Units (OBUs)** and they forward them to **PIDs** to display to the end-users.

For 802.11p there is also an upward information flow when either **OBUs** or **RSUs** detect a local road hazard, it can be pushed directly into the **Communication Provider Back Office (CPBO)** for further dissemination to **PIDs** without connection to an 802.11p **OBU**.

Table 19: Road Hazard Warning - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
DPBO-SPBO_RHW	DPBO	SPBO	local	AMQP	IPv6, IPv4, TCP	Generic Access	any	any	Not defined yet
SPBO-CPBO_RHW	SPBO	CPBO	-	ETSI ITS DENM, MQTT	IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
CPBO-PID_RHW	CPBO	PID	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS	Not defined yet
CPBO-RSU_RHW	CPBO	RSU	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
RSU-OBU_RHW	RSU	OBU	-	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5		ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. It should be noted that the DPBO is out of scope of C-MobILE with many projects under the umbrella of C-Roads setting the standards at that level (e.g. NordicWay, SCOOP@F and InterCor). This is therefore labeled as “local” to indicate that deployment sites can have different protocols here. Once the data reaches the SPBO, there is no applicable application anymore. MQTT is the highest level protocol used by the communicating applications, which is used to push DENMs via backend GeoMessaging to the receiver.

5.2.6. Emergency Vehicle Warning

The main objective of Emergency Vehicle Warning (EVW) is to provide an early warning indication of an emergency vehicle that is approaching and to allow other traffic participants to timely give way to emergency vehicles. [74]

5.2.6.1. Involved Components

This section shows which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 140.

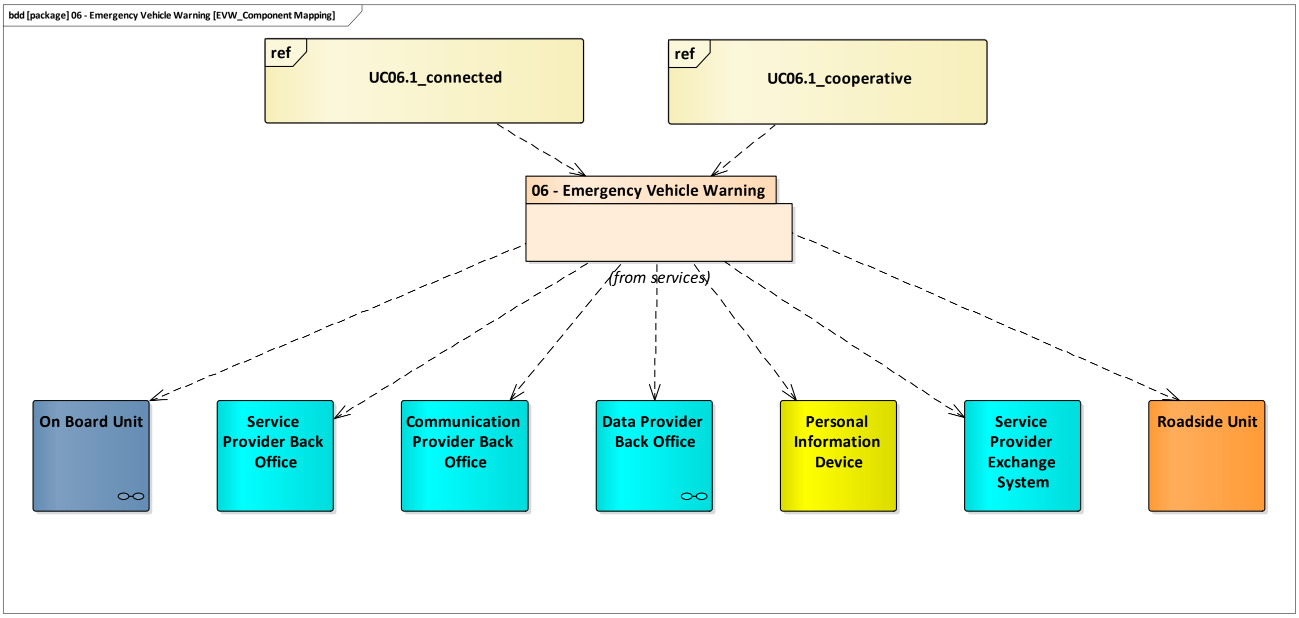


Figure 140: EVW service's component mapping diagram

The use case (UC06.1) foreseen for this service can be implemented with both communication protocols (cooperative and connected). In general, in order to implement this service, the following components are necessary:

- On Board Unit (see section 4.2.4.2.1 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Data Provider Back Office (see section 4.2.2.2.4 for details.)
- Personal Information Device (see section 4.2.5.2.1 for details.)
- Service Provider Exchange Systems (see section 4.2.3.2.2 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)

The relations among those components are described in the section 5.2.6.2, below. The general functionality of this service, as well as more detailed interactions of the involved components are further described in UML Sequence Diagrams for the unique use-case on which this service is based:

- UC06.1 “Emergency Vehicle Warning” (Appendix A)

5.2.6.2. Component Connections

The following section describes the relations between the components. In Figure 141 all the involved components and the connections among them are listed for all use cases of the service.

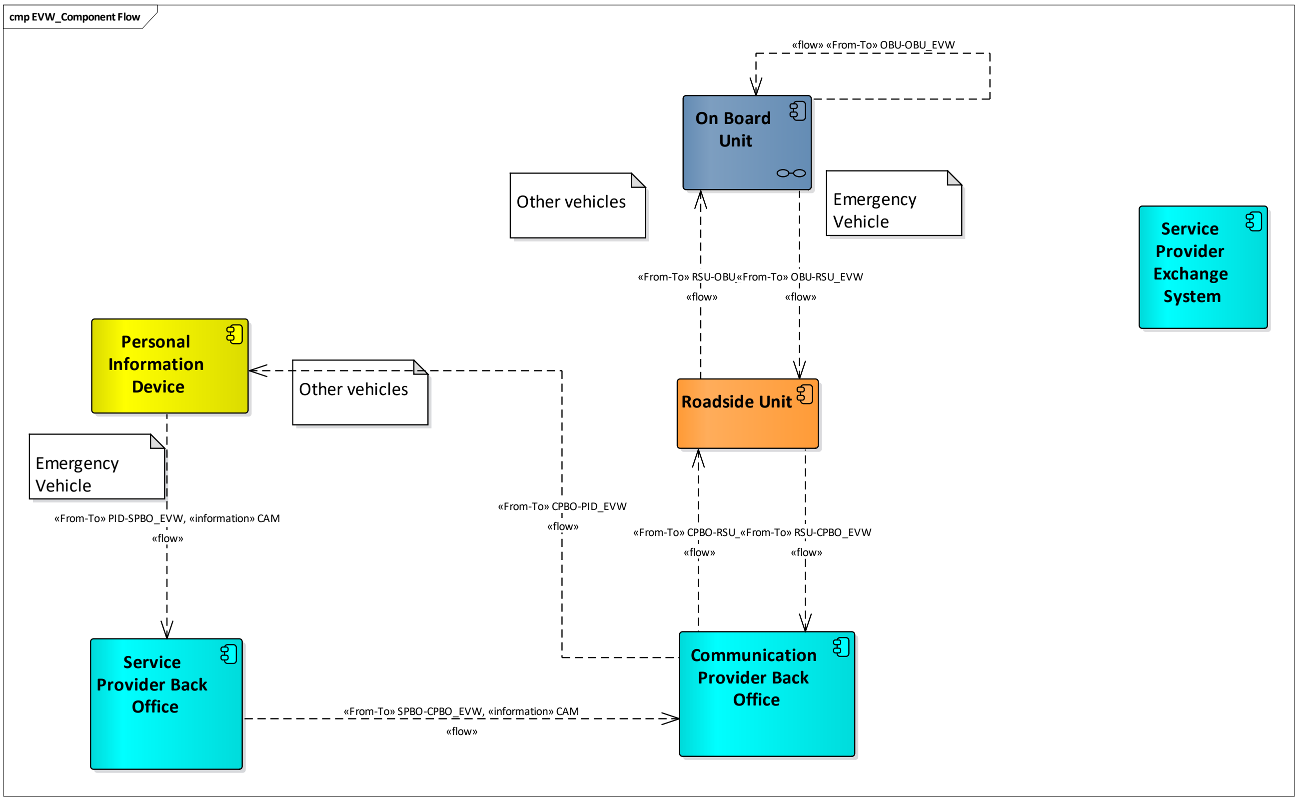


Figure 141: EVW service's components and communication flows

The component flow diagram comprises the relation among the blocks of the architecture for both communication mechanisms at the same time.

In the case of **cooperative communication (IEEE 802.11p)**, the use case starts with the emergency vehicle disseminating a CAM message, via the interface **OBU-OBU_EVW** in the diagram. This broadcasted message is received by nearby equipped stations (vehicles and Roadside Units) in the communication range of the sending emergency vehicle. Once received, the vehicles determine if the event is relevant for them and show a warning to the driver accordingly. In the case of the **Roadside Units (RSU)**, they need to convert the CAM message into a DENM message and disseminate it down to the vehicles again in the wanted relevance zone.

In the **Connected Communication** use case (UC06.1), the **Personal Information Device (PID**) of the emergency vehicle uses the **PID-SPBO_EVW** to send the CAM message to the **Service Provider Back Office (SPBO)** using a cellular communication. The SPBO forwards the message to the **Communication Provider Back Office (CPBO)** over the **SPBO-CPBO_EVW** connection in order to initiate the dissemination of the message to the other vehicles (PIDs). Therefore, the CPBO uses the GeoMessaging to be able to "broadcast" the original CAM message or a CAM-based DENM message to the relevant vehicles using a cellular communication.

In both cases, the vehicles equipped with the corresponding communication mechanism are able to receive the message. This means that in the cooperative case, the message can be sent form the RSU to the CPBO in order to reach the cellular stations and, in the connected case, the CPBO can also forward the CAM message to the RSU to reach the OBUs (after creating the corresponding DENM from the CAM message.

Table 20: EVW Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
SPBO-CPBO_EVW	SP BO	CP BO	-	ETSI ITS CAM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Figure 197
CPBO-PID_EVW	CP BO	PID	-	ETSI ITS CAM, ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS, ETSI ITS-S Security Architecture	Figure 190
CPBO-RSU_EVW	CP BO	RSU	-	ETSI ITS CAM, ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Figure 191
PID-SPBO_EVW	PID	SP BO	HTTPS	ETSI ITS CAM	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS	Figure 194
OBU-OBU_EVW	OBU	OBU	ETSI ITS BSA	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Figure 192
OBU-RSU_EVW	OBU	RSU	ETSI ITS BSA	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Figure 193
RSU-OBU_EVW	RSU	OBU	ETSI ITS BSA	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Figure 196
RSU-CPBO_EVW	RSU	CP BO	-	ETSI ITS CAM, ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	TLS, ETSI ITS-S Security Architecture	Figure 195

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols is listed in Will futher described in WP 5.

Appendix B.

The protocol layers used follow the protocol stack as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.7. Signal Violation Warning

Signal Violation Warning aims to reduce the number and severity of collisions at signalised intersections by warning drivers who are likely - due to high speed - to violate a red light, or when another vehicle is likely to make a red light violation. Also known as "Signal violation / Intersection Safety" or "Red Light Violation Warning".

The objectives of this service are providing timely in-vehicle driving assistance information on a signal violation downstream of the current position and in the driving direction of the vehicle. [74]

5.2.7.1. Involved Components

This section shows which components are involved in this service. Furthermore, it lists the different sequence diagrams for each use case and communication protocol, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 142:

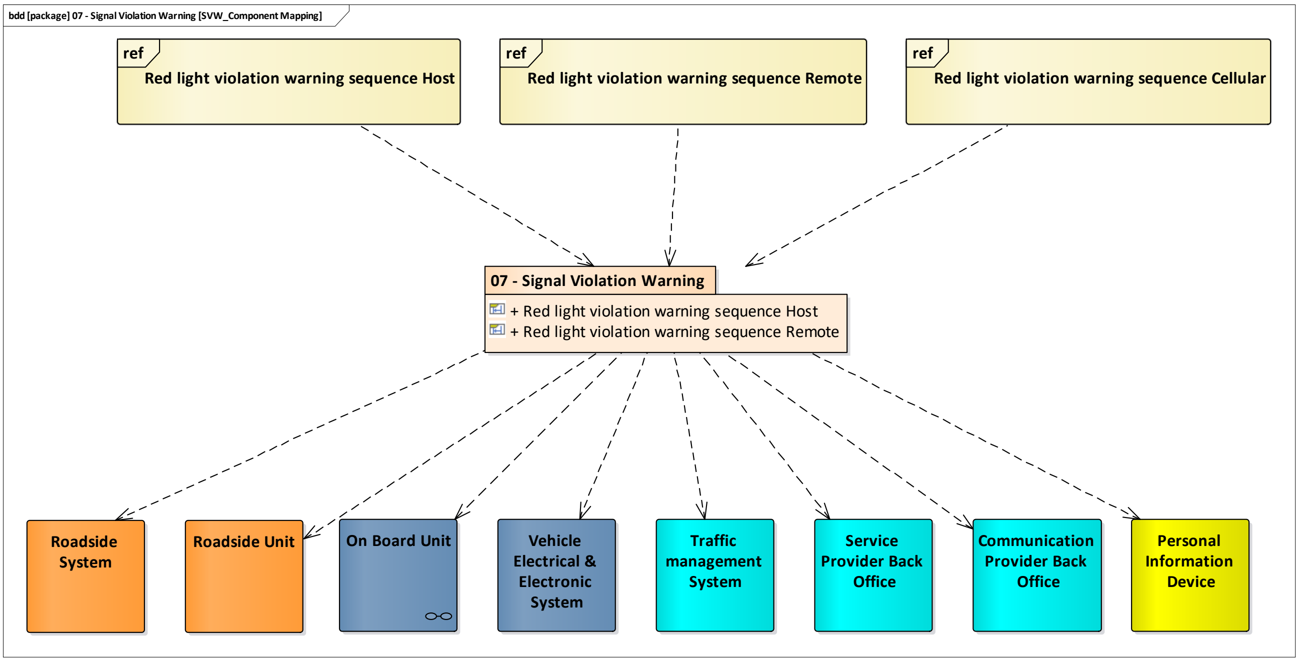


Figure 142: Signal Violation Warning - Components involved in service

To implement this service, the following components are necessary.

- Roadside System (see section 4.2.3.2.1 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Vehicle Electrical & Electronic System (see section 4.2.4.2.2 for details.)
- Traffic Management System (See section 4.2.2.2.5 for details)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components are described in the section 5.2.7.2, below. The general functionality of these services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. These are in particular:

- UC07.1 Red light violation warning sequence Host as shown in Figure 133

/ UC07.1 Red light violation warning sequence Remote as shown in Figure 199

5.2.7.2. Component Connections

The following section describes the relations between the components. In Figure 143 all the involved components and the connections between them are listed for all use cases of the service.

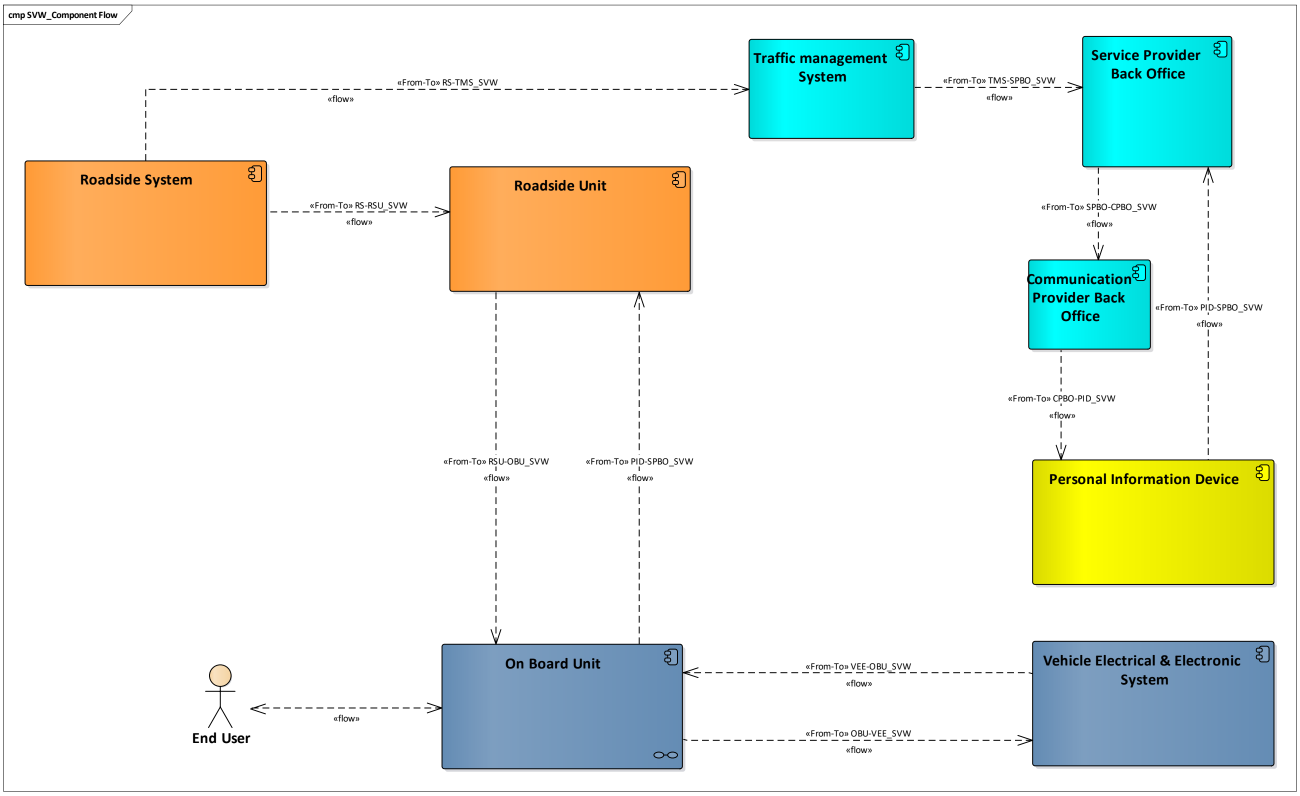


Figure 143: Signal Violation Warning – Components and communication flows

For RWW the **Roadside Unit (RSU)** receives information about the intersection state through the **RS-RSU_SVW** connection by a **Roadside System (RS)**.

This information is distributed to the **On Board Unit (OBU)** over the **RSU-OBU_SVW** relation, which can then determine a possible violation and warn the driver (UC07.1). The **OBU** shares the vehicle state to the **RSU** through the **OBU-RSU_SVW** connection, then the **RSU** can determine the violation and distribute the warning to other vehicles (UC07.2). In the same use case, if the vehicle is not equipped with a **OBU** the **RS** recognizes the violation (e.g. with sensors, cameras) and provides this information to other vehicles.

The vehicle state information can be read from the **Vehicle Electrical & Electronic System (VEE).** Therefore, the connections **VEE-OBU_SVW** and **OBU-VEE_SVW** are used. Those connections are out of scope in C-MobILE and are highly dependent by the Deployment Sites.

For the cellular way, the information gets send from the **RS** to the **Traffic Management System (TMS)**, which provides data to the Service Provider Back Office (SPBO) using the **TMS-SPBO_SVW** connection. The SPBO will receive location data from the **Personal Information Device (PID)** through PID-SPBO_SVW relation and calculates possible violations. This information is send as DENM by using GeoMessaging over the Communication Provider Back Office to the PID using SPBO-CPBO_SVW and CPBO-PID_SVW connection.

Table 21: Signal Violation Warning- Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
RS-RSU_SVW	RS	RSU	UTMC TS004.006	UTMC TS003, ETSI ITS SPATEM, ETSI ITS DENM	IPv4, IPv6, TCP	Generic Access	IETF RFC 1907	IETF RFC 6347	Figure 200
RSU-OBU_SVW	RSU	OBU	SAE J2735, CEN ISO 19091, ETSI 102 894-2	ETSI 103 301, ETSI ITS DENM	GeoNetworking	ETSI ITS-G5	G5 Congestion Control Management	ETSI IST-S Security Architecture	Figure 201
OBU-RSU_SVW	OBU	RSU	ETSI 102-894-2, ETSI 102 638	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	ETSI 102 890-1, G5 Congestion Control Management	ETSI ITS-S Security Architecture	Figure 203
OBU-VEE_SVW	OBU	VEE	Out of scope						
VEE-OBU_SVW	VEE	OBU	Out of scope						
RS-TMS_SVW	RS	TMS	DATEX	XML, ETSI ITS SPATEM	IPv4, IPv6, TCP	Generic Access	TBD	TLS, ETSI ITS-S Security Architecture	Not defined yet
TMS-SPBO_SVW	TMS	SPBO	DATEX	XML, ETSI ITS SPATEM	IPv4, IPv6, TCP	Generic Access	TBD	TLS, ETSI ITS-S Security Architecture	Not defined yet
SPBO-CPBO_SVW	SPBO	CPBO	-	ETSI ITS SPATEM , ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	TBD	TLS, ETSI ITS-S Security Architecture	Figure 202
CPBO-PID_SVW	CPBO	PID	-	ETSI ITS SPATEM , ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	TBD	TLS, ETSI ITS-S Security Architecture	Not defined yet
PID-SPBO_SVW	PID	SPBO	-	ETSI ITS CAM	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	TBD	TLS, ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layers. Those listing may also contain alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used follow the protocol stack as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.8. Warning system for pedestrian

5.2.8.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown in Figure 144.

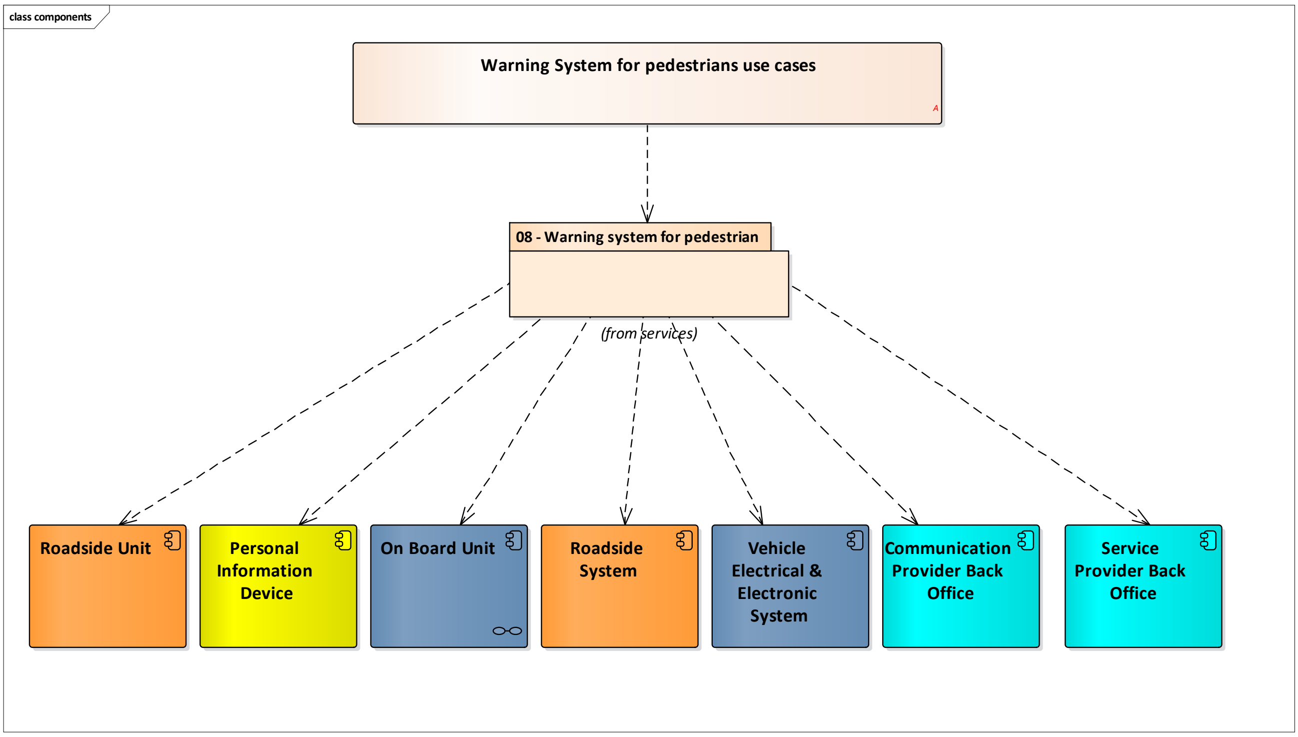


Figure 144: Warning system for pedestrian – Components involved in service

To implement this service, the following components are necessary.

- Roadside Unit (see section 4.2.3.2.2 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Roadside System (see section 4.2.3.2.1 for details.)
- Vehicle Electrical & Electronic System (see section 4.2.4.2.2 for details.)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Service Provider Back Office (See section 4.2.2.2.3 for details)

The relations between those components are described in the section 5.2.7.2, below. The general functionality of these services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. These are in particular:

- Warning system for pedestrians without RSU for detection or traffic lights shown in Figure 204
- Warning system for pedestrians with RSU for VRU detection as shown in Figure 205
- Warning system for pedestrians Signalled crossing without RSU for VRU detection as shown in Figure 206

/ Warning system for pedestrians Signalled crossing with RSU for VRU detection as shown in Figure 207

/ Warning system for pedestrians Signalled crossing with RSU for VRU detection with cellular communication to the OBU as shown in Figure 208

5.2.8.2. Component Connections

The following section describes the relations between the components. In the following figures all the involved components and the connections between them are listed for all use cases of the service.

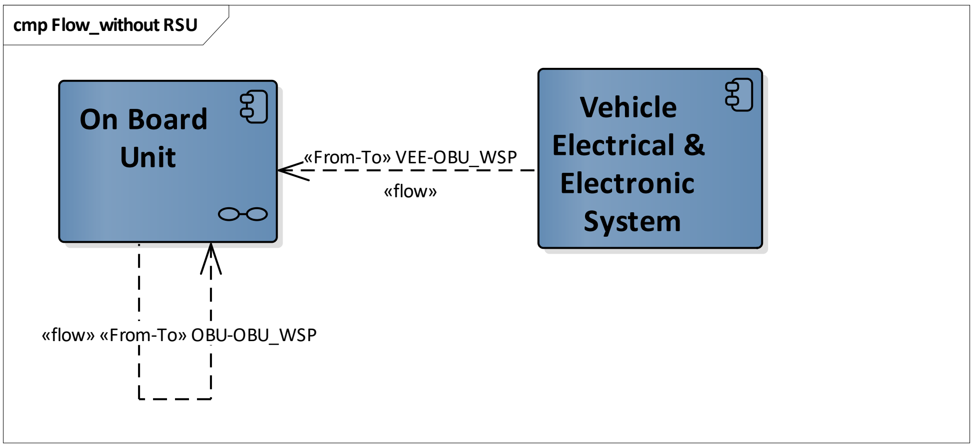


Figure 145: Warning system for pedestrians without RSU – Components and communication flows

The first use case of the Warning System for Pedestrians (WSP) is that where there are no Road Side Units (RSU), vehicles are communicating via ETSI ITS G5. There are two instances of the OBU component. One is detecting the pedestrian and transmitting the information to the other one whose trajectory possibly collides with the VRU. There is the singularity case where both instance are the same and the OBU detects itself there is an VRU on its trajectory but that is not considered as C-ITS.

The **OBU(VRU)-OBU** communication consists of a **DENM** message (See requirement R/S08-WSP-10) with cause code people on the road. The receiving OBU calculates if there is a possible collision with the VRU. If so the OBU informs the driver via the cars HMI. The OBU expects a reaction from the driver such as slow down, take a turn or acknowledge the message. It after a time-out no reaction is detected the safety protocol of the OBU is activated. The **OBU-HMI** communication and the safety protocol are proprietary car specific implementations.

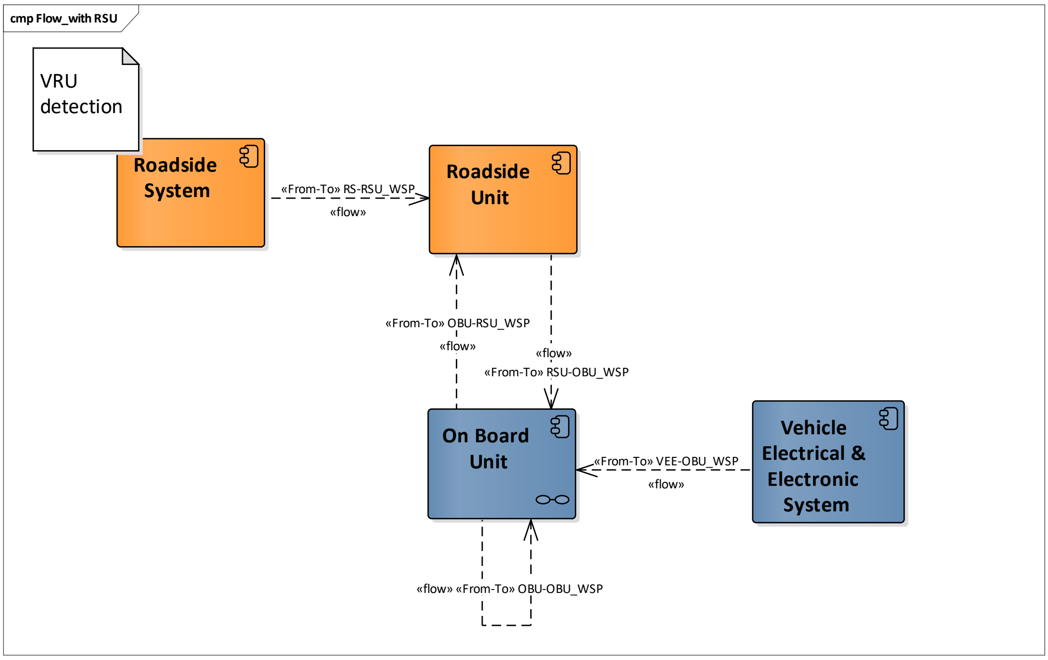


Figure 146: Warning system for pedestrians with RSU for VRU detection – Components and communication flows

In the case of a unsignalled pedestrian crossing (zebra but no traffic lights) a RSU with VRU detection capabilities can be installed. The **RSU** will monitor the trajectories of the VRU with its detection system. The connected cars indicate their presence with broadcasted CAM messages that are used in the **OBU-RSU(VRU)** communication flow. The **RSU** calculates the trajectories of both car and VRU. In case of a conflict the **RSU**(VRU)-**OBU** communication flow uses a DENM message indicating VRU on the road.

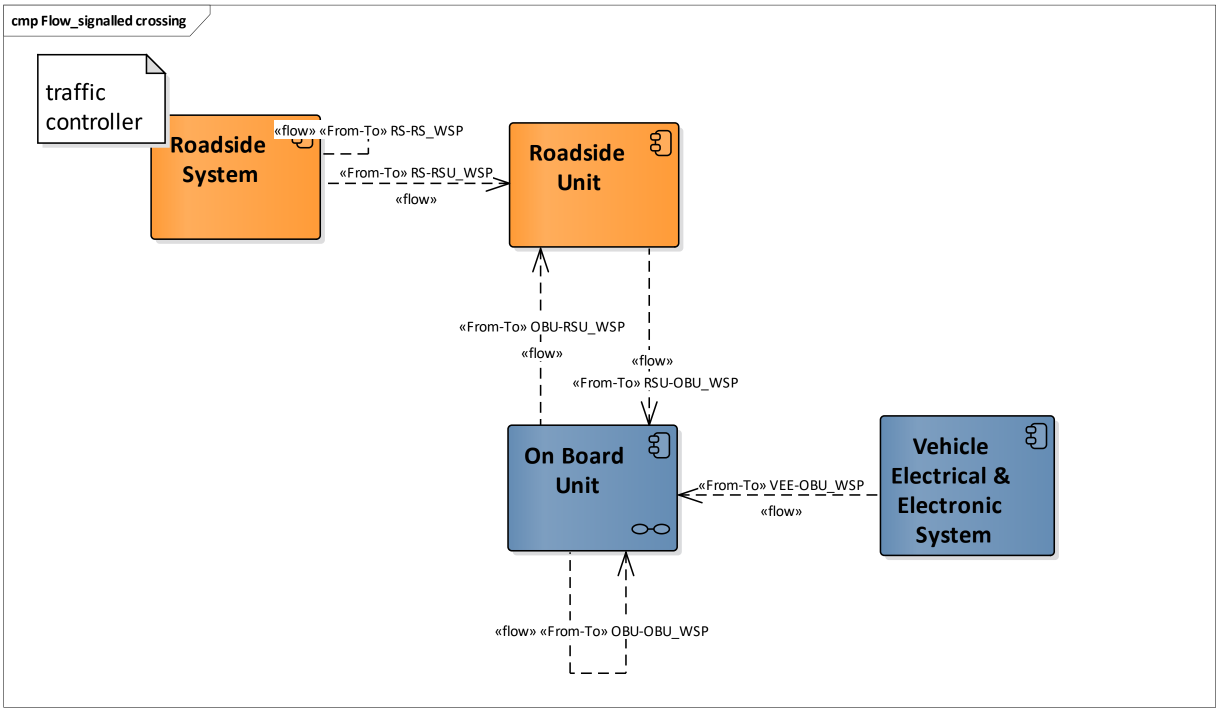


Figure 147: Warning system for pedestrians Signalled crossing without RSU for VRU detection – Components and communication flows

In the case of a signalled crossing with a **RSU** with C-ITS capabilities the **RSU** controlling the traffic lights sends a SPAT or SPATEM message. In the WSP service the **RSU**(TLC)-**OBU** only goes from the **TLC** to the car. For other services there could also be messages from the **OBU** to the **TLC** that are used to optimize the scheduling of the lights. The **OBU** uses the information in the SPAT message to decide if the VRU has priority because of the green light. In that case no warning is issued through the HMI because the driver already is informed via the status of the traffic lights on its own lane. If the VRU violates the lights than a warning is issued. If the driver does not react the safety protocol is activated. The detection of the VRU can come from another OBU that sends a DENM message (**OBU**(VRU)-**OBU**).

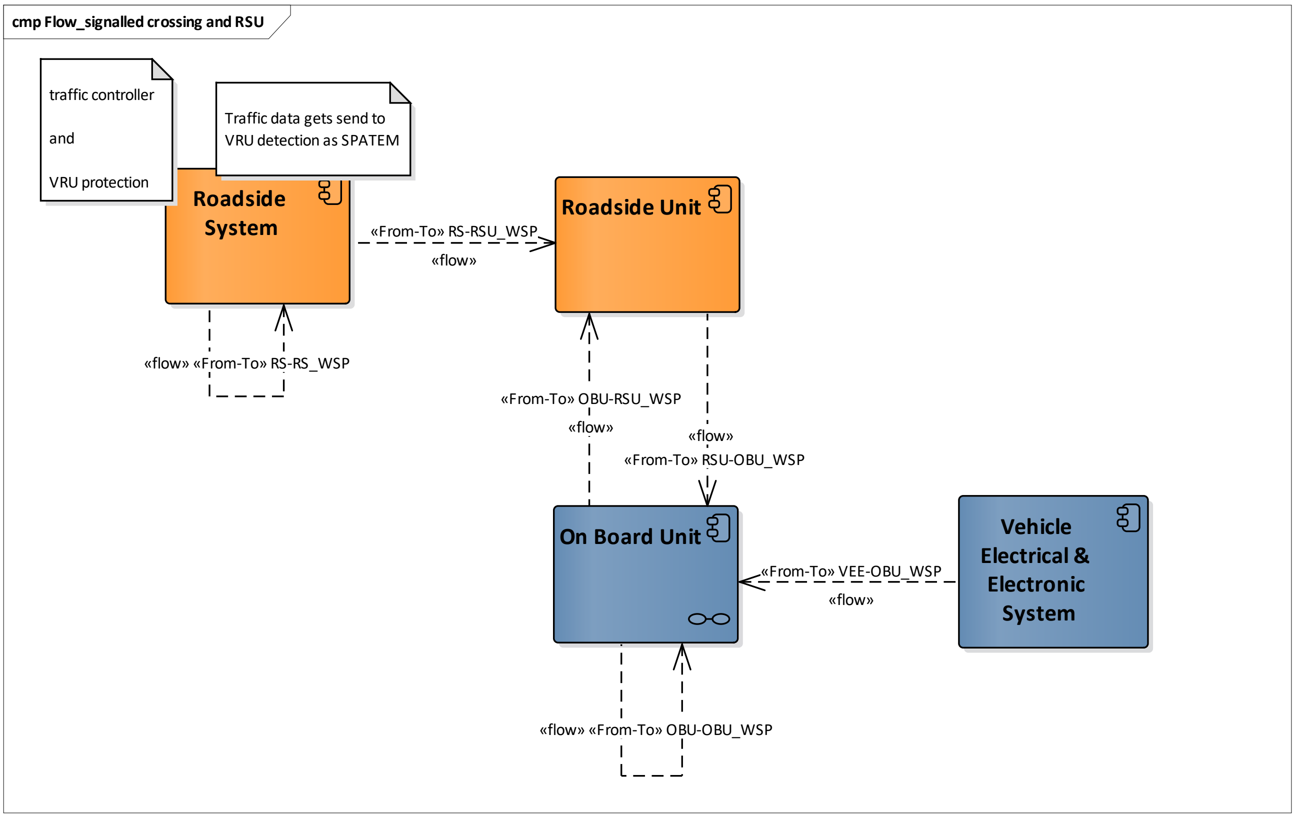


Figure 148: Warning system for pedestrians Signalled crossing with RSU for VRU detection – Components and communication flows

The uses case of a signalled crossing with a **RSU TLC** and a **RSU** with VRU detection is a combination of the previous two use cases. Here we consider the case where the **TLC** does not use DSRC communication. The **RSU** with VRU detection receives the traffic light status via a wired **RSU(TLC)-RSU(VRU)** connection. The vehicles **OBU** sends CAM messages to inform about its trajectory that are interpreted by the **RSU**. In the **RSU(VRU)-OBU** communication flow the **RSU** sends a **DENM** message if there is a conflict in the trajectories and the VRU does not have a green light. The **OBU** combines the DENM info with its own information to decide if it is necessary to warn the driver through the HMI. If so and the driver does not react the safety protocol is activated.

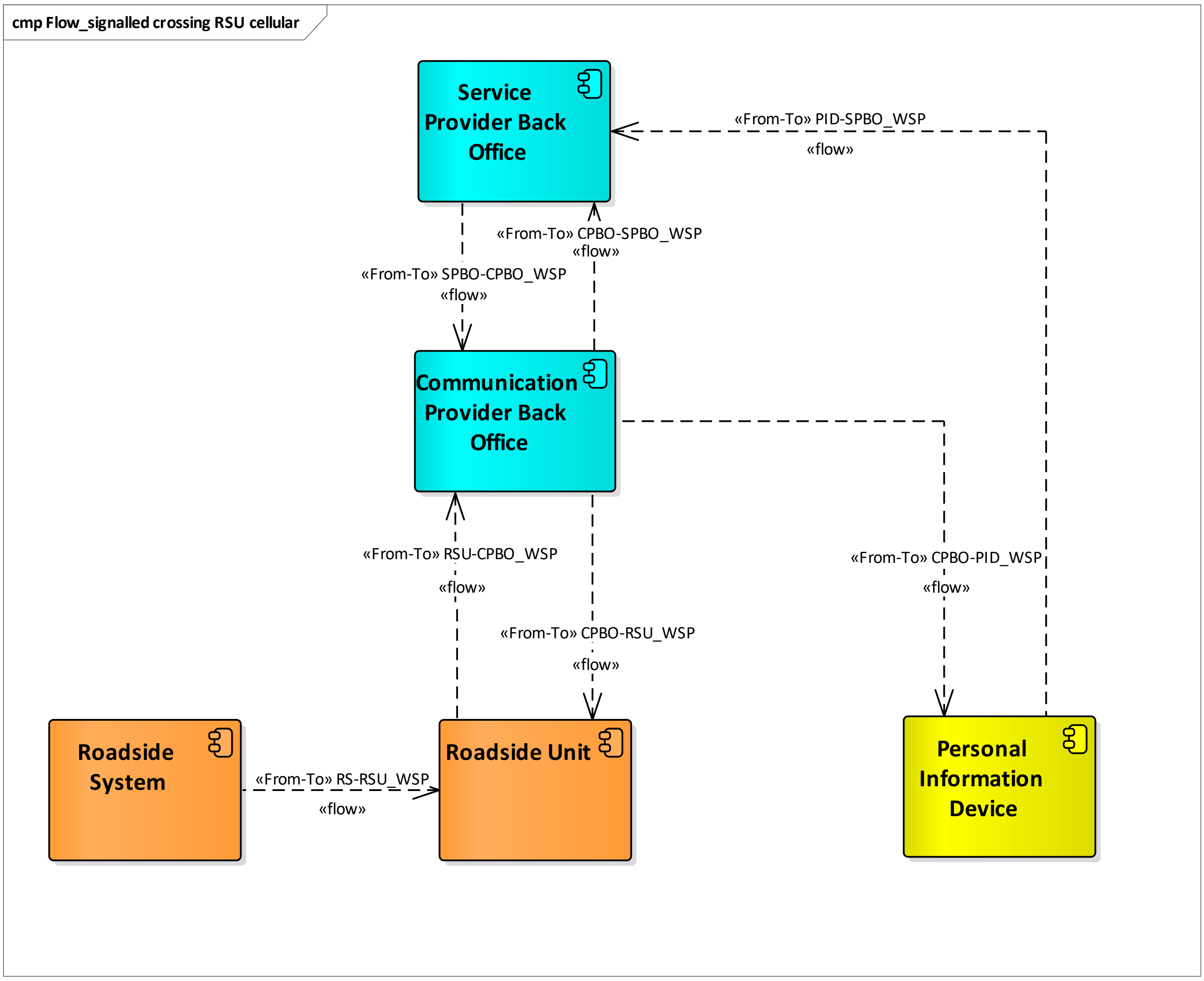


Figure 149: Warning system for pedestrians Signalled crossing with RSU for VRU detection Cellular communication with OBU – Components and communication flows

With the OBU the drive activates the WSP service at his service provider. The service provider's data center allocates a distributed data center local to the vehicles position that will monitor the vehicle. If the vehicles move away from this distributed data center another distributed data center is allocated.

The distributed data center receives frequent updates of the vehicle position. This position is send to **RSU** with VRU detection that are nearby. The **RSU** combines the traffic light status with the detection of VRUs and the vehicle position. If the light is red for the VRU and there is a possible conflict with the vehicle trajectory the RSU sends a message to the distributed data center. The distributed data center sends a message to the OBU via the cellular transport network. Finally, the **OBU** receives the message that a VRU is detection on his trajectory. The **OBU** warns the driver via the HMI. If no reaction is detected the **OBU** activates the safety procedure.

Table 22: Warning system for pedestrian- Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
OBU(VRU)-OBU	OBU	OBU	-	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Not defined yet
RSU(TLC)-RSU(VRU)	RSU	RSU	-	ETSI ITS SPAT	IPv4, IPv6, TCP	Generic Access	-	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU(VRU)-OBU	RSU	OBU	-	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Not defined yet
RSU(TLC)-OBU	RSU	OBU	-	ETSI ITS SPAT	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Not defined yet
OBU-RSU(VRU)	OBU	RSU	-	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.9. Green priority

Green Priority aims to change the traffic signals status along the route of a priority vehicle (e.g., public transportation or emergency vehicles), halting conflicting traffic and allowing the vehicle right-of-way, to help reduce service and response times and enhance traffic safety.

Green Priority aims to increase punctuality and response time of the services provided with designated vehicles and enhance traffic safety. [74]

5.2.9.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 150.

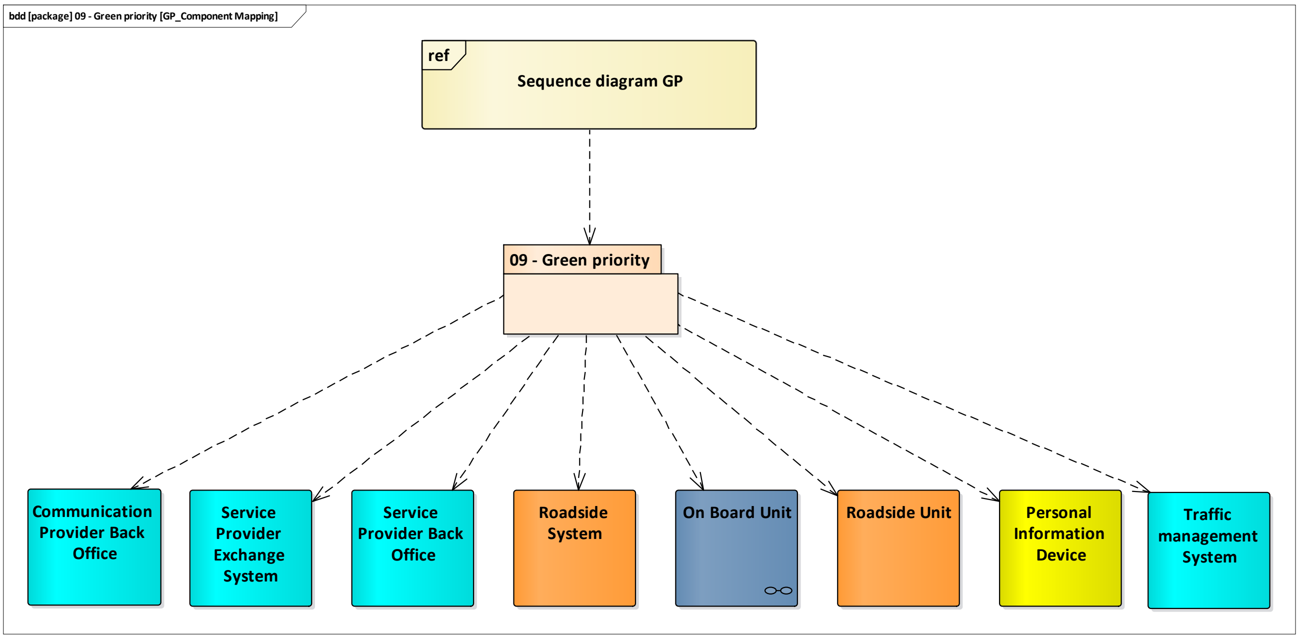


Figure 150: Green Priority - Components involved in service

To implement this service, the following components are necessary or optional.

- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Service Provider Exchange Systems, optional, services could connect manually as well (see section 0 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Roadside System, this is the traffic light controller that changes the program to facilitate the signal priority. (see section 4.2.3.2.1 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Roadside Unit, optional required for 802.11p communication only (see section 4.2.3.2.2 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)
- Traffic management system, although not included in the communication flow, this is usually the system that configures the Roadside Systems on how to accommodate priority requests (see section 4.2.2.2.5 for details.)

The relations between those components is described in the section 5.2.9.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in Sequence Diagrams for the different use-cases on which this service is based and can be found in Appendix A.

5.2.9.2. Component Connections

The following section describes the relations between the several components. In Figure 151 all the involved components and the connections between them are listed for all use cases of the service.

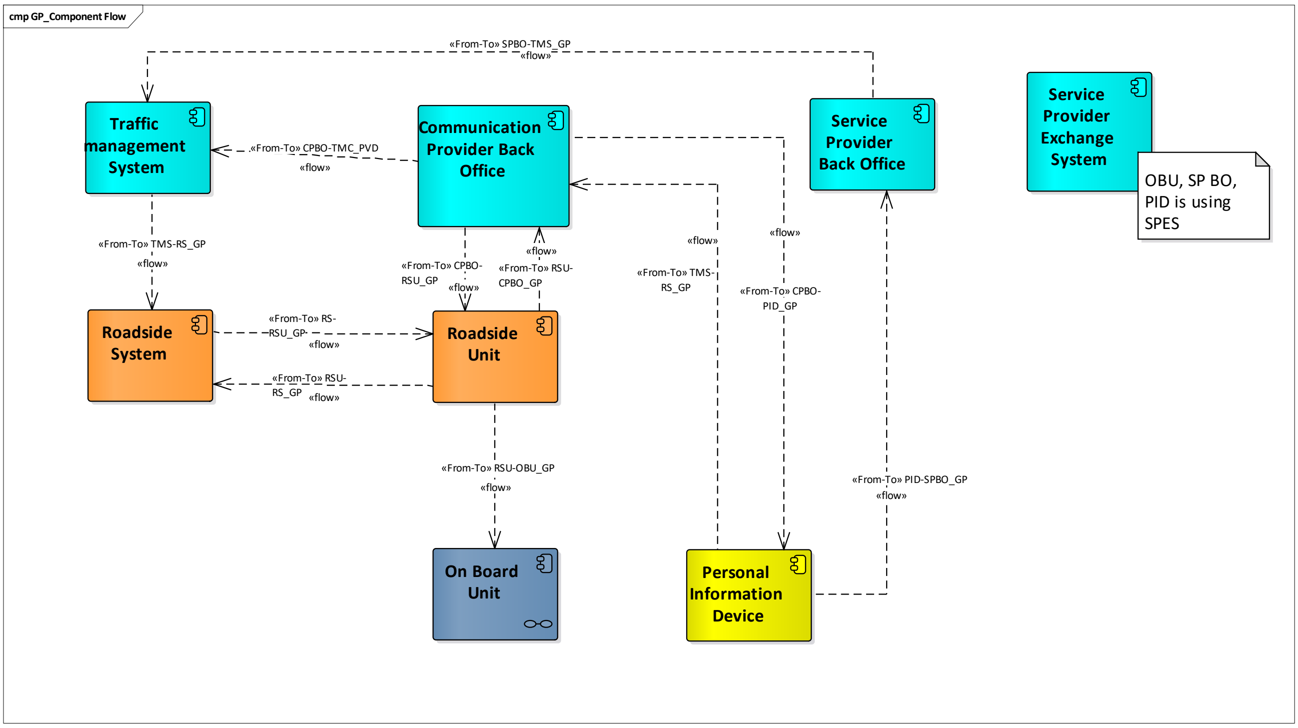


Figure 151: Green Priority – Components and communication flows

The sequence diagram in Appendix A describes the communication flow in more detail. This diagram gives a good summary. In this case the information flow starts at the vehicle, either by the **PID**, in case of the connected solution, or by the **OBU** for the 802.11p communication. For the connected communication, messages go through the **CPBO** in order to forward them to the relevant **RSUs**, for the **OBU** the range of the antenna ensures that information only arrives at relevant **RSUs**. The **RSU** then evaluates whether the priority request should be granted or not, this is based on the information supplied and the validity of PKI certificates. There is also a path back to the vehicle, this gives feedback about the status of the priority. This is again either directly to the **OBU** or through the **CPBO** to the **PID**.

The **Service Provider Back Office** arranges the authorizations and contracts on the background. However, this is not a continuous information flow and only serves for initialization. The GeoMessaging pseudonymous login is also a sequence where the **SPBO** is involved. Another actor involved in the background is the **Traffic Management System**, this system configures the level of priority and can be involved in the authorization process. Lastly, the **Service Provider Exchange System** is involved in increasing the visibility of the service to attract more consumers and to provide PKI.

For 802.11p there is also an upward information flow when either **OBUs** or **RSUs** detect a local road hazard, it can be pushed directly into the **CPBO** for further dissemination to **PIDs** without connection to an 802.11p **OBU**.

Table 23: Green Priority - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
RSU-RS_GP	RSU	RS	local	local	any	Generic Access	any	any	iVERA, RSMP+, etc.
SPBO-CPBO_RHW	RS	RSU	local	local	any	Generic Access	any	any	iVERA, RSMP+, etc.
CPBO-PID_GP	CPBO	PID	-	ETSI ITS SSM, ETSI ITS SPaT, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
PID-CPBO_GP	PID	CPBO	-	ETSI ITS SRM, ETSI ITS CAM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-RSU_GP	CPBO	RSU	-	SRM, ETSI ITS CAM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-CPBO_GP	RSU	CPBO	-	SSM, ETSI ITS SPaT, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-OBU_GP	RSU	OBU	-	SSM, ETSI ITS SPaT	GeoNetworking	ETSI ITS-G5	GeoNetworking	ETSI ITS-S Security Architecture	Not defined yet
OBU-RSU_GP	OBU	RSU	-	SRM, ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	GeoNetworking	ETSI ITS-S Security Architecture	Not defined yet
SPBO-TMS_GP	SPBO	TMS	HTTPS	JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contain alternatives, e.g. IPv4 or IPv6. It should be noted that the RS is out of scope of C-MobILE with many national standards available at this level. Implementing a different standard on the traffic light controller would be very costly. This is therefore labeled as “local” to indicate that deployment sites can have different protocols here. It should also be noted that there is no application layer protocol involved, except possibly at the RS, standardization at the facility layer ensures interoperability.

5.2.10. GLOSA

GLOSA provides vehicle drivers an optimal speed advice when they approach a controlled intersection equipped with traffic lights.

The "Green Light Optimal Speed Advisory (GLOSA)" service aims at creating an eco-friendlier and energy-efficient driving experience for vehicle drivers by providing speed advice, traffic light information and countdown to green/red, aiming to reduce energy consumption and lower the number of stops. [74]

5.2.10.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 152.

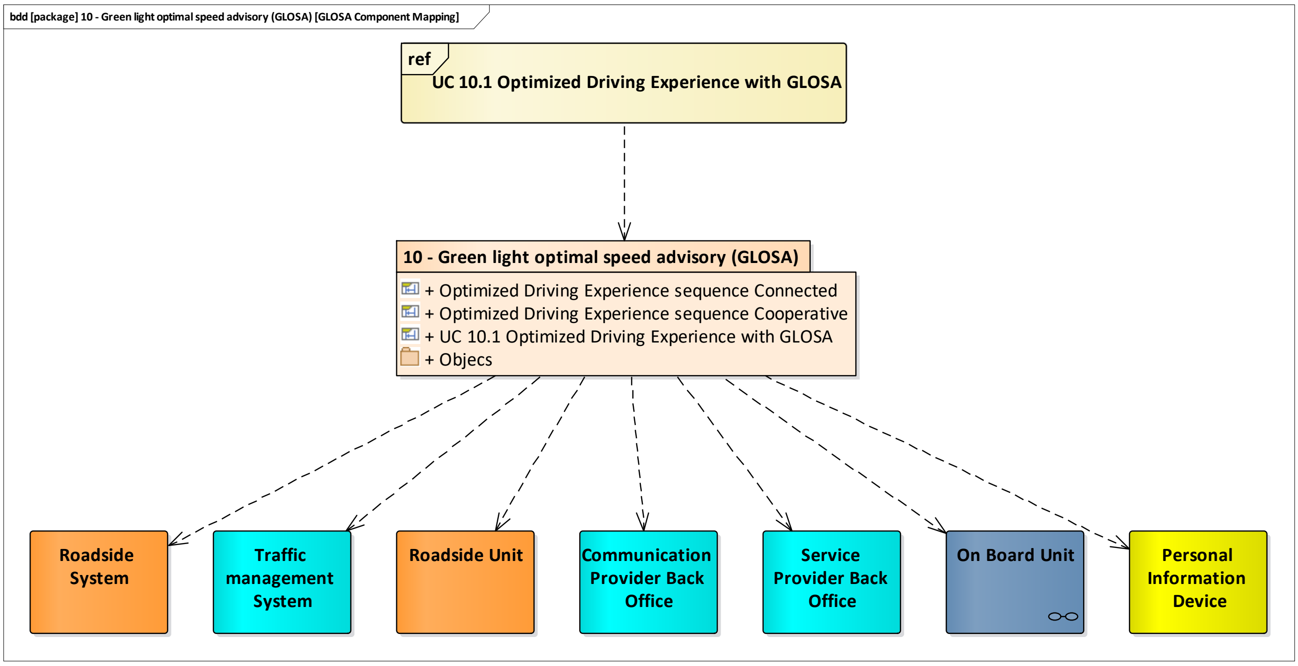


Figure 152: GLOSA - Components involved in service

To implement this service, the following components are necessary.

- Roadside System (see section 4.2.3.2.1 for details.)
- Traffic Management System (See section 4.2.2.2.5 for details)
- Roadside Unit (see section 4.2.3.2.2 for details)
- Communication Provider Back Office (see section 4.2.2.2.1 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components is described in the section 5.2.10.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- "UC 10.1 Optimized Driving Experience with GLSOA" as shown in Appendix A

5.2.10.2. Component Connections

The following section describes the relations between the several components. In Figure 153 all the involved components and the connections between them are listed for all use cases of the service.

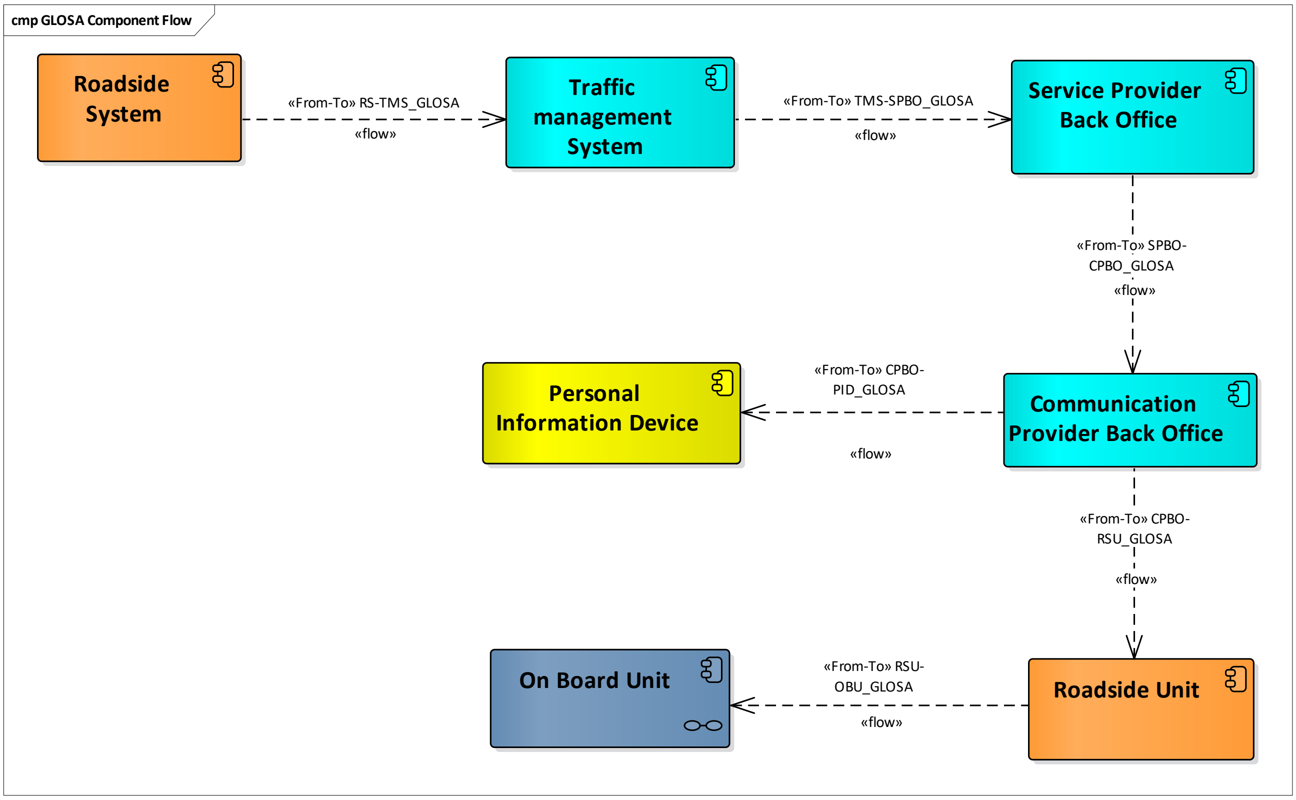


Figure 153: GLOSA – Components and communication flows

The **Roadside System (RS)** uses **RS-TMS_GLOSA** connection to broadcast the signal states and the time for the next signal to the **Traffic Management System (TMS)** that is forward to the **Service Provider Back Office (SPBO)** via the **TMS-SPBO_GLOSA** connection. The **SPBO** calculates optimal speed profiles for different locations and transmits the speed profiles to the **Communication Provider Back Office (CPBO)** via the **SPBO-CPBO_GLOSA** connection. According to the HMI selected, there are two flows. If the **Personal Identification Device (PID)** is used for the service, the **CPBO** uses the **CPBO-PID_GLOSA** connection to transmit the optimal speed profiles and the **PID** will calculate the speed advice and display it to the user. If the **On Board Unit (OBU)** is used for the service, the **CPBO** uses the **CPBO-RSU_GLOSA** connection to transmit the optimal speed profiles to the **Roadside Unit (RSU)**, which in turn forwards the speed profiles to the **OBU** via the **RSU-OBU_GLOSA** connection. At the **OBU**, the speed advice is calculated and displayed to the user.

Table 24: Green Light Optimal Speed Advisory - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
RS-TMS_GLOSA	RS	TMS	-	ETSI ITS SPATEM	IPv6, IPv4, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Figure 211
TMS-SPBO_GLOSA	TMS	SPBO	DATEX II	TBD	IPv6, IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_GLOSA	SPBO	CPBO	-	ETSI ITS CAM, MQTT	IPv6, IPv4, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-PID_GLOSA	CPBO	PID	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-RSU_GLOSA	CPBO	RSU	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Figure 212
RSU-OBU_GLOSA	RSU	OBU	-	ETSI ITS SPATEM/MAPEM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 213

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.11. Cooperative traffic light for pedestrian

An Employer (an organization, or a business/industrial zone) endorses cycling as the choice of commuting for its employees. This is with the aim to reduce the traffic around and within its premises, and reduce the need for parking spaces for cars. To foster this, a Service Provider offers a priority crossing for cyclists via a smartphone application. The Provider delivers software activation codes to the Employer, which distributes to its Employees that commute by bike.

The service should be available to all, however user recruitment will be done by approaching large employers, educational institutions, and certain groups of more-vulnerable VRUs, all of which may be able to further benefit by making this service available to their members.

The operation of the service will vary based on VRU-demand and traffic conditions for other phases. Operation during peak hour, for instance, may only adjust signal timing when large numbers of pedestrians are waiting, whilst during non-peak, the service could be used to provide priority for only a small number of VRUs.

The service could optionally be activated only during certain time periods (e.g., rush hours).

This use case is differentiating from Use Case 2 as it only operates based on detection of (self-)selected VRUs using active sensor technology.

“Traffic Light Prioritisation for Designated VRUs (Vulnerable Road Users)” aims at increasing comfort and safety of VRUs in traffic by adjusting traffic signal timing and/or assigning priority based on VRU-data collected through an app or tag carried by individual VRUs. [74]

5.2.11.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 154.

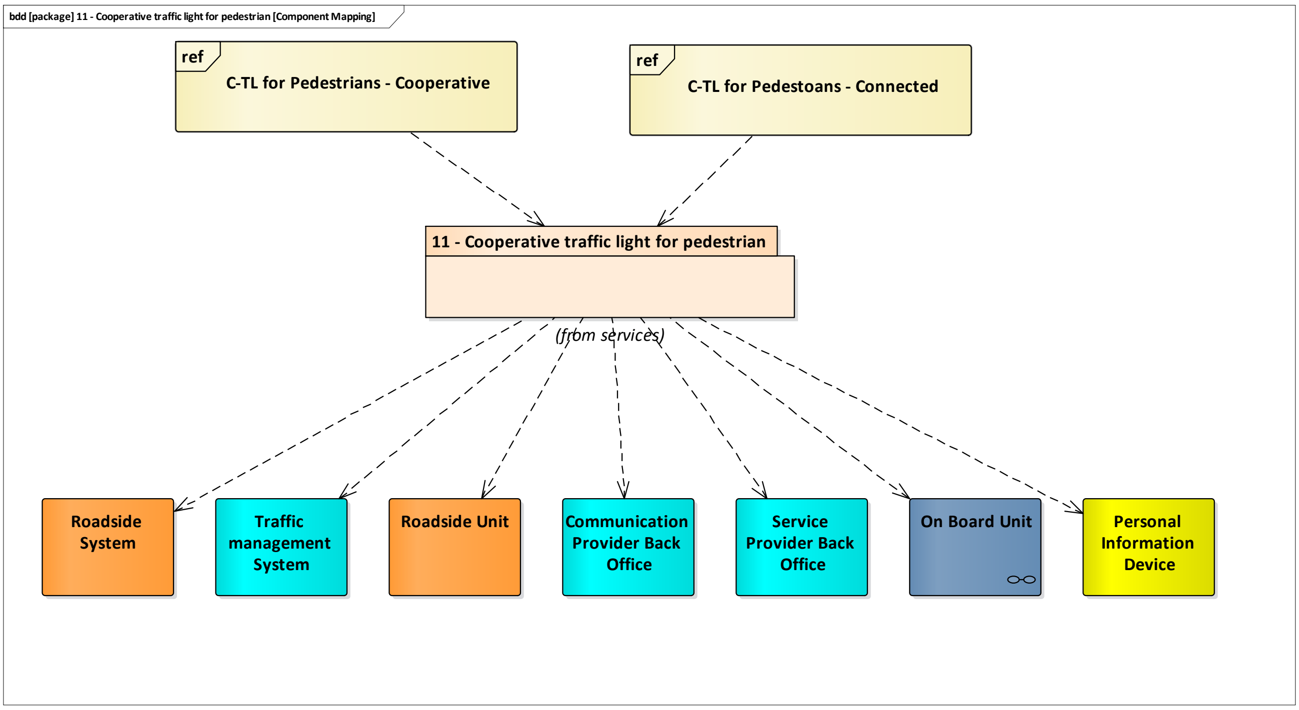


Figure 154: CTL for Pedestrians - Components involved in service

To implement this service, the following components are necessary.

- Roadside System (see section 4.2.3.2.1 for details.)
- Traffic management system (see section 4.2.2.2.5 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)

- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components is described in the section 5.2.11.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- UC11.1 “Traffic Light for Pedestrians cooperative” as shown in Appendix A
- UC11.2 “Traffic Light for Pedestrians Connected” as shown in Appendix A

5.2.11.2. Component Connections

The following section describes the relations between the several components. In Figure 155 all the involved components and the connections between them are listed for all use cases of the service.

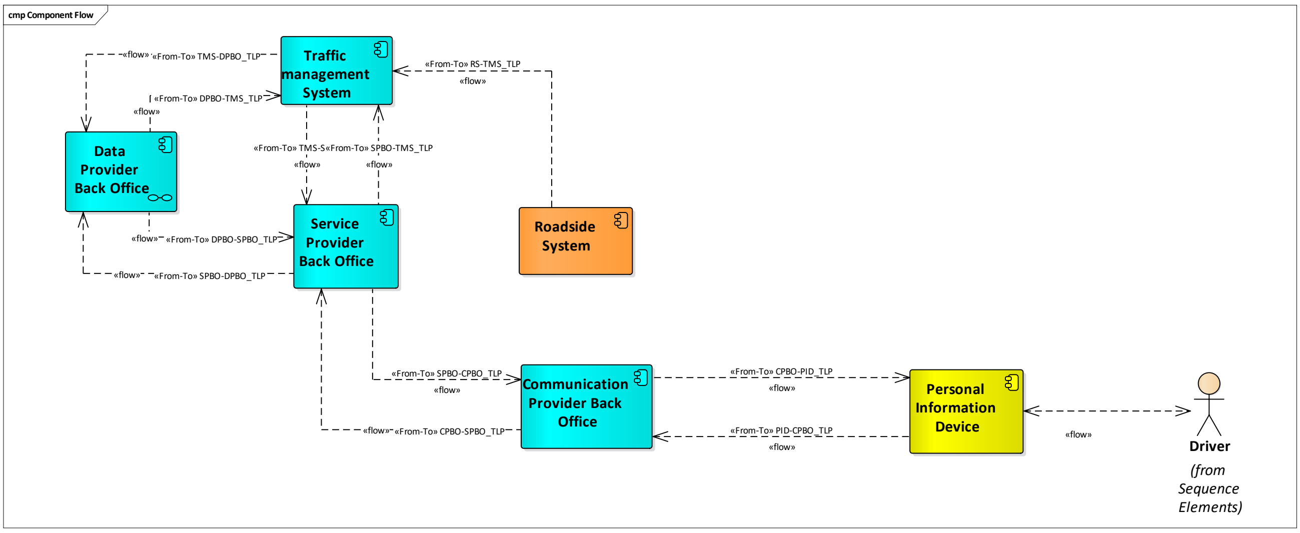


Figure 155: Cooperative Traffic Light for pedestrians – Components and communication flows

In the defined use cases the Traffic Management System (TMS) uses the Back-Office Communication Provider (CP-BO) relationship to provide information to the Service Provider in order to provide the information to the vehicle communication system. The information shared to the VCS is obtained via the VRU sensor and pushed to the Traffic Signal controller. The road side unit is able to handle Spat/Map and CAM messages in order to obtain and provide information the VIS: on-board unit.

Table 25: Cooperative traffic light for pedestrian - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
TMS-SPBO_TLP	TMS	CPBO	HTTPS	JSON	IPv4, IPv6, TCP			TLS	Not defined yet
SPBO-TMS_TLP	SPBO	TMS	HTTPS	JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_TLP	SPBO	CPBO	TBD	JSON, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
CPBOCPBO-PID_TLP	CPBO	PID	TBD	JSON, MQTT	GeoNetworking	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS	Not defined yet
RS-TMS_TLP	RS	TMS	HTTPS	JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
TMS-DPBO_TLP	TMS	DPBO	DATEX II	-	IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
DPBO-TMS_TLP	DBPO	TMS							
DPBO-SPBO_TLP	DPBO	SPBO	HTTP, DATEX,	XML, JSON	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G SuiteGeneric Access	SNMP	TLS	Not defined yet
SPBO-DPBO_TLP	SPBO	DPBO		AMQP	IPv4, IPv6, TCP	Generic Access			
PID-CPBO_TLP	PID	CPBO				3GPP 4G Suite, 3GPP 3G Suite			
CPBO-SPBO_TLP	CPBO	SPBO			IPv4, IPv6, TCP				

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.12. Flexible infrastructure

Flexible infrastructure aims to interchange information about the lanes provided to the traffic users according to the time of the day. It includes solutions such as reserved lane.

Objectives of FI are informing traffic users about the lanes provided downstream of the current position and in the driving direction of the vehicle. [74]

5.2.12.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 156.

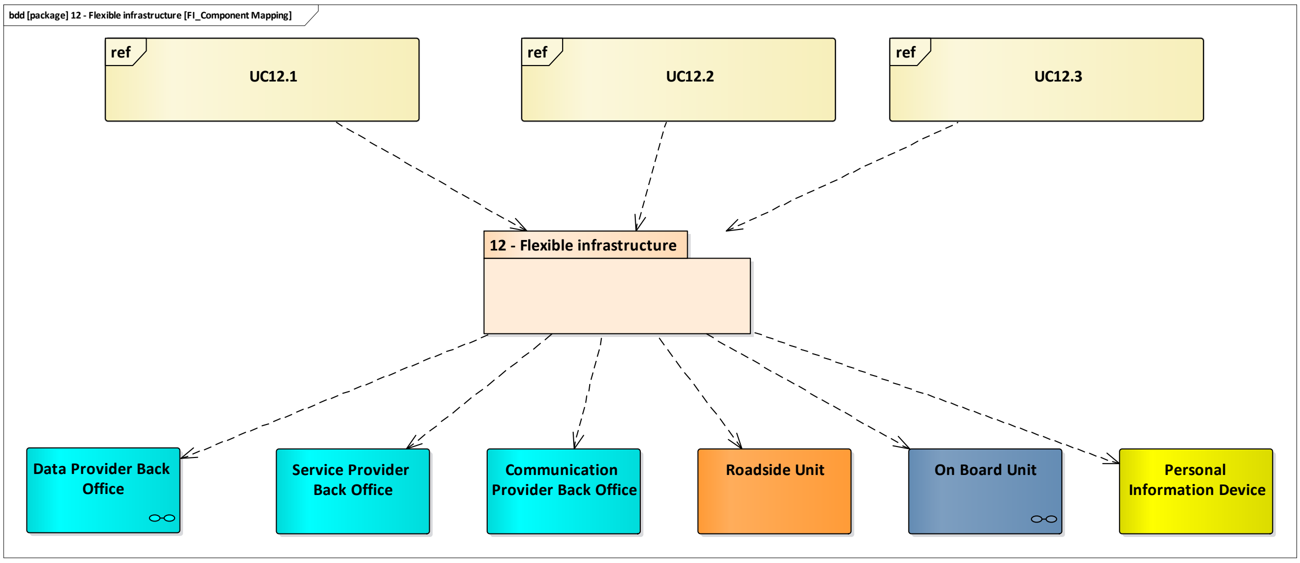


Figure 156:Flexible Infrastructure - Components involved in service

To implement this service, the following components are necessary.

- Data Provider Back Office (see section 4.2.2.2.4 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components is described in the section 5.2.12.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- 12.1 - Dynamic Lane Management – Lane Status Information as shown in Appendix A
- 12.2 - Dynamic Lane Management – Reserved Lane (with probe vehicle data) as shown in Appendix A
- 12.3 - Dynamic Lane Management – Reserved Lane (without probe vehicle data) as shown in Appendix A

5.2.12.2. Component Connections

The following section describes the relations between the several components. In Figure 157 all the involved components and the connections between them are listed for all use cases of the service.

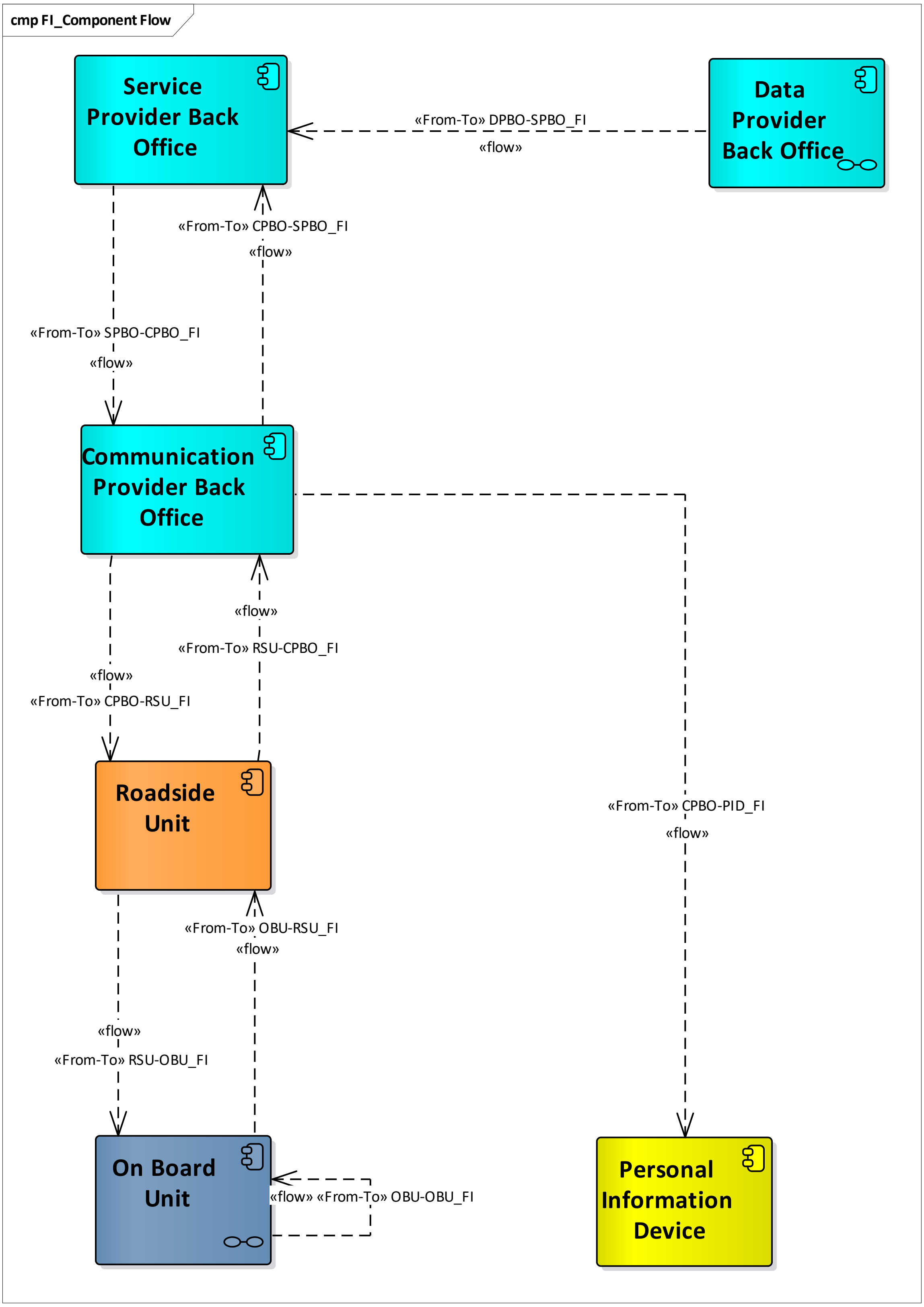


Figure 157: Flexible Infrastructure– Components and communication flows

The **Service Provider Back Office (SPBO)** receives information about the lane status from the **Data Provider Back Office (DPBO)** through the **DPBO-SPBO_FI** relation. This information is distributed to the **Roadside Unit (RSU)** through the **Communication Provider Back Office (CPBO)** by using the **SPBO-CPBO-FI** and **CPBO-RSU_FI** connection.

The **RSU** sends a **MAPEM** to the **On Board Unit (OBU)** to inform the driver about the lane status. This information is distributed by the Vehicle to other Vehicles by the **OBU-OBU_FI** connection. For Cellular case (more detailed in Figure 217) the **SPBO** is providing the lane status to a **Personal Information Device (PID)** through the **CPBO** to the **PID** using **CPBO-PID_FI** relation. Therefore, the **PID** has to register itself at the **CPBO**.

In case that probe vehicle data are used (Figure 216) **OBUs** sharing their information with the **SPBO** through using the RSU and CPBO to reach SPBO. That means the **OBU** uses the **OBU-RSU_FI** to send probe vehicle data to the **RSU** which need to aggregate this data before it forward this information through the **RSU-CPBO_FI** connections to the **SPBO** using **CPBO-SPBO_FI**.

Table 26: Flexible Infrastructure - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
DPBO-SPBO_FI	DPBO	SPBO	DATEX II	TBD	IPv6, IPv4, TCP	Generic Access	SNMPv3 MIB	TLS	Not defined yet
SPBO-CPBO_FI	SPBO	CPBO	TBD	MQTT, ETSI ITS MAPEM	IPv4, IPv6, TCP	Generic Access	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-RSU_FI	CPBO	RSU	TBD	MQTT, ETSI ITS MAPEM	IPv4, IPv6, TCP	Generic Access, 3GPP 4G Suite, 3GPP 3G Suite	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-OBU-FI	RSU	OBU	TBD	ETSI ITS MAPEM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Not defined yet
OBU-OBU_FI	OBU	OBU	TBD	ETSI ITS MAPEM	GeoNetworking	ETSI ITS-G5	TPEG2-MMC ISO 21219-6	ETSI ITS-S Security Architecture	Not defined yet
OBU-RSU_FI	OBU	RSU	TBD	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Not defined yet
RSU-CPBO_FI	RSU	CPBO	TBD	MQTT, ETSI ITS MAPEM	IPv4, IPv6, TCP	Generic Access, 3GPP 4G Suite, 3GPP 3G Suite	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-SPBO_FI	CPBO	SPBO	TBD	MQTT, ETSI ITS CAM	IPv4, IPv6, TCP	Generic Access	SNMPv3 MIB	TLS	Not defined yet
SPBO-PID_FI	CPBO	PID	TBD	ETSI ITS MAPEM, MQTT	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.13. In–vehicle signage

In-Vehicle Signage (IVS) shows both static and dynamic information of road signs inside the vehicle.

In scope of IVS. the IVS information is retrieved by means of Infrastructure-to-Vehicle (I2V) communication. IVS shows both static and dynamic information of road signs.

The service contains actual and continuous information on [74]:

- Speed limits: in-vehicle information on actual speed limit
  - Standard speed limit (incl. time-of-the-day windows)
  - Dynamic speed limit during incidents, traffic jams, etc.
  - Adjusted speed limits during road works
- Overtaking prohibition: in-car information on actual overtaking prohibition, especially for trucks
- Actual travel times and other traffic information.

5.2.13.1. Involved Components

This section shows which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 140.

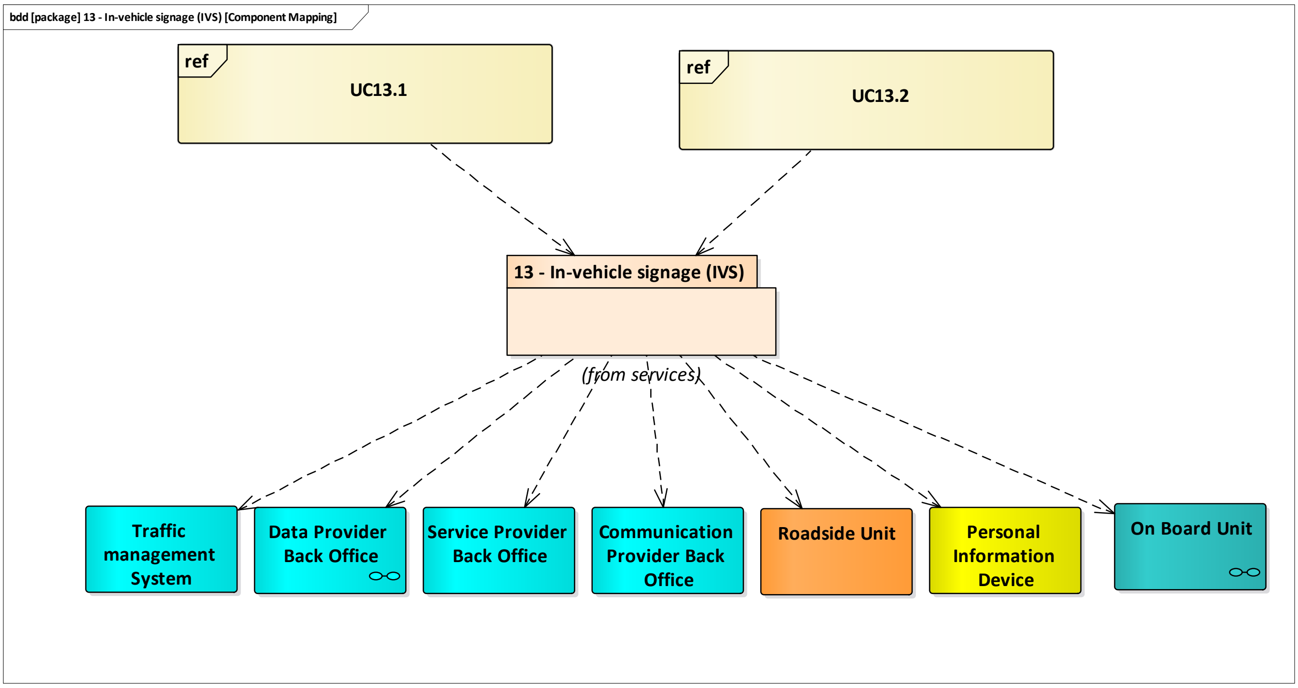


Figure 158: IVS service's component mapping diagram

This service comprises two use cases which share the same architecture and can be implemented with both communication protocols (cooperative and connected). Therefore, different architecture components are involved in each one. In general, in order to implement this service, the following components are necessary:

- Traffic management system (see section 4.2.2.2.5 for details.)
- Data Provider Back Office (see section 4.2.2.2.4 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)

/ Roadside Unit (see section 4.2.3.2.2 for details.)

/ Personal Information Device (See section 4.2.5.2.1 for details)

/ On Board Unit (see section 4.2.4.2.1 for details.)

The relations among those components are described in the section Component Connections, below. The general functionality of this service, as well as more detailed interactions of the involved components are further described in UML Sequence Diagrams for the unique use-case on which this service is based:

/ UC13.1 “In-Vehicle Signage, dynamic traffic signs”

/ UC13.2 “In-Vehicle Signage, static traffic signs”

5.2.13.2. Component Connections

The following section describes the relations between the components. In Figure 141 all the involved components and the connections among them are listed for all use cases of the service.

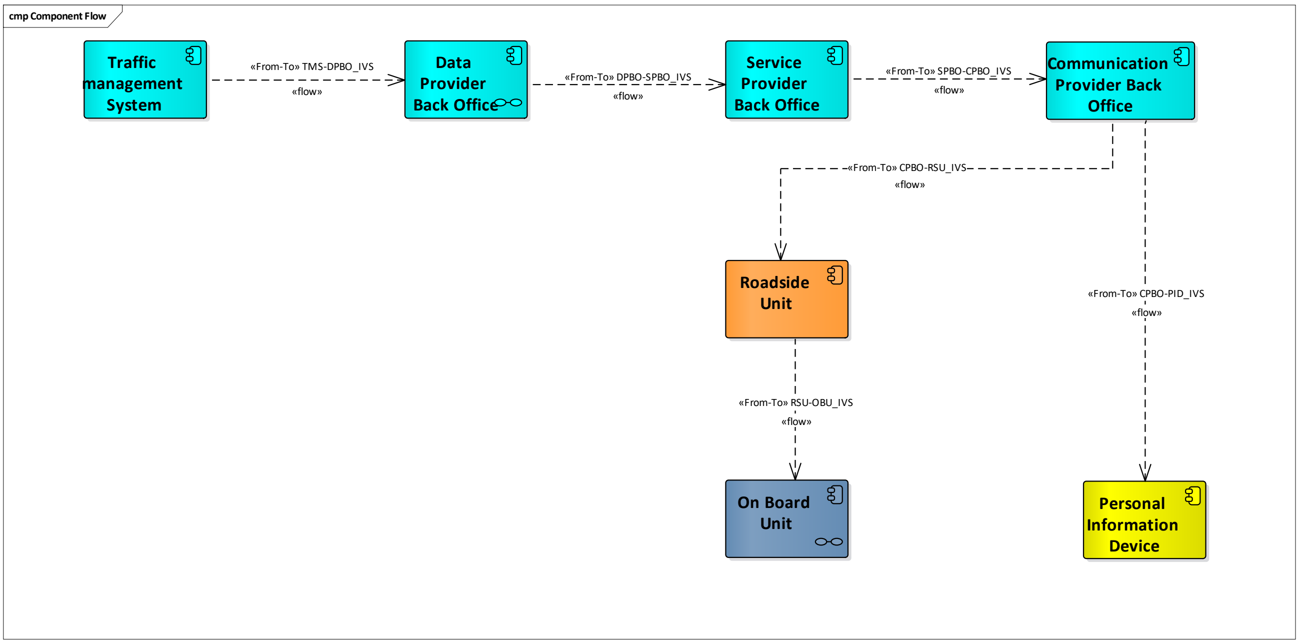


Figure 159: IVS service's components and communication flows

The component flow diagram comprises the relation among the blocks of the architecture for both communication mechanisms at the same time.

The use cases start with dynamic/static traffic signs information sent from the TMC to the **DPBO** (or, alternatively, directly to the SPBO) using the **TMS-DPBO_IVS** connection. In order to disseminate the traffic signs information, the GeoMessaging is used, therefore the **Communication Provider Back Office (CPBO)** receives the data from the **SPBO** and proceeds with the dissemination to the cooperative vehicles using the **CPBO-RSU_IVS** connection and to the connected vehicles using the **CPBO-PID_IVS** connection.

The appropriate **RSU** (covering the desired dissemination region) receives the information to be broadcasted to the cooperative vehicles using the **RSU-OBU_IVS** connection with ITS G5 communications.

Table 27: IVS Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
TMS-DPBO_IVS	TMS	DP BO	HTTPS	DATEX, JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
DPBO-SPBO_IVS	DP BO	SP BO	HTTPS	DATEX, JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_IVS	SP BO	CP BO	-	MQTT, ETSI ITS IVIM	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-RSU_IVS	CP BO	RSU	-	MQTT, ETSI ITS IVIM	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-OBU_IVS	RSU	OBU	ETSI ITS BSA	ETSI ITS IVIM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Not defined yet
CPBO-PID_IVS	CP BO	PID	ETSI ITS BSA	ETSI ITS IVIM	GeoNetworking	ETSI ITS-G5	TBD	ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols is listed in Will futher described in WP 5.

Appendix B.

The protocol layers used follow the protocol stack as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.14. Mode & trip time advice

Mode & trip time advice (e.g. by incentives) aims to provide a traveller with an itinerary for a multimodal passenger transport journey, taking into account real-time and/ or static multimodal journey information. It gives advice to its users with regards to the mode of transport, the most efficient route whilst travelling as well as the expected travel time based on floating car data (or other multi-source traffic conditions estimation technologies), allowing users to optimize their travel experience.

Mode and trip time advice aims to create an eco-friendlier, energy-efficient and more comfortable driving or travelling experience. [74]

5.2.14.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 160.

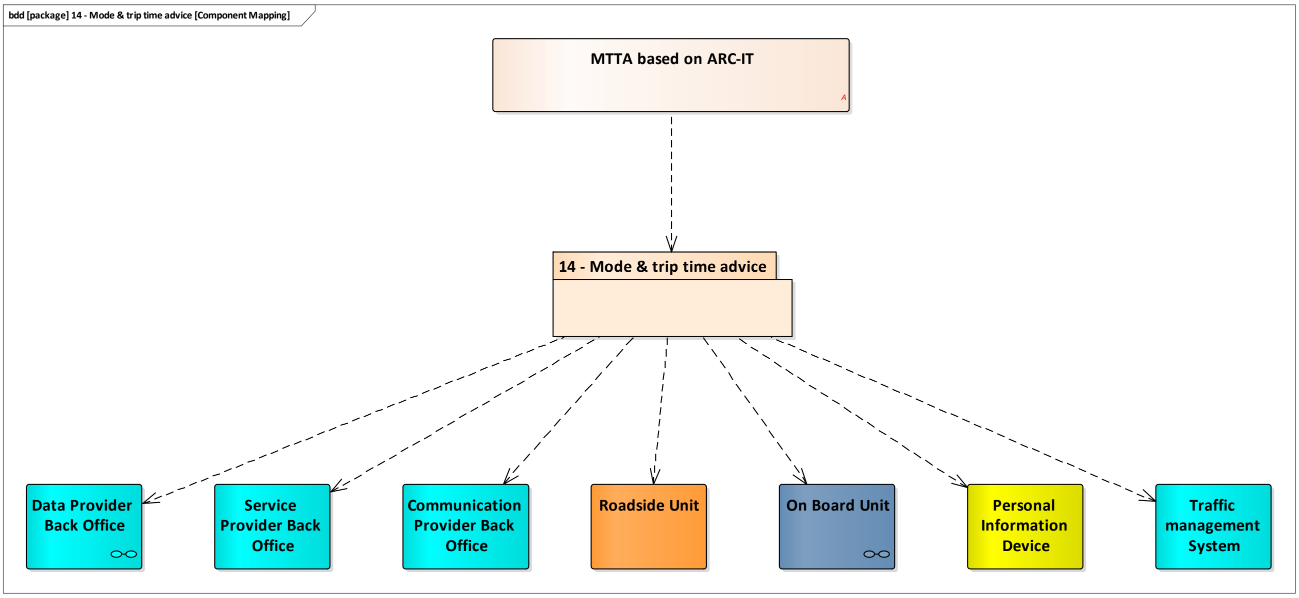


Figure 160: Mode & trip time advice - Components involved in service

To implement this service, the following components are necessary.

- Data Provider Back Office (see section 4.2.2.2.4 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Roadside Unit, optional required for 802.11p communication only (see section 4.2.3.2.2 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)
- Traffic management system (see section 4.2.2.2.5 for details.)

The relations between those components is described in the section 5.2.14.2, below. The general functionality of this service is based on the ARC-IT reference architecture. Therefore an adapted Version for C-MobILE was created and can be found in Appendix A.

5.2.14.2. Component Connections

The following section describes the relations between the several components. In Figure 161 all the involved components and the connections between them are listed for all use cases of the service.

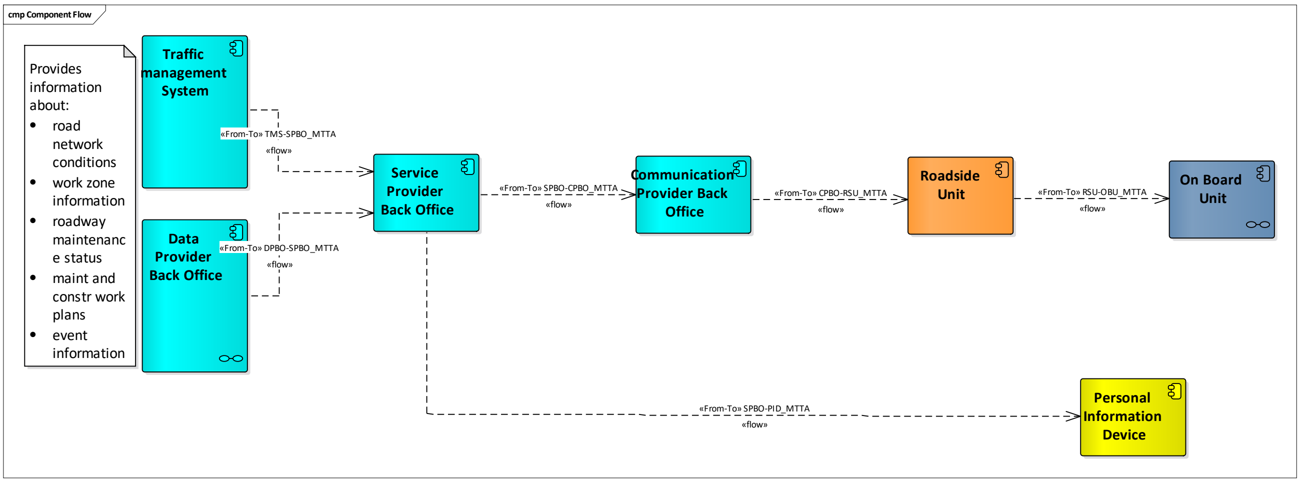


Figure 161: Mode & trip time advice – Components and communication flows

The **Service Provider (SPBO)** receiving information about e.g. the road network from the **Traffic Management System** and information about an upcoming event from the **Data Provider Back Office** which acts as a third party data provider. That information gets used by the **SPBO** to calculate the optimal route for the user. The information gets exchanged through the **TMS-SPBO_MTTA** and **DPBO-SPBO_MTTA** connection.

The **SPBO** sends the routing information to the **Communication Provider Back Office** using the **SPBO-CPBO_MTTA** relation which provides the information to the **RSU** by the **CPBO-RSU_MTTA** connection. The **RSU** will then forward the information to the **OBUs** using **RSU-OBU_MTTA** relation.

If the end user uses the **Personal Information Device (PID)** then the **SPBO** is directly providing the routing information through the **SPBO-PID_MTTA** relation.

Table 28: Mode & trip time advice - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
CPBO-RSU_MTTA	CPBO	RSU	TBD	MQTT, ETSI ITS DENM	IPv4, IPv6, TCP	Generic Access	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet
DPBO-SPBO_MTTA	DPBO	SPBO	TBD	AMQP	IPv6, IPv4, TCP	Generic Access	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-OBU_MTTA	RSU	OBU	TBD	TBD	IPv6, TCP, UDP	ETSI ITS-G5	SNMPv3 MIB	TLS, IETF RFC 6071	Not defined yet
SPBO-CPBO_MTTA	SPBO	CPBO	TBD	TBD	IPv6, IPv4, TCP	Generic Access	SNMPv3 MIB	TLS,	Not defined yet
SPBO-PID_MTTA	SPBO	PID	TBD	TBD	IPv4, IPv6, TCP, UDP	3GPP 3G Suite, 3GPP 4G Suite	SNMPv3 MIB	TLS, IETF RFC 6071	Not defined yet
TMS-SPBO_MTTA	TMS	SPBO	TBD	AMQP	IPv6, IPv4, TCP	Generic Access	SNMPv3 MIB	TLS	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.15. Probe Vehicle Data

Probe Vehicle Data is data generated by vehicles. The collected traffic data can be used as input for operational traffic management (e.g., to determine the traffic speed, manage traffic flows by - for instance- alerting users in hot spots, where the danger of accidents accumulates), long term tactical/strategic purposes (e.g. road maintenance planning) and for traveller information services. Also known as Floating Car Data (FCD).

This service aims to collect data about traffic conditions, road surface conditions and the surroundings. [74]

5.2.15.1. Involved Components

5.2.15.2. Involved Components

This section shows which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 140.

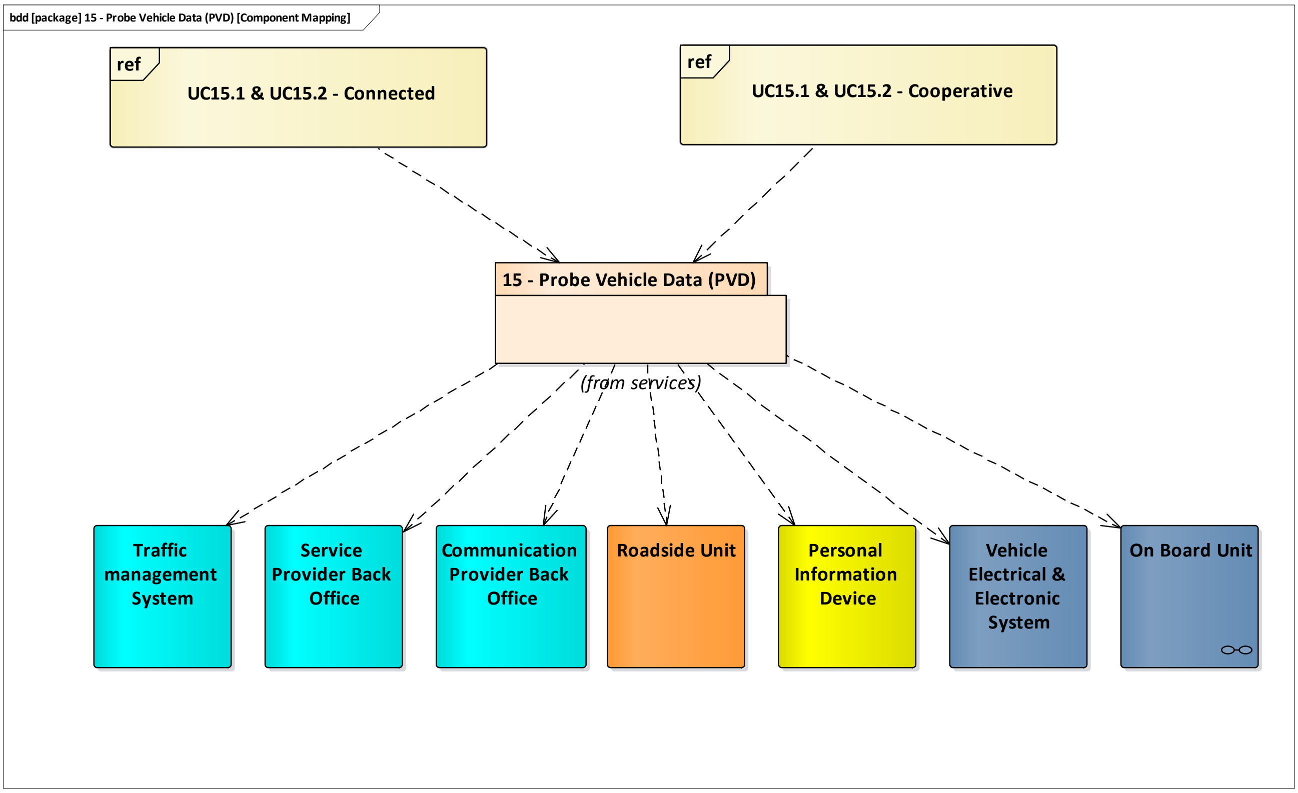


Figure 162: PVD service's component mapping diagram

This service comprises two use cases which share the same architecture and can be implemented with both communication protocols (cooperative and connected). Therefore, different architecture components are involved in each one. In general, in order to implement this service, the following components are necessary:

- Traffic management system (see section 4.2.2.2.5 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- Personal Information Device (See section 4.2.5.2.1 for details)
- Vehicle Electrical & Electronic system, (see section 4.2.4.2.2 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)

The relations among those components are described in the section Component Connections, below. The general functionality of this service, as well as more detailed interactions of the involved components are further described in UML Sequence Diagrams for the unique use-case on which this service is based:

/ UC15.1 “Basic probe vehicle data”

/ UC15.2 “Extended probe vehicle data”

5.2.15.3. Component Connections

The following section describes the relations between the components. In Figure 141 all the involved components and the connections among them are listed for all use cases of the service.

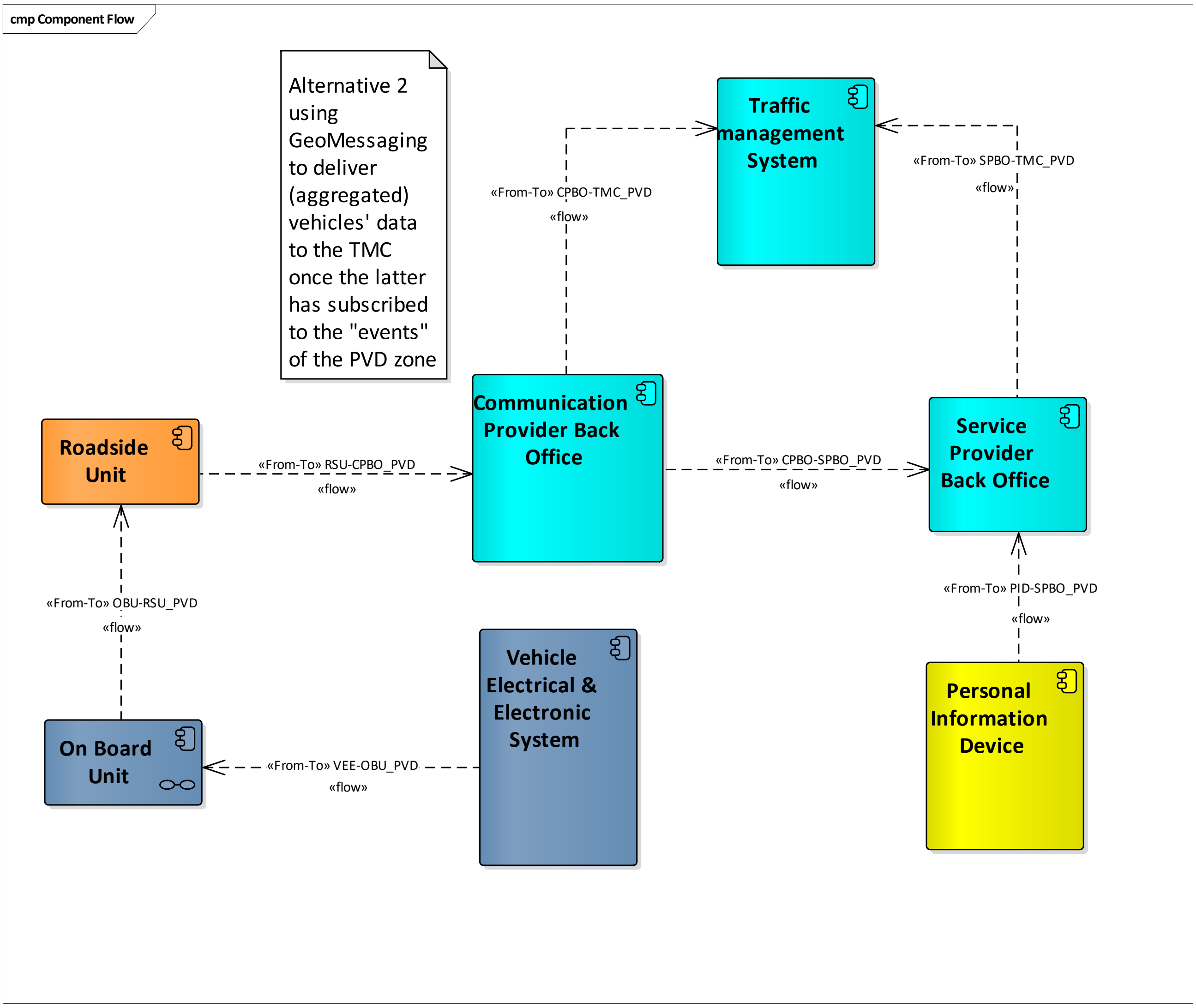


Figure 163: PVD service's components and communication flows

The component flow diagram comprises the relation among the blocks of the architecture for both communication mechanisms at the same time.

The probe vehicle data’s main target is the TMS, where this information is processed and used to detect and improve the transport network (i.e. offering appropriate Flexible Infrastructure, Road Hazard Warning and/or other services).

In the cooperative communication, the **Vehicle Electrical & Electronic** (VEE) system (GPS, sensors, cameras, etc.) gathers information about the vehicle and its surroundings constantly and delivers it to the **OBU** using the **VEE-OBU_PVD** connection. The communication protocol using in this connection is out of scope of C-MobILE. The **OBU** is in charge of building the appropriate message and transfer it to the **RSU** via ITS G5 and then, the **RSU** sends this probe data to the **Communication Provider Back Office (CP BO)**. Depending on the DS, the **SPBO** or the **TMS** can be the receiver of the data in the **CPBO**. If the data needs further processing and formatting before reaching the TMS, the **SPBO** can be subscribed to the GeoMessaging PVD service in order to receive, treat and forward the data to the **TMS**. Otherwise, the **TMS** is the one that needs to be subscribed to the GEOM PVD in order to receive the data directly form the **CPBO**.

In the connected communication approach, the information is generated in the **PID** (out of scope of C-MobILE) and transmitted to the **SPBO** using a cellular communication. Then, the information follows the same flow an in the cooperative communication, where it can be directly delivered to the **TMS** or indirectly passing through the **CPBO** with a previous GEOM subscription.

The data can be aggregated at multiple levels; in the vehicle, in the roadside equipment and/or in the back office. An early aggregation is preferred , as this helps to ensure the privacy of the drivers.

Table 29: Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
VEE-OBU_PVD	VEE	OBU							
OBU-RSU_PVD	OBU	RSU	ETSI ITS BSA	ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	TBD	TBD	Not defined yet
RSU-CPBO_PVD	RSU	CP BO	-	(Aggregated) ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM*, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-SPBO_PVD	CP BO	SP BO	-	(Aggregated) ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM*, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-TMS_PVD	CP BO	TMS	HTTPS	(Aggregated) ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM*	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
SPBO-TMS_PVD	SP BO	TMS	HTTPS	(Aggregated) ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM*	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
PID-SPBO_PVD	PID	SP BO	HTTPS	(Aggregated) ProbeVehicleData_Msg (SAE J2735), ETSI ITS CAM*	IPv4, IPv6, TCP	3GPP 4G Suite, 3GPP 3G Suite	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet

** Sending of unagregated CAM/PVD messages in the back end is not recommended, as this reduces the privacy of the users. An appropriate container format needs to be defined. For SAE PVD privacy could be enhanced if the optional VehicleData container is not used; however, it needs to be evaluated how big the privacy gains would be.*

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols is listed in Will futher described in WP 5.

Appendix B.

The protocol layers used follow the protocol stack as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.16. Emergency Brake Light

Emergency Brake Light aims to avoid (fatal) rear end collisions, which can occur if a vehicle ahead suddenly brakes, especially in dense driving situations or in situations with decreased visibility. The driver is warned before s/he is able to realize that the vehicle ahead is braking hard, especially if s/he does not see the vehicle directly (vehicles in between).

This service addresses the situation that occurs when any vehicle abruptly slows down, it switches on emergency electronic brake lights. The service warns the local followers, in due time, so they can adopt their speed to avoid collision with the vehicle. [74]

5.2.16.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 164.

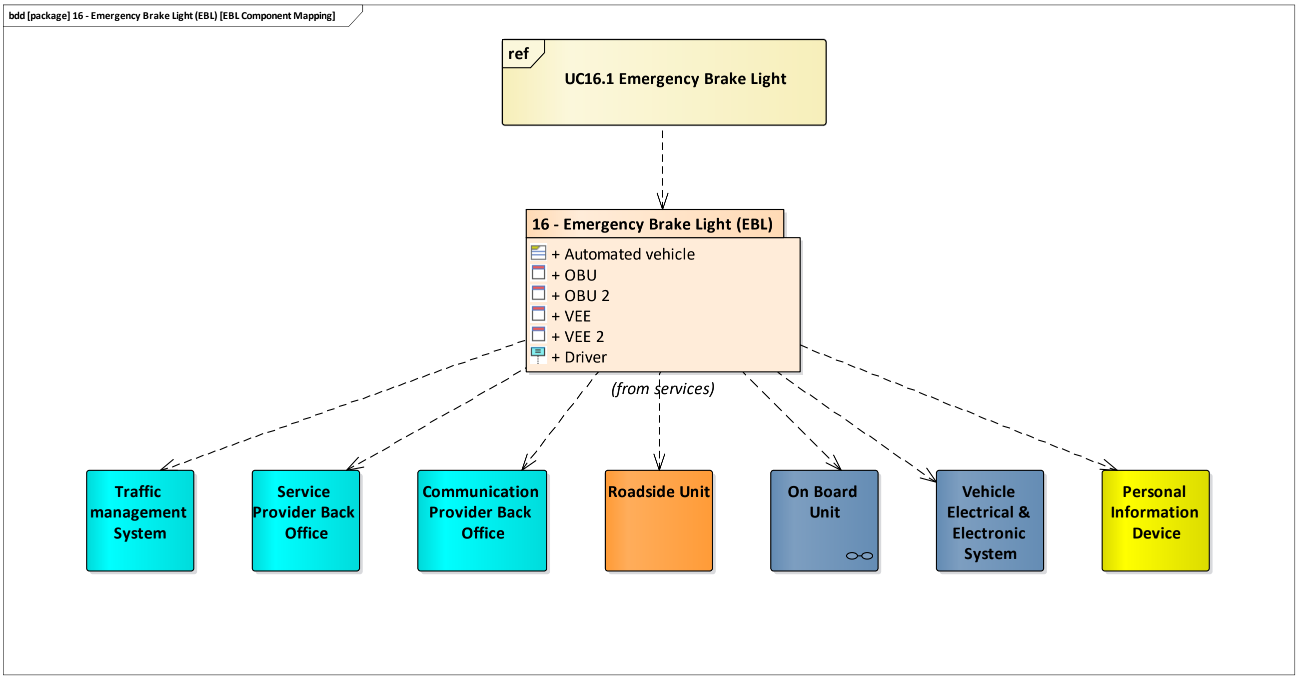


Figure 164: EBL - Components involved in service

To implement this service, the following components are necessary.

- Traffic Management System, for EBL the data is collected at the TMC following the path RSU-> CPBO -> SPBO -> TMC (See section 4.2.2.2.5 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Communication Provider Back Office, for EBL this is the gateway to share the local traffic information to interested Service Providers Back Office/TMC. (See section 4.2.2.2.1 for details)
- Roadside unit, for EBL this is optionally used for sharing local traffic awareness data to a local Traffic Management Center (TMC). (See section 4.2.3.2.2 for details.)
- On Board Unit, for EBL the minimal requirement is V2V based on ITS-G5. Extensions are V2I over ITS-G5 using local infrastructure and awareness. (See section 4.2.4.2.1 for details.)
- Vehicle Electrical & Electronic system, for EBL this is the interaction with vehicle control system, sensors and actuators. EBL can be implemented as a warning system with a notification to the driver or as automated driving function with direct vehicle control functions. And providing the information and EBL Messages to be distributed over V2V. (See section 4.2.4.2.2 for details.)
- Personal Information device, for EBL this can be a separate device, but it can also be part of another platform already on-board available like HMI or a communication/control unit. (See section 4.2.5.2.1 for details)

The relations between those components is described in the section Component Connections, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

/ UC16.1 – Emergency Brake Light: Cooperative communication

/ UML sequence diagram for basis EBL as shown in Appendix 7.1.16.1.1

/ S16: Emergency Brake Light (EBL) ARC-IT diagrams” as shown in Appendix 7.1.16.1.1

5.2.16.2. Component Connections

The following section describes the relations between the components. In Figure 165 all the involved components and the connections between them are listed for all EBL use cases.

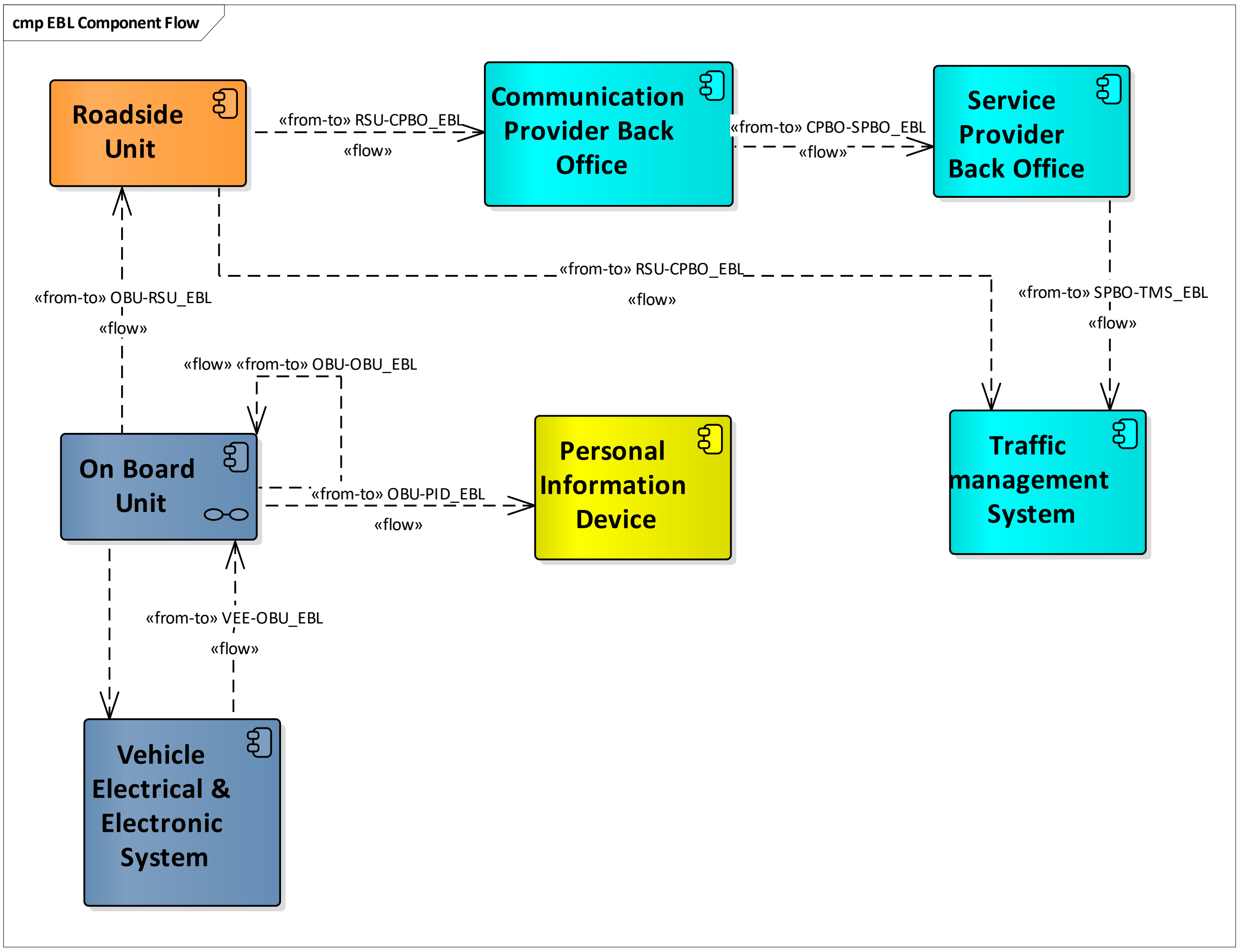


Figure 165: EBL – Components and communication flows

In the use case **UC16.1 – Emergency Brake Light**, the **On Board Unit (OBU)** uses the **OBU-OBU_EBL** relation to broadcast its EBL information needed for vehicle control warning and vehicle state information. The basic use case is based on V2V communication only in which the ego vehicle EBL application uses the information from the **Vehicle Electrical & Electronic System (VEES)** to construct the EBLC messages to be broadcasted out of the **OBU**. The EBL application is triggered based on information from **VEES**. Other vehicles receiving this EBL messages notify the driver with a warning indication on the vehicle HMI and/or **Personal Information Device (PID)**. The **PID** can also be an integrated part of the vehicle, example a touchscreen/HMI for activating/deactivating and configuring the EBL application. A more advanced implementation of EBL will be not as warning system but as ADAS function which uses the received EBL message at it **OBU** to adjust its speed or perform an emergency brake action via the **VEES** and its status is presented at the **PID.** In addition, this vehicle also transmits EBL messages so other vehicles can act upon this.

In addition, if cooperative infrastructure is available, the received EBL messages can be received with **Roadside Units (RSUs)**. This will improve local traffic awareness at **Traffic Management Systems (TMS)** for example at cooperative intersection or cooperative highway corridors. From the **RSU** the information can be forwarded to **Communication Provider Back Office (CPBO)**. The complete chain includes **CPBO** connections to **Service Provider Back Office (SPBO)**, and from this a connection to a local **Traffic Management System (TMS)** can be provided.

Table 30: EBL - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
VEE-OBU_EBL	VEES	OBU	“EBL”	CAN, propriety vehicle interface	CAN/UDP/TCP	CAN	-	-	Figure 224
OBU-VEE_EBL	OBU	VEES	“EBL”	CAN, propriety vehicle interface	CAN/UDP/TCP	CAN	-	-	Figure 225
OBU-OBU_EBL	OBU	OBU	“EBL”	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 226
OBU-RSU_EBL	OBU	RSU	“EBL”	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 227
OBU-PID_EBL	OBU	PID	“EBL”	Json, asn.1	IPv6, IPv4, UDP	Generic Access	-	TLS	Figure 228
RSU-CPBO_EBL	RSU	CP BO		Json	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Figure 229 (Optional)
CPBO-SPBO_EBL	CP BO	SP BO							(Optional, datatype like Figure 229)
SPBO-TMS	SP BO	TMS							(Optional, datatype like Figure 229)

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B. The protocol layers used here are the layers as defined by ETSI.

5.2.17. Cooperative (Adaptive) Cruise Control

The service ensures smooth driving of vehicles with enabled Cooperative Adaptive Cruise Control (CACC) function or platooning for driving through a (series of) C-ITS equipped intersection(s)

This service improves safety, comfort and traffic flow on intersections with V2I communication between CACC and intersection traffic lights (or managed intersections). [74]

5.2.17.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 164.

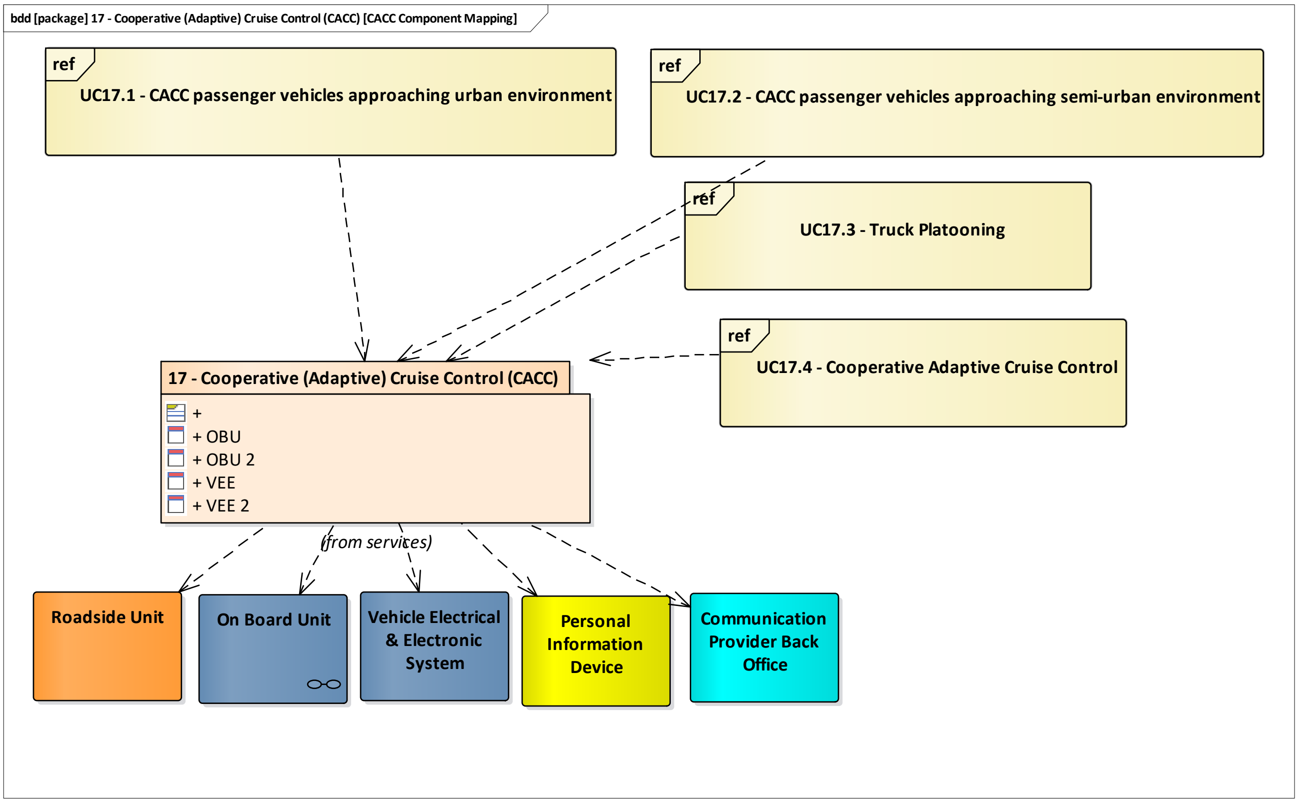


Figure 166: Urban-CACC - Components involved in service

To implement this service, the following components are necessary.

- Roadside unit, for CACC this is used for information related to traffic light information at intersections and/or “priority services”.
- On Board Unit, for CACC the minimal requirement is V2V based on ITS-G5. Extensions are V2I and I2V over ITS-G5 and/or cellular connectivity.
- Vehicle Electrical & Electronic system, for CACC this is the interaction with vehicle control system, sensors and actuators. And providing the information and CACC Messages to be distributed over V2V.
- Personal Information device, for CACC this can be a separate device, but it can also be part of another platform already on-board available like HMI or a communication/control unit.
- Communication Provider Back Office, for CACC this is used for traffic light information at intersections and/or “priority services”.

The relations between those components is described in the section Component Connections, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- / UC17.1 - CACC passenger vehicles approaching urban environment
- / UC17.2 - CACC passenger vehicles approaching semi-urban environment
- / UC17.3 - Truck Platooning
- / UC17.4 - Cooperative Adaptive Cruise Control
- / UML sequence diagram for basis CACC as shown in Appendix 7.1.16.1.1
- / S17: Cooperative Adaptive Cruise Control (CACC) ARC-IT diagrams" as shown in Appendix 7.1.16.1.1

5.2.17.2. Component Connections

The following section describes the relations between the several components. In Figure 165 all the involved components and the connections between them are listed for all CACC use cases.

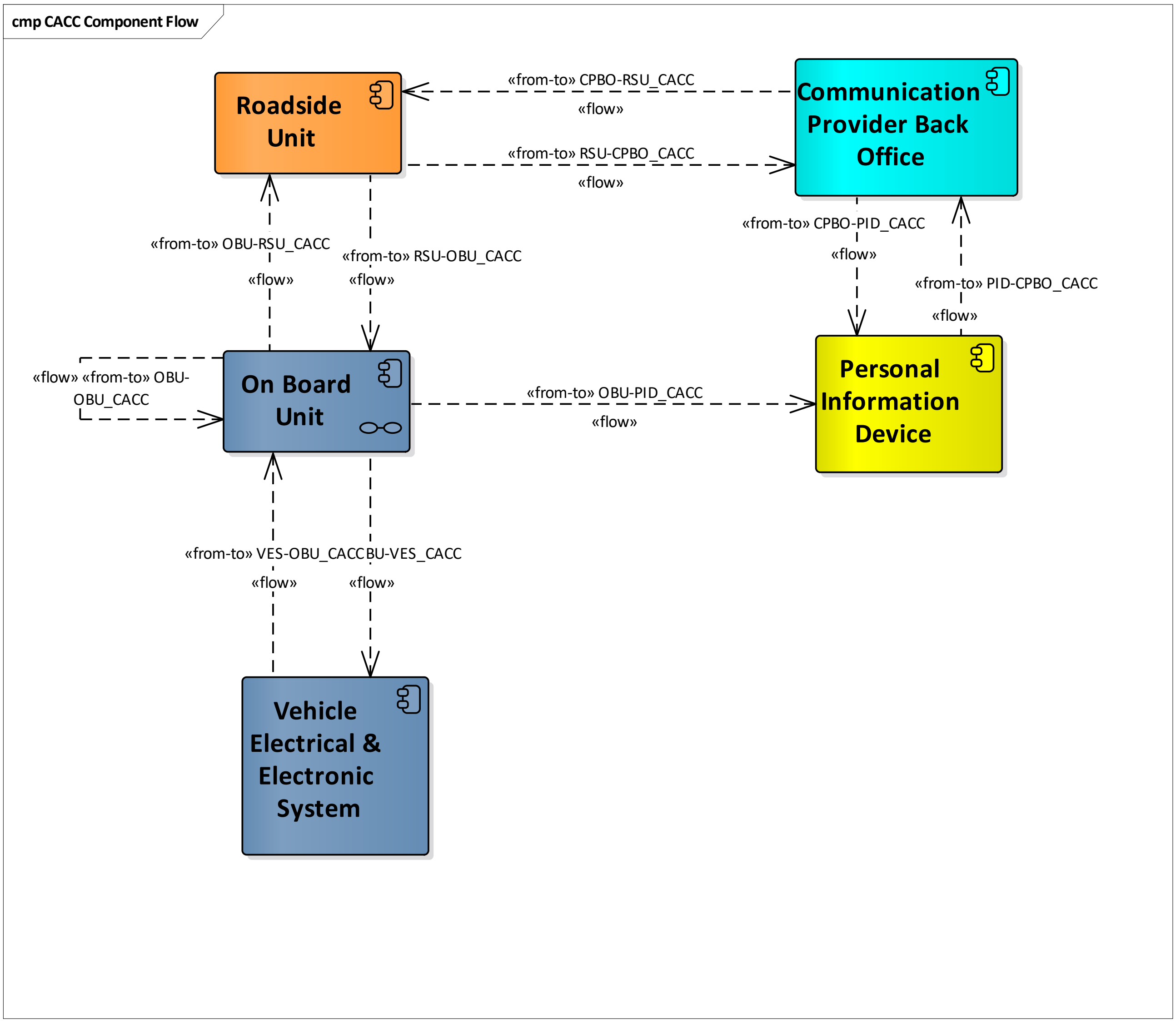


Figure 167:CACC – Components and communication flows

In the use case **UC17.4 - Cooperative Adaptive Cruise Control**, the **On Board Unit (OBU)** uses the **OBU-OBU_CACC** relation to broadcast its CACC information needed for vehicle following and/or platooning state information. This use case is based on V2V communication only in which the ego vehicle CACC application uses the information from the **Vehicle Electrical & Electronic System (VEES)** to construct the CACC messages to be broadcasted out of the **OBU**. The CACC application status is based on information from **VEES** and presented on the vehicle HMI and/or **Personal Information Device (PID)**. The **PID** can also be an integrated part of the vehicle, example a touchscreen/HMI for activating/deactivating and configuring the CACC application and an overview of the CACC application status. The following vehicle uses the received CACC message at it **OBU** to set the speed set-point via the **VEES** and its status is presented at the **PID.**

In the use case **UC17.1 - CACC passenger vehicles approaching urban environment**, the CACC application normally used in more Highway like scenarios is active in an urban environment. So vehicle speeds are relatively slow and the use case is extended with information from traffic light controllers (TLC) at cooperative intersections. This is based on I2V communication with a **Roadside unit (RSU)**. And/or this information is provided via connected services Communication **Provider Back Office (CPBO)**. The **OBU** uses the TLC data from **RSU-OBU_CACC** and this can be used to adapt CACC set points at the **VEES**. If connected services are used, the TLC data from **RSU** is provided via **RSU-CPBO_CACC** to a central **CPBO**. The TLC data is provided to the vehicle **PID** using **CPBO-PID_CACC**. Physical in-vehicle implementations can have separate components integrated. As example a **PID** can be a smart phone or be part of a hybrid **OBU,** also a **PID** can be part of existing vehicle HMI's. The use case **UC17.2 - CACC passenger vehicles approaching semi-urban environment** is comparable with UC17.1 only other traffic rules and vehicle speeds apply related to the semi-urban environment.

In use case **UC17.3 - Truck Platooning** the focus is also on deployment in (semi-)urban environments were interaction with cooperative intersections helps the truck platoon passing these urban environments. So in addition to previous use cases, the focus is on "priority services" for the truck platoon in which the truck **OBU** uses a priority request via **OBU-RSU_CACC** (V2I) or **PID-CPBO_CACC** (connected services).

Table 31: CACC - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
VES-OBU_CACC	VEES	OBU	“CACC”	CAN, raw bytes	Generic	Generic Access	-	-	Figure 224
OBU-VES_CAC	OBU	VEES	“CACC”	CAN, raw bytes	Generic	Generic Access	-	-	Figure 225
OBU-OBU_CACC	OBU	OBU	“CACC”	CACC, ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 226
OBU-RSU_CACC	OBU	RSU	“CACC	SRM, ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 227
OBU-PID_CACC	OBU	PID	“CACC”	Json, asn.1	IPv6, IPv4, UDP	Generic Access	-	TLS	Figure 228
RSU-OBU_CACC	RSU	OBU	“CACC””	ETSI ITS SPAT, ETSI ITS MAP	GeoNetworking	ETSI ITS-G5	-	ETSI ITS-S Security Architecture	Figure 238
RSU-CPBO_CACC	RSU	CP BO		Json, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Figure 229
CPBO-RSU_CACC	CP BO	RSU		Json, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
CPBO-PID_CACC	CP BO	PID		Json, MQTT	IPv4, TCP, UDP	3GPP 4G Suite, 3GPP 3G Suite		TLS	Figure 240
PID-CPBO_CACC	PID	CP BO		Json, MQTT	IPv4, TCP, UDP	3GPP 4G Suite, 3GPP 3G Suite		TLS	Figure 236

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in.Will futher described in WP 5.

Appendix B. The protocol layers used here are the layers as defined by ETSI.

5.2.18. Slow or Stationary Vehicle Warning

The slow or stationary vehicle warning system is designed to aid the driver in avoiding or mitigating rear-end collisions with vehicles in front of driver's own car. The driver will be alarmed through driver notification or warning of the impending collision on slow vehicles. The system does not attempt to control the vehicle in order to avoid an impending collision; instead it warns the following vehicles on the potential danger of the slow vehicle.

This service provides timely in-car driving assistance information on a stationary vehicle(s) downstream of the current position and in the driving direction of the vehicle [74].

5.2.18.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 168.

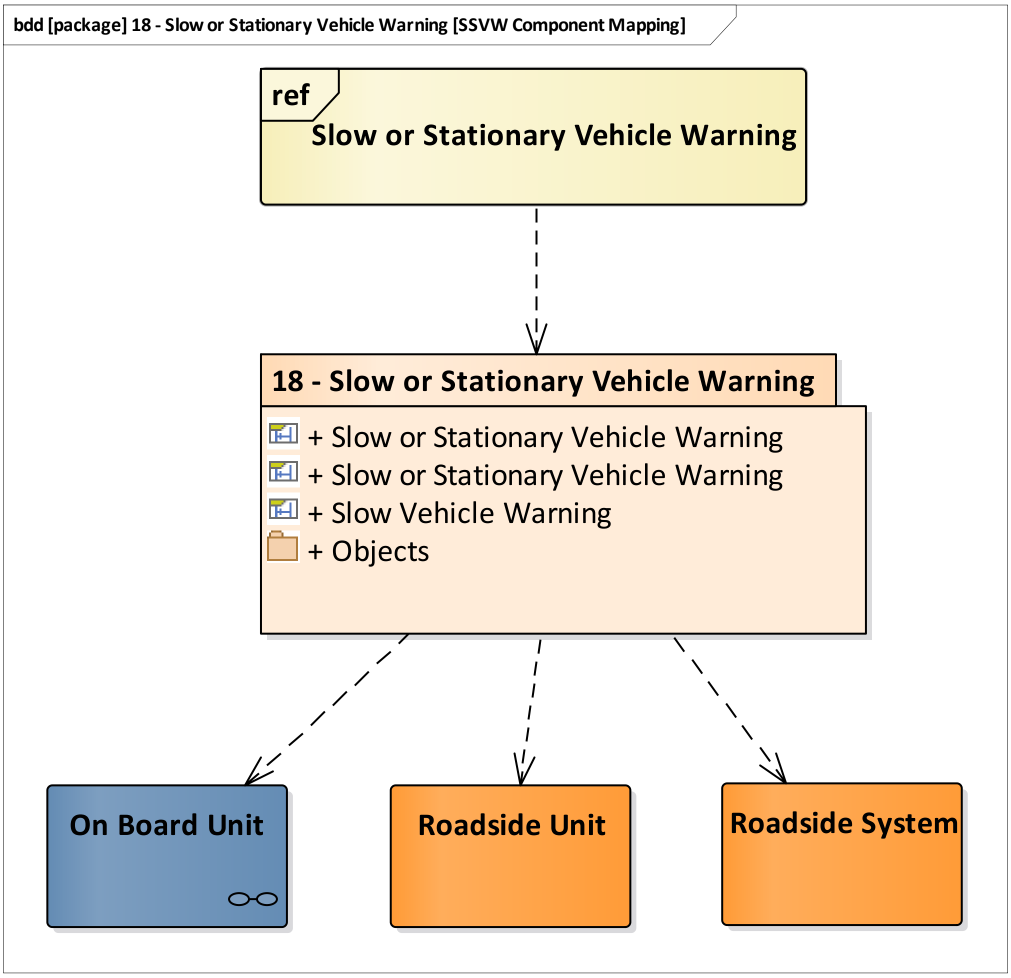


Figure 168: Slow or Stationary Vehicle Warning- Components involved in service

To implement this service, the following components are necessary.

- On Board Unit (see section 4.2.4.2.1 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- Roadside System (see section 4.2.3.2.1 for details.)

The relations between those components is described in the section 5.2.18.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- "Slow or Stationary Vehicle Warning" as shown in Appendix A

5.2.18.2. Component Connections

The following section describes the relations between the components. In Figure 169 all the involved components and the connections between them are listed for all use cases of the service.

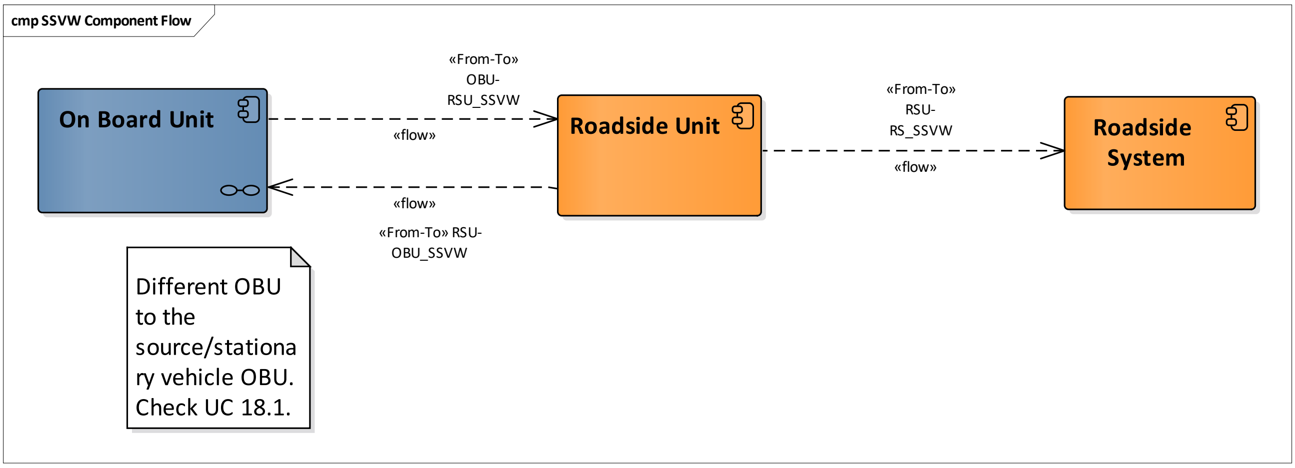


Figure 169: Slow or Stationary Vehicle Warning – Components and communication flows

In the **Slow or Stationary Vehicle Warning** scenario, the **On Board Unit (OBU)** of the stationary vehicle uses the **OBU-RSU_SSVW** connection to send the location of the stationary vehicle to the **Roadside Unit (RSU)**. From the **RSU** depending upon the display select, different flow is possible. If the warning is to be displayed on a display on the Roadside, the **RSU** uses the **RSU-RS_SSVW** connection to forward the message to the **Roadside System (RS)**, where it calculates the advice and displays it. If the warning is to be displayed in the vehicle, the **RSU** uses the **RSU-OBU_SSVW** connection to forward the message to the **OBU** of the other vehicle downstream from the stationary vehicle, where the **OBU** calculates the advice and displays it.

Table 32: Slow or Stationary Vehicle Warning - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
OBU-RSU_SSVW	OBU	RSU	-	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5		ETSI ITS-S Security Architecture	Figure 242Figure 242, p. 219
RSU-OBU_SSVW	RSU	OBU	-	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5		ETSI ITS-S Security Architecture	Figure 243, p.285
RSU-RS_SSVW	RSU	RS	-	ETSI ITS DENM	IPv4, IPv6, TCP	Generic Access		ETSI ITS-S Security Architecture	Figure 244, p.286

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.19. Motorcycle approaching indication

Motorcycle approaching indication (including other VRUs) warns the driver of a vehicle that a motorcycle is approaching/passing (the scope can be extended to cover VRUs, such as pedestrians, cyclists, or moped riders). The motorcycle could be approaching from behind or crossing at an intersection. The service assists the driver with blind spots.

European In-depth motorcycle accident analyses highlights that human error, and more specifically not seeing the motorcycle coming or misinterpreting distance and speed is the primary cause of accidents involving motorcycles. [74]

5.2.19.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 170.

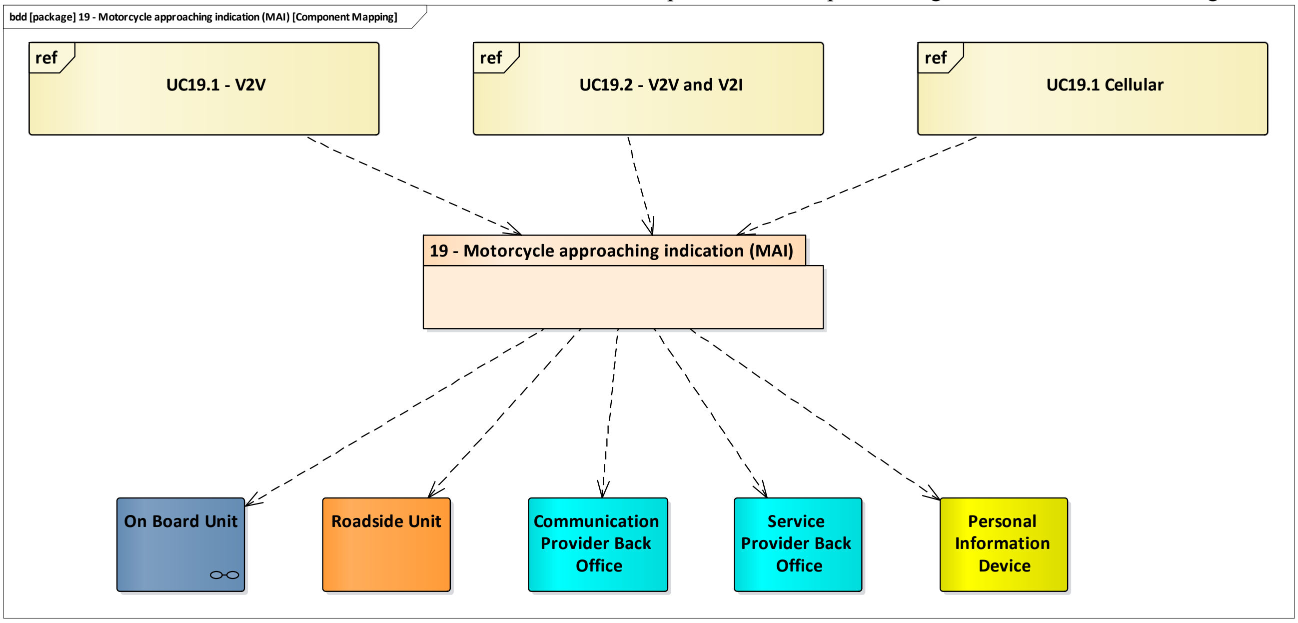


Figure 170: Motorcycle Approaching Indication - Components involved in service

To implement this service, the following components are necessary.

- On Board Unit (see section 4.2.4.2.1 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components are described in the section 5.2.19.2, below. The general functionality of this service, as well as more detailed interactions of the involved components are further described in UML Sequence Diagrams for the different use-cases on which this service is based. Those are in particular:

- UC19.1 - The approaching two-wheeler warning (V2V) as shown in section 7.1.19.1.1
- UC19.1 – The approaching two-wheeler warning (V2V cellular) as shown in section 7.1.19.1.2
- UC19.2 - The approaching two-wheeler warning (V2V and V2I) as shown in section 7.1.19.1.3

5.2.19.2. Component Connections

The following section describes the relations between the different components. In Figure 171 all the involved components and the connections between them are listed for all use cases of the service.

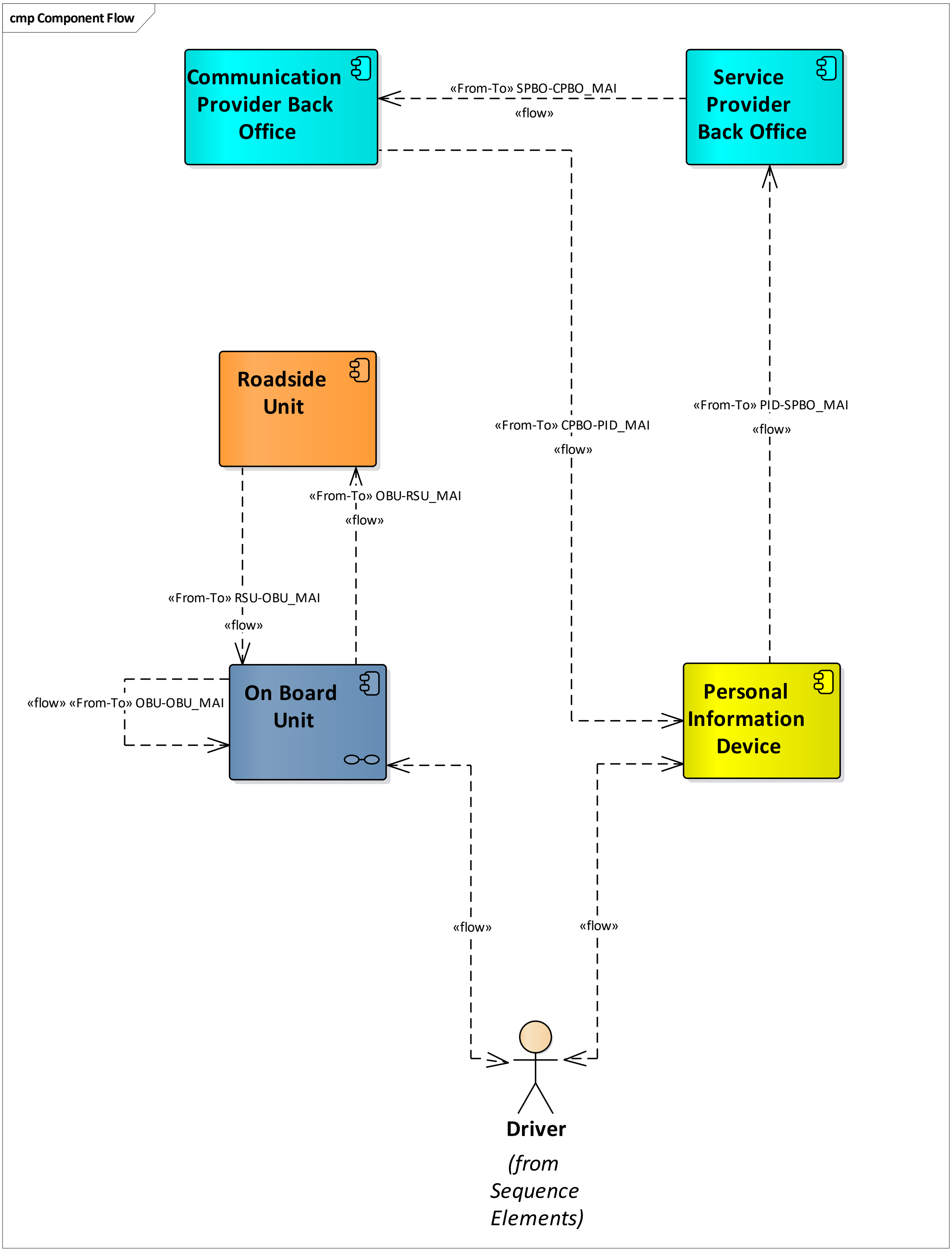


Figure 171: Motorcycle approaching indication – Components and communication flows

For the V2V ETSI ITS-G5 case of the approaching two-wheeler warning the **On Board Unit (OBU)** is periodically sending CAMs to near vehicles. Therefore, the **OBU** uses the **OBU-OBU_MAI** relation to provide location data and to calculate a possible crossing. In case of V2I the **OBU** is sending its location to the **Roadside Unit (RSU)** using **OBU-RSU_MAI** as well. If a possible collision is detected the **RSU** will warn near vehicles by sending DENMs to the **OBUs** using **RSU-OBU_MAI**.

To implement the approaching two-wheeler warning with cellular communication, the **Personal Information Devices (PID)** sending periodically CAMs to the **Service Provider Back Office (SPBO)** using **PID-SPBO_MAI** connection once they enter a specific area. If the **SPBO** detect colliding trajectories, it uses the **Communication Provider Back Office (CPBO)** through the **SPBO-CPBO_MAI** relation to send a DENM as GeoMessage to the related **PIDs** using the **CPBO-PID_MAI** connection.

Table 33: Motorcycle aproaching indication- Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
SPBO-CPBO_MAI	SPBO	CPBO	-	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMPv3 MIB	TLS, ETSI ITS-S Security Architecture	Figure 248
CPBO-PID_MAI	CPBO	PID	-	MQTT, ETSI ITS DENM	GeoNetworking	3GPP 3G Suite, 3GPP 4G Suite	TBD	TLS, ETSI ITS-S Security Architecture	Figure 249
PID-SPBO_MAI	PID	SPBO	HTTPS	ETSI ITS CAM	IPv4, IPv6, TCP	3GPP 3G Suite, 3GPP 4G Suite	TBD	TLS, ETSI ITS-S Security Architecture	Figure 252
OBU-OBU_MAI	OBU	OBU	-	ETSI ITS DENM, ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	ETSI 102 890-1	ETSI ITS-S Security Architecture	Figure 250
OBU-RSU_MAI	OBU	RSU	ETSI 102 894-2, ETSI 102 638	ETSI ITS CAM	GeoNetworking	ETSI ITS-G5	ETSI 102 890-1, G5 Congestion Control Management	ETSI ITS-S Security Architecture	Figure 253
RSU-OBU_MAI	RSU	OBU	ETSI 102 894-2, ETSI 102 638	ETSI ITS DENM	GeoNetworking	ETSI ITS-G5	ETSI 102 890-1, G5 Congestion Control Management	ETSI ITS-S Security Architecture	Figure 251

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

5.2.20. Blind spot detection

The blind spot detection aims to detect and warn the drivers about other vehicle of any type locates in predefined blind spot locations. The idea is to provide timely in-car driving assistance information on the presence of a vehicle in a designated blind spot location in the driving direction of the vehicle. The service can be defined on the bases of two diagrams being a cooperative or connected service. Both diagrams are presented below.

5.2.20.1. Involved Components

This section shows, which components are involved in this service. Furthermore, it lists the various sequence diagrams, which have been created to describe the service. The foundation of the service description is the component diagram, as shown below in Figure 172.

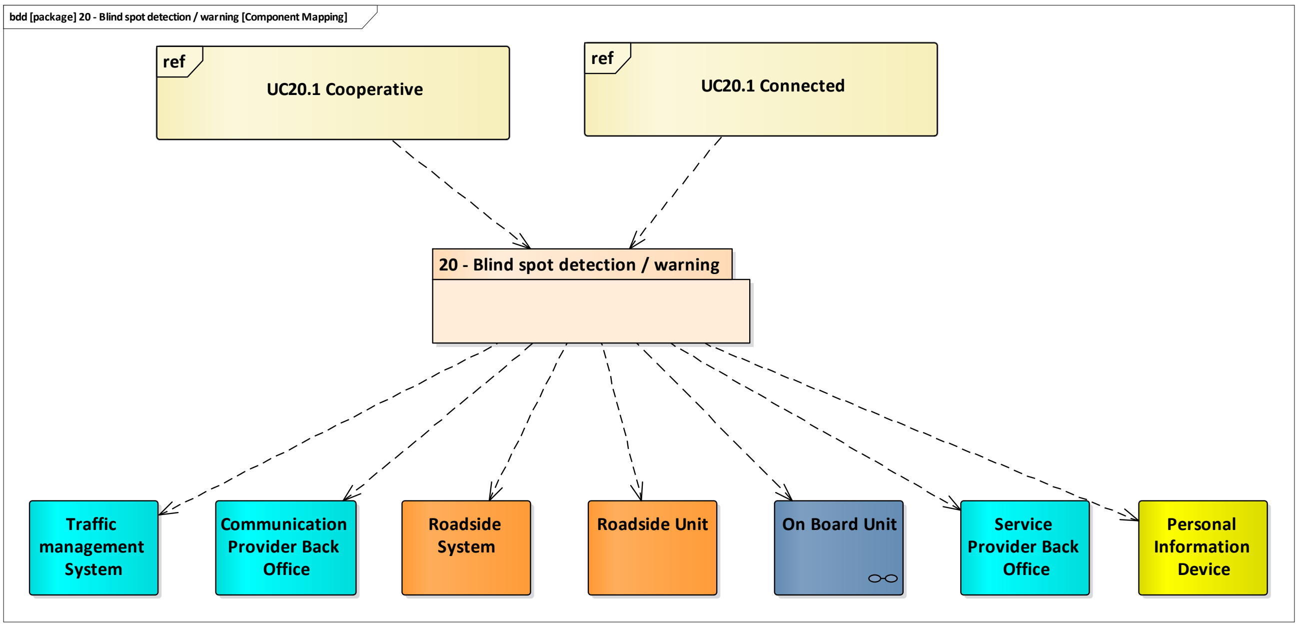


Figure 172: Blind Spot Detection - Components involved in service

To implement this service, the following components are necessary.

- Traffic management system (see section 4.2.2.2.5 for details.)
- Communication Provider Back Office (See section 4.2.2.2.1 for details)
- Roadside System (see section 4.2.3.2.1 for details.)
- Roadside Unit (see section 4.2.3.2.2 for details.)
- On Board Unit (see section 4.2.4.2.1 for details.)
- Service Provider Back Office (See section 4.2.2.2.3 for details)
- Personal Information Device (See section 4.2.5.2.1 for details)

The relations between those components is described in the section 5.2.20.2, below. The general functionality of this services, as well as more detailed interactions of the involved components is further described in UML Sequence Diagrams for the different use-cases on which this service is based. This are in particular:

- UC20.1 “Blind spot detection, cooperative” as shown in Figure 254
- UC20.2 “Blind Spot detection, connected” as shown in Figure 255

5.2.20.2. Component Connections

The following section describes the relations between the components. In Figure 173, all the involved components and the connections between them are listed for all use cases of the service.

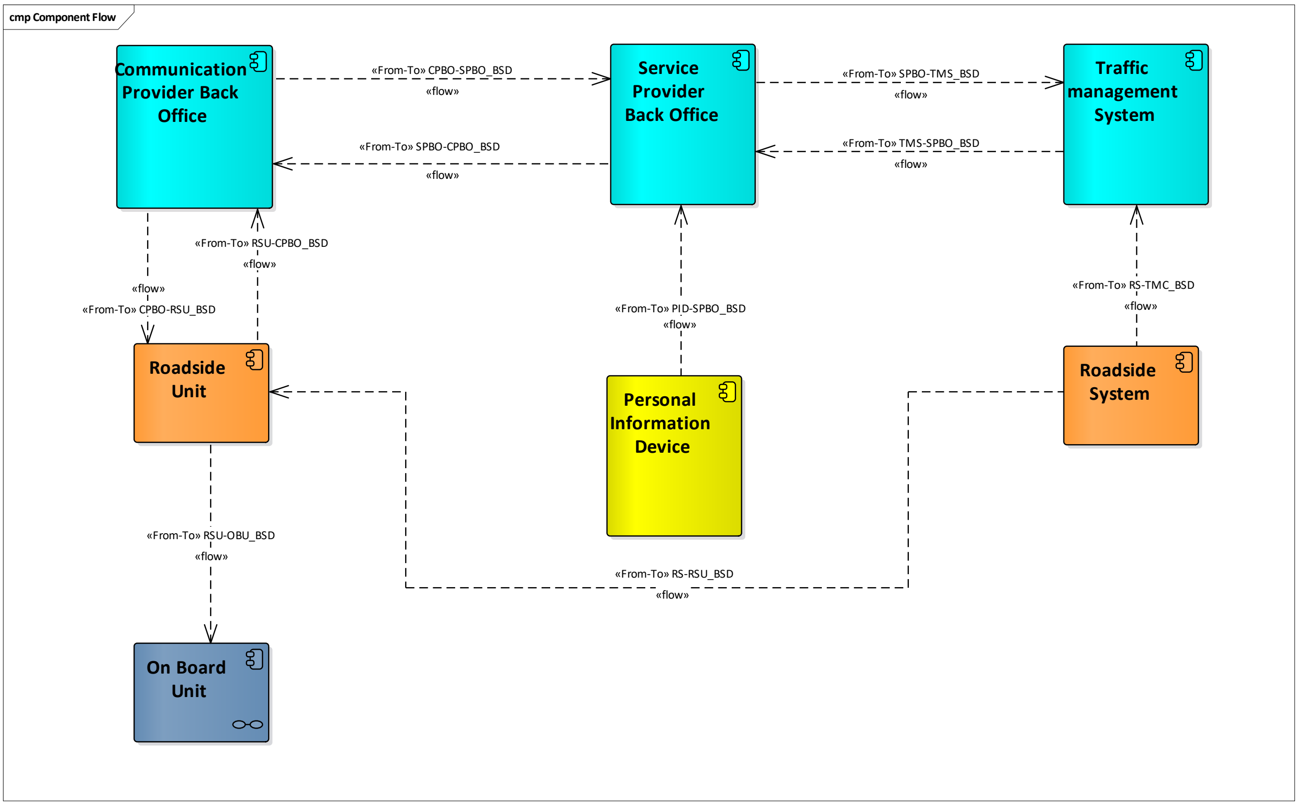


Figure 173: Blind Spot Detection – Components and communication flows

The **Roadside System**, for that case the **RS** is e.g. camera, detects vehicles in a blind spot and provides this information to the **Traffic Management System** through the **RS-TMS_BSD** connection as well as to the **Roadside Unit** trough the **RS-RSU_BSD** connection. This information gets further send through the **Communication Provider Back Office** to the **Service Provider Back Office**. The **SPBO** will receive location data for **PIDs** using **PID-SPBO_BSD** connection. The **SPBO** will then send those detection information using the **CPBO** and **RSU** to reach the **OBUs**.

Table 34: Blind Spot Detection - Protocols used for connections

Name	From	To	Protocol Layer						Datatypes Reference
			Application	Facilities	Transport & Networking	Access	Management	Security	
TMS-SPBO_BSD	TMS	SPBO	HTTPS	JSON	IPv4, IPv6, TCP			TLS	Not defined yet
SPBO-TMS_BSD	SPBO	TMS	HTTPS	JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
TMS-SPBO_MTTA	TMS	SPBO	HTTPS	JSON	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
CPBO-SPBO_BSD	CPBO	SPBO	HTTPS	JSON, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
SPBO-CPBO_BSD	SPBO	CPBO	HTTPS	ETSI ITS DENM, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-SPBO_MTTA	CPBO	SPBO	HTTPS	JSON, MQTT	IPv4, IPv6, TCP	Generic Access	SNMP	TLS	Not defined yet
CPBO-RSU_BSD	CPBO	RSU		ETSI ITS DENM, MQTT	IPv4, IPv6, TCP			TLS, ETSI ITS-S Security Architecture	Not defined yet
RSU-CPBO_BSD	RSU	CPBO		ETSI ITS CAM, MQTT	IPv4, IPv6, TCP			TLS, ETSI ITS-S Security Architecture	Not defined yet
CPBO-RSU_MTTA	CPBO	RSU			IPv4, IPv6, TCP, UDP	ETSI ITS-G5	SNMPv3 MIB	TLS	Not defined yet
RS-RSU_BSD	RS	RSU							Not defined yet
RS-TMS_GLOSA	RS	TMS			IPv4, TCP	Generic Access	SNMP	TLS	Not defined yet
RSU-OBU_MTTA	RSU	OBU			GeoNetworking	ETSI ITS-G5		ETSI ITS-S Security Architecture	Not defined yet

The table above shows the protocols which shall be used for the respective layer. Those listing may also contains alternatives, e.g. IPv4 or IPv6. The specific reference for the used protocols are listed in Will futher described in WP 5.

Appendix B.

The protocol layers used here are the layers as defined by ETSI. See ETSI EN 302 665 [75] for details.

6. Conclusion

Cooperative-Intelligent Transport Systems (C-ITS) aims to facilitate cooperative, connected and automated mobility. The C-ITS domain comprises widely spread systems like traffic management systems, traffic light controllers, and vehicle on-board units. Such complex and heterogeneous systems have independent uses but demand a strategy to facilitate their convergence. One of the main objectives of C-MobILE is to define reference, concrete, and implementation architectures for large scale C-ITS deployment and demonstration at the partner deployment sites across Europe. The C-MobILE C-ITS reference architecture is defined using the C-ITS architecture framework that is compatible with the ISO/IEC/IEEE 42010 international standard for architecture descriptions of systems. C-MobILE C-ITS reference architecture captures the needs of deployment sites and provides a guidance for future projects. Concrete and implementation architectures are defined based on the C-MobILE reference architecture using the six viewpoints defined in the scope of the C-MobILE C-ITS architecture framework: context, functional, communication, information, implementation, and physical viewpoint.

The first architecture description, with the widest scope and the shallowest depth of detail is the high-level reference architecture that forms the basis for the further course of work. For this architecture description, several existing C-ITS architectures were analysed, especially from the German CONVRGE project, the European MOBiNET project and the Dutch C-ITS Reference Architecture. The concepts and elements of those architectures have been described in SysML diagrams to show, which functional properties they have on a high-level. Those diagrams have been used to define standard concepts and create a common vocabulary for C-Mobile. The resulting reference architecture was refined in T3.2 into the more detailed mid-level concrete architecture description. The concrete architecture description follows the same principles as the reference architecture but describes them from a different perspective. The focus was primarily on fulfilling the technical requirements, which have been defined in D2.2. In addition, where the creation of blocks in the high-level architecture was purely from a functional point of view, they have now been rearranged with the various sub-systems in mind.

Building on the previous work, we analysed which components are needed to implement the services defined in D2.2 [74]. To this end, we analysed the different use cases and used the existing components and their relation each other to identify the needed interfaces. Where we found components or relations missing to fulfil a use case, we added them. This has been done mainly by the use of UML component diagram.

In order to ensure interoperability between different deployment sides, we followed the InterCor approach. They specified the so-called "interface 2" to connect data provides and service providers of the various deployment sites. This gives the DS the ability to share their back office data via a shared interface to the service providers. This allows users to use their "home service provider", even when they are roaming in a foreign city. In conclusion, more work needs to be done in terms of the information view definition to make sure all DS implementation are interoperable, as the InterCor IF2 only specifies the communication protocol, but not the exact data format. The results of this process will also be collected in D5.1.

In this deliverable, we present the reference, concrete, and implenetation architectures of the C-MobILE. As described previously, there are various existing projects being deployed at the C-MobILE partner deployment sites. To consolidate these and come up with a C-MobILE implementation architecture to be used for realizing the C-MobILE at eight different deployment sites, the following process is followed [81]:

- We analyzed the existing projects and abstracted the commonalities. We defined and discussed the common vocabulary for the project and agreed upon the terms and definitions used for the architecture definition.
- Since there was no standardized architecture framework in any of the existing projects, we defined the architecture framework using the conceptual model of ISO/IEC/IEEE 42010 [11]. This helped us in defining the views and viewpoints that satisfies the concerns of stakeholders participating in the C-MobILE project.
- We reused existing standards for the definition of the C-MobILE C-ITS reference architecture. We used SysML to describe the architecture as it is a mature language that is known to majority of system architects and designers. It being supported by many mature tools such as Enterprise Architect was helpful.
- We had weekly architecture team meetings comprising of architecture expertise from the C-MobILE partner deployment sites and other C-ITS projects that helped us in aligning the knowledge and concepts required to structure the C-MobILE C-ITS reference architecture.

The implementation architecture and detailed system design was defined by using the C-MoBILE reference and concrete architectures and the partner deployment site architectures. The different architectures from the partner deployment sites are used as an input for defining a detailed low-level implementation architecture in line with current standards. This architecture covers and satisfies each of the selected C-ITS services and can be used at the partner deployment sites. These reference, concrete, and implementation architectures can also form a base for future C-ITS deployments and implementations at other cities or regions. The C-ITS architecture framework can be used as a common practice for creating, interpreting, analyzing and using C-ITS architecture descriptions within C-ITS domain.

References

[1] Compass4D. Compass4D; Piloting Cooperative Services for Deployment; Final Results. [Accessed 09/10/2017]. http://www.compass4d.eu/download/compass4d_final_results_final.pdf.

[2] ETSI EN 302 665 - V1.1.1: Intelligent Transport Systems (ITS); Communications Architecture

[3] G. Alcaraz, S. Tsegay, M. Larsson, G. Vernet, E. Koenders, J. Vreeswijk, F. Ophelders, P. Mathias, F. Couly, J. Fernandez, A. Perpey, M. Feringa, and M. Annoni. 30/01/2015. Compass4D; D2.2 Overall reference architecture. [Accessed 20/10/2017]; Version 2.0. http://www.compass4d.eu/download/compass4d_d2_2_overallreferencearchitecture_v20_ec.pdf.

[4] CVRIA; Connected Vehicle Reference Implementation Architecture. [Accessed 09/10/2017]. http://local.iteris.com/cvria/html/about/about.html.

[5] European Commission. SCOOP@F Part 2; 2014-EU-TA-0669-S. [Updated October 2015, Accessed 20/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2014-eu-ta-0669-s_final.pdf.

[6] E. Broquaire, MC. Esposito, and JM. Tissier. 20/4/2017. Network architecture of the scoop@F project for road operators. [Updated 23/3/2017, Accessed 20/10/2017]. Version 2.00.

[7] European Commission; CORDIS; Projects and Results; IMPROVING THE SAFETY AND MOBILITY OF VULNERABLE ROAD USERS THROUGH ITS APPLICATIONS. VRUITS. [Updated 19/06/2014, Accessed 09/10/2017]. http://cordis.europa.eu/project/rcn/186986_en.html.

[8] K. Moerman, J. Scholliers, M. Penttinen, J. Luoma, M. Kallio, M. Kulju, H. Sintonen, M. Jutila, M. Valta, M. de Goede, M. van Sambeek, E. Wilschut, L. Kroon, J. González L., T. Paadín, F. Morte, J. Carranza, A. B. G. Meléndez, Ó. M. Pérez, S. P. Crespo, C. Cacciabue, and M. Cassani. 23/10/2014. VRUITS; Deliverable D4.2 Architecture for integration of VRUs and draft recommended practices for usability & user acceptance. [Accessed 20/10/2017]. Version 1.2. http://www.vruits.eu/themes/bamboo/deliverables/VRUITS_D42_141029_wm.pdf.

[9] Ministry of Infrastructure and the Environment of the Netherlands, Federal Ministry of Transport and Digital Infrastructure, Austrian Ministry for Transport, Innovation and Technology. Cooperative ITS Corridor Joint deployment. [Updated 2015, Accessed 09/10/2017]. http://c-its-korridor.de/data/download/Flyer%20C-ITS-en.pdf.

[10] Cooperative ITS Corridor Joint Deployment. [Accessed 22/10/2017]. https://itscorridor.mett.nl/English/Project+details/Cooperative+services/default.aspx.

[11] European Corridor – Austrian Testbed for Cooperative Systems. 29/07/2016. SWP 3.7 – Living Lab Definition; Living Lab; WP 3 – Functional Specification & Development. [Accessed 23/10/2017, Updated 29/07/2016]. Version 03.60.

[12] ISO/IEC/IEEE 42010:2011. Systems and software engineering – Architecture description. http://www.iso-architecture.org/

[13] Emery, D., and Rich H. Every architecture description needs a framework: Expressing architecture frameworks using ISO/IEC 42010. Software Architecture, 2009 & European Conference on Software Architecture. WICSA/ECSA 2009. Joint Working IEEE/IFIP Conference on. IEEE, 2009.

[14] Rozanski, N. and Woods, E. Software systems architecture: working with stakeholders using viewpoints and perspectives. Addison-Wesley, 2011.

[15] Kruchten, P.B. "The 4+ 1 view model of architecture." IEEE software 12.6 (1995): 42-50

[16] Haren, Van. TOGAF Version 9.1. Van Haren Publishing, 2011.

[17] Zachman, J. "The zachman framework for enterprise architecture." Zachman International 79 (2002).

[18] International Organization for Standardization. ISO-IEC 25010: 2011 Systems and Software Engineering-Systems and Software Quality Requirements and Evaluation (SQuaRE)-System and Software Quality Models. ISO, 2011.

[19] European Commission. NordicWay; 2014-EU-TA-0060-S. [Updated 09/2015, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2014-eu-ta-0060-s_final.pdf.

[20] CVRIA; Connected Vehicle Reference Implementation Architecture. [Accessed 09/10/2017]. http://local.iteris.com/cvria/html/about/about.html.

[21] C-ROADS; HARMONISATION OF C-ITS RELATED DEPLOYMENTS THROUGHOUT EUROPE. [Accessed 09/10/2017]. https://www.c-roads.eu/platform/about/about.html.

[22] European Commission; CORDIS; Projects and Results; IMPROVING THE SAFETY AND MOBILITY OF VULNERABLE ROAD USERS THROUGH ITS APPLICATIONS. VRUITS. [Updated 19/06/2014, Accessed 09/10/2017]. http://cordis.europa.eu/project/rcn/186986_en.html.

[23] C-ROADS. [Accessed 09/10/2017]. https://www.c-roads.eu/platform.html.

[24] European Commission. InterCor; 2015-EU-TM-0159-S; North Sea–Mediterranean Corridor. [Updated 11/2016, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2015-eu-tm-0159-s_final.pdf.

[25] ECo-AT; The Austrian contribution to the Cooperative ITS Corridor. [Accessed 09/10/2017]. http://www.eco-at.info/home-en.html.

[26] European Commission. 2017. CODECS; COoperative ITS DEployment Coordination Support. [Updated 31/07/2017, Accessed 09/10/2017]. http://cordis.europa.eu/project/rcn/194851_en.html.

[27] European Commission. AUTOCITS; 2015-EU-TM-0243-S; Atlantic Corridor. [Updated 09/2016, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2015-eu-tm-0243-s_final.pdf.

[28] European Commission. C-ITS for Trucks (CITRUS); 2015-BE-TM-0391-S; Rhine-Alpine, North Sea–Mediterranean Corridor. [Updated 11/2016, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2015-be-tm-0391-s_final.pdf.

[29] European Commission. PROSPECT; PROactive Safety for PEdestrians and CyclisTs. [Updated 17/08/2017, Accessed 09/10/2017]. http://cordis.europa.eu/project/rcn/193275_en.html.

[30] European Commission; Horizon 2020; XCYCLE. XCYCLE; Advanced measures to reduce cyclists' fatalities and increase comfort in the interaction with motorised vehicles. [Accessed 09/10/2017]. https://ec.europa.eu/inea/en/horizon-2020/projects/h2020-transport/safety/xcycle.

[31] European Commission. SOLRED C-ITS Monitoring Network (SolC-ITS); 2015-ES-TM-0079-S; Mediterranean & Atlantic Corridors. [Updated 11/2016, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2015-es-tm-0079-s_final.pdf.

[32] Architecture and use cases of the mobility service platform MOBiNET, Tobias Schlauch, Janki Dodiya, Andreas Rickling, Lars Mikkelsen, Dirk Beckmann, 12th ITS European Congress, Strasbourg, France, 19-22 June 2017

[33] MOBiNET: the Europe-wide e-market place of mobility services for businesses and end users. [Accessed 28/11/2017]. http://mobinet.eu/

[34] COmmunication Network VEhicle Road Global Extension. [Accessed 28/11/2017]. https://converge-online.de

[35] CITRUS: Coöperatieve ITS for Trucks. [Accessed 28/11/2017]. https://www.citrus-project.eu/

[36] Integrierte Kooperationsplattform für automatisierte Elektrofahrzeuge. [Accessed 28/112017]. https://ikopa.de/

[37] EUR-Lex Acess to European Union law. [Accessed 28/11/2017] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[38] Partnership Talking Traffic. [Accessed 28/11/2017]. https://www.partnershiptalkingtraffic.com

[39] ASFINAG, Federal Highway Research Institute, – Federal Ministry for Transport – Innovation and Technology, Rijkswaterstaat Ministry of Infrastructure and Environment, Hessen Mobil Road and Traffic Management, Federal Ministry of Transport and Digital Infrastructure, Rijkswaterstaat Ministry of Infrastructure and Environment. DEPLOYMENT OF COOPERATIVE SYSTEMS ON THE C-ITS CORRIDOR IN EUROPE. [Updated 2015, Accessed 21/11/2017]. http://c-its-korridor.de/data/download/Revue%20RT-Decembre_2015_p.50.pdf.

[40] DEN/ITS-0010005. ETSI EN 302 895 - V1.0.0: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM).

[41] Concurrent State Diagrams. [Accessed 28/11/2017]. http://etutorials.org/Programming/UML/Chapter+8.+State+Diagrams/Concurrent+State+Diagrams/

[42] C-ROADS – The Platform of Harmonized C-ITS Deployment in Europe. [Accessed 28/11/2017]. https://www.c-roads.eu

[43] Htw saar, bmt, SIT, SWARCO, ULD, FOKUS, DCAITI, NXP, ULD. iKoPA Deliverable D1v1 Requirements Analysis and System Architecture. 28/02/2017. Version number 1.0. [Accessed 28/11/2017]. https://ikopa.de/wp-content/plugins/download-attachments/includes/download.php?id=99

[44] BASt, BMW, Bosch, Ericsson, Frauenhofer AISEC, Frauenhofer FOKUS, Hessen Mobil, HTW, Opel, Vodafone, Tactilo, Volkswagen. Converge. Deliverable D4.3 "Architecture of the Car2X Systems Network". 31/01/2015. Version number 1.2. [Accessed 28/11/2017]. http://www.converge-online.de/doc/download/Del%2043%20Masterdocument.zip

[45] Perry, F. HNTB. Overview of DSRC Messages and Performance Requirements [Updated 03/2017, Accessed 23/11/2017]. http://www.transportation.institute.ufl.edu/wp-content/uploads/2017/04/HNTB-SAE-Standards.pdf

[46] Towards an Architecture for Cooperative-Intelligent Transport System (C-ITS) Applications in the Netherlands (Borgert van der Kluit, et al., April 2015)

[47] System Modelling Language http://sysmlforum.com/sysml-resources/publications/

[48] van Sambeek, M. Turetken, O., Ophelders, F., Eshuis, R., Bijlsma, T. Traganos, K., Grefen. P (2015) Towards an Architecture for Cooperative ITS Applications in the Netherlands, Version 1.0. DITCM. April 17, 2015. Available at: https://goo.gl/pHSD9D

[49] XCYCLE. [Accessed 30/11/2017]. http://www.xcycle-h2020.eu

[50] Kenis, E. Autonomous driving & Co-operative ITS in Flanders, Department of Mobility & Transport Policy Unit, ITS Belgium Congress, 2016

[51] Vandenberghe, W. Partnership Talking Traffic, Dutch Ministry of Infrastructure & Environment, ITS Belgium Congress, 2017

[52] Talking traffic project [Accessed 30/11/2017]. https://www.partnershiptalkingtraffic.com/

[53] ERTICO. [Accessed 30/11/2017]. http://ertico.com/vision-and-mission/

[54] International Road Transport Union. [Accessed 30/11/2017]. https://www.iru.org/who-we-are/about-iru/history

[55] Federation Internationale de l'Automobile. [Accessed 30/11/2017]. https://www.fia.com/organisation

[56] Dajsuren, Y. "On the design of an architecture framework and quality evaluation for automotive software systems." PhD thesis. Eindhoven University of Technology, 2015.

[57] Standard, S. V. 2016. SAE International. J2735

[58] K. Přidal, http://www.maptiler.org/google-maps-coordinates-tile-bounds-projection/, last visited 4-12-2017.

[59] RFC 75119, "JSON Web Token (JWT)", Internet Engineering Task Force (IETF) [Accessed 27/02/2018]. May 2015. https://tools.ietf.org/html/rfc7519

[60] Castells, J., Molins, R., "D2.3: Requirements for C-ITS implementation,", C-MobILE project, 2017.

[61] Daisuren, Y., Karkhanis, P., Kadiogullari, D., Fünfrocken, M., "D3.1: Reference architecture", C-MobILE project, 2017.

[62] G. Alcaraz, S. Tsegay, M. Larsson, G. Vernet, E. Koenders, J. Vreeswijk, F. Ophelders, P. Mathias, F. Couly, J. Fernandez, A. Perpey, M. Feringa, and M. Annoni. 30/01/2015. Compass4D; D2.2 Overall reference architecture. [Accessed 20/10/2017]; Version 2.0. http://www.compass4d.eu/download/compass4d_d2_2_overallreferencearchitecture_v20_ec.pdf.

[63] Rozanski, N. and Woods, E. Software systems architecture: working with stakeholders using viewpoints and perspectives. Addison-Wesley, 2011.

[64] International Organization for Standardization. ISO-IEC 25010: 2011 Systems and Software Engineering-Systems and

Software Quality Requirements and Evaluation (SQuaRE)-System and Software Quality Models. ISO, 2011.

[65] European Commission. NordicWay; 2014-EU-TA-0060-S. [Updated 09/2015, Accessed 09/10/2017]. https://ec.europa.eu/inea/sites/inea/files/fiche_2014-eu-ta-0060-s_final.pdf.

[66] Partnership Talking Traffic. [Accessed 28/11/2017]. https://www.partnershiptalkingtraffic.com

[67] Vandenberghe, W. Partnership Talking Traffic, Dutch Ministry of Infrastructure & Environment, ITS Belgium Congress, 2017

[68] Converge deliverable 4.3 Version 1.2 (30-01-2015)

[69] InterCor Milestone 4 – Common set of upgraded specifications for Hybrid communication, version 1.0 (01-03-2018)

[70] C-ROADS – The Platform of Harmonised C-ITS Deployment in Europe. [Accessed 28/03/2018]. https://www.c-roads.eu

[71] C-Roads WG3, TF2. C-ITS Infrastructure Functions and Specifications, version 3.0 (06-09-2017)

[72] C-Roads WG3, TF2. Roadside ITS G5 System Profile, version 3.0 (06-09-2017)

[73] NL_Deliverable-F-iTLC-Architecture_GLOSA-V1.2.pdf

[74] Ege Adali O., Turetken O., Grefen P., D2.2 Analysis and Determination of Use Cases; C-MobILE project, 28/02/2018.

[75] ETSI TS EN 302 665: „Intelligent Transport System (IST); Communications Architecture“.

[76] Harmonized Architecture Reference for Technical Standards. http://htg7.org.

[77] European Commission. C-ITS Platform; Final report 2016. [Updated 01/2016, Accessed 09/06/2018]. https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[78] I. Passchier *et al*, The intercor project, Milestone 4 - Common set of upgraded specifications for Hybrid communication-Specifications for IF2 for hybrid communication v1.0, 1-1-2018

[79] O'Hara, J. (2007). "Toward a commodity enterprise middleware"

[80] Vinoski, S. (2006). "Advanced Message Queuing Protocol"

[81] P. Karkhanis, M.G.J van den Brand, S. Rajkarnikar. Defining the C-ITS Architecture. WASA 2018, in press.

7. Appendix A

7.1.1. Rest-Time management

7.1.1.1. Service Diagrams

7.1.1.1.1. Rest-Time management

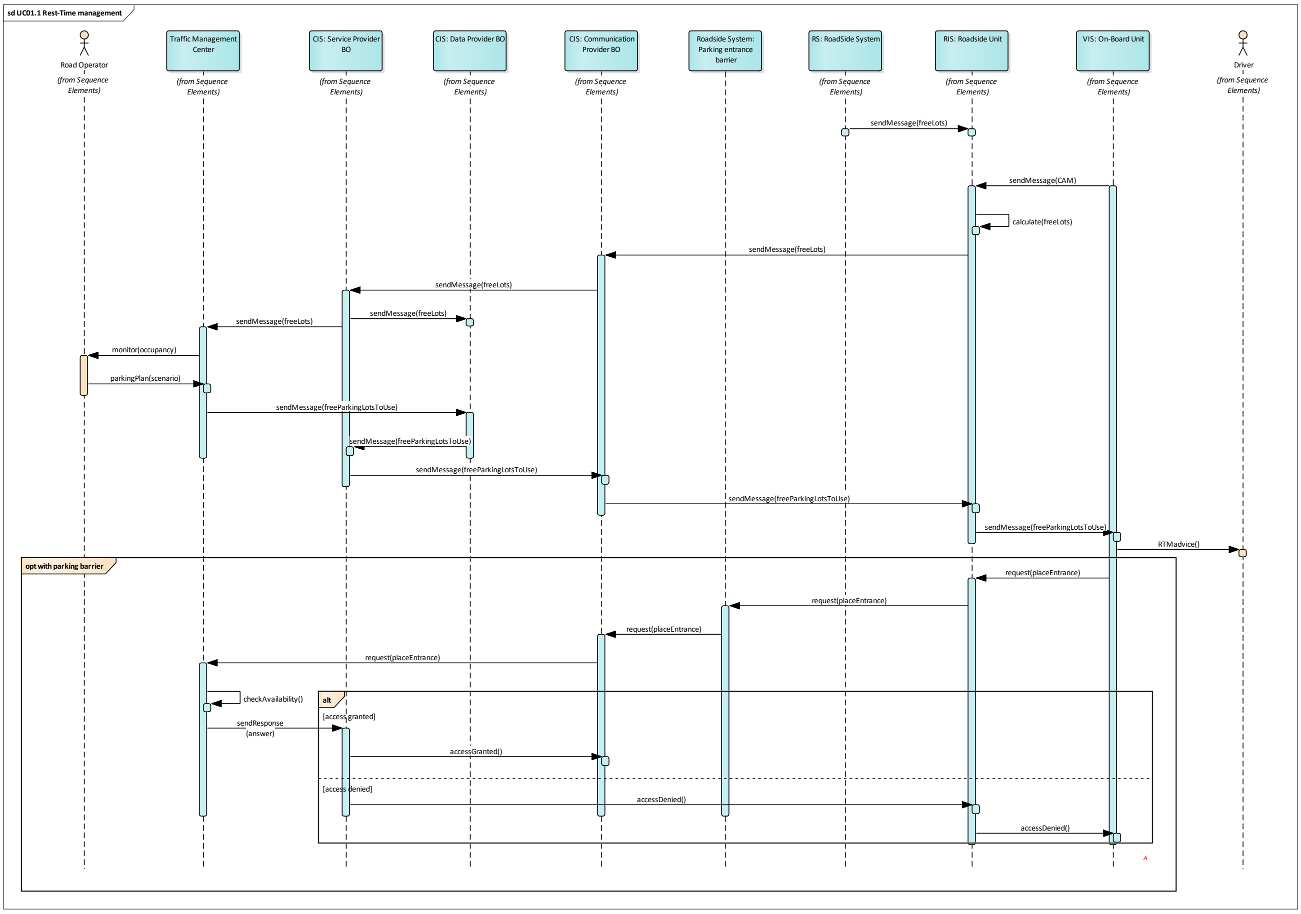


Figure 174: S01 Rest Time Management based in ARC-IT

The above sequence diagram is demonstrating Rest Time Management. In addition, it is also possible to use a barrier based system.

7.1.1.2. Service Datatypes

Will futher described in WP 5.

7.1.2. Motorway parking availability

7.1.2.1. Service Diagrams

7.1.2.1.1. Information on parking lots location, availability and services

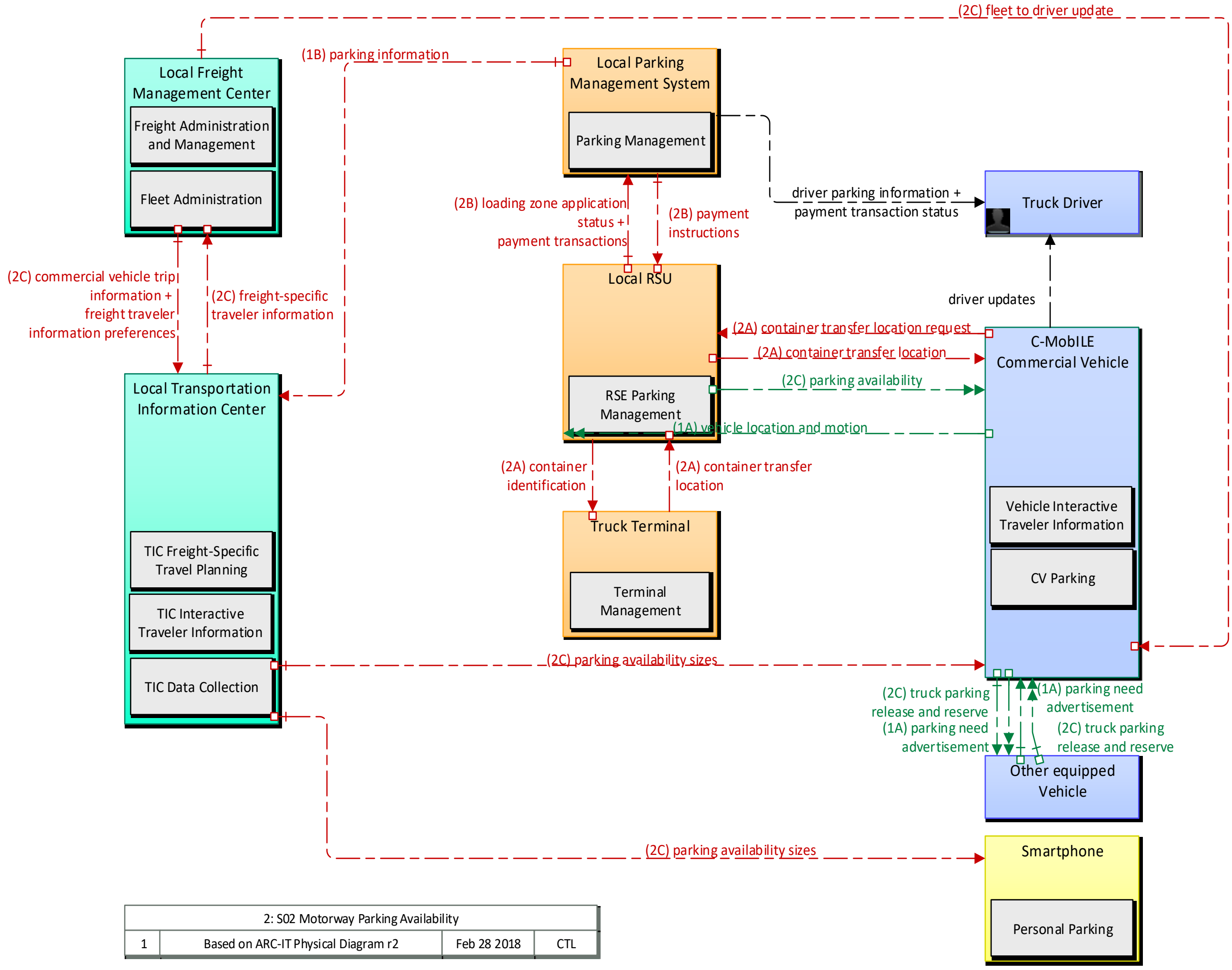


Figure 175: Motorway Parking Availability Physical View Diagram

It's based on the ARC-IT Reference architecture.

7.1.2.2. Service Datatypes

Will futher described in WP 5.

7.1.3. Urban parking availability

7.1.3.1. Service Diagrams

7.1.3.1.1. Information about a vehicle parking space released by a user

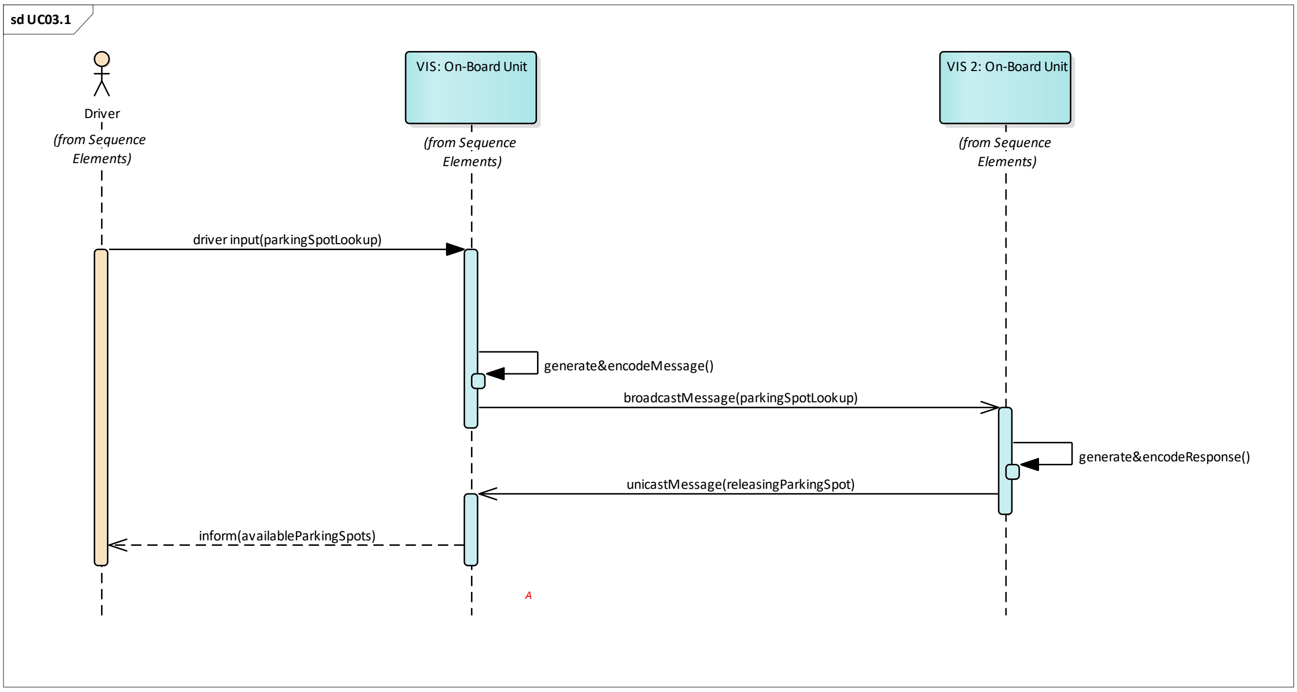


Figure 176: UC03.1- Information about a vehicle parking space released by a user

This first use case is cooperative-based parking spot releasing information. The main idea is, when a driver looks for a parking spot and a leaving vehicle announces the release, so the first driver can be aware of it.

The vehicle looking for parking, either from an automatic or manual action from the driver, sends a “parking lookup” message using the SPDP (Publishing Dynamic Parking Data) or the TTI (Traffic and Travel Information) TPEG2 standard. All nearby vehicle in the communication range of the vehicle would receive this message and the one leaving the parking spot can “answer” this messages via unicast communication. This unicast also uses one of the standards to inform the first vehicle that he is leaving a free parking spot.

7.1.3.1.2. UC03.2 “Reservation of a vehicle parking space released by a user”

Figure 177: Reservation of a vehicle parking space released by a user

This use case is an extension of the UC03.1, where the driver looking for a parking spot “reserves” the parking that is being released by the second vehicle. This reservation is a unicast message as a “reply” to the “releasing parking” unicast message sent by the leaving vehicle, that now the leaving vehicle knows that another driver is coming to occupy the parking spot and can “reserve/wait” until the first driver reaches the parking zone.

7.1.3.1.3. UC03.3 Information about on-street parking availability for urban freight (loading zones)

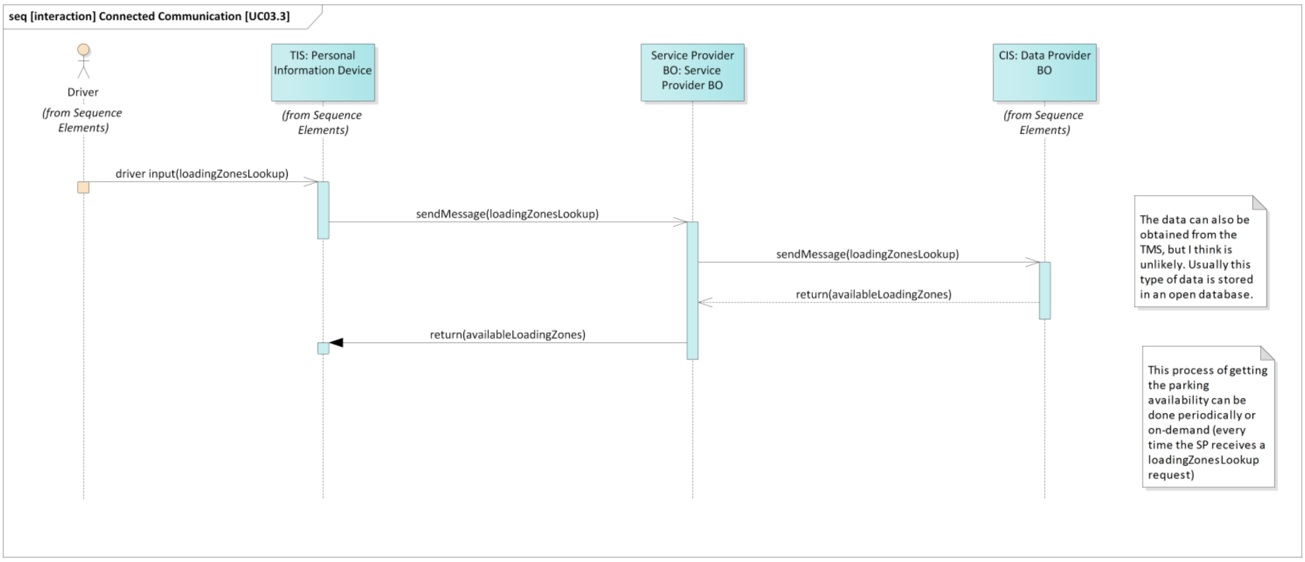


Figure 178: Information about on-street parking availability for urban freight

This connected-based use case is addressed to the professional freight sector to help them in the search for loading zones. As it is based on cellular communication, other architecture components are involved. Once the driver activates the search, the PID (e.g. smartphone) sends a message asking for loading zones to the UPA Service Provider using cellular communication. The standards are same as the previous use cases. As the requested information can be limited to a specific zone, the SPBO needs to ask the DPBO, which shall be constantly updated with the status of the loading zones in the city. The DPBO replies with this information using a DATEX or XML format (Deployment Site specific) to the SPBO, which would convert this information from the previous standard to the SPDP or TTI TPEG2 and forward it to the original requester using cellular communication.

7.1.3.1.4. UC03.4 - Information about on-street parking availability for private car drivers

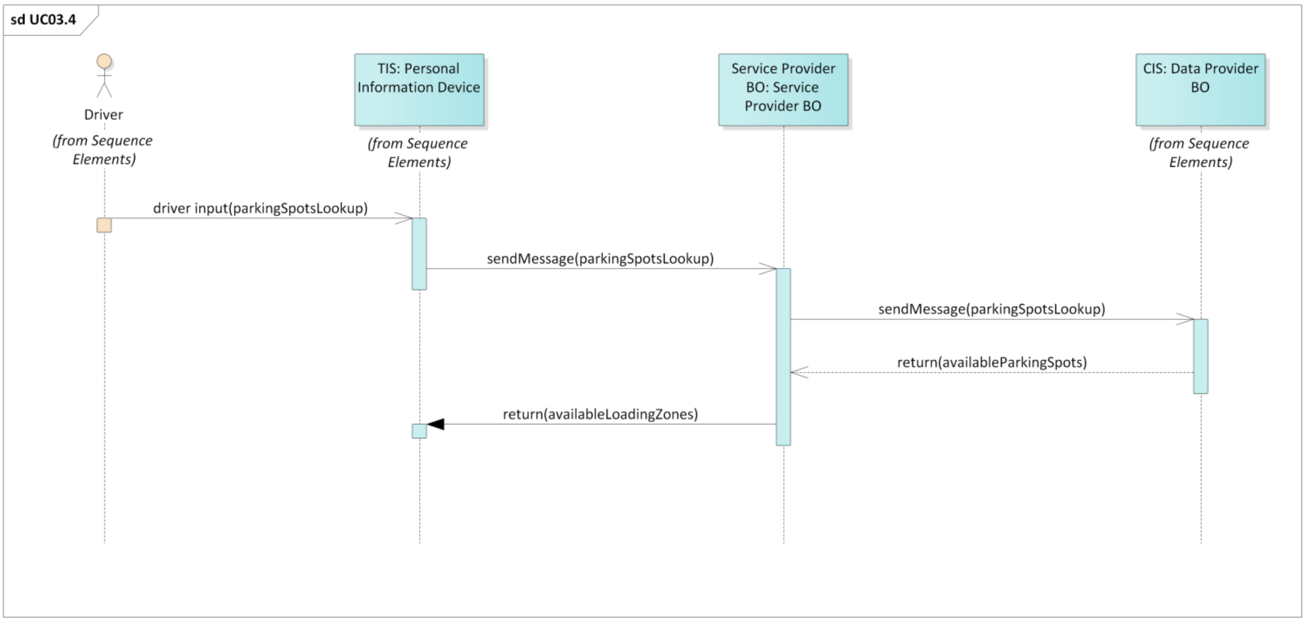


Figure 179: Information about on-street parking availability for private car drivers

This use case is essentially the same as the UC03.3 but intended for private vehicles instead of professional vehicles. This practically means that the request is done looking for free parking spots instead of loading zones, but the protocols and relations among the components follow the same approach as the previous use case.

7.1.3.2. Service Datatypes

Will futher described in WP 5.

7.1.4. Road works warning

7.1.4.1. Service Diagrams

7.1.4.1.1. Road Works Warning Sequence Connected

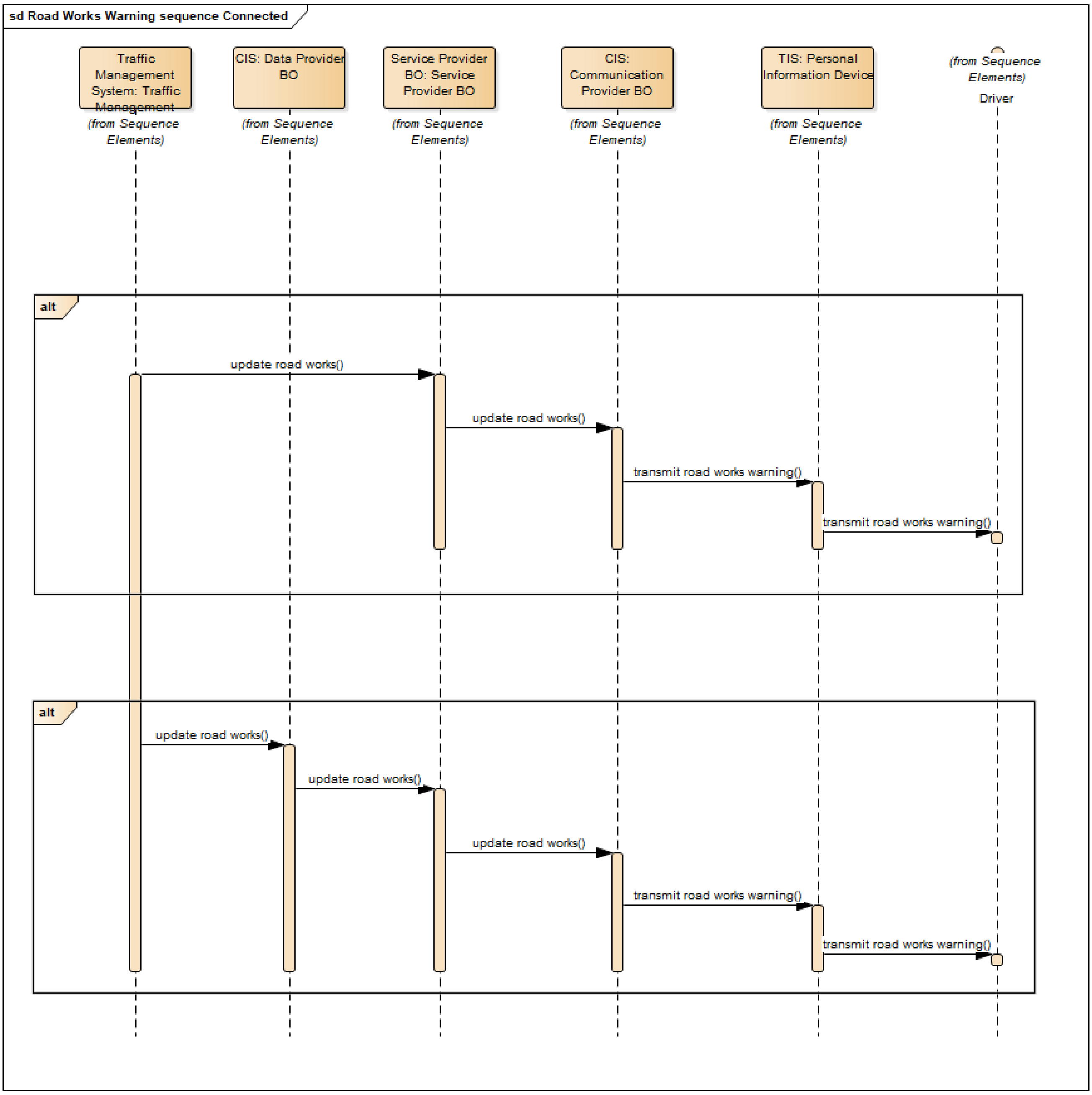


Figure 180: Road Works Warning Sequence Connected

The connected case starts from the TMS sending a road work update directly to the SP BO. The SP BO forwards this update to the CP BO in order to disseminate the message to PIDs (which can be many). At the same time, the TMS can send the road work update to a DP BO (in some sites) which forwards the update to the CP BO in order to disseminate the message to PIDs.

7.1.4.1.2. Road Works Warning Sequence Cooperative

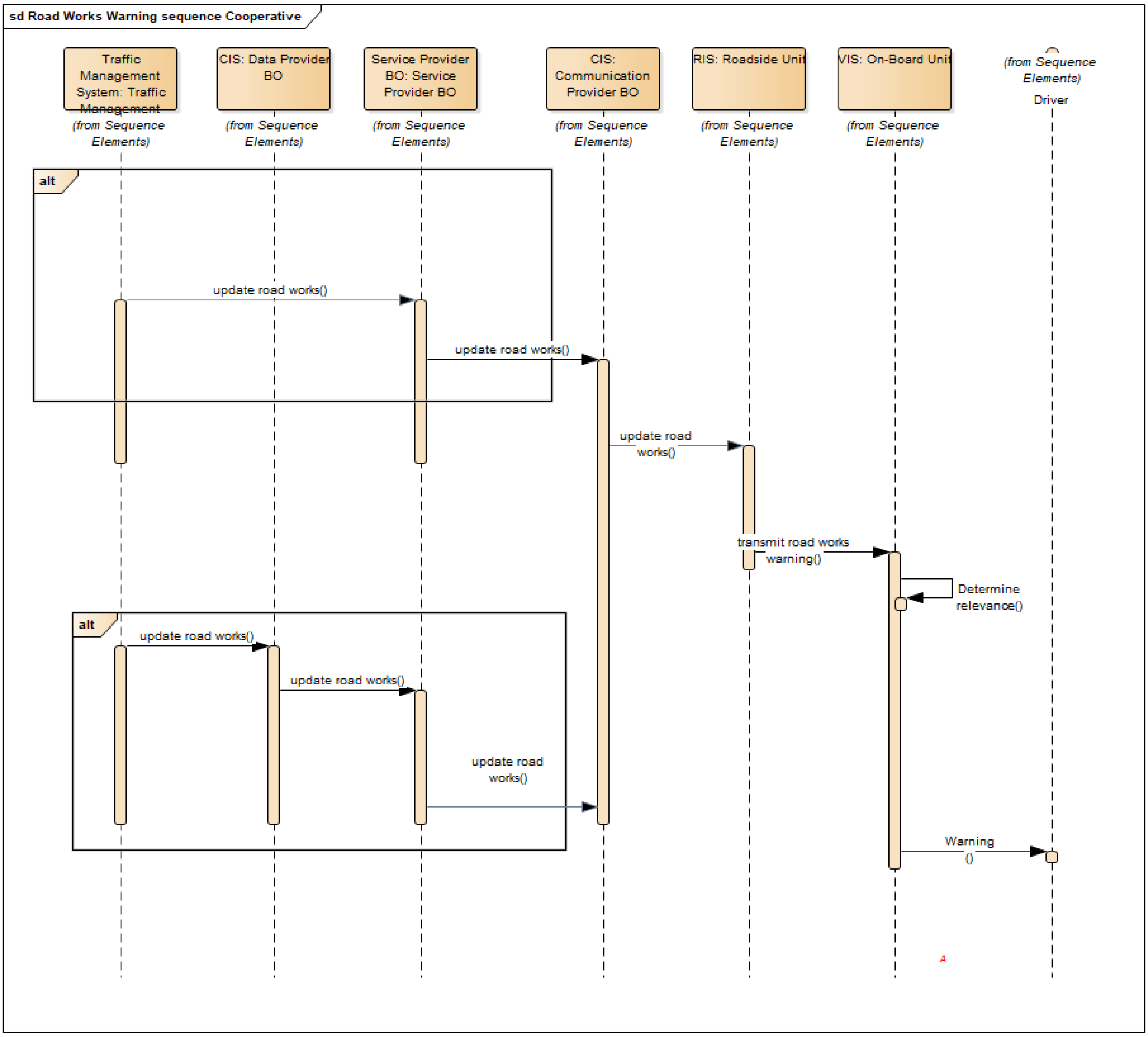


Figure 181: Road Works Warning Sequence Cooperative

The cooperative case starts from the TMS sending a road work update directly to the SP BO. The SP BO forwards this update to the CP BO. The CP BO, in turn, forwards the update to Roadside Units (RSUs) in the vicinity to disseminate the message to OBUs (which can be many) that have subscribed to the service. At the same time, the TMS can send the road work update to a DP BO (in some sites) which forwards the update to the CP BO. The CP BO, again, forwards the update to RSUs in the vicinity to disseminate the message to OBUs that have subscribed to the service.

7.1.4.1.3. With Mobile RSU

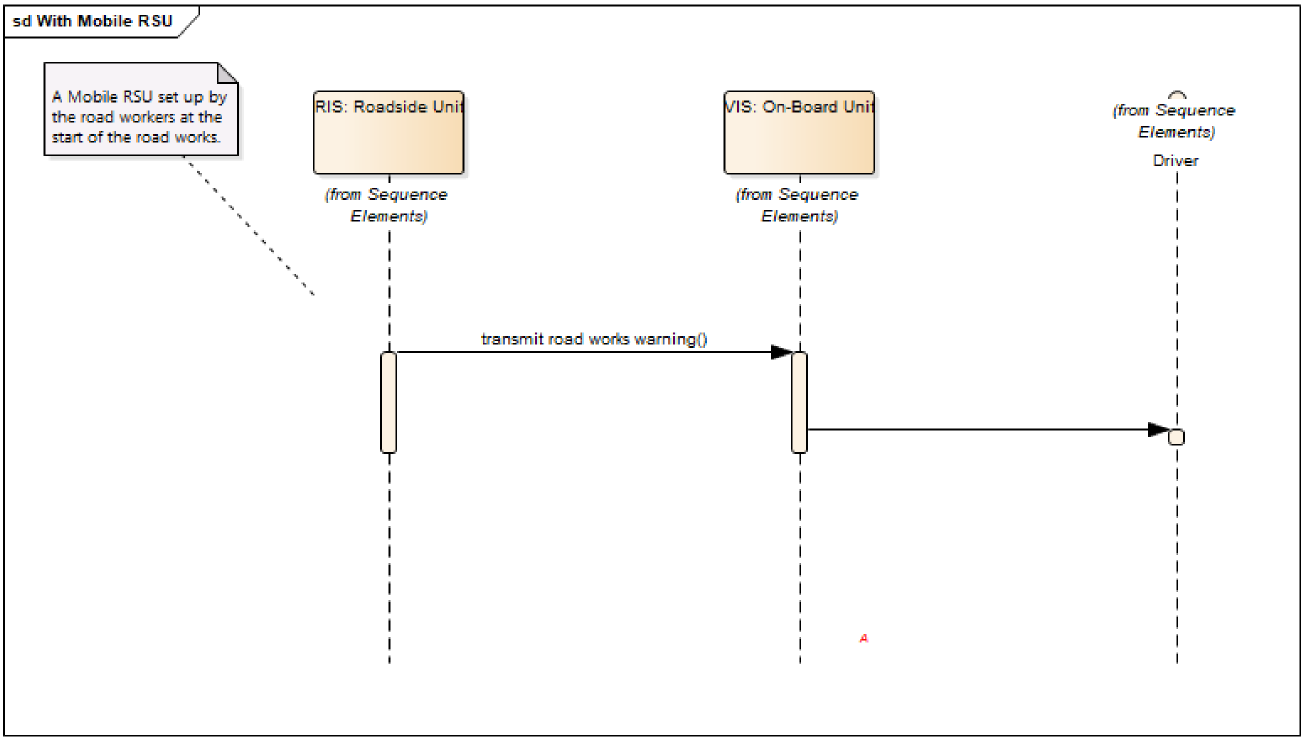


Figure 182: With Mobile RSU

The “with Mobile RSU” case starts from a RSU (that is setup by the road workers at the site of the road work) disseminating the message to OBUs that have subscribed to the services.

7.1.4.2. Service Datatypes

The following diagrams describes the datatypes and information exchanged between components. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. The range of attributes and information inside those message types are extensive and mostly out of scope, therefore the diagrams may only contain the necessary attributes with specific values.

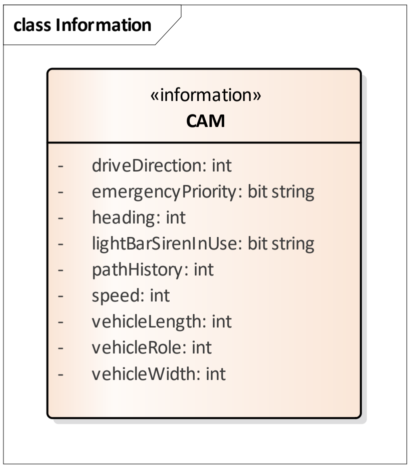


Figure 183: RWW SPBO-CPBO Data

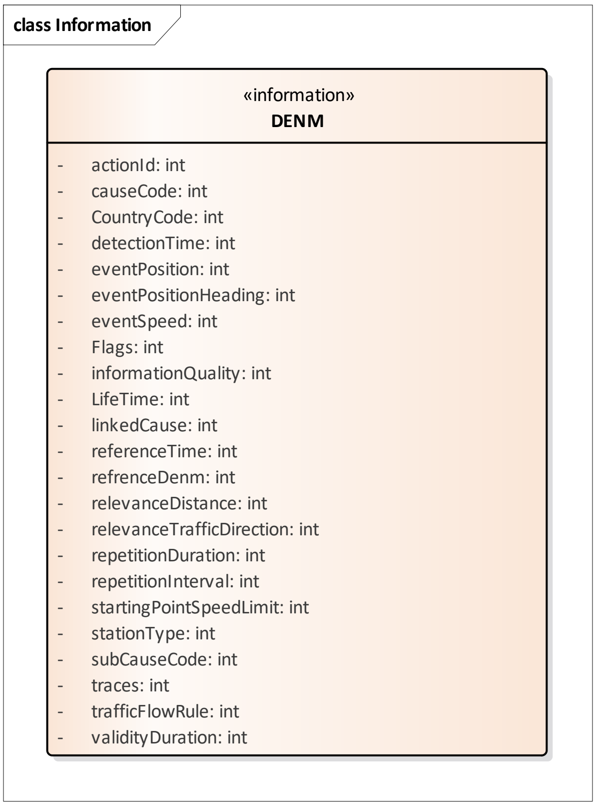


Figure 184: RWW CPBO-PID Data

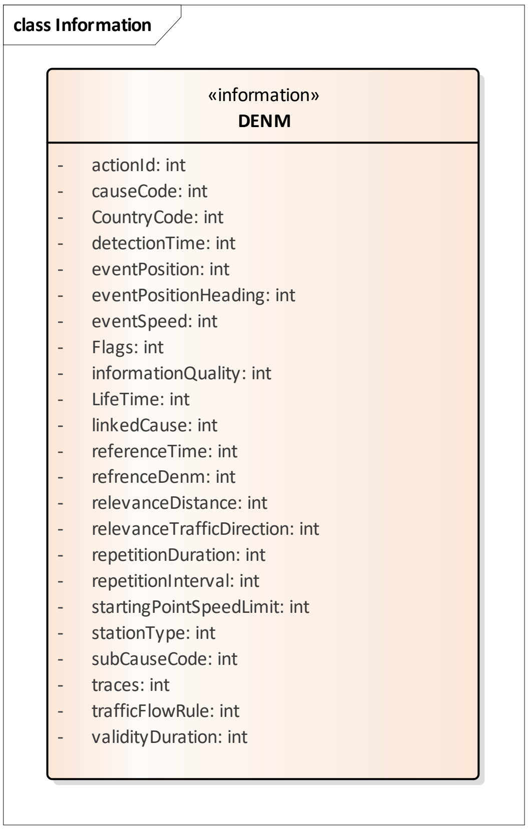


Figure 185: RWW CPBO-RSU Data

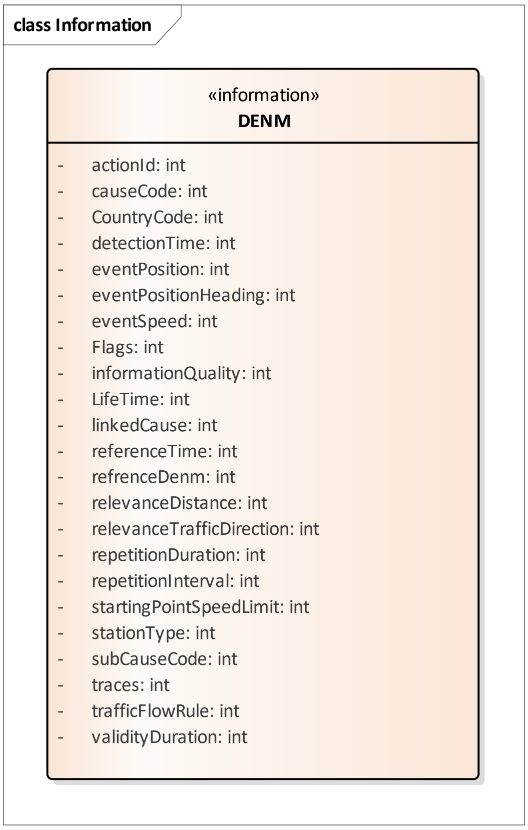


Figure 186: RWW RSU-OBU Data

7.1.5. Road hazard warning

7.1.5.1. Service Diagrams

7.1.5.1.1. Road Hazard Warning Sequence Connected

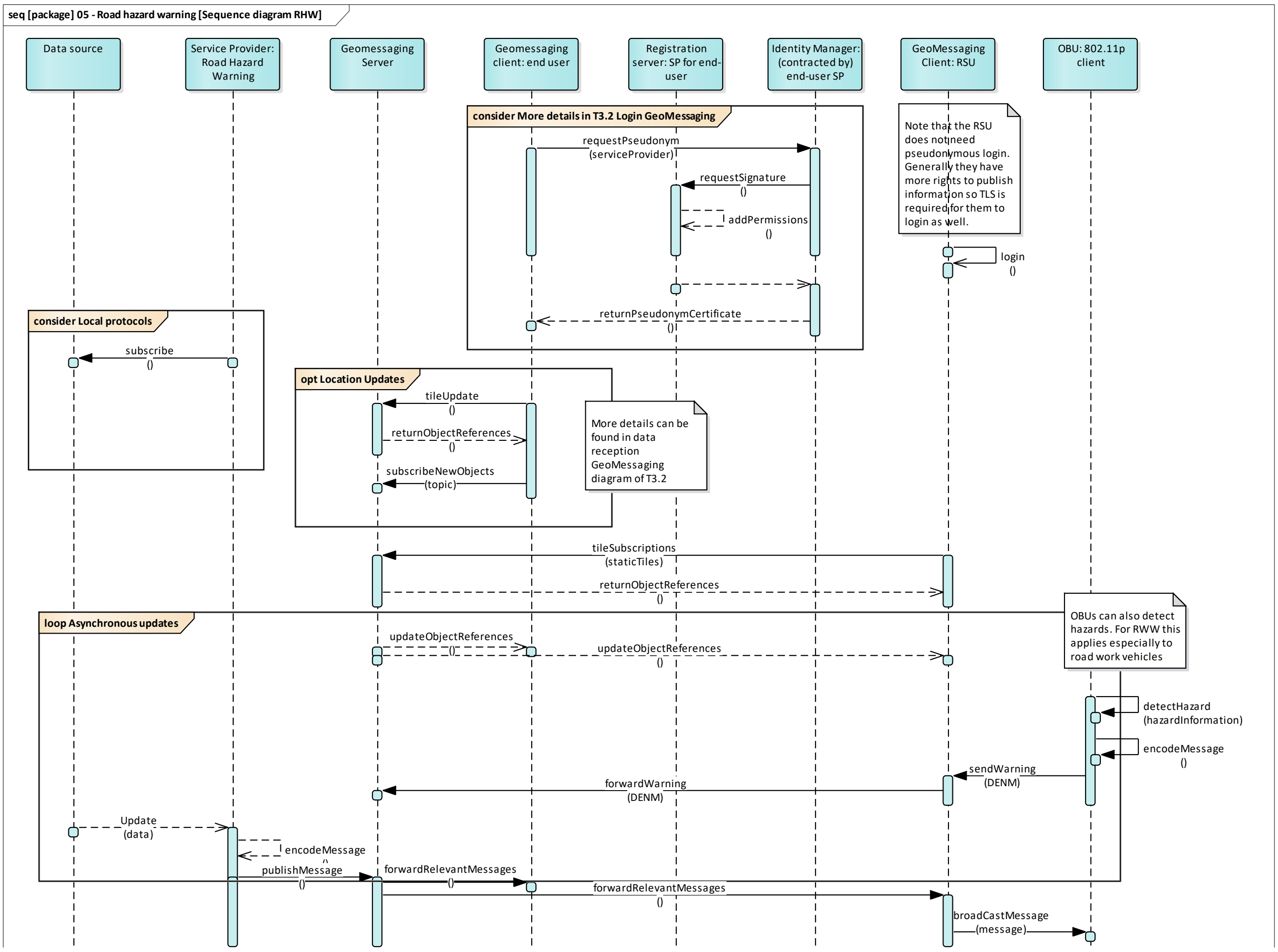


Figure 187: Road Works Warning Sequence Connected

The sequence diagram is divided in several blocks, which also refer to previously defined sequences. For PIDs to connect to the GeoMessaging server (CPBO), it is essential they are logged in. This procedure was defined in D3.2. The same applies to the sequence for PIDs to keep subscribed to location relevant data. The sequence for the connection setup between SPBO and DPBO cannot be described, because it will be depending on local protocols.

After all initialization, the basic information flow starts at the DPBO, this entity will send a new or updated road hazard. This is then translated by the SPBO into a valid DENM message and published in the CPBO (GeoMessaging server). The CPBO will forward the data to all subscribed clients, these can be either PIDs or RSUs in the relevance area. In case of an RSU, the message will also be broadcasted locally over 802.11p in order for OBUs to receive them. The last step is that both the GeoMessaging client (PID) and OBU should decode the message (for example using a C-MobILE SDK) and display it in a comprehensible way to the end user. The OBU can also be a data source and detect a road hazard. In such case it encodes a DENM and broadcasts it locally. Both RSU (shown in diagram) and OBU can forward these messages to the CPBO for further dissemination.

7.1.5.2. Service Datatypes

Will futher described in WP 5.

7.1.6. Emergency Vehicle Warning

7.1.6.1. Service Diagrams

7.1.6.1.1. UC06.1 “Emergency Vehicle Warning” (connected)

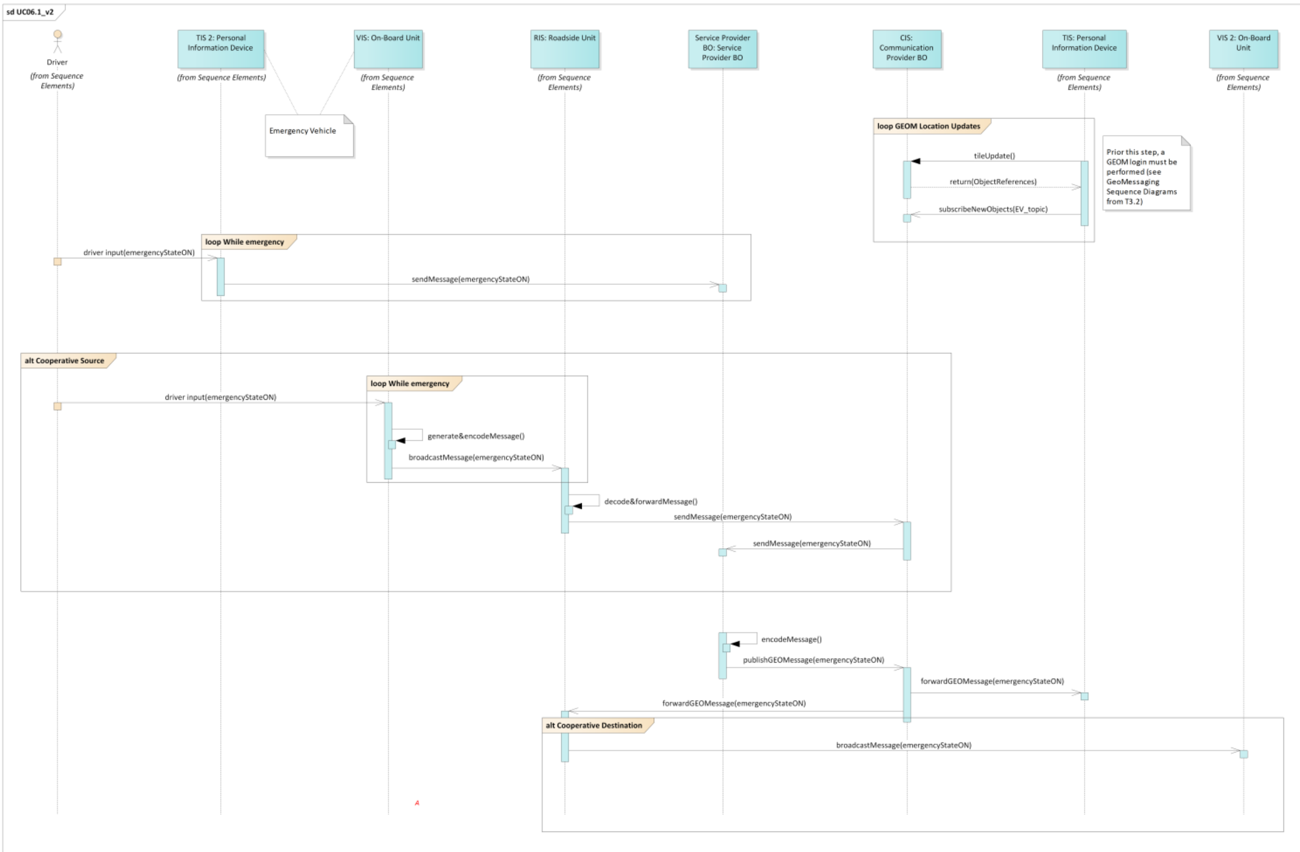


Figure 188: UC06.1 Emergency Vehicle Warning (connected)

The connected case starts from the PID sending the emergency vehicle position (CAM message) directly to the SPBO. The Service Provide Back Office forwards the CAM message to the Communication Provider Back Office in order to disseminate the message to other PIDs in the area. At the same time, the CPBO can also receive the CAM messages sent by cooperative nodes from the RSU. In any of the cases, the information is sent using GeoMessaging to the connected devices using a cellular communication and/or to the cooperative vehicles using an ITS G5 communication. Following this approach, the information from a connected source can reach cooperative vehicles and vice versa.

The connected devices need to be previously subscribed to the EVW service′s events in the GeoMessaging server to properly receive this information.

7.1.6.1.2. UC06.1 "Emergency Vehicle Warning" (cooperative)

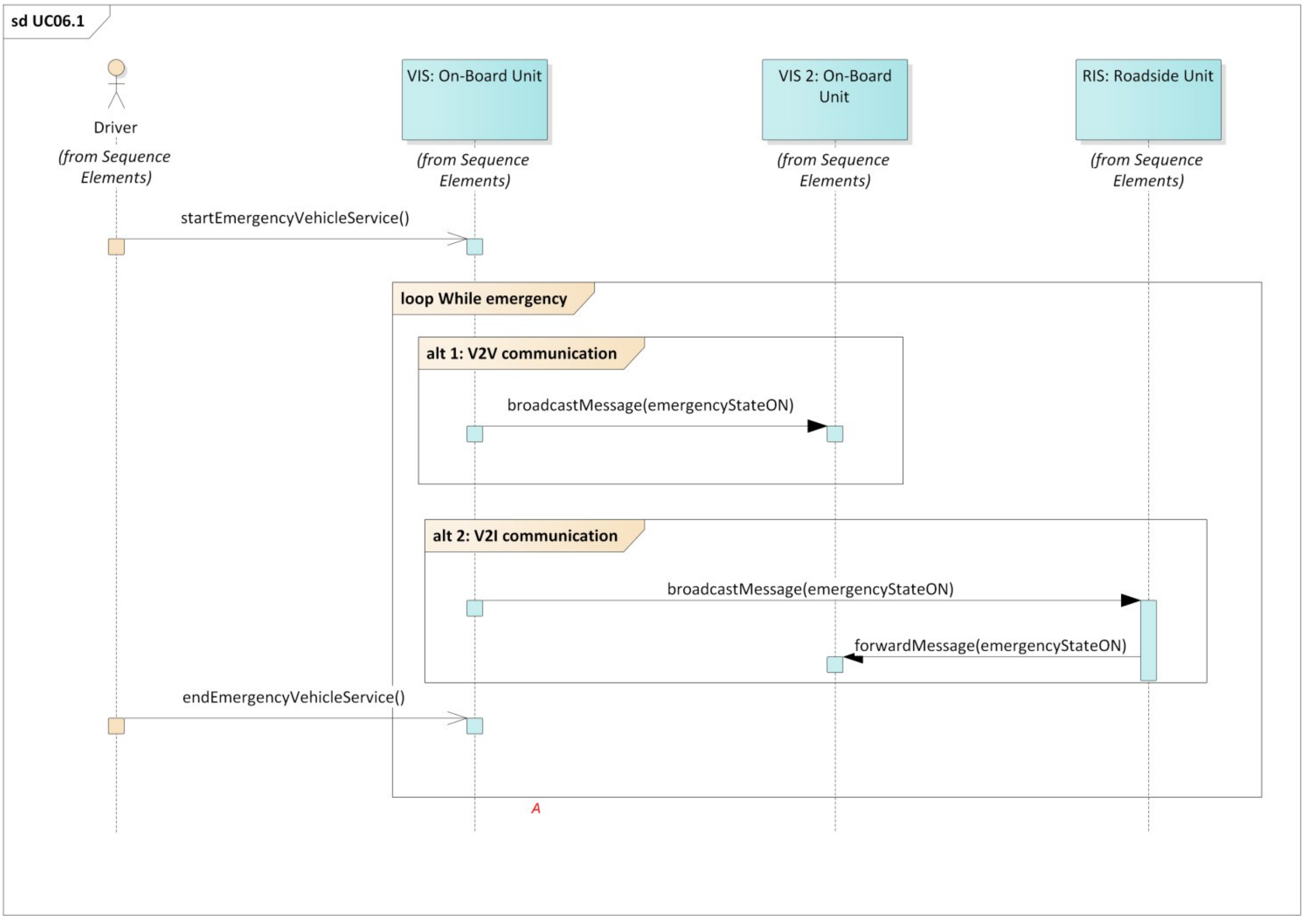


Figure 189: UC06.1 Emergency Vehicle Warning (cooperative)

The fully cooperative use case comprises only ITS G5 components. The CAM messages are broadcasted by the OBU installed in the emergency vehicle and reach other cooperative entities (OBUs and RSUs) using ITS G5. The cooperative vehicles can treat and show the driver the corresponding EV warning while the RSU must transform the CAM to a DENM messages and broadcast it downwards to the cooperative vehicles. Usually the RSU is used to disseminate a message in a zone where the emergency vehicles′ OBU cannot reach (out of communication range).

7.1.6.2. Service Datatypes

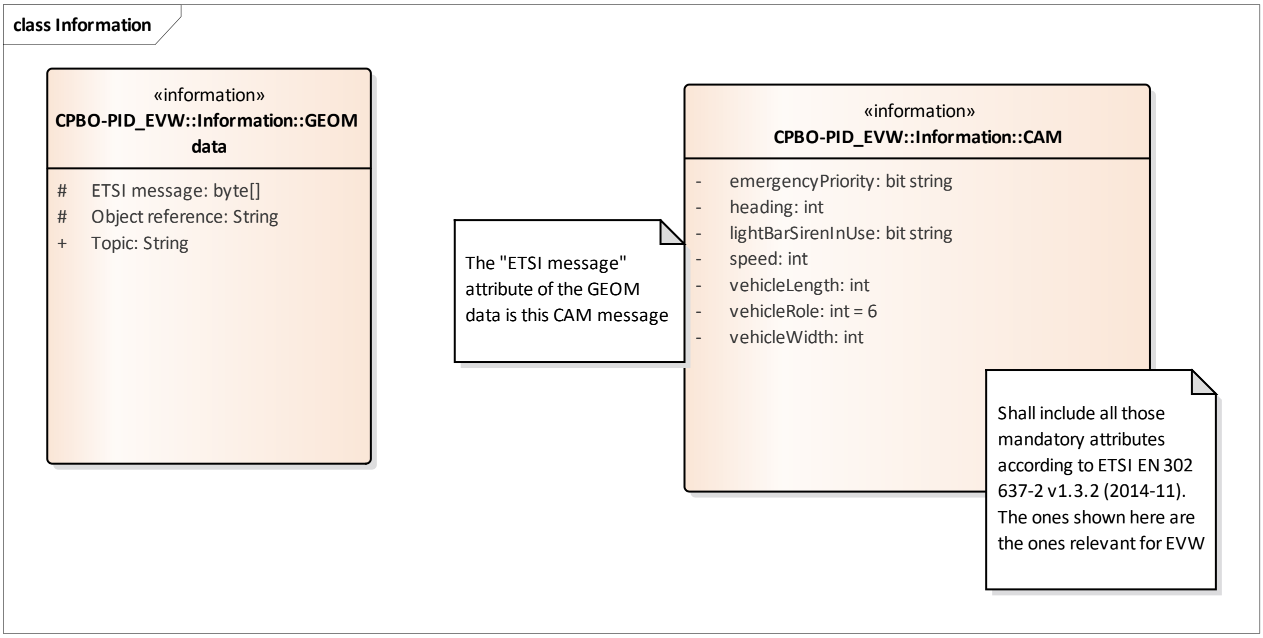


Figure 190: EVW CPBO-PID Data

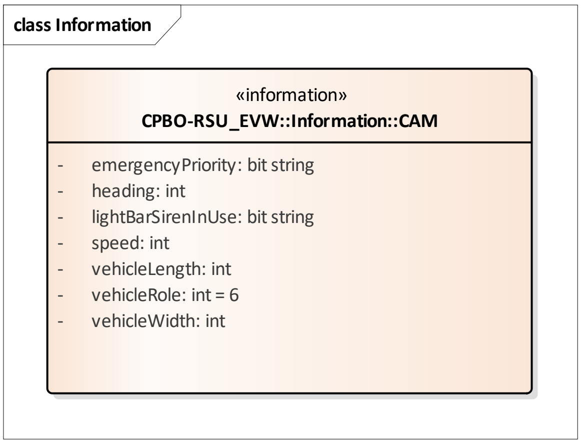


Figure 191: EVW CPBO-RSU Data

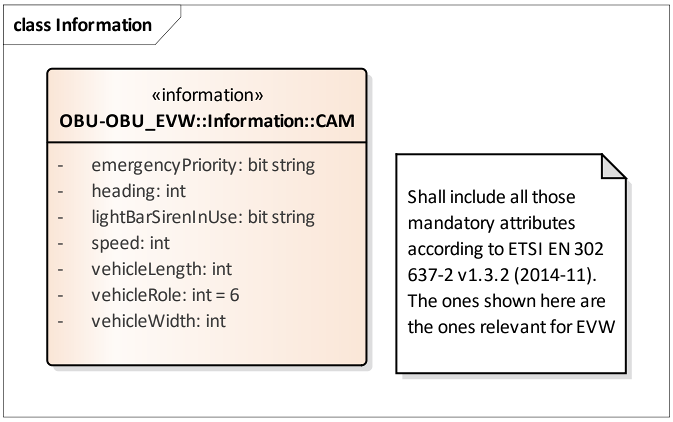


Figure 192:EVW OBU-OBU data

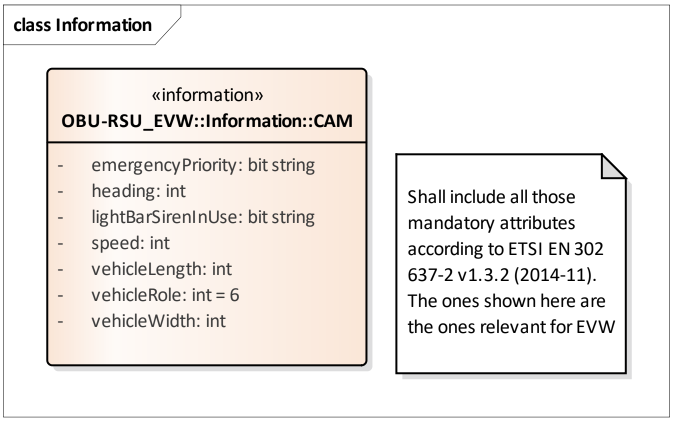


Figure 193: EVW OBU-RSU data

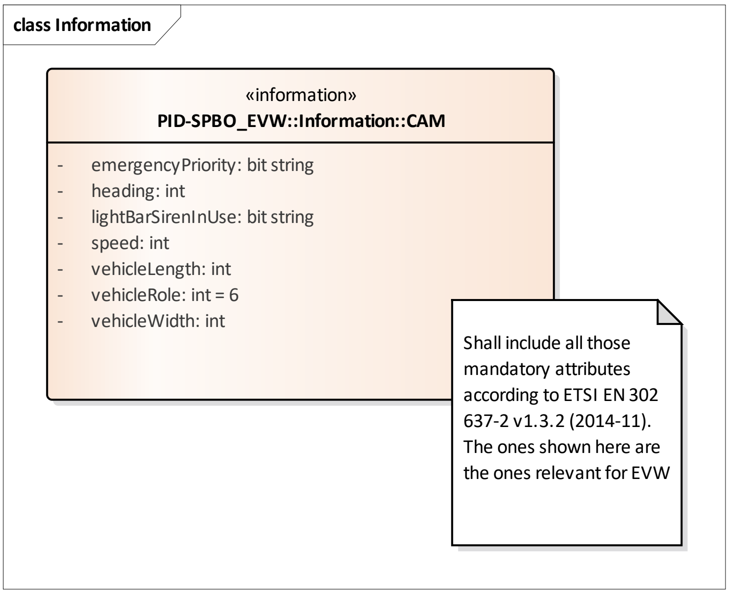


Figure 194: EVW PID-SPBO data

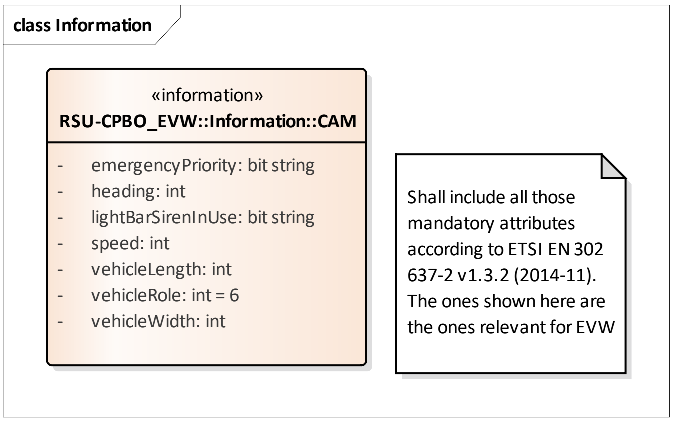


Figure 195: EVW RSU-CPBO data

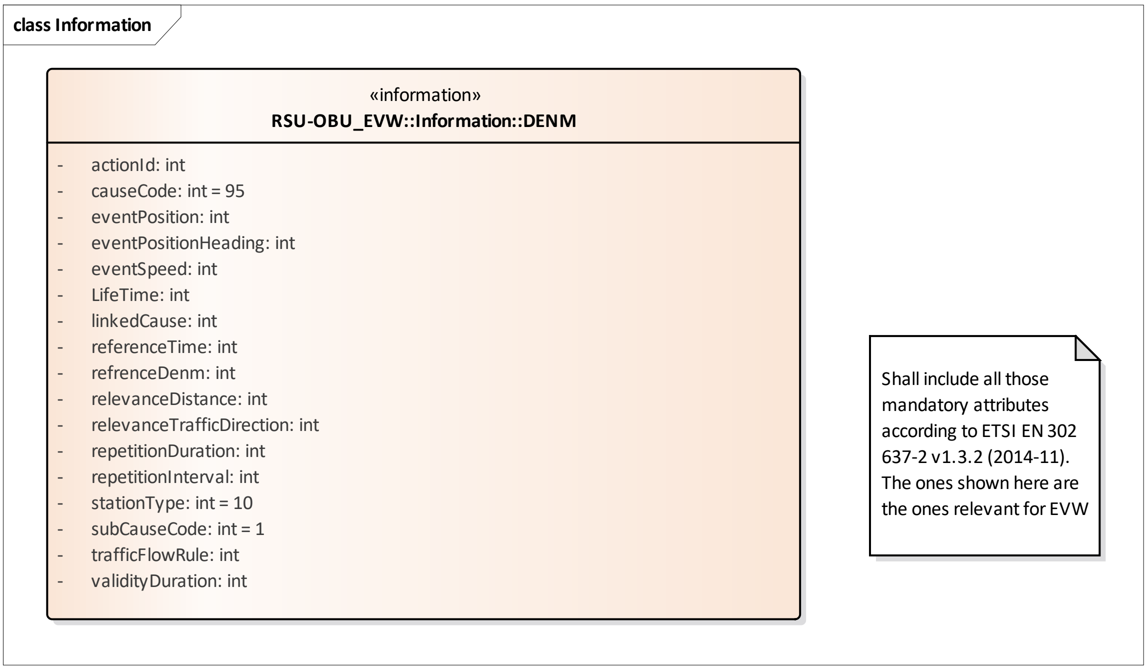


Figure 196: EVW RSU-OBU data

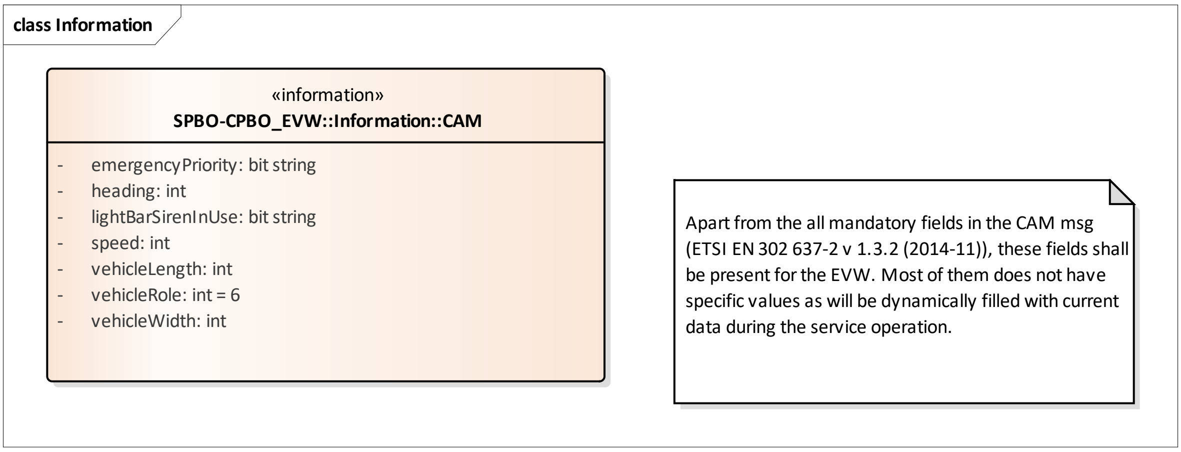


Figure 197: EVW SPBO-CPBO data

7.1.7. Signal Violation Warning

7.1.7.1. Service Diagrams

7.1.7.1.1. UC07.1 Red light violation warning sequence Host

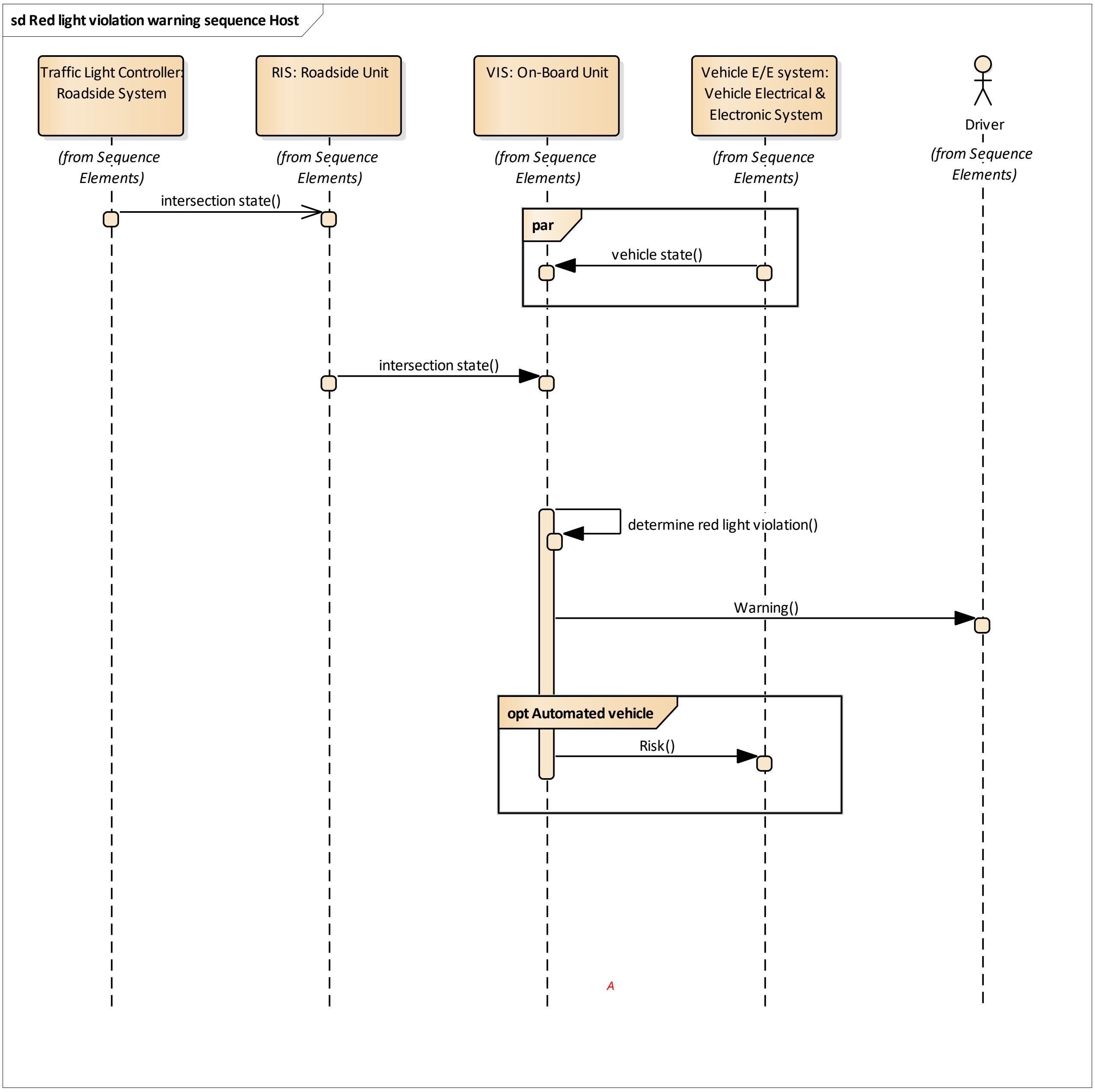


Figure 198: Red light violation warning sequence Host

The Roadside System, which becomes a Traffic Light Controller in this case, provides the intersection state (traffic lights sequence) to the Roadside Unit which forwards this information to the OBU via ITS G5 communication. The OBU uses the own vehicle state to determine a violation on the red light. If the vehicle will violate the red light, then it warns the driver.

7.1.7.1.2. UC07.1 Red light violation warning sequence Remote

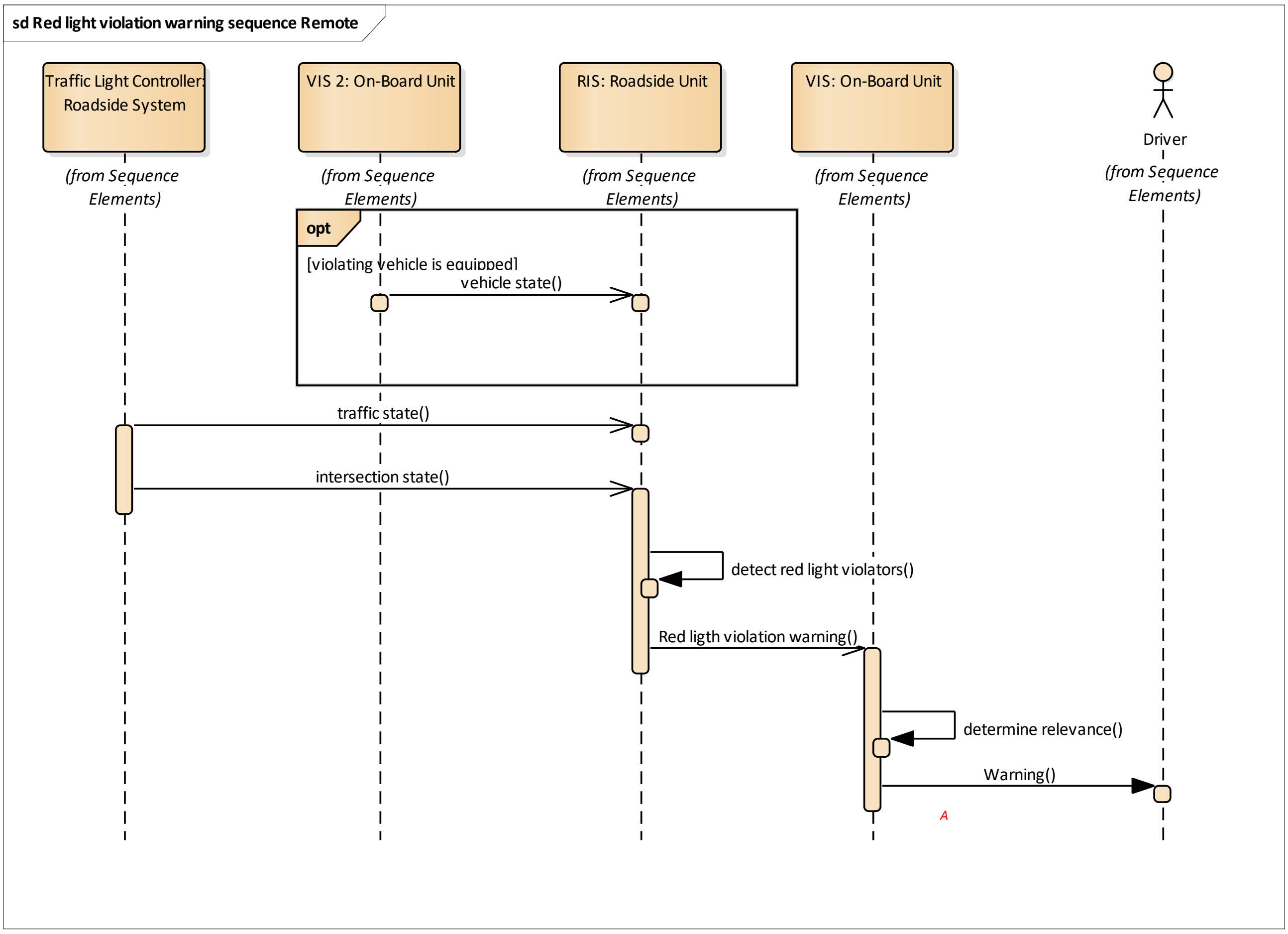


Figure 199: Red light violation warning sequnce Remote

For the case that the violation is determined remotely by the RSU, the vehicle may share information about its state to the RSU, which also gathers the Traffic Light Information, and then it proceeds with the calculations. Otherwise the violation is detected from the information distributed by the RS, which in this case became a camera, sensors or any other detection system able to determinate red light violations. If a violation is detected warning is send to the OBUs nearby.

7.1.7.2. Service Datatypes

The following diagrams describe the datatypes and information exchanged between components, which belongs to the Information Viewpoint of the architecture. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. For interoperability purposes, the attributes of the messages follow a specific profiling which indicates which ones are used, optional or discarded. The profiling used in C-MobILE follows the indication coming from Talking Traffic and C-ROADS projects.

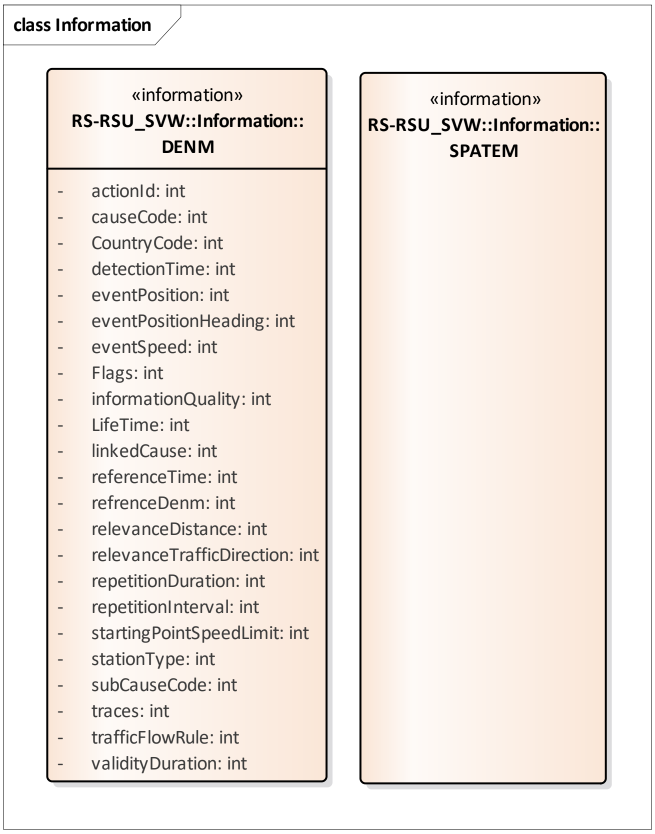


Figure 200: Roadside System to Roadside Unit DENM and SPATEM

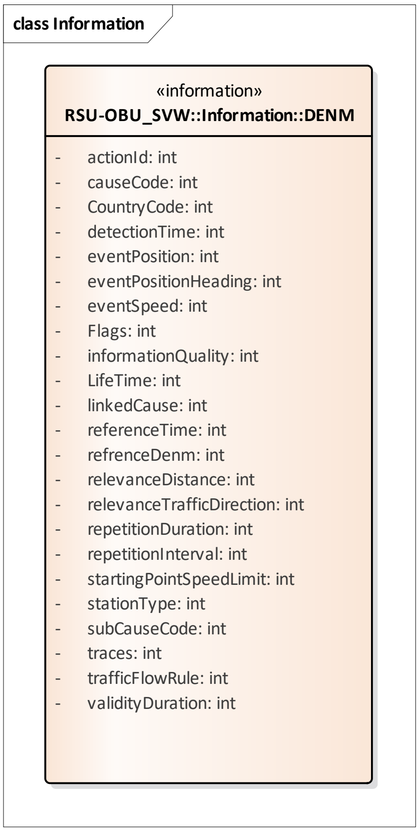


Figure 201:Roadside Unit to On Board Unit DENM

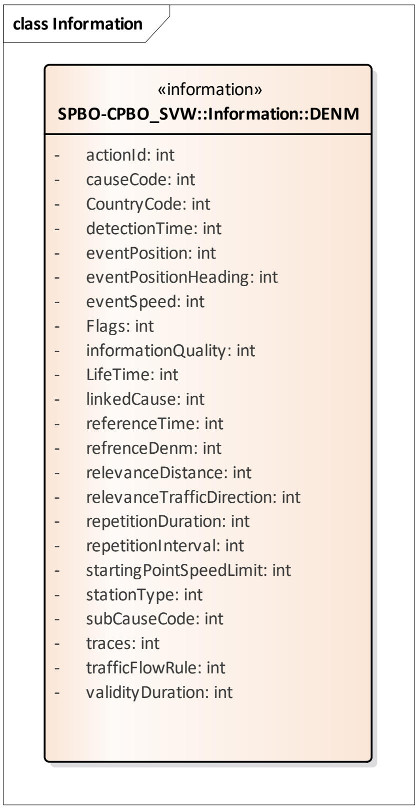


Figure 202: SPBO to CPBO DENM

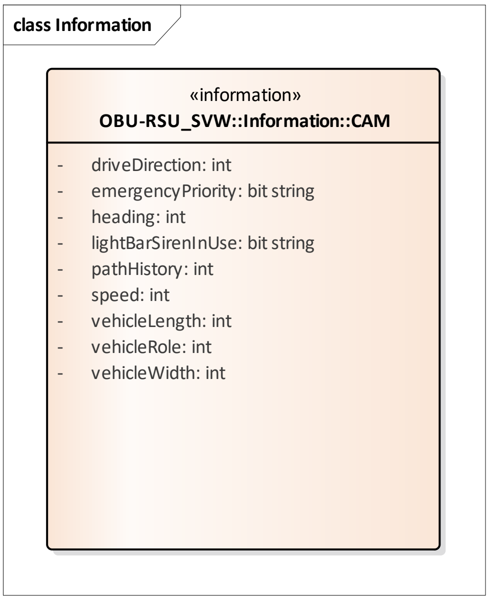


Figure 203: On Board Unit to Roadside Unit CAM

7.1.8. Warning system for pedestrian

7.1.8.1. Service Diagrams

7.1.8.1.1. Warning system for pedestrians without RSU for detection or traffic lights

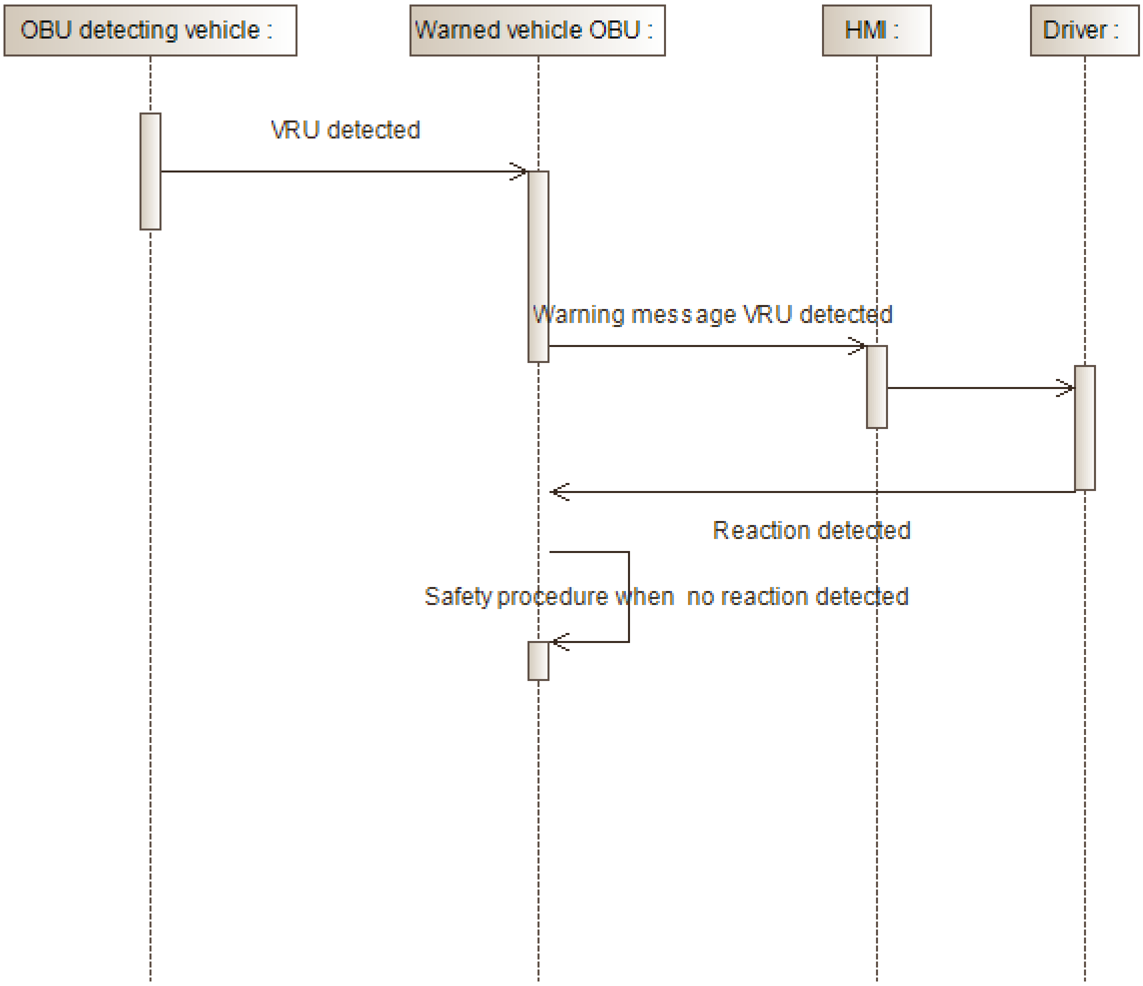


Figure 204: Warning system for pedestrians without RSU for detection or traffic lights

The ego vehicle can be warned by another OBU that there is a VRU detected. This can be a VRU that is outside the detection area of the ego vehicle. Based on the trajectory of VRU and its own trajectory the OBU decides if it is useful to warn the driver. I the driver does not react to the warning the safety protocol is activated.

7.1.8.1.2. Warning system for pedestrians with RSU for VRU detection

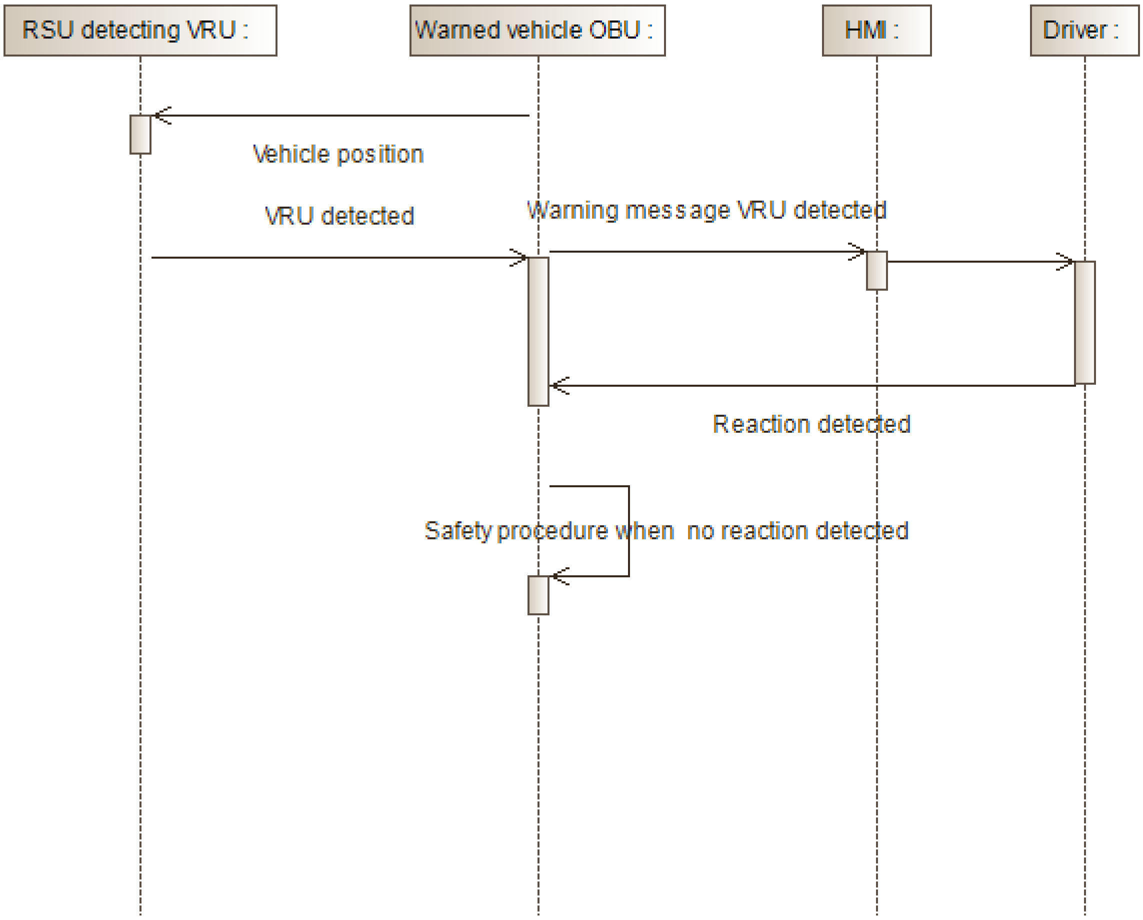


Figure 205: Warning system for pedestrians with RSU for VRU detection

The RSU combines the detection of the VRUs with the trajectory information that it receives from the vehicles. If there is a conflict the RSU sends a message to the OBJ. The DENM message is a DSRC broadcasted message that is received by all OBJ in the neighborhood. The OBJ calculates if the DENM is relevant for him. If so, he informs the driver via the HMI. If no reaction from the driver is detected the safety protocol is activated.

7.1.8.1.3. Warning system for pedestrians Signaled crossing without RSU for VRU detection

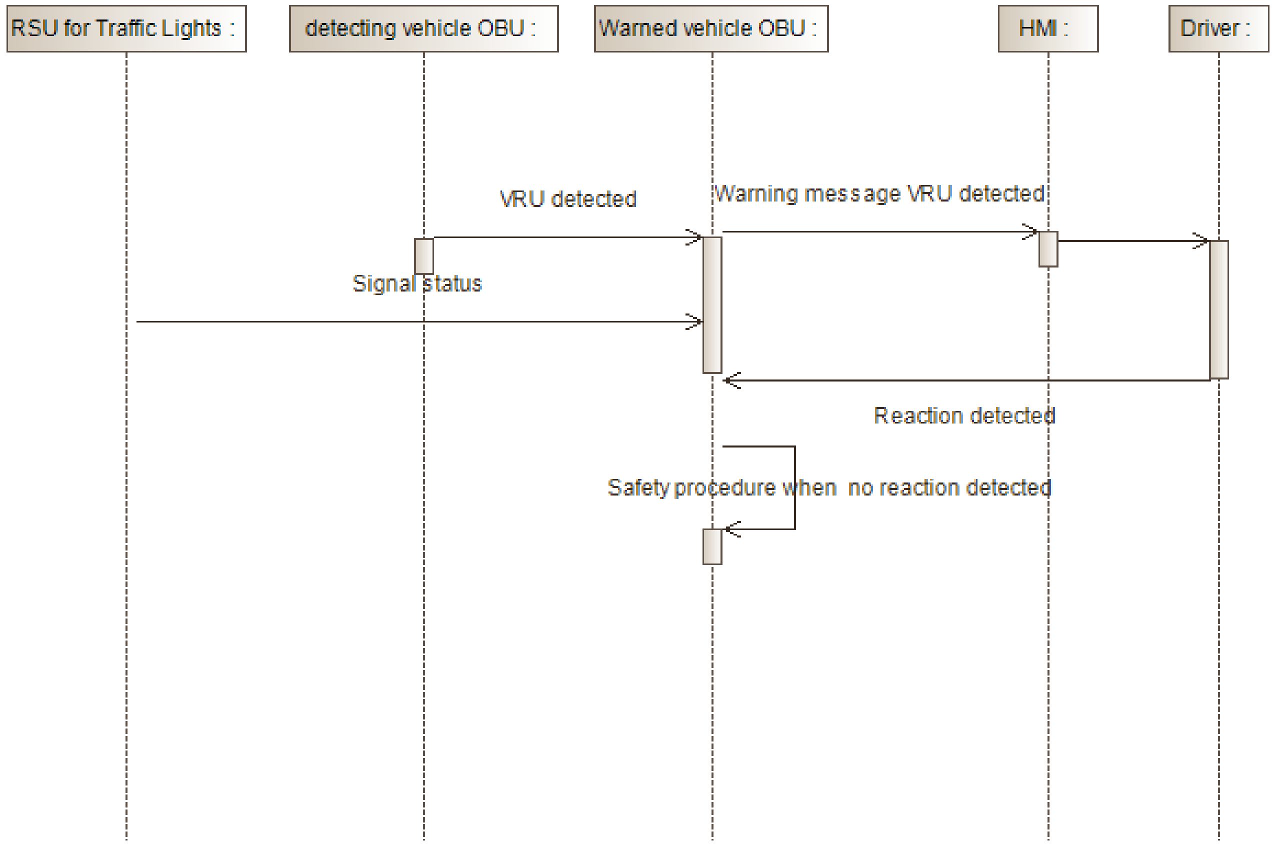


Figure 206: Warning system for pedestrians Signaled crossing without RSU for VRU detection

The OBU takes into account the status of the traffic lights

7.1.8.1.4. Warning system for pedestrians Signaled crossing with RSU for VRU detection

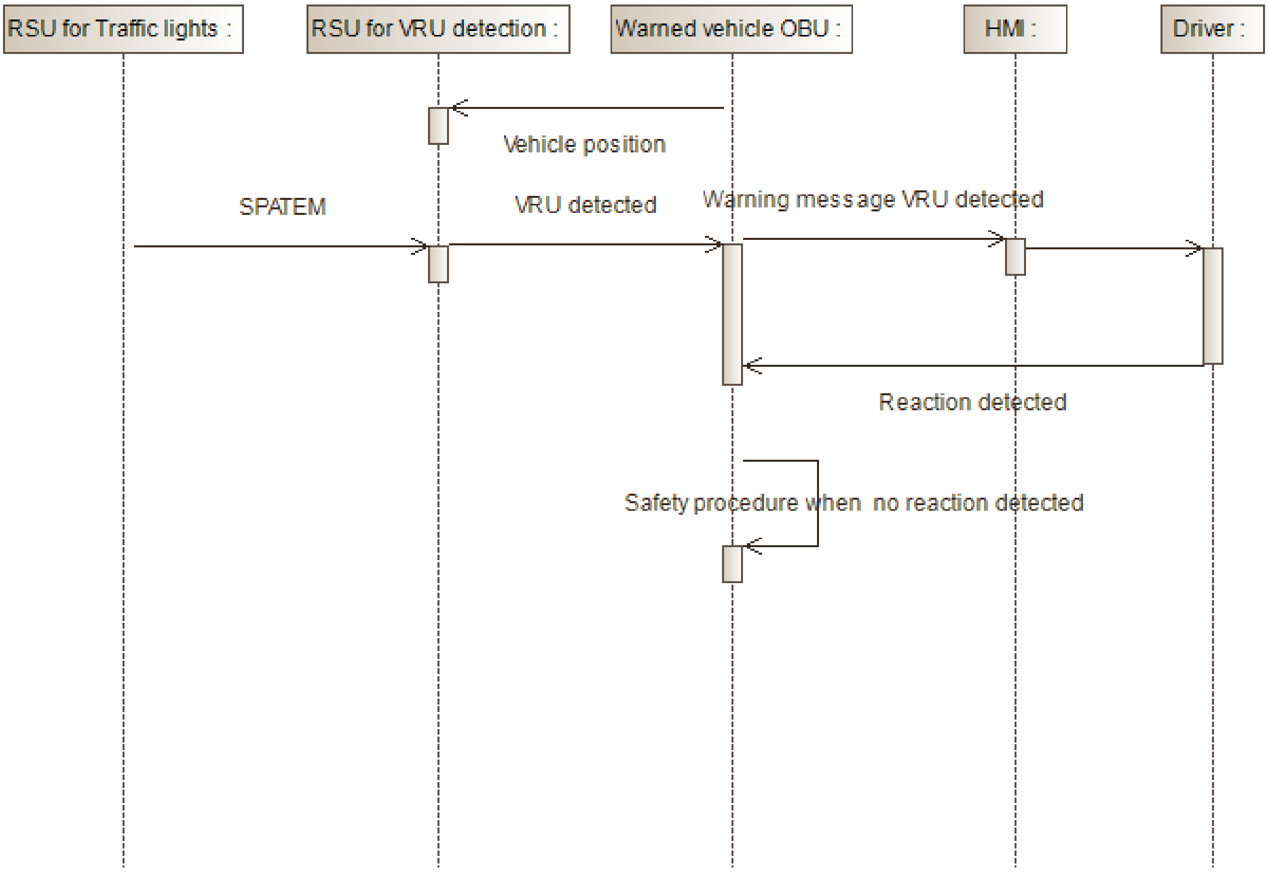


Figure 207: Warning system for pedestrians Signaled crossing with RSU for VRU detection

The RSU uses the information from the TLC and the OBU to decide if it is useful to inform the OBU about a detected VRU. The OBU than operates as in the previous sequence diagrams.

7.1.8.1.5. Warning system for pedestrians Signaled crossing with RSU for VRU detection with cellular communication to the OBU

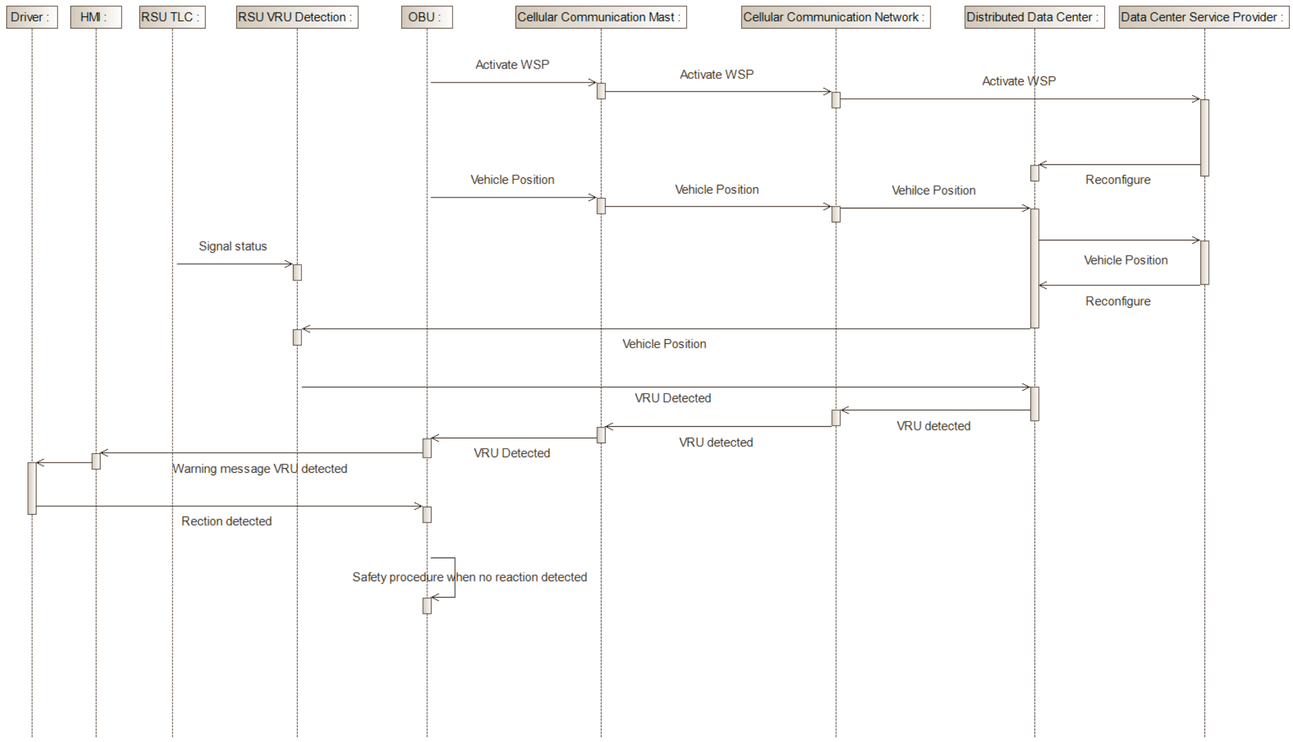


Figure 208: Warning system for pedestrians Signaled crossing with RSU for VRU detection with cellular communication to the OBU

7.1.8.2. Service Datatypes

Will futher described in WP 5.

7.1.9. Green priority

7.1.9.1. Service Diagrams

7.1.9.1.1. Green Priority Sequence

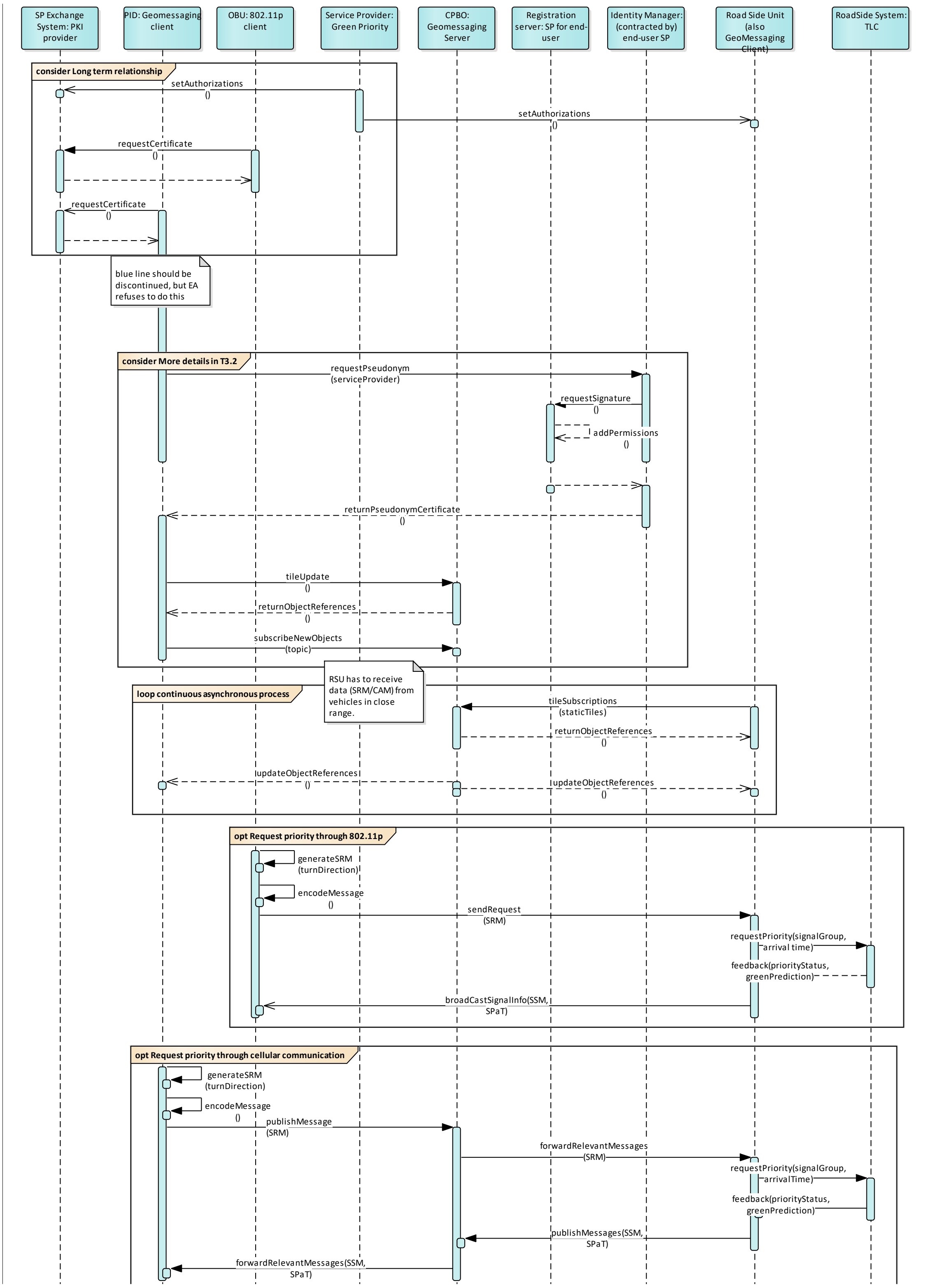


Figure 209: Green Priority Sequence

The sequence diagram is divided in several blocks, which also refer to previously defined sequences. The first block considers long term relationships required for authorization and result in both OBU and PID being able to request PKI certificates to sign their messages of the data flow. For PIDs to connect to the GeoMessaging server (CPBO), it is essential they are logged in. This procedure was defined in D3.2. The same applies to the RSU, but in that case it doesn't require a pseudonym. The RSU also needs to be subscribed to location relevant data, which can also be considered an initialization sequence, since the location of the RSU doesn't change during runtime.

After all initialization, there are two sequences to request priority, one over 802.11p and one for cellular communications. The 802.11p requests priority directly at the RSU, while for cellular the data goes through the CPBO. The communication to the traffic light controller (the RS) will vary per deployment site and is out of scope of C-MobILE to standardize due to high replacement costs, service providers have to implement their own interface adapters on the RSU.

7.1.9.2. Service Datatypes

Will futher described in WP 5.

7.1.10. GLOSA

7.1.10.1. Service Diagrams

7.1.10.1.1. UC 10.1 Optimized Driving Experience with GLSOA

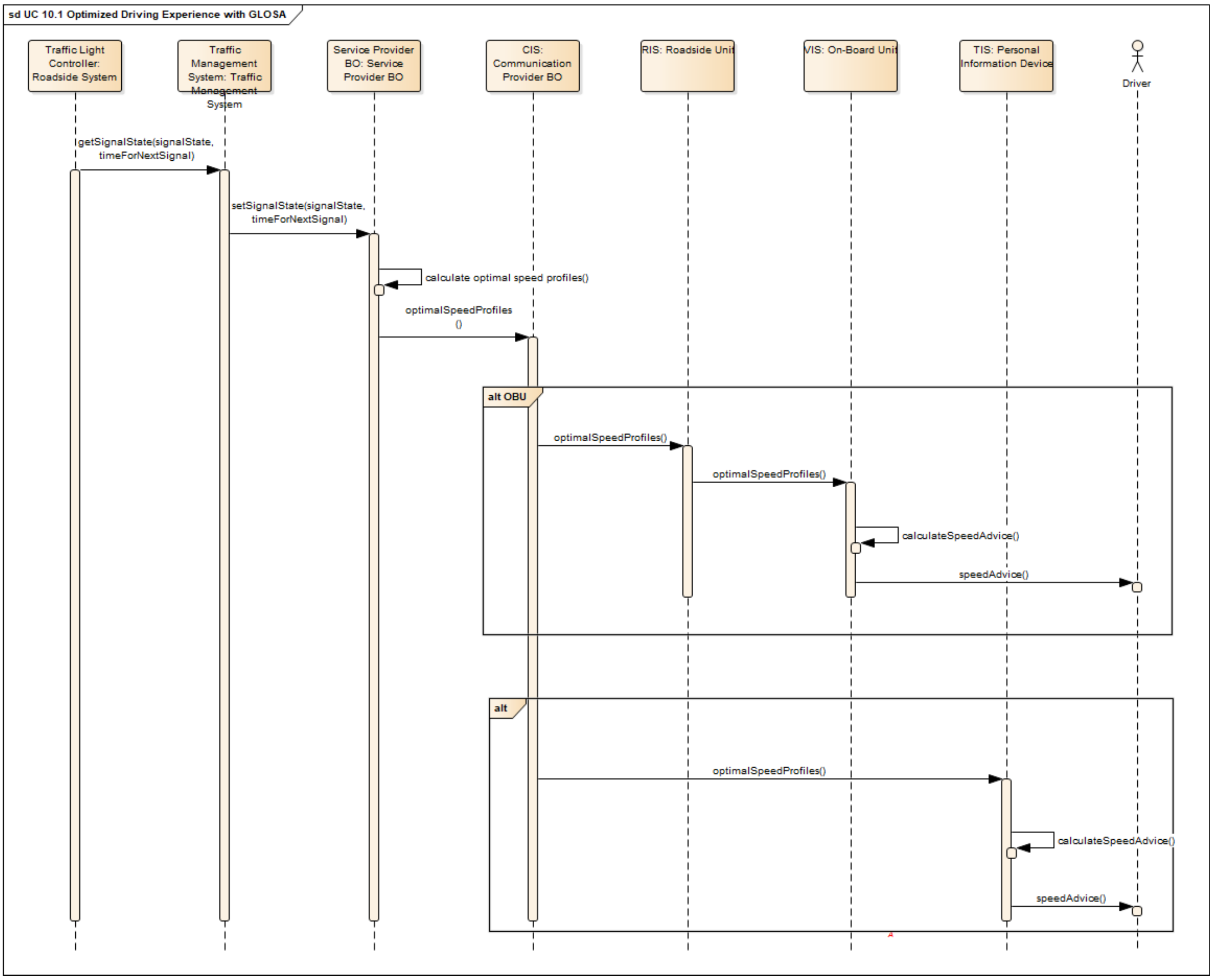


Figure 210: Sequence diagram name

The GLOSA case starts from the Traffic Light Controller that is a Roadside System (RS) transmitting the current signal state together with the time for the next signal as a DENM to the TMS. The TMS forwards this to the SP BO, where optimal speed profiles are calculated. The optimal speed profiles are transmitted to the CP BO that in turn forwards it to the RSUs in the vicinity. The RSU then disseminates the speed profile to the OBUs in the vicinity of the RSU. The OBU then calculates the speed advice and displays it to the driver. At the same time, the CP BO can directly disseminate the speed profiles to PIDs, where a speed advice is calculated and displayed to the driver.

7.1.10.2. Service Datatypes

The following diagrams describes the datatypes and information exchanged between components. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. The range of attributes and information inside those message types are extensive and mostly out of scope, therefore the diagrams may only contain the necessary attributes with specific values.

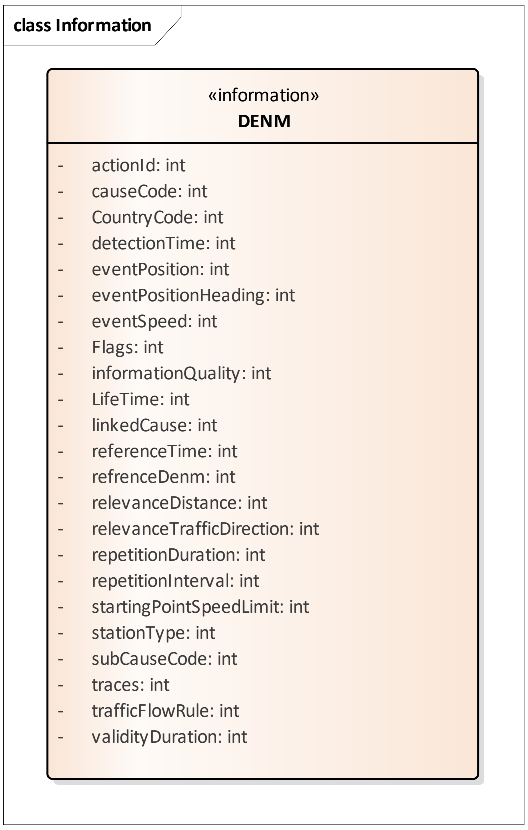


Figure 211: GLOSA RS-TMS

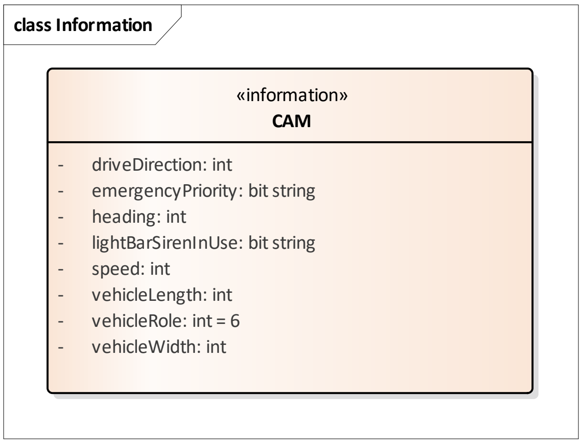


Figure 212: GLOSA CPBO-RSU

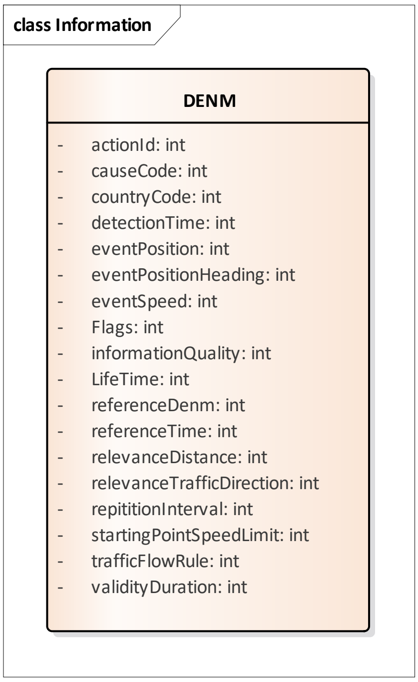


Figure 213: GLOSA RSU-OBU

7.1.11. Cooperative traffic light for pedestrian

7.1.11.1. Service Diagrams

7.1.11.1.1. UC11.1: C-TL for Pedestrians - Cooperative

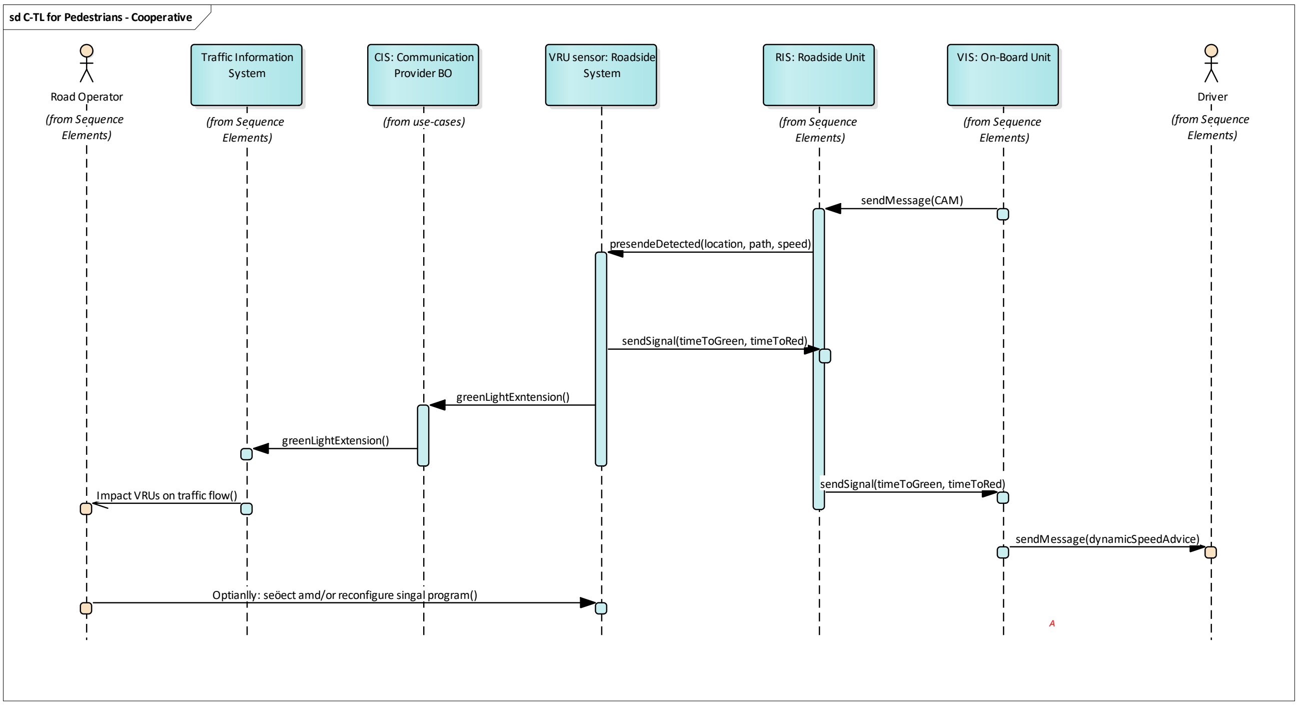


Figure 214: Sequence diagram UC11: C-TL for Pedestrians - Cooperative

The above sequence diagram is demonstrating the C-TL for Pedestrians in Cooperative mode.

7.1.11.1.2. UC11.2: C-TL for Pedestrians - Connected

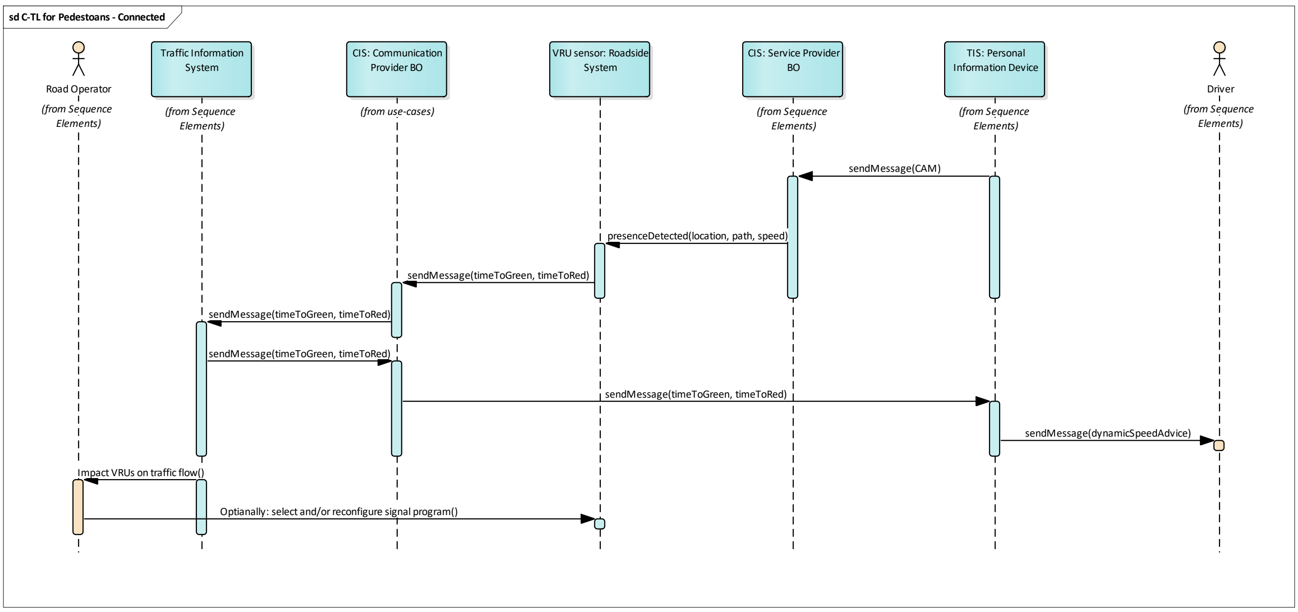


Figure 215: Sequence diagram UC11: C-TL for Pedestrians - Connected

The above sequence diagram is demonstrating the C-TL for Pedestrians in Connected mode.

7.1.11.2. Service Datatypes

Will be futher described in WP 5.

7.1.12. Flexible infrastructure

7.1.12.1. Service Diagrams

7.1.12.1.1. UC12.1- Dynamic Lane Management - Lane Status Information

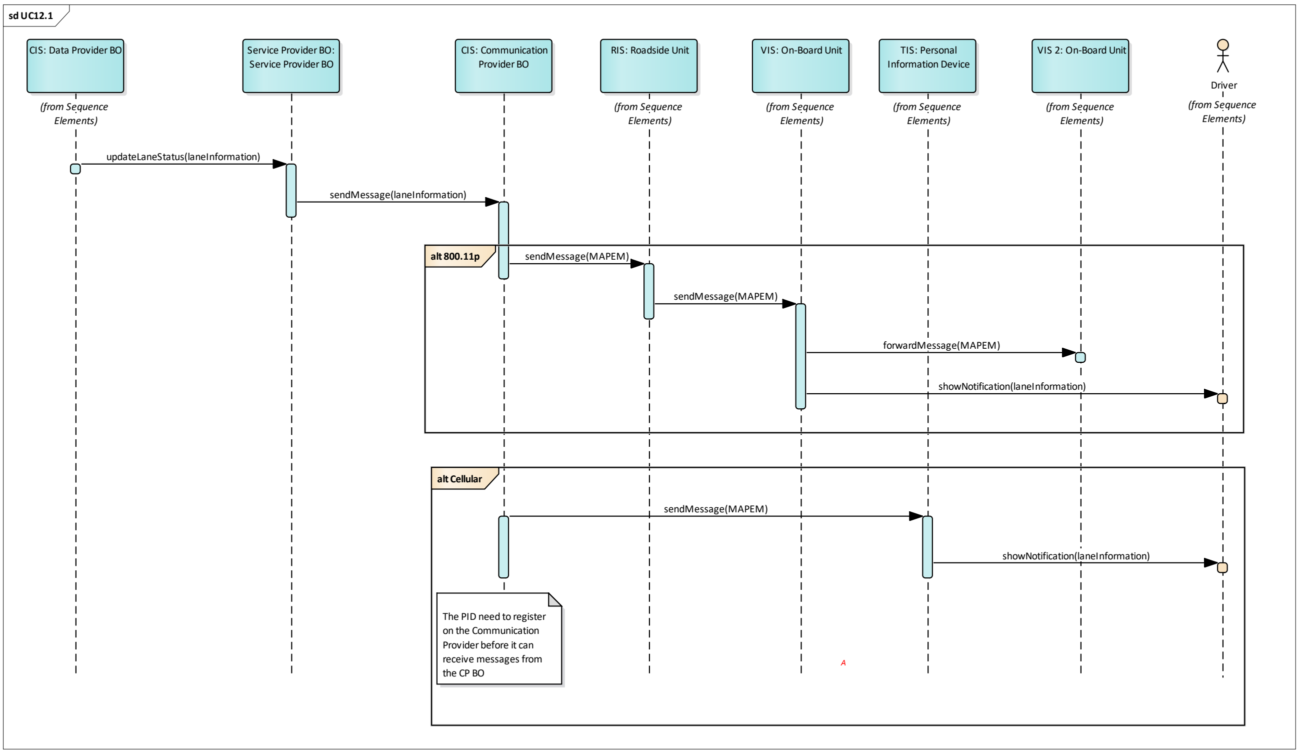


Figure 216: Dynamic Lange Management lane Status information Sequence

For the Dynamic Lane Management Use case the Service provider uses the lane information provided by the DPBO to inform the driver about the lane status. There are two scenarios for that case. The first one is to distribute the lane status over ETSI ITS-G5. Therefore, the SPBO is sending a MAPEM to the OBUs through the CPBO to the RSU, which forwards the message to the OBUs.

For cellular case the PID needs to register itself at the CPBO to receive information from the SPBO.

7.1.12.1.2. UC12.2 - Dynamic Lane Management - Reserved Lane (without probe vehicle data alt: with probe vehicle data)

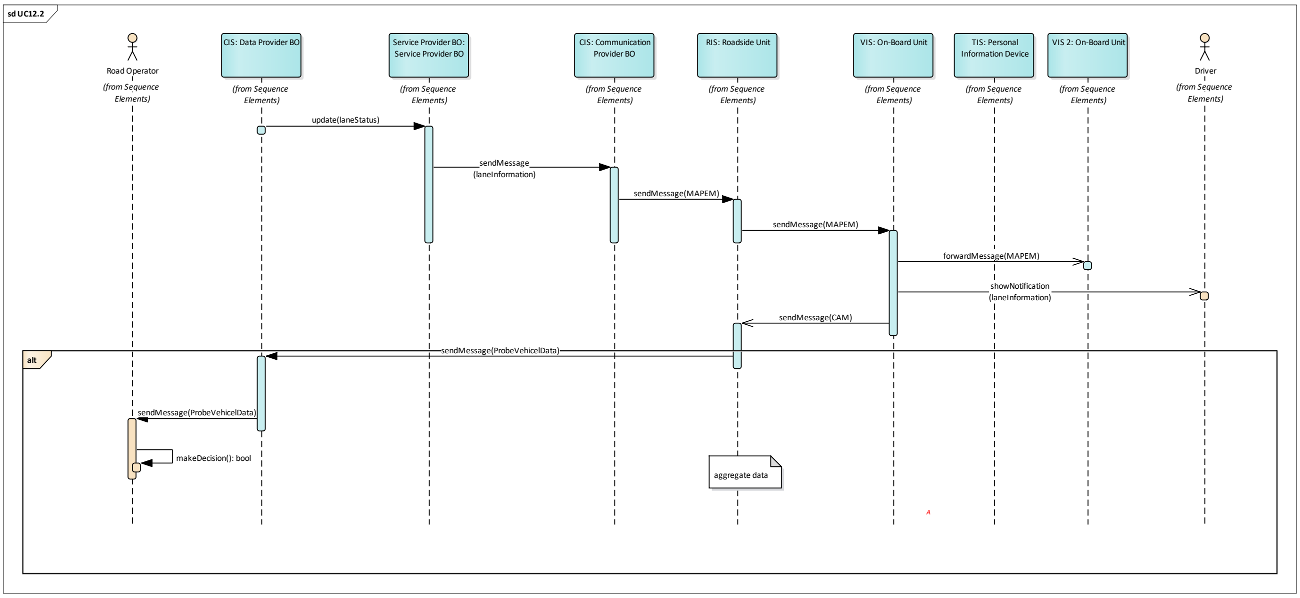


Figure 217: Dynamic Lane Management - Reserved Lane (with and without probe vehicle data)

The SPBO receives the lane status from the DPBO and sends it through the CPBO to the RSU. The RSU is then sending a MAPEM to the OBUs. The message gets distributed to other vehicles as well.

To provide probe vehicle data the OBUs sending CAMs to the RSU, which aggregate the data before it sends the data back to the DPBO. Based on the received information, the road operator is able to make a decision which lane should be opened or closed.

7.1.12.2. Service Datatypes

Will futher described in WP 5.

7.1.13. In–vehicle signage

7.1.13.1. Service Diagrams

7.1.13.1.1. UC13.1 & UC13.2 In-Vehicle Signage

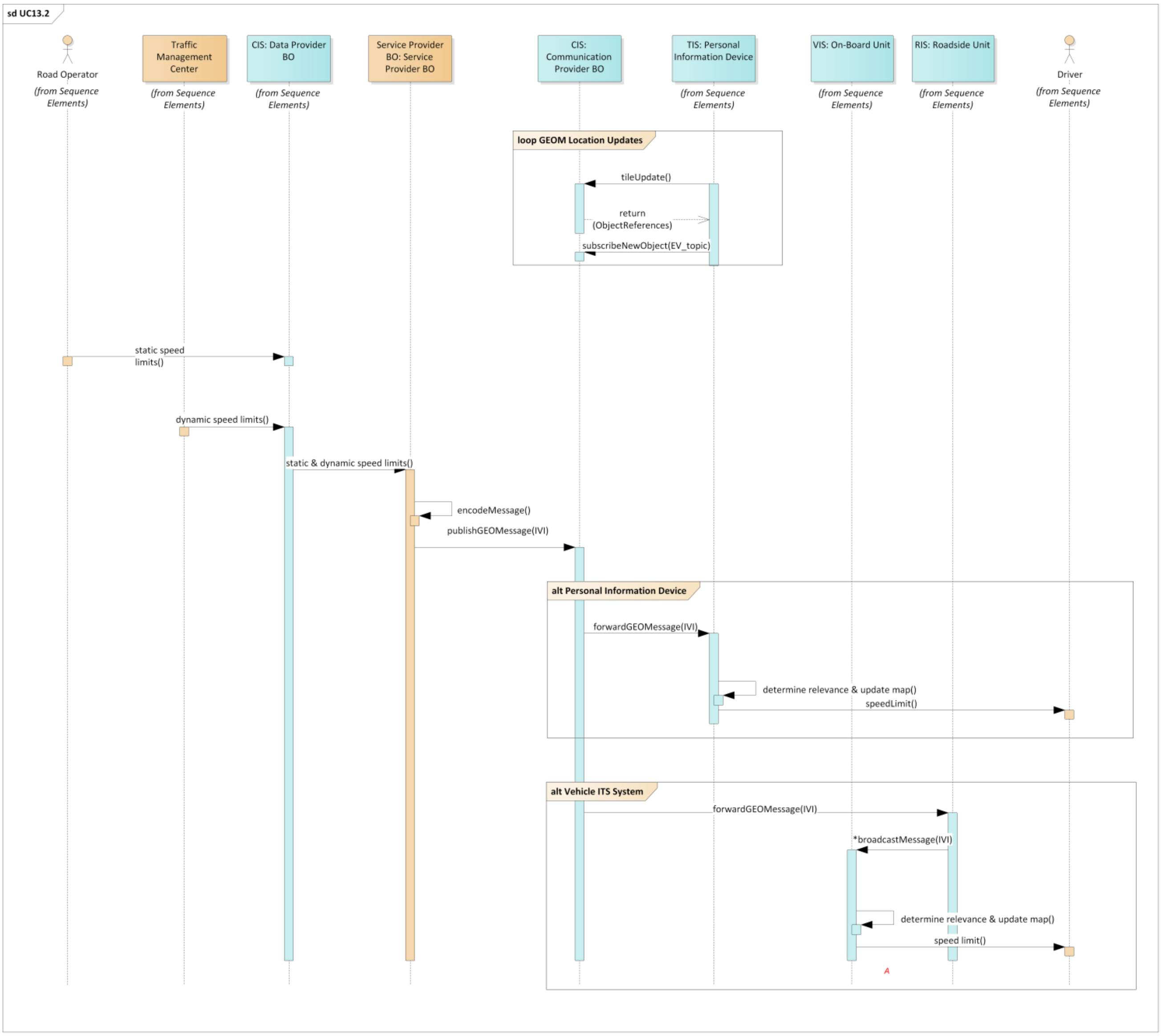


Figure 218: In-Vehicle Signage

Both use cases share the same architecture components so just one diagram is needed to describe the services.

The road operator, who is the TMS manager, provides the IVS information to the **Data Provider Back Office (DP BO)** or directly to the **Service Provider Back Office (SPBO),** usually in DATEX or JSON format. The **SP BO** is in charge of translating the information received in a standard IVIM message that is forwarded to the **Communication Provider Back Office (CPBO)**, where there are two dissemination options, the cooperative and the connected.

In the cooperative dissemination, the **CPBO** determines the RSUs that will be covering the IVS relevance area and forward the IVIM message to them. Then, the **RSU**s broadcast the IVIM message to reach the equipped vehicles.

In the connected dissemination, the **CPBO** matches the connected devices location (tile-based) with the IVS area and transmits the IVIM message with a message queuing protocol like MQTT. It is important to mentions that the connected devices (receivers) need to be subscribed to the GeoMessaging server for the IVS service in advance, once they enter in the IVS relevant areas.

7.1.13.2. Service Datatypes

Will futher described in WP 5.

7.1.14. Mode & trip time advice

7.1.14.1. Service Diagrams

7.1.14.1.1. Mode & trip time advice based on ARC-IT

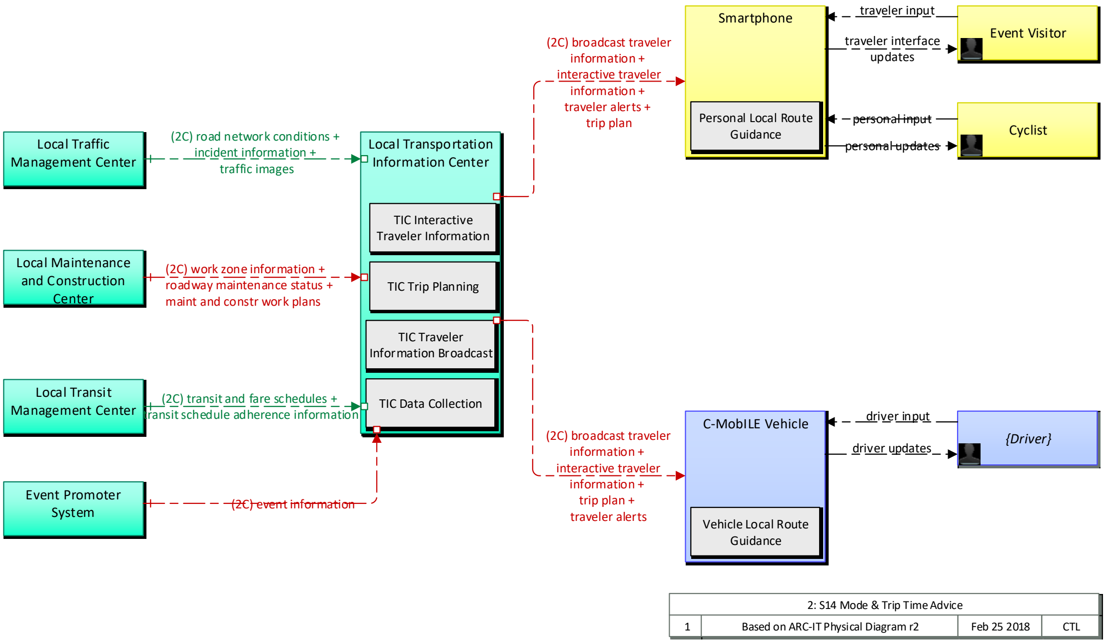


Figure 219: Mode & trip time advice based on ARC-IT reference architecture

The diagram above is an aligned Version of Mode & trip time advice based on ARC-IT reference architecture. The flows between two components are called triples and consists of a source, destination and information. A further description of the triples can be found on the ARC-IT website[9].

7.1.14.2. Service Datatypes

Will futher described in WP 5.

[9] http://htg7.org/html/analysis/triplessolutions.html

7.1.15. Probe Vehicle Data

7.1.15.1. Service Diagrams

7.1.15.1.1. UC15.1 & UC15.2 Probe Vehicle Data (connected)

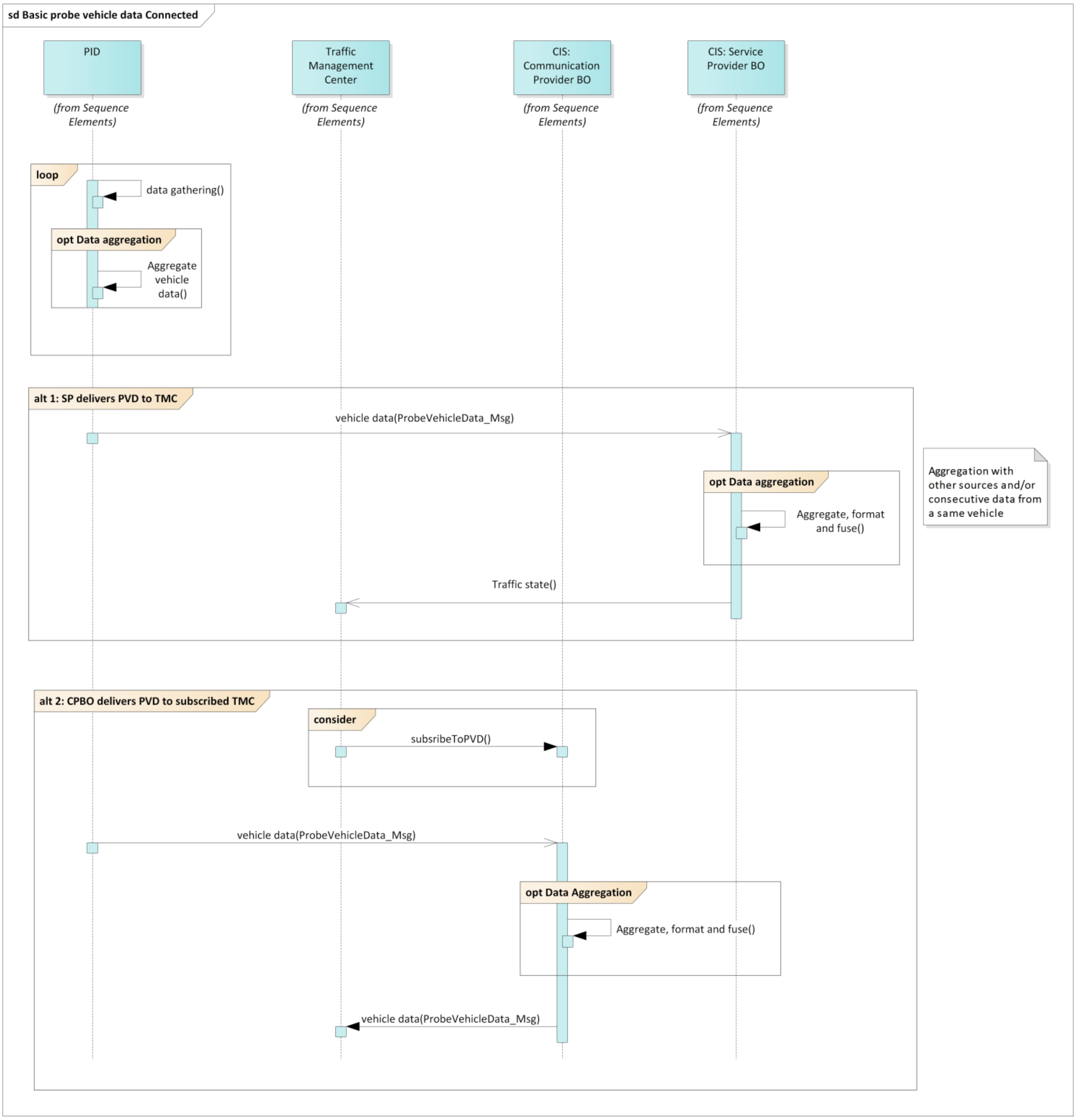


Figure 220: Probe Vehicle Data (connected)

Both use cases share the same architecture components so just one diagram is needed to describe the services.

The PID collects the probe data using any desired mechanism (Deployment Site specific), builds the appropriate message (ProbeVehicleData_Msg or ETSI ITS CAM) and sends it (optionally aggregated) via a cellular communication to the Service Provider Back Office (SPBO) and/or the Communication Provider Back Office (CPBO). This would depend on the possibility to implement GeoMessaging subscriptions in the TMS. The SPBO would send directly this information (with a previous aggregation if needed) to the

TMS. Instead, the CPBO would deliver the data to a GEOM subscribed TMS. In both cases, the TMS is the last destination of the probe data where it is processed and actions could be taken depending on it.

7.1.15.1.2. UC15.1 & UC15.2 Probe Vehicle Data (cooperative)

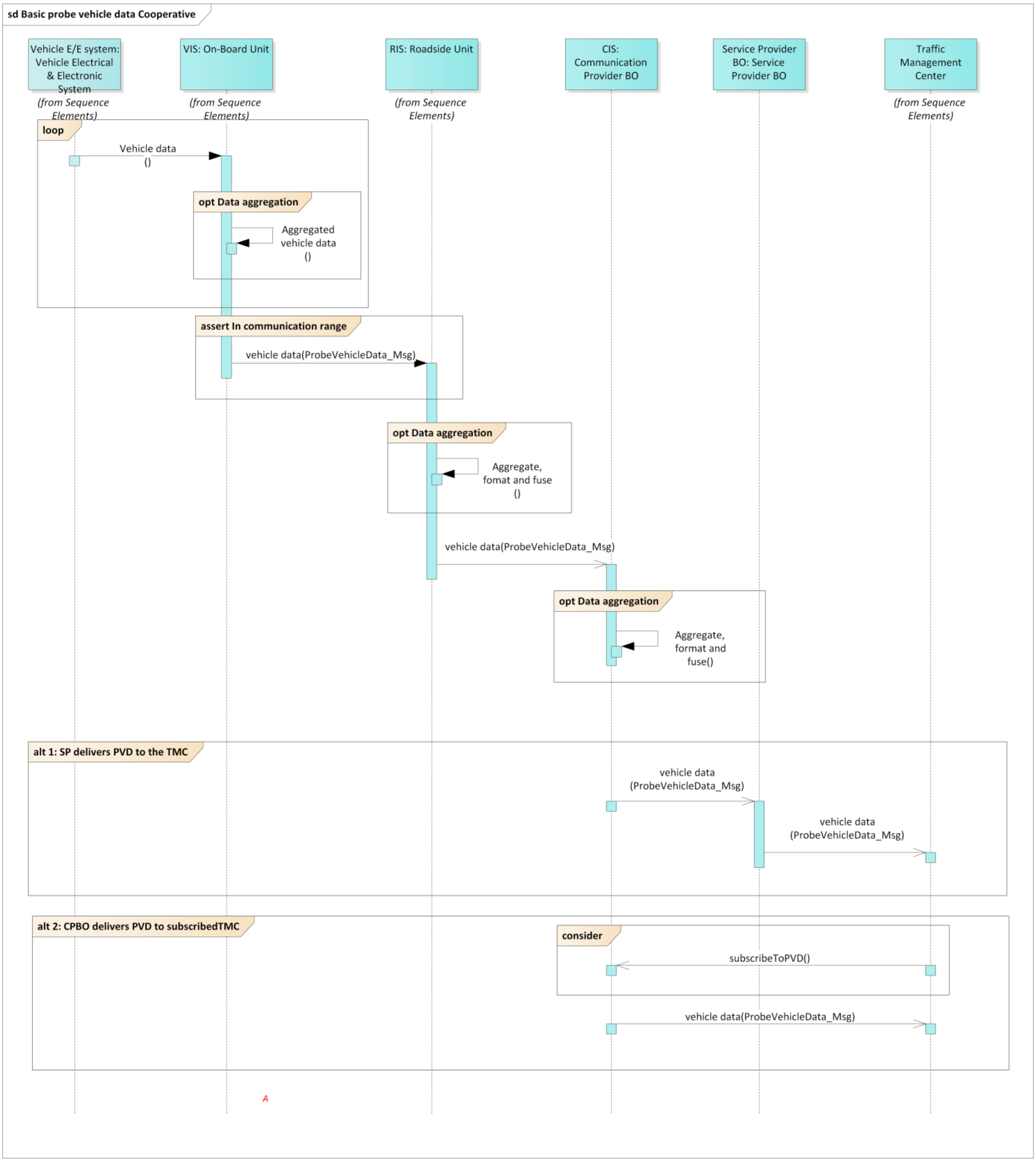


Figure 221: UC15.1 & UC15.2 Probe Vehicle Data

For the cooperative case, the information is generated in the VEE system and passed to the On-Board Unit (OBU). The OBU disseminates this information with destination the RSU via ITS G5. The RSU can process, aggregate and send the message to the CPBO where an aggregation can also be possible. From the CPBO, the TMS can receive the probe data after a subscription to this type of data or the SPBO can do the same to make a middle step before reaching the TMS. In all interactions, the same type of message is used (ProbeVehicleData_Msg or ETSI ITS CAM). Only when GEOM is involved, there could be some metadata also included in the message.

7.1.15.2. Service Datatypes

Will futher described in WP 5.

7.1.16. Emergency Brake Light

7.1.16.1. Service Diagrams

7.1.16.1.1. Information shared between vehicles for Emergency Brake Light operations

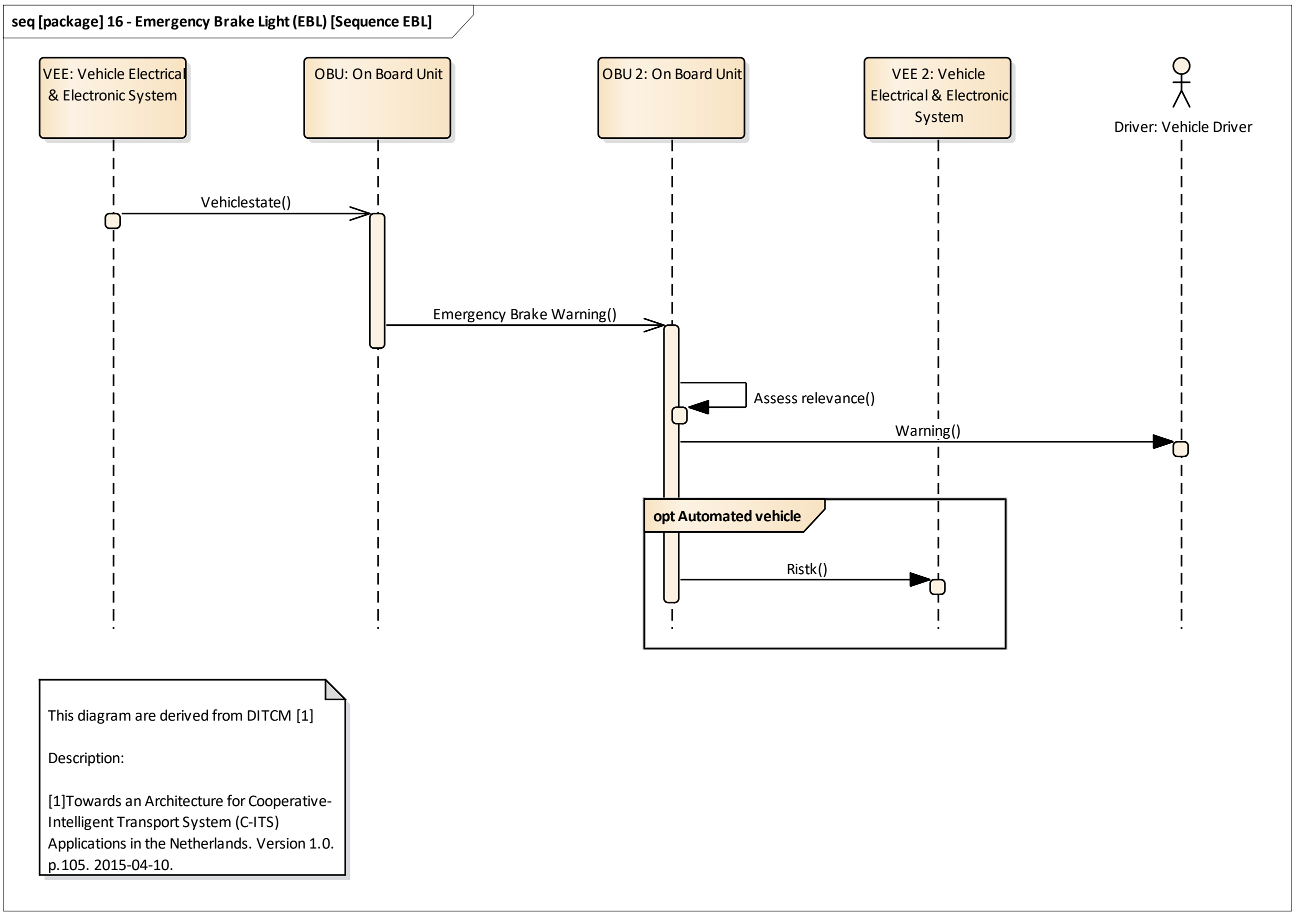


Figure 222: EBL sequence diagram

The sequence diagram is the minimal set required for a basic EBL operation. The first vehicle sends out its vehicle state to the OBU. This is processed at the OBU and an EBL message is transmitted with relevant vehicle state information (speed, acceleration/deceleration, heading etc.). The following vehicle 2 (OBU 2) assesses this information and presents this as a warning to the driver via the vehicle HMI and/or PID.

Optionally this can be a more ADAS like function were the received EBL data is directly used as input to vehicle control (VEE 2).

This can also be scaled to N vehicles as vehicle 2 can also share it vehicle state information via an EBL message to a vehicle 3 which use this information again as warning or for direct vehicle control (VEE 3)

In addition to the sequence diagram the ARC-IT diagram for Emergency Brake Light is presented below, for the EBL use case based on ITS-G5 communication only.

Driver inputs are the actuators for activating and deactivating EBL and vehicle control. Driver updates are presented via the vehicle HMI or a personal information device.

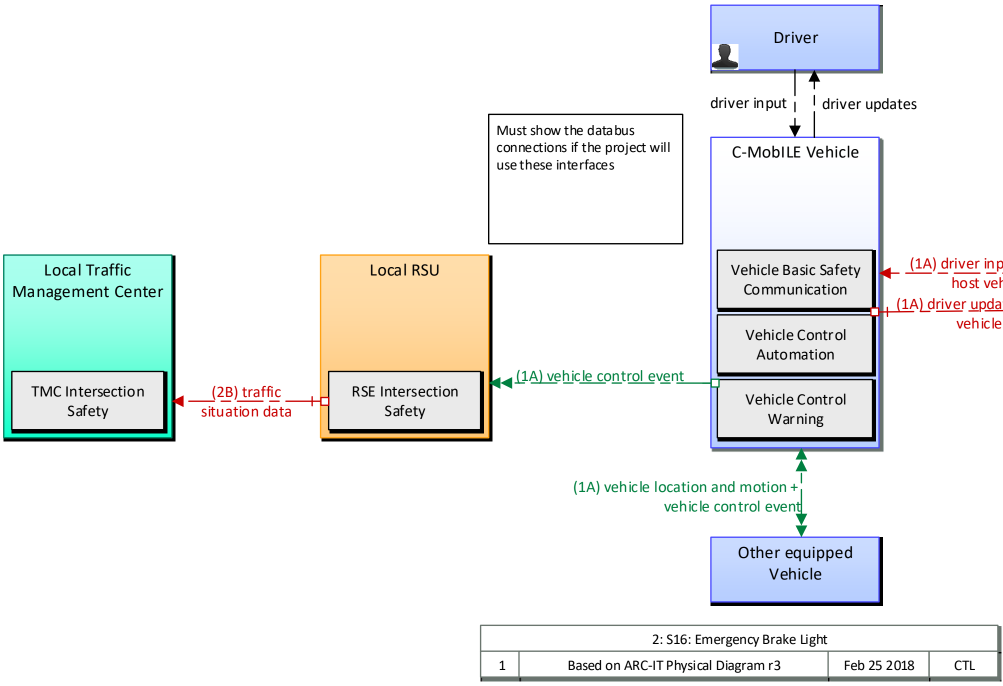


Figure 223 ARC-IT diagrams for Emergency Brake Light

If cooperative infrastructure is available, the EBL data can be shared via the RSU for improved local traffic awareness at a Traffic Management Center. Not in the diagram, but the connection between RSU and TMC is normally realized with more elements: RSU -> CPBO -> SPBO -> TMC.

7.1.16.2. Service Datatypes

The following diagrams describes the datatypes and information exchanged between components. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. The range of attributes and information inside those message types are extensive and mostly out of scope, therefore the diagrams may only contain the necessary attributes with specific values.

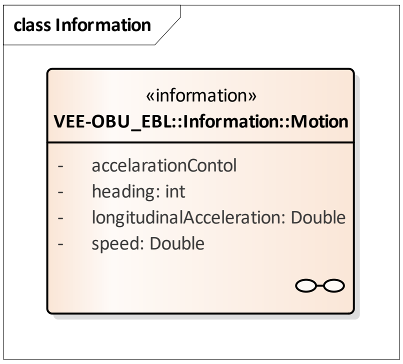


Figure 224: EBL VEE-OBU data

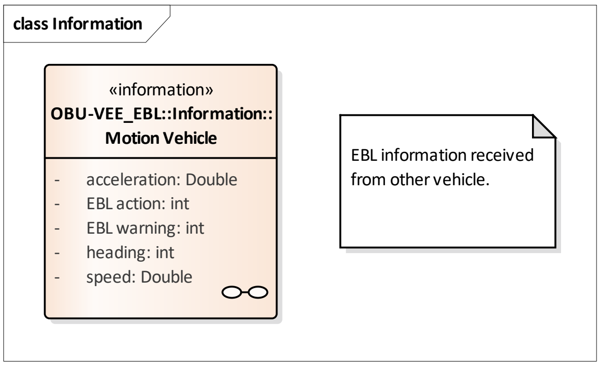


Figure 225: EBL OBU-VEE data

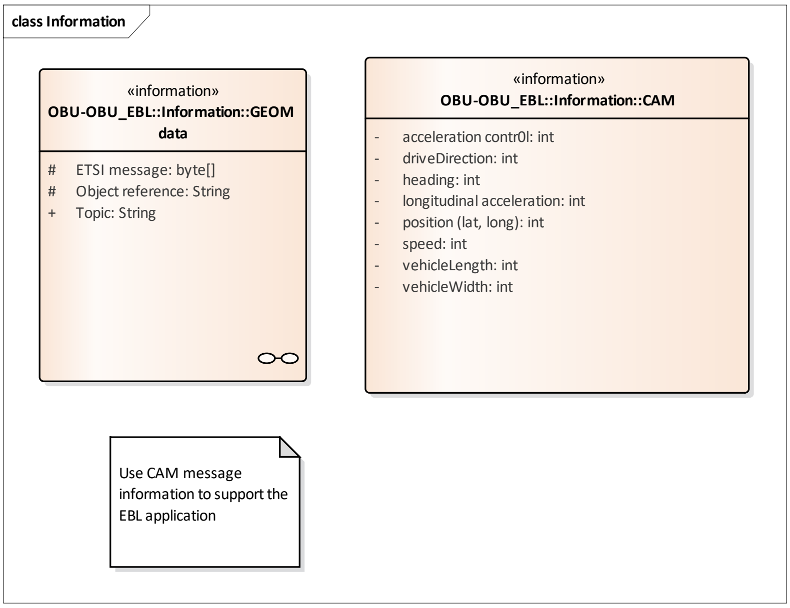


Figure 226: EBL OBU-OBU data

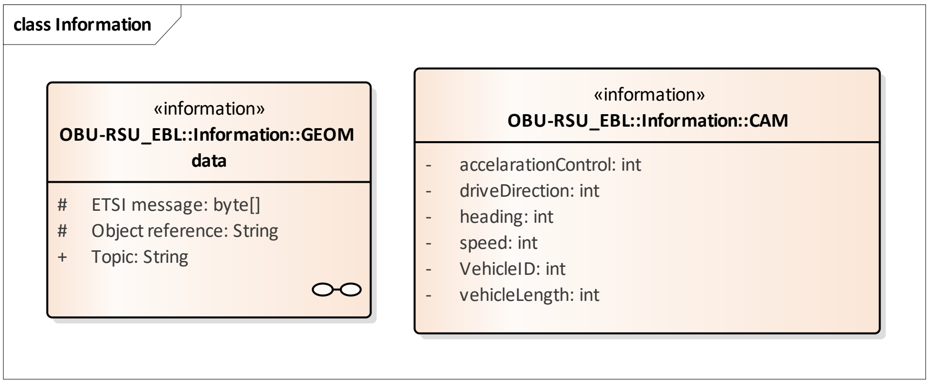


Figure 227: EBL OBU-RSU data

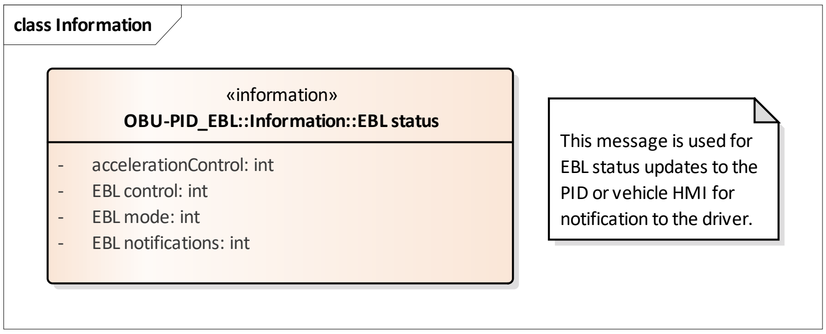


Figure 228: EBL OBU-PID data

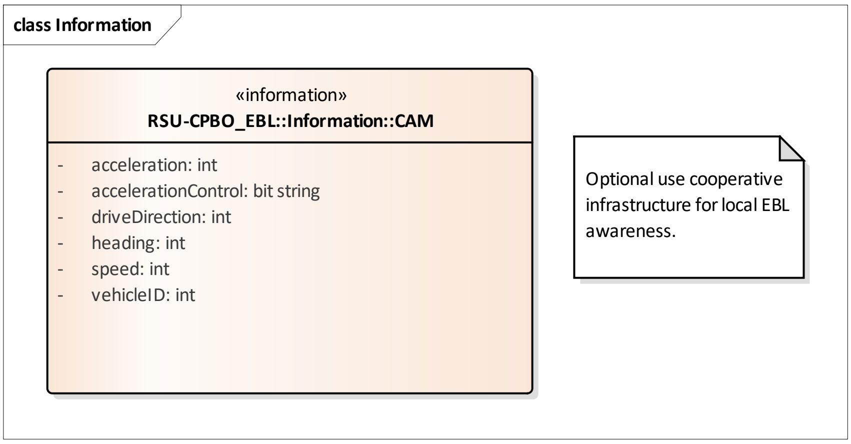


Figure 229: EBL RSU-CPBO data

As mentioned before the complete chain for including cooperative infrastructure in EBL would be from: RSU -> CPBO -> SPBO -> TMS. The datatypes are expected to be the same over these links.

7.1.17. Cooperative (Adaptive) Cruise Control

7.1.17.1. Service Diagrams

7.1.17.1.1. Information shared between vehicles for cooperative adaptive cruise control

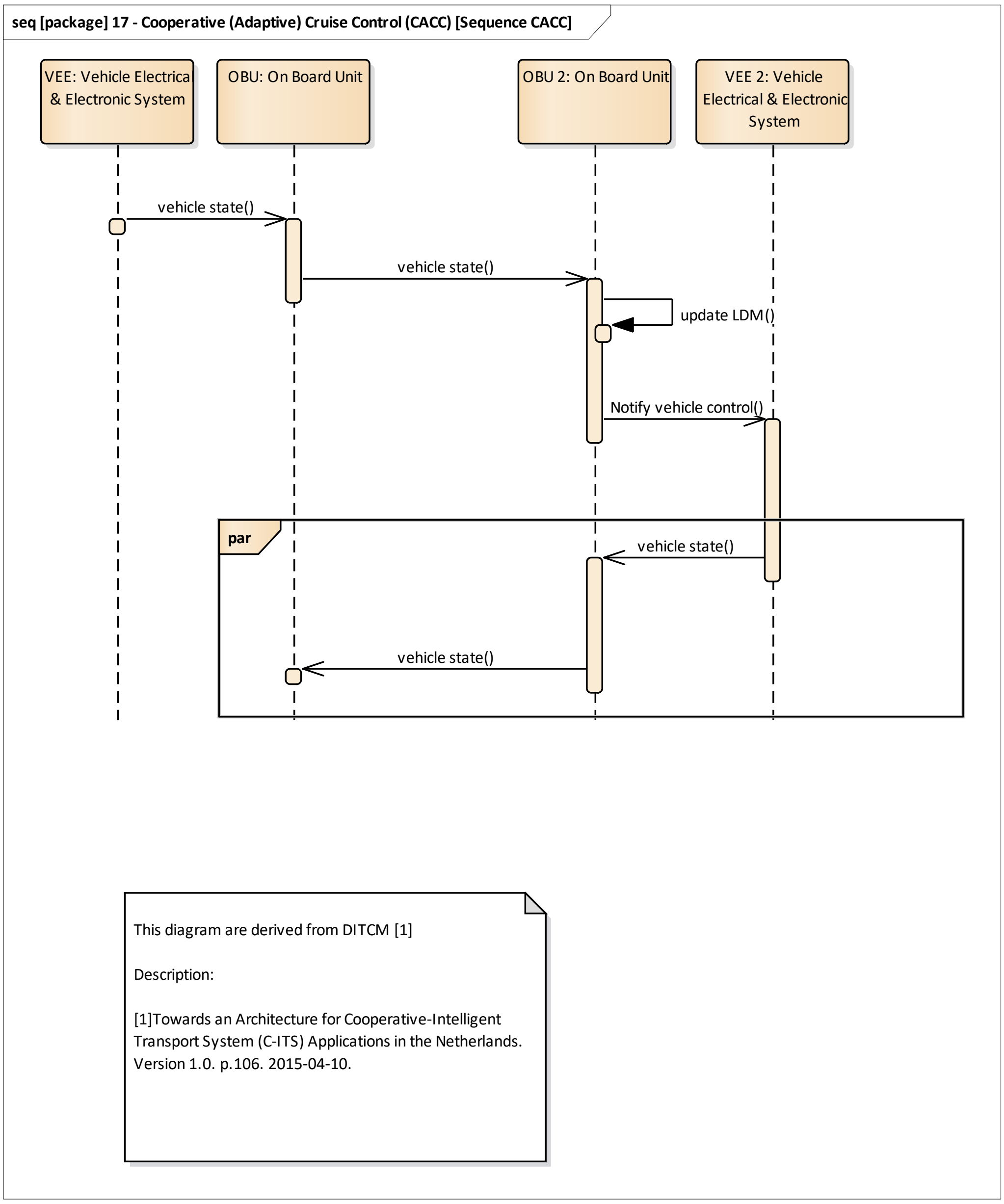


Figure 230: CACC sequence diagram

The sequence diagram is the minimal set required for a basic CACC application. The first vehicle sends out a "CACC" message with relevant vehicle state information (speed, acceleration, heading etc.) for the CACC application. The following vehicle 2 (OBU 2) uses this information as input for its own CACC setpoint and vehicle control. In addition, a feedforward mechanism Is possible sharing vehicle state information from Vehicle 2 to Vehicle 1 for improved vehicle following (CACC+) or sharing Platooning sate information.

This can also be scaled to N vehicles as vehicle 2 can also share it vehicle state information to a vehicle 3 which use this information for its CACC setpoint, etc.

Only this basic CACC sequence diagram is available. Additional information is provided in the use case descriptions UC17.1, UC17.2, UC17.3 and UC17.4.

In addition to the sequence diagram the ARC-IT diagram for Cooperative Adaptive Cruise Control is presented below, for the CACC use case based on V2V communication only.

Driver inputs are the actuators for activating and deactivating CACC. Driver updates are presented via the vehicle HMI or a personal information device.

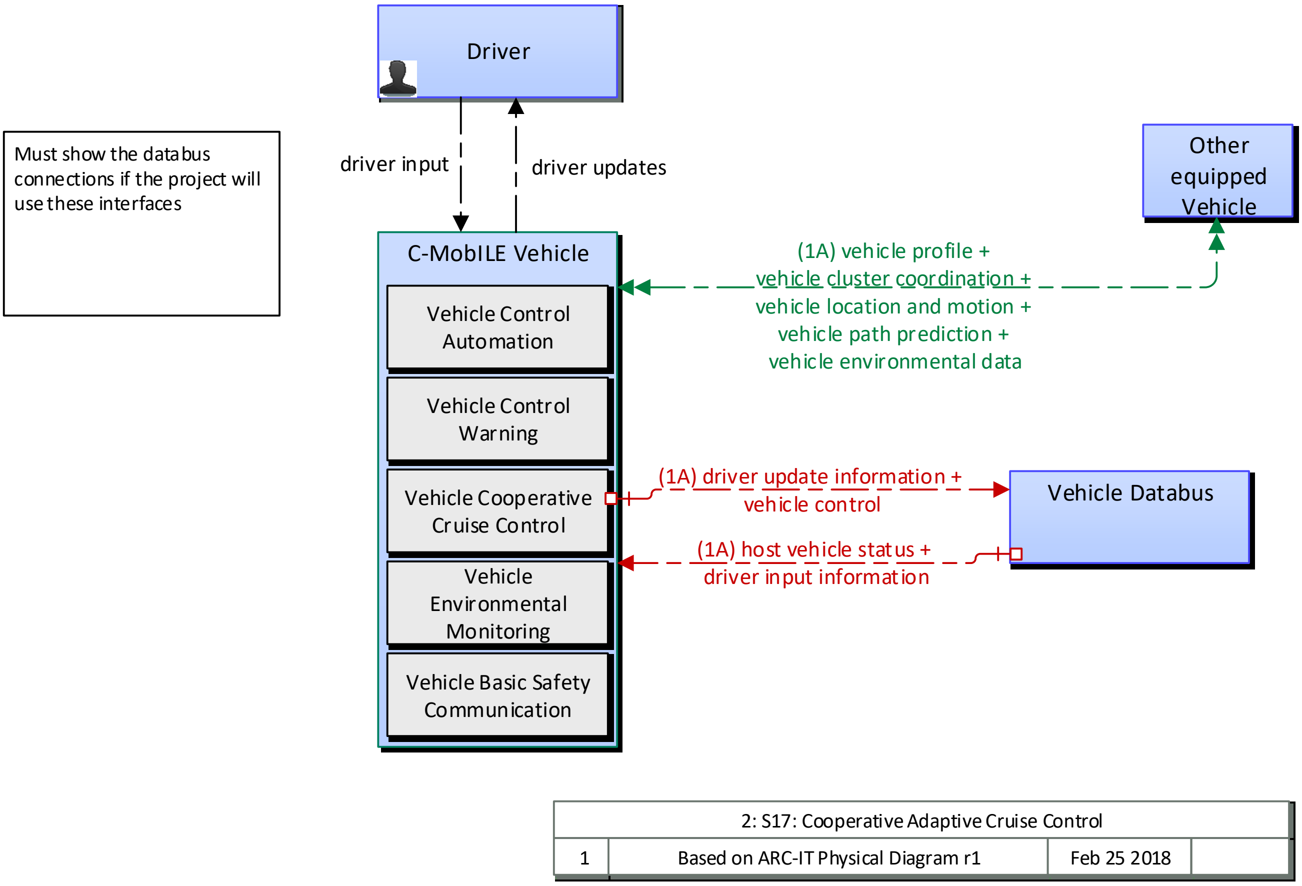


Figure 231 ARC-IT diagrams for Cooperative Adaptive Cruise Control

7.1.17.2. Service Datatypes

The following diagrams describes the datatypes and information exchanged between components. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. The range of attributes and information inside those message types are extensive and mostly out of scope, therefore the diagrams may only contain the necessary attributes with specific values.

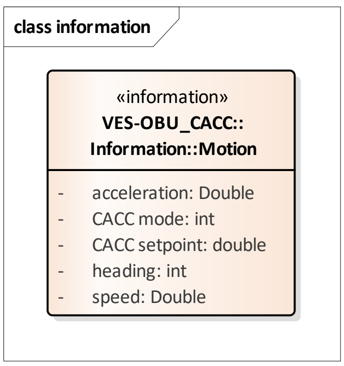


Figure 232: CACC VES-OBU data

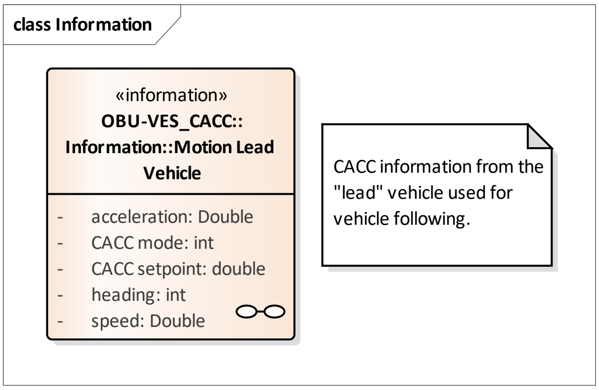


Figure 233: CACC OBU-VES data

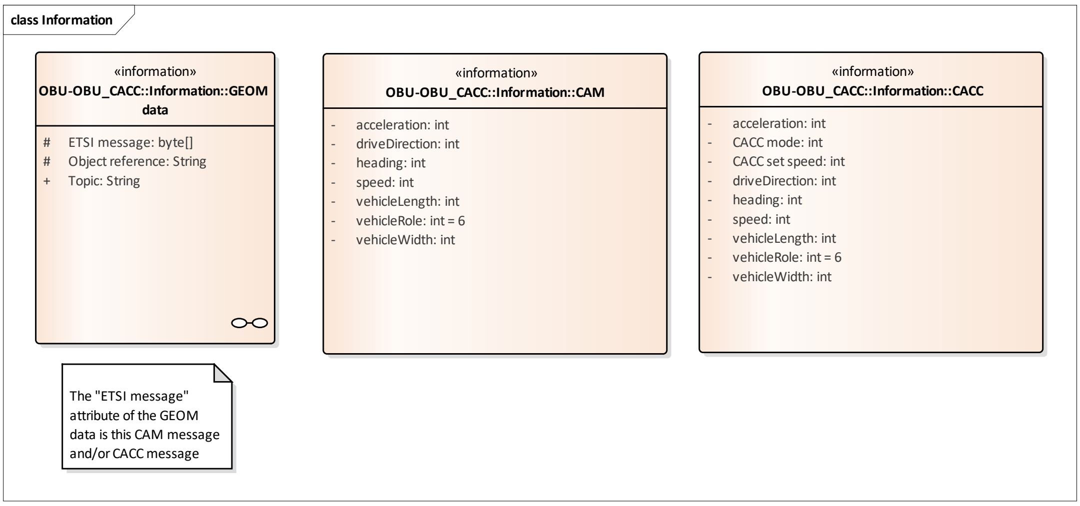


Figure 234: CACC OBU-OBU data

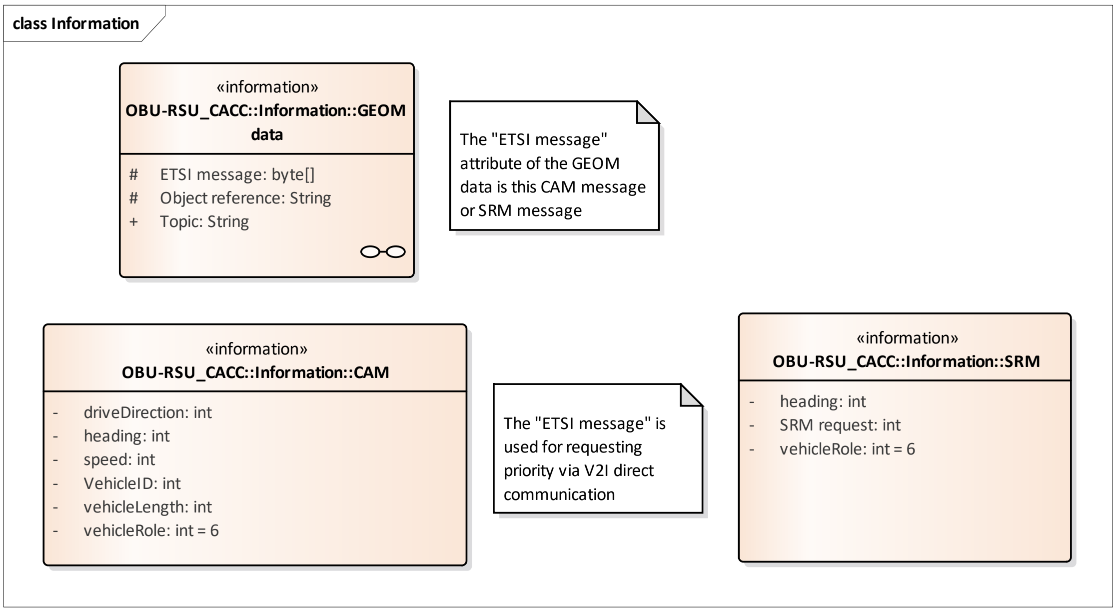


Figure 235: CACC OBU-RSU data

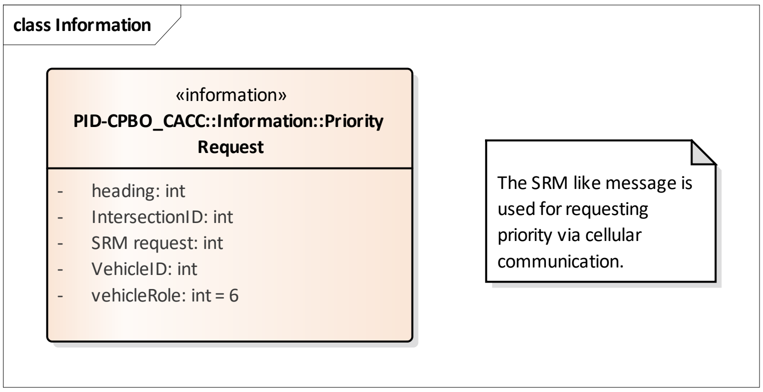


Figure 236: CACC PID-CPBO data

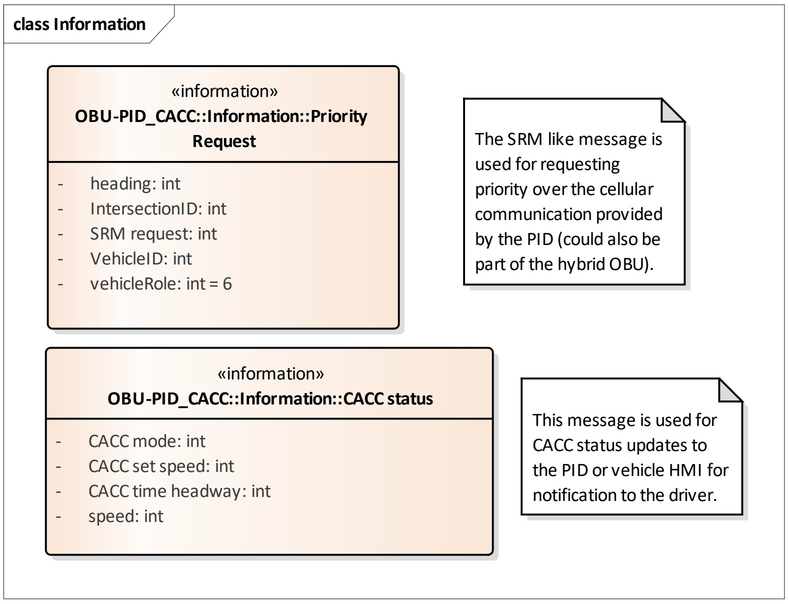


Figure 237: CACC OBU-PID data

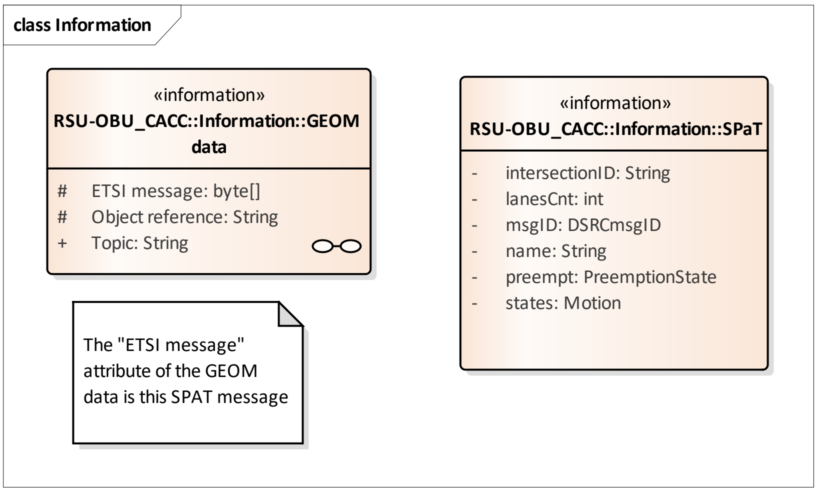


Figure 238: CACC RSU-OBU data

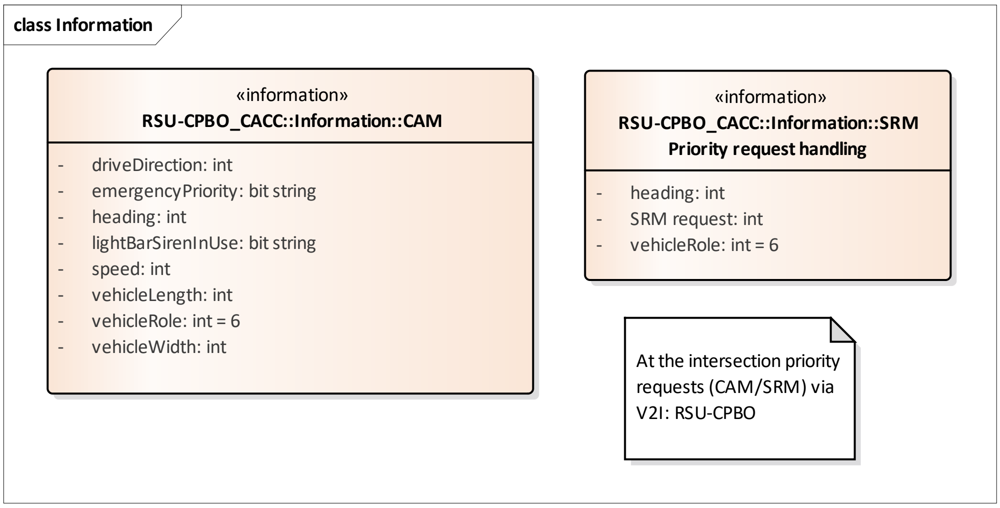


Figure 239: CACC RSU-CPBO data

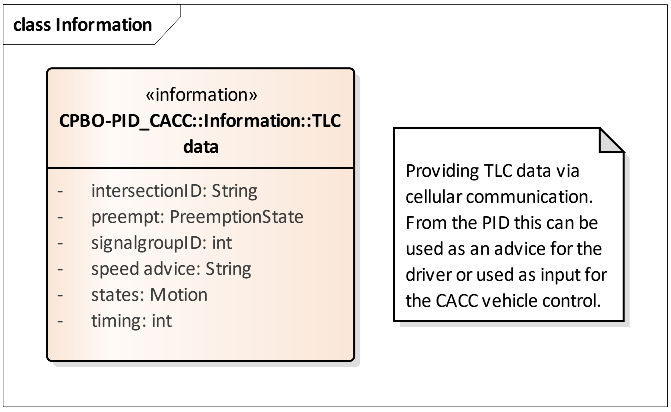


Figure 240: CACC CPBO-PID data

7.1.18. Slow or Stationary Vehicle Warning

7.1.18.1. Service Diagrams

7.1.18.1.1. Slow or Stationary Vehicle Warning

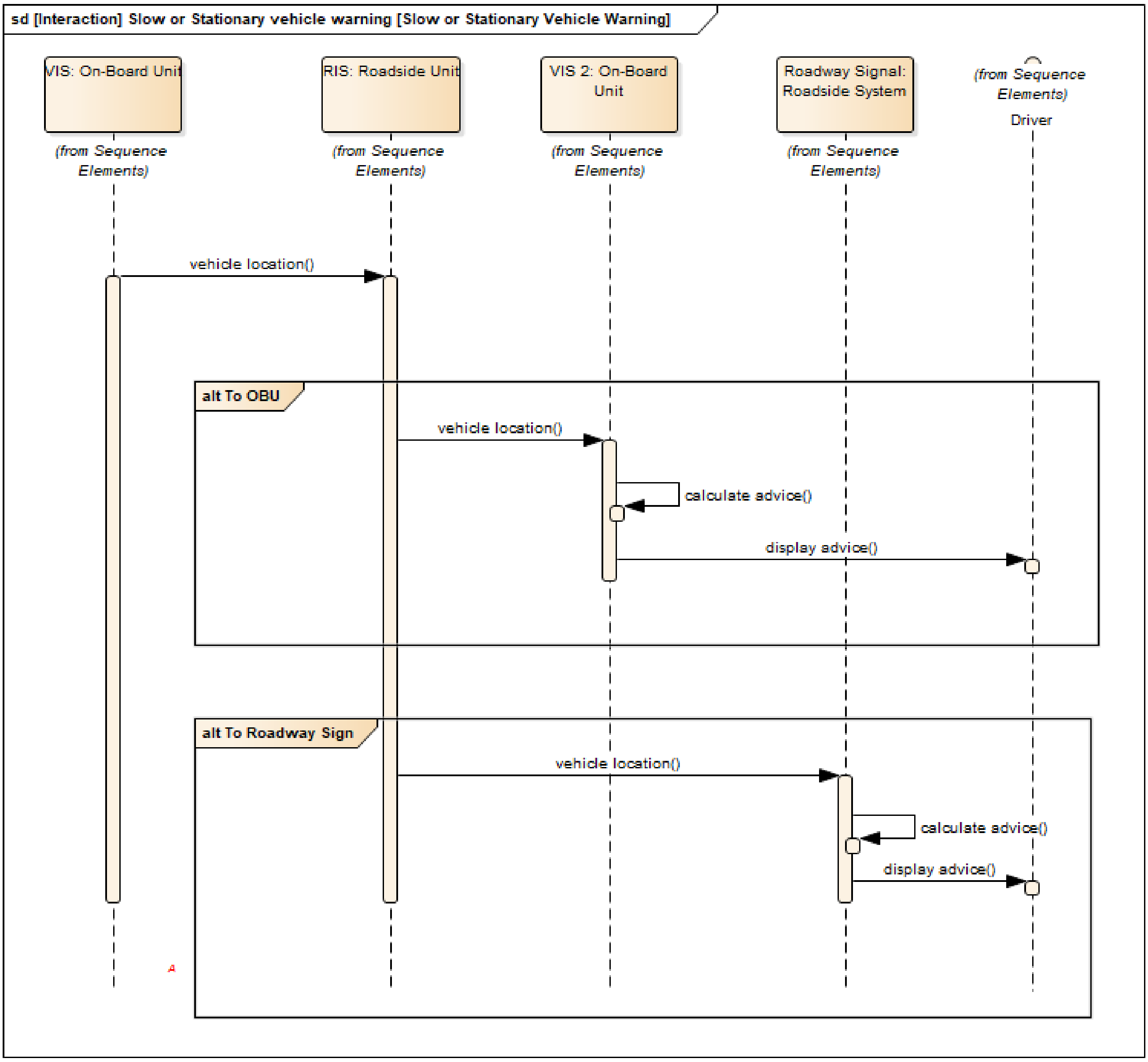


Figure 241: Slow or Stationary Vehicle Warning sequence diagram

The Slow Stationary Vehicle Warning starts from the On-Board Unit (OBU) of a vehicle that is stationary or a vehicle moving in a slow speed (a maintenance vehicle or a vehicle with some issues) sending the location of the slow or stationary vehicle to the closest Roadside Unit (RSU). The RSU forwards this location to the OBU of the receiving vehicle, where an advice is calculated and displayed to the driver. At the same time, the RSU can forward the location to a Roadway Signal, which is a Roadside System (RS), where the advice is calculated and displayed.

7.1.18.2. Service Datatypes

The following diagrams describes the datatypes and information exchanged between components. Most of them are based on standardized message types e.g. ETSI EN 302 637-2. The range of attributes and information inside those message types are extensive and mostly out of scope, therefore the diagrams may only contain the necessary attributes with specific values.

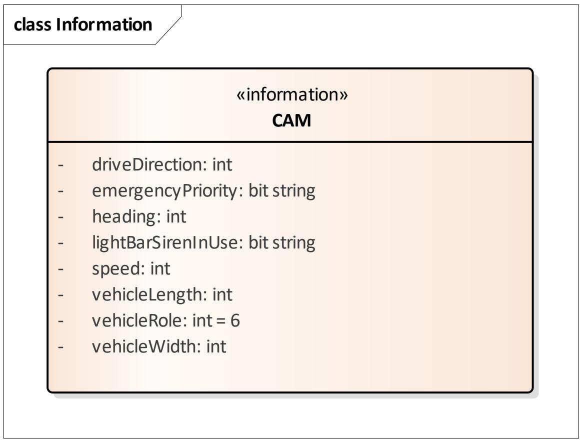


Figure 242: SSVW OBU-RSU

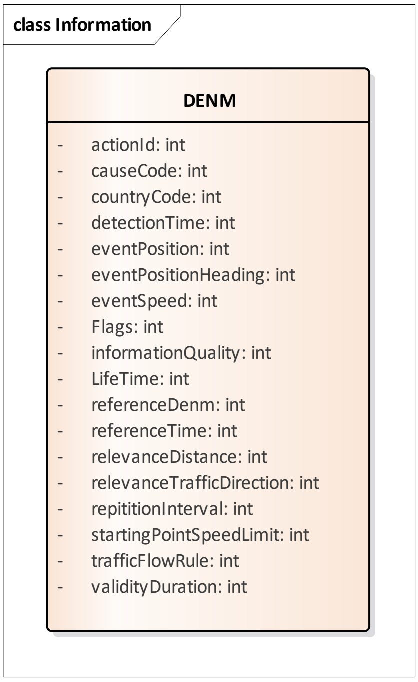


Figure 243: SSVW RSU-OBU

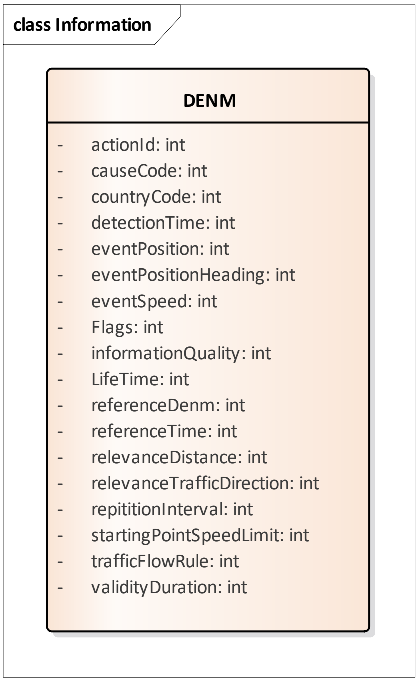


Figure 244: SSVW RSU-RS

7.1.19. Motorcycle approaching indication

7.1.19.1. Service Diagrams

7.1.19.1.1. The approaching two-wheeler warning (V2V)

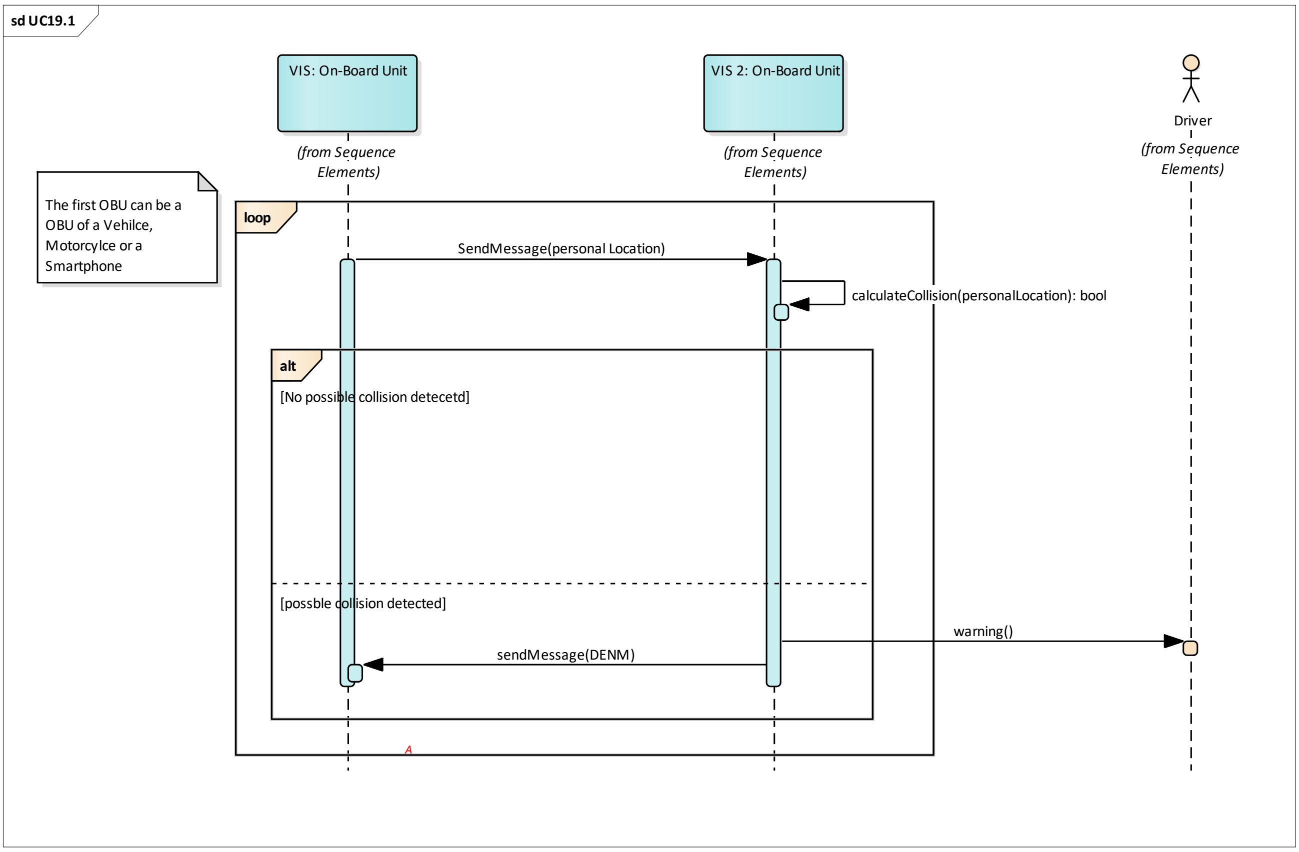


Figure 245: The approaching two-wheeler warning (V2V) - Sequence diagram

The Vehicle ITS-S on the two-wheeler continuously provides movement and position information to vehicles nearby. The Vehicle ITS-S on the surrounding vehicles receive the information and can automatically compare their own movement data with the two-wheeler data. If a possible crossing with the two-wheeler is detected or the relative distance between the two vehicles decreases below a given safety margin, a warning is issued to the driver.

7.1.19.1.2. The approaching two-wheeler warning (V2V cellular)

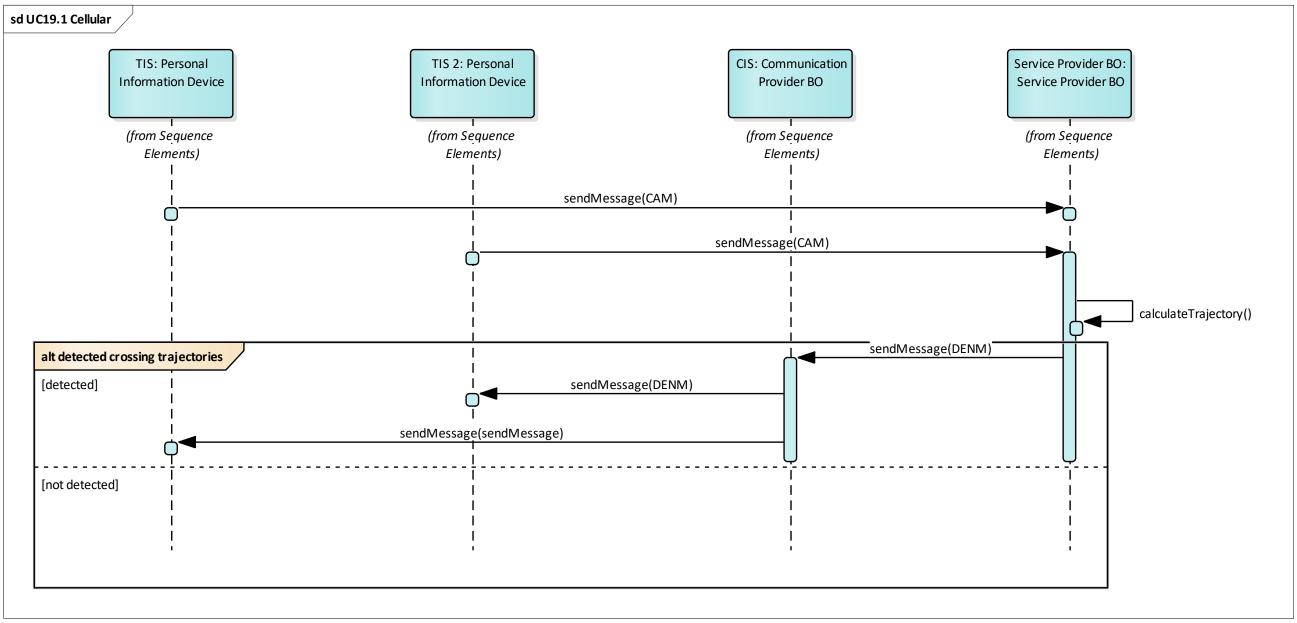


Figure 246: The approaching two-wheeler warning (V2V cellular) - Sequence diagram

For the cellular way of the approaching two-wheeler warning the PIDs are start sending CAMs to the SPBO if they enter a specific area. The SPBO will calculate the colliding trajectories and generate a DENM which get send by GeoMessaging to the PIDs.

7.1.19.1.3. The approaching two-wheeler warning (V2I)

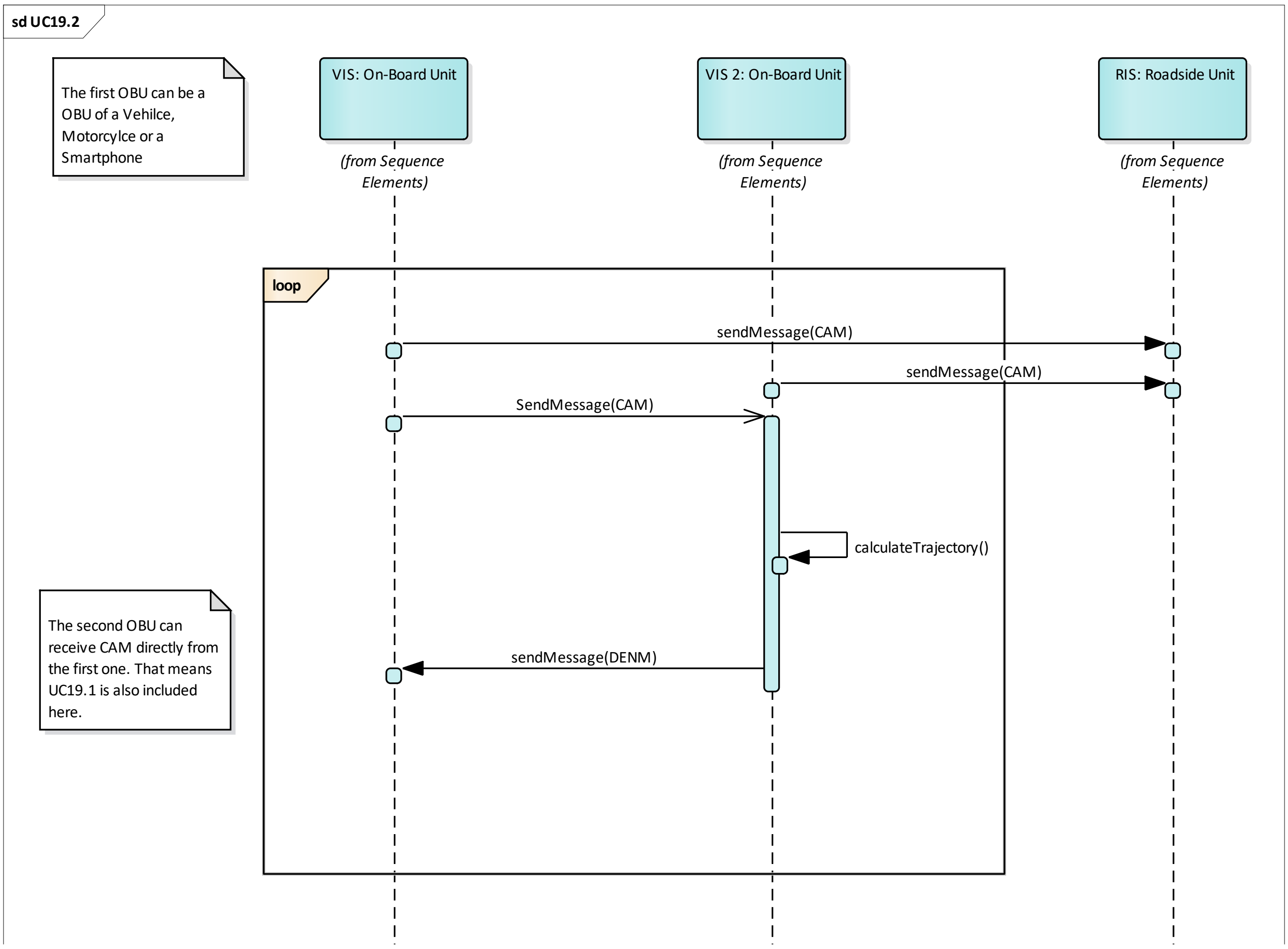


Figure 247: The approaching two-wheeler warning (V2I) - Sequence diagram

The approaching two wheeler use case for V2I is mostly the same as V2V, but the OBU is sending the its personal location as CAM to the RSU nearby.

7.1.19.2. Service Datatypes

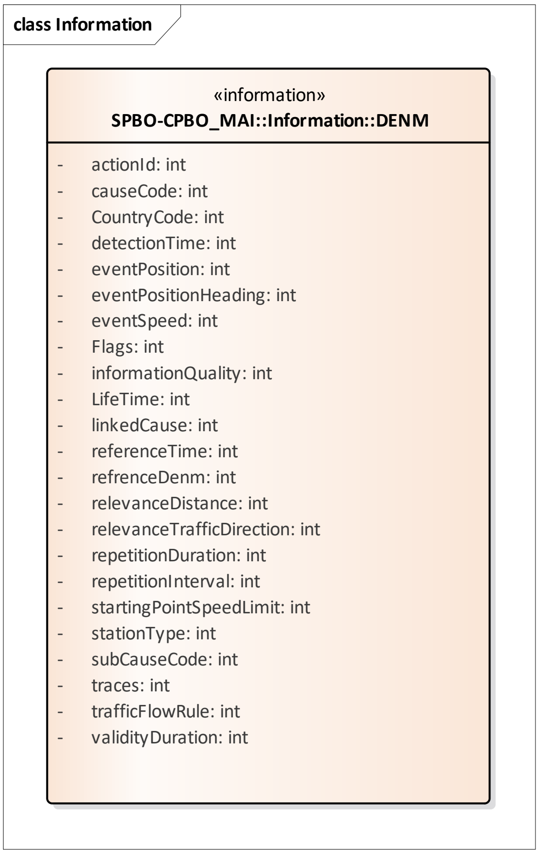


Figure 248: SPBO-CPBO_MAI DENM

Figure 249: CPBO-PID DENM

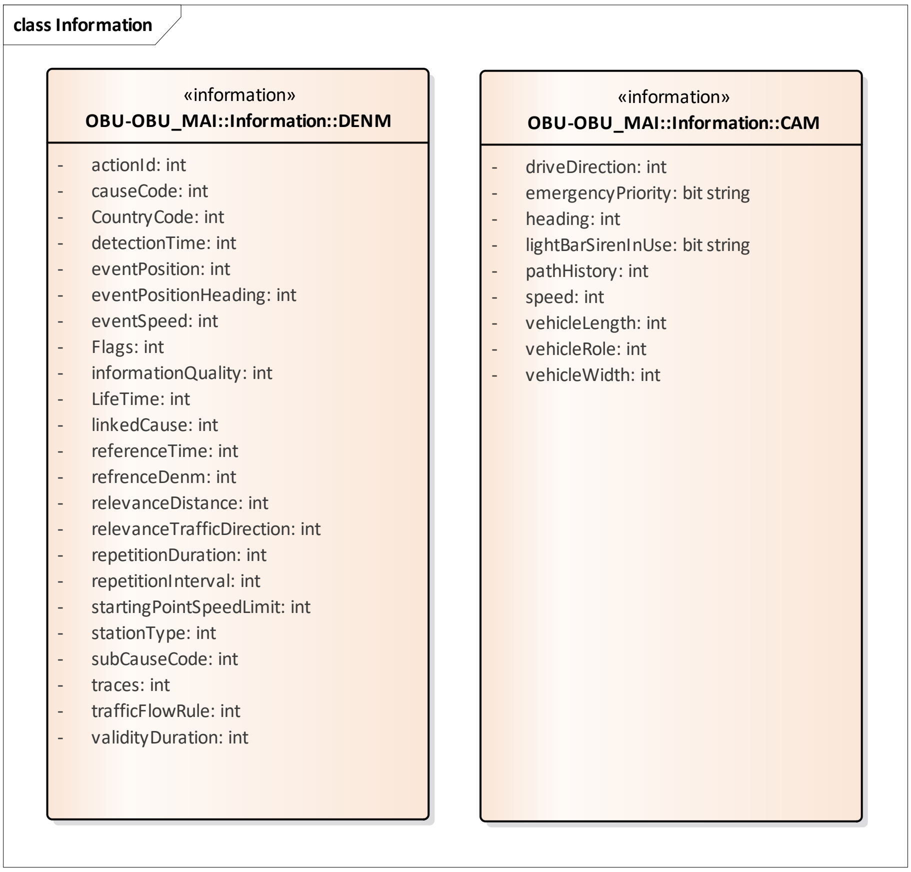


Figure 250: OBU-OBU_MAI CAM and DENM

Figure 251: RSU-OBU_MAI DENM

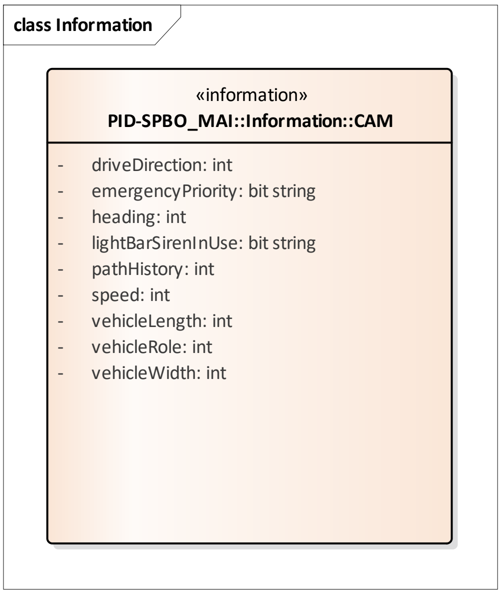


Figure 252: PID-SPBO_MAI CAM

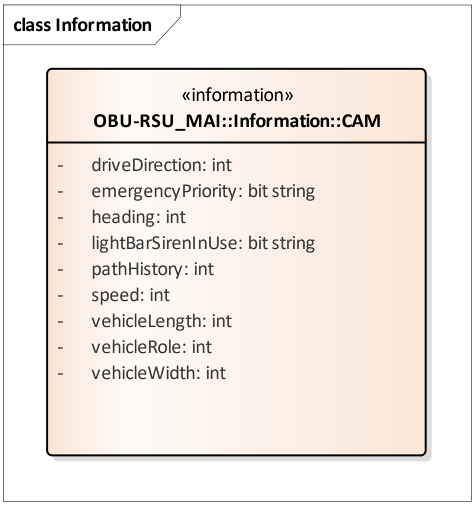


Figure 253: OBU-RSU_MAI CAM

7.1.20. Blind spot detection

7.1.20.1. Service Diagrams

7.1.20.1.1. "UC20.1: Blind spot detection - Cooperative"

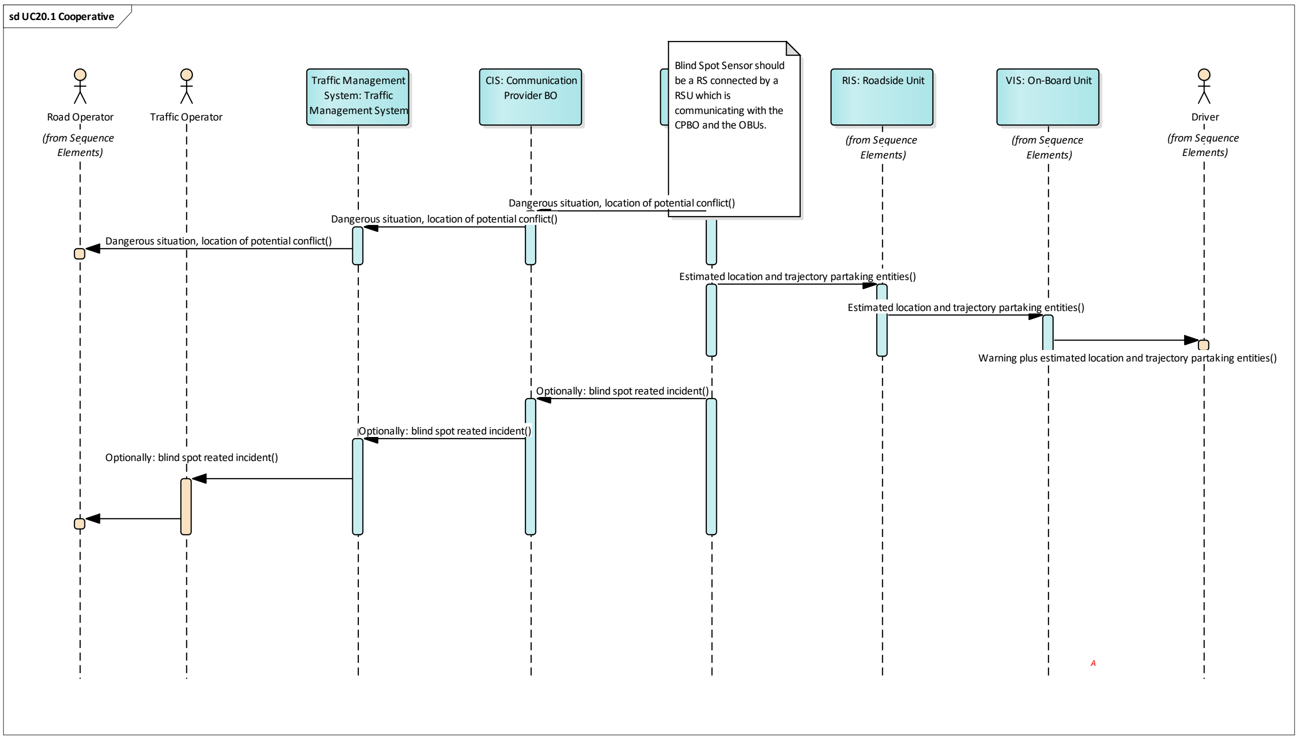


Figure 254: Sequence diagram UC20.1: Blind spot detection - Cooperative

The above sequence diagram is demonstrating Blind spot detection in Cooperative mode. In the diagram above the blind spot detector sensor is part of the Road Side Unit. From the sensor two information streams will take place, one towards the driver addressing potential harmfull situation on the bases of the estimated trajectory of the vehicle and associated blind spot. The service will inform the driver by sending a warning message. On the same side the Traffic Operator gets informed via the traffic management system that there has been a potential dangerous situation.

7.1.20.1.2. "UC20.2: Blind spot detection - Connected"

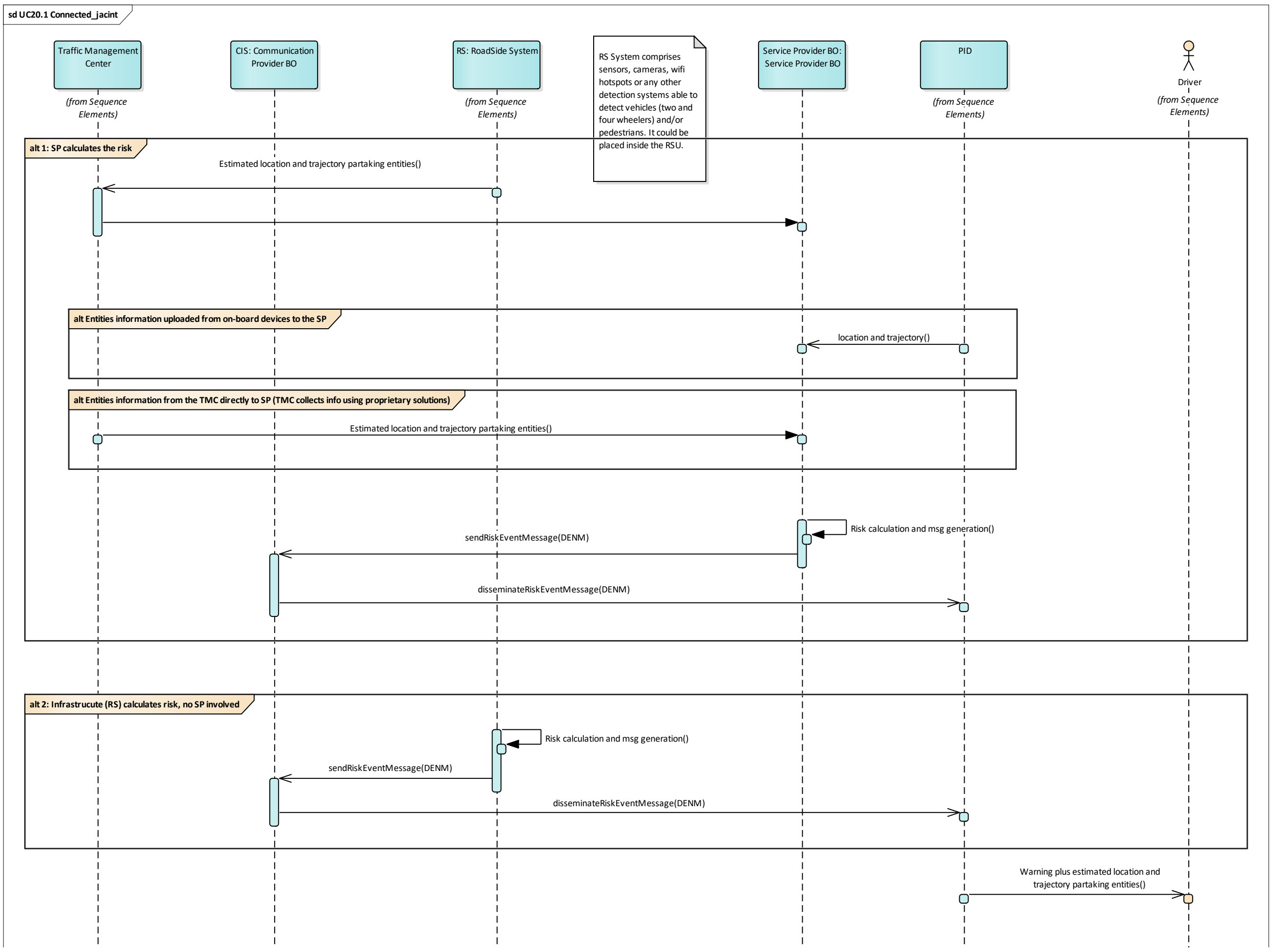


Figure 255: Sequence diagram UC20: Blind spot detection - Connected

In the connected setup the information stream and involvement of the Traffic Management systems comes in place as demonstrated below the way the risk assessment is being calculated is done differently in which the Service Provider and the Traffic Management center play a greater role. In this case it is not the Roadside system to provide the direct messaging to the driver but it will be handled via the Service Provider on the basis of a DENM event as shown in the sequence diagram below Blond spot detection.

7.1.20.2. Service Datatypes

Will futher described in WP 5.

8. Appendix B

8.1. Protocol References

The next sections describe the protocols used in C-MobILE. Most of the descriptions were adopted from the Harmonized Architecture Reference for Technical Standards Website. To have a better overview of the used standards, they have combined multiple protocols to a so called protocol bundle, e.g. ETSI ITS-S Security Architecture consists of four different standards.

First of all, the protocols are assigned to the layer they belong e.g. Access, Security etc. and if a protocol has underlying sections that means that they are part of a bundle mentioned before.

8.1.1. Security

8.1.1.1. IETF RFC 6347 - Datagram Transport Layer Security Version 1.2

Transport Layer Security [TLS] is the most widely deployed protocol for securing network traffic.However, TLS must run over a reliable transport channel -- typically TCP [TCP]. Therefore, it cannot be used to secure unreliable datagram traffic. For this purpose, Datagram Transport Layer Security (DTLS) has been introduced. It is a collection of differences (deltas) to TLS, which allows to secure datagram packets. The protocol is standardized as DTLS v1.2 in IETF RFC 6347.

8.1.1.2. ETSI ITS-S Security Architecture

The following sections describe the different ETSI ITS-S documents related to their ITS security architecture.

8.1.1.2.1. ETSI TS 102 731

ETSI TS 102 731 Intelligent Transport Systems (ITS); Security; Security Services and Architecture specifies “mechanisms […] for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization.” According to its own introductory text. It defines different elements of the security architecture and describes the general principles. It is currently available as ETSI TS 102 731 V1.1.1.

8.1.1.2.2. ETSI 102 940

ETSI 102 940 *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management* specifies “a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731, it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665” according to its introductory text. It also “identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment”. The document can be found as ETSI TS 102 940 V1.3.1.

8.1.1.2.3. ETSI 102 941

ETSI 102 941 *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management* specifies “the trust and privacy management for Intelligent Transport System (ITS) communications. […] it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in EN 302 665” according to its own introductory text. It also “identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in an Intelligent Transport System (ITS). Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS”. The document is available as ETSI TS 102 941 V1.1.1.

8.1.1.2.4. ETSI 103 097

ETSI 103 097 *Intelligent Transport Systems (ITS); Security; Security header and certificate formats* specifies “the secure data structure including header and certificate formats for Intelligent Transport Systems.” According to its own introductory text. It is available as ETSI TS 103 097 V1.3.1.

8.1.1.3. IETF RFC 6071 - IP Security and Internet Key Exchange

IETF RFC 6071 IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap is a snapshot of IPsec and IKE-related RFC's. It provides an overview of the various RFC's and how they work together. As such, it is not a single protocol or standard, but provides the entry point to multiple standards. It can be found as IETF RFC 6071.

8.1.1.4. IETF RFC 5246 - Transport Layer Security Protocol

RFC 5246 specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS is the most widely deployed protocol for securing network traffic. It is widely used for protecting web traffic ("https") and for e-mail protocols such as IMAP [IMAP] and POP [POP]. The primary advantage of TLS is that it provides a transparent connection-oriented channel. Thus, it is easy to secure an application protocol by inserting TLS between the application layer and the transport layer. The protocol is standardized as TLS v1.2 in IETF RFC 5246.

8.1.1.5. ISO 21219-24 - TPEG2-LTE

ISO/TS 21219-24 - Intelligent transport systems - Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) -- Part 24: Light encryption (TPEG2-LTE) defines "the LTE encryption mechanism for TPEG Service Data Frames. It has been specifically designed for use with Business to Business (B2B) business models. The objective of this document is to provide a simple to use, yet effective Conditional Access mechanism for TPEG including encryption for use with both broadcast and/or point-to-point delivery. For both service providers and device manufacturers, a standardized conditional access mechanism is beneficial to avoid a proliferation of proprietary methods with multiplied implementation effort and lead times" according to the ISO introduction. It can be obtained from the ISO webpage for ISO/TS 21219-24:2017.

8.1.2. Management

8.1.2.1. ETSI 102 890-1

Intelligent Transport Systems (ITS); Facilities layer function; Part 2: Services announcement specification.

Development of the Technical Specification of the services announcement which is part of the facilities layer' services management function[10]

8.1.2.2. G5 Congestion Control Management

The following standards are defining the G5 Congestion Control Management.

8.1.2.2.1. ETSI 102 687

Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part.

DCC is a cross layer function, i.e. it has functions located on several layers of the ITS station reference architecture.

Therefore, the present document defines which DCC components are located on which layer of the ITS station communication architecture [5]. Furthermore, the present document specifies the DCC mechanisms on the access layer (DCC_access) including transmit power control (TPC) per packet, transmit rate control (TRC) and transmit data rate control (TDC). The latter two control functions modify the average transmit power by modifying the duty cycle of the ITS station, i.e. the fraction of time that the ITS station is in "transmit" state. Additionally, DCC sensitivity control (DSC) adapts the clear channel assessment to resolve local channel congestion. Packets with higher priority are handled less restrictive introducing a transmit queueing concept and transmit access control (TAC).

The DCC mechanisms rely on knowledge about the channel. The channel state information is gained using channel

probing. Channel probing measures are defined that enable the DCC methods TPC, TRC and TDC. The measures are on receive signal level thresholds or preamble information of detected packets.

The present document does not define the mechanisms at other layers than the access layer nor defines management aspects. These other mechanisms and the management aspects are necessary in order to make DCC work properly. The present document is primarily intended for trial use and may need to be updated after validation in field trials and/or other projects. [76]

8.1.2.2.2. ETSI 103 175

Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium.

"The present document specifies the functionality of the decentralized congestion control (DCC) entity residing in the management plane for the ITS-G5A, ITS-G5B, and ITS-G5D radio interfaces, collectively known as the 5 GHz ITS frequency band.

The purpose of the DCC operation is to evaluate the load of the active radio channels and to optimize the radio channel usage by managing the ITS-S DCC parameters. Another purpose is to keep track and help the exchange of DCC parameters which cannot be conveyed via the data plane between the different layers.

The present document specifies:

/ The necessary support functions of DCC that needs to be in the management plane, i.e. cross-layer DCC operations.

/ The required interface parameters between the DCC management entity and the DCC entities in the facilities, the networking & transport and the access layers.

/ The testing procedures and corresponding test cases."

Develop the Multimedia Content Dissemination basic service specification enabling the V2X exchange of multimedia information comprising video, audio, images and data. Messages can be exchanged through broadcast / multicast/unicast or peer to peer communication. [76]

[10] http://www.etsi.org/deliver/etsi_ts/102800_102899/10289001/01.01.01_60/ts_10289001v010101p.pdf

8.1.2.3. SNMPv2 (IETRF RFC 1907)

Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).

It is the purpose of this document, Protocol Operations for SNMPv2,

to define the operations of the protocol with respect to the sending

and receiving of the PDUs. [76]

8.1.2.4. SNMPv3 MIB

Secure management is available with SNMPv3, the ``Full Standard," IETF-recommended version of the Internet-Standard Management Framework. This technology provides commercial-grade security and the ease of administration, which includes authentication, authorization, access control, and privacy.

The secure management of SNMPv3 is an important enabling technology for safe configuration and control operations. SNMPv3 provides security with authentication and privacy, and its administration offers logical contexts, view-based access control, and remote configuration. This technology is available for networks, systems, applications, manager-to-manager communications, and proxy management of legacy systems.

SNMPv3 is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2c). All versions (SNMPv1, SNMPv2c, and SNMPv3) of the Internet-Standard Management Framework share the same basic structure and components. Furthermore, all versions of the specifications of the Internet-Standard Management Framework follow the same architecture. [76]

8.1.2.4.1. IETF RFC 2863

This RFC defines the MIB to manage and control interfaces on a device. [76]

8.1.2.4.2. IETF RFC 3411

An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

This RFC defines the basic architecture for SNMPv3 and includes the definition of information objects for managing the SNMP entity's architecture. [76]

8.1.2.4.3. IETF RFC 3412

Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

This RFC contains a MIB that assists in managing the message processing and dispatching subsystem of an SNMP entity. [76]

8.1.2.4.4. IETF RFC 3413

Simple Network Management Protocol (SNMP) Applications.

This RFC includes MIBs that allow for the configuration and management of remote Targets, Notifications, and Proxys. [76]

8.1.2.4.5. IETF RFC 3414

User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

This RFC contains a MIB that assists in configuring and managing the user-based security model. [76]

8.1.2.4.6. IETF RFC 3415

View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

This RFC contains a MIB that supports the configuration and management of the View-based access control model of SNMP. [76]

8.1.2.4.7. IETF RFC 3418

Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).

This RFC defines the MIB to configure and manage an SNMP entity. [76]

8.1.2.4.8. IETF RFC 4022

Management Information Base for the Transmission Control Protocol (TCP).

This RFC defines a MIB for the management of TCP implementations. [76]

8.1.2.4.9. IETF RFC 4113

Management Information Base for the User Datagram Protocol (UDP).

This RFC defines the MIB to allow for the management of UDP implementations. [76]

8.1.2.4.10. IETF RFC 4292

IP Forwarding Table MIB.

This RFC defines a MB to manage IP forwarding in routers. [76]

8.1.2.4.11. IETF RFC 4293

Management Information Base for the Internet Protocol (IP).

This RFC defines the MIB that manages an IP entity. [76]

8.1.2.5. TPEG2-MMC (ISO 21219-6)

ISO 21219-6 - Intelligent transport systems - Traffic and travel information via transport protocol experts group, generation 2(TPEG2) -- Part 6: Message management container (TPEG2-MMC). [76]

8.1.3. Access

8.1.3.1. 3GPP 3G Suite

Also known as Universal Mobile Telecommunications Systems (UMTS). UMTS is an umbrella term for the third generation radio technologies developed within 3GPP.

The radio access specifications provide for Frequency Division Duplex (FDD) and Time Division Duplex (TDD) variants, and several chip rates are provided for in the TDD option, allowing UTRA technology to operate in a wide range of bands and co-exist with other radio access technologies.

UMTS includes the original W-CDMA scheme using paired or unpaired 5 MHz wide channels in globally agreed bandwidth around 2 GHz, though subsequently, further bandwidth has been allocated by the ITU on a regional basis.

These are detailed in 3GPP Technical Specifications 25.101[11] (FDD) and 25.102[12] (TDD), and allow for the eventual re-use of bands currently assigned to 2G services.

W-CDMA was specified in Release 99 and Release 4 of the specifications. High Speed Packet Access (HSPA) was introduced in Releases 5 (Downlink) and 6 (Uplink) giving substantially greater bit rates and improving packet-switched applications. [13]

Specification work for UMTS is done in the Radio Access Network (RAN) group[14]

8.1.3.2. 3GPP 4G Suite

Also known as 4G Cellular Communications. This alternative standard set includes any standard that meets the requirements for the fourth generation of mobile communications technology, including 100+Mbps data rates. This would include release numbers 12, 13, and 14 of 3GPP. LTE Advanced is a mobile communication standard and a major enhancement of the Long Term Evolution (LTE) standard. It was formally submitted as a candidate 4G system to ITU-T in late 2009 as meeting the requirements of the IMT-Advanced standard, and was standardized by the 3rd Generation Partnership Project (3GPP) in March 2011 as 3GPP Release 10. [15]

8.1.3.3. ETSI ITS-G5

The ITS G5A band (5,875 GHz to 5,905 GHz) contains the channels CCH, SCH1 and SCH2. They are dedicated to road safety related service.

CCH: The Control Channel (CCH) is basically dedicated to cooperative road safety. &c.

SCH1: The Service Channel 1 (SCH1) is the default channel for announcing and offering ITS services for safety & road efficiency under the DCC state ACTIVE and RESTRITIVE of the CCH. &c&c.

SCH2: The Service Channel 2 (SCH2) is the second service channel on ITS G5A and is used as an alternate channel for traffic safety-related services. Due to its frequency band allocation between the CCH and the SCH1 and the resulting potential adjacent channel interference issues, the flexibility of the deployment of the SCH2 is limited. The limitations are taken into account in the requirement descriptions for the SCH2.

The following sections are part of the ETSI ITS-G5 protocol.

8.1.3.3.1. ETSI 102 687

This standard describes the Decentralized Congestion Control (DCC) Mechanisms for Intelligent Transport Systems operating in the 5 GHz range for the Access layer part. Because the wireless channel is a shared medium with limited resources, this is needed to avoid congestion of the wireless channel by means of rate and power control.

DCC is a cross layer function, i.e. it has functions located on several layers of the ITS station reference architecture.

Therefore, the present document defines which DCC components are located on which layer of the ITS station communication architecture [5]. Furthermore, the present document specifies the DCC mechanisms on the access layer (DCC_access) including transmit power control (TPC) per packet, transmit rate control (TRC) and transmit datarate control (TDC). The latter two control functions modify the average transmit power by modifying the duty cycle of the ITS station, i.e. the fraction of time that the ITS station is in "transmit"

[11] http://www.3gpp.org/ftp/Specs/html-info/25101.htm

[12] http://www.3gpp.org/ftp/Specs/html-info/25102.htm

[13] http://www.3gpp.org/technologies/keywords-acronyms/103-umts

[14] http://www.3gpp.org/tb/RAN/RAN.htm

[15] https://www.itu.int/net/ITU-R/information/promotion/e-flash/2/article4.html

state. Additionally, DCC sensitivity control (DSC) adapts the clear channel assessment to resolve local channel congestion. Packets with higher priority are handled less restrictive introducing a transmit queueing concept and transmit access control (TAC).

The DCC mechanisms rely on knowledge about the channel. The channel state information is gained using channel

probing. Channel probing measures are defined that enable the DCC methods TPC, TRC and TDC. The measures are on receive signal level thresholds or preamble information of detected packets.

The present document does not define the mechanisms at other layers than the access layer nor defines management aspects. These other mechanisms and the management aspects are necessary in order to make DCC work properly. The present document is primarily intended for trial use and may need to be updated after validation in field trials and/or other projects. [76]

8.1.3.3.2. ETSI 102 724

The European channel specifications for ITS communications at 5.9 GHz is described in this standard.

8.1.3.3.3. ETSI 102 792

Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range describes the mitigation techniques for DSRC and ITS G. Conformance tests are specified in ETSI TS 102 916-x.

8.1.3.3.4. ETSI 302 663

The full name of this standard is Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band.

The scope of the present document is to define the two lowest layers, physical layer and the data link layer, grouped into the access layer of the ITS station reference architecture EN 302 665 [i.8]. The access layer technology that is specified in the present document is collectively called ITS-G5. It is part of the communication stack supporting data exchange between mobile stations without prior network set-up, i.e. ad hoc mode, for the following frequency bands in Europe:

ITS-G5A: Operation of ITS-G5 in European ITS frequency bands dedicated to ITS for safety related applications in the frequency range 5,875 GHz to 5,905 GHz.

ITS-G5B: Operation in European ITS frequency bands dedicated to ITS non-safety applications in the frequency range 5,855 GHz to 5,875 GHz.

ITS-G5D: Operation of ITS applications in the frequency range 5,905 GHz to 5,925 GHz.

The ITS-G5 technology is based on IEEE 802.11-2012 and IEEE/ISO/IEC 8802-2-1998. By setting the MIB variable dot11OCBActivated to true in IEEE 802.11-2012 communication outside the context of a BSS is possible. This type of communication allows for immediate exchange of data frames, avoiding the management overhead used with the establishment of a network. All requirements in IEEE 802.11-2012 associated with communication "outside the context of a BSS" are also requirements in the present document. All optional functionality in IEEE 802.11-2012 associated with communication "outside the context of a BSS" is also optional in the present document.

8.1.3.4. Generic Access

This is a kind placeholder for every possible connection between back office systems.

8.1.4. Network & Transport

8.1.4.1. CALM FAST

The Communications Access for Land Mobiles (CALM) concept contains as an essential part the abstraction of ITS- applications from communication protocols (EN ISO 17423 from ISO TC204 WG18), allowing for dynamic selection of communication profiles dependent on needs of applications, capabilities of access technologies, current situation of communication channels, which also includes all kinds of handover (ISO 24102-6). [76]

8.1.4.2. GeoNetworking

The GeoNetworking protocol is a network layer protocol that provides packet routing in an ad hoc network. It makes use of geographical positions for packet transport. GeoNetworking supports the communication among individual ITS stations as well as the distribution of packets in geographical areas. [76]

8.1.4.2.1. ETSI 102 636-4-2

Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5

The present document specifies the media-dependent functionalities for GeoNetworking [1] over ITS-G5 [2] as a network protocol for ad hoc routing in vehicular environments. [76]

8.1.4.2.2. ETSI 102 636-4-1

Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality

The present document specifies the media-independent functionality of the GeoNetworking protocol. [76]

8.1.4.2.3. ETSI 102 636-5-1

Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol

The present document specifies the Basic Transport Protocol (BTP) for the transport of packets among ITS stations. It resides on top of the GeoNetworking protocol specified in ETSI EN 302 636-4-1 [5] and ETSI TS 102 636-4-2 [i.2] and below the ITS-S facilities layer. It provides an end-to-end, connection-less and unreliable transport service. [76]

8.1.4.3. IPv4 (RFC 760)

RFC 760 - The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. Such a system has been called a "catenet" [1]. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

8.1.4.4. IPv6 (RFC 2460)

RFC 2460 - IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4) [RFC-791]. The changes from IPv4 to IPv6 fall primarily into the following categories:

- Expanded Addressing Capabilities

  IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes.

/ Header Format Simplification

Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.

/ Improved Support for Extensions and Options

Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

/ Flow Labeling Capability

A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

8.1.4.5. TCP (RFC 761)

RFC 761 - The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks.

This document describes the functions to be performed by the Transmission Control Protocol, the program that implements it, and its interface to programs or users that require its services.

8.1.4.6. UDP (RFC 768)

RFC 768 - This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) [1] is used as the underlying protocol. This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) [2].

8.1.5. Facilities

8.1.5.1. Advanced Message Queuing Protocol

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.[79]

AMQP mandates the behavior of the messaging provider and client to the extent that implementations from different vendors are interoperable, in the same way as SMTP, HTTP, FTP, etc. have created interoperable systems. Previous standardizations of middleware have happened at the API level (e.g. JMS) and were focused on standardizing programmer interaction with different middleware implementations, rather than on providing interoperability between multiple implementations.[80] Unlike JMS, which defines an API and a set of behaviors that a messaging implementation must provide, AMQP is a wire-level protocol. A wire-level protocol is a description of the format of the data that is sent across the network as a stream of bytes. Consequently, any tool that can create and interpret messages that conform to this data format can interoperate with any other compliant tool irrespective of implementation language.

8.1.5.2. J2353 - Advanced Traveler Information Systems (ATIS)

This data dictionary provides the data elements needed to provide services related to traveller's information. The data dictionary herein provides the foundation for ATIS message sets for all stages of travel (pre-trip and end route), all types of travellers (drivers, passengers), all categories of information, and all platforms for delivery of information (in-vehicle, portable devices, kiosks, etc.). The elements of this document are the basis for the SAE ATIS Message Set Standard J2354 and are entered into the SAE Data Registry for ITS wide coordination.

In C-MobILE, this protocol can be used to provide parking information for MPA and UPA services, as recommended by the ARC-IT Reference Architecture in the US.[16]

8.1.5.3. Standard for Publishing Dynamic Parking Data (SPDP)

It is a Dutch open standard that not only describes the meaning and format of the data elements, but also the exchange protocol. Dynamic data is the primary concern (the number of currently available parking places). It is also possible to add various static features of the parking facilities in question.

C-MobILE MPA and UPA's services can make use of this standard to provider parking information to the drivers.[17]

8.1.5.4. CAM (ETSI 302 637-2)

Cooperative awareness within road traffic means that road users and roadside infrastructure are informed about each other's position, dynamics and attributes. Road users are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians and roadside infrastructure equipment including road signs, traffic lights or barriers and gates. The awareness of each other is the basis for several road safety and traffic efficiency applications with many use cases as described in ETSI TR 102 638 [i.1]. It is achieved by regular exchange of information among vehicles (V2V, in general all kind of road users) and between vehicles and road side infrastructure (V2I and I2V) based on wireless networks, called V2X network and as such is part of Intelligent Transport Systems (ITS).
The information to be exchanged for cooperative awareness is packed up in the periodically transmitted Cooperative Awareness Message (CAM).[18]

8.1.5.5. DENM (ETSI 302 637-3)

A DENM contains information related to a road hazard or an abnormal traffic conditions, such as its type and its position. The DEN basic service delivers the DENM as payload to the ITS networking & transport layer for the message dissemination. Typically for an ITS application, a DENM is disseminated to ITS-Ss that are located in a geographic area through direct vehicle-to-vehicle or vehicle-to-

[16] https://www.sae.org/

[17] https://nationaalparkeerregister.nl

[18] https://portal.etsi.org

infrastructure communications. At the receiving side, the DEN basic service of a receiving ITS-S processes the received DENM and provides the DENM content to an ITS-S application.[19]

8.1.5.6. IVIM (ETSI TS 103 301)

IVI service is one instantiation of the infrastructure services to manage the generation, transmission and reception of the IVIM messages. An IVIM supports mandatory and advisory road signage such as contextual speeds and road works warnings. IVIM either provides information of physical road signs such as static or variable road signs, virtual signs or road works. The IVIM message follows the structure defined in CEN ISO/TS 19321 with an ETSI header. The header of the IVIM is defined in the data dictionary ETSI TS 102 894-2.

ETSI TS 103 301:
https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=50633
ETSI TS 102 894-2:
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=43353&curItemNr=2&totalNrItems=3&optDisplay=10&qSORT=HIGHVERSION&qETSI_ALL=TRUE&SearchPage=TRUE&qETSI_NUMBER=102+894-2&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=&qKEYWORD_BOOLEAN=&qCLUSTER_BOOLEAN=&qFREQUENCIES_BOOLEAN=&qSTOPPING_OUTDATED=&butSimple=Search&includeNonActiveTB=FALSE&includeSubProjectCode=&qREPORT_TYPE=SUMMARY
CEN ISO/TS 19321:
https://www.iso.org/standard/64606.html

8.1.5.7. MAPEM (ETSI TS 103 301)

The MAPEM is used to represent the topology/geometry of a set of lanes. E.g. considering an intersection MAPEM defines the topology of the lanes or parts of the topology of the lanes identified by the intersection reference identifier. The MAPEM does not change very often in time. The same MAPEM is retransmitted with the same content. The MAPEM message follows the structure defined in SAE J2735 with an ETSI header. The header of the IVIM is defined in the data dictionary ETSI TS 102 894-2.

ETSI TS 103 301:
https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=50633
ETSI TS 102 894-2:
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=43353&curItemNr=2&totalNrItems=3&optDisplay=10&qSORT=HIGHVERSION&qETSI_ALL=TRUE&SearchPage=TRUE&qETSI_NUMBER=102+894-2&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=&qKEYWORD_BOOLEAN=&qCLUSTER_BOOLEAN=&qFREQUENCIES_BOOLEAN=&qSTOPPING_OUTDATED=&butSimple=Search&includeNonActiveTB=FALSE&includeSubProjectCode=&qREPORT_TYPE=SUMMARY
SAE J2735:
https://www.sae.org/standards/content/j2735_200911/

8.1.5.8. SPATEM (ETSI TS 103 301)

The SPATEM is used to represent the status of a set of traffic lights usually placed in the same geographical area. It is usually sent together with the MAPEM message to have a very accurate representation of the traffic lights and the topology of the lanes and roads where they are relevant. The SPATEM message follows the structure defined in SAE J2735 with an ETSI header. The header of the SPATEM is defined in the data dictionary ETSI TS 102 894-2.
The SPATEM messages are used in I2V services such as GLOSA, SVW and CTLP within C-MobILE .

ETSI TS 103 301:
https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=50633
ETSI TS 102 894-2:
https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=43353&curItemNr=2&totalNrItems=3&optDisplay=10&qSORT=HIGHVERSION&qETSI_ALL=TRUE&SearchPage=TRUE&qETSI_NUMBER=102+894-2&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=&qKEYWORD_BOOLEAN=&qCLUSTER_BOOLEAN=&qFREQUENCIES_BOOLEAN=&qSTOPPING_OUTDATED=&butSimple=Search&includeNonActiveTB=FALSE&includeSubProjectCode=&qREPORT_TYPE=SUMMARY
SAE J2735:
https://www.sae.org/standards/content/j2735_200911/

[19] https://portal.etsi.org

8.1.5.9. MQTT (ISO/IEC PRF 20922)

MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.

The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. The C-MobILE project uses this protocol to create a GeoMessaging system able to disseminate geo-messages using cellular communications to specific areas.[20]

8.1.5.10. TTI (TPEG2) (ISO 21219-14)

This standard specifies the TPEG Parking Information application which has been designed to deliver parking information to a variety of receivers using a number of different channels, foremost of course are digital broadcasting and Internet technologies. Parking information may be presented to the user in many different ways, including text, voice, or graphics. [21]

8.1.6. Application

8.1.6.1. CEN (ISO 19091)

Description: This standard defines the message, data structures and data elements to support exchanges between the roadside equipment and vehicles to address applications to improve safety, mobility and environmental efficiency. This focuses on specifying the details of the SPaT (Signal Phase and Time), MAP, SSM and SRM supporting the use cases defined. [22]

8.1.6.2. DATEX

Description: DATEX standards was developed for information exchange between traffic management centers, traffic information centers and service providers. DATEX II, the second generation of DATEX, also supports exchange with all actors in the traffic and travel information sector. It is a standardized e-language for traffic and travel data exchange. It makes use of mainstream IT technologies such as XML and web services.[23]

The below technical specification specifies and defines component facets supporting the exchange and shared use of data and information in the field of traffic and level. They establish specifications for data exchange between any two instances of the following actors:

i. Traffic Information Centers (TIC)
ii. Traffic Control Centers (TCC)
iii. Service Providers (SP).

The below technical specification is applicable to:

i. Traffic and Travel information which is of relevance to road networks
ii. Public transport information that is of direct relevance to the use of road network

They cover, at least, the following types of informational content:

i. road traffic event information – planned and unplanned occurrences both on the road network and in the surrounding environment;
ii. operator initiated actions;
iii. road traffic measurement data, status data, and travel time data;

[20] https://www.iso.org/standard/69466.html

[21] https://www.iso.org/standard/63115.html

[22] https://www.evs.ee/tooted/cen-iso-ts-19091-2017

[23] http://www.datex2.eu/, https://portal.its-platform.eu/index.php?q=filedepot_download/1729/5367

iv. travel information relevant to road users, including weather and environmental information;
v. road traffic management information and information and advice relating to use of the road network

8.1.6.2.1. CEN 16157-1

This part specifies the DATEX II framework of all parts of this Technical Specification, the context of use and the modelling approach taken and use throughout the technical specifications. This approach is described using formal methods and provides the mandatory reference framework for all other parts. [24]

8.1.6.2.2. CEN 16157-2

This part specifies the informational structures, relationships, roles, attributes and associated data types, for the implementation of the location referencing systems used in association with the different publications defined in the Datex II framework. It also defines a DATEX II publication for exchanging predefined locations. This is part of the DATEX II platform independent data model. [25]

8.1.6.2.3. CEN 16157-3

This part specifies the informational structures, relationships, roles, attributes and associated data types required for publishing situation traffic and travel information within the DATEX II framework. This is specified as a DATEX II Situation Publication sub-model which is part of the DATEX II platform independent model, but this Part excludes those elements that relate to location information which are specified in CEN/TS 16157-2 and those elements that relate to VMS settings which are specified in Part 4 of CEN/TS 16157. [26]

8.1.6.2.4. CEN 16157-4

This part specifies the informational structures, relationships, roles, attributes and associated data types required for publishing variable message sign (VMS) information within the Datex II framework, which is specified in two parts:

i. DATEX II VMS publication sub-model, and
ii. A VMS Table publication sub-model.

The VMS publication supports the exchange of the graphic and textual content of one of several VMS plus any status information on device configuration that aid the comprehension of the informational content.[27]

8.1.6.2.5. CEN 16157-5

This part of the specifies the informational structures, relationships, roles, attributes and associated data types required for publishing measured and elaborated data within the Datex II framework. This is specified in three sub-models, a DATEX II Measurement Site Table Publication sub-model, a DATEX II Measured Data Publication sub-model and a DATEX II Elaborated Data Publication sub-model. [28]

8.1.6.2.6. CEN 16157-6

This technical specification is applicable to Parking Information (static and dynamic information about urban or interurban parking sites including Truck Parking information). In addition to TICs, TCCs, and SPs, this specification can be used by Parking Operators as well.

This covers the following type of information content:

[24] https://infostore.saiglobal.com/preview/is/en/2011/srcen-ts16157-1-2011.pdf?sku=1496220

[25] https://www.evs.ee/tooted/cen-ts-16157-2-2011

[26] https://www.evs.ee/tooted/cen-ts-16157-3-2011

[27] https://infostore.saiglobal.com/preview/is/en/2014/s.r.cen-ts16157-4-2014.pdf?sku=1730302

[28] https://infostore.saiglobal.com/preview/is/en/2014/s.r.cen-ts16157-5-2014.pdf?sku=1730303

Parking information including static content (description and attribution of parking areas, parking facilities and single parking spaces) and dynamic content (occupancy and vehicle measurement information). It covers Urban Parking information as well as Truck Parking information.

This part specifies the informational structures, relationships, roles, attributes and associated data types required for publishing parking information within the DATEX II framework. This is specified as a DATEX II Parking Publication sub-model which is part of the DATEX II platform independent model, but this part excludes those elements that relate to location information which are specified in CEN/TS 16157-2. [29]

8.1.6.3. ETSI 102 638

This defines a Basic Set of Applications (BSA) to be specified by Intelligent Transport Systems mainly focusing on V2V, V2I and V2V communications in the V2X dedicated frequency band. However, it does not exclude using other access technologies such as cellular networks and/or broadcasting systems. [30]

8.1.6.4. ETSI 102 894-2

This defines a repository of a set of data elements and data element sets, denoted as data frames, that are commonly used in the ITS applications and facilities layer messages. It focused on data elements being used by Cooperative Awareness and by the Decentralized Environmental Notification basic service. It does not specify the syntax and requirements of data elements in the specific context of any message.[31]

8.1.6.5. ETSI ITS BSA

Basic Set of Applications (BSA) is defined as a set of ITS applications/use cases that are considered as deployable within a three years' time scale after the complete standardization of the system.[32]

8.1.6.6. NTCIP 1202

National transportation Communications for ITS Protocol (NTCIP) 1202 defines objects which are specific to actuated signal controllers and standardized object groups which can be used for conformance statements. This consists of mandatory requirements which are classified as NEMA (http://www.nema.org/pages/default.aspx) standard publication and information that is in conformance with NEMA Authorized Engineering Information.[33]

8.1.6.7. SAE J2735

This SAE Standard specifies a message set, and its data frames and data elements specifically for use by applications intended to utilize the 5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments. The message set designed in this standard has been designed, to an extent, to also be of potential use for applications that may be deployed in conjunction with other wireless communications technologies.[34]

8.1.6.8. UTMC TS004.006

This provides standards for UTMC (Urban Traffic Management and Control) "common data", which is data communicated between applications of a UTMC system, or between a UTMC system and an external system. It does this by holding definitions of current UTMC

[29] http://www.datex2.eu/sites/www.datex2.eu/files/TC_278_prCEN_TS_16157-6_E.pdf

[30] http://www.etsi.org/deliver/etsi_tr%5C102600_102699%5C102638%5C01.01.01_60%5Ctr_102638v010101p.pdf.

[31] http://www.etsi.org/deliver/etsi_ts/102800_102899/10289402/01.02.01_60/ts_10289402v010201p.pdf

[32] http://www.etsi.org/deliver/etsi_ts/102800_102899/10289401/01.01.01_60/ts_10289401v010101p.pdf

[33] https://www.ntcip.org/library/documents/pdf/1202v0107d.pdf

[34] https://www.sae.org/standards/content/j2735_200911/

Objects and session management protocols and making them available to users. It specifies that a new UTMC system should normally use currently registered UTMC Objects and session management protocols as far as they are applicable.[35]

[35] https://img1.wsimg.com/blobby/go/e3f917f3-2941-4106-a2c5-a25d4230e979/downloads/1bnfocn06_900975.pdf