EUROPEAN COMMISSION

HORIZON 2020
H2020-ART-2016-2017/H2020-ART-2017-Two-Stages
GA No. 769115

ENSEMBLE

ENabling **S**af**E** **M**ulti-**B**rand p**L**atooning for **E**urope

Deliverable No.	D4.2	
Deliverable Title	Service and Strategic Layer Design	
Dissemination level	Public	
Written By	Jörg Lützner, Continental; Jonas Martensson, KTH; Alejandro Manilla, IDIADA; Nico Deschle, TNO; Ernst Jan van Ark, TNO	09-10-21
	Lead Partner: Jörg Lützner, Continental	09-10-21

Checked by	[WP Leader: Franziska Schmidt, Universite Gustaf Eiffel]	01-10-2021
Approved by	Coordinator: Marika Hoedemaeker, TNO	08-10-2021
Status	APPROVED BY EC	13-12-2022

Please refer to this document as:

Lützner, J. (2021). *Service and Strategic Layer Design.* D4.2 of H2020 project ENSEMBLE, (www.platooningensemble.eu)

Disclaimer:

ENSEMBLE is co-funded by the European Commission, DG Research and Innovation, in the HORIZON 2020 Programme. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

TABLE OF CONTENTS

Revision history

Version	Date	Author	Summary of changes	Status
2.0	10/05/2021	J. Lützner (Continental)	First content complete draft	Prepared
3.0	18/05/2021	J. Lützner (Continental)	Refinements	Revised
4.0	27/05/2021	J. Lützner (Continental)	Further refinement	Revised
7.0	22/06/2021	J. Lützner (Continental)	Final draft for review	Revised
9.0	07/09/2021	J. Martensson A. Manila	Update of T4.2.1 & T4.2.3 content	Revised
10	10/09/2021	J. Lützner	Final draft for review	Revised
11	27/09/2021	J. Lützner	Final version	Revised
12	10/08/2022	Van Ark	Updated after EC comments (1)	
13	04/11/2022	Hoedemaeker	Updated after EC comments (1)	

FIGURES

TABLES

1. EXECUTIVE SUMMARY

1.1. Context and Need of Service and Strategic Layers

Context

The commercial viability of platooning not only depends on successful multi-brand platooning itself, but also on the availability of connectivity from the vehicles involved to a backend/cloud. This enables a range of services, some of which are mandatory for safe and efficient platooning. Other services also add value but are more in the field of “nice to have”. These could also enable differentiation between different service providers.

There are already numerous backends/clouds in commercial transportation. It is not unusual for each stakeholder to have one, e.g. OEMs, fleet management service providers, carriers, and road authorities. This landscape is given in the project. The platooning service and strategic layers must blend into this landscape and cannot expect this to be adapted to accommodate for platooning.

The focus of the Strategic and Service Layers covers all services which are based on cellular communication. Services which are based on V2X communication are address in the deliverables D3.1 (tactical layer), D2.8 (V2V communication), D2.9 (V2X security) and D2.6 & D2.7 (I2V communication).

T4.2 scope

While the actual (commercial/business-grade) services based on the Strategic and Services layers will not be developed in ENSEMBLE, we aim to specify the interfaces, required data, formats etc., in a similar vein as APIs are developed to connect various software packages together, without building the actual (commercial) software packages. With these information prescriptions, truck OEMs, telematics providers, mapping solution providers, location-based service start-ups etc. may implement their own commercial (multi-brand) platooning coordination services on the Strategic and Service Layer. The following work was done to achieve this:

1. Collect possible macro and micro-issues associated with the Strategic and Service Layers including platooning services and identify possible solutions thereof
2. Identify and distinguish between mandatory and non-mandatory services for both Platooning Support Function and Platooning Autonomous Function. The APIs are only described for the mandatory services
3. Identify possible cyber security risks and associated countermeasures for the services and their IT landscape
4. Use simulations to understand the influence of various parameters involved in platoon matching services

The results are verified through reviews with the projects partners as well as external stakeholders.

Abstract of this Deliverable

Connectivity is mission critical for platooning. This applies first and foremost for the low latency V2V communication between vehicles to engage, maintain and leave a platoon. There is a second category of communication which is equally important for platooning, the (often cellular) communication to a backend that provides the delineation and context for a platoon. In example under which conditions forming a platoon is allowed on that specific road segment. This link is vital for the efficient formation of platoons but can also enable numerous other services which help to make platooning viable and attractive. This deliverable describes the services and specifies their system architecture and the API for a platoon formation service. Generic issues and associated solutions are formulated. Cyber security requirements are also described in alignment with accepted standards. Finally, real world transportation data was used to verify possible platooning penetration. All tasks were theoretical work which pave the way for a future level playing field.

2. INTRODUCTION

2.1. Background

Figure 1 shows the layered structure of the communication involved in platooning as used in the ENSEMBLE project. Most initial researches and pre-development activities on platooning focused on demonstrating and refining platooning itself. Only the Tactical and Operational Layers are required for this. These layers are covered in other deliverables, as mentioned before.

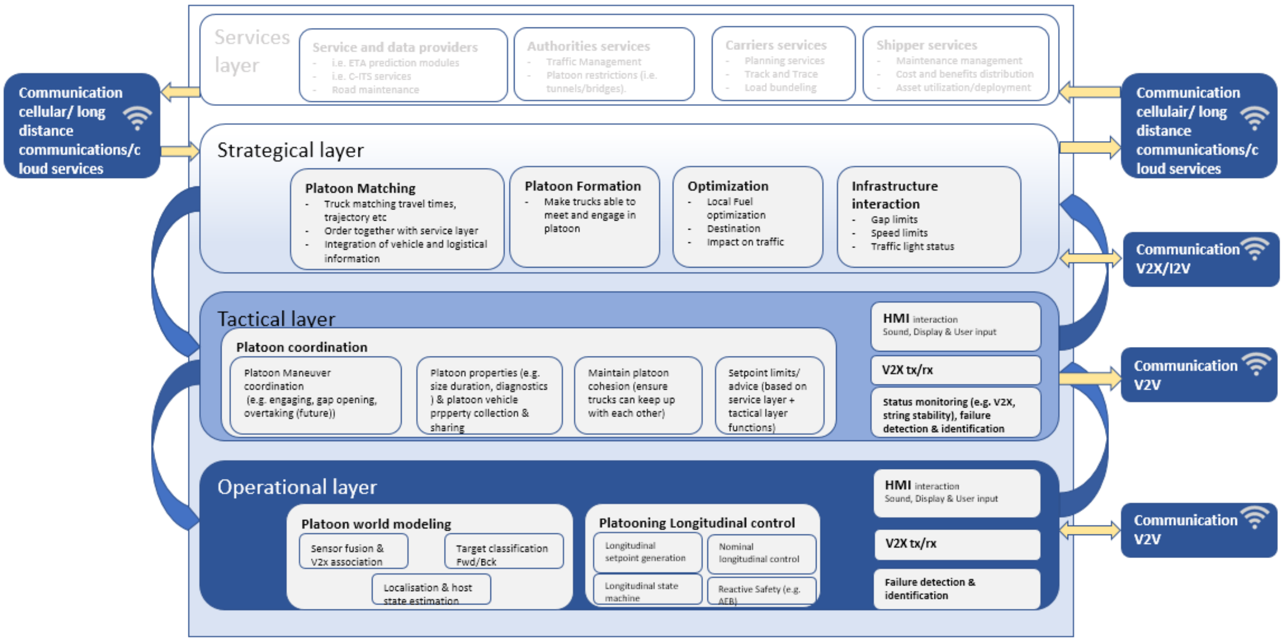


Figure 1. Diagram depicting the platooning layers.

More recent projects like Sweden4Platooning (Dellrud, 2020) have also identified the need of services as part of a solution to make platooning a commercially viable proposition. These services are located in the Strategic and Service layers. These, in turn, are connected to established parts of the commercial transportation ecosystem like OEM clouds, carrier clouds, fleet management clouds, road operator clouds etc.

All services mentioned in this deliverable require a cellular connection from the vehicle to a backend/cloud. The nature of this connection means that these services, while being necessary for platooning, cannot be safety critical. No services based on V2X communication will be described in this deliverable. The services also require some sort of human machine interface (HMI) in the vehicles to either receive information or input data. This could either be the vehicle HMI, a tablet or smartphone, or the HMI of a fleet management solution.

Two different platooning functions have been derived in ENSEMBLE: Platooning Support Function and Platooning Autonomous Function. Both will be considered in this deliverable; whereby Platooning Support Function will be the basis. Platooning Autonomous Function leads to certain add-ons. Both functions are described in ENSEMBLE deliverable D2.3

Various stakeholders must be considered. This includes the carriers which will probably commission the services. The OEMs play a major role since the vehicles are key data providers (position, velocity, etc.). Road authorities must be considered since they are responsible for the safety on highways as well as allowing or restricting functionality in certain areas. Finally, the interests of the drivers must also be considered. The issues for all these stakeholders must be considered to find a viable and optimal solution.

The services required are partly related to which phase of platooning the market is in. We expect partially differing services between day 1, when platooning is first available and later, when there is a market penetration of vehicles on the road with platooning capability. Both phases will be considered in the deliverable.

It is mandatory to consider the regulatory environment. The key driver in this arena is European Data Protection Regulation (Comission, 2018). All services proposed and specified must be GDPR compliant. This will be validated as part of the deliverable.

Society demands that state-of-the-art cyber security is implemented in any connected solutions. In our project this is even more important since the vehicles are capable of autonomous driving (see Platooning Autonomous Function). If hackers access these vehicles; they could hijack and drive these which could lead to severe damages and even fatalities. For this reason, there is a dedicated subtask on this subject.

2.2. Aim

From a technical point of the view the target of this deliverable is to provide service providers with a framework so that they can develop and operate attractive platooning services which firstly make platooning possible and secondly make platooning a more even efficient and attractive proposition.

The ultimate goal of this task is to provide possible service providers a level playing field, giving each an equal chance of business success. This being the case it was decided not to program a reference implementation of any service so that no partner has a head start in the race for this lucrative business.

2.3. Structure of this report

The task T4.2 is split into 4 subtasks:

- T4.2.1: This activity will yield an overview of which (multi-brand) specific issues arise when trying to form multi-brand platoons. For instance, braking distances may be longer from a functional

safety point of view. In terms of Service Layer specification, it may be beneficial to coordinate platoons that show as little heterogeneity between trucks as possible.
- T4.2.2: Describe the requirements for the high-level decision-making regarding the scheduling and routing of platoons (Strategic Layer) and define the interfaces for the Service Layer regarding coordination of platoons and additional third-party services and communication to road authorities.
- T4.2.3: Delineate (cyber)security prerequisites for data exchange and management for the Strategic and Service Layer, and the interaction with Tactical layer. If platoon coordination is happening with a combination of LRC and DSRC, it is necessary to focus on the cyber security of the technology. This activity lists potential security threats and potential mitigation strategies.
- T4.2.4: Develop a proof-of-concept for multi-brand platoon coordination. The aim is to prove the feasibility of scheduling and routing of platoons.

The core of this deliverable will be the individual reporting of the approach taken and the results achieved of each subtask. In addition, the deliverable will confirm the commitment given in the Description of Work has been achieved.

3. DELIVERABLE CHAPTERS

During the work, it became apparent that T4.2.2 is the center of gravity of the task. The result of this work is the input for the other subtasks, especially T4.2.1 and T4.2.3 as can be seen in figure 2. Thus, the work will be presented in the order T4.2.2, T4.2.1, T4.2.3 and then T4.2. 4.

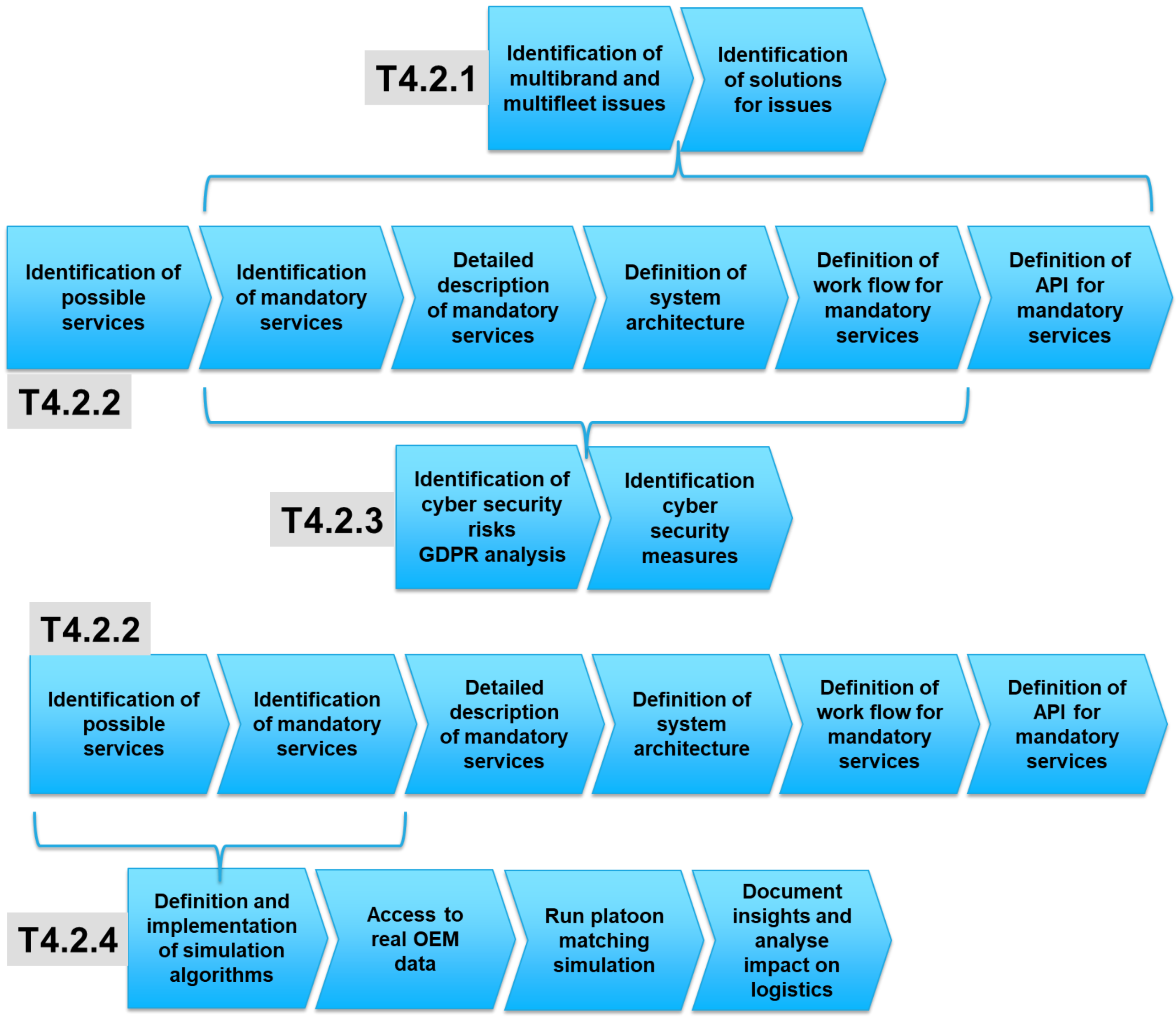


Figure 2. Interdependencies of subtasks T4.2.1, T4.2.2. and T4.2.3. T4.2.4

3.1. T4.2.2

Many technologies are viewed as enablers for platooning. A starting hypothesis is that a connectivity to a backend and associated services is one of these enablers. The purpose of the subtask is to investigate this hypothesis and, if confirmed, then to describe the interface to a backend to provide potential services providers with a level playing field. The work in this subtask followed a defined workflow:

1. Brainstorming of possible service ideas in alignment to the platooning use cases and method of platoon formation
2. Identification of the mandatory services without which platooning would not be possible and safe
3. Definition of system architecture and how this is embedded in the transportation ecosystem
4. Description of mandatory services including data required and workflow
5. Definition of the API for each mandatory service from the view of a service provider

The work and results of these steps will be described in detail as part of the next sections, the order above is hereby adhered to.

3.1.1. Collection of possible services

The primary method for the collection of possible service ideas was brainstorming in the team. Three criteria were introduced to give the brainstorming structure. Firstly, the platooning phases were considered, i.e., formation, engaging, platooning, and disengaging. Secondly the stakeholders were considered. While there are many of these, the work focused on carriers, drivers, and road authorities. Lastly the method by which the platoon was formed was considered. This was structured as shown below:

Table A. The four main cases in which platoon can be formed.

Orchestrated @ hub	Spontaneous @ parking
Orchestrated @ road	Spontaneous @ road

Table B below shows the result of the brainstorming for Platooning Support Function. The ideas are structured according to the use case, stakeholder, and way in which the platoon was formed.

Table B. Possible services for platooning support function.

Use Case	**Stakeholders**			
	Carriers/Drivers*		**Authorities/Infrastructure***	
Formation	Mission/load bundling service to create platoons @ hub Driver rating service Vehicle capability service	Real time platoon matching service to analyze best partner Driver rating service Vehicle capability service	Information on go/no go road segments for platooning	Information on go/no go road segments for platooning
	Cross-fleet fleet management service as basis for platoon matching Driver rating service Vehicle capability service	Real time platoon matching service to analyze best partner Driver rating service Vehicle capability service	Information on go/no go road segments for platooning	Information on go/no go road segments for platooning
Engage	n/a	n/a	Information on go/no go road segments for platooning	Information on go/no go road segments for platooning
	n/a	n/a	Information on go/no go road segments for platooning	Information on go/no go road segments for platooning
Platoon	Communication service between drivers	Incentivization service to distribute savings Communication service between drivers	Information on go/no go road segments for platooning Platoon documentation service	Information on go/no go road segments for platooning Platoon documentation service
	Incentivization service to distribute savings Communication service between drivers	Incentivization service to distribute savings Communication service between drivers	Information on go/no go road segments for platooning Platoon documentation service	Information on go/no go road segments for platooning Platoon documentation service
Disengage	Truck parking service Driver rating service Documentation service	Truck parking service benefits Driver rating service Payment service to share benefits Documentation service	n/a	n/a
	Truck parking service Driver rating service Payment service to share benefits Documentation service	Truck parking service Driver rating service Payment service to share benefits Documentation service	n/a	n/a

A similar methodology was used to identify possible services for Platooning Autonomous Function. This revealed the results shown in Table C below. The red text indicates incremental services for Platooning Autonomous Function compared to Platooning Support Function

Table C. Possible services for platooning autonomous function.

Use Case	Stakeholders			
	Carriers/Drivers*		Authorities/Infrastructure*	
Formation	Mission/load bundling service to create platoons @ hub Driver rating service Vehicle capability service	n/a	Information on go/no go road segments for platooning	n/a
	n/a	n/a	n/a	n/a
Engage	Remote control service	n/a	Information on go/no go road segments for platooning	n/a
	n/a	n/a	n/a	n/a
Platoon	Communication service between drivers Remote control service	n/a	Information on go/no go road segments for platooning Platoon documentation service Dynamic road information service	n/a
	n/a	n/a	n/a	n/a
Disengage	Truck parking service Driver rating service Documentation service Remote control service	n/a	n/a	n/a
	n/a	n/a	n/a	n/a

The focus of Platooning Autonomous Function is driverless (or even unmanned) following vehicles. These can only be formed in an orchestrated manner since a driver will need to get out of the following truck prior to the platoon starting. Spontaneous platoon formation only makes sense if a driver is present. Effectively this is identical to a join from behind maneuver and thus no services are required. This is the reason the columns associated with spontaneous platoon formation are "n/a" in Table C. Similarly, orchestrated platoon formation on the road does not fit to Platooning Autonomous Function since the driver of the following vehicle cannot leave the truck.

All services listed in the table above are described in more detail in Table D below. In addition to the description, the table also shows which input and output data the service requires. This is necessary for the later description of the API for the platooning service provider.

Table D. Description of possible platooning services

Service	Description	Output data	Input data	Stakeholder	Use Case
Mission/load bundling service	Identification of how loads can be assigned to available transport capacity = mission Vehicles/trailer are fill based on load description and schedule of loads Identification of which vehicle/trailer missions can be combined to a platoon The service can be accessed via a web or app interface	Load per vehicle Vehicle schedule Vehicle routing Platooning vehicle identification Position of tractors & trailers	Load description Departure window of load Arrival window of load Destination of load Location of load	Shippers/ Carriers	Formation
Cross-fleet fleet management service	Pre-departure identification of which x-fleet missions could be linked to form a platoon on the road Optional real time guidance of the trucks to meeting point The service can be accessed via a web or app interface	Vehicle meeting location Vehicle meeting timing	Vehicle schedule Vehicle routing Vehicle position	Carriers/ Service Provider	Formation
Vehicle capability service	Service broadcasts the capabilities of a vehicle which are relevant for platooning	Vehicle capability rating	Vehicle horsepower Vehicle load/weight Vehicle braking capacity Vehicle height & width	Carriers/ Service Provider	Formation
Real time matching service	Real time identification of which x-fleet vehicles could be linked to form a spontaneous platoon based on actual location, destination, platooning length, drivers' rest time, ETA and flexibility regarding delays. The driver is informed via mobile device or vehicle HMI	Location of best suited partner	Vehicle location Vehicle destination Vehicle route (w/ alternatives) Drivers rest time Vehicle ETA Schedule agility	Service Provider/ Carriers / Drivers	Formation

Incentivization service	Financial compensation of the fleet of leading trucks in platoons so that all vehicles in the platoon have an equal financial benefit. Based on calculation of fuel saving considering platoon speed, platooning distance and vehicle separation The service can be accessed via web interface	Financial compensation per fleet	Platoon ID Position of the platoon Vehicle Id Vehicle separation Vehicle speed Vehicle position in the platoon	Carriers / Service Provider	Platoon
Communication service between drivers	Push-to-talk or duplex audio communication between the drivers in a platoon The driver can access the service via mobile device or vehicle HMI	Speech channel between drivers	Id of vehicles in the platoon (Call number) of vehicles in a platoon	Carriers / Drivers	Engage & Platoon
Truck parking service	Identification of best suited and vacant parking lot at the end of a drivers' driving time in advance Option: reservation of parking space in parking lot in advance A driver accesses the service via mobile device or vehicle HMI	Parking lot proposal Option: Parking space reservation	Vehicle location Vehicle route Driver's drive and rest time data Parking lot location Parking lot occupancy Vehicle size (l*w*h)	Drivers / Service Provider	Disengage
Driver rating service	Star rating of driver performance/reliability/ friendliness from other drivers in a platoon while platooning. A driver can call up his current rating at any time via a mobile device, vehicle HMI or web interface	Driver ID Star rating in one or more categories for a specific driver	Driver ID Scoring from other drivers in a platoon in one or more categories	Carriers / Drivers / Service Provider	Disengage
Information on go/no go road segments for platooning	Service to provide the location of go / no-go road segments for platooning to the vehicles. The driver and platooning system solution are both informed of a forthcoming change of status	Advance notice of forthcoming change in road status	Weather data Real time roadwork locations Bridge location Toll booth locations Tunnel locations	Authorities	all

Platoon documentation service	Geolocation and recording of the position, composition and of platoons Access of authorities to this data via web interface	Records of the location of platoons	GPS location of platoon PlatoonID (locally unique)	Authorities	all
Remote Control Service	The ability of an operator to control a driverless vehicle from an offboard control center either directly or indirectly This is a safety related fallback for a driverless following vehicle	Trajectory for the driverless vehicle to maneuver or set of commands for the vehicle's actuators	Signals from various vehicles sensors like cameras radar and lidar	Carrier	Platoon
Dynamic Road Information Service	Close to real time advanced information on possible restriction and dangers of the road ahead This information is provided to the driver of the leading vehicle in an autonomous platoon	Location and description of restrictions/dangers per road segment	Floating car data, road sensor data, roadwork information	Authorities	Platoon

While all these services add value, the ENSEMBLE project decided to focus on the services which are mandatory and to offer API specifications for these only. That does not mean only mandatory services will be visible in the market. A service provider or OEM could provide more than the mandatory services to differentiate from their competitors.

3.1.2. Identification of mandatory services

The criteria for the decision about whether a service is mandatory are quite simple and as follows:

1. Services which are necessary for the safety of the vehicle, platoon or other road users
2. Services without which platooning will not function, i.e., platoons cannot be formed
3. Services mandated by a stakeholder

These criteria were applied to the above services and led to the following selection (bold = mandatory) shown in Table E.

Table E. Identification of mandatory platooning services.

Service	Description	Mandatory	Reasoning

Mission/load bundling service	Identification of how loads can be assigned to available transport capacity = mission Vehicles/trailers are filled based on load description and schedule of loads Identification of which vehicle/trailer missions can be combined with a platoon The service can be accessed via a web or app interface	No	Will be performed by the carrier/shipper in their available IT landscape and not by a platooning service provider
Cross-fleet truck matching service	**Pre-departure identification of which x-fleet missions could be linked to form a platoon on the road Optional real time guidance of the trucks to meeting point The service can be accessed via a web or app interface. The output is available to the fleet and the drivers**	**Yes**	**Platoons cannot be formed without this matching service, especially if there is low penetration of platooning capable vehicles on the roads**
Vehicle capability service	Service broadcasts the capabilities of a vehicle which are relevant for platooning	No	The minimum distance between vehicles is pre-defined by the platooning technology so that this service is not required
Real time matching service	Real time identification of which x-fleet vehicles could be linked to form a spontaneous platoon based on actual location, destination, platooning length, drivers' rest time, ETA and flexibility regarding delays The driver is informed via a mobile device or vehicle HMI	No	Under the assumption that there is a high density of vehicle capable of platooning on a highway, the formation can be managed by short range communication and does not need a backend-based service
Incentivization service	Financial compensation of the fleet of leading trucks in platoons so that all vehicles in the platoon have an equal financial benefit. Based on calculation of fuel saving considering platoon speed, platooning distance and vehicle separation The service can be accessed via a web interface	No	The separation of the vehicles in the platoon is such that there are no significant fuel savings for the following vehicle. This makes the services obsolete.

Communication service between drivers	Push-to-talk or duplex audio communication between the drivers in a platoon The driver can access the service via mobile device or vehicle HMI	No	No dedicated service is required. If necessary, drivers could communicate via cellular communication.
Truck parking service	Identification of the best suited and vacant parking lot at the end of a drivers' driving time in advance Option: reservation of parking space in parking lot in advance A driver accesses the service via a mobile device or vehicle HMI	No	Parking is not a mandatory function inside platooning
Driver rating service	Star rating of driver performance/reliability/friendliness from other drivers in a platoon while platooning. A driver can call up his current rating at any time via a mobile device, vehicle HMI or web interface	No	The working assumption is that all drivers in platooning capable vehicles have a minimum of training before platooning. That makes a driver rating service obsolete
Information on go/no go road segments for platooning	**Service to provide the location of go / no-go road segments for platooning to the vehicles. The driver and platooning system solution are both informed of a forthcoming change of status**	**Yes**	**Road authorities impose restrictions on road segments e.g., bridges which limit vehicle speed or vehicle separation. These must be transmitted to vehicles so that platoons can take appropriate action before the restriction**
Platoon documentation service	Geolocation and recording of the position, composition and of platoons Access of authorities to this data via web interface	No	It will not be mandatory to track these vehicles since the vehicle separation while platooning is as legally mandated for individual vehicles
Remote Control Service	The ability of an operator to control a driverless vehicle from an offboard control center either directly or indirectly This is a safety related fallback for a driverless following vehicle	Depends on outcome of ongoing safety analysis	Could be a fallback in case the driverless vehicle must be externally maneuvered into a safe state

Dynamic Road Information Service	Close to real time advanced information on possible restrictions and dangers of the road ahead This information is provided to the driver of the leading vehicle in an autonomous platoon	No	Platoon negotiates hazards as it was a single truck

3.1.3. Definition of system architecture to enable mandatory services

The next task was to describe the offboard system architecture which can enable the mandatory services described above. It is highly desirable that this architecture utilizes interfaces which already exist in today's transportation ecosystem. There are 2 important interfaces which we assume are available in all platooning vehicles:

1. Each truck is connected to the backend of the OEM. This is a bidirectional interface allowing vehicle data to be uploaded and driver information or vehicle configuration data to be downloaded.

2. Most trucks today are connected to the fleet management system of the owner/carrier. This allows relevant vehicle data e.g., position to be uploaded and driver information to be downloaded. The driver interface for this is a smartphone, tablet or dedicated hardware.

Figure 3 illustrates the interfaces in a diagram. The diagram also considers the multi-brand, multi-fleet environment which must be considered. The clouds represent reality today as services are usually hosted in clouds and not on dedicated servers.

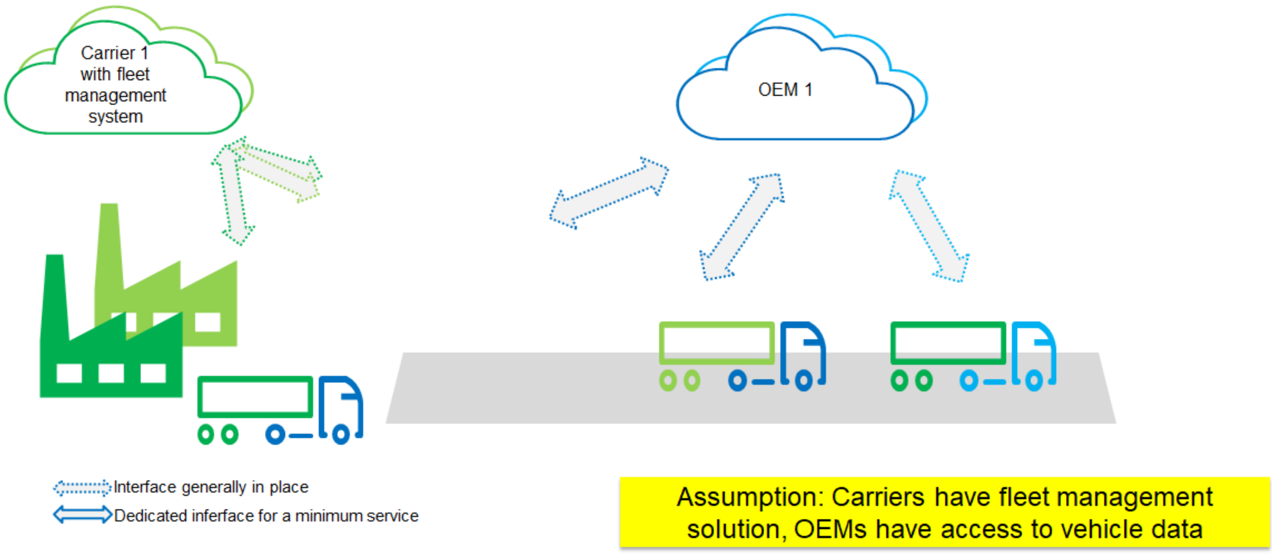


Figure 3. Existing interfaces in the transportation ecosystem, which are relevant for platooning.

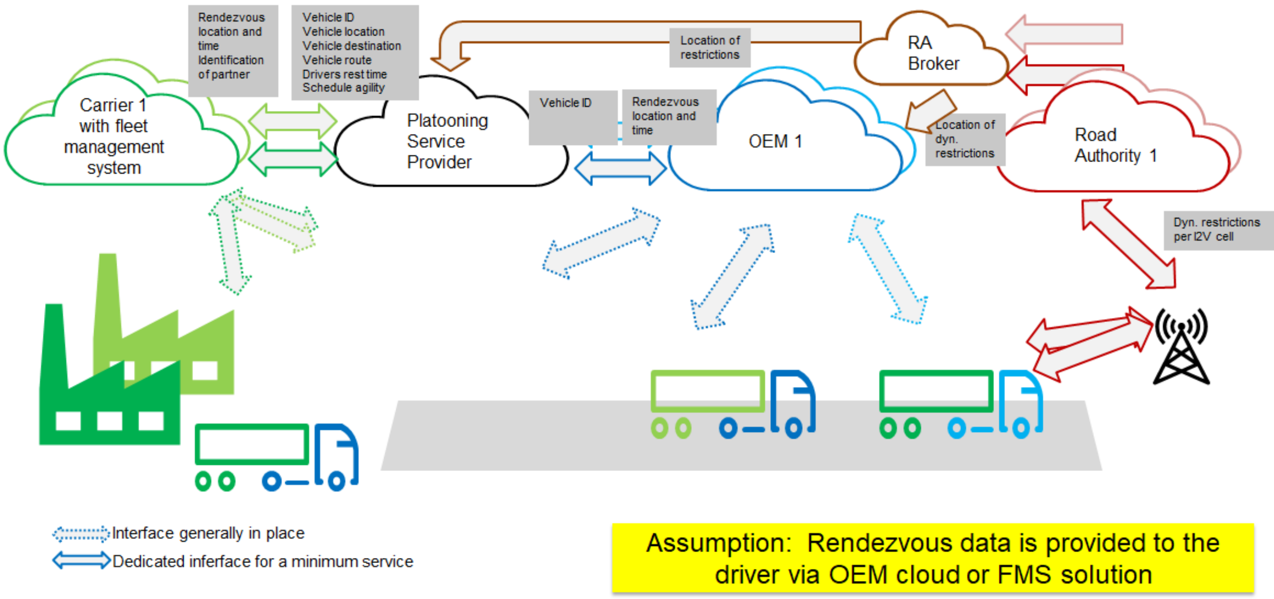


Figure 4. Offboard system architecture for mandatory platooning services.

Further infrastructure and interfaces were added to the basis interfaces to enable mandatory services. The resulting architecture schematic for the mandatory services is shown in Figure 4.

Two further clouds are added. The black cloud represents the 3rd party platooning service provider (PSP) which will provide a mandatory platoon matching service. The red clouds represent the road authorities. These are responsible for the provision of information on road restrictions. In Europe there are multiple road authorities providing heterogeneous information. Today it is already typical that brokers aggregate this information to make it more digestible for potential users. A broker (brown cloud) is included in the schematic. The fact that the arrow from the broker to the PSP is unidirectional demonstrates that this is more a simple data interface rather that a full-blown service.

To enable the platoon matching service the PSP obviously needs interfaces to the carriers. These query for possible platoon partners by providing future mission information. In return they receive proposals for platoons with rendezvous time and locations. A driver/truck can receive this information via a multitude of channels like smartphones, tablets, or dedicated FMS hardware. For the sake of simplicity, we assume the re-use of existing technology. As a fallback the rendezvous information can also be provided to the vehicle/driver via the OEM cloud. This is also included in the diagram (figure 4).

Road restriction information can be an important input for platoon matching as this affects the platoon route or, in the worst case, stipulates that platooning is not possible between starting and end points. Hence the interface between the PSP and the broker. A further assumption which is taken here is that no road authority approval is required on a trip-by-trip basis. If at all a general approval is granted by the road authority based on a certain vehicle configuration which is guaranteed by the carrier/fleet.

Dynamic road restriction information is vital for platoons. Based on this the platoon may have to increase separation or even disengage locally. There are two paths by with the driver can receive this information. The first is via infrastructure to vehicle communication. This interface is/will be described in the deliverable D2.6. The identical information can be delivered to the driver via the OEM (cloud based) interface to the vehicle. Both possibilities are shown in the system architecture diagram (figure 4).

When comparing this architecture to Figure 1, it is difficult to identify the service and strategic layers. It is worth deliberating whether a segmentation actually makes sense, or whether all backend related serves should be aggregated in a combined Service & Strategic Layer. This will not affect any results but could simplify the architecture shown in Figure 1.

3.1.4. Description of mandatory services

Further upfront definition work / assumptions are required to be able to start the definition of the required offboard APIs. The next step is to describe the services in some more detail. This is valid for the platoon matching service. A possible workflow was described for the matching service. It assumes that the carrier has two options when searching for a platoon:

1. The carrier can join an existing platoon. This option means that the carrier must tweak their schedule to adapt to the timing and location of an existing platoon. This is represented by the left branch in Figure 5.

2. The carrier can request to be the entity which defines the platoon parameters (starting time and location). The PSP would then try to find matches from other carriers. This is represented by the right branch in Figure 5.

It is not unlikely that a carrier first tries option 1 and then changes to option 2 if the existing platoon does not fit their mission data.

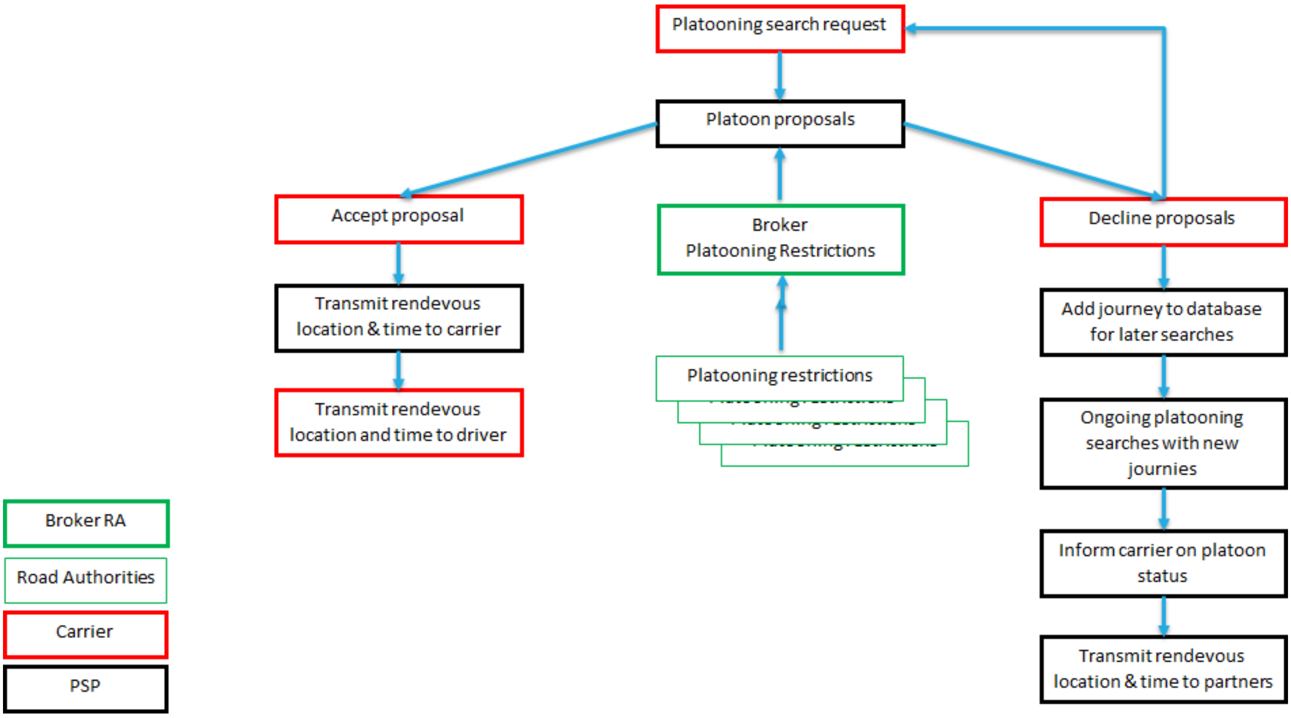


Figure 5. Possible workflow of a matching service.

The aforementioned is an assumption for a future service.

3.1.5. Definition of the API for mandatory service

Referring to the system architecture shown in Figure 3, three APIs must be defined:

1. Between PSP and carriers
2. Between PSP and Road Authority (RA) broker
3. Between PSP and OEM

Due to the complex nature of the API description this is not deemed suitable as general reading. The API is therefore documented in the annex 6.2. In addition to the text-based description, the API has also been programmed in the well-known Swagger tool. This is available upon request.

3.1.6. Summary

After a series of intermediate steps, the API for the mandatory platooning services was successfully defined. The key learnings in this sub-task were:

1. Numerous services can be identified which help to make platooning more attractive. These services open the door for business opportunities for service providers.

- Only a subset of the possible services can be classified as mandatory for safe and efficient platooning. The key enabling service for platooning is a platoon formation service. The key service for safe platooning is the provision of road restriction information.

- The services can require mission data from fleets and/or vehicle date from the vehicles and driver input. Provision of this data requires interfaces, whereby the re-use of established interfaces is at least partly possible

- Standard tooling can be used to describe the platooning service provider API. This enables easy transfer of the knowledge gain for later commercialization. The API for the platoon matching service is a recommendation and certainly not the only possible solution.

- The API specification for the services which were not classified as mandatory can be freely defined by platooning service providers giving them freedom to differentiate

Further work still needs to be done on services for Platooning Autonomous Function. A first indication of possible services was provided. The maturity if this however reflects the fact that the function is still currently in definition as part of D2.5 Vers. B. This topic could be revisited once the specification has been closed. However, first work indicates that Platooning Autonomous Function will not demand a range of specific service.

In conclusion this work now levels the playing field for possible service providers.

3.2. T4.2.1

The aim of this task is to identify and analyze the potential issues that need to be addressed in the development of the strategical and service layers, illustrated in Figure 1, for multi-brand and multi-fleet platooning.

Truck platooning has been a subject of study for more than two decades (Tsugawa., 2013; A. Alam, 2015; Horowitz, 2000) and is now reaching a certain level of technical maturity. The majority of the research effort has focused on platoon feasibility, scalability and benefit analysis. Such research has shown how platooning can yield significant benefits for the transportation economy, for traffic safety and for the environment. However, it has also highlighted how, in general, the benefits from platooning per truck scales linearly with the number of other trucks it can platoon with, for a small to medium level for platoon technology penetration. Only with a high level of platoon technology penetration, the benefits per truck are expected to reach a saturation level, see e.g., (Liang, et al., 2016; A. Johansson, 2021) and simulation results in Section 3.2.6.

The latter considerations have motivated truck OEMs to cooperate on researching and developing multi-brand platoon technologies. The platoon benefits can more quickly offset the costs for research, development, and deployment of platoon technologies if trucks from multiple brands and carriers can form platoons, making the commercialization of platooning technologies more appealing. The extension of truck platooning to multiple brands and fleets, however, introduces new issues that require attention. In this task, we aim at identifying and analyzing such issues in the service and strategic layers.

3.2.1. Issues classification

We have identified four issues categories, namely:

- **Information sharing**: issues related to the sharing of information among competitive entities willing to cooperate;
- **Cooperation profitability**: issues related to the profitability of solo platooning, multi-brand platooning and multi-fleet platooning;
- **Service-related**: issues related to the development and deployment of platooning services;
- **Interface standardization**: issues related to the definition of interfaces among platooning stakeholders, namely OEMs, carriers, and road authorities.

For each category we then identified issues related to multi-brand platooning and multi-fleet platooning. An outline of the identified issues ordered by expected criticality in decreasing order is displayed in Table F. In the next four sections we explore the identified categories and discuss in detail the issues within them.

Table F. Outline of the identified issues (ordered by expected criticality).

Issue	Category	Multi-brand issue	Multi-fleet issue	Expected criticality (1—5)
Heterogenous return of investment for OEMs	Cooperation profitability	X		4
Heterogenous return of investment for carriers	Cooperation profitability		X	4
Carriers sharing mission data with PSP and competitors	Information sharing		X	3
Carrier data heterogeneity	Service-related		X	2
Driver HMI heterogeneity	Service-related	X	X	2
Standardization of PSP-carrier interface	Interface standardization		X	2
OEMs sharing truck data with PSP and competitors	Information sharing	X		1
Standardization of PSP-OEM interface	Interface standardization	X		1
Standardization of PSP-road authority broker interface	Interface standardization			1

3.2.2. Information sharing

The first issues that needs to be addressed when competing companies decide to cooperate are related to information sharing. Competition in the transportation sector is tight and companies within the field are known to strongly protect their industrial secrets. The first step for the successful implementation of multi-brand and multi-fleet platooning is the willingness of stakeholders to share information.

OEMs and carriers are expected to internally conduct risk-benefit analysis to determine which information they are willing to share. In this case, the presence of a trusted third-party entity, as the platooning service provider, can be beneficial since sensitive information can be shared with it, while only an agreed limited subset of such information reaches the competitors.

OEMs sharing truck data with PSP and competitors

Table G. Overview of the "OEMs sharing truck data with PSP and competitors" issue.

Classification	Multi-brand issue
Description	In order to form safe and efficient platoons, platooning services may require OEMs to share potentially sensitive information about their

	trucks with PSP and/or competitors, e.g., truck weight, truck cross-sectional aera, and powertrain and braking system specifics.
Expected criticality	1 of 5

Platooning trucks are already required to share some basic information (such as braking system status) for the correct functioning of the tactical and operational layers. And OEMs have shown their willingness to share such data in the recently concluded Sweden4platoon project (Dellrud, 2020) and in the ENSEMBLE project.

Sharing additional truck data in the strategical and service layers is not essential, but has shown to be an effective way to increase the overall efficiency of platooning, see e.g., (A. Alam, 2015) and (Besselink, et al., 2016). Powertrain maximum power, truck weight and cross-sectional area can be for example incorporated in the match matching algorithm in order to recommend more homogeneous and therefore more efficient platoons. The same truck information can be also used for computing the most efficient platoon speed trajectory for those hilly roads where trucks are usually not able to keep constant speed.

Given the already proven willingness of OEMs to share some truck data in joint platooning projects, and the low-sensitivity and non-essentiality of the additional truck data, we expect this issue to have low criticality.

Carriers sharing mission data with PSP and competitors

Table H. Overview of the “Carriers sharing mission data with PSP and competitors” issue.

Classification	Multi-fleet issue
Description	Platoon services require carriers to share sensitive transportation data with PSP and/or competitors. On one side, data sharing constitutes a risk for carriers, while, on the other side, higher quality of the shared data is expected to yield higher platooning performance. Furthermore, as mission data may contains driver-related data, carrier should make sure that the data sharing complies with GDPR regulations. GRPR is discussed more in detail in task T4.2.3.
Expected criticality	3 of 5

In order to achieve multi-fleet platooning, information sharing between carriers is essential. As a matter of fact, platooning services have to rely on some sort of information about the transportation task of each platoon-ready truck. This information can include pre-planned information, such as routes, schedules, driver resting time constraints, and load weight. The information can also include online information, such as current location, next stopping location, and fuel remaining.

This kind of data is often considered highly sensitive in terms of both competitiveness and privacy, and carriers are generally reluctant in sharing it. A carrier having access to transportation mission details of a competitor in a raw form, may use them to approach the competitor clients with better offers. The presence of a third-party PSP, independent from each single carrier, is expected to facilitate the sharing process. The highly sensitive data can be then shared only with the PSP, under the guarantee that the PSP shares only an agreed limited subset of such data with competing carriers in an anonymous form. In this kind of scenario, the trustworthiness of the PSP plays a substantial role. Publishing the source code, encrypting carrier-to-PSP communication and additional tools from privacy-enhancing technologies (Wang, 2009) and secure multi-party computation (Cramer, 2015) should be considered to reach the required level of trust. The research project FEDeRATED focuses on data sharing between different actors in EU logistics (FEDeRATED, 2021).

As sharing data involves always a certain level of risk, carriers are still expected to conduct a risk-benefit analysis and discuss which data they are willing to share with the PSP and which data the PSP is allowed to communicate to competing carriers. Providing limited information to the PSP, such as the real-time position and the next stop location, allows the PSP to combine in platoons only trucks driving at an already relatively short distance. On the other hand, providing complete mission details gives to the PSP more flexibility in modifying trucks' route increasing the probability of forming platoons.

The information sharing issue for carrier is expected to be more challenging to address than for OEMs and to have a medium level of criticality. We believe that the creation of a publicly funded platooning project involving two or more carriers should be the first step to address such issue.

3.2.3. Cooperation profitability

Multi-brand and multi-fleet platooning are not only a technical challenge, but, more importantly, is a business investment. A commonly used approach for evaluating investments is based on the return on investment (ROI), defined as the ratio between expected profit and expected cost for a specific investment, i.e.,

$$\mathrm{ROI}_i = \frac{\mathrm{profit}_i}{\mathrm{cost}_i} = \frac{\mathrm{revenue}_i - \mathrm{cost}_i}{\mathrm{cost}_i}$$

for investment i. In general, companies aim at investing in projects with the highest ROI as this translates to the highest profit for a given cost. However, when the decision of a company also effects the ROIs of competitor investments, the scenario become more complex. In the multi-brand and multi-fleet platooning case, each company, either an OEM or a carrier, has three options:

- not investing in platooning,
- investing in solo-platooning (i.e., without cooperation with competitors),

- investing in multi-platooning (i.e., with cooperation with competitors).

While the solo-platooning ROI can be easily computed, the multi-platooning ROI depends on the decision of competitors to cooperate (the probability of platooning, and therefore the revenue from platooning, depend on the number of platoon-able trucks). Paraphrasing the latter observation, we can also state that the decision of a single company to invest in multi-platooning affects the multi-platooning ROIs of its competitors.

The interdependence of multi-platooning ROIs is crucial in the issue investigation, as each company will not only aim at maximizing their absolute ROI but will also pay attention to their relative ROI with respect to its competitors. In fact, an investment decision that maximizes the company ROI, but also increases the gap between competitor ROIs and own ROI can be counterproductive as competitors can use the surplus to decrease their transportation prices becoming therefore more attractive.

Heterogeneous return of investment for OEMs

Table I. Overview of the “Heterogeneous return of investment for OEMs” issue.

Classification	Multi-brand issue
Description	OEM cooperation through multi-brand platooning is expected to maximize the ROI for platooning for each OEM. However, OEMs with larger fleets may experience the lowest ROI increase from solo platooning to multi-brand platooning. Therefore, they have a limited incentive in developing technology for multi-brand platooning. However, if multi-brand platooning becomes widely common, they will have an incentive in joining it.
Expected criticality	4 of 5

The revenue from platooning for a single truck is expected to grow linearly with the number of other trucks it can platoon with, for low to medium level of platooning technology penetration. Only with a high level of platoon technology penetration, the revenue per truck is expected to reach a saturation level, see e.g., (Liang, et al., 2016; A. Johansson, 2021) and simulation results in Section 3.2.6. As the cost per truck for deploying platooning can be approximated to a constant (i.e., the cost of additional hardware for enabling platooning, under the assumption that research and development costs can be fully diluted over the production), ROI is also expected to grow with the number of vehicles each truck can platoon with.

Under the assumption that OEMs can increase the selling price of their platoon-able trucks with the increase of the platoon-able fleet they belong to, the latter observation yields the following results:

- Truck OEMs with the largest fleet of platoon-able trucks gets the highest ROI for solo-platooning (under the assumption that OEMs can increase the selling price of their platoon-able trucks with the size of the fleet the truck can platoon with).

- If all OEMs cooperate in multi-brand platooning, all OEMs will experience a larger ROI with compered to solo-platooning and such ROI will be the same for all of them.

- If all OEMs cooperate in multi-brand platooning, OEMs with the largest market share will experience the smallest ROI increase by switching from solo to multi-brand platooning.

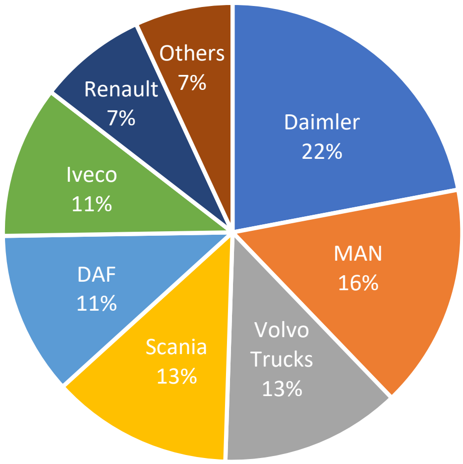


Figure 6: Truck manufacturing market share in Europe, estimated by summing the number of new vehicles registered by each OEM between 2017 and 2019 in EU+EFTA (ACEA, 2021).

Given the low margins in the truck manufacturing business and the fact that few players dominate the market (Figure 6 shows an estimation of the truck OEM market share computed by summing the number of trucks commercialized between 2017 and 2019 (ACEA, 2021)), although it maximizes their ROI, deciding to invest in multi-brand platooning instead of solo-platooning for large OEMs may result in loss of competitivity and the risk of losing market shares.

We expect the OEM heterogeneous return of investment issue to have a high level of criticality. Possible ways to overcome the issue are:

- Driven by market pull. Carriers, OEMs' clients, may call for multi-brand platoon functionalities. This can be the case for carriers owning trucks of multiple brand or multiple carriers that want to cooperate forming multi-fleet platooning

- Required by EU regulations. Multi-brand platooning allows to increase the size of platoon-able truck fleets and, therefore, to increase the environmental benefits of platooning. Furthermore, platooning may improve traffic safety.

Heterogeneous return of investment for carriers

Table J. Overview of the "Heterogeneous return of investment for carriers" issue.

Classification	Multi-fleet issue
Description	Multi-fleet platooning is expected to return higher ROIs for all carriers that they decide to cooperate with compared to the case they opt for solo-platooning. However, carriers with the largest fleets are expected to experience the lowest ROI increase from solo platooning to multi-fleet platooning, if platooning benefits are shared uniformly within the platoon. This translates in limited incentive for the largest carriers in investing in multi-fleet platooning. However, if multi-fleet platooning becomes widely common, they will have an incentive in joining it. Also, non-uniform benefit sharing approaches can be studied to address the problem.
Expected criticality	4 of 5

Under the assumption of uniform sharing of benefits within platoons, also the ROI per vehicle for carriers is expected to grow linearly with the size of the platoon-able fleet for low to medium level of platooning technology penetration. Only at a high level of platoon technology penetration, ROI per vehicle is expected to reach saturation. The carrier market in Europe is significantly more fragmented with compared to the truck OEM market. It is estimated that more than 590 000 road freight haulage companies operate in Europe, with the top 20 players having more than 10% of the total market share (Effigy, 2021).

Following similar arguments to those one expressed in the previous section, we expect that the largest carriers do not have a direct incentive to invest in multi-fleet platooning with compared to solo-platooning. This also makes the carrier heterogeneous return of investment issue of high criticality. Investigating benefit sharing algorithms aiming at uniformizing the return of investment for carriers a potential response to this issue. Such algorithms should not share the platooning benefits uniformly between platooning trucks, but compute the compensations accordingly to the size of the carrier fleets they belong to.

3.2.4. Service-related

The system architecture discussed in Section 3.1.3 allows third-party platoon service providers to connect and sell their services. Here, we focus on the issues related to the development and deployment of such services.

Carrier data heterogeneity

Table K. Overview of the "Carrier data heterogeneity" issue

Classification	Multi-fleet issue
Description	Because of the different perceived risk of sharing mission data with PSP and competitors, carriers may share data in different formats. The heterogeneity of mission data makes the development of platooning services more challenging.
Expected criticality	2 of 5

As discussed in Section 3.2.2, depending on the results of the benefit-risk analysis, carriers may be willing to share mission data in different manners. Some carriers may be comfortable with sharing complete mission data including both offline data (such as departure and arrival locations and time windows, driver resting time constraints, load weight) and real-time data (such as current location, next stopping location and fuel remaining). Other carriers may instead prefer to only share real-time information of their vehicles. The heterogeneity of the carrier data needs therefore to be considered in the platoon services development.

Integrating multiple mission data formats in the same cross-fleet truck matching service can provide significant challenges to service providers. Service providers can therefore decide if to consider carriers that share data in different formats independently, simplifying the matching problem, or jointly, aiming at higher platoon benefits.

Driver HMI heterogeneity

Table L. Overview of the "Driver HMI heterogeneity" issue.

Classification	Multi-brand issue, multi-fleet issue
Description	If OEMs and carriers do not agree on standardizing their driver HMIs, the platoon system architecture needs to be robust to the various HMI.
Expected criticality	2 of 5

With platooning as support function, the driver is still in the vehicle control loop and is fully responsible for traffic safety. The information that enables platooning computed by the platooning service providers is therefore expected to pass by the fleet management system of the carrier and ultimately communicated to the driver through an HMI that is embedded in the truck interface or running on an external device. The HMI can be embedded in the truck (OEM-proprietary) or running in an external device (carrier-proprietary). As carriers have generally different fleet management systems and OEM specific driver interfaces, both scenarios require the platooning system architecture to be robust to the heterogeneity of HMI driver interfaces. Although the standardization of driver HMIs between all carriers and OEMs would easily solve the problem, we do not expect carriers and OEMs to be willing to uniform them.

3.2.5. Interface standardization

Communication between platooning stakeholders is at the basis of multi-fleet and multi-brand platooning, and, for the platoon system architecture to work, communication interfaces need to be standardized. Here, we consider the platoon system architecture presented in Section 3.1.3 and we discuss potential issues related to the API definitions discussed in Section 3.1.5.

Standardization of PSP-OEM interface

Table M. Overview of the "Standardization of PSP-OEM interface" issue.

Classification	Multi-brand issue
Description	A PSP-OEM interface has been proposed and reviewed by all OEMs involved in the ENSEMBLE project. This API will be the starting point for standardization.
Expected criticality	1 of 5

Thanks to the limited number of large truck OEMs in Europe and thanks to the involvement of all of them in the ENSEMBLE project, a first proposal for the PSP-OEM API for multi-brand platooning has been developed and presented in Section 3.1.5. The proposed API has been reviewed by all OEMs involved in the project and will be the starting point for the future standardization.

Standardization of PSP-carrier interface

Table N. Overview of the "Standardization of PSP-carrier interface" issue.

Classification	Multi-fleet issue
Description	Due to the high fragmentation of the carrier market, discussions for the PSP-carrier API standardization should include a large number of stakeholders. Furthermore, as each carrier may be willing to share their mission data in a different manner, carriers should agree on a limited set of possible mission data sharing representations.

Expected criticality	2 of 5

Because of the large number of existing carriers and the fragmentation of the carrier market, discussions for the standardization of the PSP-carrier interface may involve a significant number of stakeholders. As a consequence, the standardization process of the PSP-carrier interface is expected to be more complex with respect to the PSP-OEM interface.

Furthermore, as discussed in Section 3.2.2, carriers may be willing to share mission data in different manners. On one hand, a carrier may be willing to share detailed mission data, including both offline data (such as departure and arrival locations and time windows, driver resting time constraints, load weight) and real-time data (such as current location, next stopping location and fuel remaining). On the other hand, another carrier may be willing to only share the current location of its trucks. In order to define a limited set of possible mission data sharing representation and their related APIs, round-table discussions between multiple carriers are needed.

Standardization of PSP-road authority broker interface

Table O. Overview of the "Standardization of PSP-road authority broker interface" issue.

Classification	General issue
Description	The API provided by road data brokers needs to be extended to include road authority information concerning platooning.
Expected criticality	1 of 5

In Europe there are multiple road authorities that provide heterogeneous information about their roads. This information may include both static data (such as traffic signs, speed limits and lane number) and dynamic data (such as constriction work, temporary speed limits and temporary signs). Nowadays, such heterogeneous information is typically aggregated by road data brokers that are able to provide a uniform interface to vehicles. We expect that the existing API provided by road data brokers can be easily extended to include road authority information concerning platooning. This issue has therefore a low level of criticality. Initiatives focusing on standardizing traffic data are, for example, (ETSI, 2021) and (DATEX II, 2021).

An explicative scenario

In order to illustrate some of the identified issues in the previous sections, here we present a possible scenario of platooning. In details, we consider a realistic scenario of trucks belonging to multiple carriers entering the highway network of Sweden in a two-hour span. First, we show how the benefit from platooning grows with respect to the size of the platoon-able truck fleet. Second, we compare two platoon matching algorithms that rely on different sets of mission data and we show how the platoon benefits differ. Finally, we show how the benefits vary with the choice of carriers to cooperate in multi-fleet platooning or not.

Simulation setup

We consider the Swedish highway network in Figure 7. The nodes are hubs at which trucks can wait for others to form platoons, and the links are roads connecting the hubs. The origins of the trucks are drawn randomly from the set of nodes. The destination of each truck is drawn randomly from the set of nodes which fulfil that the distance between the origin and destination is between 300 km and 800 km. We assume that each follower truck saves 10 % of the fuel, which is reasonable according to the field experiments in (A. Alam, 2015), and we assume the platooning benefit is shared evenly within each platoon. Moreover, we assume that the monetary benefit of platooning is €0.35/km, which is realistic if the benefit comes from the fuel savings. We also assume that the cost for waiting is €0.45/min and that trucks have a waiting budget of 20 min for their entire trips. Each of the trucks belongs to one of four considered carriers with a market share of 5%, 20%, 30%, and 45%, respectively.

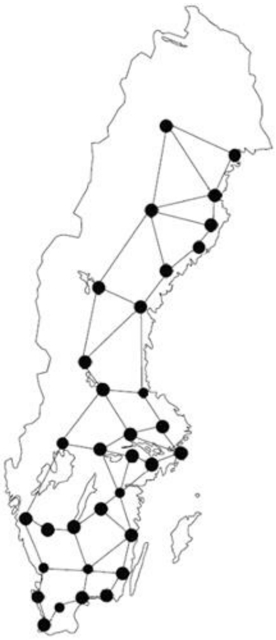


Figure 7. Swedish highway network.

Two platoon matching algorithms

We compare two different platoon matching algorithms. The first algorithm, referred to as orchestrated platooning, requires complete mission data and real-time position of the trucks. Based on that, each truck's profit is optimized, one at a time, until the algorithm converges. The second algorithm, referred to as real-time platooning, only requires the real-time position of the trucks near hubs. The real-time algorithm is based on grouping trucks that will arrive at a hub within intervals of 5 minutes. For more details of the platoon matching algorithms, see *(A.*

Johansson, 2021), in which the orchestrated platooning algorithm and the real-time platooning algorithm are referred to as the stochastic receding horizon solution and spontaneous platooning, respectively.

Results: platooning benefit vs fleet size

Here, we consider that the carriers are cooperating in multi-fleet platooning. Figure 8 shows the average platooning profit per truck as a function of the total number of platoon-able trucks in the system. The figure underlines that the profit per truck grows approximately linearly with the size of the platoon-able truck fleet for low to medium level of platooning technology penetration, and the profit per truck saturates for a high level of platoon technology penetration.

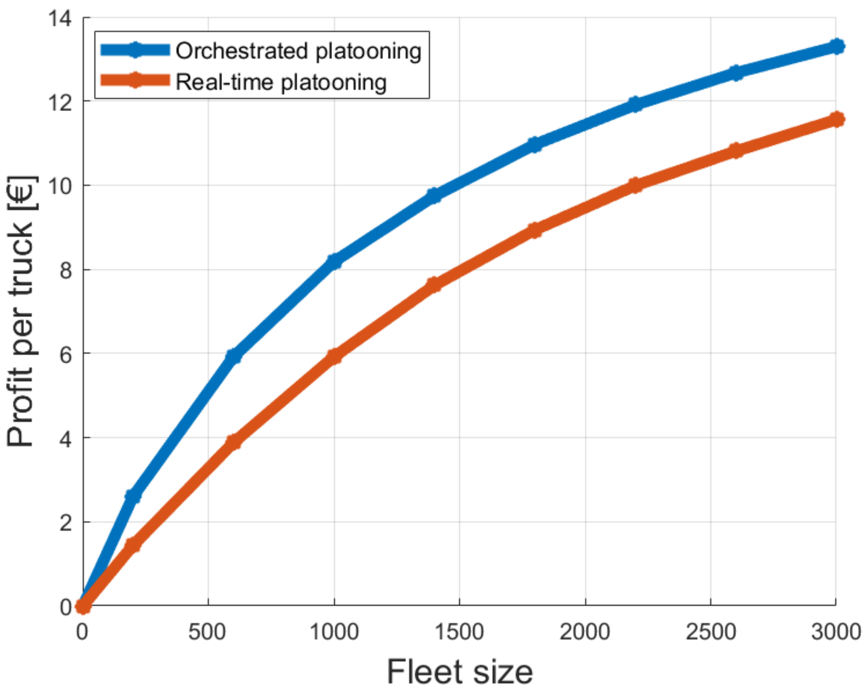


Figure 8. Platooning profit per truck in multi-fleet platooning as a function of the total number of trucks.

Results: platooning benefits vs matching design

Figure 8 shows the platooning profit per truck for two different platoon matching algorithms, namely, orchestrated and real-time platooning. The former matching algorithm requires complete mission data and real-time positions of trucks, while the latter algorithm only requires real-time positions of the trucks. The figure underlines that orchestrated platooning returns higher platooning profits than real-time platooning.

Results: The issue of heterogeneous return of investments

Here, the number of platoon-able trucks is fixed to 3000 and each of the trucks belong to one of four carriers with market share of 5 %, 20 %, 30 % and 45 %. We assume that the platooning benefits are shared equally within each platoon, and we consider orchestrated platooning. Figure 9 shows the total platooning profit of each fleet under single-fleet platooning and multi-fleet platooning. The figure shows that the carriers obtain higher profits when cooperating to form platoons. Figure 10 shows the platooning profit per truck and per carrier under single-fleet platooning and multi-fleet platooning. The figure underlines that although multi-fleet platooning returns a higher benefit per truck for all carriers, the largest carriers experience the smallest variation for the benefit per truck from single-fleet platooning and multi-fleet platooning. Therefore, the larger carriers do have less incentive than smaller carriers to support multi-fleet platooning. In this simulation study, we considered uniform profit sharing among platoon members. A possibility is to study non-uniform profit-sharing algorithms to compensate for the heterogeneous return of investments.

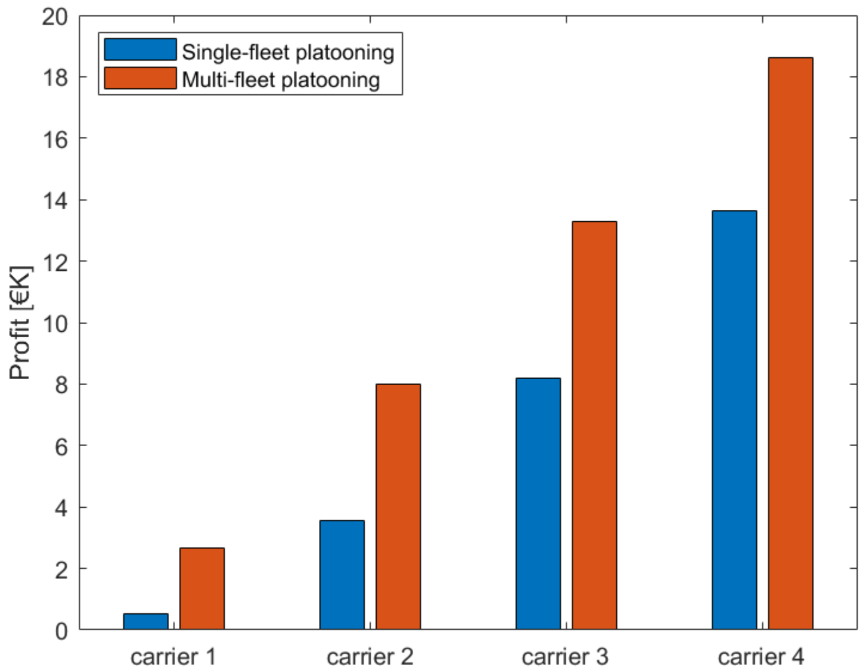


Figure 9. The profit of four carriers (fleets) under single and multi-fleet platooning.

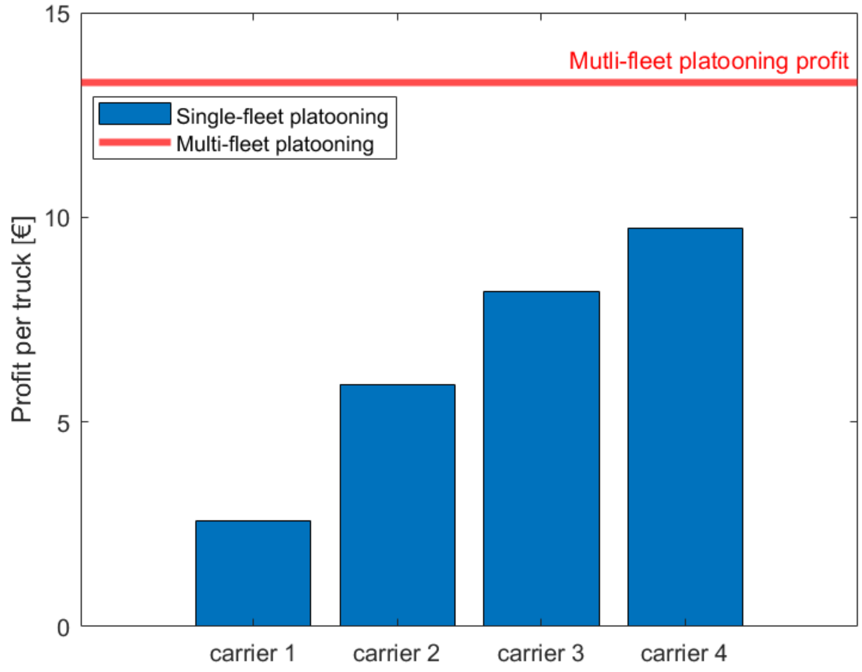


Figure 10. The platooning profit per truck and per carrier under single-fleet platooning. The platooning profit under multi-fleet platooning is noted as a horizontal line.

3.2.6. Summary

Several issues related to multi-brand and multi-fleet platooning have been identified, and solutions to these issues are proposed. The issue that stands out as the most critical for multi-brand and multi-fleet platooning is the heterogeneity in earnings generated by the cooperation of competing entities. More precisely, fleets and brands with many trucks are less dependent on others to form profitable platoons and thus have a lower incentive in cooperating with others. Fair profit-sharing mechanisms and regulations are proposed as solutions to overcome this issue. Other, less critical, identified issues include the reluctance of carriers and brands in sharing data as well as standardization of data formats and HMIs.

Finally, a simulation over the Swedish road network was given to illustrate the importance of multi-fleet and multi-brand platooning and to highlight the heterogeneity in gained profits across competing entities. The simulation also showed that a matching approach where mission data and truck positions are shared achieves higher profits than a matching approach where only truck positions are shared.

3.3. T4.2.3

3.3.1. Introduction

Cybersecurity attacks on vehicles with connected features are currently a real threat to the safety of road users, regarding both their physical safety and their data and privacy. In addition, cybersecurity is a “hidden” quality of a vehicle and is only perceived by the user after an event (as with passive safety). In order to guarantee protection to users, it is necessary to analyse potential cybersecurity threats and to perform a risk analysis in order to be able to define countermeasures and requirements to mitigate them.

Platooning communications considers two main blocks of communication channels, one of the blocks considers the communication between trucks and road-side units for the platooning manoeuvres, the cybersecurity considered for this communication was considered in WP2.

On the other hand, the second block of communication channels considers the communication with the back-end servers for the additional IT landscape services that can be provided.

The scope of this chapter focuses on identify possible cyber security risks and associated countermeasures for these services defined in task 4.2.1 and their IT landscape.

3.3.2. Threat analysis risk assessment

An analysis technique that is applied in the concept phase to help identify potential threats to a feature and to assess the risk associated with the identified threats. Identifying the potential threats and assessing the risk associated with these threats, allows an organization to prioritize follow-on cybersecurity activities associated with the threats so efforts and resources can be focused on the highest priority threats.

- **TARA Methodology**

In order to follow ISO 21434, we’ve defined a TARA for each asset following the next steps:

First, it’s necessary to do an asset identification, which is an identification of damage scenarios and assets of an item or component, and after, the identification of threat scenarios to the cybersecurity properties of the assets under analysis.

When asset and threat scenario analysis is done, an impact rating analysis must be performed. In this analysis, an estimation of the magnitude of damage or physical harm associated with a damage scenario must be done.

The third step is to do an attack path analysis, where identification and linking of potential attack paths to one or more threat scenarios is done. This attack paths form the basis for the assessment of attack feasibility. They are also used for the refinement of cybersecurity goals to cybersecurity requirements and to support the selection of appropriate controls.

After attack path analysis, attack feasibility rating must be done. The rating of the feasibility of attack paths based on the ease of exploitation. It is intended to be able to handle information at different abstraction levels during an attack feasibility rating. A high-level attack path description might be available from the concept phase, and a more concrete attack path description might be available in the later phases. An attack feasibility rating is possible in both cases.

Finally, the risk determination and the risk treatment decision must be done. The first one is the determination of the risk value of a threat scenario, and the risk treatment decision consists on addressing identified risks by selecting a suitable risk treatment option

- **Asset and threat scenario:**

In this step, we identify the damage scenarios for each threat, which are linked to each damage scenario, and then we must do a threat scenario identification.

ITEM	Asset	Security Property (C/I/A)	ID D.x	Damage Scenario	ID T.x	Threat Scenario
Platooning	Load scheduling service	C	D.01	User privacy may be compromised	T.01	Back-end servers used as a means to attack a vehicle or extract data
		A	D.02	Load information becomes inaccessible	T.02	Vehicle related data held on back-end servers being lost or compromised ("data breach")
		I	D.03	Wrong load data sent to the carrier	T.03	Spoofing of messages or data received by the vehicle
		A	D.04	Load scheduling service won't be available	T.04	Denial of service attacks via communication channels to disrupt vehicle functions
		C	D.05	Load of the client can be leaked in case of interception of the message	T.05	Cryptographic technologies can be compromised or are insufficiently applied

Table P. Example on asset and threat scenario definition

- **Impact rating:**

In this step, the damage scenarios shall be assessed against potential adverse consequences in the independent impact categories, which are safety, financial, operational and privacy, and which are represented as S, F, O and P respectively.

The result of impact rating shall be determined as severe, major, moderate or negligible.

Asset	Security Property (C/I/A)	ID D.x	Damage Scenario	ID T.x	Threat Scenario	Impact Rating				
						S	F	O	P	Justification
Load scheduling service	C	D.01	User privacy may be compromised	T.01	Back-end servers used to attack a vehicle or extract data	S1: Negligible	S1: Negligible	S1: Negligible	S2: Moderate	Privacy S2: The privacy damage leads to significant inconveniences to the road user In this case, the information regarding the road user is not sensitive but easy to link to a PII principal
	A	D.02	Load information becomes inaccessible	T.02	Vehicle related data held on back-end servers being lost or compromised ("data breach")	S1: Negligible	S1: Negligible	S2: Moderate	S1: Negligible	Operational S2: The operational damage leads to partial degradation of a vehicle function or performance.
	I	D.03	Wrong load data sent to the carrier	T.03	Spoofing of messages or data received by the vehicle	S2: Moderate	S1: Negligible	S2: Moderate	S1: Negligible	Safety S2: If vehicle alerts are not displayed correctly, light and moderate injuries can happen. Operational S2: The operational damage leads to partial degradation of a vehicle function or performance.
	A	D.04	Load scheduling service won't be available	T.04	Denial of service attacks via communication channels to disrupt vehicle functions	S1: Negligible	S1: Negligible	S3: Major	S1: Negligible	Operational S3: The operational damage leads to partial degradation of a vehicle function or performance.
	C	D.05	Load of the client can be leaked in case of interception of the message	T.05	Cryptographic technologies can be compromised or are insufficiently applied	S1: Negligible	S1: Negligible	S1: Negligible	S2: Moderate	Privacy S2: The privacy damage leads to significant inconveniences to the road user In this case, the information

										regarding the road user is not sensitive but easy to link to a PII principal

Table Q. Example on impact rating definition

- **Attack path analysis:**

In this phase, the threat scenarios shall be analysed in order to describe possible attack path. The attack path description should include a reference to the threat scenarios that can be realized by the attack path.

ID T.x	Threat Scenario	ID AP.x	Attack path
T.01	Back-end servers used as a means to attack a vehicle or extract data	AP.01	Abuse of privileges by staff (insider attack)
		AP.02	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
		AP.03	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)
T.02	Vehicle related data held on back-end servers being lost or compromised ("data breach")	AP.04	Abuse of privileges by staff (insider attack)
		AP.05	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers
		AP.06	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
		AP.07	Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)
		AP.08	Information breach by unintended sharing of data (e.g. admin errors)
T.03	Spoofing of messages or data received by the vehicle	AP.09	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)
		AP.10	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)
T.04	Denial of service attacks via communication channels to disrupt vehicle functions	AP.11	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner
		AP.12	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles

T.05	Cryptographic technologies can be compromised or are insufficiently applied	AP.13	Combination of short encryption keys and long period of validity enables attacker to break encryption
		AP.14	Insufficient use of cryptographic algorithms to protect sensitive systems
		AP.15	Using already or soon to be deprecated cryptographic algorithms

Table R. Example on attack path definition

- **Attack Feasibility Rating:**

In this case, for each attack path, the attack feasibility rating shall be determined as high, medium, low or very low, and the defined rating method should be based on one of the following assessment approaches:

a) Attack potential-based approach

b) CVSS based approach

c) Attack vector-based approach

If an attack potential-based approach is used, it should be determined based on core factors including elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, and equipment.

If a CVSS based approach is used, it should be determined based on the exploit metrics group of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.

If an attack vector-based approach is used, it should evaluate the predominant attack vector (cf. CVSS) of the attack path.

- **TARA Results:**

Asset	ID T.x	Threat Scenario	ID AP.x	Attack path	Risk Determination					
					Aggregated Attack Feasibility	S	F	O	P	Risk recommendation

Load Schedule Service	T.01	Back-end servers used as a means to attack a vehicle or extract data	AP.01	Abuse of privileges by staff (insider attack)	Medium	R1	R1	R2	R1	Reduce Risk
			AP.02	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)						
			AP.03	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)						
	T.02	Vehicle related data held on back-end servers being lost or compromised ("data breach")	AP.04	Abuse of privileges by staff (insider attack)	Medium	R2	R1	R2	R1	Reduce Risk
			AP.05	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers						
			AP.06	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)						
			AP.07	Unauthorized physical access to the server (conducted for example by USB sticks or other media connecting to the server)						
			AP.08	Information breach by unintended sharing of data (e.g. admin errors)						
	T.03	Spoofing of messages or data received by the vehicle	AP.09	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	Very Low	R1	R1	R2	R1	Reduce Risk
			AP.10	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)						
	T.04	Denial of service attacks via communication channels to disrupt vehicle functions	AP.11	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	Low	R1	R1	R1	R2	Reduce Risk
			AP.12	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles						

	T.05	Cryptographic technologies can be compromised or are insufficiently applied	AP.13	Combination of short encryption keys and long period of validity enables attacker to break encryption	Very Low	R1	R1	R1	R1	Accept Risk
			AP.14	Insufficient use of cryptographic algorithms to protect sensitive systems						
			AP.15	Using already or soon to be deprecated cryptographic algorithms						
Mission Load Bundling Service	T.01	Services from back-end server being disrupted, affecting the operation of a vehicle	AP.01	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	Very Low	R1	R1	R1	R1	Accept Risk
	T.02	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	AP.02	Accepting information from an unreliable or untrusted source	Very Low	R1	R1	R1	R1	Accept Risk
			AP.03	Man in the middle attack/ session hijacking						
			AP.04	Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway						
	T.03	Information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	AP.05	Interception of information / interfering radiations / monitoring communications	Very Low	R1	R1	R1	R1	Accept Risk
			AP.06	Gaining unauthorized access to files or data						
	T.04	Software or hardware development permits vulnerabilities. For example, software bugs.	AP.07	Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	Medium	R1	R1	R1	R2	Reduce Risk
Cross-fleet Fleet	T.01	Back-end servers used as a means to attack a vehicle or extract data	AP.01	Abuse of privileges by staff (insider attack)	Medium	R1	R1	R1	R2	Reduce Risk

			AP.02	Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)						
			AP.03	Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)						
	T.02	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	AP.04	Communications channels permit code injection, for example tampered software binary might be injected into the communication stream	Low	R1	R1	R2	R1	Reduce Risk
			AP.05	Communications channels permit manipulate of vehicle held data/code						
			AP.06	Communications channels permit overwrite of vehicle held data/code						
			AP.07	Communications channels permit erasure of vehicle held data/code						
			AP.08	Communications channels permit introduction of data/code to the vehicle (write data code)						
Service Go-Non Go Road Segments	T.01	Services from back-end server being disrupted, affecting the operation of a vehicle	AP.01	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	Very Low	R1	R1	R1	R1	Accept Risk
	T.02	Spoofing of messages or data received by the vehicle	AP.02	Spoofing of messages by impersonation (e.g. 802.11p V2X during platooning, GNSS messages, etc.)	Very Low	R1	R1	R1	R1	Accept Risk
			AP.03	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)						
	T.03	Denial of service attacks via communication channels to disrupt vehicle functions; in that case the platooning functionality	AP.04	Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	Low	R1	R2	R2	R1	Reduce Risk
			AP.05	Black hole attack, in order to disrupt communication between vehicles the attacker is able to block messages between the vehicles						

	T.04	Cryptographic technologies can be compromised or are insufficiently applied	AP.06	Combination of short encryption keys and long period of validity enables attacker to break encryption	Very Low	R1	R1	R1	R1	Accept Risk
			AP.07	Insufficient use of cryptographic algorithms to protect sensitive systems						
			AP.08	Using already or soon to be deprecated cryptographic algorithms						

Table S. TATA results

- **Requirements**

  - **Objectives:**

The objective of the cybersecurity requirements is to specify and allocate them to the item and/or the operational environment

The method to perform the cybersecurity requirements follows the guides indicated in the ISO-21434.

  - **CS Goals and CS Requirements:**

The information required to perform the activity to define the assets, damage scenario and threat scenario:

- Platooning Services V10

The result of this activity provides the definition of:

- Cybersecurity goals
- Cybersecurity requirements description
- Cybersecurity requirements allocation

CS Goal	Cybersecurity Requirement	
	Description	Allocation
Security Controls are applied to back-end systems to minimize the risk of insider attacks	Services shall log actions identifying user whose doing each action.	Load Schedule Service, Cross-fleet fleet management service, Vehicle Capability Service, Vehicle Incentivization Service & Driver Rating Service
	Services shall add staff levels to decide who can access to each information.	

Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage		Real Time Matching Service
The vehicle shall verify the authenticity and integrity of messages it receives, and security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)	Services shall verify if received data is sent from a valid entity	Load Schedule Service & Vehicle Capability Service
	Services shall implement security controls to store cryptographic keys	
Measures to detect and recover from a denial of service attack shall be employed	Services shall implement a firewall and monitor all requests to the service	Load Schedule Service, Real Time Matching Service, Vehicle Incentivization Service, Truck Parking Service, Driver Rating Service, Service to provide go/no go road segments for platooning & Platoon Documentation Service
Cybersecurity best practices for software and hardware development shall be followed and cybersecurity testing with adequate coverage	Entities shall implement a cybersecurity training for all employees related to the cybersecurity potential vulnerabilities.	Mission/load bundling service
	Entities shall implement effective security and functional test to validate and verify the services deployed	
Systems shall implement security by design to minimize risks, and access control techniques and designs shall be applied to protect system data/code	Services shall only allow access to data for which user is permitted, ensure data is not tampered or altered by unauthorized users and	Cross-fleet fleet management service

Access control techniques and designs shall be applied to protect system data/code	ensure systems and data are available for authorized users when they need it.	Vehicle Capability Service
Confidential data transmitted to or from the vehicle shall be protected, and, through system design and access control, it should not be possible for unauthorized personnel to access personal or system critical data		
Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data		Vehicle Incentivization Service
Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege	Services shall implement measures to allow only access to perform the required task to the responsible user.	Communication Service Between Drivers

Table T. Cybersecurity goals and requirements

- **Requirements List:**

All the requirements mentioned in this document are:

- **REQ [01]**
  - Services shall log actions identifying user whose doing each action.
- **REQ [02]**
  - Services shall add staff levels to decide who can access to each information.
- **REQ [03]**
  - Services shall verify if received data is sent from a valid entity
- **REQ [04]**
  - Services shall implement security controls to store cryptographic keys
- **REQ [05]**
  - Services shall implement a firewall and monitor all requests to the service

- **REQ [06]**
  - Entities shall implement a cybersecurity training for all employees related to the cybersecurity potential vulnerabilities.
- **REQ [07]**
  - Entities shall implement effective security and functional test to validate and verify the services deployed
- **REQ [08]**
  - Services shall only allow access to data for which user is permitted, ensure data is not tampered or altered by unauthorized users and ensure systems and data are available for authorized users when they need it.
- **REQ [09]**
  - Services shall implement measures to allow only access to perform the required task to the responsible user.

3.3.3. GDPR

3.3.3.1. GDPR at glance

The GDPR provides the rules for the processing of personal data of natural persons, stipulates that some of these data should be treated as sensitive and sets out the rights of citizens and the obligations of organizations that process their personal data. Furthermore, it assigns the monitoring of its application by entities in the public and the private sector to national independent supervisory authorities, the Data Protection Authorities (hereafter the "DPAs") and sets out the rules for these authorities‟ cooperation, particularly where enforcement is required. While the Directive served its purposes well for more than 21 years, it had some shortcomings that needed to be remedied. To understand the GDPR, one must have a basic insight to what this legislation aims to achieve and how it attempts to remedy the shortcomings of the Directive.

3.3.3.2. Principal aims of the GDPR

The GDPR aims at improving the existing legislation and at achieving the following:

(a) To remedy some of the problems that occurred because of the defragmented transposition and implementation of the Directive by introducing uniform relevant rules,

(b) To strengthen the existing rights of the citizens,

(c) To introduce new rights and obligations, particularly regarding citizens‟ activities in the digital environment,

(d) To reduce administrative burdens and to cut red-tape procedures, both for DPAs and for enterprises which operate in more than one Member States,

(e) To consider the impact of the costs inherent in compliance with data protection rules on micro, small and medium size enterprises (SMEs),

(f) To enhance the principles of transparency, accountability and self-regulation,

(g) To enhance the supervisory role of the DPAs and to strengthen their cooperation, particularly, in cross-border cases where persons are affected in more than one Member States,

(h) To better regulate the responsibilities of controllers and processors and their liability and to introduce more stringent sanctions and penalties,

(i) To better regulate transfers of personal data to (third) countries outside the EU and,

(j) To promote research, innovation and technology and to contribute to EU‟s social integration and economic development, particularly in the field of e-commerce while, at the same time, ensuring sufficient respect to the rights to privacy and personal data protection.

3.3.3.3. Fundamental principles

- **Lawfulness, fairness, and transparency:**

The GDPR requires personal data to be processed lawfully. Lawful processing requires the consent of the data subject or another legitimate ground provided in the data protection legislation.

In addition to lawful processing, regulation requires personal data to be processed fairly. The principle of fair processing governs primarily the relationship between the controller and the data subject.

The GDPR strengthens the principle of lawfulness and fairness by adding that personal data shall be processed “in a transparent manner in relation to the data subject”. This principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects – who may be users, customers or clients – informed about how their data are being used.

- **Accountability and Self-Regulation:**

The GDPR stipulates that controllers should comply with its provisions but also, they should be responsible and able to demonstrate their compliance (accountability). Accountability should be linked to transparency. GDPR promotes the principle of self-regulation by encouraging the drawing up of codes of conduct, certification mechanisms and data protection privacy seals and marks.

- **Purpose limitation:**

The principle of purpose limitation is strongly connected with transparency, predictability and user control: if the purpose of processing is sufficiently specific and clear, individuals know what to expect and transparency and legal certainty are enhanced.

- **Data minimization:**

Controllers shall ensure that the personal data is:

- adequate, i.e. is enough to properly fulfil the stated purpose;
- relevant, i.e. has a rational link to that purpose; and
- limited to what is necessary, i.e. no more data than is needed for that purpose.

- **Data accuracy:**

A controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. This principle must be seen in the context of the purpose of data processing. Inaccurate data must be erased or rectified without delay. Data may need to be checked regularly and kept up to date to secure accuracy.

- **Storage limitation:**

The GDPR requires personal data to be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data” are processed. The data must therefore be erased or anonymized when those purposes have been served. To this end, “time limits should be established by the controller for erasure or for a periodic review” to make sure that the data are kept for no longer than is necessary. The time limitation for storing personal data only applies to data kept in a form which permits identification of data subjects.

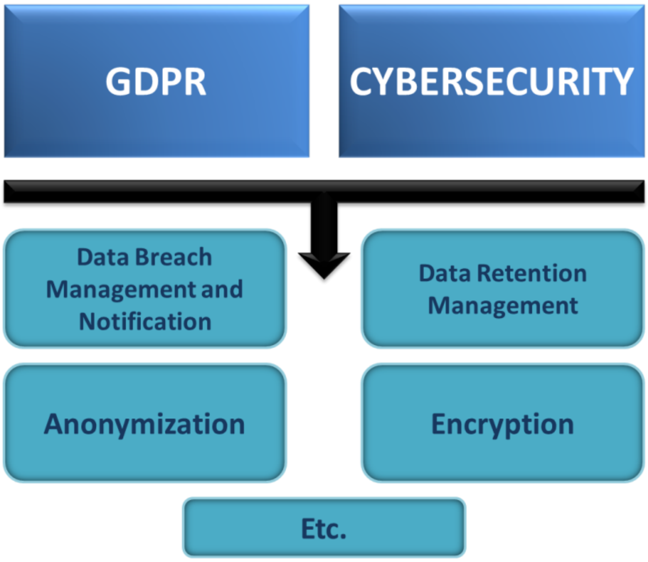
- **Data security:**

The principle of data security requires that appropriate technical or organizational measures are implemented when processing personal data to protect the data against accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage. The GDPR states that the controller and the processor should take into account “the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons” when implementing such measures.

3.3.3.4. Responsibilities, Liability and Enforcement

The GDPR introduces more legal certainty for the respective responsibilities of controllers and processors. For example, a controller must be able to demonstrate compliance with the GDPR, joint controllers must determine their respective responsibilities in a transparent manner and a processor must give to the controller all information necessary to be able to demonstrate his compliance.

3.3.3.5. GDPR and Cybersecurity



3.3.3.5.1. GDPR compliance

Besides technical specifications, compliance with the General Data Protection Regulation (GDPR) is something to consider. This regulation entered into force the 25th May 2018 and it aims to harmonise data privacy laws across all European member states. GDPR repeals the previous directive 95/46/EC on the protection of individuals regarding the processing of personal data and on the free movement of such data.

- **Data related risks:**

Service providers shall be aware that they are receiving 'personal data' from users and they must comply with GDPR.
Users may not be yet prepared to share these data, since they are aware of the possible privacy implications. Transmitting and receiving capabilities of vehicle and surrounds means information that maybe will be public.
Users need to be aware of the types of data collected, the recipients, how these are processed and for what purpose. This awareness is needed to establish user consent, which is a tricky question in general. In effect, users will become continuous broadcasters. They must be fully aware of the scope of the processing.
Article 7 of the EU GDPR explicitly states that the controller must be able to demonstrate users consent in terms of processing their personal data. Also, data subjects have the choice to exercise their rights to withdraw their consent, to rectification and erasure of their personal data.
Pilot sites should explicitly be able to demonstrate users' consent, when user data is collected, in terms of processing their personal data. Control of personal data can be ensured through a few tools for informed consent.

Messages can be received by an unrestricted number of entities, whose intentions and technological capacity cannot be known to the sender. Thus, control of personal data is imperative.

Last, the amount of data collected may be used for business exploitation. This opens questions on the free flow of non-personal data (either technical or anonymized) and the question of data access and data ownership. This area is not yet sufficiently legislated to make a definitive judgment of what will happen.

Next steps for data protection can be summarized as follows:

- *Legal*: The regulations on e-Privacy and Free Flow of Data, once adopted, will provide more depth to the legal development.

- *Political*: A fundamental decision on data ownership and consent for processing will be crucial. Given the lack of awareness by end users in this regard, this is likely to be top-down. If car data is understood to be personal data and consent as currently exercised found to be invalid, then political initiatives are needed.

- *Practical*: It is crucial to determine the role and the responsibilities of each partner involved in the application of the GDPR. New regulation introduces changes in relation to duties and rights.

- **Principles of processing personal data outlined in Article 5 of the GDPR:**

According to Article 5 of the GDPR[2], the following are the principles of processing personal data:

- *Lawfulness, fairness and transparency:* The objective is to process the data lawfully, fairly and in a transparent manner in relation to the data subject.
- *Purpose limitation:* The purpose of the data collected. Specify the exact purpose and assessing which data is necessary.
- *Data minimisation:* The main aim of data minimisation is guaranteeing that data only will be asked when adequate, relevant and necessary for the purpose.
- *Accuracy*: Delete the information once processed, since is possible want to keep the information for a long time, in this situation, the personal identifiers should be removed, making the identification of the Data Subject impossible.
- *Storage limitation:* Depending on the legal basis of processing data may also have to be stored for limited time periods for liability reasons
- *Integrity and confidentiality*: Personal data should be used according to technical and organisational measures, such as: protection against unauthorised processing and against disclosure, accidental loss, destruction or damage

In addition to the General Data Protection Regulation, the EU also applies sectorial data protection legislation-2002/58/EC ‘concerning the processing of personal data and the protection of privacy in the electronic communication sector’, also known as ‘Privacy and Electronic Communication Directive or ‘ePrivacy Directive’. The current directive strongly focusses on obligations for providers of electronic communication services.

3.3.3.5.2. Cybersecurity (GDPR)

From the data point of view, the security is a top layer that protects it from external entities. However, the legitimate communicating entities may also make a bad use of it. The new GDPR regulations try to protect this data and this section provides the technical steps.

3.3.3.6. Sensitive data that can compromise GDPR

Some services can compromise GDPR principles, and they have some sensitive data that must be treated according to the Article 5 of the GDPR.

- GPS Location: Position of the truck used in multiples services as “Real time matching Service” or “Platoon documentation Service”
- Financial Data: Sensitive data including bank account of the driver used in “Incentivization Service”

Users need to be aware of the types of data collected, the recipients, how these are processed and for what purpose, so user should have given consent to use this data in order to run these services according to the article 6 of the GDPR. As we said previously, messages can be received by an unrestricted number of entities, whose intentions and technological capacity cannot be known to the sender. Thus, control of personal data is imperative.

These data must be stored for the shortest time possible. That period should take into account the reasons why your company/organization needs to process the data, as well as any legal obligations to keep the data for a fixed period of time (for example national labor, tax or anti-fraud laws requiring you to keep personal data about your employees for a defined period, product warranty duration, etc.).

3.3.4. Conclusions

Several threats have been identified for the high-level services defined in the IT landscape, and the TARAs performed reveal the necessity to consider cybersecurity requirements to provide protection on the relevant systems.

Additionally, main key points of GDPR have been depicted, since services may contain sensitive information that shall be considered inside the scope of GDPR.

In conclusion, since platooning is a service based on connected features that also includes communication between trucks and back-end servers is important to perform the analysis risk assessment and it has been performed according to ISO 21434 supporting the definition of a baseline of cybersecurity pre-requirements and key points for GDPR.

3.4. T4.2.4

3.4.1. Introduction

In order to evaluate the platoon feasibility and its benefits, an analysis of the impact of platooning on logistic plans is required. The properties of the current fleets need to be known, based on them it can be analyzed what would need to be change in order to have the vehicles forming platoons. In essence, this chapter will link the theoretical platoon research to the real world answering a key question for the logistic operators; how often a truck will be able to engage in a platoon if the technology is deployed assuming the current transport schedules. Then, two main scenarios are to be compared, with and without platooning capabilities. A vast family of sub scenarios emerge within each of the two main ones. In the scenario with the platooning option availability, many different platooning settings and constrains can be explored whereas in the scenario without platooning a very involved analysis is required to ensure it can be used as a realistic unbiased baseline i.e., current vehicle behavior can maintain headway and speeds small and steady enough such that needs to be precisely taken into account when comparing to the platooning scenario.

Outcome measures

Assessing the advantages and disadvantages of platooning requires the choice of a metric or set of metrics over which the comparison can be taken. The natural and already ubiquitous measure relates to fuel savings due to the reduction of air friction specially on the platoon followers. The financially driven measures propagate through all the operational costs, including insurance, vehicle damage or wear and notably, the driver costs. The latter is typically studied on different degrees: whether platooning requires less awareness and the driver can work longer hours to the case in which follower trucks require no driver at all, potentially making the business case particularly attractive (for more extensive analysis of what platoon can bring please refer to Truck platooning value case (van Ark, et al., 2017)). There are though, several platooning potential advantages that can be assessed besides those economically driven. These include its impact on safety and on traffic flow.

Real world data versus simulation

To carry out such an analysis, there are typically two options namely, simulating fleet data or using real world data. Although both approaches have their advantages and disadvantages, using real world data ensures a minimum degree of calibration, such that the results at least on the measure region of the parameter space are exactly those that happened in reality. Furthermore, real data incorporates stochasticity inherently, which is difficult to model when simulating data. In the last decades a considerable amount of research has been carried out addressing the question of platoon formation. Due to the lack of data availability and the special treatment that this data needs to have, most of it was done by means of simulated data. Such an analysis with real logistic data was, to the best of our knowledge, missing. This section attempts to cover such gap.

3.4.2. Truck Platoon Matching overview

When addressing the platooning task, the truck platoon matching is a key component that must be solved. The truck matching problem can be briefly stated as the one that answers *when, where and how will be the platoons formed*. Central to this problem is the distribution of vehicle trajectories in time and space with the trivial limiting case being such that all vehicles start at the same time at the same location and have the same target time at the same destination; and the opposite extreme limiting case is that one in which the vehicles are uniformly distributed in time and space. In reality the logistic schedules are somewhere between those two cases, and due to typical scheduling patterns, it is placed particularly distant from the uniform case making it attractive for technologies like platooning.

3.4.2.1. Optimization objective

An outcome measure needs to be chosen in order to address the benefits of truck platooning. So far, a great part of the truck matching research for assessing the platooning benefits focused on economic measures such as fuel and driver time savings. In those cases, the common split of the tasks involved in platooning that includes four main processes as described in 3.2.1 and aligned with the terminology used in the literature (Janssen, 2015) is used. These four tasks are formation, engaging, platooning, disengaging of the platoon. From these four, the focus is on formation and platooning. Engaging is the process required to join the platoon which is typically inefficient and on the contrary platooning is an efficient form of driving. In this way the problem reduces to an optimization one, whose objective is to find those truck combinations such that the savings are maximized.

As anticipated in the previous section, another set of outcome measures started to be taken into account in recent years. Notably the platooning impact on vehicle and traffic safety, traffic flow and throughput. In such cases, the platooning problem formulation needs to be reshaped. It is not a one-dimensional problem anymore, and some of the benefits cannot be quantified with a single indicator. Furthermore, both platoon functions studied in Ensemble (Autonomous and Support) have different requirements and operational modes; the properties of a platoon in one or the other function are different and so are the benefits that each of them can provide. Hence, in this chapter, no figures of platoon benefits are used until the very last step. In this fashion, a more generic platoon formation estimation can be made, where the different benefits can be plugged in as scaling factors. From the reported results then, different benefits can be computed once the savings per vehicle per distance are known.

Hence, the results are expressed in terms of distance, time, number of vehicles and number of platoons that can be formed as a function time and distance thresholds.

3.4.2.2. Types of truck platoon matching

The way in which the trucks are matched spans the 2-dimensional space defined by the degree of orchestration and the real-timeness of the process. This is illustrated in Figure 11. On the real-time case with minimal orchestration the platoons are creating on the fly by means of vehicle-to-vehicle communication only. On the other extreme, a centralized system analyses not only current time but vehicles schedules and solves the multi vehicle problem. The higher the degree of orchestration and less spontaneity in the platoon allows for a closer to optimal solution whereas real time problems are by definition constrained to suboptimal results. As described in 3.2.1 this can be reduced to the four relevant main cases described in table 0 namely, two cases of orchestrated matching, at the hubs or on the road and two cases of spontaneous matching, at parking places or on the road. Another dimension plays a role in this space, the level of data aggregation (see figure 1 brown lines). As is inherent for the matching algorithms, the level of detail of the data for the real time case is higher than that required to the orchestrated one. This is also true when performing the platoon analysis offline as is the case of the current work.

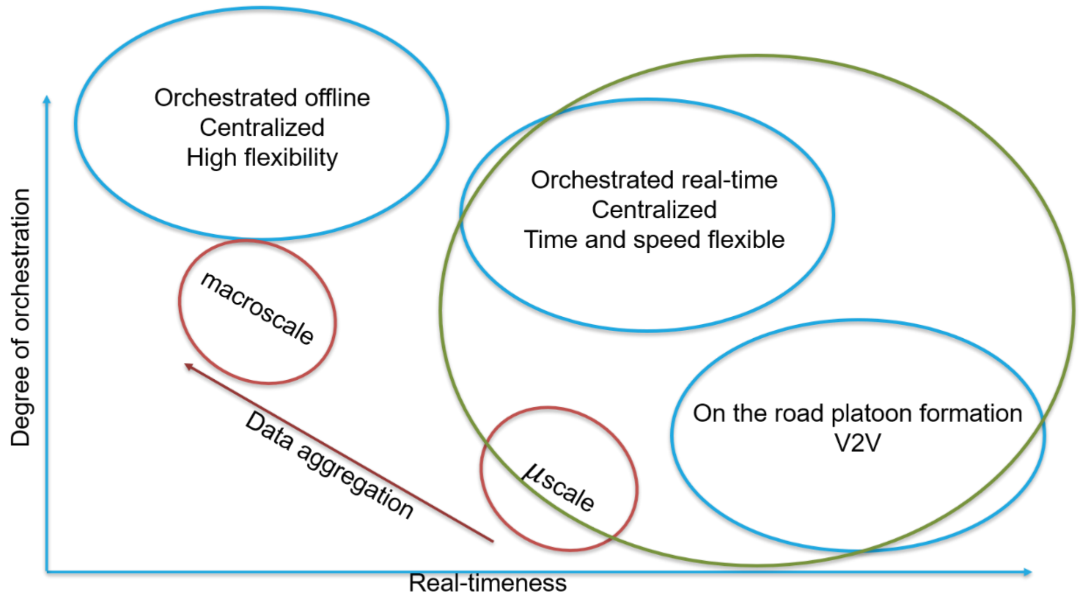


Figure 11. Truck Matching as a function of degree of orchestration and real-timeness. In blue, different types of truck matching on the different region of the space. In brown, an auxiliary axis showing that the different truck matching algorithms depend on the data aggregation level, e.g. a certain platoon matching algorithm can impose specific requirements in terms of data. Finally, in green is the region of the space that this work addresses.

In the present work, we performed a transversal type of analysis, as it will be described in the Methodology Section, our analysis although closer to the spontaneous platoon, allows for interpretations relating it to orchestrated platooning.

3.4.3. Data

3.4.3.1. TNO-DAF collaboration

As originally stated in the introduction of this section there are two main methodologies to consider to research the operational aspects of truck platooning; namely a more statistical approach by simulating fleet data and a more data-driven approach that uses real-world data from trucks. Given that there have been few previous initiatives that have applied real-world data and that it is relatively easy to translate any results to the real-world practice of logistical operators this task has ambitioned to collaborate with the OEMs from the ENSEMBLE project. Various conversations with different partners have been held, and DAF has expressed the interest to collaborate and facilitate this research. Because of the sensitivity of the data, this agreement was not of trivial nature. Several parties were required to approve the process to ensure it was GDPR compliant.

The provision of the real-world data from an OEM to participate in this task was purely voluntary. Given the ‘dynamic’ policy landscape with the GDPR that came into force in 2018, just when the ENSEMBLE project was started, no explicit prior commitment could be made by the OEMs in the original ENSEMBLE proposal, forthcoming grant agreement and description of work. For this reason it was required that the task itself included an investigation if and how data could be shared while complying with all legal laws and regulations. An important prerequisite is that the (raw) data is not owned by the OEMs but by the individual vehicle owners; processing, using such data by the OEM for such a specific purpose should explicitly be included in the terms of use. And even if such a clause (and therefore legitimate ground) was included in the terms of usage, the data could only be applied in the ENSEMBLE project if it was anonymized by the OEM. This is a considerable effort for the OEM and only DAF saw both the (legal) possibility and the means to support this analysis with an extensive (anonymous) dataset and the associated knowledge to apply it. The other OEMS supported this task by attending and contributing to the regular discussions in which the methodology and results were presented, discussed and interpreted.

3.4.3.2. Data

As addressed in detail in section 3.3.2, the General Data Protection Regulation (GDPR) General Data Protection Regulation (EU) 2016/679 needs to be followed when utilizing (including processing, transferring or storing) personal data. Determining whether a particular data set accounts or contains personal information is the first step. As already cited in 3.3.2.5,

> **Art. 4 GDPR:** “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The decision taken in a TNO/DAF agreement and communicated to the members of WP4.2 in the regular meetings was that no personal data was going to accessed by TNO. Hence, with the approval of the data protection officers of both TNO and DAF, only a subset of the data attributes was used guaranteeing at the same time its usability and anonymity without being classified as personal data as in the article 4.

3.4.3.1. Description of the data

The DAF technology responsible for onboard data collection and storage is called DAF Connect. This is an optional system which can be selected by the customer when configuring the vehicle for assembly. The DAF Connect platform consists of an onboard unit that is connected with the electronic system of the vehicle and which acquires data from different sources in the vehicle. The data is temporary cached in the vehicle and periodically transmitted to a centralized DAF cloud platform. The information is collected from different sources including the CAN bus and, in some cases, computations are performed over measured quantities to obtain indirect measurements. TNO accessed a subset of the DAF connect dataset. A non-exhaustive list of the data attributes is given in Table . This dataset spans over several countries and had data from 2018 until 2021. The dataset received by TNO was a subset of it, containing, as mentioned, only some of the data attributed and spanning only one month of data on 2020. This particular study was done with the data on Dutch routes during September 2020. Over this period, more than 5500 unique trucks have been observed. Figure 12 shows the total number of active vehicles as a function of time. It can be observed that about 2000 vehicles are simultaneously active during the day, and over this vehicles, the potential platooning candidates are to be found.

Table U. DAF connect fields.

Field	*Detail*	*Units*
unixTimestamp	Date and time of the measurement	Seconds from 1970
tripID	Identification number of the trip	#
GPSLatitude	Latitude in WGS84	degree
GPSLongitude	Longitude in WGS84	degree
totalDistance	Distance travelled by the vehicle	m
GPSAltitude	Altitude in WGS84	m
GPSHeading	Direction angle w.r.t WGS84	degree
fuelLevel	Fuel level	%
grossCombinationWeight	Vehicle + load mass	kg
wheelbasedSpeed	Speed measured based on the wheel	km/h
tachographSpeed	Speed measured from the CAN bus	km/h
GPSSpeed	Speed measured from the GPS	km/h
AmbiantAirTemperature	Outside air temperature	°C
engineCoolantTemperature	Coolant temperature	°C
GPSHDOP	GPS accuracy	#
acceleration	Vehicle acceleration	m/s
engineLoad	Engine torque	%
engineSpeed	Speed of the engine	RPM
gearCurrent	Current gear	#

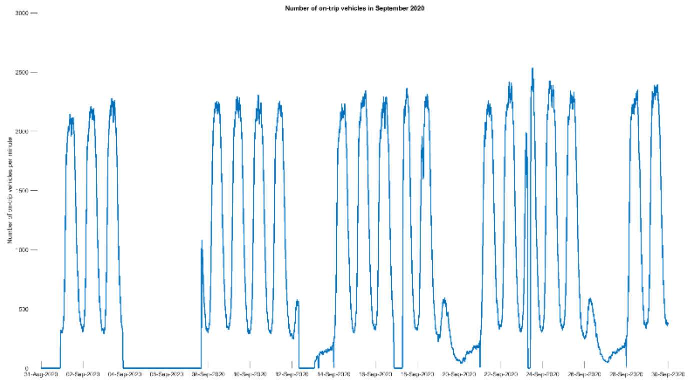


Figure 12 Total number of active vehicles as a function of time for the total period of one month. It can be noted the daily and weekly seasonal effects. The total number of active vehicles on an average day is above 2000. In blue, the 5 second base data.

3.4.4. Methodology

To measure the platoon possibilities for the fleet we used an approach based on the proximity in time and space between vehicles. Despite being this approach closely linked to the spontaneous platooning case, the interpretation of the results for different values of the parameters visits the on the road orchestrated platoons as well. As probably the simplest case of truck matching, we attempt to have a very clean, reproducible and easy interpretable results of what is the platooning potential. The principle of the algorithm is as explained forthwith. All the vehicles travelling on the same road segment in the same direction are potential platooning candidates. Several constrains follow when assessing whether they will effectively form a platoon with distance and time between them being the two main constraints criteria to be explored. Other conditions are to be checked for the platoons to be realistic such as the total distance that the potential vehicle would be part of a given platoon. The logics of these steps in the algorithm are depicted in Figure 13.

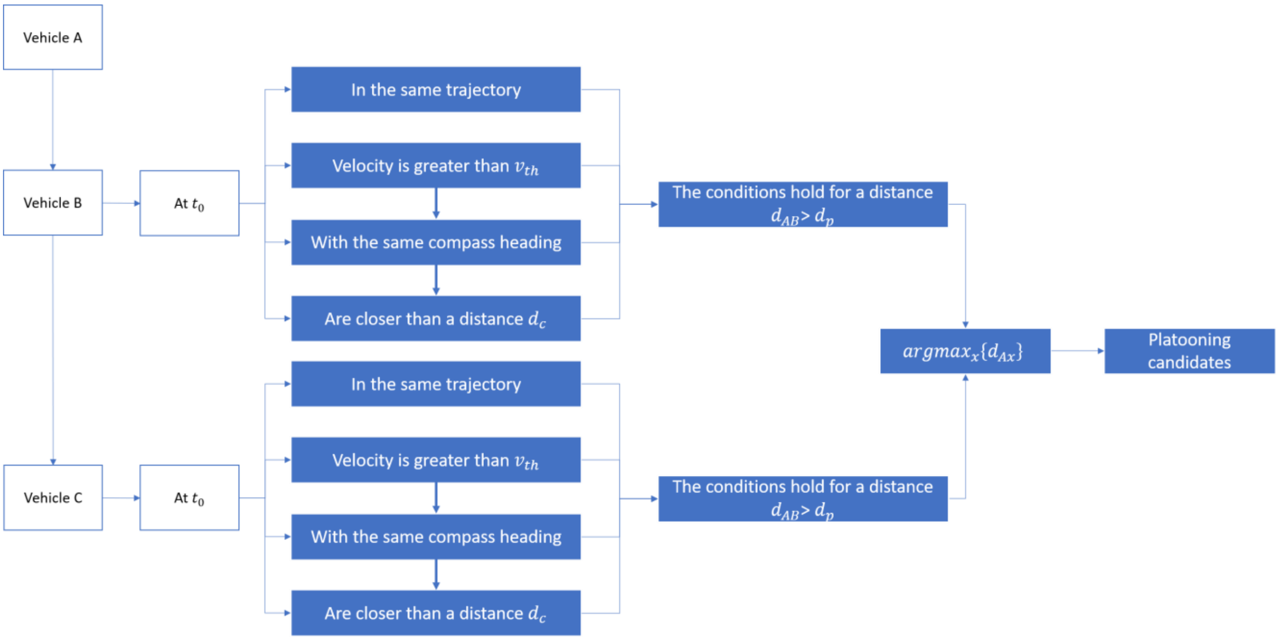


Figure 13. Logic flow of the algorithm used to determine the potential platoons on the data.

In brief, if at the same moment, two vehicles are moving in the same direction of travel on the same road section, both vehicles will be able to form a platoon if the mutual distance is less than the d_c, the maximum platoon distance and disengage when the routes no longer overlap or the mutual distance has become too great. If multiple vehicle combinations are possible, the combination with the greatest joint distance will be assigned.

3.4.4.1. Data pre-processing

In order to execute the aforementioned algorithm, the data is processed and enriched via an extensive data processing pipeline. This includes a trip recognition algorithm and a map matching stage as can be seen in Figure 14.

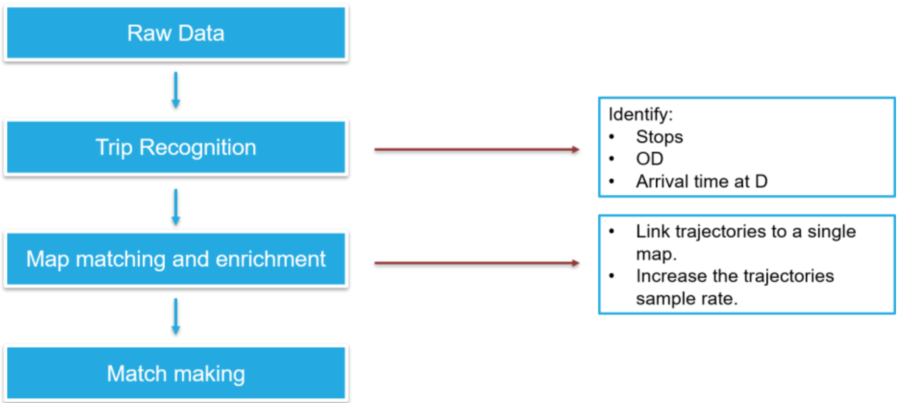


Figure 14. Pipeline of the preprocessing of the data before running the truck matching analysis.

Trip recognition. The timeseries from the DAF Connect platform includes all points in which the ignition of the vehicle was turned on. This ensures that no points are missed, but not all those timeseries are relevant for the platoon matching demonstrator. To select the subset of points where the vehicle is on the road with finite speed between an origin and destination, trips are identified. A trip is then the set of timeseries between origin and destination where the vehicle's speed is higher than zero. The origin and the destination are determined as the places where the vehicle spent more than $T = 15\,min$. Note that these points are not necessarily contiguous in the original dataset. Vehicles can also stay standing for periods shorter than the threshold defined to be considered a final destination. These segments of time series defined what we call a stop. Several stops can take place within the same trip. The different timeseries that constitute a trip are referred as routes. Every trip consists of $N_s + 1$ routes with N_s the number of stops in the trip.

Map Matching. The dataset records the position of the vehicle based on Global Navigation Satellite System (GNSS) meaning that the timeseries are in latitude and longitude to a reference world shape model. Determining the section in which the platoons are together with the distance between them results in an involved process. Furthermore, the original timeseries' sample rate is 5' which is particularly large sample rate to determine spontaneous platoons. To overcome the later problem, determine the segment on the network the vehicle is in and ease the computation of distance in the current work we decided to link the routes to a network. In order to do so, the Open-Source Routing Machine (OSRM) (Luxen & Vetter, 2011) has been used. OSRM is system that given a sequence of points and times determines what is the most likely route in the real network that was taken. From the OSRM we obtain the specific links from the network that correspond to each of the points. With this information it is also easy to resample the data to a higher sampling rate by means of interpolation. In Figure 15 we show an example of an individual route before being map matched, and in Figure 16, the same route after being matched to the map.

In order to determine a timeframe in which the platoon feasibility was to be analyzed in the dataset, it was considered that vehicle trips often span more than one weekday. Since the number of trips decreases considerably during Sundays, the data was analyzed in continuous pieces each containing an entire week from Monday morning to Sunday night.

Figure 15. Example of an individual route in the map before being linked to the network and interpolated.

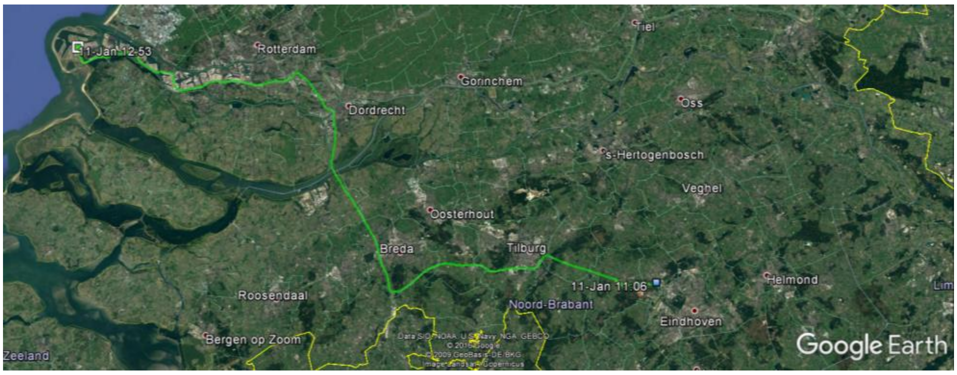


Figure 16. Example of the same route shown in figure 4, after being linked to the network by means of OSRM and interpolated to 5s intervals.

3.4.4.2. Implementation

The algorithm schematized in Figure 13 was implemented over this new pre-processed and enriched dataset. The main steps of such implementation are summarized in the following steps. The current implementation only takes into account platoons formed by two vehicles, generalization two more vehicles is straight forward and will be done in further research.

- For each timestep:
  - Is there more than one vehicle on the network? (phase 1)
  - Is more than one vehicle active? (phase 2)
    In case both previous answers are affirmative,
    - For each of these vehicles (phase 3)
      - For each other vehicle within the platooning distance d_c
        - Is its speed greater than speed threshold?
        - Do the vehicles have the same direction?
          In case both answers are affirmative, a detailed analysis of candidates described below determines whether the vehicles effectively form a platoon.

Analysis of candidates. When the mentioned conditions are fulfilled, two further conditions are checked. First, the overlap of the routes of the vehicles $T_p = 10\,min$ around the timestep being evaluated. It needs to be higher than a given threshold in this case 80%. Second, the overall overlap for potential platooning distance is computed, in order for the platoon to be accepted such a distance need to be higher than the minimum platoon distance d_M which in this case was set to d_M 10 km. Figure 17 to Figure 20 explain the platoon matching algorithm for one timestep. Figure 17 shows a snapshot of an arbitrary timestep. It can be seen that there are several vehicles in the network. In Figure 18 the following step is visualized: whether is there more than one active vehicle, which is also true. Figure 19 and Figure 20 illustrate the rest of the process. First, and second, selection based on the shared distance between the two vehicles.

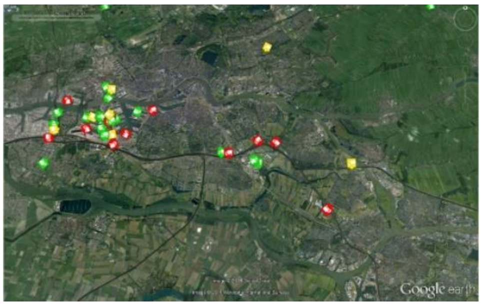


Figure 17. Phase 1,the vehicles present on the network are determined.

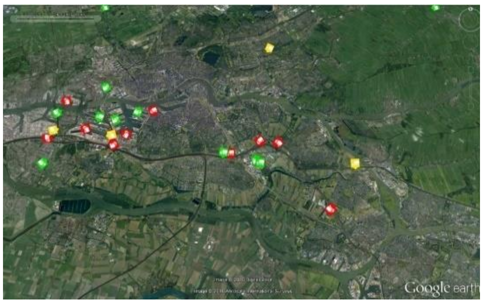


Figure 18. Phase 2, the inactive vehicles in the network are discarded.

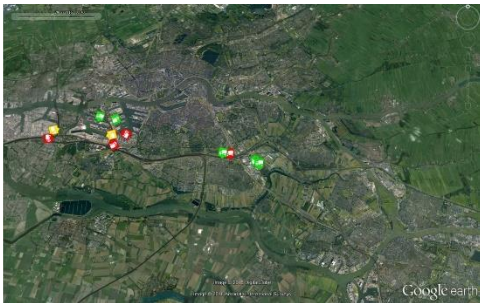


Figure 20. Phase 3 Vehicle pairs that are closer than d_c, will drive together for more than d_M, their speeds are greater than v_{th} and their have the same compass heading are selected.

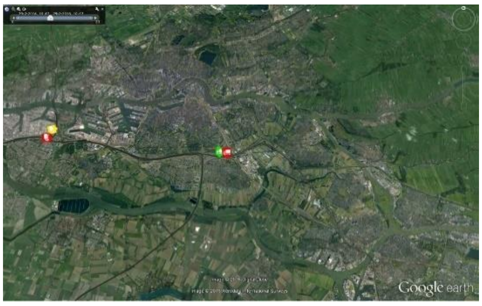


Figure 19. Phase 4 The best pair of vehicles for each case are defined as the platoon candidates.

Implementation performance. The main reason for the design of the current implementation was computational performance. The current design allows to trivially parallelize the analysis of each second of data. First of all, the possible platoons are determined for each individual time step and then the relationship over the overarching period is reduced. From 10:10:05, for example, a possible platoon combination is registered on any date and continues to return from the analysis until 10:55:40; this means that this particular combination could have formed a platoon during this period. Within the aggregation of the time points, it is taken into account that a platoon may temporarily not be able to be traced back as a possible combination in the meantime. This can occur, for example, if the intermediate distance temporarily exceeds the used threshold value or if one of the trucks has briefly taken a different route (for example a parallel lane). Any stops of short size are filtered out, so that such situations are registered as one platoon. If a vehicle journey occurs in several platoon combinations, the combination of vehicle journeys with the greatest possible distance is chosen.

Since this is not an operational platooning algorithm, it naturally has several practical events that are not considered. Notably the (dis)engaging processed are not contemplated. This is not a problem as it would scale with the number of vehicles in platoon and an estimation of its potential drawbacks can be easily estimated. Nevertheless, given that these processes happen in a given period of time, another condition was added to the algorithm. A platoon was required to last at least 500 s. That avoids the cases in which the platoons are not plausible due to the (dis)engaging times. Thanks to the algorithm design, the costs of engaging and disengaging can be easily incorporated as penalties when forming the platoons. Distance and time that the engaging and disengaging needs are already part of the algorithm, since the speed and position are already determined.

Outcome variables. Several observables are collected from as the outcome measures of this algorithm. These are them used to obtain Key Performance indicators (KPI).

- Platoon starting time and location in GCS,
- Platoon end time and location in GCS,
- Vehicle ids for the members of the platoon,
- Route the platoon has travelled,
- Total distance travelled by the platoon,
- Total time in which both vehicles could have driven as platoons.

3.4.4.3. Parameter Setting

The outcome of interest is the probability to find a platoon match for every truck. This of course heavily depends on many parameters. In particular, two of them are interesting to explore namely, the number of vehicles included in the analysis (N_v, which works as a proxy for the penetration rate) and the minimum distance between vehicles for them to be considered matching candidates (d, from which the interpretation is more involved and it is related to the degree of on the road orchestration that the matching system has).

For the analysis to be independent of the vehicle ordering in the dataset, the vehicles selected in each iteration of the analysis were selected at random from a uniform distribution.

3.4.5. Representativeness

The analysis of impact of platoon, feasibility and benefits on the current fleet is, naturally, heavily dependent on the number of vehicles that are on the road and the number of vehicles that are included in the analysis. For that reason, it is necessary to determine what is the representativeness of the sample that is used as part of this Platoon Feasibility study (DAF vehicles in the Netherlands that are connected via DAF Connect) in comparison to the total fleet of Heavy Goods Vehicles in the Netherlands (across all OEMs). By means of the penetration rate any results can be translated and extrapolated further. In order to do so, the total number of trucks on several points of the Dutch highway network was estimated. This was done by means of the recordings of the induction loops on the Dutch network provided by NDW and processed by TNO. The pre-processed version of the data by TNO includes the number of vehicles per category in each segment of the road. Those numbers were contrasted to the ones from the DAF Connect sample and see what the representativeness of the latter was.

Not only the overall representativeness needs to be evaluated but whether it is stable in time and space. In order to do so, first, the number for both the DAF connect subsamples and the population was observed either they were stable in time which turned out to be true. Hence, to have a better estimated, we proceeded to compute a month average of all the vehicles counts in all the road segments in time windows of 1 minute. We ended up with a daily average in each position detector.

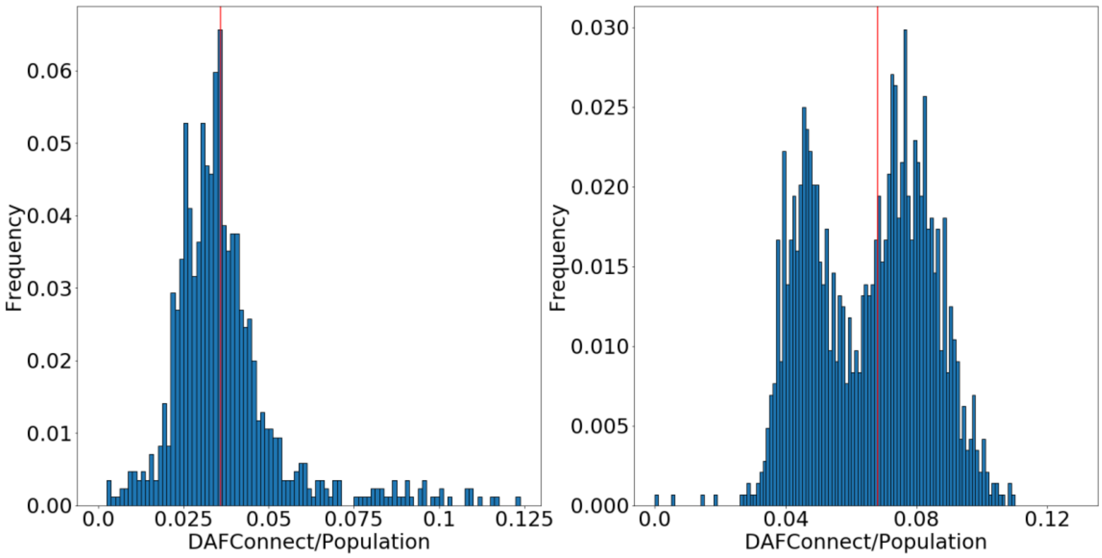


Figure 21. Distribution of the ratio between the DAF sample and the population. On the left panel the distribution averaged over all the minutes of the day, showing the distribution over the different segments of the network. On the right, averaged over the different segments, showing the distribution over the day. In red the means of the distribution in each case.

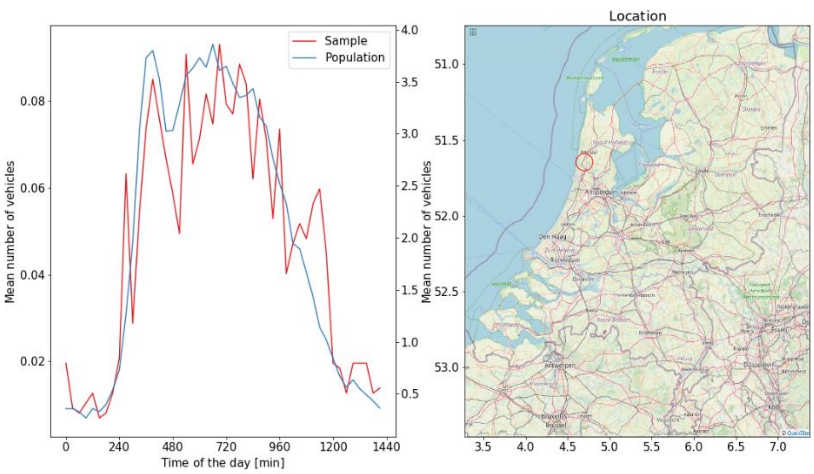


Figure 22. Example 1 of the representativeness of the DAF Connect sample on the total population for a specific location in North Holland Region. On the left, in red the DAF data and in Blue the data

obtained from the induction loop sensors as a function of time of the day in windows of 30 min. This data has been averaged over the whole month of September 2021 with the purpose of obtaining smoother and more accurate values.

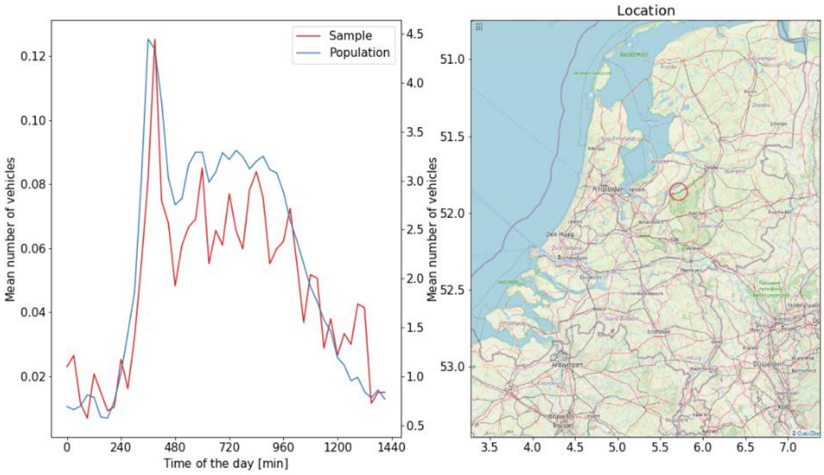


Figure 23. Example 1 of the representativeness of the DAF Connect sample on the total population for a specific location in Gelderland Region. On the left, in red the DAF data and in Blue the data obtained from the induction loop sensors as a function of time of the day in windows of 30 min. This data has been averaged over the whole month of September 2021 with the purpose of obtaining smoother and more accurate values.

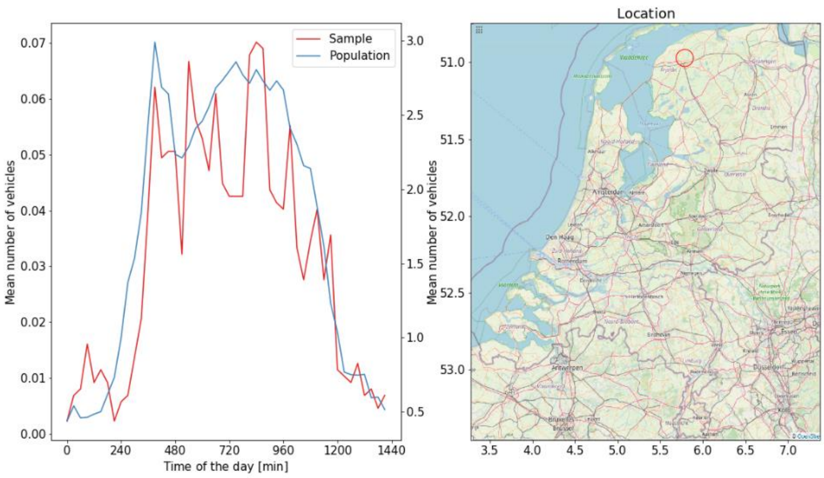


Figure 24. Example 1 of the representativeness of the DAF Connect sample on the total population for a specific location in Friesland Region. On the left, in red the DAF data and in Blue the data obtained from the induction loop sensors as a function of time of the day in windows of 30 min. This data has been averaged over the whole month of September 2021 with the purpose of obtaining smoother and more accurate values.

The overall ratio for a random subsample of the detectors is shown in Figure 22 (left). It can be seen that such a number seems stable, with a uniform distribution along the different locations (the 5% tail has been removed from the figure). Figure 21 (right) shows a similar comparison but for different hours of the day, but in this case bimodal, arguably with different representations during the night and day periods. The overall ratio is 3.6%. Finally, in Figure 22 to Figure 24 several examples are shown, where the seasonal trend can be appreciated as expected. It is worth to notice that for this step was determinant to have map-matched the routes in order to be able to identify the location of the induction loops on the DAF connect sample.

Given that data from one OEM has been studied in this task the results and forthcoming learnings are based on a sample set that is not necessarily representative for the whole fleet in the Netherlands. To investigate the representativeness of the sample dataset an analysis has been conducted in which it was examined how many heavy goods vehicles have passed a (static) measuring point and how many of these vehicles were available from the DAF connect dataset. The results show that overall, the penetration rate was 3.6% and moreover the patterns were consistent in both space and time. Based on this, the dataset was deemed suitable for the subsequent analyses.

3.4.6. Results

The matching analysis was running for several weeks of September 2020. Each of these weeks was treated separately and the results presented in this section are derived from week 38. The algorithm span two parameter space namely number of vehicles N_v and the minimum distance between vehicles to be able to join a platoon, d_c. The fraction of the distance travelled in a platoon in this space, averaged over the four weeks analyzed, is shown in Figure 25.

The fraction is monotonically increasing with both N_v and d, as expected. The relation, that seems linear at first glance, can be observed to be rather a power law relation with exponent $\gamma < 1$, at least for large number of N_v. This can be interpreted as follows, for small numbers of N_v, the likelihood of finding a platooning candidate is small, but the ratio of the platooning and the total distance can as large as 1. On the contrary, when the number of vehicles is large, although finding platooning candidates for a new vehicle is extremely likely, the distance it travels will be a small fraction on the overall fleet.

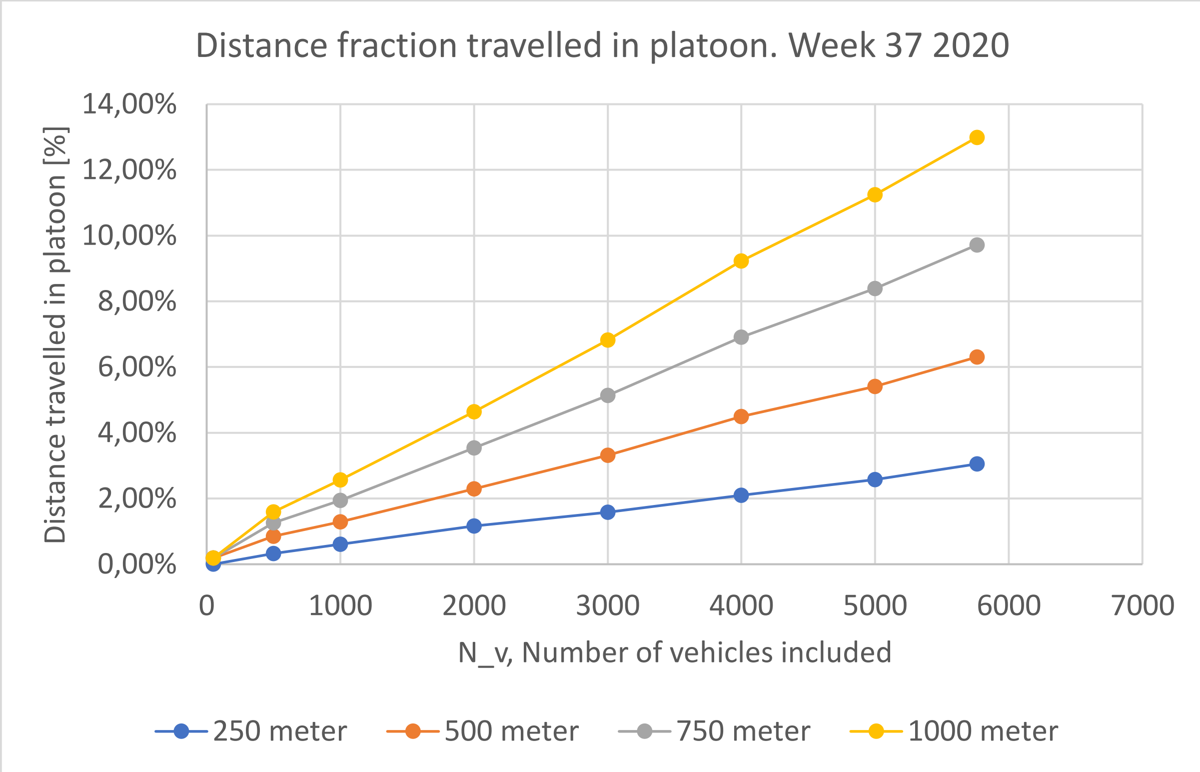


Figure 25. Fraction of the distance in platooning as a function of the number of vehicles for three different minimum platooning distances, 500, 100 and 1500 m.

This can be further corroborated in Figure 26 and Figure 27. In Figure 26, the total distance is shown instead of the ratio. It can be observed that the total platooning distance does increase rapidly with the number of vehicles, faster than linearly. Figure 27 is similar to Figure 26 but for the travelling times, which since the velocity of the vehicles is relatively stable, the functional shape remains the same.

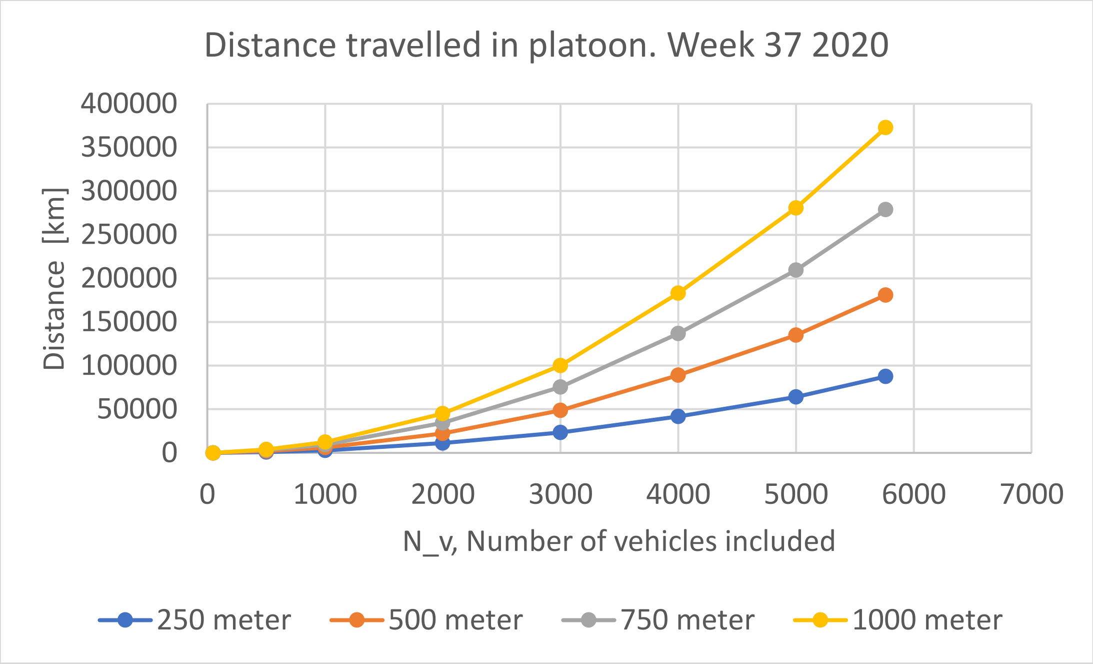


Figure 26. Total distance in platoon for the four different values of d_c and a function of the number of vehicles N_v. Each curve is for a diffrenent value of d_c as indicated in the legend. Analysis was done on the circular markers, lines connecting them have been added for readibility.

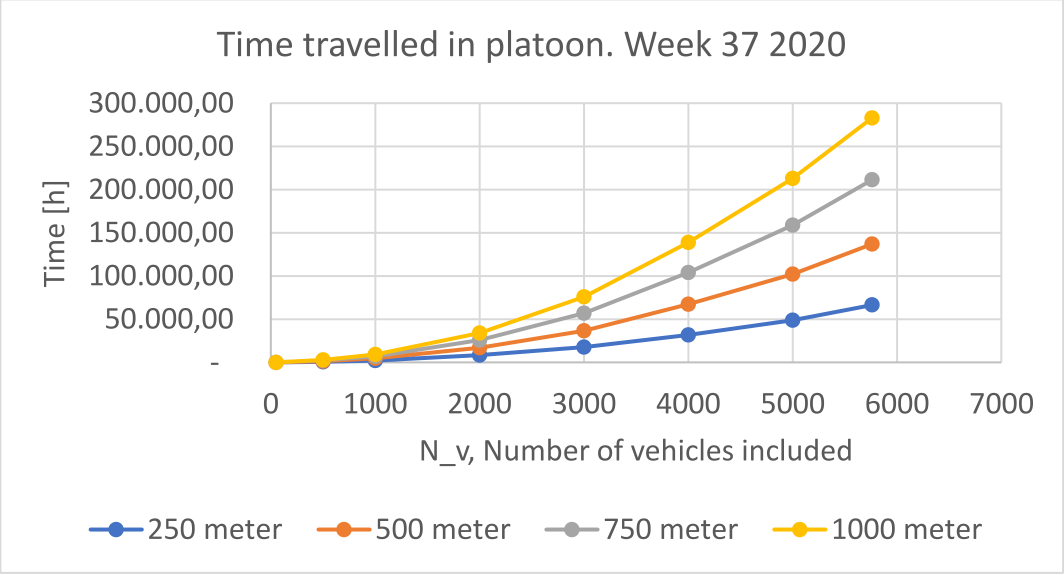


Figure 27. Total time in platoon for the four different values of d_c and a function of the number of vehicles N_v. Each curve is for a different value of d_c as indicated in the legend. Analysis was done on the circular markers, lines connecting them have been added for readibility.

The spatial distribution of the platoons is a relevant observable with a clear impact on the planning. The normalized density function for the start and end locations of the platoons is shown in Figure 28 and Figure 29. The Region of the port of Rotterdam emerges as the densest area for both start and end of platoons. Other regions, as Den Haag also have high density, which means that the likelihood of a platoon starting in this area is high.

Figure 28. Spatial distribution of the locations where the platoons start. It can be seen that the origin of the platoons are focused around the region of the Port of Rotterdam, also other locations in which highways intersect (e.g. Utrecht area) are apparent. Lastly also the various important border crossings for freight traffic (Bergen op Zoom, Venlo and Maastricht) are noticeable.

Figure 29. Spatial distribution of the locations where the platoons end. As in the Figure 28, it can be seen that the origin of the platoons is centered in the region neighboring the port as expected. Interestingly enough, there are some regions that emerge as platoon ending location that were not platooning starting locations.

3.4.7. Conclusion and Discussion

Platoon potentials have been assessed with real logistical data from a subpopulation of the DAF fleet in the Netherlands region. The simulation has shown that, for a (sub)population of 5500 vehicles that have driven aa daily aggregated average of 700.000 km, 14% of the total travel distance could have been driven as part of a platoon (assuming a match distance of 1000 m) if the technology was available and operation in the vehicles. This match rate has been determined without any changes to the schedules or routes of the vehicle, this implies that the match-rate might be higher when optimizations are considered.

As a result of the simulation study, it became apparent that potential platoons are registered especially in areas that are logistically important (e.g., Port of Rotterdam) and/or where major arterial roads converge. As part of future pilots, it might be relevant to focus on specific use cases.

The results show that the match increases when the number of vehicles of enabled vehicles increase (penetration rate). When more vehicles are platooning capable the chance of finding a gainful match increase on a given trajectory. Given that the simulation only included 3,5% of the Dutch heavy vehicles there is potential for growth. The estimations indicate that for a case of ~150 000 vehicles, which would correspond to the total number of vehicles observed in The Netherlands the distance performed in platooning can be up to 20%.

Potential benefits are being constantly explored and analyzed. Whereas the fuel came up originally as the main drive for the platooning technology also other benefits are considered, for example the potential benefits in terms of traffic safety and throughput. The methodology applied in this research can be used to further investigate these benefits based on the resulting match rates and the distances resulting from the analysis. For example, the results of the described simulation study can be applied as part of an economic cost/benefit analysis in which the future benefits on the various impact areas (logistics, livability, traffic safety and accessibility) can be further elaborated.

3.4.8. Applicability

Integration within the logistical operation

As concluded in the previous section the platoon matching demonstrator has shown that, without any (sophisticated) optimization algorithms, a significant match rate of 10% is possible. This match rate indicates that, given the 'existing' real-life logistical operation, 10% to 14% of the total vehicle distance can be driven as part of a platoon assuming that enough vehicles are platooning enabled. However, technology is not the only boundary condition, in addition, the willingness of logistical operators and drivers is an important factor.

For logistical operators the final decision to equip vehicles with platooning technology is largely a cost/benefit consideration. As part of this consideration the direct economic costs/benefits are of primary importance and secondarily the qualitative benefits (e.g., driver comfort). Possible societal aspects may be considered in the context of sustainable entrepreneurship but are difficult to take into account or need to be internalized by the government by providing subsidies.

Given that Roland Berger estimates the additional costs for a platooning capable vehicle range from 12.000 to 20.000 there must be a significant positive business case to persuade the Logistics Service Providers (LSPs) to invest in platooning technology. Especially since these costs only consider the technical modifications to the vehicles (automatic transmission, various sensors, automated steering column, testing and maintenance) and do not include additional costs for driver training or additional maintenance.

The ENSEMBLE project as mainly focuses on the development and implementation of the 'platooning' support function, including longitudinal control at a headway of 1,5 seconds, and in which the driver is still in the truck and legally responsible. Given the relatively large vehicle separation it is expected that the fuel benefits and traffic throughput are minimally influenced; in real-life traffic vehicles often drive at a smaller distance gap (even if this might not correspond to traffic rules/safe distance). Since the driver is still fully responsible it is unlikely that the support function will have benefits in terms of driver efficiency or asset utilization optimizations (reduced truck idle times).

Perhaps the traffic safety is improved (safer distance control, V2V communications and coordinated braking maneuvers) however this improvement is especially evident when comparing platooning-capable vehicles with current (traditional) vehicles and less evident when comparing platooning-capable vehicles with modern (state-of-the-art) vehicles. The modern vehicles, for example, include the mandatory Autonomous Emergency Braking system (AEB) and moreover from 2022 also additional safety systems become mandatory (e.g., drowsiness and attention detection, distraction recognition, event accident data recorder and intelligent speed assistance). If we then bring the various arguments together it becomes apparent that the main remaining benefit for the platooning support function is a potential improved driver comfort which makes the costs somewhat skewed with the benefits.

When regarding the autonomous function the expectations are more nuanced since this function assumes that the driver is no longer in the vehicle. Given that the costs of labor constitute (roughly) around 60% of the operational costs of a truck this will significantly affect the cost of operating a vehicle for a logistical service provider. Additionally, since the driver is out of the loop also other aspects i.e., a reduction of the insurance costs, and an improved additional asset utilization (reduced idle time of vehicle) can be regarded as direct monetary benefits. Additionally, the autonomous function allows constant smaller following distances (20 m) which in turn provides a positive effect on fuel consumption (due to the reduced aerodynamic drag) and traffic flow (due to the higher truck density). However, because future truck configurations are unknown and furthermore the ODD has not yet been determined (i.e., how autonomous vehicles operate as part of the mixed traffic operation) it is difficult to predict and describe this future situation. Given that the stop towards autonomous platooning lies several years ahead it is complicated to make a detailed and reliable business case.

Further considerations

As part of this study an extensive data analysis has been conducted based on actual logistical data provided by DAF.
Of course the DAF data only provides a subset which is not fully representative from two perspectives:

- The other OEM’s are not included.
- DAF Connect is a paid service that has undergone major developments in the recent years, during Ensemble it was a (paid) service from the vehicle option list potentially targeting a specific customer group. This results in the service mainly being available for modern vehicles and possibly specific use cases.

Given these known characteristics our work specifically included an analysis of the representativeness of the DAF sample compared to the Dutch fleet (see section 3.4.5). As part of this analysis we saw that the average DAF sample size was 3.6% of the total fleet of vehicles and that these statistics were stable in both time and space; the daily patterns of the DAF data really followed the patterns of the total fleet that passed the sensors. Given that the analysis focused on platooning at highways (where the detectors were located and the verification was performed) we are confident that the dataset provides a reliable foundation for the analysis that was conducted.

Possibly an analysis that focused on a Europe scale would have had added value, but this really required us to bring integrate local loop data (e.g. loops from France) into the methodology. Given the extensive effort that was required to obtain a FCD dataset (from DAF) while adhering to rules and regulations (such as the GDPR) this did not fit in the scope of the task.

The value of this work is that it contributed to a better understanding of the potential integration of platooning in a logistical operation. Especially for end-users such as fleet owners and drivers this analysis makes it more tangible how a certain service is envisioned and what added value it might bring. With the Ensemble platooning simulation study we have taken the (earlier) analysis in 2016 with a sample of 200 vehicles to a new level with a fleet of 5.500 vehicles that are simultaneously driving. As part of the analysis a large dataset has been processed, pushing the boundaries in terms of computational performance and memory usage. There are broader applications of this type of analysis, for example to gain a better insight into freight movements (origins and destinations), loads (both vehicles and strain on the infrastructure) and other applications.

4. SUMMARY AND CONCLUSION

The results documented in this deliverable clearly prove that objectives mentioned in the description of work have been achieved. To be more specific:

1) An API has been defined for future service providers which want to offer mandatory platoon formation service

2) Possible issues associated with platooning services and solutions thereof have been documented

3) Potential cyber security risks and required countermeasures have been identified

4) A simulation of platooning probability based on real world transportation data was performed

The results of research and development work is not only the achievement of targets but also consists of what was learned along the way. Some additional findings are listed below:

A) The starting hypothesis that backend-based services are mandatory for platooning can be confirmed. The results should be added of the overall specification for platooning.

B) In Figure 1 we started with the assumption that there is a layered architecture in the backend with both strategic and service layers. The work done could not specifically confirm this. Moreover, it seems that the platooning services backend follows the trend to an architecture in which clouds are linked, something typical in the IT industry.

C) The initial success of platooning is dependent on fleets making mission data available to a platooning service provider which enables platoon matching, even if this is against the nature of a fleet to disclose this.

Looking into the future it is difficult to foresee when first platoon matching services will be available. It might be that these only become visible in a second step, the first step being when predominantly large fleets organize their own intra-fleet platoons. This is a likely entry scenario especially for large fleets in which there are regular missions with multiple vehicles travelling from hub to hub. No service provider is required as this can be organized in the established transportation management solutions. The necessary platooning capable vehicles would then also be available to platoon with vehicles from other fleets opening the door for the second step.

Recommendations on future research work are quite challenging since there is much work and convincing to get to the first step described above. It is not unthinkable that the first platooning vehicles are robots and not trucks. The service portfolio of such vehicles could differ significantly

5. BIBLIOGRAPHY

A. Alam, B. B. (2015). Heavy-duty vehicle platooning for sustainable freight transportation: A cooperative method to enhance safety and efficiency. *IEEE Control Systems Magazine*.

A. Johansson, E. Nekouei, K. H. Johansson & J. Mårtensson . (2021). Strategic Hub-Based Platoon Coordination under Uncertain Travel Times. *IEEE Transactions on Intelligent Transportation Systems*.

ACEA. (2021). *Consolidated Registrations*. Retrieved from European Automobile Manufacturers Association: https://www.acea.be/statistics/tag/category/by-manufacturer-registrations/

Besselink, B., Turri, V., van de Hoef, S. H., Liang, K.-Y., Alam, A., Mårtensson, J., & Johansson, K. H. (2016). Cyber-physical Control of Road Freight Transport. *Proceedings of the IEEE*, 1128-1141.

Comission, E. (2018). *European General Data Protection Regulation.*

Cramer, R. &. (2015). Secure multiparty computation. *Cambridge University Press*.

Dellrud, J. (2020). *Sweeden4Platooning Technical Report .* Södertälje: Scania AB.

DATEX II. (2021). Information about DATEX. Retrieved from https://www.datex2.eu/

Effigy. (2021). Retrieved from Effigy Consulting: https://www.effigy-consulting.com/road-freight-market-report/

ETSI. (2021). Description of ETSI. Retrieved from https://www.etsi.org/

FEDeRATED. (2021). Description of FEDeRATED. Retrieved from http://www.federatedplatforms.eu/

FMS-Standard. (2017). *Information about the FMS-Standard*. Retrieved from FMS-Standard Startpage: http://bus-fms-standard.com/Truck/down_load/Technical_Specification_rFMS_V2.1.0_13.10.2017.pdf

Horowitz, R. V. (2000). Control design of an automated highway system. *Proceedings of the IEEE*.

Janssen, Z. B. (2015). *Truck platooning: Driving the future of transportation.*

Liang, K.-Y., van de Hoef, S., Terelius, H., Turri, V., Besselink, B., Mårtensson, J., & Johansson, K. H. (2016). Networked control challenges in collaborative road freight transport. *European Journal of Control*.

Luxen, D., & Vetter, C. (2011). Real-time routing with OpenStreetMap data. *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems* (pp. 513-516). Chicago, Illinois: ACM.

Tsugawa., S. (2013). An overview on an automated truck platoon within the energy ITS project. *In 7th IFAC Symposium on Advances in Automotive Control*.

van Ark, E., Duijnisveld, M., Eijk, E. v., Hendrickx, N., Janssen, G., Malone, K., . . . Soekroella, A. (2017). *Value Case Truck Platooning - an early exploration of the value of large-scale deployment of truck platooning.* TNO. Retrieved from https://repository.tno.nl/islandora/object/uuid:770c9b7c-40f0-4036-93e8-caba19c2b311

Wang, Y. (2009). Privacy-enhancing technologies. In *Handbook of research on social and organizational liabilities in information security* (pp. 203-227). IGI Global.

6. APPENDIX A. EXAMPLE OF APPENDIX AND SUB-SECTIONS

6.1. Glossary

6.1.1. Definitions

Term	Definition
Convoy	A truck platoon may be defined as trucks that travel together in convoy formation at a fixed gap distance typically less than 1 second apart up to 0.3 seconds. The vehicles closely follow each other using wireless vehicle-to-vehicle (V2V) communication and advanced driver assistance systems
Cut-in	A lane change manoeuvre performed by vehicles from the adjacent lane to the ego vehicle's lane, at a distance close enough (i.e., shorter than desired inter vehicle distance) relative to the ego vehicle.
Cut-out	A lane change manoeuvre performed by vehicles from the ego lane to the adjacent lane.
Cut-through	A lane change manoeuvre performed by vehicles from the adjacent lane (e.g. left lane) to ego vehicle's lane, followed by a lane change manoeuvre to the other adjacent lane (e.g. right lane).
Ego Vehicle	The vehicle from which the perspective is considered.
Emergency brake	Brake action with an acceleration of <-4 m/s2
Event	An event marks the time instant at which a transition of a state occurs, such that before and after an event, the system is in a different mode.
Following truck	Each truck that is following behind a member of the platoon, being every truck except the leading and the trailing truck, when the system is in platoon mode.
Leading truck	The first truck of a truck platoon
Legal Safe Gap	Minimum allowed elapsed time/distance to be maintained by a standalone truck while driving according to Member States regulation (it could be 2 seconds, 50 meters or not present)
Manoeuvre ("activity")	A particular (dynamic) behaviour which a system can perform (from a driver or other road user perspective) and that is different from standing still, is being considered a manoeuvre.

Term	Definition
ODD (operational design domain)	The ODD should describe the specific conditions under which a given automation function is intended to function. The ODD is the definition of where (such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an automation function is designed to operate.
Operational layer	The operational layer involves the vehicle actuator control (e.g. accelerating/braking, steering), the execution of the aforementioned manoeuvres, and the control of the individual vehicles in the platoon to automatically perform the platooning task. Here, the main control task is to regulate the inter-vehicle distance or velocity and, depending on the Platooning Level, the lateral position relative to the lane or to the preceding vehicle. Key performance requirements for this layer are vehicle following behaviour and (longitudinal and lateral) string stability of the platoon, where the latter is a necessary requirement to achieve a stable traffic flow and to achieve scalability with respect to platoon length, and the short-range wireless inter-vehicle communication is the key enabling technology.
Platoon	A group of two or more automated cooperative vehicles in line, maintaining a close distance, typically such a distance to reduce fuel consumption by air drag, to increase traffic safety by use of additional ADAS-technology, and to improve traffic throughput because vehicles are driving closer together and take up less space on the road.
Platoon Automation Levels	In analogy with the SAE automation levels subsequent platoon automation levels will incorporate an increasing set of automation functionalities, up to and including full vehicle automation in a multi-brand platoon in real traffic for the highest Platooning Automation Level. The definition of "platooning levels of automation" will comprise elements like e.g. the minimum time gap between the vehicles, whether there is lateral automation available, driving speed range, operational areas like motorways, etc. Three different levels are anticipated; called A, B and C.
Platoon candidate	A truck who intends to engage the platoon either from the front or the back of the platoon.
Platoon cohesion	Platoon cohesion refers to how well the members of the platoon remain within steady state conditions in various scenario conditions (e.g. slopes, speed changes).
Platoon disengaging	The ego-vehicle decides to disengage from the platoon itself or is requested by another member of the platoon to do so. When conditions are met the ego-vehicle starts to increase the gap between the trucks to a safe non-platooning gap. The disengaging is completed when the gap

Term	Definition
	is large enough (e.g. time gap of 1.5 seconds, which is depends on the operational safety based on vehicle dynamics and human reaction times is given). A.k.a. leave platoon
Platoon dissolve	All trucks are disengaging the platoon at the same time. A.k.a. decoupling, a.k.a. disassemble.
Platoon engaging	Using wireless communication (V2V), the Platoon Candidate sends an engaging request. When conditions are met the system starts to decrease the time gap between the trucks to the platooning time gap. A.k.a. join platoon
Platoon formation	Platoon formation is the process before platoon engaging in which it is determined if and in what format (e.g. composition) trucks can/should become part of a new / existing platoon. Platoon formation can be done on the fly, scheduled or a mixture of both. Platoon candidates may receive instructions during platoon formation (e.g. to adapt their velocity, to park at a certain location) to allow the start of the engaging procedure of the platoon.
Platoon split	The platoon is split in 2 new platoons who themselves continue as standalone entities.
Requirements	Description of system properties. Details of how the requirements shall be implemented at system level
Scenario	A scenario is a quantitative description of the ego vehicle, its activities and/or goals, its static environment, and its dynamic environment. From the perspective of the ego vehicle, a scenario contains all relevant events. Scenario is a combination of a manoeuvre (“activity”), ODD and events
Service layer	The service layer represents the platform on which logistical operations and new initiatives can operate.
Specifications	A group of two or more vehicles driving together in the same direction, not necessarily at short inter-vehicle distances and not necessarily using advanced driver assistance systems
Steady state	In systems theory, a system or a process is in a steady state if the variables (called state variables) which define the behaviour of the system or the process are unchanging in time. In the context of platooning this means that the relative velocity and gap between trucks is unchanging within tolerances from the system parameters.

Term	Definition
Strategic layer	The strategic layer is responsible for the high-level decision-making regarding the scheduling of platoons based on vehicle compatibility and Platooning Level, optimisation with respect to fuel consumption, travel times, destination, and impact on highway traffic flow and infrastructure, employing cooperative ITS cloud-based solutions. In addition, the routing of vehicles to allow for platoon forming is included in this layer. The strategic layer is implemented in a centralised fashion in so-called traffic control centres. Long-range wireless communication by existing cellular technology is used between a traffic control centre and vehicles/platoons and their drivers.
Tactical layer	The tactical layer coordinates the actual platoon forming (both from the tail of the platoon and through merging in the platoon) and platoon dissolution. In addition, this layer ensures platoon cohesion on hilly roads, and sets the desired platoon velocity, inter-vehicle distances (e.g. to prevent damaging bridges) and lateral offsets to mitigate road wear. This is implemented through the execution of an interaction protocol using the short-range wireless inter-vehicle communication (i.e. V2X). In fact, the interaction protocol is implemented by message sequences, initiating the manoeuvres that are necessary to form a platoon, to merge into it, or to dissolve it, also taking into account scheduling requirements due to vehicle compatibility.
Target Time Gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds, agreed by all the Platoon members; it represents the minimum distance in seconds allowed inside the Platoon.
Time gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds.
Trailing truck	The last truck of a truck platoon
Truck Platoon	Description of system properties. Details of how the requirements shall be implemented at system level
Use case	Use-cases describe how a system shall respond under various conditions to interactions from the user of the system or surroundings, e.g. other traffic participants or road conditions. The user is called actor on the system, and is often but not always a human being. In addition, the use-case describes the response of the system towards other traffic participants or environmental conditions. The use-cases are described as a sequence of actions, and the system shall behave according to the specified use-cases. The use-case often represents a desired behaviour or outcome. In the ensemble context a use case is an extension of scenario which add more information regarding specific internal system interactions, specific interactions with the actors (e.g. driver, I2V) and will add different flows (normal &

Term	Definition
	alternative e.g. successful and failed in relation to activation of the system / system elements).

6.1.2. Acronyms and abbreviations

Acronym / Abbreviation	Meaning
ACC	Adaptive Cruise Control
ADAS	Advanced driver assistance system
AEB	Autonomous Emergency Braking (System, AEBS)
ASIL	Automotive Safety Integrity Level
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
C-ACC	Cooperative Adaptive Cruise Control
C-ITS	Cooperative ITS
CA	Cooperative Awareness
CAD	Connected Automated Driving
CAM	Cooperative Awareness Message
CCH	Control Channel
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DITL	Driver-In-the-Loop
DOOTL	Driver-Out-Of-the Loop
DSRC	Dedicated Short-Range Communications
ETSI	European Telecommunications Standards Institute
EU	European Union
FCW	Forward Collision Warning
FLC	Forward Looking Camera
FSC	Functional Safety Concept

Acronym / Abbreviation	Meaning
GN	GeoNetworking
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
HARA	Hazard Analysis and Risk Assessment
HIL	Hardware-in-the-Loop
HMI	Human Machine Interface
HW	Hardware
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITL	In-The_Loop
ITS	Intelligent Transport System
IVI	Infrastructure to Vehicle Information message
LDWS	Lane Departure Warning System
LKA	Lane Keeping Assist
LCA	Lane Centring Assist
LRR	Long Range Radar
LSG	Legal Safe Gap
MAP	MapData message
MIO	Most Important Object
MRR	Mid Range Radar
OS	Operating system
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
OOTL	Out-Of The-Loop
PAEB	Platooning Autonomous Emergency Braking

Acronym / Abbreviation	Meaning
PMC	Platooning Mode Control
QM	Quality Management
RSU	Road Side Unit
SA	Situation Awareness
SAE	SAE International, formerly the Society of Automotive Engineers
SCH	Service Channel
SDO	Standard Developing Organisations
SIL	Software-in-the-Loop
SPAT	Signal Phase and Timing message
SRR	Short Range Radar
SW	Software
TARA	Threat And Risk Analysis
TC	Technical Committee
TOR	Take-Over Request
TOT	Take-Over Time
TTG	Target Time Gap
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WP	Work Package

6.2. API descriptions

API between PSP and carrier

The following assumption have been made:

- PSP manages the platoons during the timeframe of platoon forming until platoon departure
- PSP does not consider the platoon journey
- Each platoon gets a unique identification = PlatoonID
- Platoon rendezvous location identification
  - Task of carrier, who initiates the platoon: where platoon to form, wait, start
- Platoon management
  - Carrier proposes new platoon
    - PSP allocates a platoon identifier = PlatoonID
    - Carrier suggests the location for platoon creation / rendezvous
    - PSP stores all platoon details in a platoon database (managed by the PSP)
  - Vehicle position in the platoon
    - no involvement of PSP
    - out of scope of interface description
- Platoon impact by road authorities / route management
  - PSP validates platoon route via road authorities
  - PSP requests (static) platoon limitations along the route from RA broker
    - PSP stores those limitations in the platoon database
    - On request, the PSP provides the limitations to the client
  - Comment: This feature gets importance in case the vehicle platoon is an L4 AD platoon, whereby this is not specifically in the scope of ENSEMBLE.
- Platoon monitoring
  - After the definition of a new platoon, the platoon status will be monitored by the PSP
    - Which vehicles belong to the platoon (via VehicleID)
  - Possible client request about platoon status to the PSP
    - Which vehicles already belong to the platoon (VehicleID)
  - Monitoring ends after disengagement of the platoon

The API definition can be split into 3 tasks

- Platoon Management
- Vehicle Management
- Carrier Management

These are described forthwith:

Table V. Functions related to the platoon management between PSP and carrier.

Function	Description
Create Platoon	PSP creates on request of the carrier a new platoon entry in the platoon DB, checks optionally limitations with road authorities, creates an identifier (PlatoonID), allocates an owner (CarrierID), stores the suggested start location, destination, start time, earliest time to join the platoon, etc. *Input parameters:* CarrierID VehicleID Rendezvous location Platoon destination Platoon Route Platoon Start time Platoon Start time agility *Return parameters:* Status (ok) Value: 200 PlatoonID Platoon Route confirmation Remark: complete Platoon tuple will be returned Status (Nok) value: 405 (invalid input data)
Change Platoon	The owner of the PlatoonID has the right to change platoon parameters of an existing platoon; this might affect any parameter; it might be done at any time of the existence of the platoon (with all inconveniences to the other platoon participants); this can only be done by the platoon owner! *Input parameters:* PlatoonID Lead CarrierID Rendezvous location Platoon destination Platoon Route Platoon Start time Platoon Start time agility *Return parameters:* Status (ok) Value: 200 PlatoonID, Lead CarrierID Rendezvous location Platoon destination Platoon Route Platoon Start time Platoon Start time agility Number of registered vehicles for this PlatoonID Status Nok values: 400: wrong PlatoonID 405: wrong content

Request Platoon List	Provides an overview about existing platoons, which fit to the filter criteria; it also clarifies which carrier is the platoon owner and the level of platoon completion (currently 1, 2, or 3); Remark: in case the PlatoonID is set as input parameter, the Return list includes a dedicated Tuple related to the PlatoonID *Input parameters:* Platoon tuple with filtering criteria, like Intended destination Intended start time Intended start time agility *Return parameters:* Status (ok) List of Platoon tuples fitting the search criteria: PlatoonID, Lead CarrierID Rendezvous location Platoon destination Platoon Route Platoon Start time Platoon Start time agility VehicleIDs Status (Nok): 405: wrong content
Delete Platoon	Allowed for platoon owner only Only as long as no vehicles are allocated to the platoon *Input parameters:* PlatoonID Own CarrierID *Return parameters:* Status (ok): 200 Status (nok): 400 – wrong input parameter
Add Vehicle to Platoon	PSP adds a new vehicle to an existing platoon, PS validates the input data (e.g. that the VehicleID is not yet part of the platoon – no double counting) and checks the status of the platoon. *Input parameters:* PlatoonID Carrier ID Vehicle ID *Return parameters:* Status (ok): 200 Status (nok): 400 – wrong PlatoonID 405 – wrong Input data
Request Platoon Vehicle List	Find all vehicle data already registered for a platoon *Input parameters:* PlatoonID

	Return parameters: Status (ok): 200 List of (PlatoonID, CarrierID, VehicleID) Status (Nok): 400: invalid PlatoonID
Delete Vehicle from Platoon	Allows each platoon participant to delete its vehicle from the platoon *Input parameters:* PlatoonID Own Carrier ID Vehicle ID *Return parameters:* Status (ok): 200 Status (nok): 400: wrong PlatoonID 405: wrong input data

Table W. Functions related to vehicle management between PSP and carrier.

Function	Description
Register Vehicle	Register in the vehicle DB the vehicle from a specific Carrier for matching service; VIN, OEM, vehicle specific data; only registered vehicles are allowed to join platoons. *Input parameters:* CarrierID Vehicle specific data (VIN, etc.) *Return parameters:* Status (ok): 200, VehicleID Status (Nok): 405: invalid Input data
Modify Vehicle Data	Modify parameters of a registered vehicle in the vehicle DB; Remark: the VehicleID cannot be modified *Input parameters:* *CarrierID* VehicleID Vehicle specific data *Return parameters:* Status (ok): 200 Status (nok): 400: invalid VehicleID 405: invalid Input Data
Check Vehicle Data	Find all vehicle data already registered in vehicle DB and fit to the filter

	Remark: one specific vehicle can be checked by putting the VehicleID in the filter criteria *Input parameters:* Vehicle filter criteria data *Return parameters:* Status (ok): 200 List of tuples of vehicle items which match to the filter criteria Status (nok): 405: invalid input data
Delete Vehicle	Delete vehicle from the vehicle database; the PSP first checks the current participation of this vehicle in a platoon; in this case the vehicle will not be deleted from the vehicle DB. *Input parameters:* CarrierID VehicleID *Return parameters:* Status (ok): 200 Status (Nok): 400: invalid VehicleID

Table X. Functions related to carrier management between PSP and carrier.

Function	Description
Register Carrier	Register in the Carrier DB the Carrier; Carrier specific data; only registered carriers are allowed to work with their vehicles and the platoons. *Input parameters:* Carrier specific data *Return parameters:* Status (ok): 200 CarrierID CarrierSpecificData Status (nok): 405: invalid input
Modify Carrier Data	Modify parameters of a registered carrier in the Carrier DB; Remark: the CarrierID cannot be modified *Input parameters:* CarrierID Carrier specific data (tbd) *Return parameters:* Status (ok): 200 Status (nok): 400: wrong CarrierID

	405: wrong input data
Check Carrier Data	Find all carrier data already registered in carrier DB and fit to the filter *Input parameters:* Carrier filter criteria data *Return parameters:* Status (ok): 200 List of tuples of carrier items which match to the filter criteria Status (nok): *405: invalid input data*
Delete Carrier	Delete carrier from the carrier database; the PSP checks first the current participation of the carrier's vehicles in the vehicle database; in this case the carrier will not be deleted from the carrier DB. *Input parameters:* CarrierID *Return parameters:* Status (ok): 200 Status (nok): 400: invalid CarrierID
Login Carrier	Carrier logs in into PSP *Input parameters:* CarrierID Password *Return parameters:* Status (ok): 200 Status (nok): 400
Logout Carrier	Carrier logs out from PSP

API between PSP and road authority (RA) broker

The following assumption have been made:

- RA permission for platooning is optional
    - Valid since it assumed a platoon does not violate the current legal framework
- RA permission is mandatory in all other cases
- RA information via broker due to
    - Missing standards of regional road authorities
    - Opportunity to propose a defacto standard for RA information
- RA information are informal, currently no QoS parameter integrated
    - Platoon can use the RA information
    - RA should provide 2 types of data

- Planning data, to be provided prior to the platoon journey starts → essential for platoon route planning
- Dynamic data, to be provided during the journey → out of scope of current deliverable

The API definition can be broken down into 2 tasks:

- RA Info
- PSP Management

These are described forthwith.

Table Y. Functions related to the requests of road authority information by the PSP.

Function	Description
Request RA INFO	PSP asks for info for a platoon through (several) RA's; PSP creates tuple (Route, Set of RA's) RA broker clarifies request with all regional RA's (API spec out of scope) RA broker collects all response information and provides a response to the PSP; In case the suggested route is not confirmed by the RA broker, the PSP is in charge to search for alternative routes No need for platoon identification for the RA broker / RA ----------------------------------- Input: route (route,), expected time window, option: planned rests Output: ok, nok, limitations (limits) Output limits: reason (e.g. time/location/reason of restrictions), geo reference if applicable

PSP MANAGEMENT

Remark: All PSPs should be known and validated by the RA broker prior to providing RA information to the PSP

Table Z. List of functions related to the PSP management, i.e., creation, deletion and authentication of PSPs.

Function	Description
Create PSP	Register PSP in RA Broker
Delete PSP	Delete PSP from RA Broker
Login PSP	PSP logs in into RA Broker
Logout PSP	PSP logs out from RA Broker
Change PSP	Change PSP data in RA Broker
Check PSP	Read currently stored PSP data from RA Broker

API between PSP and OEM

The following assumption have been made:

- OEM has no right to manage platoons
- OEM has only the right to get information about the vehicles which have been produced by the OEM
- Therefore, the OEM must register
- The OEM can find his vehicle in the Vehicle DB (via the VIN)
- The OEM can find the CarrierID via the Carrier DB
- The function described above will be combined into one interface function
- The OEM can afterwards apply the “Request Platoon Status” function for the purpose to get an overview of the platoon(s) where the OE produced Vehicle is part of.
- The Platoon Management functions are a specific subset of the Platoon Management functions between PSP and carrier (read only functions)
- Purpose of that feature: the appropriate platoon info can be partially displayed at the vehicle’s display

The API definition can be broken down into 3 tasks:

- Vehicle Management
- OE Management
- Platoon Management

These are described forthwith.

Table AA. Functions related to vehicle management between PSP and OEM.

Function	Description
Search OE Vehicle	Validate the availability of a dedicated vehicle in the PSP database(s) *Input parameters:* VIN OEID *Return parameters:* Status (ok, nok) CarrierID VehicleID Nok values: Tbd

Table BB. Functions related to the OE management for the communication between PSP and OEM.

Function	Description

Create OE	Register in the COE DB the OE; OE specific data; only registered OEs are allowed to work with their vehicles and the platoons. Remark: for the time being all those data are not really used; purpose: security checks. *Input parameters:* OE specific data *Return parameters:* Status (ok, nok) OEID Nok values: Tbd
Delete OE	Delete OE from the OE database; *Input parameters:* OEID *Return parameters:* Status (ok, nok) OEID Nok values: Tbd
Login OE	OE logs in into PSP
Logout OE	OE logs out from PSP
Check OE	Check parameters of a registered OE in the OE DB; *Input parameters:* OEID *Return parameters:* Status (ok, nok) OEID OE specific data (tbd) Nok values: Tbd
Modify OE	Modify parameters of a registered OE in the OE DB; Remark: the OE ID cannot be modified *Input parameters:* OEID OE specific data (tbd) *Return parameters:* Status (ok, nok) OEID Nok values: Tbd

Table CC. Functions related to the platoon management.

Function	**Description**
Search Vehicle in Platoons	Search vehicle over all platoons (might be in several platoons); return list of platoon IDs

	Input parameters: CarrierID VehicleID *Return parameters:* Status (ok, nok) List of (PlatoonID, CarrierID, VehicleID) Nok values: Tbd
Request Platoon status	Provides an overview about a dedicated platoon, which the VehicleID is registered for; helps to monitor potential parameter changes of the platoon *Input parameters:* CarrierID PlatoonID *Return parameters:* Status (ok, nok) PlatoonID, Lead CarrierID Rendezvous location Platoon destination Platoon Route Platoon Start time Platoon Start time agility Number of registered vehicles for this PlatoonID Nok values: Tbd

6.3. Implementation of the platooning algorithm

The implementation of algorithm described in section 3.4.4 and Figure 13, i.e., the main engine for the platooning algorithm, is shown in this section. Figure 30 shows the pseudocode of such implementation for a given arbitrary time t'. The process is repeated for different values of t'. Naturally, the selection of t' affects the results. In practice, such t' is chosen such that the number of active vehicles is maximized, which it is still a suboptimal choice. The problem of finding the optimal solution is believed to be NP-hard.

```
for t'
    If more than one vehicle on the network
        If more than one active vehicle
            All active vehicles: S
            For each vehicle s in S
                For each vehicle i in S \ s
                    If distance(s,i) < D
                        S and i are platoon candidates
```

Figure 30. Pseudocode of the platooning algorithm described on section 3.4.4.