Tele-Operated Driving (ToD): Business Considerations

5GAA Automotive Association

Technical Report

CONTACT INFORMATION:
Executive Manager – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:
5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	1.0
DATE OF PUBLICATION:	12 July 2021
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	No
DATE OF APPROVAL BY 5GAA BOARD:	30 June 2021

Contents

Foreword

This Technical Report has been produced by 5GAA.

The contents of the present document are subject to continuing work within the Working Groups (WG) and may change following formal WG approval. Should the WG modify the contents of the present document, it will be re-released by the WG with an identifying change of the consistent numbering that all WG meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

(1) This numbering system has six logical elements:

(a) x: a single letter corresponding to the working group:

where x =

T (Use cases and Technical Requirements)

A (System Architecture and Solution Development)

P (Evaluation, Testbed and Pilots)

S (Standards and Spectrum)

B (Business Models and Go-To-Market Strategies)

(b) nn: two digits to indicate the year. i.e. ,17,18 19, etc

(c) zzzz: unique number of the document

(2) No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version

(3) The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

Introduction

The 5GAA cross-working group work item Tele-operated Driving (ToD) aims to describe the requirements and framework needed for remote vehicle operation. The proposed results should reliably enable remote steering and manoeuvring including a human remote driver with both Direct and Indirect Control in an OEM-agnostic, inter-MNO and cross-authority operation. The intention of this work item is to study both use case and scenario definition, technical design, and business considerations. This document focuses on business considerations.

It does not pretend to provide an exhaustive analysis of all possible challenges and solutions regarding business models, governance challenges or go-to-market constraints. But it does aspire to identify the different elements that should be taken into account when considering the deployment of a ToD ecosystem from a business perspective.

Further, the document provides valuable first insights enabling stakeholders with a keen interest in realising and deploying ToD products to commence with their own business and governance modelling in this context, thanks to the background information on technical and safety requirements.

This Technical Report was designed to analyse the practical business aspects, in particular market constraints, concerning the implementation of the various ToD models. As noted, it contains “considerations” or “first thoughts” on the business issues that companies active in the space might face when they present themselves to the market. There is no intention to recommend any business strategies or request adherence to any business terms – it is simply an academic exercise to explore possible business issues, and to advance debate and reflection on those issues.

This exercise relies on the general market expertise of the contributors, but is not the result of any sharing or pooling of confidential or business-sensitive information. The individual strategies and business secrets of contributors remain their own.

1 Scope

The present document is the third deliverable of XW5 Tele-operated Driving (ToD). This deliverable addresses Task 3 of the ToD XWI [1] by analysing business-related topics. This includes initial stakeholder identification, detailing of potential operational processes, identification of potential go-to-market constraints, and theoretical/abstract business modelling. These analyses are based on the prioritised use cases and scenarios from deliverable D1.1 [2], and take the output of deliverable D1.2 [3] on requirements analysis and communication architecture into account.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 5GAA XW5-190009, Work Item Description, Tele-operated Driving , July 2019.

[2] 5GAA XW5-200029, Cross Working Group Work Item; Tele-operated Driving (ToD); D1 Use Cases and Technical Requirements, July 2020, https://5gaa.org/news/tele-operated-driving-tod-use-cases-and-technical-requirements/

[3] 5GAA XW5-200025, Cross Working Group Work Item; Tele-operated Driving (ToD); D2 Requirements Analysis and Communication Architecture, January 2021. Draft version 0.8, not yet available publicly for download.

[4] 5GAA XW4-210009, Cross Working Group Work Item; Safety Treatment in Connected and Automated Driving Functions (STiCAD); Technical Report, July 2021, http://5gaa.org/wp-content/uploads/2021/07/5GAA_T-210009_STiCAD-TRv1.0_Final.pdf

[5] 5GAA, Working Group 5, Business Models and Go-To-Market Strategies, Business Aspects and Requirements of 5G Network Slicing (BARNS) Report, November 2020, https://5gaa.org/news/business-aspects-and-requirements-of-5g-network-slicing-barns-report/

[6] 5GAA TR A-200094, V2X Application Reference Architecture, June 2020, https://5gaa.org/news/v2x-application-layer-reference-architecture/

[7] 5GAA Working Group 1; TR Use Cases and Service Level Requirements Volume II, January 2021, https://5gaa.org/wp-content/uploads/2021/01/5GAA_T-200116_TR_C-V2X_Use_Cases_and_Service_Level_Requirements_Vol_II_V2.1.pdf

[8] 5GAA Working Group 5, Cross Working Group Item NetExp; White Paper MNO Network Expansion Mechanisms to Fulfil Connected Vehicle Requirements; https://5gaa.org/wp-content/uploads/2020/06/5GAA_B-200044_WI-NetExp-White-Paper.pdf

[9] SAE J3016_202104, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

- **Non-ToD**: the ToD operator is not engaged in the act of driving, i.e. taking no role in the act of driving. All three levels of driving operations, i.e. Strategic level, Tactical level, and Real-Time Operational and Real-time Tactical level are performed by an in-vehicle user [9] or system.
  - Note 1: 'system' in this definition refer to 'driving automation system' defined in [9].
  - Note 2: in this case the ToD operator may monitor the status of the vehicle and send information to the in-vehicle user or system supporting the act of driving.
- **Dispatch ToD**: the ToD operator takes on the role of **Dispatcher**, which is only to perform the Strategic level operations of driving, e.g. travel planning, route and itinerary selection, while the Tactical and Operational level operations are performed by the in-vehicle user or system.
  - Note 3: For driving automation systems, this type of ToD corresponds to the dispatch [in driverless operation] function defined in [9].
- **Indirect Control ToD**: the ToD operator takes the role of **Indirect Controller** (**Remote Assistant**), to perform the Tactical level functions like pathway planning, which corresponds to the remote assistance function defined in [9] for driving automation systems. If needed, the Indirect Controller may also perform Strategic level operations of driving. In Indirect Control ToD, real-time Operational level and real-time Tactical level functions, i.e. Dynamic Driving Task (DDT) [9], are performed by in-vehicle user or system.
  - Note 4: When engaged in the act of driving, the remote operator of Indirect Control ToD may disengage the in-vehicle system from performing DDT, by either taking over the all DDT tasks, i.e., the role of Direct Controller, or by bringing the vehicle to a minimal risk condition [9].
  - Note 5: When Indirect Control ToD is engaged, the ToD operator may also perform Strategic level operation such as reselecting the route, when such operations are needed to complete the act of driving, e.g. to avoid a blocked road.
- **Direct Control ToD**: the ToD operator takes the role of **Direct Controller** (**Remote Driver)**, to perform all or part of real-time operational and real-time tactical functions (i.e. DDT), which corresponds to the remote driving function defined in [9] for driving automation systems. If needed, the Direct Controller may also perform Tactical and Strategic level operations of driving.
  - Note 6: When Direct Control ToD is engaged, part of the DDT functions, e.g. lateral and/or longitudinal vehicle motion control, may be performed by the In-vehicle user or system, e.g. through adaptive cruise control and/or lane keeping, while the ToD operator (Direct Controller) is still responsible for the OEDR task.
  - Note 7: When Direct Control ToD is engaged, the ToD operator (Direct Controller) may also perform Strategic level operations such as reselecting the route and Tactical level operations such as replanning the pathway, when such operations are needed to complete the act of driving, e.g. to avoid a blocked road or get around an obstacle in the road.

Note 8: The Remote Vehicle (RV) operator can be a remote user [8] or a remote system.

This distinction between ToD types is summarised in Table 1.

Table 1: The role and engagement of the ToD operator in the act of driving in different types of ToD

ToD Type (Role of ToD operator)	**Act of Driving**		
	Strategic Operation (Travel planning, route and itinerary selection)	Tactical operation (Pathway planning)	Real-time Operational and Real Time Tactical Functions (DDT incl. OEDR and sustained lateral and longitudinal vehicle motion control)
Non-ToD (No Role)	In-vehicle user or system	In-vehicle user or system	In-vehicle user or system
Dispatch ToD (Dispatcher)	ToD operator	In-vehicle user or system	In-vehicle user or system
Indirect Control ToD (Indirect Controller or Remote Assistant)	ToD operator (if needed)	ToD operator	In-vehicle user or system

Direct Control ToD (Direct Controller or Remote Driver)	ToD operator (if needed)	ToD operator (if needed)	ToD operator (all or part of DDT)

3.2 Symbols

For the purposes of the present document, no symbols apply.

3.3 Abbreviations

For the purposes of the present document, the following acronyms and abbreviations apply:

ADAS Advanced Driver Assistance Systems

ALKS Automated Lane Keeping Systems

App Application

AS Application Server

ASIL Automotive Safety Integrity Level

AV Automated Vehicle

CA Certificate Authority

CC Control Centre

CCU Connectivity Control Unit

CV Controlled Vehicle

C-V2X Cellular V2X

FC Fault Category

HMI Human-Machine Interface

HV Host Vehicle

ISP Internet Service Provider

ITS Intelligent Transport Systems

LoA Level of Automation

Mbps Megabits per second

MEC Multi-access Edge Computing

MNO Mobile Network Operator

NRI Network Reselection Improvements

NW Network

OEM Original Equipment Manufacturer

ODD Operational Design Domain

PFSR Potential Functional Safety Requirements

QoS	Quality of Service
RTA	Road Traffic Authority
RTTI	Real-Time Traffic Information
SG	Safety Goal
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SP	Service Provider
SRTI	Safety-Related Traffic Information
STiCAD	Safety Treatment in Connected and Automated Driving
ToD	Tele-operated Driving
TSP	Transportation Service Provider
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything
VMS	Variable Message Signs
XWI	Cross-Work Item

4 ToD use cases and scenarios from Task 1

The deliverable produced by Task 1 within this 5GAA ToD cross-work item [2] reported the analysis, extension and classification of a set of Tele-operated Driving use cases[1]. This was done with the aim of providing a shortlist, which can serve as a basis for further activities related to technical requirement derivations and business considerations. A survey of public source (or other non-confidential) information on the state of the art was performed, analysing existing (pre-) commercial solutions and highlighting major outcomes and guidelines as useful input to shape and guide ToD developments. A review of public sources revealing the main achievements of previous and ongoing R&D projects in the automotive domain was also carried out with the same purpose. The survey ended with the lessons learned and recommendations.

Afterwards, use cases and corresponding scenarios were specified and analysed. ToD use cases from 5GAA Working Group 1 were taken as initial input and extended in the scope of multi-OEM, multi-MNO, and multi-RTA scenarios. Additional service operation scenarios were also considered, taking realistic and operational situations into account. For each use case, the deliverable provided its rationale, an overall description, and the related information flows. The outcome of this work was a subset of scenarios meant to be taken as the basis for further ToD XWI activities. They will therefore be used as the starting point of this deliverable regarding ToD business considerations. These are summarised in Table 2. More details and examples are given in [2].

Table 2: Summary of ToD use cases selected for further study by Task 1

Scenario ID	Description	Proposed Scenarios
T-180205 Tele-operated Driving	The goal of this use case is to enable a ToD operator (human or machine) to remotely drive a Host Vehicle. The HV needs to receive and apply	ToD with ‘Remote Driving Paths’ (ToD Type “Indirect Control"): The service is provided by one ToD

[1] *Continuing the first thoughts on ToD written down by 5GAA in the Technical Report ‘C-V2X Use Cases and Service Level Requirements Volume II’ [7]*

Scenario ID	Description	Proposed Scenarios
	the driving instructions sent by the ToD operator. The HV provides the environmental information and data to enable remote driving functionality.	provider to a single OEM fleet owner. The area of operation is confined. ToD with 'Remote Steering' (ToD Type "Direct Control"): Remote driving service from one ToD provider to a single OEM fleet: • From a certain port to the destination city • From an area outside the city centre, for example the airport to the city centre (car sharing)
T-180206 Tele-operated Driving Support	The goal of this use case is to remotely support the tasks of a vehicle with automated capabilities (e.g. by providing a driving manoeuvre) for a short period of time, when the vehicle faces highly uncertain situations rendering decision-making difficult. The difference between this use case and the ToD use case (described above), is that a Remote Driving service is needed in this case for a limited period of time.	ToD with 'Remote Driving Paths' (ToD Type "Indirect Control"): Single ToD provider sending manoeuvre instructions and the trajectory to the vehicle fleet of a single OEM, in a confined area (green zone) or following a pre-determined route: • If mandated by regulation (geo-fenced areas) • When commandeered by authorities • In emergency situations ToD with 'Remote Steering' (ToD Type "Direct Control"): Remote driving support from a single ToD provider to fleet vehicles in a confined area (green zone) or following a pre-determined route: • If mandated by regulation (e.g., geo-fenced areas) • When commandeered by authorities • In emergency situations
T-180207 Tele-operated Driving for Automated Parking	The goal of this use case is to execute automated parking of vehicles using ToD services. A remote entity, either human or machine, provides the appropriate path and manoeuvre instructions to the vehicle for efficient and safe parking.	ToD for Automated Park with 'Remote Driving Paths' (ToD Type "Indirect Control") for a vehicle fleet from a single car OEM in constrained/confined areas (e.g. automotive OEM factories). ToD for Automated Park with 'Remote Driving Paths' (ToD Type "Indirect Control") for a fleet of vehicles from multiple car OEMs *using communication services from different mobile network operators* in constrained/confined areas (e.g. garages or seaports). ToD for Automated Park with 'Remote Steering' (ToD Type "Direct Control") for a vehicle fleet from a single car OEM in constrained/confined areas (e.g. automotive OEM factories), allowing

Scenario ID	Description	Proposed Scenarios
		only authorised staff to enter, such as trained workers. ToD for Automated Park with 'Remote Steering' (ToD Type "Direct Control") for a fleet of vehicles from a legacy fleet provider of multiple car OEMs in constrained/confined areas (e.g. garages or seaports).
T-190062 Infrastructure-based Tele-operated Driving	The goal of this use case is to remotely support the tasks of a vehicle with automated capabilities (e.g. by providing a driving manoeuvre) for a short period of time, when the vehicle's own sensory or computational capabilities are failing, uncertain or the on-board sensor coverage is not sufficient. The difference in this use case, compared to the use case described with a human operator, is that the remote support relies mainly on environment perception provided by sensors outside the vehicle, which for availability reasons are fixed sensors under direct control of the infrastructure. These infrastructure-based sensors are the tele-operator's primary information source, capable of producing a temporal and locally complete picture of the environment in real time. This type of infrastructure support is envisioned primarily for vehicles that drive on pre-defined routes such as shuttle or bus services.	Infrastructure-based ToD (remote operator is human): • In public areas or special zones such as harbours, airports, or factory grounds • Provided by a remote operator associated with the road section or zone • Support vehicles from different automotive OEMs • Use a single MNO network Infrastructure-based ToD (remote operator is machine): • In public areas or special zones such as harbours, airports, or factory grounds • Provided by remote operator associated with the road section or zone • Support vehicles from different automotive OEMs • Use a single MNO network

In addition to proposing a subset of scenarios to be taken as a basis for further ToD XWI activities, [2] also identified some preliminary business requirements/considerations for these scenarios. As valuable input for this deliverable, they are summarised in Table 3, and more details are given in [2].

Table 3: Summary of preliminary business requirements/considerations identified by Task 1

Scenario ID	Considerations
T-180205 Tele-operated Driving	• To the extent that the TOD service is discretionary and requested on different occasions, it could be interpreted as a premium service. • Incorporation of tele-operation capabilities in the vehicle by the OEM is a necessary ingredient for service delivery. • It is up to the commercial policy of the OEM to factor the service into the price of the vehicle or sell it as an add-on. • Depending on who owns the vehicle, the pricing scheme and the service package will differ. This can include 'fair use' policy when the price of ToD is factored into the vehicle's price, or different potential offerings (passes, pay-as-you-go, recurring subscriptions, hybrid plans) in the event ToD is presented as an add-on. • The party that acts as the ToD service owner is likely to be the OEM, regardless of whether the actual service delivery has been outsourced to a specialised third-party company. • If the owner of the vehicle is a fleet operator, then they could bear the cost of the service. In that case, the ToD service could be arranged, for example, through a bulk

Scenario ID	Considerations
	multi-year agreement e.g. offering 1000 hours of tele-operation per month to a 1000-vehicle fleet in a ‘shared pool’ fashion for three years. • ToD might be just one of the various services offered by an OEM to the fleet operator. In such cases, the price could be part of a package deal, covering the vehicles and a basket of ancillary services, such as ToD. • The cost of cellular communications used in the ToD service delivery could burden the ToD service provider. Therefore, they may wish to cut an enterprise connectivity deal with an MNO. • It is likely that the services delivered by humans could be pricier.
T-180206 Tele-operated Driving Support	• To the extent that the ToD service is discretionary and is requested in different emergency situations, it could be priced as a premium service. • The fleet operator could be the party that pays the ToD service provider, and the price could be set through a wholesale agreement that covers the entire vehicle fleet. • One way to cost it could be to set a price per minute, whereby the fleet operator buys x thousands of minutes at a bulk price for a number of years to serve any and all vehicles in their fleet. • The price could vary depending on whether the ToD service provider offers Direct or Indirect Control of the vehicles. The Direct Control service might be priced higher. • Communication expenses for the support of the ToD service on the vehicle side could be borne by fleet operators, through a wholesale agreement with an MNO.

T-180207 Tele-operated Driving for Automated Parking	• Regarding business model considerations, the analysis carried out above applies to these use cases too. Of course, in particular cases there may be variations, as follows:
	    ○ If the confined area is the OEM’s factory, then it is likely that the OEM can perform the remote driving task itself, in which case there might be no monetary exchange with a ToD service provider.
	    ○ If the confined area is a port, then it is likely that the ToD service will be offered by an entity performing additional port operational tasks. In this case, the price of the ToD task could be absorbed in a bundled service package offered to the fleet operator.

T-190062 Infrastructure-based Tele-operated Driving	• The following differences regarding business model considerations can be identified when adding infrastructure-assistance to ToD:
	    ○ The road operator offering the infrastructure could apply an extra charge to cover its service, to be borne by the fleet operator.
	    ○ This charge may differ depending on whether the ToD driving is carried out by a machine or a human.
	    ○ To the extent that the ‘coupling’ of vehicle and infrastructure is mandatory when the vehicle is entering the infrastructure-equipped stretch of the highway, the charge for the coupling itself could be perceived as an extra ‘toll/flat fee payment’ covering the whole fleet for a long period of time.
	    ○ If and when there is a need for the actual ToD service delivery there could be a separate charge issued to the fleet operator covering the premium remote driving service, most likely on a per-minute basis (possibly covered by a bulk agreement).

5 ToD requirements and architecture from Task 2

Starting from the ToD use cases and scenarios introduced in the previous chapter, Task 2 of the 5GAA ToD cross-work item has defined a deployment view of the ToD application layer architecture [3]. It illustrates the functional components and reference points from the 5GAA V2X application layer reference architecture [6] that are required for the deployment of ToD services in different scenarios. The deployment views also illustrate the role of stakeholders in the deployment, making it valuable input for business considerations. This deployment view of the ToD application layer architecture is depicted in Figure 1.

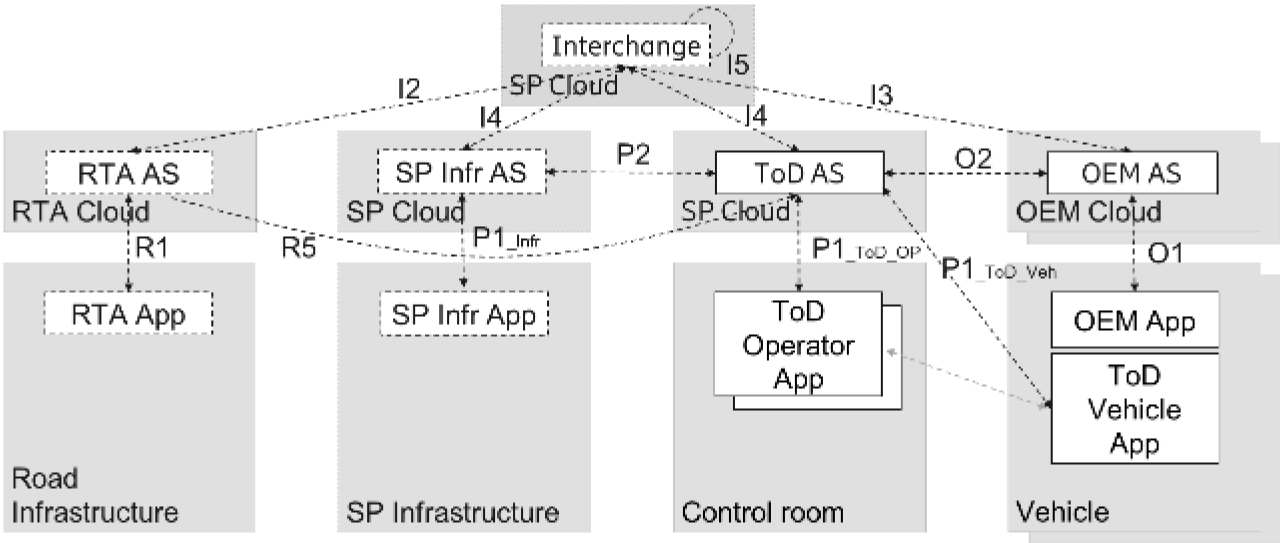


Figure 1: Deployment view of application layer architecture for ToD

The interfaces (e.g. P1, P2, R1) have been defined in 5GAA Tele-operated Driving (ToD); D2 Requirements Analysis and Communication Architecture [3].

The following components and stakeholder roles can be identified:

Table 4: ToD application layer architecture components and stakeholders

Component Acronym	Component Long Name	Component Function	Component Deployed By
ToD AS	ToD Application Server	Enables secure communication between trusted ToD Operator App and ToD Vehicle App that is controlled by the OEM AS in the cloud and OEM APP on the vehicle. It manages registration and authentication requests from ToD Operator Apps and from ToD Vehicle Apps. It handles ToD service requests from either a ToD Operator App or a ToD Vehicle App.	ToD Service Provider
ToD Operator App	ToD Operator Application	Provides ToD Operator functionalities in ToD services. Functionalities include receiving information and data from ToD Vehicle App, RTA AS, and/or SP Inf AS, helping the ToD Operator to	ToD Service Provider using technologies provided by a ToD technology provider

Component Acronym	Component Long Name	Component Function	Component Deployed By
		build environmental perception, performing the driving tasks, transmitting commands to the ToD Vehicle App, etc.	
OEM AS	Original Equipment Manufacturer Application Server	The trust anchor for all vehicles comes from this automotive OEM. The OEM AS communicates with OEM App and is responsible for secure and trusted remote access from or to vehicles.	Car OEM
OEM App	Original Equipment Manufacturer Application	The OEM App integrates services offered by the OEM AS into vehicles. For ToD services, the OEM App communicates with OEM AS and is responsible for secure and trusted remote access from or to vehicles.	Car OEM
ToD Vehicle App	ToD Vehicle Application	The ToD Vehicle App provides all functionalities and software/hardware components on a vehicle for ToD operation with a ToD Operator App. Functionalities include detecting abnormal events and requesting ToD support, collecting and sending sensor and camera data to ToD Operator App, receiving and executing commands from ToD Operator App, etc.	Car OEM using technologies provided by a ToD technology provider
RTA AS	Road Traffic Authority Application Server	The RTA AS offers traffic efficiency and traffic safety information to ToD Operator Apps via the ToD AS. Furthermore, RTA AS manages road infrastructure, such as variable road signs, traffic lights and video surveillance cameras. Note: RTA AS is an optional component and only present in the architecture when information from the RTA is required by the ToD use case.	Road Traffic Authority
RTA App	Road Traffic Authority Application	The RTA App integrates the services offered by the RTA AS into the road infrastructure. Note: RTA APP is an optional component and only present in the architecture when information from the RTA is required by the ToD use case.	Road Traffic Authority
SP Infr AS	Service Provider Infrastructure Application Server	The SP Infr AS offers infrastructure management and monitoring capabilities to the Service Provider infrastructure application for the deployment of the ToD Application. Note: SP Infr AS is an optional component and only present in the architecture when information from the	Infrastructure Service Provider

Component Acronym	Component Long Name	Component Function	Component Deployed By
		service provider infrastructure is required by the ToD use case.	
SP Infr App	Service Provider infrastructure Application	The Infr AS is supported by the Service Provider Infrastructure Application Server and will be used for operators to monitor and control the deployment of the ToD Applications. Note: SP Infr App is an optional component and only present in the architecture when information from the service provider infrastructure is required by the ToD use case.	Infrastructure Service Provider
Interchange	Interchange Function	Given the large number of different RTA and SP infrastructures in the world, Interchange Functions are needed to scale up and secure the message exchanges between RTA ASs, OEM ASs and SP ASs. Note: Interchange is an optional component and only present in the architecture when scalability becomes a challenge to data exchange among ITS back-end systems for ToD services.	Service Provider, Mobile Network Operator, or Road Traffic Authority

6 ToD functional safety requirements from STiCAD

The 5GAA cross-work item ‘Safety Treatment in Connected Automated Driving Functions’ (STiCAD) investigated two different use cases from a functional safety point of view: Tele-operated Driving and Emergency Brake Warning. The ToD-related results are a valuable input for this deliverable regarding ToD business considerations. They are therefore summarised in this section.

In that work, both the Direct Control and the Indirect Control approach towards ToD were investigated. For safety considerations within a certain function, it is important to define the so-called Operational Design Domain (ODD). The ODD describes conditions and constraints under which the considered function is designed to work in a safe manner. The ODD considers different types or classes of defined conditions, limitations and circumstances (e.g. on which type of road the function will be allowed to work or under which weather conditions it might be used). As part of the safety concept, the underlying system providing the function needs to be able to safely detect, at any time, whether the conditions defining the ODD are met or not. If conditions are met, the function is allowed to be active, and vice versa. If the system leaves the ODD while active, the respective actions defined in the safety concept (e.g. safe stop or function degradation) need to be safely performed. In [4], the ODD for ToD has been described in detail.

In addition to the ODD definition, it was also important to identify the different elements to be included in the ToD solution before requirements regarding functional safety could be identified by STiCAD. These were also identified and described in [4].

Based on those insights in ODD with ISO26262 elements included, the following safety goals were defined by STiCAD:

Table 5: Safety goals for ToD

Hazardous Event and Associated Risk	**Safety Goal**	**Possible Impact Scenarios of the Hazardous Event**	**Related ASIL Rating**
CV (Controlled Vehicle) causes an accident by receiving wrong or late information from CC (Control Centre) and thus causes a severe accident	**SG1:** Avoid wrong control information being received by the CV **SG2:** Avoid late control information being received by the CV	• If vehicle autonomous sensors are still functional, the validity of the control information could be checked through the separate sensor data and therefore accidents due to wrong control information can be avoided • If vehicle autonomous sensors are no longer functional or degraded (e.g. because CC commands put vehicle in non-ODD)	QM ASIL D
CV becomes an obstacle to other vehicles which might cause accidents	**SG1:** Avoid wrong control information being received by the CV **SG2:** Avoid late control information being received by the CV	• Drivers of other vehicles are still capable of avoiding crashes, as in normal traffic situations; hard brakes can be avoided due to still functioning CV vehicle autonomous sensors • The reaction of the CV is unforeseeable by other traffic participants and thus normal reaction times cannot avoid accidents	QM to ASIL B ASIL B to ASIL D
CV causes an accident because the operator at CC gets wrong sensor information and thus provides wrong information to the vehicle or performs dangerous driving manoeuvres at the CV	**SG3:** Avoid wrong sensor information being received by the CC **SG4:** Avoid late information being received by the CC	• If vehicle autonomous sensors are still functional the validity of the received information could be checked and therefore accidents due to wrong received information can be avoided • If autonomous sensors of the vehicle are no longer functional or degraded (e.g. because CC commands put vehicle in non-ODD)	QM ASIL D
CV becomes an obstacle to other vehicles which might cause accidents due to wrong commands generated by the CC or late reaction to such commands	**SG3:** Avoid wrong information being received by the CC **SG4:** Avoid late information being received by the CC	• Drivers of other vehicles are still capable of avoiding crashes, as in normal traffic situations; hard brakes can be avoided due to still functioning CV vehicle autonomous sensors • The reaction of the CV is unforeseeable by other traffic participants and thus normal reaction times cannot avoid accidents	QM to ASIL B ASIL B to ASIL D

Based on these safety goals, the following major requirements for ToD regarding functional safety were derived:

Table 6: Safety requirements for ToD

Fault location	Fault Category (FC)	Potential Functional Safety Requirements (PFSR)
CC	**FC1:** CC does not generate control messages when it should	<u>**Strategies for fault avoidance:**</u> • **PFSR-FC1-1** (Requirement on CC): CC shall implement a watchdog that assures regular control messages are not missing. • **PFSR-FC1-2** (Requirement on CC): A real-time supervision system shall be implemented at CC that takes care of regular message generation and transmission. <u>**Strategies for fault detection and mitigation:**</u> • **PFSR-FC1-3** (Requirement on CC): CC shall inform the operator about sent messages and provide a warning if message intervals reach or exceed a predefined maximum value. <u>**Strategies for fault detection and transition to safe state:**</u> • **PFSR-FC1-4** (Requirement on CV): CV shall monitor the time since last control message received and, if a certain threshold has been exceeded, either move to 'fail operational state' (e.g. reduce speed) or, in case another higher maximum value has been reached, enter 'safe stop' based on ego sensors.
CV	**FC5:** Control messages are correctly received by the CV but cannot be processed correctly by the application	<u>**Strategies for fault avoidance:**</u> • **PFSR-FC5-1** (Requirement on CC): CC and CV shall have the same set of semantic rules for the control messages. The CC shall assure that only semantically correct messages are generated and transmitted. <u>**Strategies for fault detection and mitigation:**</u> • **PFSR-*FC5-2*** (Requirement on CV): *Receiving CV should check the contents of all received correct messages (that all syntactical checks were successful) against semantic mistakes (e.g. non-performable manoeuvres) and shall ignore the semantically wrong messages.* <u>**Strategies for fault detection and transition to safe state:**</u> • ***PFSR-FC5-3*** *(Requirement on CV): If ignored messages are necessary for further operation (e.g. because of timing etc.) the CV should enter 'safe state' or 'degrade function'.*

NW	**FC3:** Messages correctly generated by CC are lost during transmission to the CV	**<u>Strategies for fault avoidance:</u>** • **PFSR-FC3-1** (Requirement on NW): NW shall provide means to guarantee high quality of service for the transmitted messages on the complete chain from CC output to CV input (CCU – CCU). • **PFSR-FC3-2** (Requirement on NW): NW shall provide means to predict Quality of Service (QoS) on the complete chain from CC output to CV input (CCU – CCU), and allow CC and CV to regularly be assigned the appropriate QoS. **<u>Strategies for fault detection and mitigation:</u>** • **PFSR-FC3-3** (Requirement on NW): NW shall provide means to safely detect connection loss or degradation on both CC and CV sides. • **PFSR-FC3-4** (Requirement on CC): CC shall continuously monitor communication state, using means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. stop generating control messages based on potentially outdated information). • **PFSR-FC3-5** (Requirement on CV): CV shall continuously monitor communication state, using means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. move to fail operational state or enter safe stop). **<u>Strategies for fault detection and transition to safe state:</u>** • **PFSR-FC3-6** (Requirement on CV): CV shall continuously monitor communication state, using means from PFSR-FC3-3, and implement strategies to cope with network errors or degradation (e.g. move to fail operational state or enter safe stop).

7 Stakeholder overview

In the previous chapters, the relevant inputs from other activities within 5GAA have been summarised. Using this knowledge, it is now possible to dive into the potential business considerations for ToD. The first step in this process is to identify the different stakeholders. When doing so, it is important to distinguish between a functional classification and identification of the actual entities. The former is a generic way of describing which types or roles could be taken up within the ToD ecosystem in order to realise a functional, safe and profitable end-to-end ToD solution. The latter identifies possible candidates to take up those roles. It is important to make this distinction, because this mapping between functional classification and entities can be different per use case and even per explored business model configuration for that use case. For instance, an automotive OEM could in one context be both the fleet owner and the ToD Service Provider (e.g. when realising use case T-180207 Tele-operated Driving for Automated Parking on their own manufacturing plants), but in another approach it could be only the fleet owner, only the ToD Service Provider, or neither. The identified stakeholders, both in perspective of function and entity, are presented in *Table 7*.

Table 7: Functional classification of ToD stakeholders, and mapping to entities

Stakeholder Role	Corresponding Function	Possible Entities (to take up this role)
Fleet owner	Owns one or multiple vehicles that are equipped with ToD capabilities.	• Vehicle OEM (light vehicles, buses and shuttles, trucks, emergency response vehicles, industrial vehicles, agricultural vehicles, delivery bots) • Consumer owning a personal vehicle • Leasing company

		• Transport and logistics company • Taxi company • Public transport company
User	Makes use of a vehicle with ToD capabilities as a Passenger or Transportation Service Provider.	• Fleet owner • Consumer using a personal leased vehicle • Transportation Service Provider
Passenger	Uses a vehicle with ToD capabilities for undertaking a trip.	• Person using a personal vehicle (driver, other passenger) • Client of taxi company • Client of public transport company
Transportation Service Provider	Makes use of a vehicle with ToD capabilities for providing transportation services to Passengers or Shippers (when moving goods instead of people).	• Vehicle OEM • Transport and logistics company • Taxi company • Public transport company
Shipper	Makes use of a vehicle with ToD capabilities for transporting its goods from a certain source to a certain destination. The equivalent of the Passenger stakeholder when in the domain of transport and logistics, since it is also the party that is requesting transport and will be paying for it.	• Manufacturer of goods • Retailer
Vehicle Access Provider	Exposes a vehicle with ToD capabilities through certain APIs so they can be tele-operated by another party.	• Vehicle OEM
Mobile Network Operator	Provides the mobile network connectivity to the vehicle and/or control centre.	• MNO providing nationwide coverage in a single country • MNO providing nationwide coverage in neighbouring countries • Operator of private mobile network in specific confined area • MNO roaming aggregation authority (e.g. on top of MEC services of MNO's)
Internet Service Provider	Provides fixed network connectivity to the control centre, in the event the control centre is connected through a fixed line instead of a mobile network.	• Fixed-connectivity-only ISP providing nationwide coverage in a single country • Fixed-connectivity-only ISP providing nationwide coverage in neighbouring countries • MNO also providing nationwide fixed network connectivity in a single country • MNO also providing nationwide fixed network connectivity in neighbouring countries
Cloud Service Provider	Provides the cloud infrastructure to run the cloud services on.	• Over-the-top cloud service provider • MNO providing cloud services (central but connected to the core network, or MEC) • Cloud services aggregation authority (e.g. on top of MEC services of MNOs, see GSMA MEC Operator Platform for more background information)

ToD Technology Provider	Provides the specific technical tools needed for tele-operating a vehicle, both for the control centre (driving stations) as well as for the ToD-capable vehicle (on-board unit). Contains both the main technology providers (tier 1) as the auxiliary (tier 2/3).	• Vehicle OEM • Specialised ToD technology company
ToD Service Provider	Performs the actual tele-operation by providing one or more ToD operators that remotely take over control (direct or indirect) of the fleet(s) of its client(s).	• Vehicle OEM • Transport and logistics company • Taxi company • Public transport company • Specialised ToD service provider company
Road Authority	Determines policy and general regulations needed for using ToD capabilities on public roads under certain conditions.	• Municipality • Ministry (regional or national) • European Commission • United Nations
Road Operator	Determines local regulations governing the roads it operates for ToD to be used on those specific roads, performs traffic management on those roads, provides information from and/or interaction with roadside infrastructure (traffic lights, VMS, etc).	• Municipality • Regional or national road operator • Private road operator (highways, tunnels, bridges, etc.)
Road Information Service Provider	Provides information about road conditions to enhance the awareness layer on the ToD operator HMI, and to compensate for the loss of sensory perception caused by the physical decoupling of the operator and the vehicle.	• Road operator • Commercial Real-Time Traffic Information (RTTI) service provider • Safety-Related Traffic Information (SRTI) source (vehicle OEM or neutral server provider)
Interchange Service Provider	Provides the Interchange function.	• Road operator • Specialised Interchange Service Provider company
Infrastructure Service Provider	Provides infrastructure in the field (confined area and/or public road) that supports the ToD function through additional video feeds and/or automated vehicle control functions that can take control of the vehicle from a human ToD operator, e.g. in the case of automated parking.	• Terminal owner (harbour, airport, logistic hub) • Owner of manufacturing plant • Parking lot owner (municipality, private parking lot company)
Certificate Authority	Trusted party that provides security certificates to the different ToD stakeholders that have to deploy technical components in the ToD ecosystem.	• Road Authority • Road Operator • Specialised CA company
Insurer	Through a contractual agreement, undertakes to compensate specified losses, liability, or damages incurred by another individual in the context of tele-operating a vehicle.	• Bank • Insurance company

8 Operational processes and requirements on the interfaces

When determining how the different identified stakeholders can collaborate, it is important to understand the different processes in which they will interact, and which operational requirements they might impose on the corresponding interfaces, as given in Figure 1. In this chapter, those processes and requirements are introduced under the following headings:

- Establishing connection between the different components of the architecture
- Initiating and terminating a ToD session between a certain vehicle and operator
- Handovers between components in an active ToD session

Table 8: Description of processes that require interaction between stakeholders, and the requirements they impose on the interfaces

Type of Process	Involved End Points	Description	Operational Requirements on Interfaces
Establishing connection between the different components of the architecture	ToD AS – OEM AS	The back-end systems of the ToD Service Provider and the Vehicle Access Provider have to be connected as part of a long-lasting partnership to allow tele-operation by the ToD SP of vehicles exposed by the Vehicle AP. This long-lasting connection is therefore manually configured, as a result of contractual agreements between both parties. Contractual agreements between both parties are captured in an SLA covering *technical* requirements, and *availability* requirements for performing the ToD service as designated.	• Secure (authentication, authorisation, integrity, confidentiality, non-repudiation) • Manual configuration • Since this link will form the backbone of the connection between operator and vehicle (control plane or data plane/control plane), it has to be a low-latency link with consistently accurate time synchronisation, providing the *technical* requirements, e.g. throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2] • Redundancy where needed to improve availability
	ToD AS – ToD Operator App	When an operator starts his/her work shift at the control centre of the ToD Service Provider, the ToD Operator App of his/her operating station will connect to the ToD AS, establishing both a control and data plane connection. Through the control plane it will start and stop ToD sessions to specific vehicles, as presented or requested by the AS. Once the session is established, it will also trigger the data plane to exchange both sensor data from the vehicle and control	• Secure (authentication, authorisation, integrity, confidentiality, non-repudiation) • Automated configuration (establishing and tearing down the connection) • Since this link will form the backbone of the connection

[2] More details regarding the appropriate values for such technical requirements, and the framework to determine them, are studied in [3]. It is important to highlight that such technical requirements/quantifications will always represent the knowledge level of a certain moment in time, and will always be part of a continuous refinement process. Another element to take into account is that some of these technical requirements will be more determined by the use case itself (such as latency, jitter and time synchronisation requirements), while others will be more determined by the envisaged scale of a specific deployment (e.g. bandwidth). And a last remark is that these specific technical requirements will always be captured in an SLA, which means that any technical requirement that will be imposed on this interface should be measurable.

		commands to the vehicle. At the end of the shift, when the operator disengages from the operator station, this connection will be closed again.	between operator and vehicle (control plane or data plane/control plane), it has to be a low-latency link with consistently accurate time synchronisation, providing the required throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2] • Acknowledge driving ability/vitality and requirements for driving vehicles (remotely) • Redundancy where needed to improve availability
	OEM AS – OEM App	ToD sessions can be immediately requested, both by the OEM App and by the OEM AS, and details can be OEM-implementation specific. To support ToD sessions, the connection between OEM AS and OEM App will support a low-latency control channel, and possibly also a low-latency high-throughput data channel (in case the ToD AS does not make use of the possibility to directly connect its data plane to the ToD Vehicle App).	• Secure (authentication, authorisation, integrity, confidentiality, non-repudiation) • Automated configuration (establishing and tearing down the connection) • Since this link will form the backbone of the connection between operator and vehicle (control plane or data plane/control plane), it has to be a low-latency link with consistently accurate time synchronisation, providing the required throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2] • Redundancy where needed to improve availability
	ToD AS – ToD Vehicle App	To shorten the path between ToD AS and the ToD Vehicle App, a direct connection between ToD AS and ToD Vehicle App can be established as the data plane for a ToD session. This can be done when the ToD Vehicle App is, for example, installed by the fleet owner in the vehicle as an after-market add-on provided by a ToD Technology Provider, or if the OEM that included the ToD Vehicle App and exposes it externally through the OEM App for this type of direct ToD data plane connection to the Vehicle (but still requires the control plane to run through the OEM AS for ToD session initiation and termination).	• Secure (authentication, authorisation, integrity, confidentiality, non-repudiation) • Automated configuration (establishing and tearing down the connection) • Since this link will form the backbone of the data plane connection between operator and vehicle, it has to be a low-latency link with consistently accurate time synchronisation, providing the required throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2]
	Interchange – OEM AS	The back-end system of the Vehicle Access Provider has to be connected to an Interchange of its Interchange Service Provider as part of a long-	• Secure (authentication, authorisation, integrity, confidentiality)

		lasting partnership. This allows tele-operated vehicles exposed by the VAP to make use of external information regarding its immediate environment, e.g. originating from a Road Operator, Road Information Service Provider or Infrastructure Service Provider. This can, for example, be valuable additional input for safety fallback functions when the vehicle is tele-operated. This long-lasting connection between an Interchange and OEM AS is therefore manually configured, as a result of contractual agreements between both parties. To configure which data should be sent to the OEM AS, a pub-sub control mechanism is put on top of the long-lasting connection.	• Manual configuration
	Interchange – ToD AS	The back-end system of the ToD Service Provider has to be connected to an Interchange of its Interchange Service Provider as part of a long-lasting partnership. This allows tele-operators to make use of external information about the immediate environment of the vehicle, e.g. originating from a Road Operator, Road Information Service Provider or Infrastructure Service Provider. This can, for example, be valuable additional input to be displayed on the HMI of the operator station. This long-lasting connection between Interchange and ToD AS is therefore manually configured, as a result of contractual agreements between both parties. To configure which data should be sent to the ToD AS, a pub-sub control mechanism is put on top of the long-lasting connection.	• Secure (authentication, authorisation, integrity, confidentiality) • Manual configuration
	Interchange – RTA AS	The back-end system of the Road Operator or Road Information Service Provider has to be connected to an Interchange by its Interchange Service Provider as part of a long-lasting partnership. This allows information to be distributed to ToD Service Providers and Vehicle Access Providers in support of ToD operations. This long-lasting connection between interchange and RTA AS is therefore manually configured, as a result of contractual agreements between both parties.	• Secure (authentication, authorisation, integrity, confidentiality) • Manual configuration
	Interchange – SP Infr AS	The back-end system of the Infrastructure Service Provider has to be connected to an Interchange of its Interchange Service Provider as part of a long-lasting partnership. This allows distribution of its meta-data to ToD Service Providers to support service discovery and activation/termination of Infrastructure Services in the ToD operations. This long-lasting connection between the Interchange and RTA AS is therefore manually configured, as a result of contractual agreements between both parties. Note that the actual ToD data plane (sensory data and control commands) are not sent through this connection; these are sent on the interface that directly connects the SP Infr AS of the	• Secure (authentication, authorisation, integrity, confidentiality) • Manual configuration

		Infrastructure Service Provider with the ToD AS of the ToD Service Provider.	
	Interchange – Interchange	The Interchange component has the capability to provide its clients with information that was actually made available by another Interchange (information routing). For this purpose, the Interchanges of different Interchange Service Providers establish connections as part of a long-lasting partnership. This long-lasting connection between Interchange and RTA AS is therefore manually configured, as a result of contractual agreements between both parties.	• Secure (authentication, authorisation, integrity, confidentiality) • Manual configuration
	RTA AS – RTA App	In order to provide relevant information regarding the conditions on its roads, the Road Operator or Road Information Service Providers need to capture data about the road itself. That data is continuously transmitted to the AS of the same organisation. Therefore, the establishment of this connection is part of the internal operation of this organisation but guaranteeing the requirements for the link and data of the RTA AS – ToD AS interface	• Secure (authentication, authorisation, integrity, confidentiality) • Manual or automatic configuration • This link has to be a low latency with consistently accurate time synchronisation, providing the required *technical* requirements, e.g. throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2]
	SP Infr AS – SP Infr App	In order to provide relevant information regarding the conditions on its infrastructure, and to provide ToD sensor or control services to ToD Service Providers, the Infrastructure Service Providers need to capture data about the infrastructure itself. That data is continuously transmitted to the AS of the same organisation. Therefore, the establishment of this connection is part of the internal operation of this Infrastructure SP, which has the free choice to automate this, or establish all these connections manually.	• Secure (authentication, authorisation, integrity, confidentiality) • Manual or automatic configuration
	RTA AS – ToD AS	Certain high-throughput data feeds, e.g. video feeds of roadside cameras, are transmitted directly from the RTA AS of the Road Operator to the ToD AS of the ToD Service Provider. These connections are established on request of the ToD Service Provider, making use of the Interchange for the corresponding control plane (discovery, establishment request, termination). Ad-hoc safety relevant data is transmitted from the RTA AS to the ToD AS with highest priority and according to agreed service requirements. Contractual agreements between both parties are captured in an SLA covering *technical* requirements, and *safety* requirements for performing the ToD service as designated.	• Secure (authentication, authorisation, integrity, confidentiality) • Automated configuration (establishing and tearing down the connection) • This link has to be a low-latency link with consistently accurate time synchronisation, providing the required *technical* requirements, e.g. throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2] • Redundancy where needed to improve availability
	SP Infr AS – ToD AS	Certain high-throughput or safety-critical control data feeds, e.g. video feeds of local cameras or control commands of automated parking services	• Secure (authentication, authorisation, integrity, confidentiality)

		of the Infrastructure Service Provider, are transmitted directly from the SP Infr AS of the Infrastructure Service Provider to the ToD AS of the ToD Service Provider. These connections are established on request of the ToD Service Provider, making use of the Interchange for the corresponding control plane (discovery, establishment request, termination). Contractual agreements between both parties are captured in an SLA covering *technical* requirements, and *safety* requirements for performing the ToD service as designated.	• Automated configuration (establishing and tearing down the connection) • This link has to be a low-latency link with consistently accurate time synchronisation, providing the required *technical* requirements, e.g. throughput of X Mbps and Y maximum latency for 99.XXXX % of the time[2] • Redundancy where needed to improve availability
Initiating and terminating a ToD session between certain vehicle and operator	ToD Operator App – ToD Vehicle App: control plane through OEM	When a certain ToD-capable vehicle is known by the ToD AS to be waiting for an operator (because someone in the vehicle activated a ToD request, or because another system declared the vehicle as ready for starting a ToD journey, e.g. terminal or plant management services), it will be assigned to a stand-by operator which will take over (direct or indirect) control. Depending on the policy of the Vehicle Access Provider, it is possible that the ToD AS of the ToD Service Provider will first negotiate the ToD session with the OEM AS of the Vehicle Access Provider, and will then establish a direct data plane (sensory data and control commands) connection between the ToD AS and the ToD Vehicle App. The required response time between declaring a vehicle as waiting for an operator, and having an operator in control through an active ToD session can vary in different situations. A truck that has finished loading and can now start its long journey will have less stringent requirements than a vehicle that became a dangerous obstacle on the road because its driver or autonomous driving functions can no longer drive the vehicle safely. The way in which the ToD Service Provider can meet every imposed requirement will not only depend on the technical latency of the network and control mechanisms, but also on the dimensioning of the pool of stand-by operators by the ToD Service Provider.	• Different response time requirements per situation. This can be considered part of the ODD, and has to be agreed upon before ToD Service initiation. • Appropriate dimensioning of pool of standby operators by ToD Service Provider is essential
	ToD Operator App – ToD Vehicle App: control plane and data plane through OEM	Identical to the case 'ToD Operator App – ToD Vehicle App: Control Plane Through OEM', with the only difference that the data plane is not established directly between ToD AS and ToD Vehicle App. Instead, it follows the same path of the control plane, going through the OEM AS of the Vehicle Access Provider to reach the vehicle.	• Different response time requirements per situation; this can be considered part of the ODD, and has to be agreed upon before ToD Service initiation • Appropriate dimensioning of pool of standby operators by ToD Service Provider is essential
Handovers between components in an active	Changing ToD type	In certain conditions, e.g. in the context of use case 'T-180206 Tele-operated Driving Support' it is possible that a ToD vehicle will first be tele-operated with Indirect Control, but will need the operator to take over Direct Control in the event	• Different response time requirements per situation. This can be considered part of the ODD, and has to be

ToD session		of challenging situations that the automation functions of the vehicle cannot manage, even with Indirect Operator Control as guidance. In that case, during an active ToD session, the ToD Type has to change from Indirect to Direct Control. Depending on the design of the operator stations provided by the ToD Technology Provider and used by the ToD Service Provider, this can also require the migration of the ToD session from one operator to another (Direct Control stations use steering wheels and pedals to control one vehicle per operator, Indirect Control stations use keyboard and mouse to control one or more vehicles at the same time). This change of ToD Type can be requested by the vehicle itself, or by the operator managing the vehicle in Indirect Control. Similar to the process of initiating and terminating a ToD session between certain vehicles and operators, the corresponding response time requirements can be different depending on the situation, and are influenced both by the technological approach towards the interfaces, but also by the way in which the ToD Service Provider dimensions the pool of stand-by operators. Note that the inverse process, changing from Direct Control to Indirect Control can also occur, e.g. when the directly controlled vehicle enters an ODD where it can be safely controlled indirectly. In this case, the response time requirements are less stringent, though the change of ToD mode is not to ensure safety, but to optimise the business case of tele-operation activities.	agreed upon before ToD Service initiation. • Appropriate dimensioning of pool of standby operators by ToD Service Provider is essential
	Changing ToD remote operator	In the context of use case 'T-180205 Tele-operated Driving', it is possible that long-haul journeys are undertaken with tele-operated vehicles, especially in the transport and logistics sector. The duration of such a session can last longer than the remaining duration of the assigned operator's work shift. As a result, the ToD remote operator will need to change during an active ToD session, both for Direct and Indirect Control. Similarly, even for shorter journeys it could be desirable to be able to change ToD operator during an active session, to make sure that operators can be active during their entire shift, and not have to wait in idle mode during the last part of their shift because all newly presented ToD session requests would take longer than the remainder of their shift. Also, when a tele-operator becomes unwell he/she could, for instance, press an emergency stop button to immediately handover the current session(s) to another operator, taking advantage of the decoupling of the physical location of vehicle and operator to improve road safety. The response time requirement for an active Direct Control ToD session can be different on the control plane depending on the context: changing operator at the end of the shift is less critical in terms of reassigning to another operator than	• Different response time requirements per situation; this can be considered part of the ODD, and has to be agreed upon before ToD Service initiation • Less stringent response time requirements for Indirect Control than for Direct Control • Appropriate dimensioning of pool of standby operators by ToD Service Provider is essential

		doing so as a reaction to an emergency stop button. On the data plane, though, the handover should be performed seamlessly during a Direct Control session, since the vehicle has to be controlled at all times. The handover of an Indirect Control ToD session will be less stringent in terms of response time requirements, since in that case the vehicle is also relying on its internal automation functions, and not only on the operator for control.	
	Handover to other ToD service provider	Ideally, ToD service provider operational boundaries should not cross frequently used vehicles trajectories, to avoid or minimise handover between ToD service providers. Handover between ToD service providers could, however, be required under certain conditions, e.g. if the first ToD service provider becomes unable to continue the control of the vehicle for any reason, e.g. remote driver falls ill and there is no standby replacement (load condition), or the service provider's system enters non-operational mode for technical or other reasons.	
	Handover to other mobile network – QoS degradation	If during an active ToD session it is noticed that the mobile network will no longer be able to deliver the promised performance guarantees, connectivity may need to be handed over to another MNO operating in the same area. In a Direct Control ToD session, this imposes stringent handover time requirements, and accurate detection and even prediction of QoS degradation. This can be considered as an MNO-supported national roaming handover, and hence requires solid business agreements between competing MNOs, and an appropriate regulatory framework. An alternative would be to consider a vehicle-oriented approach, where the vehicle has multiple SIM-cards of different MNOs, and can decide itself when to use which connection based on QoS measurements. This, however, multiplies the connectivity costs for the vehicle. Judging from the requirements of OEMs, when it comes to requesting cellular network connectivity for automated vehicle use cases, it is unlikely that the MNO will not be able to deliver the promised performance, as there are failover solutions and dedicated resources deployed according to the agreed SLA terms. In territories where MNOs share networks (e.g. in Canada) the handover is transparent to the OEM.	• Stringent handover time requirements in Direct Control cases in combination with MNO-supported national roaming • Less stringent in Indirect Control cases, but also less stringent QoS requirements, reducing the probability that a handover because of QoS degradation is needed • Solid business and regulatory framework needed
	Handover to other mobile network – International roaming	If an active ToD session crosses an international border, it has to perform a seamless international roaming handover to allow the operator to remain in control. This is especially important for Direct Control where the handover time constraints are very stringent. To realise this, MNOS will need to collaborate on both sides of the border, by jointly adopting technical solutions for pro-active signalling and handover, instead of the current	• Stringent handover time requirements, pro-active signalling and handover needed • Appropriate upfront business arrangements between MNOs on both sides of the border needed

		situation where the handover is only initiated after losing connection with the home network.	

9 Go-to-market constraints

Based on all insights presented in the previous chapters, it is now possible to identify some questions regarding market constraints. As mentioned in the introduction of this deliverable, this document does not envisage to answer all of them. It provides some first thoughts on possible questions, but these are only intended to facilitate others working on their own business models in the ToD domain, and to use these identified constraints and thoughts as inspiration for all the elements they could tackle in their own business model definition.

9.1 Technical constraints

Questions:

Can the communication path between Controlled Vehicle and Control Centre meet the stringent QoS requirements for security, latency and bandwidth at all times within the MNO's coverage area?

- Judging from the requirements of OEMs when it comes to requesting cellular network connectivity for automated vehicle use cases, it is unlikely that the MNO will not be able to deliver the promised QoS requirements, as there are failover solutions and dedicated resources deployed according to the agreed SLA terms. However, it needs to be investigated for any considered deployment if such measures are indeed provided by the corresponding MNO, and if the corresponding QoS requirements will be met.

Is it possible to predict QoS degradation and proactively mitigate it in a timely manner in order to allow for Direct Control ToD? If so, can this be done without avoiding the need for multiple SIM cards in the vehicle, and hence multiplied connectivity costs?

- There is no additional value from an OEM perspective to integrate multiple SIMs, nor is there reason for the eSIM that will most likely be used to switch profiles from one MNO to another. The MNO providing connectivity to the OEM is compensated for the deployment of dedicated resources and failover solutions necessary to deliver the promised QoS.

Can cross-border connectivity handover be performed seamlessly to allow for Direct Control ToD?

- This is under development and testing in various cross-border areas in the world, and also subject to research by the MEC4AUTO, 5G-Blueprint and 5GAA Network Reselection Improvements (NRI) work items.

Is the autonomous sensing and actuating vehicle technology mature enough to avoid accidents because of wrong or late information received from the Control Centre (from the vehicle perspective) or from the vehicle (from the operator perspective)? Is certification needed to ensure the maturity of the deployed technology?

- This remains to be investigated. But given the current state of deployed advanced driver-assistance systems (ADAS), it seems reasonable to expect that (maybe with some further optimisation) state-of-the-art technology would be capable of immediately bringing a disconnected vehicle to a safe stop. And similarly, in the case of clearly visible road markings, it can also be expected that the vehicle could continue its journey safely for a few seconds in autonomous mode before engaging the 'safe stop' procedure. This could overcome the need for immediate stopping in the event of very brief connectivity interruptions, resulting in less distortion of the traffic flow and hence safer tele-operation adoption. Perhaps this line-marking requirement can also be seen as an indication that similar to Level 4 (L4) autonomous driving, ToD Type "Direct Control" will only be possible on certain roads that are validated beforehand (as Operational Design Domain).

Is it possible to place Control Centres at any location? Or do they need to be located physically near certain connection points of their MNO or ISP? Could operator stations also be installed in operators' homes, or in different time zones to allow ToD operation at night (e.g. for the transport and logistics sector)? Are there minimum technical requirements for such Control Centres?

- Depending on the territory, OEMs may require connection with the MNO infrastructure at several locations across the territory, as well as the deployment of distributed core network infrastructure. Control Centres may then be placed physically close to each connection point so that the QoS requirements are satisfied across all time zones in the territory.

Is it possible to have sufficient redundancy in the vehicle and the operator station to keep costs of ToD technology at an acceptable level?

- Fallback (safe-state) technology in the *vehicle is probably the only way to bring the solution up to* necessary a*utomotive* s*afety* i*ntegrity* l*evel* (*ASIL*). Redundancy outside the vehicle, e.g. in the network or operator station, can be seen as measures that improve availability, but not as measures that can guarantee functional safety as defined in ASIL.

Recommendations:

Industry-agreed standards would be beneficial to make sure that Controlled Vehicle and Control Centre have the same set of semantic rules for the control messages.

Also, standardisation is needed on the technical interfaces of the architecture (Figure 1), given the large amount of possible entities that could take up the different stakeholder roles. This does not only involve the data plane, but also the control plane for automated interface configuration.

9.2 Legal constraints

Background:

To the best of our knowledge, **nowhere in the world does legislation today allow for both ToD Type "Indirect Control" and ToD Type "Direct Control" operations on a day-to-day basis on public roads**. There are some examples of legislative work being done to accommodate the latest technological developments, but these are targeting autonomous driving, and not ToD per se.

Example 1: **Regulation on automated lane-keeping systems that was adopted by the United Nations in June 2020**[3].

This regulation establishes strict requirements for Automated Lane Keeping Systems (ALKS) for passenger cars which, once activated, are in primary control of the vehicle. However, the driver can override such systems and can be requested by the system to intervene, at any moment.

Adopted on 23 June by UNECE's World Forum for Harmonisation of Vehicle Regulations, this is the first binding international regulation on so-called Level 3 vehicle automation. It entered into force in January 2021. It stipulates that ALKS can be activated under certain conditions on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions.

In its current form, the regulation limits the operational speed of ALKS systems to a maximum of 60 km/h. It also requires that on-board displays used by the driver for activities other than driving when the ALKS is activated shall be automatically suspended as soon as the system issues a transition demand, for instance in advance of the end of an authorised road section.

The regulation also lays down requirements on how the driving task shall be safely handed back from the ALKS to the driver, including the capability that the vehicle comes to a stop if the driver does not reply appropriately. The regulation includes the obligation for car manufacturers to introduce Driver Availability Recognition Systems. These systems control both the driver's presence (on the driver's seats with seat belt fastened) and the driver's availability to take back control.

The regulation also introduces an obligation to equip vehicles with a 'black box' so-called Data Storage System for Automated Driving, which will record when ALKS is activated. The regulation includes provisions governing Type approval, technical requirements, auditing, reporting and testing. ALKS functionalities will also have to be compliant with the cybersecurity and software update requirements laid out in the two new UN regulations adopted on the same day.

---

[3] https://unece.org/transport/press/un-regulation-automated-lane-keeping-systems-milestone-safe-introduction-automated

Although many elements of this regulation could also be relevant for ToD operation[4], the requirement for a driver to be able to override the system at any moment makes it unfit for ToD use cases where only passengers or no people at all are present in the vehicle. Though it can be considered as a valuable framework on which appropriate legislation for ToD could be built upon in the future.

Example 2: **Regulation that has been approved by the federal cabinet of Germany on 10 February 2021**[5].

In contrast to the UN regulation described above, this regulation applies to automated functions of Levels 4 or 5. Accordingly, vehicles are allowed to drive autonomously in what is described as "defined operating areas" if so-called technical supervision can deactivate the vehicle "at any time" during operation or enable offer alternative driving manoeuvres. For this purpose, there must be a permanent radio connection with the vehicle.

The new law aims at deployment concepts such as shuttle traffic, people movers, Hub2Hub traffic, demand-oriented offers in off-peak times, the transport of people and/or goods on the first or last mile, and "dual-mode vehicles" such as at Automated Valet Parking (AVP).

In these cases, there should no longer be drivers in the autonomous vehicles who can intervene in an emergency. Instead, a "natural person" provides technical supervision by remotely monitoring the vehicle and can intervene in an emergency. However, the federal government does not want to allow the supervisor to take over the driving task from a distance. Instead, the vehicle must be able to recognise its system limits itself and be able to put itself in a "risk-minimal state". This means that the German legislation could be considered as the **first legal framework that allows for ToD Type "Indirect Control"** on a day-to-day basis on public roads. It, however, **explicitly does not allow for ToD Type "Direct Control"**.

Note that the German Federal Ministry of Transport considers the permanent radio link to be necessary so that the law is compatible with the Vienna Convention on Road Traffic of 8 November 1968. This means that even if Germany takes on a pioneering role in autonomous driving and does not want to wait for any international UN/ECE regulation, existing agreements must nonetheless be complied with. For this reason, the autonomous vehicles are not allowed to drive through an urban tunnel, for example, if there is no permanent internet connection with the supervision.

The regulation also specifies other requirements. The journeys do not have to be permanently monitored by the supervisor. In addition, the vehicle should have a "system for accident avoidance", which among other things is designed to avoid and reduce damage. It should also take into account the importance of legal interests "in the event of unavoidable alternative damage to different legal interests", with the protection of human life having the highest priority. In the event of such risk to human life, the system may not provide for "any further weighting based on personal characteristics".

The government is thus implementing the recommendations of the ethics committee on autonomous driving. In addition, the vehicle must refuse driving manoeuvres approved by the supervisory authority if the driving manoeuvre would endanger people either involved or not directly involved in traffic (conditions). The requirement that the vehicle must stop automatically when it leaves the specified operating area has been added. However, it does not regulate how many cars may be monitored by the supervisor at the same time. The vehicle owners are obliged to save 13 data categories. These range from the vehicle identification number and position data to environmental and weather conditions, as well as lighting status and power supply. The Federal Motor Transport Authority and state authorities should be able to access the data.

According to the German government's plans, the law is to be passed by the Bundestag and Bundesrat before the summer break. The required EU notification procedure has therefore already been initiated. At the same time, the government advocates international rules at the UN/ECE level. Therefore, the law on autonomous driving is only "an interim solution until there are harmonised regulations at international level". **From the ToD perspective, the possible integration of this German regulation in a future UN regulation is a very interesting process to keep following**. It will also be valuable to see whether ToD Type "Direct Control" allowances will be included as part of this process.

While awaiting these legislative evolutions, the only way to deploy ToD vehicles will be to integrate them in research and development activities, and not yet in day-to-day operations. For such R&D experiments on public roads, **many countries have a legal process of exemptions to test prototype vehicles on public roads** under certain

[4] Usage is only allowed under certain road conditions and vehicle speeds. Requirements include: the capability (when needed) to come to a safe stop when the driver has no control, driver availability recognition which could also be applied to ToD operators, black box, cybersecurity and software updates, and provisions for governing Type approval, technical requirements, auditing, reporting and testing.

[5] https://www.golem.de/news/gesetzentwurf-beschlossen-autonome-autos-an-der-langen-leine-2102-154077.html , referring to the regulation that is published on https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile

conditions. Some examples of such frameworks are the Dutch Exceptional Transport Exemptions Decree (BOEV)[6] or more recent Dutch Experimentation Law on Self-driving Vehicles[7], which also allows the testing of vehicles with no human fallback driver present; something not allowed under BOEV, but as a result leads to more stringent prerequisites for getting the exemption approved). Similarly, Belgium has defined a framework called the 'Code of Practice autonomous vehicles'[8]. These are just a few examples of a regulatory framework that can be found in many countries worldwide, allowing for the testing of ToD Type ”Indirect Control” and Type ”Direct Control” on public roads, but not for deployment.

When focusing on **confined areas**, and not on public roads, these regulations are not applicable. So from that perspective there seem to be no regulatory constraints for deployment of ToD Type “Indirect Control” and Type “Direct Control”. However, when planning a specific deployment, it is important to **also check if no other legislation applies to the corresponding site** which should be taken into account, e.g. regulations on guaranteeing the safety of employees on company sites. An analysis of those constraints is beyond the scope of this study.

Questions:

Legislation today does not allow for ToD operations on a day-to-day basis on public roads. It only provides (in some countries) a legal framework to organise ToD tests on public roads when adopting specific procedures and providing specific documentation of the solutions being tested and when applying the tests themselves.

- Confined areas may take precedence in the commercial operation of ToD for this reason.

Will national roaming be allowed for managing QoS degradation? And if so, how to make sure that MNOs could not be accused of using this new regulatory framework to infringe competition laws in other domains than ToD?

- National roaming is not the predominant way to mitigate QoS degradation. However, where network sharing agreements exist, these dictate which uses they cover, and which are out of scope, to be sure that the applicable regulatory and competition law frameworks are not violated by the deployment in question.

9.3 Liability constraints

Questions:

Given the large number of involved stakeholders, could it be expected that they all might come to a consensus on liability before starting the ToD service? Does this suggest the need to fulfil the different stakeholder roles with as little variation in the entities as possible, meaning it would be better for every involved entity to take up multiple roles among those identified?

- While it is clear that liabilities will be considered before starting the service, and that contracts will include the corresponding terms, the primary driver for the assumption of multiple roles in the value network is not necessarily the avoidance of liability.

Do specific training exercises need to be organised for the operators to be able to make acceptable liability agreements? Will this need to be translated into specific licences or other requirements for operators?

- Yes, it is expected that training and certification will both be mandated. In ToD deliverable D2 [3], one of the requirements of the ToD Operator subsystem is that the human remote driver needs to be qualified to operate the ToD Operator subsystem.
- Some more considerations:
    - As the remote driver will perform part of or all dynamic driving tasks of an automotive vehicle, the remote driver should at least hold the driver's licence of the corresponding vehicle category, or permission to operate the vehicle in the given environment.
    - Technically, performing part of or all dynamic driving tasks at a remote location imposes additional requirements on the remote driver, compared with traditional local drivers. Additional knowledge and skills are needed for handling situations that do not exist in the traditional 'local' operation of the

---

[6] https://www.rdw.nl/over-rdw/information-in-english/about-rdw/annual-prospect-2021/safety

[7] https://www.government.nl/latest/news/2019/07/02/green-light-for-experimental-law-for-testing-self-driving-vehicles-on-public-roads , law itself can be found on https://zoek.officielebekendmakingen.nl/stcrt-2019-34245.html

[8] https://mobilit.belgium.be/en/resource/code_practice_autonomous_vehicles

vehicle, e.g. connectivity problems. Such skill can only be obtained via dedicated training. In this sense, a specific licence should be needed for a remote operator in order to establish acceptable liability agreements. Such a specific ToD remote operators' licence should authorise the holder to remotely drive the corresponding vehicle category in addition to traditional location operation.

9.4 Business constraints

Questions:

Will ToD Technology Providers and/or ToD Service Providers also need to be looking at fulfilling the role of Vehicle Access Provider to get their business model positive? And if so, will the vehicle OEMs be open to this? And if not, to what degree would the vehicle OEMs consider taking up the role of Vehicle Access Provider themselves? This is key to allowing the ToD ecosystem to become a reality.

- For retrofit ToD technology, it could be possible to imagine a ToD Technology or Service Provider being the Vehicle Access Provider. However, for public roads it seems that factory-fit solutions may be the norm as they are perceived as more safe and secure. In this case, the OEM will be the Vehicle Access Provider in order to control access to the ToD technology and the service, while also controlling who will play the role of the Technology Service Provider, over time.

Is the willingness-to-pay of the user regarding the ToD premium service likely to be high enough to ensure a positive business case for all involved stakeholders? Is there a big difference between type of user in this context? Could this be mitigated by marketing the service with appropriate pricing schemes and service packages?

- Provided that there is a consensus between the stakeholders over the necessity of ToD as a support function for automated vehicles, there will always be entities willing to implement ToD as a feature of their AV proposition. If there is demand for AV, the cost of ToD could be covered by the value capture mechanisms of the AV product/service owner(s). Those with failed mechanisms will exit the market eventually.

- ToD Type "Direct Control" could also be brought to market as a standalone feature, rather than a support function of autonomous or automated vehicles. Relying on human drivers (remote operators), but removing the physical link between vehicle and local driver, can lead to interesting value propositions even without advanced automated driving capabilities within the vehicle. Resolving 'idle time' cost is one of the elements of that ToD Type "Direct Control" value proposition (since operators can switch to another vehicle as soon as the idle time begins, something that is not possible with local drivers). Another advantage of ToD Type "Direct Control" is the lowered danger level in hazardous and non-human-friendly environments, because the need to have a local driver present in that environment is mitigated. Whether the willingness-to-pay of this approach will be high enough though remains to be seen.

Could the connectivity cost be low enough to allow for a positive business case covering the entire ecosystem?

- The price of connectivity could be negotiable between buyers and sellers (often subject to a request for proposal, RFP) and uniform across uses with similar QoS characteristics to ToD and other low-latency C-V2X use cases.

Will the operator labour cost of the ToD Service Provider be low enough to allow for a positive business case covering the entire ecosystem (i.e. especially when relatively large pools of standby operators have to be put in place to be able to handle the stringent response time requirements of certain initiation or handover scenarios)? Which use cases and underlying ODD/scenario combinations suffer more than others from this aspect? Is there a big difference in answers to these questions if the operator is on the payroll of the ToD Service Provider, or of an independent contractor of the Service Provider?

- There are businesses all over the world, such as road assistance providers, that deliver services with similar characteristics. Labour cost could be one of the factors to take into account when pricing the service, but not necessarily the primary driver for ODD selection. One case of a low-cost Type "Indirect Control" ToD implementation for an AV vendor involved an RFP for the selection of ToD Service Providers involved in outsourcing solution, such as Accenture and Cognizant. The successful candidate would be expected to cover the whole North American operation of the AV vendor with 87 Type "Indirect Control" ToD operator seats.

Can insurance costs be low enough to allow for a positive business case on public roads? If not, can the business case at least cover confined areas?

- Liability differs between public road and confined area usage, therefore it is foreseen that insurers would address each ODD differently. Confined areas would naturally be the first to adopt ToD and there is experience in how to insure for liability related to the use of tele-operated industrial equipment. For public roads, if ToD usage is allowed by the authorities and there are enough ToD-enabled vehicles, insurers are likely to arrive at commercially viable plans as these represent an incremental business opportunity for them.

Will ToD as a concept be accepted by Passengers, Shippers or other road users?

- A public campaign to counteract concerns and increase acceptance by Passengers could be valuable.

- If ToD would be brought to market as a feature in vehicle automation analogous to GPS, the question is whether road users will accept automated and autonomous vehicles.

Will ToD as a concept be accepted by current professional drivers? And if not, is this an issue?

- The question is whether professional drivers have the power to stop or delay the adoption of automated/autonomous vehicles. They do have some sway but there are other powerful players involved in this market as well. If automation is proven to decrease costs and safety hazards, it will be difficult to put a brake on its growth.

- Other experiences with the transition from local to remote operation of equipment, e.g. rubber tyre gantry cranes in ports, has shown that, after the initial adjustment period, the operators do understand and embrace the advantages of tele-operation[9]**.** Organising an appropriate on-boarding process during this paradigm transition could be good mitigation for this concern.

- ToD relies on the expertise of professional drivers and demands additional skills. One of ToD's goals is make vehicle driving less labour intensive, but it also provides opportunities for early adopters (it need not render their jobs obsolete). This key message can be helpful when tackling professional driver concerns.

Will MNOs with international activities block MNOs operating in only one country from making international handover agreements with them, keeping them outside the ToD market for international transport?

- Internationally active MNOs and national operators have been known to forge agreements because some customers require collaboration with a single MNO across countries (which in turn has roaming agreements with MNOs in other countries to deliver this 'international service'), and others require a separate MNO as a 'direct partner' per country (in which case the two MNOs across the border work together for the cross-border handover). So, in meeting customer preferences, all types of MNOs have the right to be regarded either as a direct contractor or as a roaming partner.

Which policy should Road Authorities adopt to stimulate the business case and have a positive impact on society?

- Road Authorities should enable ToD infrastructure in their road network as part of their investment and service modernisation roadmap.

Which policy should national and regional governments adopt to stimulate the business case and have a positive impact on society?

- They should establish clear regulatory environments for automated driving and facilitate ToD service provision by improving network coverage in rural and cross-border scenarios, together with MNOs [8].

9 Example: https://www.youtube.com/watch?v=ID9ksGcj4To

10 Business models

T-180205 Tele-operated Driving

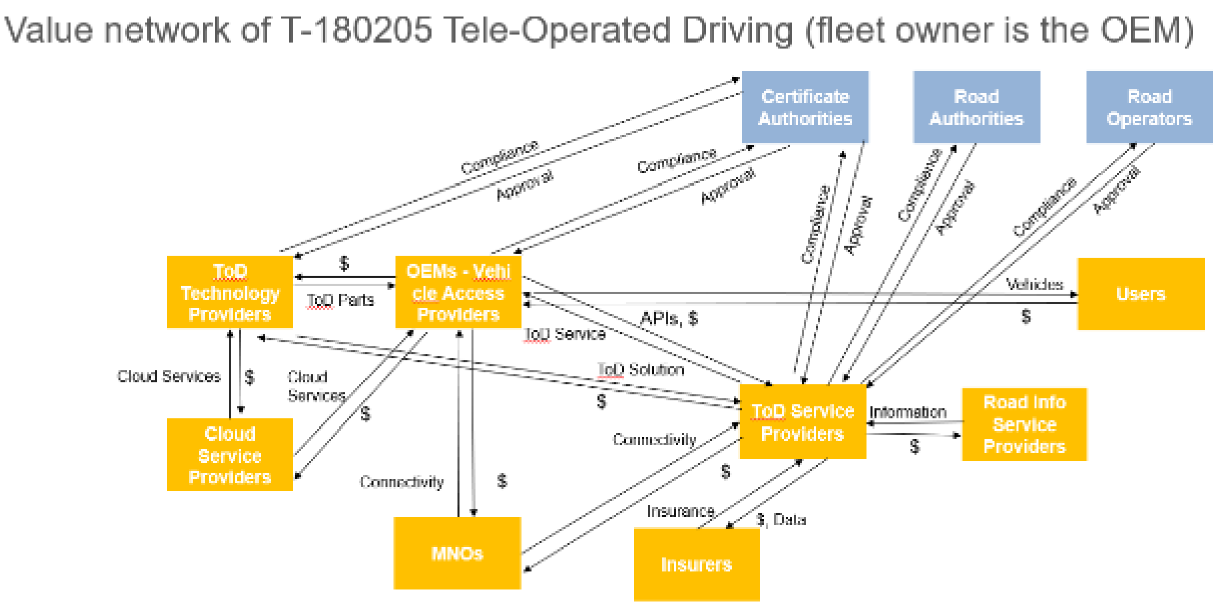
The first use case to be analysed is T-180205 Tele-operated Driving, with the following important constraints: service provided by one ToD service provider to a single OEM fleet owner in a confined area or for a standard trip, e.g. from a certain port to the destination city or from an area outside the city centre (e.g. airport) to the city centre. There is no important differentiation in terms of business analysis between Indirect Control and Direct Control implementations of ToD, so the following sections apply to either mode, unless otherwise noted.

There are a number of assumptions regarding functional roles defined in Chapter 7 that will be made in order to ensure that the business analysis of the use case represents realistic situations. Namely:

- The Vehicle Access Provider is the OEM. Factory-fit ToD solutions are assumed to be the norm, as opposed to retrofit solutions. In such a case, the OEM will be the Vehicle Access Provider so they can control access to the ToD technology and the service, while also controlling who will play the role of ToD Service Provider over time.
- The MNO is the Internet Service Provider, as most telecommunication providers offer both mobile and fixed services.
- For the particular use case, as described in Chapter 4, there is no involvement of Passengers, Shippers, Interchange Service Providers, or Infrastructure Service Providers.
- The fleet owner is the user of the service. It is either an OEM or some other Transportation Service Provider (e.g. a leasing company, a transport and logistics company, a taxi company or a public transport company). The analysis that follows will first look at the scenario where the fleet owner is the OEM, and then at the scenario where the fleet owner is some other Transportation Service Provider.

  The first stage of the analysis focuses on the value network of the use case with the characteristics described above. Only the relevant functional roles will be depicted (non-operational roles are shown in blue), and then only the exchanges that have to do with ToD:

Value network of T-180205 Tele-operated Driving (fleet owner is the OEM)



This scenario represents situations where, for example, an OEM ships vehicles to a port and then the vehicles need to be taken for temporary storage using ToD to a parking lot in a nearby location. This means that this scenario is situated in a confined area. The value network cooperates in the following manner:

- ToD Technology Providers: they have supplied the OEM with the parts that implement ToD in the vehicle, and at the same time they have supplied the ToD solution (for which they use cloud services) to the entity that will deliver the ToD service (the ToD Service Provider).
- OEMs: they have integrated the ToD parts in their vehicles at the manufacturing stage and are exposing APIs to the ToD Service Providers that are necessary for the delivery of the ToD service. OEMs are using cloud services for their platform and connect their vehicles at all times using cellular connectivity.
- Cloud Service Providers: they offer various cloud services to OEMs and ToD Technology Providers.
- MNOs: they offer cellular connectivity to OEM vehicles for all uses, including ToD and mobile and/or wireline connectivity to the ToD Service Providers, and for the delivery of the ToD service.
- Road Information Service Providers: they provide information on road conditions to the ToD Service Providers.
- ToD Service Providers: they offer the ToD service to the fleet owner user, which is the OEM in this case. The service is enabled using different components: a ToD solution supplied by the ToD Technology Provider, connectivity by the MNO, road information by the Road Information Service Provider, and access to APIs exposed by the OEM. The liability of the ToD Service Provider is covered by insurance for the ToD tasks.
- Users are the consumers or enterprises that will eventually buy the OEM's vehicles that are being remotely driven to their intended destination. Users will pay the OEM for the vehicles (often indirectly through a dealer), and a part of the price they pay will go towards covering the ToD service cost incurred by the OEM. In case this is lower than the cost of having vehicles transported in the traditional way (using trucks and drivers at the wheel), the OEMs also gain thanks to savings offered while automating a once manual process.
- Insurers: they offer insurance to the ToD Service Providers, making use of data obtained from them related to the ToD tasks being insured.
- Certificate Authorities, Road Authorities and Road Operators: these roles are non-operational in this scenario, as they do not provide input necessary for the delivery of the ToD service per se. Nevertheless, they approve the operation of ToD Service Providers in their jurisdiction and they offer certification of parties that are critical in the implementation and delivery of the ToD service, i.e. OEMs/Vehicle Access Providers, ToD Technology Providers and ToD Service Providers.

The value exchanges described above are also summarised in the table below with value creation mechanisms shown in red and value capture mechanisms in green. It is interesting to notice that sometimes an exchange involves both mechanisms: for the delivery of the ToD Service, the OEM compensates the ToD Service Provider, while also contributing to value creation by exposing the necessary APIs. Similarly, ToD Service Providers compensate insurers, but also provide them with data that is necessary for the implementation of insurance policies.

		Main Roles					Enablers	Services	Customers	Authorities
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Cloud Service Providers	MNOs	Road Information Service Providers	Insurers	Users (Enterprises, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution	$					Compliance
	OEMs/Vehicle Access Providers	$		$, APIs	$	$			Vehicles	Compliance
	ToD Service Providers	$	ToD Service			$	$	$, Data		Compliance
	Cloud Service Providers	CloudServices	CloudServices							
	MNOs		Connectivity	Connectivity						
Enablers	Road Information Service Providers			Information						
Services	Insurers			Insurance						
Customers	Users (Enterprises, Consumers)		$							
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval						

Another important observation is that the only party that seems not to monetise its participation in this value network directly is OEMs. This is understandable if we consider that they are the ultimate consumer of the ToD service in their capacity as fleet owner users. Still, it is tempting to entertain the possibility that OEMs could at least contemplate carrying out the ToD service tasks themselves in settings where they are the users. In this case, where OEMs are also the ToD Service Providers, the table of exchanges would change as follows:

	Provides	Main Roles					Enablers	Services	Customers	Authorities
		ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Cloud Service Providers	MNOs	Road Information Service Providers	Insurers	Users (Enterprises, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution	$					Compliance
	OEMs/Vehicle Access Providers	$		APIs	$	$			Vehicles	Compliance
	ToD Service Providers		ToD Service				$	$, Data		Compliance
	Cloud Service Providers	Cloud Services	Cloud Services							
	MNOs		Connectivity	Connectivity						
Enablers	Road Information Service Providers			Information						
Services	Insurers			Insurance						
Customers	Users (Enterprises, Consumers)		$							
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval						

OEMs could possibly obtain better prices from ToD Technology Providers (for ToD Solutions), MNOs (for Control Centre connectivity) and Insurers than independent ToD Service Providers. From a business perspective, *ceteris paribus*, OEMs could assume these extra costs but avoid the expenditure of compensating ToD Service Providers for the same cost categories (but at higher prices) plus their profit margin.

Regarding go-to-market strategies, we will now examine what might make sense for ToD Service Providers to consider. Here, the analysis will focus on independent ToD Service Providers, because in the situation where OEMs execute the ToD tasks there is no need for a go-to-market strategy (the service provider and the service user are the same entity, and we may assume that no money would change hands even if different departments within the OEM are responsible for vehicle logistics and ToD service delivery). As can be seen below, we considered the possibility of an indirect go-to-market strategy option where the ToD Service Provider sells to a ToD Technology Provider who, in turn, sells to the OEM. While this option may be feasible, it will not be analysed independently (similar to the analysis above regarding business models), and the analysis that follows regarding pricing is likely to be similar for both direct and indirect sales channel approaches.

Go-to-Market Strategy options for ToD Service Providers selling to OEMs

Offering	Who To Sell	What To Sell	How To Sell	
			Channel	Approach
Delivery of ToD service	Vehicle OEMs	ToD service delivered as follows: - Support of Indirect and Direct Control modes of ToD, depending on type of vehicle and situation - Support of retrofit and factory fit ToD solutions as needed - Support of well-defined Operation Design Domains - With SLAs regarding the Control Centre, the time available for response to request for service and the time available for service delivery completion - With contract describing the insurance necessary to cover for liabilities related to humans and vehicles	Direct sales to OEMs with partner ToD Technology Provider(s)	Target partner's OEM customers, and bid to win their ToD business as sole/preferred provider
			Indirect sales to ToD Technology Provider(s)	Bid to win OEM's ToD business as sole/preferred provider
			Direct sales to OEMs	Bid to win OEM's ToD business as sole/preferred provider

Regarding pricing, the ToD Service in scenarios such as the one we are using here (moving vehicles from port to parking lot) could most likely be priced as a business service, with a fee for CC operator-hour, which could be scaled. No actual price modelling has been done, but for the purposes of illustrating a possible pricing structure the model could be, say, \$150 per CC operator-hour, for 0-10 hours per month, \$100/h for 10-100 hours/month, \$80/h thereafter. The hypothetical pricing scheme might involve a base price, as in the above for Indirect Control service, and a premium price (e.g. X%

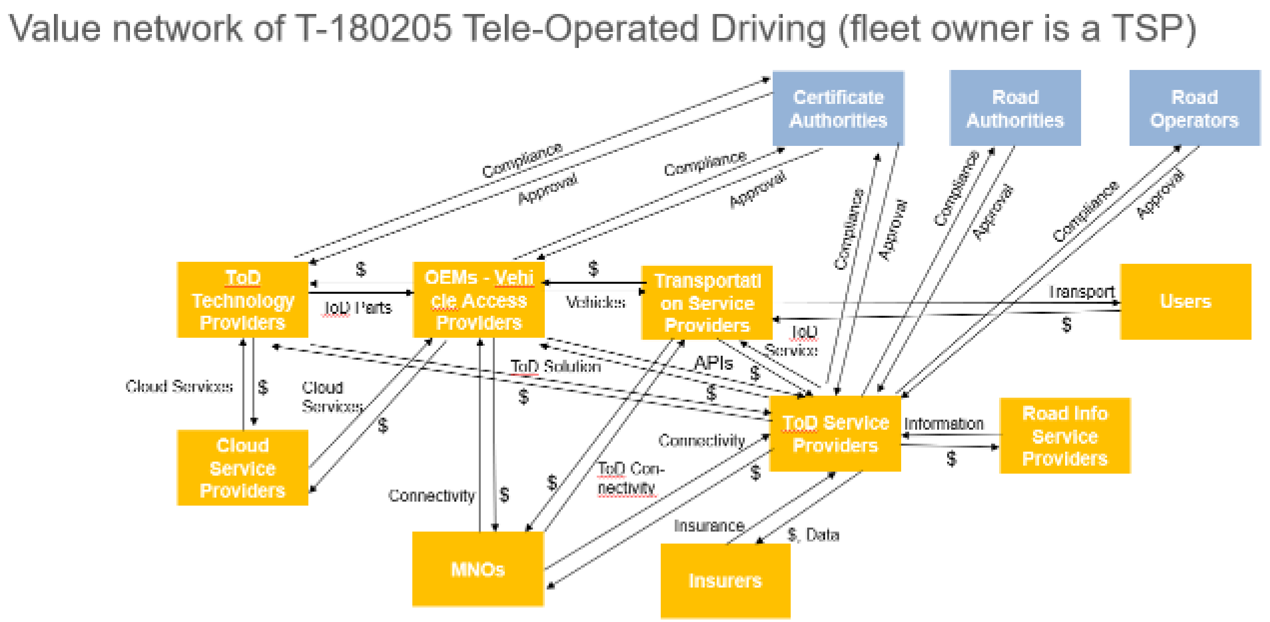
higher prices) for Direct Control service. The contract governing this service could be a multi-year agreement with SLA terms, and compensation could be based on CC operator occupation data verified by the OEM at ToD system usage level.

Now, it is time to analyse the scenario where the fleet owner is a Transportation Service Provider (a Carrier or Logistics Service Provider, a Public Transport company, a Ride Hailing service or Transportation Network Company, a Car Rental or Car Sharing company, etc.).

The first stage of the analysis focuses on the value network of the use case with the same characteristics as described above, but modified for the particular scenario. Only the relevant functional roles will be depicted (non-operational roles are shown in blue), and only the exchanges that have to do with ToD. It must be noted that although the user is a Transportation Service Provider, we will assume – judging from the description of the particular use case – that (paying) Passengers do not participate here. The fleet vehicles are being transported by means of ToD, empty of customers, from for instance a car rental parking lot in an airport to another 'Point of Presence' associated with the car rental agency downtown. This means that this scenario is situated as a standard trip on open public roads.

Value network of T-180205 Tele-operated Driving (fleet owner is a Transportation Service Provider)

This scenario represents situations where, for example, a Car Rental company has its vehicles moved by ToD from an



airport to a downtown Point of Presence. The value network cooperates in the following manner:

- ToD Technology Providers: they have supplied the OEM with the parts that implement ToD in the vehicle, and at the same time they have supplied the ToD solution (for which they use cloud services) to the entity that will deliver the ToD service.
- OEMs: they have integrated the ToD parts in their vehicles at the manufacturing stage and are exposing APIs to the ToD Service Providers that are necessary for the delivery of the ToD service (for which they are compensated). OEMs are using cloud services for their platform and connect their vehicles at all times using wholesale cellular connectivity (which does not cover the ToD connectivity needs though). Most importantly, they sell or lease their vehicles to the Transportation Service Provider.
- Cloud Service Providers: they offer various cloud services to OEMs and ToD Technology Providers.
- MNOs: they offer wholesale cellular connectivity to the OEMs' vehicles for all uses considered non-discretionary consumer services such as ToD (but are necessary for the vehicle's function), and for consumer cellular connectivity to Transportation Service Providers for such services as ToD, and also wholesale mobile and/or wireline connectivity to the ToD Service Providers for the delivery of the ToD service. [Note: we use the term 'consumer cellular connectivity' here to describe the connectivity that an MNO sells to a business customer, such as a Transportation Service Provider, to cover the needs stemming from 'discretionary' services which are up to the customer to decide when and how much to consume (i.e. ToD or fleet management). A Transportation Service Provider may choose to use ToD for a vehicle many times a day, with each use generating high volumes of cellular data traffic, especially

from the vehicle’s sensors to the Control Centre. It could be considered fair that the business customer might pay for this use, rather than the OEM.]

- Road Information Service Providers: they provide information on road conditions to the ToD Service Providers.
- ToD Service Providers: they offer the ToD service to the Transportation Service Provider. The service is enabled using different components: a ToD solution supplied by the ToD Technology Provider, connectivity by the MNO, road information by the Road Information Service Provider, and access to APIs exposed by the OEM. The liability of the ToD Service Provider could be covered by insurance for the ToD tasks.
- Transportation Service Providers acquire or lease vehicles from the OEMs, and enjoy ToD services offered by the ToD Service Providers, for which they also need fleet cellular connectivity which they source from MNOs.
- Users are the consumers or enterprises that will eventually make use of the vehicle in the Transportation Service Provider’s fleet being remotely driven to their intended destination. Users could pay to use the transportation service, and a part of their fee could go indirectly towards compensating the party delivering the ToD service.
- Insurers: they offer insurance to the ToD Service Providers, making use of data obtained from them related to the ToD tasks being insured.
- Certificate Authorities, Road Authorities and Road Operators: these roles are non-operational in this scenario, as they do not contribute input necessary for the delivery of the ToD service per se. Nevertheless, they approve the operation of ToD Service Providers in their jurisdiction and they offer certification of the parties that are critical in the implementation and delivery of the ToD service, i.e. OEMs/Vehicle Access Providers, ToD Technology Providers and ToD Service Providers.

The value exchanges described above are also summarised in the table below with value creation mechanisms shown in red and value capture mechanisms in green. It is interesting to note that sometimes an exchange involves both mechanisms: ToD Service Providers compensate insurers, but also provide them with data that is necessary for the implementation of insurance policies.

		Main Roles						Enablers	Services	Customers	Authorities
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Transportation Service Providers	Cloud Service Providers	MNOs	Road Information Service Providers	Insurers	Users (Enterprises, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution		$					Compliance
	OEMs/Vehicle Access Providers	$		APIs	Vehicles	$	$				Compliance
	ToD Service Providers	$	$		ToD Service		$	$	$, Data		Compliance
	Transportation Service Providers		$	$			$			Transport	
	Cloud Service Providers	Cloud Services	Cloud Services								
	MNOs		Connectivity	Connectivity	ToD Connectivity						
Enablers	Road Information Service Providers			Information							
Services	Insurers			Insurance							
Customers	Users (Enterprises, Consumers)				$						
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval							

Another important observation is that Transportation Service Providers (TSP), in parallel with being the ultimate consumer of the ToD service in their capacity as fleet owner users, can contemplate carrying out the ToD service tasks themselves. There are multiple reasons why this might make business sense. They could avoid paying a profit margin for the service to a ToD Service Provider, they could avoid becoming dependent on any one OEM, and most importantly they could use the ToD capability, assets and skills to deliver ToD to their own customers (e.g. citizens renting an AV). ToD would complement their core business (e.g. car rental), benefit the company in terms of efficiencies from economies of scale, and could be directly monetisable as an add-on offering. In this case, where TSPs are also the ToD Service Providers, the table of exchanges could change as follows:

	Provides →	Main Roles						Enablers	Services	Customers	Authorities
		ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Transportation Service Providers	Cloud Service Providers	MNOs	Road Information Service Providers	Insurers	Users (Enterprises, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution		$					Compliance
	OEMs/Vehicle Access Providers	$		APIs	Vehicles	$	$				Compliance
	ToD Service Providers	$	$		ToD Service		$	$	$, Data		Compliance
	Transportation Service Providers									Transport	
	Cloud Service Providers	Cloud Services	Cloud Services								
	MNOs		Connectivity	Connectivity	ToD Connectivity						
Enablers	Road Information Service Providers			Information							
Services	Insurers			Insurance							
Customers	Users (Enterprises, Consumers)				$						
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval							

Turning now to the study of go-to-market strategies, we will examine what could make sense for ToD Service Providers when the user is a TSP. Here, the analysis will focus on independent ToD Service Provider companies, because in the case where TSPs execute the ToD tasks there is no need for a go-to-market strategy (the service provider and the service user are the same entity, and we may safely assume that no money changes hands even if different departments within the TSP are responsible for vehicle logistics and for ToD service delivery). As can be seen below, we explore three options: 1) the ToD Service Provider could leverage relations with a partner OEM and seek to sell directly to the TSP customer when the partnership OEM-ToD service provider bids in a TSP AV RFP, 2) the ToD Service Provider could sell indirectly by offering the service to its OEM partner, who in turn could bid for the whole package deal (vehicles plus ToD) in the TSP customer's AV RFP, or 3) the ToD Service Provider could bid directly for the ToD service part of a TSP AV RFP. The analyses above regarding business models, and the analysis that follows regarding pricing, could be applicable for both direct and indirect sales channel approaches.

Go-to-Market Strategy options for ToD Service Providers selling to TSPs

Offering	Who To Sell	What To Sell	How To Sell: Channel	How To Sell: Approach
Delivery of ToD service	Transportation Service Providers	ToD service delivered as follows: - Support of Indirect and Direct Control modes of ToD, depending on type of vehicle and situation - Support of retrofit and factory fit ToD solutions as needed - Support of well-defined Operation Design Domains - With SLAs regarding the Control Centre, the time available for response to request for service and the time available for service delivery completion - With contract describing the insurance necessary to cover for liabilities related to humans and vehicles	Direct sales to TSPs with partner OEM	Target OEM partner's TSP customers, and bid to win their ToD business as sole/preferred provider
			Indirect sales through OEM	In OEM partner's bid to win TSP's business, seek role as sole /preferred provider of ToD part of the solution
			Direct sales to TSPs	Target TSPs, and bid to win their ToD business as sole/preferred provider

Regarding pricing, the ToD Service in scenarios, such as the one we are using here (moving vehicles from airport to city centre), could be priced as a business service, with a fee for CC operator-hour, which could be scaled. Again, no actual price modelling has been done, but to illustrate the concept a price structure could include $150 per CC operator-hour, for 0-10 hours per month, $100/h for 10-100 hours/month, and $80/h thereafter. The pricing scheme might involve a base price such as the above for Indirect Control service, and a premium price (e.g. X% higher prices) for Direct Control service. The contract governing this service could be a multi-year agreement with SLA terms, and compensation could be based on CC operator occupation data verified by the TSP at ToD system-usage level.

T-180206 Tele-operated Driving Support

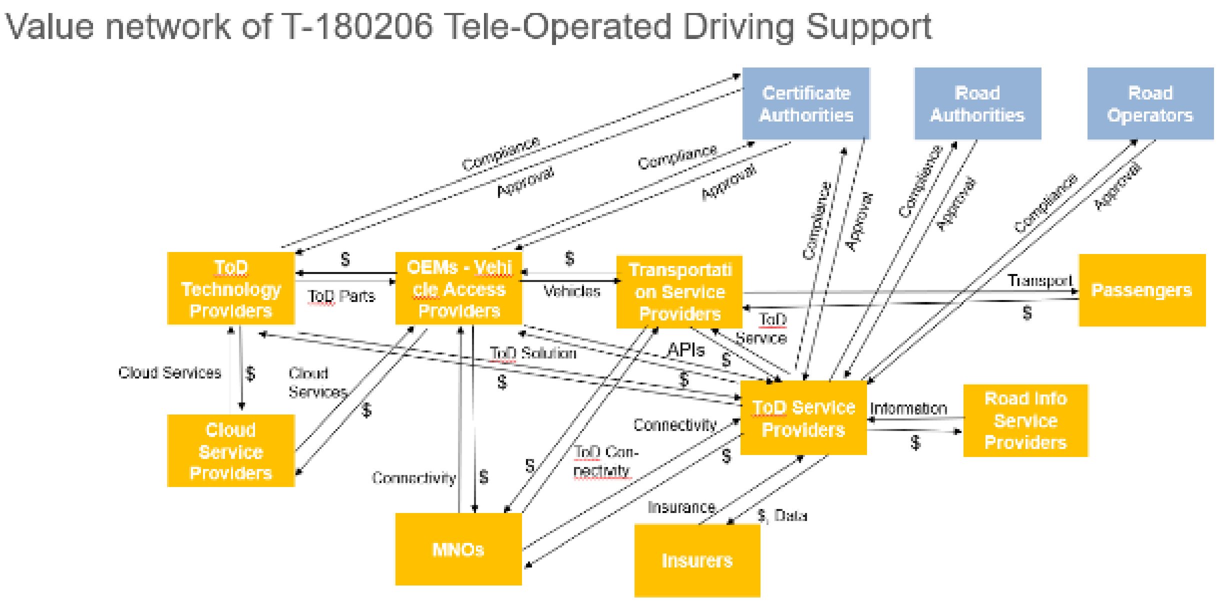
The second use case to be analysed is T-180206 Tele-operated Driving Support, with the following important constraints: the service is provided by one ToD provider to a single OEM fleet owner, in a confined area (green zone) or following a pre-determined route, for a short period of time (e.g. by providing a driving manoeuvre), and applies to every occasion in which the automated vehicle is facing highly uncertain situations, making decision-making difficult. Such occasions include the following examples: if mandated by regulation (geo-fenced areas such as a construction site), when commandeered by authorities, and in emergency situations. The nature of the occasions where engaging ToD is needed, according to the use case description, leads us to conclude that the availability of the service is not discretionary; rather it is mandatory for the approval of the operation of the AV fleet in the green zone (or route), even though it will be needed on an on-demand basis, if needed at all. There is no important differentiation in terms of business analysis between Indirect Control and Direct Control implementations of ToD, so the following sections apply to either mode, unless otherwise noted.

There are a number of assumptions regarding functional roles defined in Chapter 7 that will be made in order to ensure that the business analysis of the use case represents realistic situations. Namely:

- The Vehicle Access Provider is the OEM. Factory-fit ToD solutions are assumed to be the norm, as opposed to retrofit solutions. In such a case, the OEM will be the Vehicle Access Provider so they can control access to the ToD technology and the service, while also controlling who will play the role of the ToD Service Provider over time.
- The MNO is the Internet Service Provider, as most telecommunication providers offer both mobile and fixed services.
- For the particular use case, as described in Chapter 4, there is no involvement of Shippers, Interchange Service Providers, or Infrastructure Service Providers.
- The fleet owner is the user of the service. To maximise the applicability of the business analysis that follows, we will assume that it is a Transportation Service Provider, e.g. a public transport company operating automated shuttle buses to transport citizens within a green zone and along pre-determined routes.

  The first stage of the analysis focuses on the value network of the use case with the characteristics described above. Only the relevant functional roles will be depicted (non-operational roles are shown in blue), and only the exchanges that have to do with ToD:

<u>Value network of T-180206 Tele-operated Driving Support</u>



The value network cooperates in the following manner:

- ToD Technology Providers: they have supplied the OEM with the parts that implement ToD in the vehicle, and at the same time they have supplied the ToD solution (for which they use cloud services) to the entity that will deliver the ToD service.
- OEMs: they have integrated the ToD parts in their vehicles at the manufacturing stage and are exposing APIs to the ToD Service Providers necessary for the delivery of the ToD service (for which they are compensated). OEMs are using cloud services for their platform and connect their vehicles at all times using wholesale cellular connectivity (which does not cover the ToD connectivity needs though). Most importantly, they sell or lease their vehicles to the Transportation Service Provider.
- Cloud Service Providers: they offer various cloud services to OEMs and ToD Technology Providers.
- MNOs: they offer wholesale cellular connectivity to the OEMs' vehicles for all uses that are not ad-hoc or urgent in nature, but are necessary for the vehicle's regular function, and they offer consumer cellular connectivity to Transportation Service Providers for services such as ToD, and also wholesale mobile and/or wireline connectivity to the ToD Service Providers for the delivery of the ToD service. [Note: we use the term 'consumer cellular connectivity' here the same way as in the previous use case.]
- Road Information Service Providers: they provide information on road conditions to the ToD Service Providers.
- ToD Service Providers: they offer the ToD service to the fleet owner user, which is the Transportation Service Provider in this case. The service is enabled using different components: a ToD solution supplied by the ToD Technology Provider, connectivity by the MNO, road information by the Road Information Service Provider, and access to APIs exposed by the OEM. The liability of the ToD Service Provider is covered by insurance for the ToD tasks. It must be noted that, in the scenario discussed here, it is unlikely that an OEM would play this role, because shuttle bus OEMs sell globally, without necessarily having the capability to offer services such as ToD in all territories they serve. The ToD service requires purpose-built equipment and local presence that guarantees the necessary low latency, therefore we may assume that the ToD Service Provider is a local player. Likewise, given the occasional and unplanned need for emergency ToD Support, as defined in this use case, it is unlikely that a TSP could itself provide the ToD service for its own fleet vehicles. Only a player serving a wider market within the territory would be likely to have the economies of scale to deliver the ToD Support service in a profitable manner.
- Transportation Service Providers acquire or lease vehicles from the OEMs to offer transport services to Passengers, and enjoy ToD services offered by the ToD Service Providers, for which they also need fleet cellular connectivity sourced from MNOs.
- Passengers are the paying customers of Transportation Service Providers.
- Insurers: they offer insurance to the ToD Service Providers, making use of data obtained from them related to the ToD tasks being insured.
- Certificate Authorities, Road Authorities and Road Operators: these roles are non-operational in this scenario, as they do not contribute inputs necessary for the delivery of the ToD service per se. Nevertheless, they approve the operation

of ToD Service Providers in their jurisdiction and they offer certification of the parties that are critical in the implementation and delivery of the ToD service, i.e. OEMs/Vehicle Access Providers, ToD Technology Providers and ToD Service Providers.

The value exchanges described above are also summarised in the table below with value creation mechanisms shown in red and value capture mechanisms in green. It is interesting to notice that sometimes an exchange involves both mechanisms: ToD Service Providers compensate insurers, but also provide them with data that is necessary for the implementation of insurance policies.

		Main Roles						Enablers	Services	Customers	Authorities
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Transportation Service Providers	Cloud Service Providers	MNOs	Road Information Service Providers	Insurers	Passengers	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution		$					Compliance
	OEMs/Vehicle Access Providers	$		APIs	Vehicles	$	$				Compliance
	ToD Service Providers	$	$		ToD Service		$	$	$, Data		Compliance
	Transportation Service Providers		$	$			$			Transport	
	Cloud Service Providers	Cloud Services	Cloud Services								
	MNOs		Connectivity	Connectivity	ToD Connectivity						
Enablers	Road Information Service Providers			Information							
Services	Insurers			Insurance							
Customers	Passengers				$						
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval							

Turning now to the study of go-to-market strategies, we will examine what could make sense for independent ToD Service Providers. As can be seen below, we discuss three options: 1) the ToD Service Provider can leverage relations with a partner OEM and seek to sell directly to the TSP user when the partnership OEM-ToD service provider bids in a TSP AV RFP, 2) the ToD Service Provider may sell indirectly by offering the service to its OEM partner, who in turn will bid for the whole package deal (vehicles plus ToD) in the TSP customer's AV RFP, or 3) the ToD Service Provider bids directly for the ToD service part of a TSP AV RFP. The analyses above regarding business models, and the analysis that follows regarding pricing, are applicable for both direct and indirect sales channel approaches.

Go-to-Market Strategy options for ToD Service Providers selling to TSPs

Offering	Who To Sell	What To Sell	How To Sell	
			Channel	Approach
Delivery of ToD service	Transportation Service Providers	ToD service delivered as follows: - Support of Indirect and Direct Control modes of ToD, depending on type of vehicle and situation - Support of retrofit and factory fit ToD solutions as needed - Support of well-defined Operation Design Domains - With SLAs regarding availability of service, issue categorization, time of response to request for service, problem resolution, and service quality - With contract describing the insurance necessary to cover for liabilities related to humans and vehicles	Direct sales to TSPs with partner OEM	Target OEM partner's TSP customers, and bid to win their ToD business as sole/preferred provider
			Indirect sales through OEM	In OEM partner's bid to win TSP's business, seek role as sole/preferred provider of ToD part of the solution
			Direct sales to TSPs	Target TSPs, and bid to win their ToD business as sole/preferred provider

Regarding pricing, the ToD Service in scenarios such as the one we are using here (shuttle bus moving in green zone that faces an emergency situation for which the invocation of ToD Support is mandated) could potentially be priced as a premium business service. Given the on-demand nature of the service, the potential severity of situations, the liability of the ToD SP, and the uncertain duration of service delivery per incident, a mixed fee model might be workable. For example, a base fee of $50 per incident could be charged, which grants the TSP user 10 minutes of a CC operator's time, over which a charge of $15 for every subsequent five-minute intervals could be applied (as above, no actual modelling has been done – this merely models the concept). The pricing scheme could involve a base price, just as above for Indirect Control service, and a premium price (e.g. X% higher prices) for Direct Control service. The contract governing this service could be a multi-year agreement with SLA terms covering the entire vehicle fleet of the TSP, and compensation could be based on CC operator occupation data verifiable by the TSP at ToD system-usage level. It must also be noted that Passenger fees might not vary according to the use of ToD Support by the TSP, which is transparent to them. Fees could be priced so that they provide adequate compensation of the TSP for the transportation service, whichever way it is delivered.

T-180207 Tele-operated Driving for Automated Parking

The third use case to be analysed is T-180207 Tele-operated Driving for Automated Parking. The use case refers to two distinct contexts (parking in constrained/confined areas such as AV OEM factories, and parking in garages or seaports) and the business analysis differs considerably from case to case. To be precise, the first setting where the fleet owner user is the OEM follows the business logic presented earlier for T-180205 Tele-operated Driving (fleet owner is the OEM), so the analysis will not be repeated here for either the Direct or Indirect Control mode. The second setting will be studied under the following constraints: the service is provided by one ToD SP to vehicles coming from different OEMs and connected by different MNOs, and consists of automated parking of vehicles using ToD in constrained/confined areas (e.g. garages or seaports).

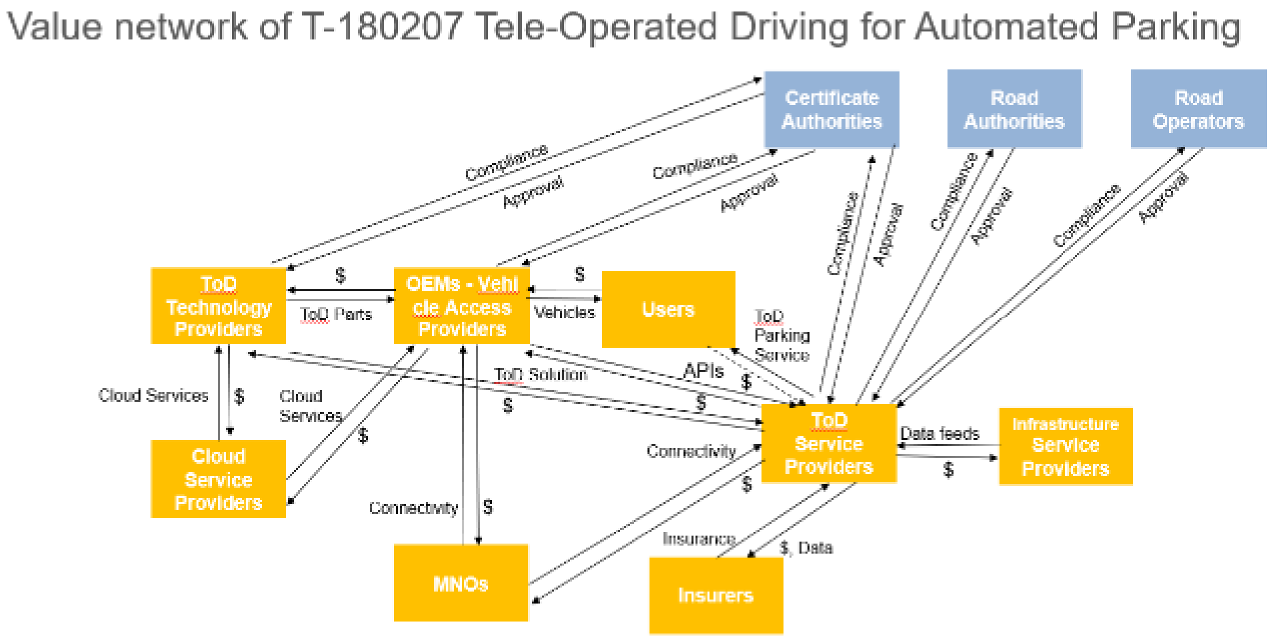
This context points us to assume that the vehicles to be parked may have a single or multiple owners and users, either fleet owner(s) or consumers. The analysis will apply to all possible combinations. There is no important differentiation in terms of business models and go-to-market strategies between Indirect Control and Direct Control implementations of ToD, so the following sections apply to either mode, unless otherwise noted.

There are a number of assumptions regarding functional roles defined in Chapter 7 that will be made in order to ensure that the business analysis of the use case represents realistic situations. Namely:

- The Vehicle Access Provider is the OEM. Factory-fit ToD solutions are assumed to be the norm, as opposed to retrofit solutions. In such a case, the OEM will be the Vehicle Access Provider so that they can control access to the ToD technology and the service, while also controlling who will play the role of the ToD Service Provider over time.
- The MNO is the Internet Service Provider, as most telecommunication providers offer both mobile and fixed services.
- For the particular use case, as described in Chapter 4, there is no involvement of Shippers, Interchange Service Providers, or Passengers (it is assumed that the vehicles are parked without passengers in them).
- The role of Road Authorities and Road Operators will be similar to the one described in the previous use cases, if we assume that even a confined area such as a seaport terminal may use services from a Road Operator and may be under the supervision of a Port Authority dictating what vehicles and uses are permitted.
- There will be no involvement of Road Information Service Provider but there will be a potential contribution from an Infrastructure Service Provider supporting the ToD function through the supply of additional video feeds, for example. We will assume that the terminal owner or parking operator will be the party actually fulfilling this role, but we will not discuss the case where automated vehicle control functions can take over the vehicle from a human ToD operator. Rather, we assume that the safety regulations and insurance policies in place dictate the delivery of automated parking by a human.
- A fleet owner or a consumer is the user of the service, or both. To maximise the applicability of the business analysis that follows we will assume that the automated parking service is available to all entities and individuals regardless of the vehicle make and the MNO used for cellular connectivity.

The first stage of the analysis focuses on the value network of the use case with the characteristics described above. Only the relevant functional roles will be depicted (non-operational roles are shown in blue), and only the exchanges that have to do with ToD:

Value network of T-180207 Tele-operated Driving for Automated Parking (not applicable for AV OEM factories)



The value network cooperates in the following manner:

- ToD Technology Providers: they have supplied the OEM with the parts that implement ToD in the vehicle, and at the same time they have supplied the ToD solution (for which they use cloud services) to the entity that will deliver the ToD service.
- OEMs: they have integrated the ToD parts in their vehicles at the manufacturing stage and are exposing APIs to the ToD Service Providers that are necessary for the delivery of the ToD service (for which they are compensated). OEMs are using cloud services for their platform and connect their vehicles at all times using wholesale cellular connectivity (which also covers the connectivity needs of the ToD Parking, as ToD Parking must be operational at all times – regardless of user actions – for safety reasons, hence for the use case to be feasible). Most importantly, they sell or lease their vehicles to the users. Vehicles from multiple OEMs, connected by different MNOs, can partake in the use case at the same time.
- Cloud Service Providers: they offer various cloud services to OEMs and ToD Technology Providers.
- MNOs: they offer wholesale cellular connectivity to the vehicle OEMs (different OEMs may be served by different MNOs), and for all uses that are not discretionary consumer services (e.g. infotainment or fleet management) but are necessary for the vehicle's function (including ToD Parking, which must be operational at all times, and not rely on user actions, following initial activation), and also wholesale mobile and/or wireline connectivity to the ToD Service Providers for the delivery of the ToD service. [Note: we assume that ToD Parking will be performed in an efficient manner, and on an as-needed basis, so that it does not consume excessive data volumes.]
- Infrastructure Service Providers: they provide additional data (e.g. video feeds) to the ToD Service Providers.
- ToD Service Providers: they offer the ToD service to the users, which is enabled using different components: a ToD solution supplied by the ToD Technology Provider, connectivity by the MNO, additional data feeds from the Infrastructure Service Provider, and access to APIs exposed by the OEMs. The liability of the ToD Service Provider is covered by insurance for the ToD tasks. It must be noted that the ToD service provider will be served by a single MNO, but it will have deals with different OEMs to have access to their ToD APIs and will be enabled to tele-operate vehicles regardless of which MNO connects the vehicle to the cellular network.
- Users acquire or lease vehicles from the OEMs, and enjoy ToD services offered by the ToD Service Providers. Users include individual consumers and fleet owners, both of which pay for the parking service, including the capability to handle parking tasks through ToD. Therefore, there are no separate fees paid by users for ToD Parking per se, but part of the parking fees go – indirectly (denoted by a dashed line), through the parking operator – towards the ToD Service Providers' compensation for the ToD Parking service.
- Insurers: they offer insurance to the ToD Service Providers, making use of data obtained from them related to the ToD tasks being insured.
- Certificate Authorities, Road Authorities and Road Operators: these roles are non-operational in this scenario, as they do not contribute inputs necessary for the delivery of the ToD service per se. Nevertheless, they approve the operation of ToD Service Providers in their jurisdiction and they offer certification of the parties that are critical in the implementation and delivery of the ToD service, i.e. OEMs/Vehicle Access Providers, ToD Technology Providers and ToD Service Providers.

The value exchanges described above are also summarised in the table below with value creation mechanisms shown in red and value capture mechanisms in green. It is interesting to note that sometimes an exchange involves both mechanisms: ToD Service Providers compensate insurers, but also provide them with data that is necessary for the implementation of insurance policies.

		Main Roles					Enablers	Services	Customers	Authorities
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	ToD Service Providers	Cloud Service Providers	MNOs	Service Providers	Insurers	Users (Fleet Owners, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	ToD Solution	$					Compliance
	OEMs/Vehicle Access Providers	$		APIs	$	$			Vehicles	Compliance
	ToD Service Providers	$	$			$	$	$, Data	ToD Parking Service	Compliance
	Cloud Service Providers	Cloud Services	Cloud Services							
	MNOs		Connectivity	Connectivity						
Enablers	Infrastructure Service Providers			Information						
Services	Insurers			Insurance						
Customers	Users (Fleet Owners, Consumers)		$	$						
Authorities	Certification, Road Authorities &Operators	Approval	Approval	Approval						

An important observation is that the Parking or Seaport Terminal Operators could be very well positioned to offer the ToD Parking service. Assuming their scale allows them to deliver this service cost effectively (also taking into account the necessary investments for generating video feeds in their role as Infrastructure Service Provider), they could offer it themselves rather than pay another party to do it on their premises. In this case, they could be compensated – directly – by users' fees for both the right to park and for the valet parking task, and the table of exchanges could change as follows:

		Main Roles					Enablers	Services	Customers	Authorities
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	Cloud Service Providers	MNOs	ToD Service Providers	Infrastructure Service Providers	Insurers	Users (Fleet Owners, Consumers)	Certification, Road Authorities & Operators
Main Roles	ToD Technology Providers		ToD Parts	$		ToD Solution				Compliance
	OEMs/Vehicle Access Providers	$		$	$	APIs			Vehicles	Compliance
	Cloud Service Providers	Cloud Services	Cloud Services							
	MNOs		Connectivity			Connectivity				
	ToD Service Providers	$	$					$, Data	ToD Parking Service	Compliance
Enablers	Infrastructure Service Providers					Data Feeds				
Services	Insurers					Insurance				
Customers	Users (Fleet Owners, Consumers)		$			$				
Authorities	Certification, Road Authorities & Operators	Approval	Approval			Approval				

Turning now to the study of go-to-market strategies and pricing principles, we will examine what could make sense for independent ToD Service Providers, and for Parking Operators delivering the ToD Parking service themselves. The analysis is simple in the sense that there is only one strategy (going 'directly' to customers) that might apply in both cases:

If the ToD Service Provider is an independent company targeting Parking Operators as customers, they need to go for economies of scale and deliver a cost-effective service, while also supplying the infrastructure for additional video feeds to improve their margin. On top of a set-up fee, they are likely to price their service by the number of cars parked. This scheme (e.g. $1 per car parked, but with a proper SLA in place to secure people and vehicles) aligns the incentives of Parking Operator and ToD Parking SP: the Parking Operator has costs that are easy to forecast, and minimises the time that the ToD service provider will spend in service delivery per vehicle (and indirectly the connectivity costs incurred in this task, which the OEM pays).

If the ToD Service Provider is the Parking Operator, it could target consumers and fleet owners with an end-to-end parking service, which could maximise convenience for the users and command a premium price. Obviously, fleet owners might be able to get a better deal per car than consumers since they are buying at bulk prices. Again, scale is how the margin can be maximised, and under the right conditions could be achieved if the service provider can serve additional parking lots/seaport terminals (which they do not own) for the valet parking services.

The pricing scheme could involve a base price, as above for Indirect Control service, and a premium price (e.g. X% higher prices) for Direct Control service.

T-190062 Infrastructure-based Tele-operated Driving

The last use case to be analysed is T-190062 Infrastructure-based Tele-operated Driving. The use case refers to contexts where ToD, based on environment perception provided by sensors outside the vehicle, is required. Such contexts can be encountered when the vehicle's own sensory or computational capabilities are failing, their efficacy is considered uncertain, or the on-board sensor coverage is not sufficient. Such problems with on-board systems – and the solution given by infrastructure-based ToD – may occur in various settings, either public areas or special zones, which are controlled environments (hence an entity can install and operate special ToD-supporting infrastructure) but with special challenges for AVs (hence the need for this type of ToD). Such a setting can be a tunnel on the border between two countries with special lanes for AVs executing pre-defined routes (e.g. a commuting service), and we will use this example to make the use case come alive. There is no important differentiation in terms of business models and go-to-market strategies between having a human or a machine as remote operator, so the following sections apply to either mode, unless otherwise noted.

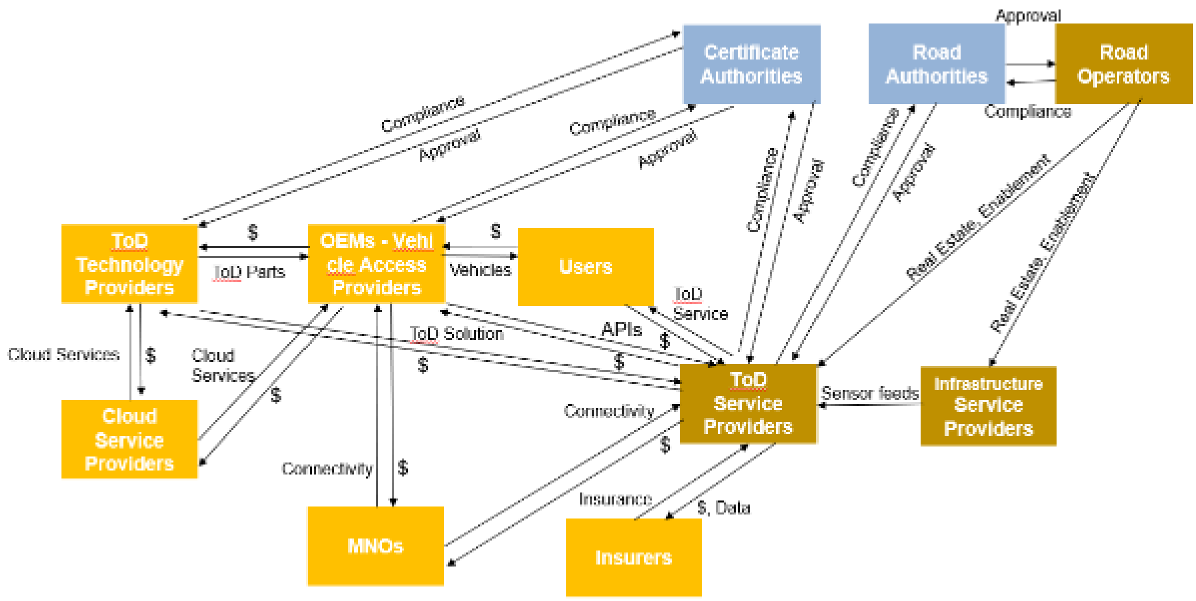
There are a number of assumptions regarding functional roles defined in Chapter 7 that will be made in order to ensure that the business analysis of the use case represents realistic situations. Namely:

- The Vehicle Access Provider is the OEM. Factory-fit ToD solutions are assumed to be the norm, as opposed to retrofit solutions. In such a case, the OEM will be the Vehicle Access Provider so that they can control access to the ToD technology and the service, while also controlling who will play the role of the ToD Service Provider over time.
- The MNO is the Internet Service Provider, as most telecommunication providers offer both mobile and fixed services.
- For the particular use case, as described in Chapter 4, there is no involvement of Interchange Service Providers.
- The role of Road and Certificate Authorities will be similar to the one described in the previous use cases, but the Road Operator (or more precisely the Tunnel Operator in the scenario we are discussing) is a role that has special significance in this use case as it is the entity that will enable and deliver the infrastructure-based ToD service, i.e. acting as the ToD service provider under the most plausible business scenario.
- There will be no Road Information Service Provider involvement but there will be vital contribution from the Infrastructure Service Provider that will enable the ToD function through the supply and operation of infrastructure-based sensors, external to the vehicles.
- Fleet owners and consumers are both users of the service, and in general they carry Passengers (for example, workers living in one country and working in the neighbouring one in the cross-border commuting service scenario). Of course, a Shipper or a Transportation Service Provider can be the actual owner of the fleet (for example, a ride sharing company serving the commuters). To maximise the applicability of the business analysis that follows, we will assume that the infrastructure-based ToD service is available to all entities and individuals regardless of the vehicle make and the MNO used for regular cellular connectivity of the vehicle.

The first stage of the analysis focuses on the value network of the use case with the characteristics described above. Only the relevant functional roles will be depicted (non-operational roles are shown in blue), and only the exchanges that have to do with ToD. The three roles played by the same entity (Tunnel Operator) in our scenario are shown in brown.

Value network of T-190062 Infrastructure-based Tele-operated Driving

Value network of T-190062 Infrastructure-based Tele-Operated Driving



The value network cooperates in the following manner:

- ToD Technology Providers: they have supplied the OEM with the parts that implement ToD in the vehicle, and at the same time they have supplied the ToD solution (for which they use cloud services) to the entity that will deliver the ToD service.
- OEMs: they sell or lease their vehicles to the users. Also, they have integrated the ToD parts in their vehicles at the manufacturing stage and are exposing APIs to the ToD Service Providers that are necessary for the delivery of the ToD service (for which they are compensated). OEMs are using cloud services for their platform and connect their vehicles at all times using wholesale cellular connectivity (each OEM with a different MNO, potentially). The wholesale connectivity deal of each OEM will also cover the connectivity needs of infrastructure-based ToD for two reasons: 1) infrastructure-based ToD must be operational at all times – regardless of user actions – for safety reasons, hence for the use case to be feasible; 2) connectivity in the setting chosen for the scenario (cross-border tunnel) may be available by just one operator at a time (MNO X on 'this' side of the border, and MNO Y on the 'other' side), therefore connectivity for each vehicle in the specific area must be provided through roaming agreements of the different MNOs originally serving the different OEMs, and the two MNOs providing coverage in the tunnel for seamless session continuity (hence secure operation even in low-latency use cases such as ToD).
- Cloud Service Providers: they offer various cloud services to OEMs and ToD Technology Providers.
- MNOs: they offer wholesale cellular connectivity for the vehicles to the OEMs (different OEMs may be served by different MNOs), for all uses that are not discretionary consumer services (i.e. infotainment or fleet management) but are necessary for the vehicle's function (including infrastructure-based ToD, which must be operational at all times, and not rely on user actions, as explained above), and also for wholesale mobile and/or wireline connectivity to the ToD Service Providers for the delivery of the ToD service. [Note: we assume that one MNO will supply the entity – e.g. Tunnel Operator – that will serve concurrently as Road Operator, Infrastructure Service Provider and ToD SP. Also, we assume that infrastructure-based ToD will be performed in an efficient manner, and on an as- needed basis, so that it does not consume excessive data volumes.]
- Infrastructure Service Providers: they provide external sensor feeds to the ToD Service Providers.
- ToD Service Providers: they offer the infrastructure-based ToD service to the users, which is enabled using different components: a ToD solution supplied by the ToD Technology Provider, connectivity by the MNO, external sensor feeds from the Infrastructure Service Provider, and access to APIs exposed by the OEMs. The liability of the ToD Service Provider is covered by insurance for the ToD tasks. It must be noted that the ToD SP will be served by a single MNO, but it will have deals with different OEMs to have access to their ToD APIs and will be enabled to tele-operate vehicles regardless of which MNO originally connects the vehicle to the cellular network (because the MNO of the Road Operator/ToD SP will have session continuity agreements with MNOs serving the different makes to enable the vehicles to be operational in the tunnel).
- Road Operators: under the constraints described for this use case, the Road Operator is the party best positioned to act as Infrastructure Service Provider (as the entity controlling the zone's infrastructure, a natural monopoly really) and to perform the task of the infrastructure-based ToD SP for this zone (as the entity that can do this in the most cost-effective manner). To describe the different roles that this entity (e.g. Tunnel Operator) plays, we may say that

under the hat of Road Operator they provide real estate and overall enablement (utilities, personnel etc.) to both their ToD SP and Infrastructure SP subdivisions.

- Users acquire or lease vehicles from the OEMs, and enjoy ToD services offered by the ToD Service Providers. Users include individual consumers and fleet owners, both of which pay for the infrastructure-based ToD service.
- Insurers: they offer insurance to the ToD Service Providers, making use of data obtained from them related to the ToD tasks being insured.
- Certificate Authorities and Road Authorities: these roles are non-operational in this scenario, as they do not contribute inputs necessary for the delivery of the ToD service per se. Nevertheless, they approve the operation of ToD Service Providers and Road Operators in their jurisdiction, and they offer certification of the parties that are critical in the implementation and delivery of the ToD service, i.e. OEMs/Vehicle Access Providers, ToD Technology Providers and ToD Service Providers.

The value exchanges described above are also summarised in the table below with value creation mechanisms shown in red and value capture mechanisms in green. It is interesting to note that sometimes an exchange involves both mechanisms: ToD Service Providers compensate insurers, but also provide them with data that is necessary for the implementation of insurance policies. As expected, it is assumed that the same entity (e.g. Tunnel Operator) will play the roles of ToD SP, Infrastructure SP and Road Operator.

		Main Roles					Enablers	Services	Customers	Authorities	
	Provides	ToD Technology Providers	OEMs/Vehicle Access Providers	Cloud Service Providers	MNOs	ToD Service Providers	Infrastructure Service Providers	Insurers	Users (Fleet Owners, Consumers)	Certification and Road Authorities	Road Operators
Main Roles	ToD Technology Providers		ToD Parts	$		ToD Solution				Compliance	
	OEMs/Vehicle Access Providers	$		$	$	APIs			Vehicles	Compliance	
	Cloud Service Providers	Cloud Services	Cloud Services								
	MNOs		Connectivity			Connectivity					
	ToD Service Providers	$	$					$, Data	ToD Service	Compliance	
Enablers	Infrastructure Service Providers					Sensor Feeds					
Services	Insurers					Insurance					
Customers	Users (Fleet Owners, Consumers)		$			$					
Authorities	Certification and Road Authorities	Approval	Approval			Approval					Approval
	Road Operators					Real estate, enablement				Compliance	

Turning now to the study of go-to-market strategies and pricing principles for this scenario, we may observe that the analysis is simple in the sense that there is only one strategy (going ‘directly’ to customers) that could apply in the use case scenario we presented. When the Road Operator is also the Infrastructure Service Provider and the infrastructure-based ToD SP, it targets the consumers and fleet owners who make use of its road infrastructure. Regardless of the existence of tolls, the infrastructure-based ToD service will likely charge its own fees that will essentially compensate the ToD SP according to parameters such as: date and time of infrastructure-based ToD invocation, class of vehicle, section of the zone where the ToD service was needed, distance travelled with the infrastructure-based ToD capability engaged. Also, the pricing scheme could involve a base price for Indirect Control service, and a premium price (e.g. X% higher prices) for Direct Control service.

11 Conclusion

The work presented in this document focused on business considerations in the domain of Tele-operated Driving. It does not pretend to provide an exhaustive analysis of all possible challenges and the corresponding solutions regarding business models, governance challenges or go-to-market constraints. But it does aspire to identify the different elements that should be taken into account when considering the deployment of a ToD ecosystem from a business perspective, including initial stakeholder identification, detailing of operational processes, identification of go-to-market constraints, and examples on how the business modelling techniques defined in the 5GAA BARNS work item [5] can also be applied to different deployment scenarios.

This document thus provides valuable first insights and inspiration to enable stakeholders with a keen interest in realising and deploying Tele-operated Driving products to commence with their own business and governance modelling, taking specific (individual) characteristics of the deployment scenario into account, and making use of the generic considerations and methodologies that were introduced in this study.

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see https://5gaa.org

5GAA Automotive Association