Deliverable **D4.3** /

“Fleet Preparation and Support” Summary Report

Version: 1.0 Final

Dissemination level: PU

Lead contractor: RENAULT GROUP

Due date: 30.06.2021

Version date: 28.09.2021

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 723051.

Document information

AUTHORS

Yves Page – Renault Group
Thibault Griffon – Stellantis
Nicolas Vignard – Toyota Motor Europe
Anastasia Bolovinou, ICCS

Coordinator

Aria Etemad
Volkswagen Group Research
Hermann-Münch-Str. 1
38440 Wolfsburg
Germany

Phone: +49-5361-9-13654
Email: aria.etemad@volkswagen.de

Project funding

Horizon 2020
ART-02-2016 – Automation pilots for passenger cars
Contract number 723051
www.L3Pilot.eu

Legal Disclaimer

Acknowledgment

The authors prepared this document on behalf of the huge group of partners who carried out the preparation of the prototypes fleet tested in L3Pilot. Correspondingly, all Pilot Site Leaders from Aptiv, AUDI, BMW, CRF, FEV, FORD, HONDA, JaguarLandRover, IKA, Stellantis, Renault Group, Toyota Motor Europe, Volvo Cars, VW, are acknowledged here.

Table of Contents

List of Figures

List of Tables

Executive Summary

In the sub-project “Fleet Preparation & Support”, we aimed at:

- Providing a description and a taxonomy of automated driving functions of the L3Pilot fleet to be evaluated.
- Adapting, implementing, and pre-testing the functions in the pilot fleet vehicles.
- Providing technical support to the project.
- Considering legal issues such as compliance to laws and regulations, including data privacy and insurance.
- Considering cybersecurity recommendations.

As for the first objective (WP4.3), deliverable D4.1 presented all AD functions tested in the project in a simple and visual manner. In addition, a task force was created to propose a taxonomy (or classification) of the AD functions as L3Pilot was not intending to evaluate each function one by one but by groups. This task force delivered two taxonomies that could be used depending on the objectives of the evaluations. At the end, the simplest taxonomy was used for evaluation (Motorway, Urban areas, Parking) using generic mature functions characteristics as described in D7.4.

As for objectives 4 and 5, the work consisted of depicting regulations in place in 7 countries (France, Germany, the Netherlands, Belgium, the UK, Sweden, Italy) to conduct AD experiments. As for cybersecurity, a task force prepared a review of all aspects to be considered, enhancing an approach available in the state of the art (TARA). The outcome is Deliverable D4.2, considering regulations and cyber protection.

As for the objective 3, the work was included in SP6 once the experiments started.

The core of SP4 “Fleet Preparation and support” was objective 2: adapting, implementing, and pre-testing AD functions on test tracks and open roads. A table with milestones and deadlines was proposed to monitor the progress of each Pilot leader in preparing their fleets, experimental procedures, study design, testing cars and pre-piloting.

The deliverables of this sub project “Fleet Preparation and support” are the following:

D4.1 "Description and taxonomy of automated driving functions" was delivered in its final version in April 2019. Each of the 18 AD systems is presented in a single sheet with summarized information about how each AD function works.

D4.2 "Legal requirements for AD Piloting and cybersecurity analysis" was delivered in April 2019 with details on how to apply AD experiments in compliance with national regulations and recommendation on how to comply with cybersecurity issues.

D4.3 “Summary report” which presents an update and the description of the final ADFs tested in the pilots and the work done in the Project. It also proposes a series of lessons learnt.

Overall, the SP4 “Fleet preparation and support” was successful in preparing the prototypes fleet for piloting (i.e., ADF implementation and testing) and in conceiving the experimental design. Pre-piloting started between April and November 2019 and pilots were conducted from spring 2019 to February 2021, despite several challenges (technical issues, data collection-conversion-storage issues, delay in clearance from the public authorities, availability of prototypes, changes in in-house organisation, temporary lack of resources, changes in experimental routes, pandemic, etc.). Pilots collected 200 000 kilometres of data in AD mode and 200 000 kilometres of data for baseline, mostly on motorways but also in urban areas and in parking spaces. At the end, 750 participants drove 70 prototypes.

The preparation phase benefitted from the past experience of the Pilot Leaders in setting up large-scale experiments, either internally or in EU-funded projects such as Euro-FOT or U-Drive, but it also gave an opportunity to gain additional knowledge about setting up that kind of challenging experiments, noticeably because of the special and unusual size and nature of the trials: testing prototypes with high level of technology, collecting large amount of data and ensuring the highest safety of participants and surrounding traffic.

Propositions and recommendations will certainly be taken into consideration in follow-up projects such as Hi-Drive, and other in-house initiatives. In any case L3Pilot explored new domains in setting up large-scale multi-centric experiments and adapted the FESTA approach with new challenges that were properly overcome: technical readiness of cars equipped with complex technology, experimental designs with higher safety requirements, collection/conversion/storage of big amount of complex data, compliance to new regulations (AD and GDPR), and last but not least, the SARS-COV-2 pandemic. SP4 “Fleet Preparation and support” was not affected by the pandemic since it was completed by mid-2019 but SP6 “Piloting” showed that trials stopped for a while and re-started with even higher health and safety requirements.

1 Introduction

1.1 Motivation for the L3Pilot Project

Over the years, numerous projects have paved the way for automated driving (AD). Especially, numerous vehicles are now equipped with Advanced Driver Assistance Systems (ADAS), and drivers are progressively getting used to them.

However, automation demands integrating more and better technology as well as compliance of the technology to user behaviour and acceptance of automated driving functions (ADF). In addition, there are many broad legal considerations which need to be addressed before AD can be rolled out.

The L3Pilot project is taking one of the further steps before the introduction of automated vehicles (AVs) in daily traffic. Its overall motivation is to test and study the viability of AD as a safe and efficient means of transportation, to gain knowledge base for exploring and promoting new service concepts to provide inclusive mobility.

1.2 L3Pilot Objectives

The newly attained level of technology maturity ensures an appropriate assessment of the impact of AD, what is happening both inside and outside the vehicles, how vehicle security can be ensured, evaluating user acceptance, societal impacts, and emerging business models.

Previous work indicated how driver assistance systems and ADF could be best validated by means of extensive road tests (Pilots), with a sufficiently long operation time, to allow extensive interaction with the driver and testable functions.

The project used large-scale testing and piloting of AD with developed SAE Level 3 (L3) functions (Figure 1.1) exposed to different users, mixed traffic environments, including conventional vehicles and vulnerable road users (VRUs), along different road networks. Level 4 (L4) functions were also assessed, to a lesser extent.

The data collected in these extensive pilots supported the main aims of the project to:

- Lay the foundation for the design of future user accepted L3 and L4 functions to ensure their commercial success. This is achieved by assessing user reactions, experiences, preferences, and acceptance of the AD functionalities.
- Enable non-automotive stakeholders, such as authorities and certification bodies, to prepare measures that support the uptake of AD, including updated regulations for the certification of vehicle functions with a higher degree of automation, as well as incentives for the user.
- Create unified de-facto standardised methods to ensure further development of AD applications (Code of Practice for the development of Automated Driving Functions).

- Create a large database to enable simulation studies of the performance of ADF over time which can't be investigated in road tests, due to the time and effort needed. The data is one outcome of the pilots.

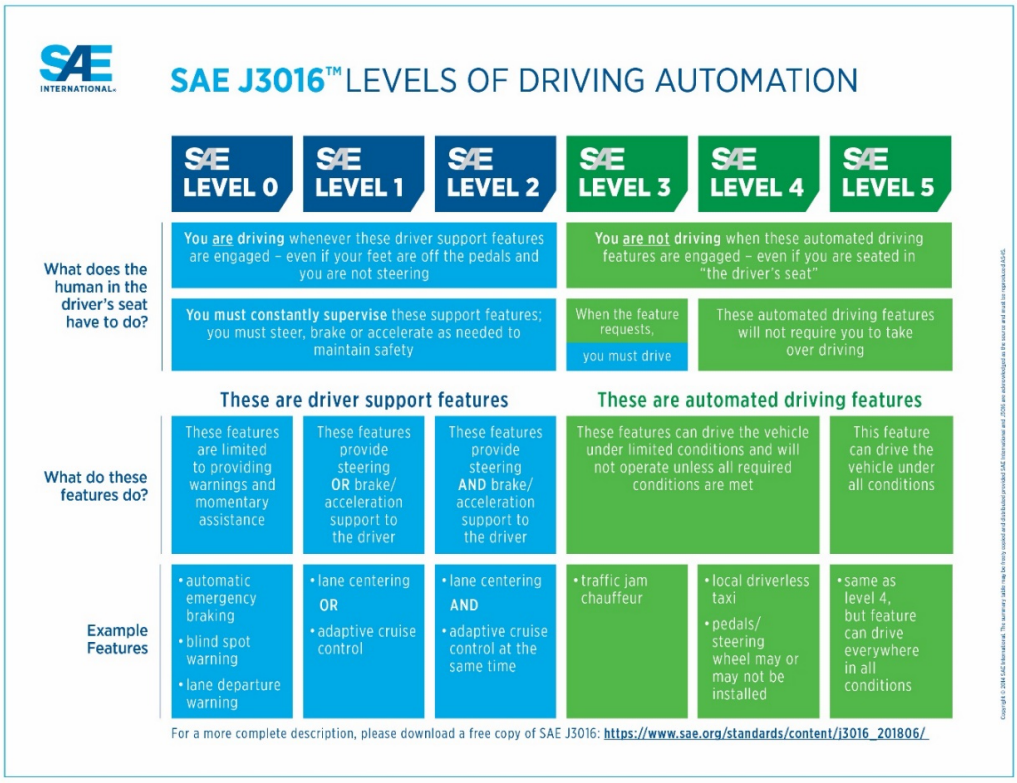


Figure 1.1: SAE Levels of Driving Automation J3016 (Copyright 2021 SAE International).

The consortium addressed the four major technical and scientific objectives listed below:

1. Create a standardized Europe-wide piloting environment for automated driving.
2. Coordinate activities across the piloting community to acquire the required data.
3. Pilot, test, and evaluate automated driving functions and connected automation.
4. Innovate and promote AD for wider awareness and market introduction.

1.3 Approach and Scope

The L3Pilot project focused on large-scale piloting of ADFs, primarily L3 functions, with additional assessment of some L4 functions. The key in testing was to ensure that the functionality of the systems used was exposed to variable conditions, and performance was consistent, reliable, and predictable. This enhanced a successful experience for the users (Figure 1.2). A good experience of using AD would accelerate acceptance and adoption of the technology and improve the business case to deploy AD.

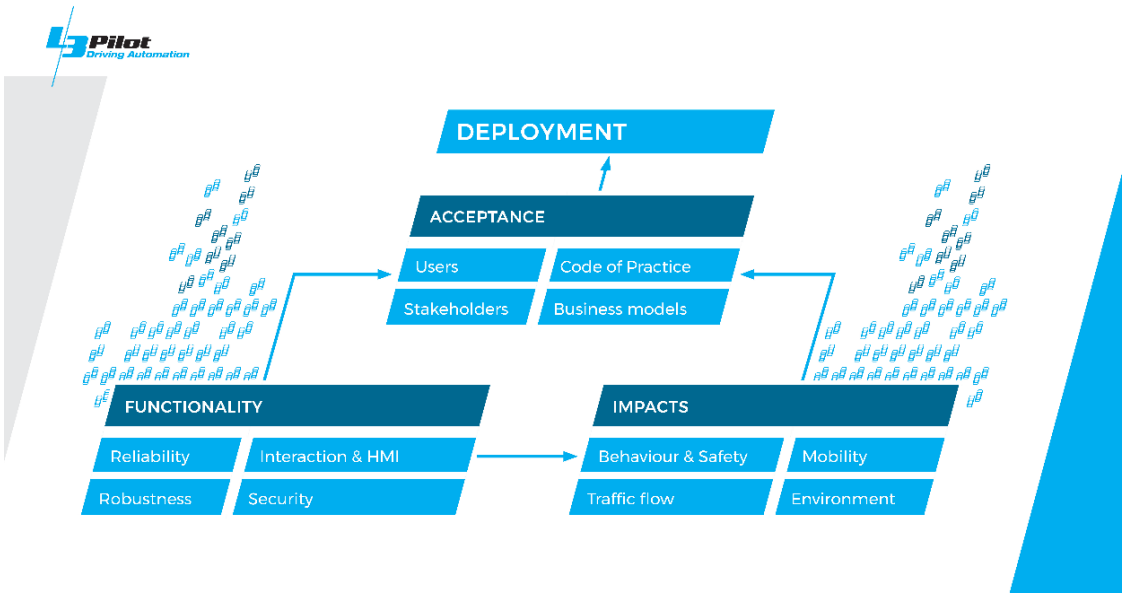


Figure 1.2: L3Pilot approach and the mechanism for deployment.

The L3Pilot consortium brought together stakeholders from the whole value chain, including OEMs, suppliers, academic institutes, research institutes, infrastructure operators, governmental agencies, the insurance sector and user groups.

More than 750 users tested 70 vehicles across Europe with bases in 7 Countries, including Belgium, France, Germany, Italy, Luxembourg, Sweden, and the United Kingdom, as shown in Figure 1.3.

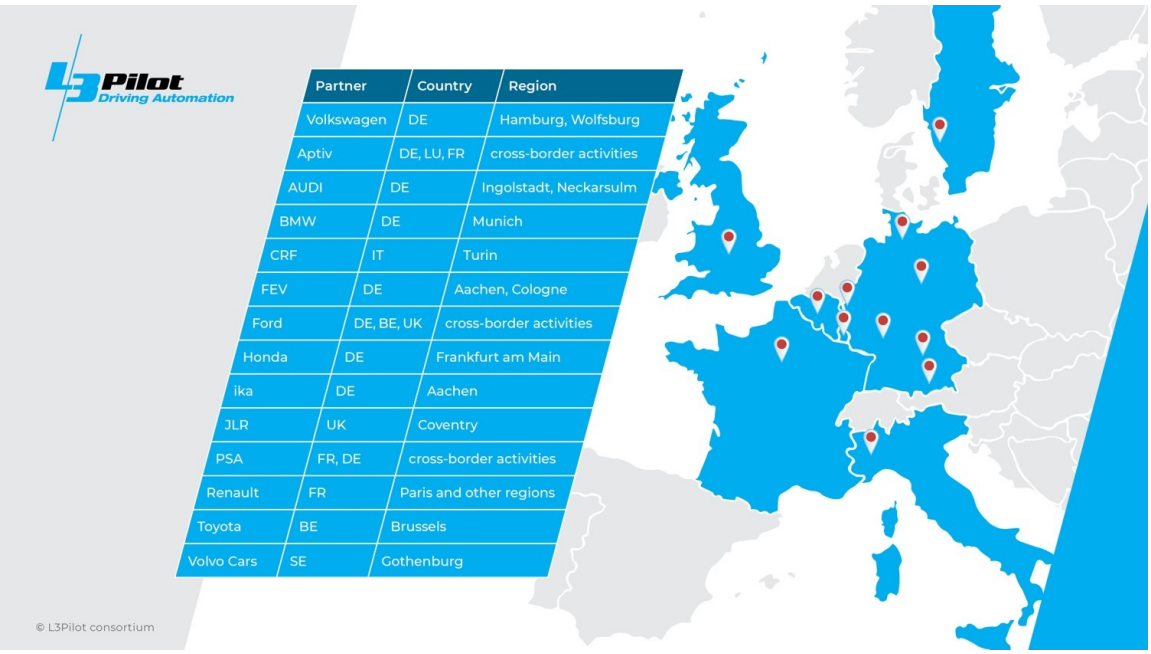


Figure 1.3: L3Pilot testing areas and cross-borders.

Since the development of AD functions, especially at SAE L3, the aim was not only to pilot the functions, but also to study user preferences, reactions, and willingness to use vehicles equipped with AD applications. This information led the consortium to create plans for the market introduction of AD. The L3Pilot concept can be split into the following two parallel, but intertwined, major activities:

- *Development of test and evaluation methodologies*, and actual testing and evaluation of functions, to answer the open questions. In this scientific part, a variety of controlled experiments were carried out.
- *Promotion of the project work for maximum impact.* This included dissemination of the project results and communication to the public, through showcases, to accelerate deployment of AD.

1.4 Methodology and Evaluation

The project followed the FESTA V process methodology, adapted to suit L3Pilot needs, of setting up and implementing tests with the four main pillars, as follows: (i) Prepare, (ii) Drive, (iii) Evaluate, and (iv) Address legal and cybersecurity aspects. FESTA (Field opErational teSt supporT Action) was originally created as an ADAS testing methodology to be used in FOTs (Field Operational Test). L3Pilot adapted it, however, to the piloting of AD functions.

When functions and use cases have been determined, research questions (RQs) and hypotheses (HYPs) were formulated. The piloting mainly focused on RQs and HYPs in four impact areas: (i) safety (ii) mobility (iii) efficiency, and (iv) environment. Additional evaluation

areas were carried out separately to address issues such as legal aspects and cybersecurity, as well as user evaluation and acceptance.

In the evaluation stage, a holistic approach was used by analysing different aspects of AD based on real-world driving data. As such, the approach followed FESTA evaluation domains: technical, user acceptance, driving and travel behaviour, impact on traffic, and societal impacts (Figure 1.4). The evaluation also took into account that the test vehicles were not market-ready products.

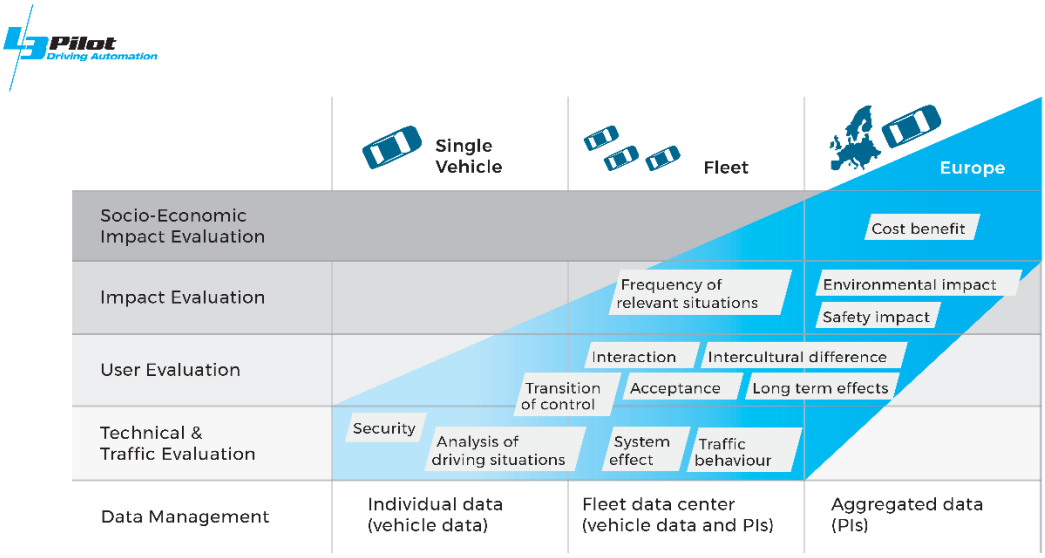


Figure 1.4: Evaluation aspects depending on evaluation domain and level of traffic.

1.5 Objectives of Subproject SP4 “Pilot Preparation & Support”

L3Pilot has defined the following main objectives for subproject SP4:

- The selection of the cars to be equipped with the AD functions used in the experiments by each OEM, supplier or research institute participating in the Pilot phase. The selected cars constituted the so-called “experimental fleet”.
- The detailed description of the automated functions to be investigated and a comprehensive taxonomy providing their classification.
- The implementation of the functions in the experimental fleet, including sensors, algorithms, hardware and software, recording devices, etc.
- The technical pre-tests of a single car from each sub-fleet and then the technical pre-tests of each car in all the sub-fleets.

- The submission of “dossiers” to public authorities to obtain the licence for driving AD cars in the different EU countries (Belgium, Sweden, Germany, France, the UK, Italy, The Netherlands)
- The technical support for the teams involved in the pilot phase.
- The strategies of cybersecurity of the AD functions implemented in the car fleet.

In short, the final target of subproject SP4 provided with the readiness for all the Pilot cars, so that they can be driven on public roads during the piloting phase of the project.

1.5.1 Objective of WP 4.3 “AD Functions”

12 OEMs, 2 suppliers and one university (they are called Pilot Leaders in the rest of the document) were participating in the L3Pilot experiments with various cars and various AD functions, working in various use cases, with different technical limitations and different HMI. These functions needed to be described in detail before the impact assessment can be done about capabilities of these functions, the role of the driver, and interactions between the driver and the automated system.

A first task consisted of describing these functions one by one, with the help of a list of criteria that structured the descriptions in a comprehensive and understandable manner. Such criteria were developed in WP4.3 and all involved Pilot Leaders were requested to describe their functions according to this grid.

A second task consisted of proposing a taxonomy of these functions to highlight similarities and discrepancies to facilitate the assessment as it was foreseeable that each function could not be evaluated one by one. Again, criteria for taxonomy (or taxonomies) were developed as for making it simpler to group functions into similar ones, each group being as different as possible from other groups.

The description particularly emphasized where the function applies (motorway, urban areas, parking) and the role of the driver (monitoring of the environment or not).

1.5.2 Objective of WP 4.4 “Implementation of functions”

Most test vehicles with AD functions were series cars modified into prototypes with additional sensors and technical equipment including data loggers. Therefore, the cars needed to be equipped in workshops so that they could be submitted for the Pilot phase (driving on open roads). The test vehicles that were copied, e.g., by installing redundant actuators and additional sensors, needed to be compared to the existing test vehicle to ensure that the same driving and data are delivered.

As vehicles were driven not only by professional test drivers but also in supervised natural mode by naïve drivers, additional measures were necessary to e.g., start /shut-down a vehicle with minimal differences to a series car and to provide a smooth operation (hidden cabling, computer noise, rattle and squeak with instrument carriers).

This WP4.4 was allocated to the preparation of the cars: sensor installation, measurement and computing equipment installation, modifications of controls (steering, braking, and pedals if required for a co-driver/safety driver), modifications of navigation systems, specific cluster or additional HMI, validation of safety. At the end of WP4.4, all cars were (technically) ready for insertion into the car fleet for the Pilot driving phase in WP4.5.

1.5.3 Objective of WP 4.5 “Testing and pre-piloting”

Once the cars were fitted with sensors, hardware, software, measurement material and data loggers, and before each car was ready for being driven by test subjects on open roads, they had to be tested for a few hundreds of kilometres by professional drivers. It was expected that functional safety had been tested before L3Pilot and that the software would have been tested at least on one car by each Pilot leader before Pilot started. However, the safety concept (safety of experiments) had to be validated.

Some technical validation remained to be done in some cases though, but that was not the main focus of this WP. Each Pilot leader tested and pre-piloted their car(s) according to their own internal procedures and with some additional procedures, methods and tests specific to L3Pilot. WP 4.5 was then in charge of establishing these specific L3Pilot procedures, especially to test the performance of data loggers recommended by SP5 and/or the correct collection of data by the loggers and to finalise the study design.

1.5.4 Objective of WP 4.6 “Legal Requirements for AD Piloting and Cybersecurity Analysis”

There were two distinct aspects in this WP:

- Ensure that driving on open roads with cars equipped with AD functions was permitted in all pilot countries by compiling guidelines which address and support requests for the permission to do so in case national legislations/rules require it.
- Establish a common approach to recommend cybersecurity requirements.

In most countries, legislation requires specific authorization for experimenting automated cars on open roads. For example, in France, any applicant must fill in a questionnaire and supply two dossiers, one describing the experiment in full details and another one describing the modifications brought to a series vehicle to make it a test vehicle for AD functions. Both dossiers have to underline what safety actions are envisaged by the applicant to secure the experiment at the highest level (contract with road maintenance operator, description of the functional safety analysis process, explanation about who takes over the vehicle in case of a system failure, etc.).

For cross-border driving legislation authorization in at least two countries must be obtained as well. A review of these requirements was conducted in seven countries.

The work on cybersecurity produced an analysis of the current state of the art and a methodology for identifying relevant cyber-attacks, while assessing their criticality. In turn,

this allowed the development of Deliverable D4.2 and technical recommendations for Pilot leaders. The employed methodology was a “Threat Analysis and Risk Assessment” (TARA), tailored to the objectives of level L3 functions with respect to cyber-attacks. In addition to TARA well established state-of-the-art framework proposed by SAE J3061, a novel model for the cybersecurity analysis of Level 3 (L3) Automated Driving (AD) systems was proposed by integrating aspects of functional safety. The proposed TARA+ model quantifies the likelihood and the impact of an attack and combines them in order to derive an attack risk value as in the traditional model. The novelty lies in the bespoke integration of the impact calculation, which incorporates the notion of controllability of an attack by the AD system and/or by the driver (ISO 26262 controllability definitions were extended to fit the proposed analysis). As a part of this method, the probable points of intrusion were identified, both external (e.g. road infrastructure manipulation) or internal (e.g. AV connectivity with the cloud) to the system, for each use case a risk assessment was done considering the probability and the impact of each attack. Finally, based on the above analysis and the SoA (Service Oriented Architecture) general cybersecurity guidelines were recommended to every Pilot Leader.

1.6 Objectives of the deliverable D4.3

The objectives of this deliverable are the following:

- Update the effective number and the description of AD functions in the end of the project in case there were some severe or slight changes compared to what was reported in D.4.1 “Description and Taxonomy of Automated Driving Functions”. This is done in Chapter 2.
- Report about the main activities and achievements conducted in each of the WP over the L3Pilot project period. This is done in Chapter 3.
- Compile lessons learnt for future experiments on Automated Driving or Connected Automated Driving. This is done in Chapter 4.

2 Update in the description of AD Functions

2.1 Introduction

The description of AD functions was obtained by means of detailed questionnaires, filled out by Pilot Leader responsible for the experiments (see D.4.1 for more details). The topics covered by the questionnaire are described in the Sections 2.3–2.8. below.

2.2 Methodology

The following principles were applied to guide the Pilot Leaders providing piloting vehicles in the process of filling in the template:

- The AD functions were pre-production or prototypes, not those that were being targeted to be sold.
- The AD functions had to be described mainly at a high level, providing a comprehensive viewpoint focused on their operational requirements.
- The description had to be self-sufficient and clear.
- The description had to be oriented towards the needs of the evaluation phase for an impact analysis.
- The taxonomy of AD functions was established ex-post once they have been depicted. The descriptions were the sole basis for the taxonomy.

When filling in the template, the Pilot Leaders followed a logical sequence, as shown in Figure 2.1.

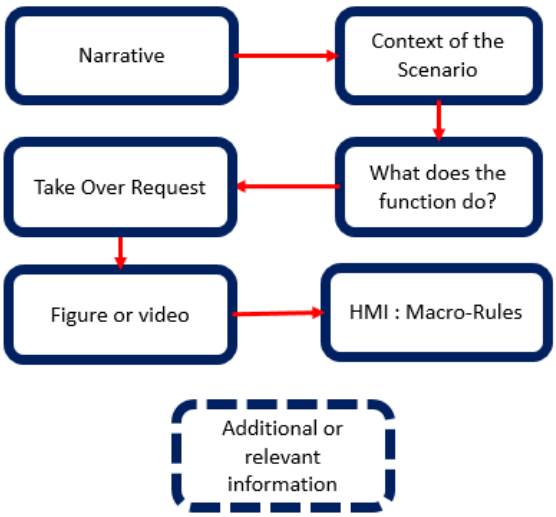


Figure 2.1: Sequence of AD functions description.

In this process, some questions required free text, while others allowed both free text and a list of options. An additional spreadsheet in the template was used to describe the vehicles of the fleet in which automated driving functions were implemented.

The components of the sequence are described in the following sections.

2.3 Narrative

2.3.1 AD function description and automation target

In this first part of the template, the Pilot Leaders gave a general description. The target of automation that the function was intended to deliver follows the SAE level of automation and includes the status of the driver as in “mind-on/mind-off”; “eyes-on/eyes-off”; and “hands-on/hands-off” (Figure 2.2).

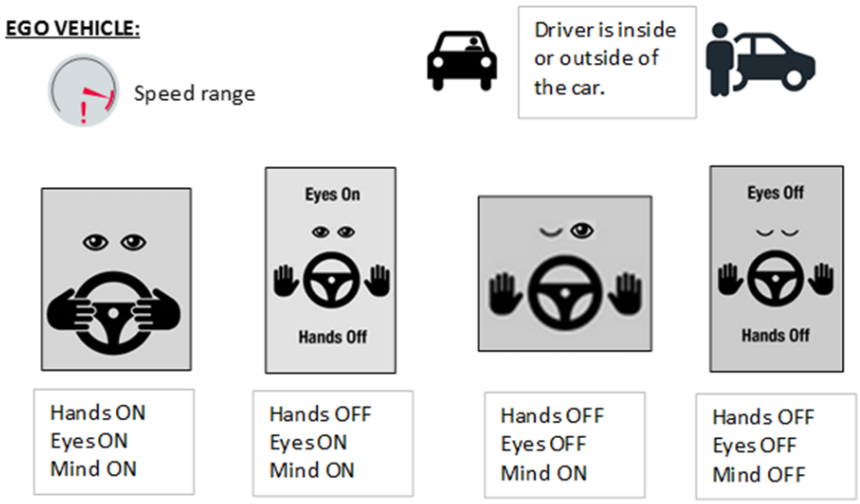


Figure 2.2: AD functions description and automation target.

- **Hands-On**: the driver must keep his/her hands on the steering wheel during AD mode, even though the AD system ensures lateral and longitudinal control.
- **Hands-Off**: the driver does not have to keep his/her hands on the steering wheel during AD mode.
- **Eyes-On**: the driver must be attentive and monitor the driving scene. In reference to SAE terms, the driver is in charge of the OEDR (Object and Event Detection and Response).
- **Eyes-Off**: the driver does not have to be attentive to driving all the time. He/she can engage in certain side activities (but not all). **“Eyes-Off” should not be used alone**. “Mind-on” or “Mind-off” must be added to fully understand what the driver must do and can do.
- **Eyes-Off – Mind-On**: the driver does not have to be attentive to driving all the time. However, he/she must be perceptive to take-over requests and to obvious dangers.

- **Eyes-Off – Mind-Off**: the driver does not need to be nor attentive nor perceptive to take-over requests. If there is a take-over request and the driver does not respond, the vehicle switches to a minimal risk manoeuvre to reach a minimal risk condition.

SAE standard J3016 never refers to these terms. They have been proposed afterwards for the sake of quick understanding but must be used appropriately. For example, a SAE level 2 can be hands-on or hands-off but is always eyes-on and mind-on. A SAE level 3 system is eyes-off, mind-on. A SAE level 4 system is eyes-off, mind-off in the sense of the above definitions.

2.3.2 Pilot site

The template also asked the Pilot Leader to specify the main location for piloting and any optional additional locations. This is relevant to enable the project to provide tests on a comprehensive set of locations with different traffic conditions, weather circumstances, kinds of roads, etc.

2.4 Context

2.4.1 ODD – Function boundaries

To describe the context in which the function was tested, and additionally to determine the boundaries of the functions, the description was divided into three parts: road, traffic, and visibility.

2.4.2 Environment – Road

To describe the road, the Pilot Leader indicated the road type (motorway, urban streets, parking area, etc.) and its characteristics, such as surface condition (good, bumpy, etc.) and geometry (straight, curved, inclined, etc.) (Figure 2.3).

The next type of question concerned the characteristics of the road, to obtain information about the existing infrastructure, such as lane dividers, guard rails, or limitations such as bicycle lanes and intersections.

Other questions referred to the accessibility of the test sites (private or public area) and the level of mapping required.

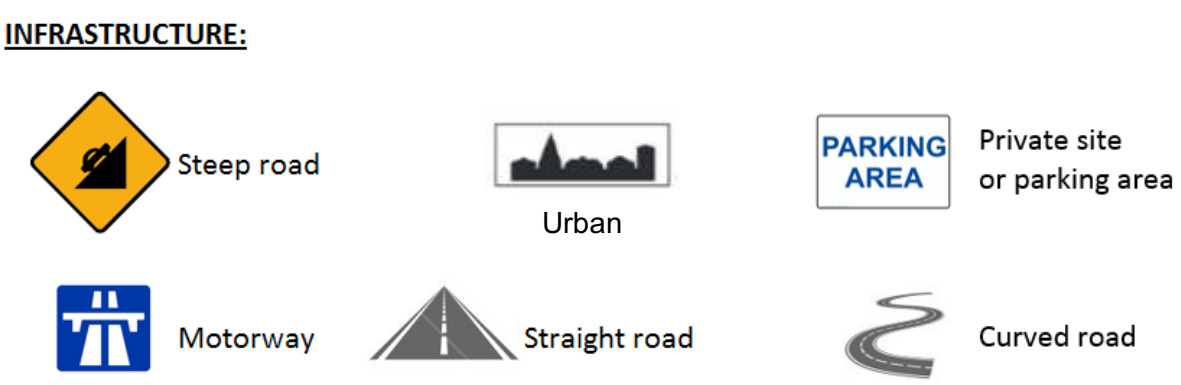


Figure 2.3: AD function description regarding infrastructure.

2.4.3 Environment – Traffic

To describe the situation, the Pilot Leader indicated planned traffic conditions (flow, mixed traffic, or automation only) (Figure 2.4).

Figure 2.4: AD function description regarding traffic environment.

2.4.4 Environment – Visibility

Visibility is mainly a consequence of weather conditions (sun, fog, rain, snow, etc.) but also of lighting conditions and of possible obstacles such as vehicles and infrastructure (Figure 2.5).

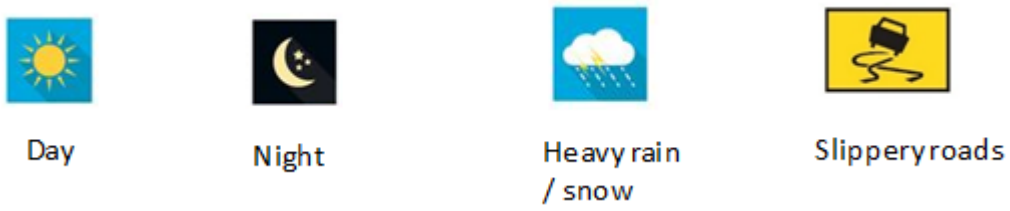


Figure 2.5: AD function description regarding road environment.

2.5 Function

2.5.1 Driver

The information on the driver was an essential part of the overall description of the tested function. Therefore, before determining the “Service provided by the AD function” and its scope, the questionnaire posed queries about the driver.

Depending on the SAE automation level, but also on the function, Pilot Leaders indicated the driver position (inside or outside of the vehicle, remote operation) and the need for monitoring (Figure 2.6). If the driver could do alternative tasks, a question required the Pilot Leader to specify if the driver could be drowsy or sleeping.

There was also a query about the target population of drivers (professional or non-professional) and their condition. The last question was about parameter settings by the driver, such as inter-vehicle distance, maximum speed, and other choices directly indicated during the driving process.

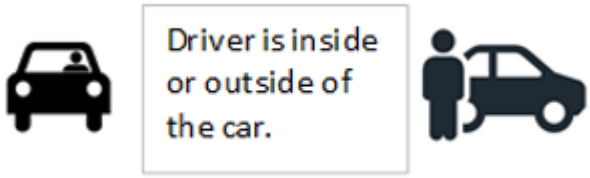


Figure 2.6: AD function description: driver inside or outside the car.

2.5.2 Service provided by the AD function

In this section, information was collected about the activation of the AD function, for instance in terms of duration, speed range, and type of manoeuvres (lane following, lane change, reversing, etc.). The section also described boundaries such as longitudinal and lateral control forces, lower and upper speed limit, etc.

Finally, the questionnaire referred to the connectivity with other vehicles, in particular with two questions about “coordination V2X” and “following distances” (Figure 2.7).

Figure 2.7: AD function description regarding connectivity.

2.6 Give-back Sequence

In this part of the questionnaire, the Pilot Leader described an expected and unexpected “give-back” sequence in a timeline. Details are given on the give-back process (initiated by the AD) and the take-over process (initiated by the driver) if available. The template also

described the position of hands and the detection of inattention by a driver monitoring system, if any.

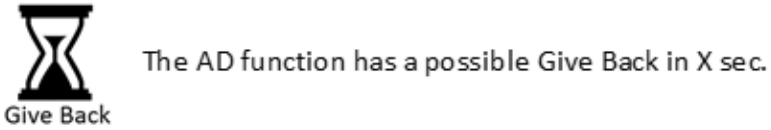


Figure 2.8: AD function description and give back sequence timeline.

2.7 Video and HMI

In this part, the Pilot Leader pictorially described the AD function, using a video or figures.

The template also illustrated the HMI of the dashboard or of the phone for those functions that used this device. The aim was to have a general view of the interface. If the Pilot Leader had macro rules for HMI, they could be included in this section.

2.8 Vehicles

For each function, a short description of the piloting vehicles was added in this last section.

The Pilot Leader described the number of cars (prototype or serial) and the model for the given function. Then, they described the actuators (steering, throttle, braking system, etc.) and all the sensors (cameras, LiDAR, GPS, radar, etc.) used for the AD function.

Finally, the template asked for communication protocols and data logging. It also requested that the hardware providing the HMI and the main features of the communication channel be specified.

2.9 Description of AD functions

The full scope of all L3Pilot functions, as obtained in the initial questionnaires and updated during the course of the project depending on modifications, is presented in Table 2.1. The project covered four types of road scenarios and three levels of automation according to the SAE classification – with a distinct focus on Level 3, as shown in Table 2.2.

Table 2.1: L3Pilot functions by SAE automated driving level (ID=Identity Document).

		Parking	Motorway	Traffic Jam	Urban
ID	1		Level 3		
ID	2			Level 3	
ID	3		Level 4		
ID	4		Level 3		
ID	5				Level 3
ID	6		Level 3		
ID	7			Level 3	
ID	8	Level 4			
ID	9		Level 3		
ID	10		Level 3		
ID	11				Level 3
ID	12	Level 4			
ID	13			Level 3	
ID	14	Level 2			
ID	15		Level 3		
ID	16				Level 3
ID	17		Level 3		
ID	18			Level 3	

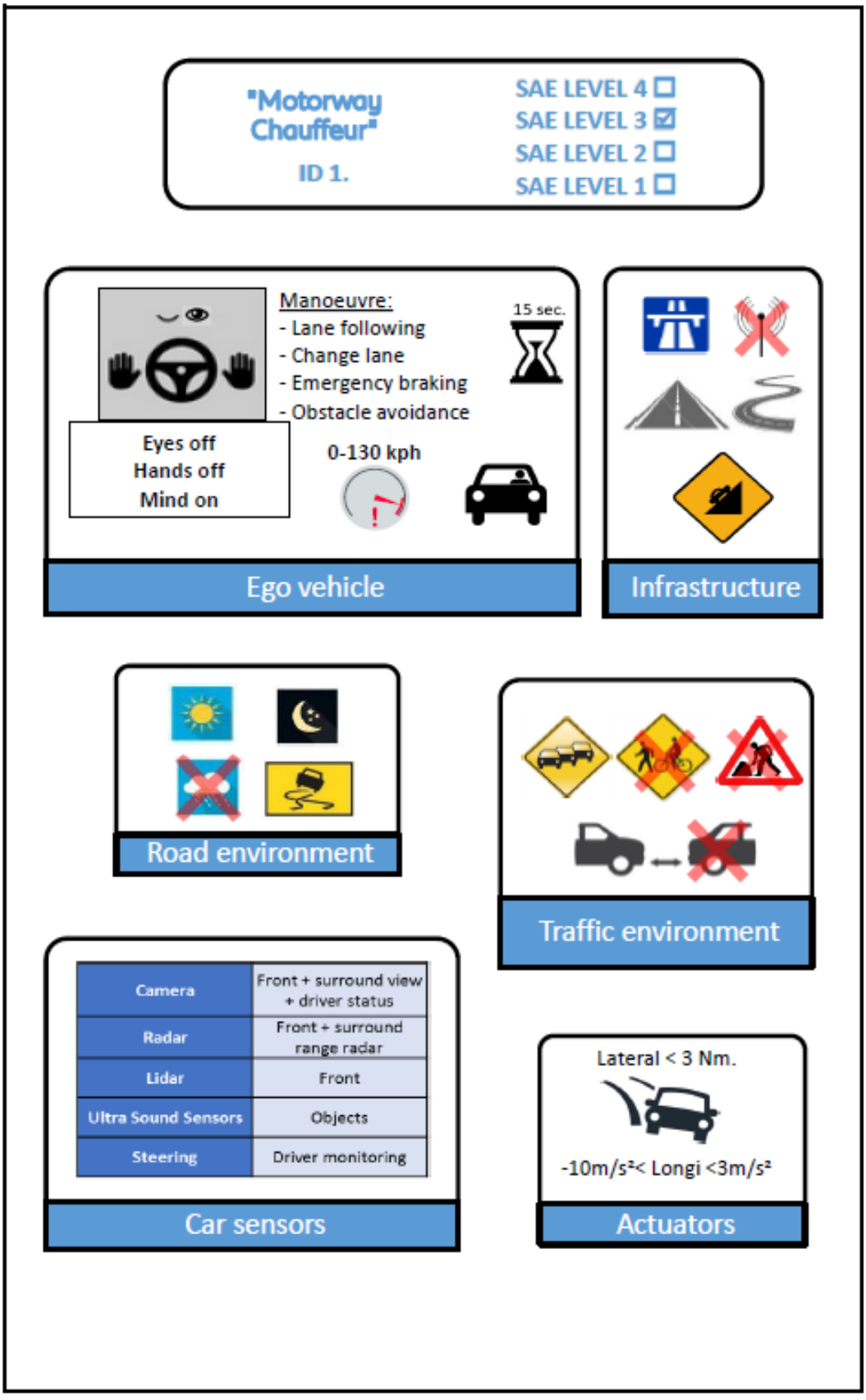
Table 2.2: Distribution of functions according to SAE levels and types of ADF.

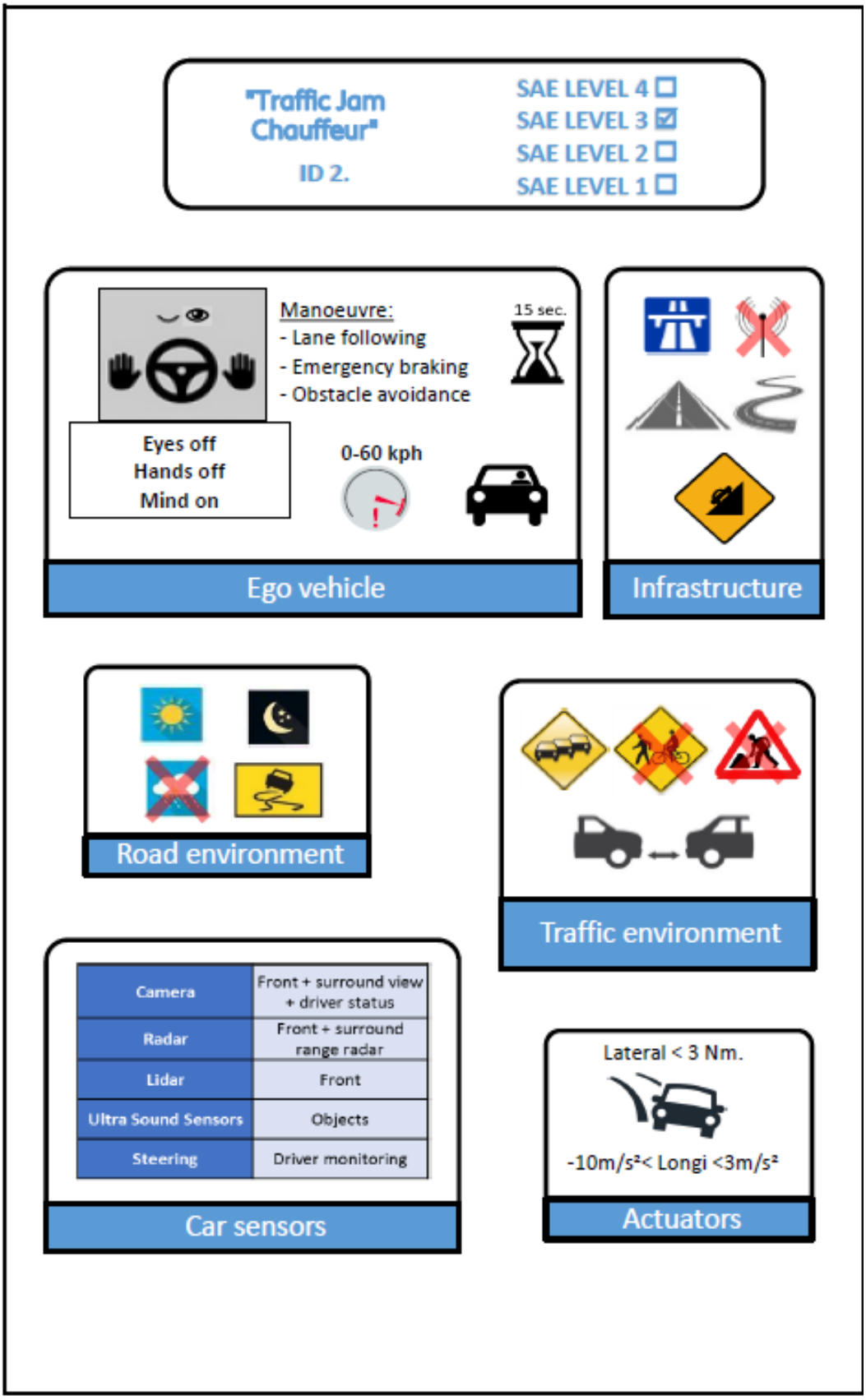
	Number of ID
Function Level 2	1
Function Level 3	14
Function Level 4	3

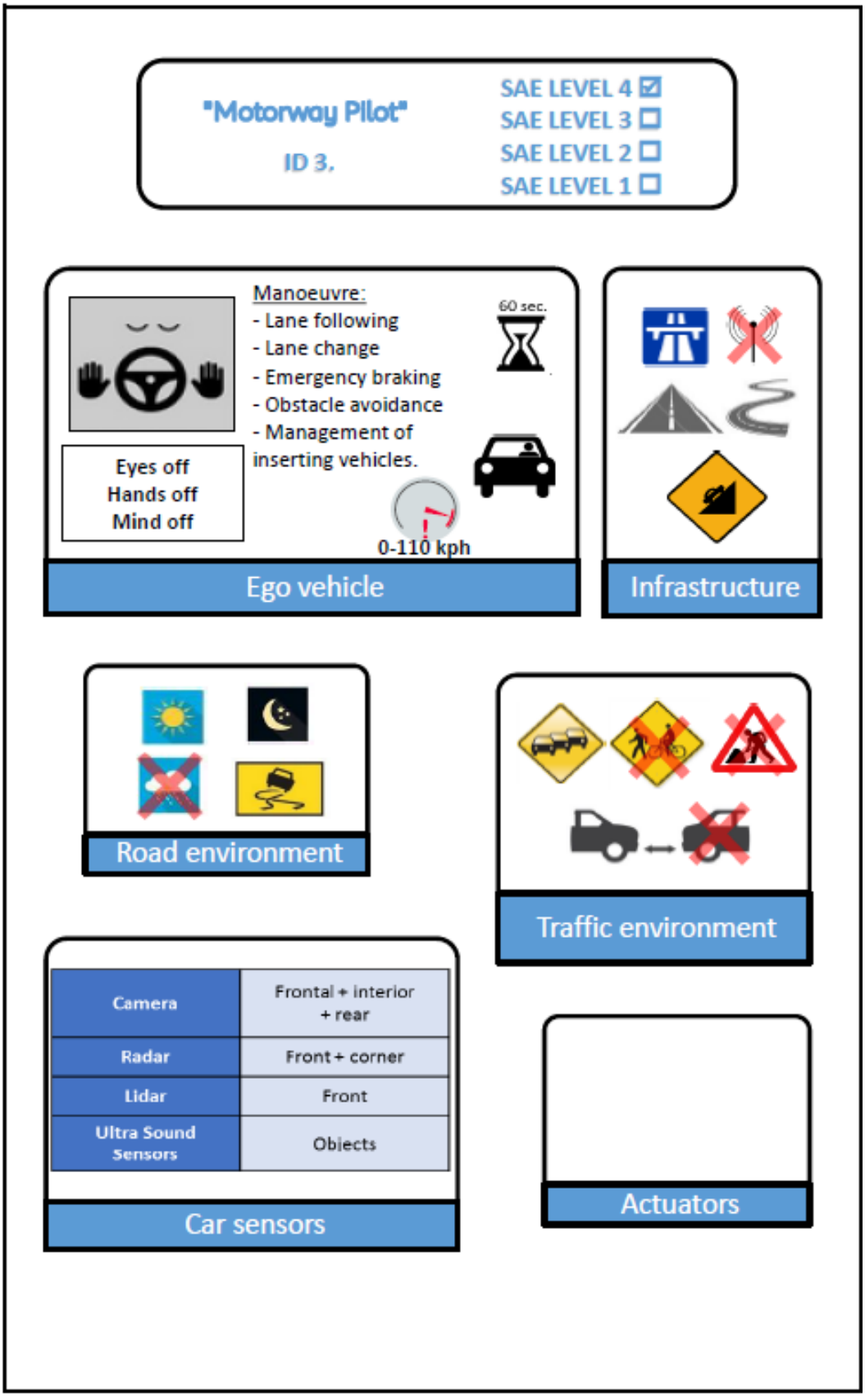
	Number of ID
Parking	3
Motorway	8
Traffic jam	4
Urban	3

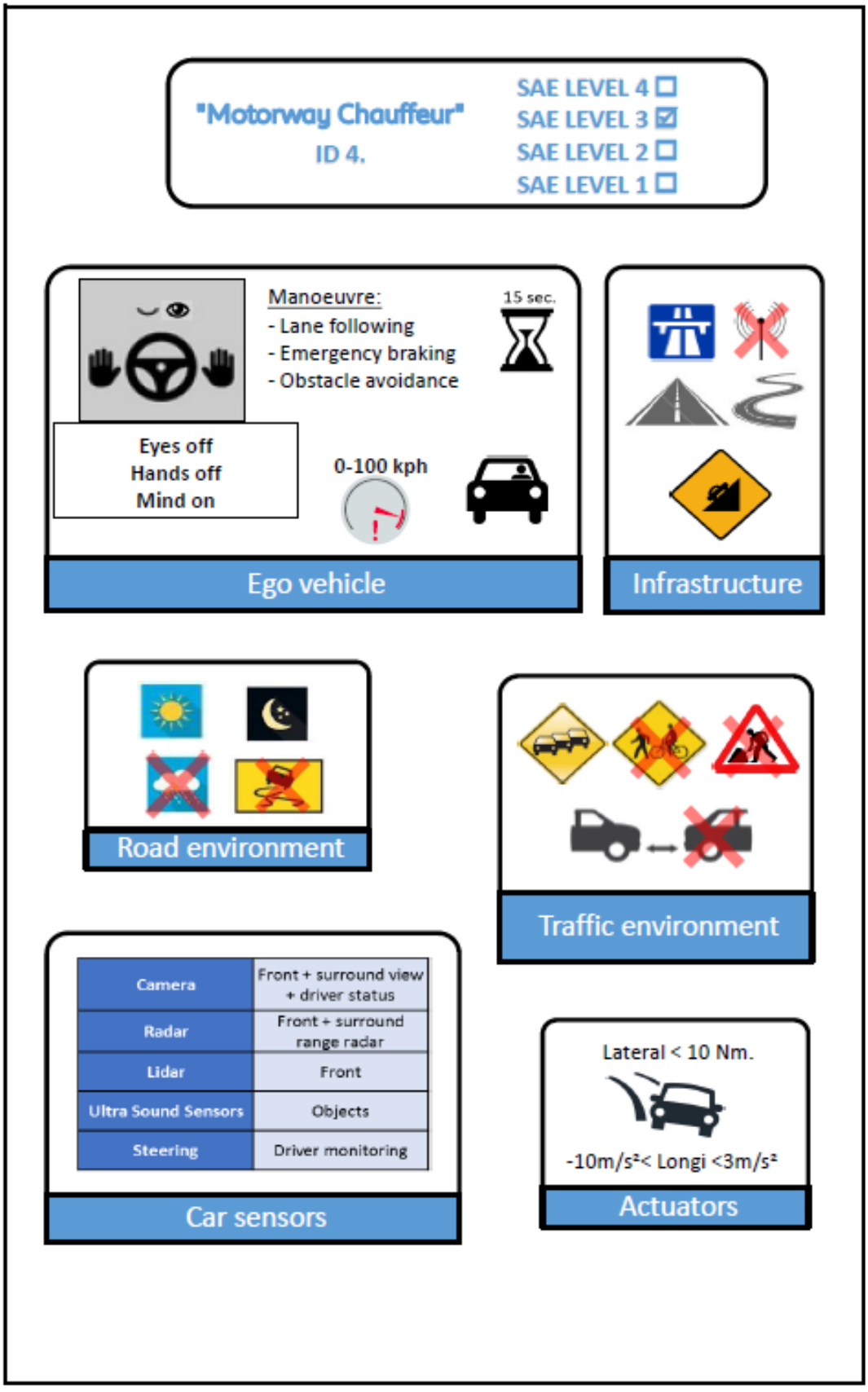
The following pictorial depiction represents the functions tested during the project for a total of 18 AD functions. Each representation covers the main topics of the questionnaire and delivers a general and visual approach of each ADF. The function name and SAE level are given in the upper box, followed by symbols indicating the key characteristics, and by a sketch of the topics as they were described by the Pilot Leaders. Each Pilot Leader was assigned an ID for the sake of confidentiality. A Pilot Leader can have multiple IDs because the partner is testing multiple AD functions.

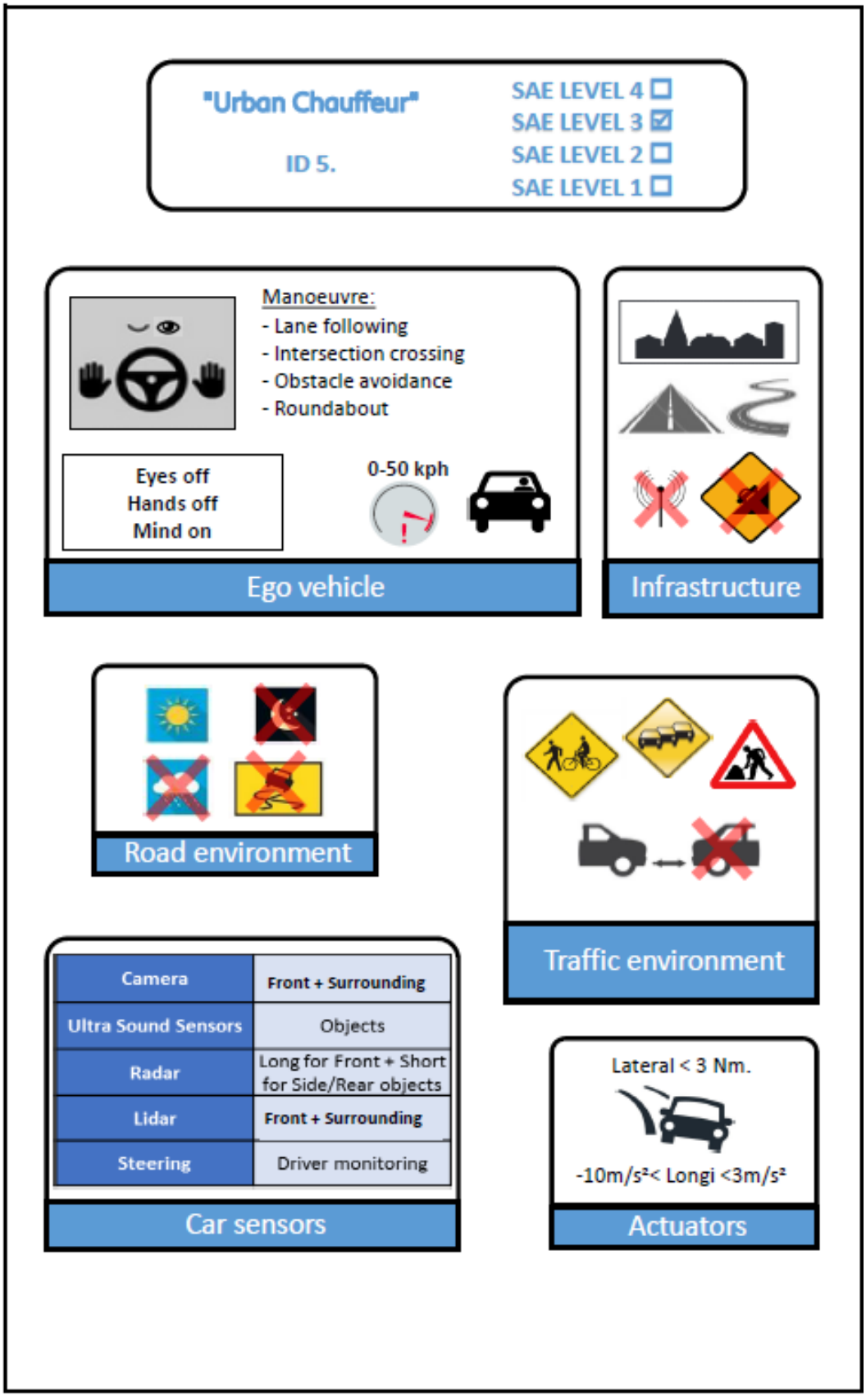
More insights into the literal description of the AD functions, the ODDs, the test vehicles, the study designs and the track routes, pilot site per pilot site, heavily started in SP4 and continued in SP6, can be found in Deliverable 6.3 “Pre-test results”. It was not necessary and certainly redundant to mention them in this summary report.

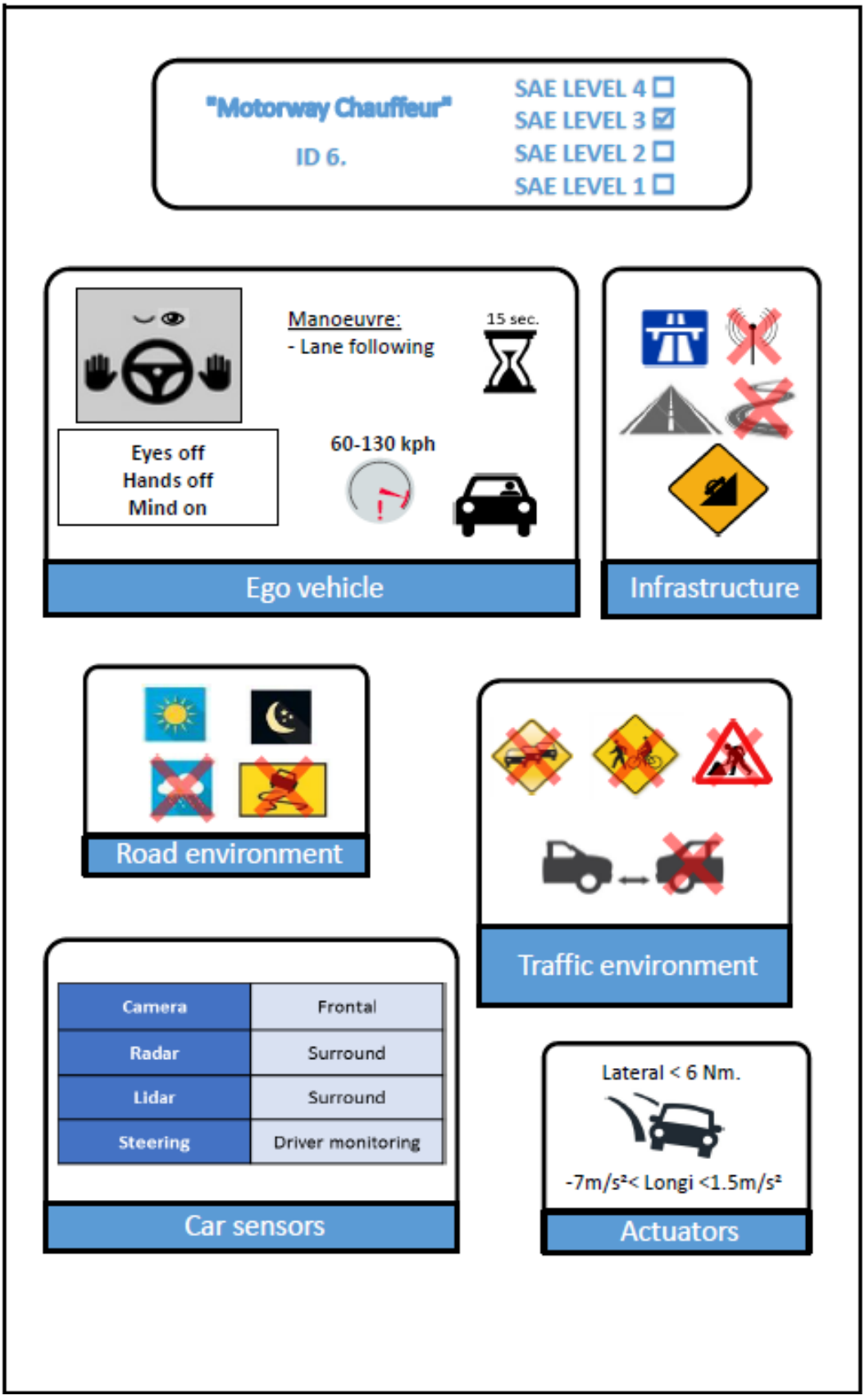

"Motorway Chauffeur"
ID 1.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Change lane
- Emergency braking
- Obstacle avoidance
15 sec.
Eyes off
Hands off
Mind on
0-130 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + surround view + driver status
Radar
Front + surround range radar
Lidar
Front
Ultra Sound Sensors
Objects
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators

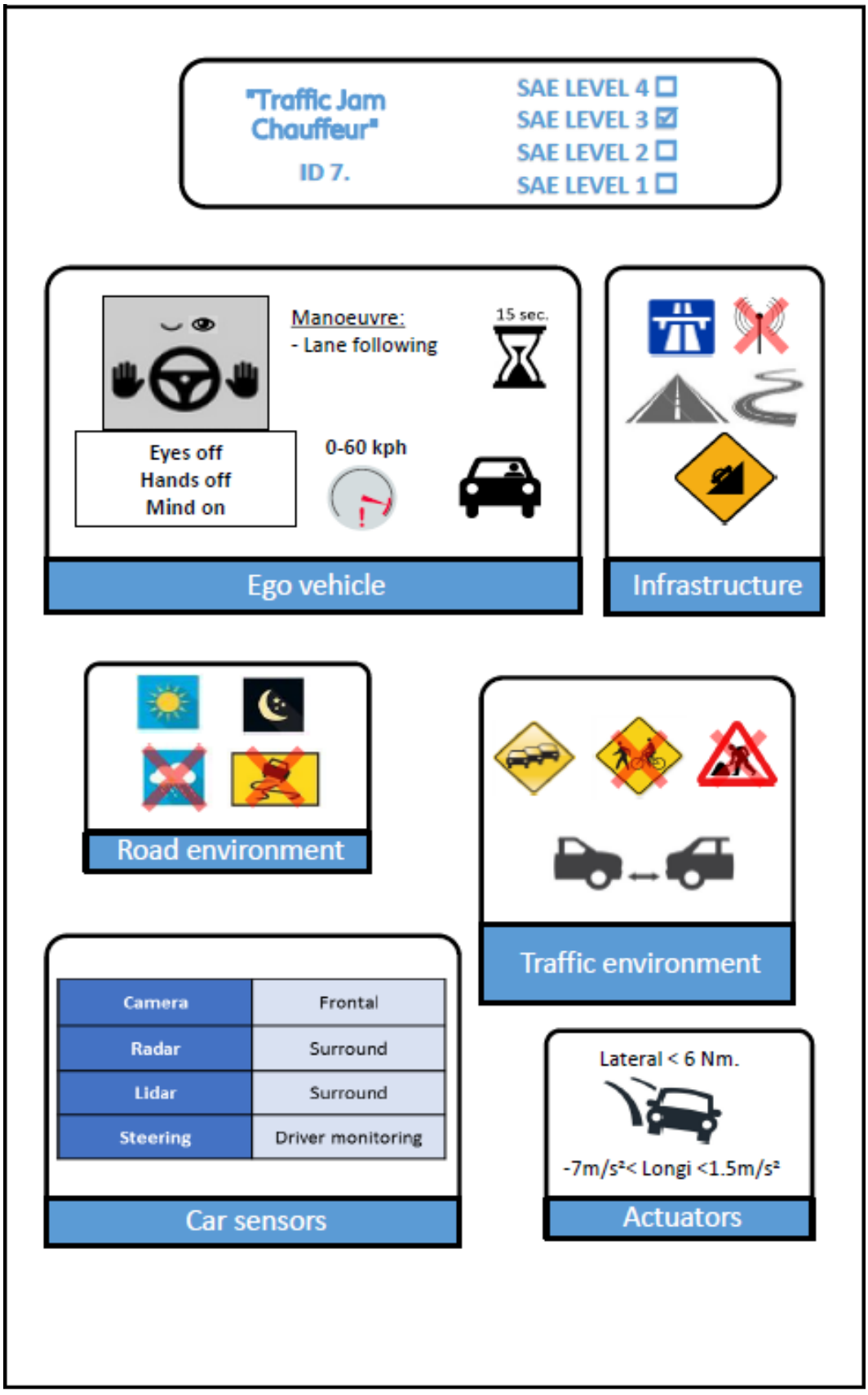

"Traffic Jam Chauffeur"
ID 2.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Emergency braking
- Obstacle avoidance
15 sec.
Eyes off
Hands off
Mind on
0-60 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + surround view + driver status
Radar
Front + surround range radar
Lidar
Front
Ultra Sound Sensors
Objects
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators

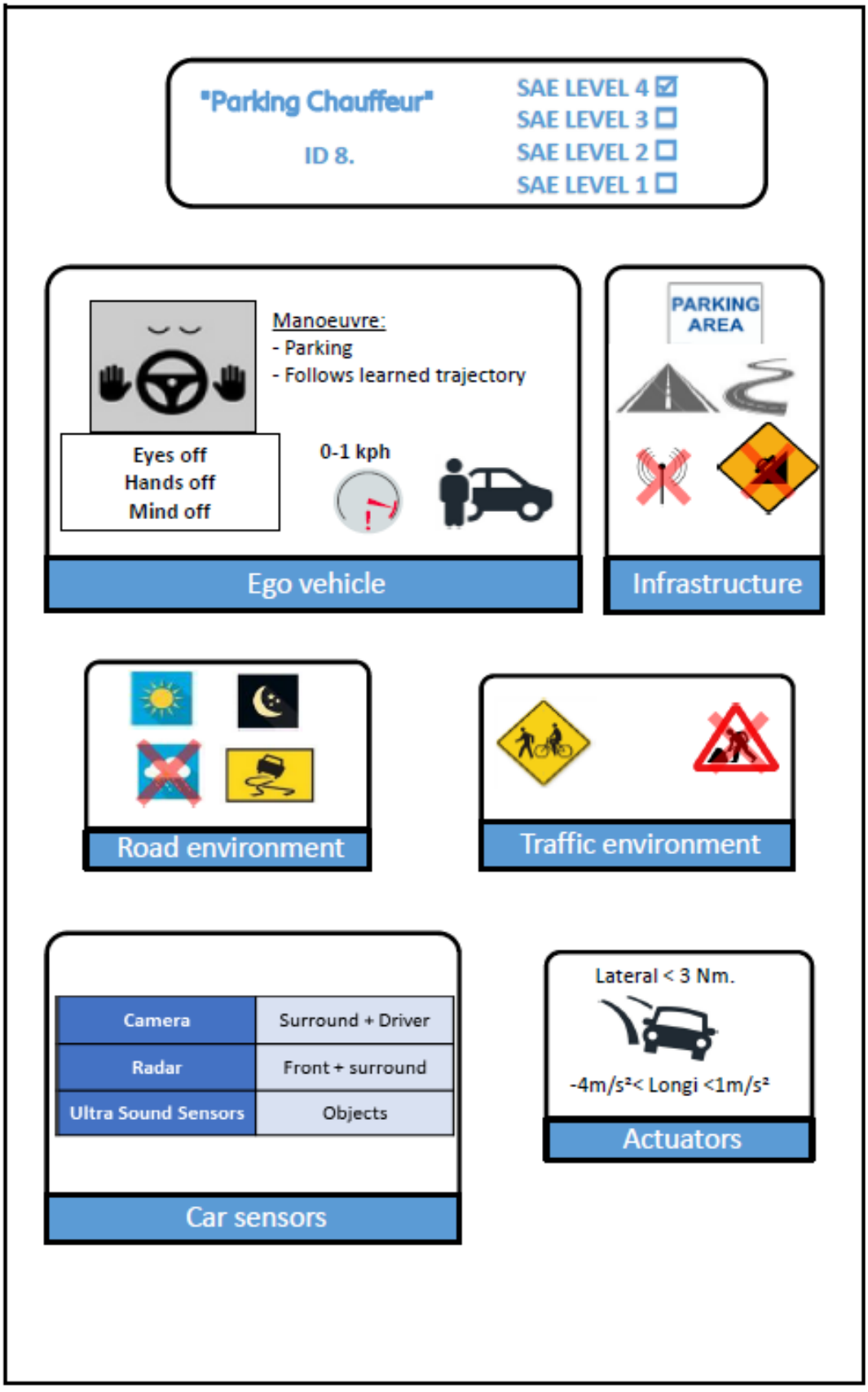

"Motorway Pilot"
ID 3.
SAE LEVEL 4 ☑
SAE LEVEL 3 ☐
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Lane change
- Emergency braking
- Obstacle avoidance
- Management of inserting vehicles.
60 sec.
Eyes off
Hands off
Mind off
0-110 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Frontal + interior + rear
Radar
Front + corner
Lidar
Front
Ultra Sound Sensors
Objects
Car sensors
Actuators

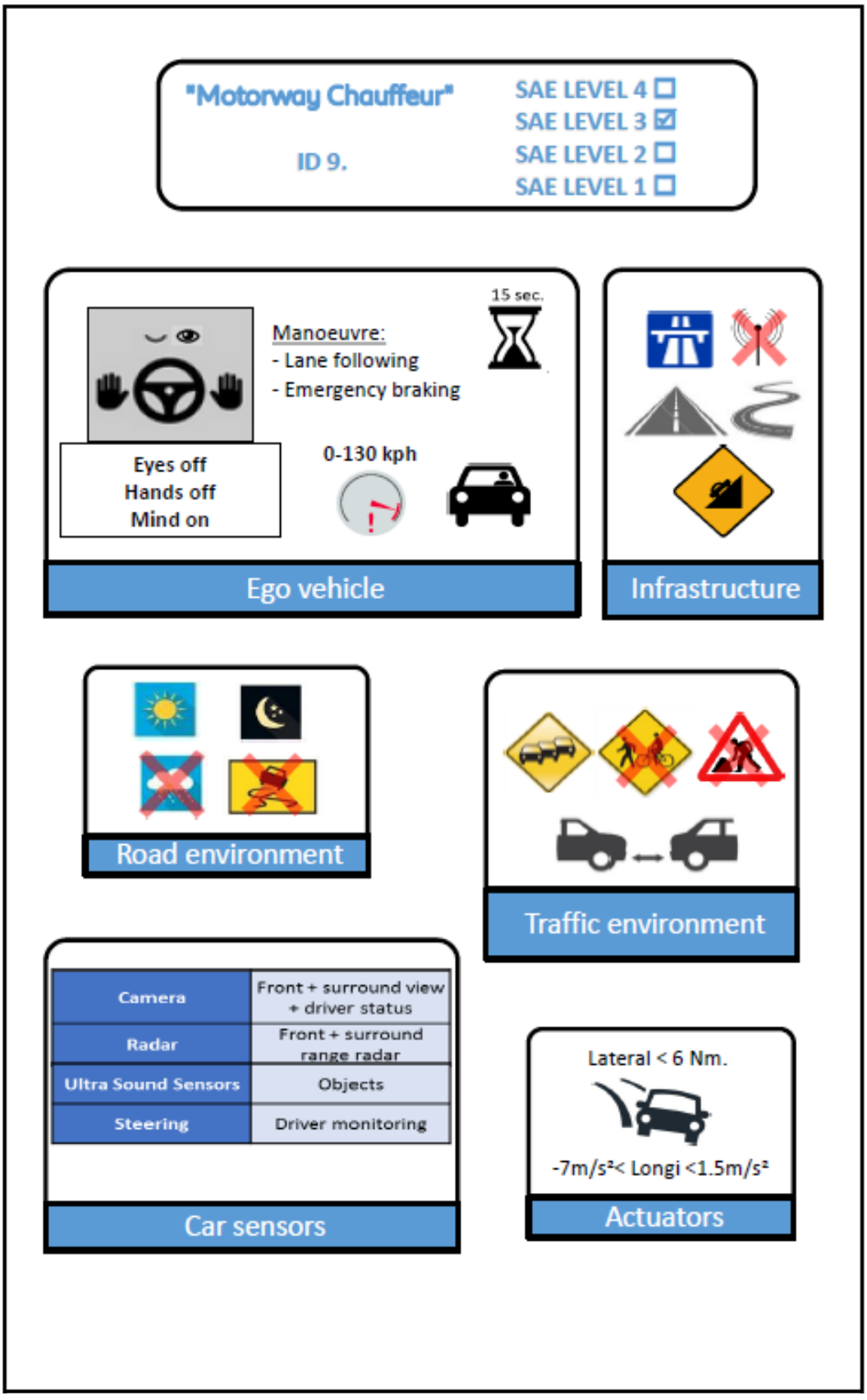

"Motorway Chauffeur"
ID 4.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Emergency braking
- Obstacle avoidance
15 sec.
Eyes off
Hands off
Mind on
0-100 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + surround view + driver status
Radar
Front + surround range radar
Lidar
Front
Ultra Sound Sensors
Objects
Steering
Driver monitoring
Car sensors
Lateral < 10 Nm.
-10m/s²< Longi <3m/s²
Actuators

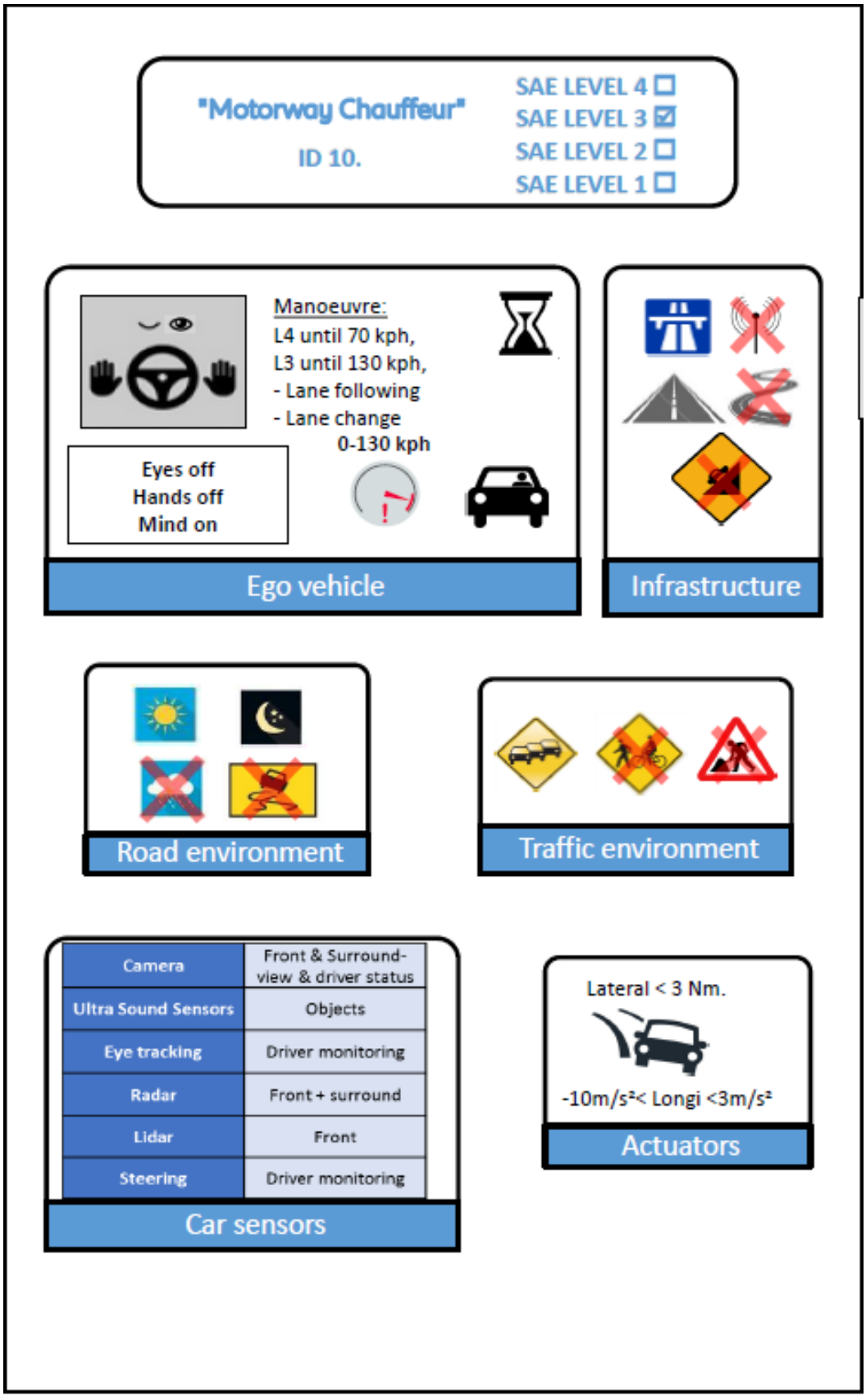

"Urban Chauffeur"
ID 5.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Intersection crossing
- Obstacle avoidance
- Roundabout
Eyes off
Hands off
Mind on
0-50 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + Surrounding
Ultra Sound Sensors
Objects
Radar
Long for Front + Short for Side/Rear objects
Lidar
Front + Surrounding
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators

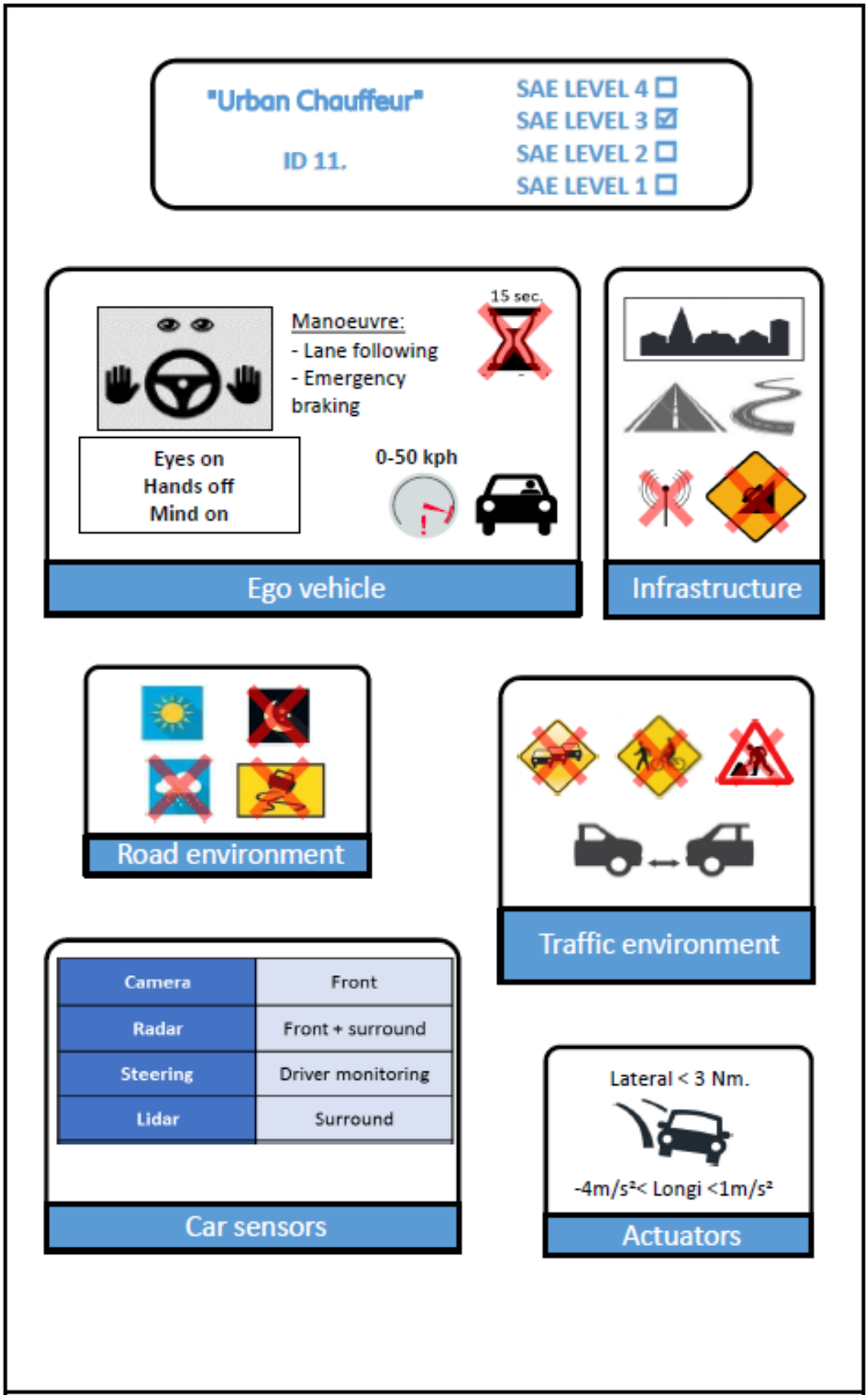

"Motorway Chauffeur"
ID 6.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
15 sec.
Eyes off
Hands off
Mind on
60-130 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Frontal
Radar
Surround
Lidar
Surround
Steering
Driver monitoring
Car sensors
Lateral < 6 Nm.
-7m/s²< Longi <1.5m/s²
Actuators

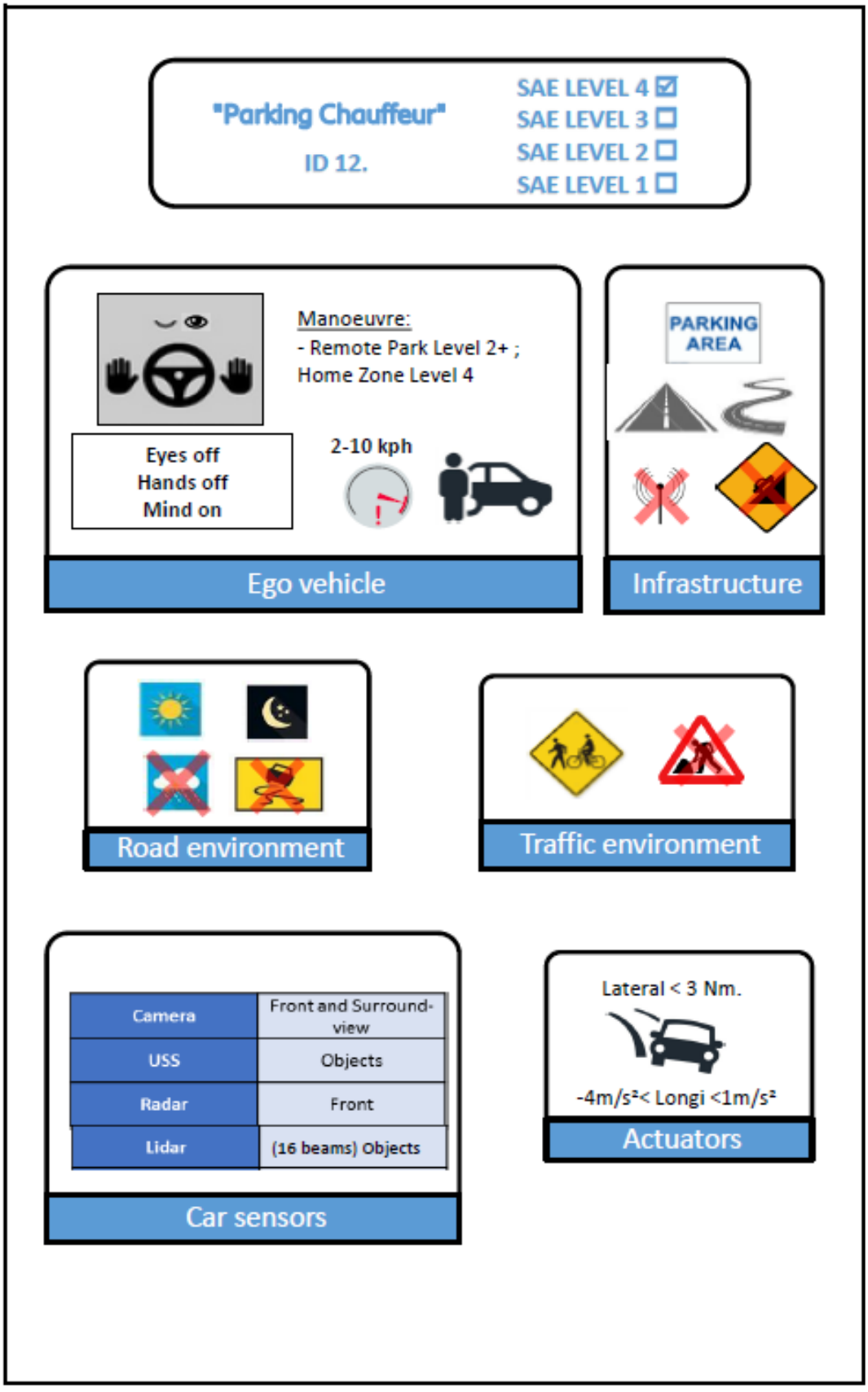

"Traffic Jam Chauffeur"
ID 7.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
15 sec.
Eyes off
Hands off
Mind on
0-60 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Frontal
Radar
Surround
Lidar
Surround
Steering
Driver monitoring
Car sensors
Lateral < 6 Nm.
-7m/s²< Longi <1.5m/s²
Actuators

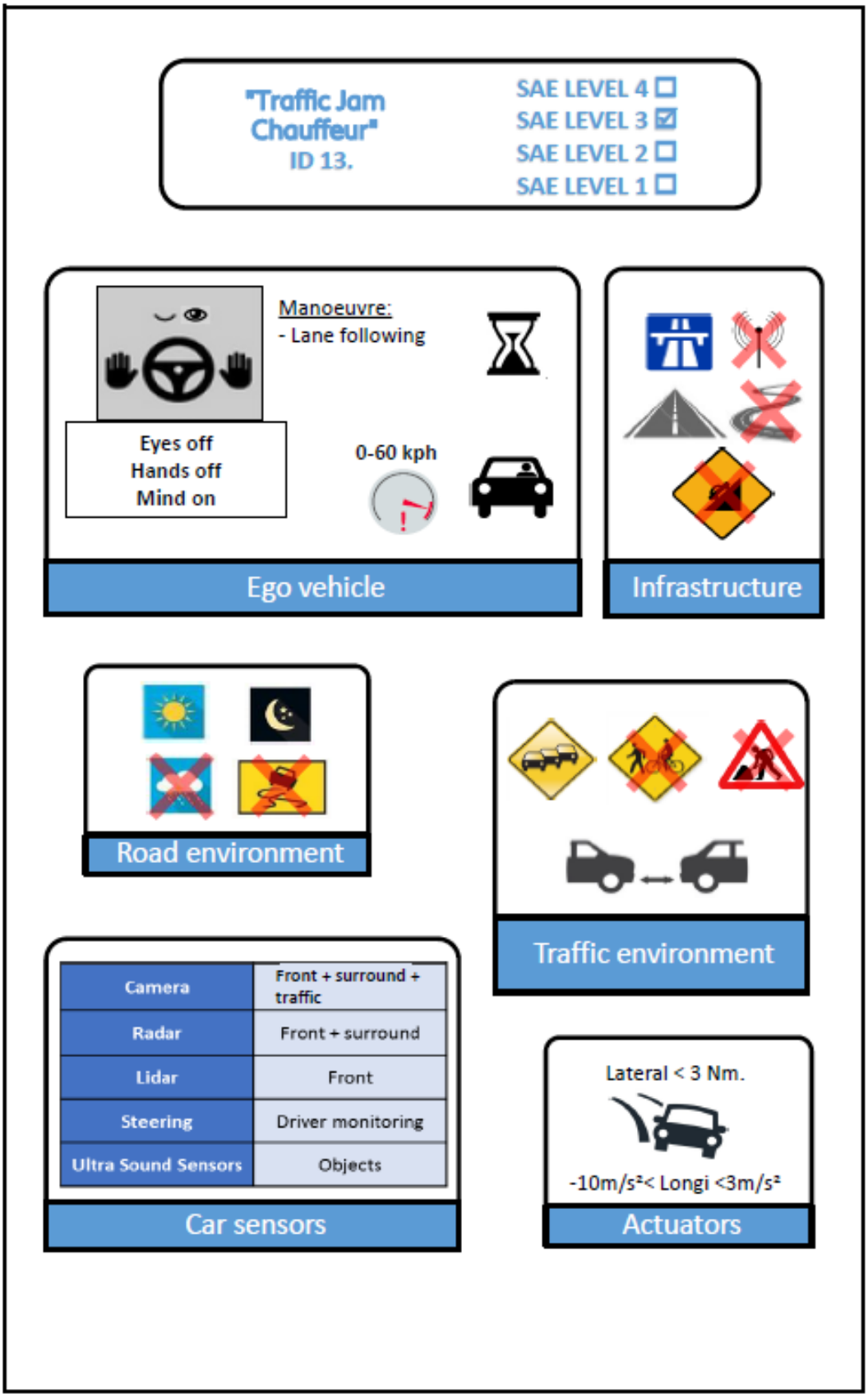

"Parking Chauffeur"
ID 8.
SAE LEVEL 4 ☑
SAE LEVEL 3 ☐
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Parking
- Follows learned trajectory
Eyes off
Hands off
Mind off
0-1 kph
Ego vehicle
PARKING AREA
Infrastructure
Road environment
Traffic environment
Camera
Surround + Driver
Radar
Front + surround
Ultra Sound Sensors
Objects
Car sensors
Lateral < 3 Nm.
-4m/s²< Longi <1m/s²
Actuators

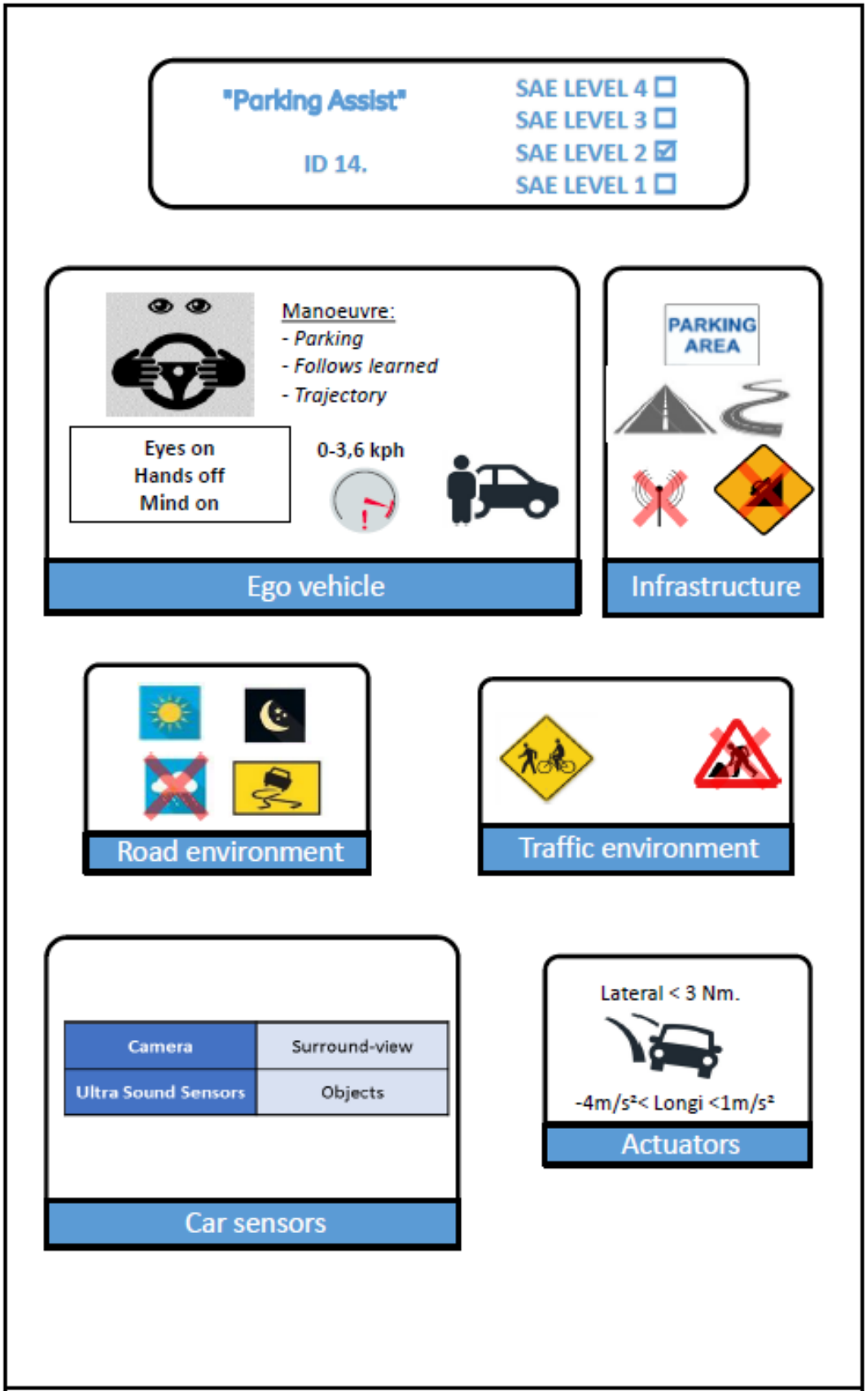

"Motorway Chauffeur"
ID 9.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
15 sec.
Manoeuvre:
- Lane following
- Emergency braking
Eyes off
Hands off
Mind on
0-130 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + surround view + driver status
Radar
Front + surround range radar
Ultra Sound Sensors
Objects
Steering
Driver monitoring
Car sensors
Lateral < 6 Nm.
-7m/s²< Longi <1.5m/s²
Actuators

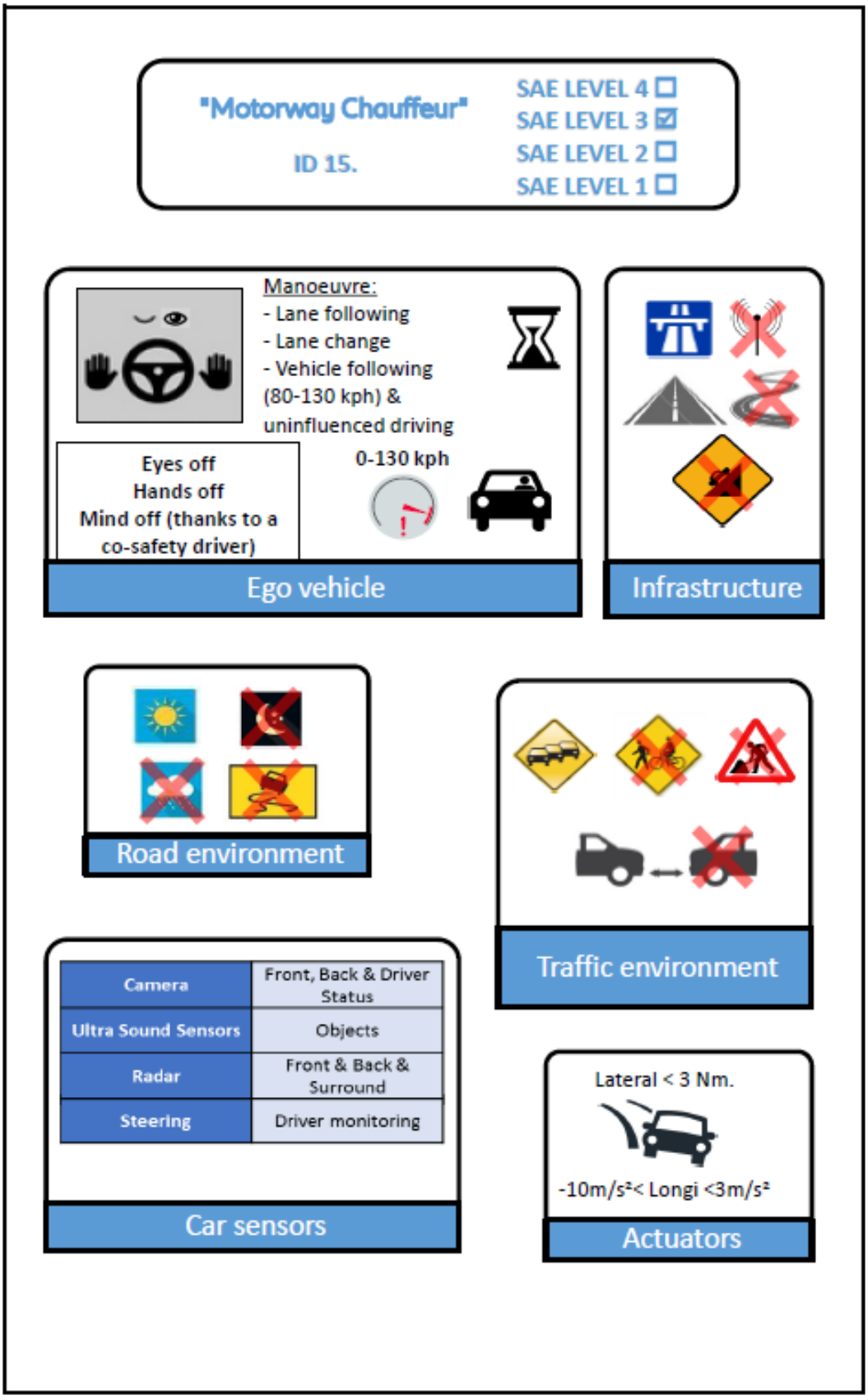

"Motorway Chauffeur"
ID 10.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
L4 until 70 kph,
L3 until 130 kph,
- Lane following
- Lane change
0-130 kph
Eyes off
Hands off
Mind on
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front & Surround-view & driver status
Ultra Sound Sensors
Objects
Eye tracking
Driver monitoring
Radar
Front + surround
Lidar
Front
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators

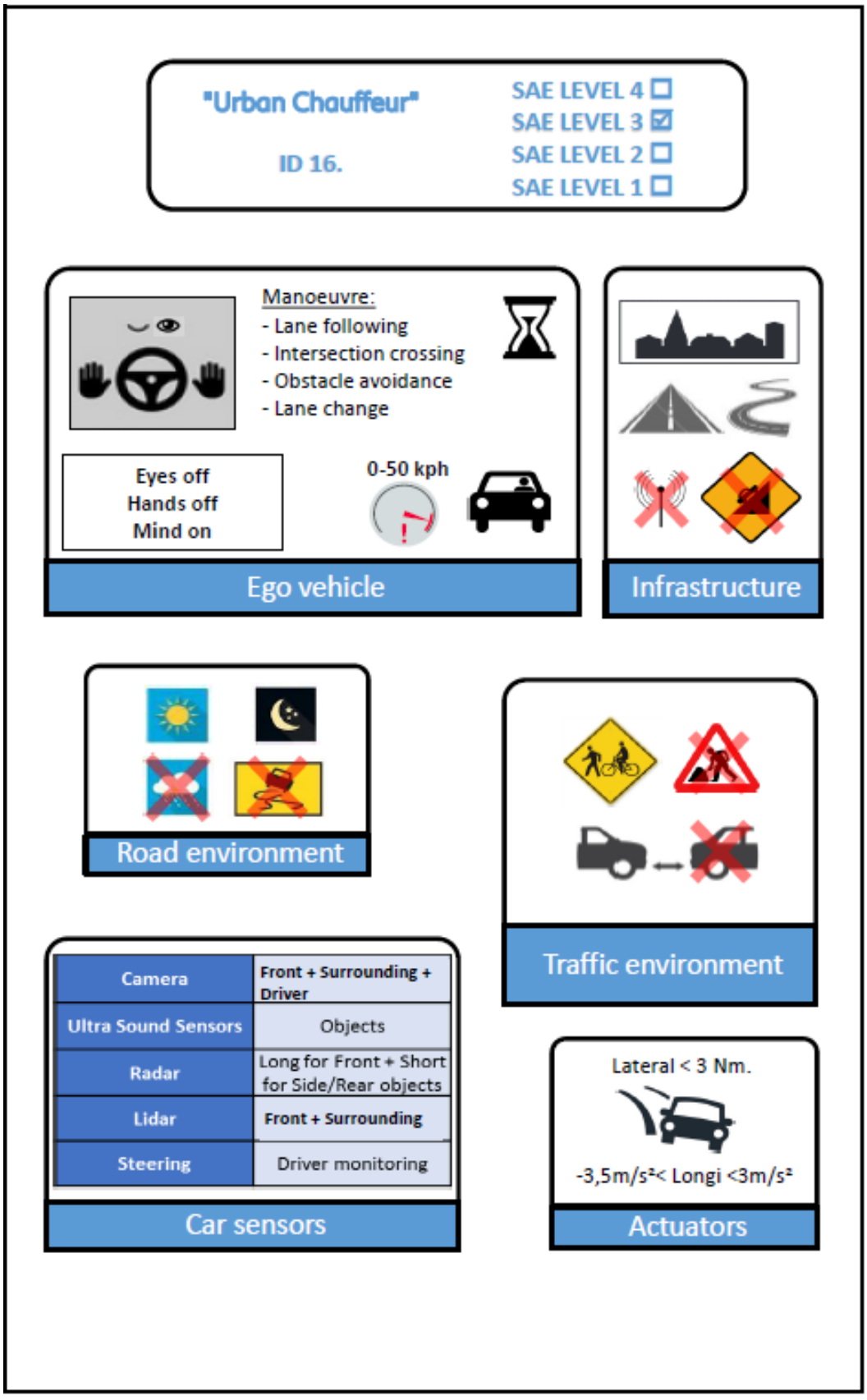

"Urban Chauffeur"
ID 11.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
15 sec.
Manoeuvre:
- Lane following
- Emergency braking
Eyes on
Hands off
Mind on
0-50 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front
Radar
Front + surround
Steering
Driver monitoring
Lidar
Surround
Car sensors
Lateral < 3 Nm.
-4m/s²< Longi <1m/s²
Actuators

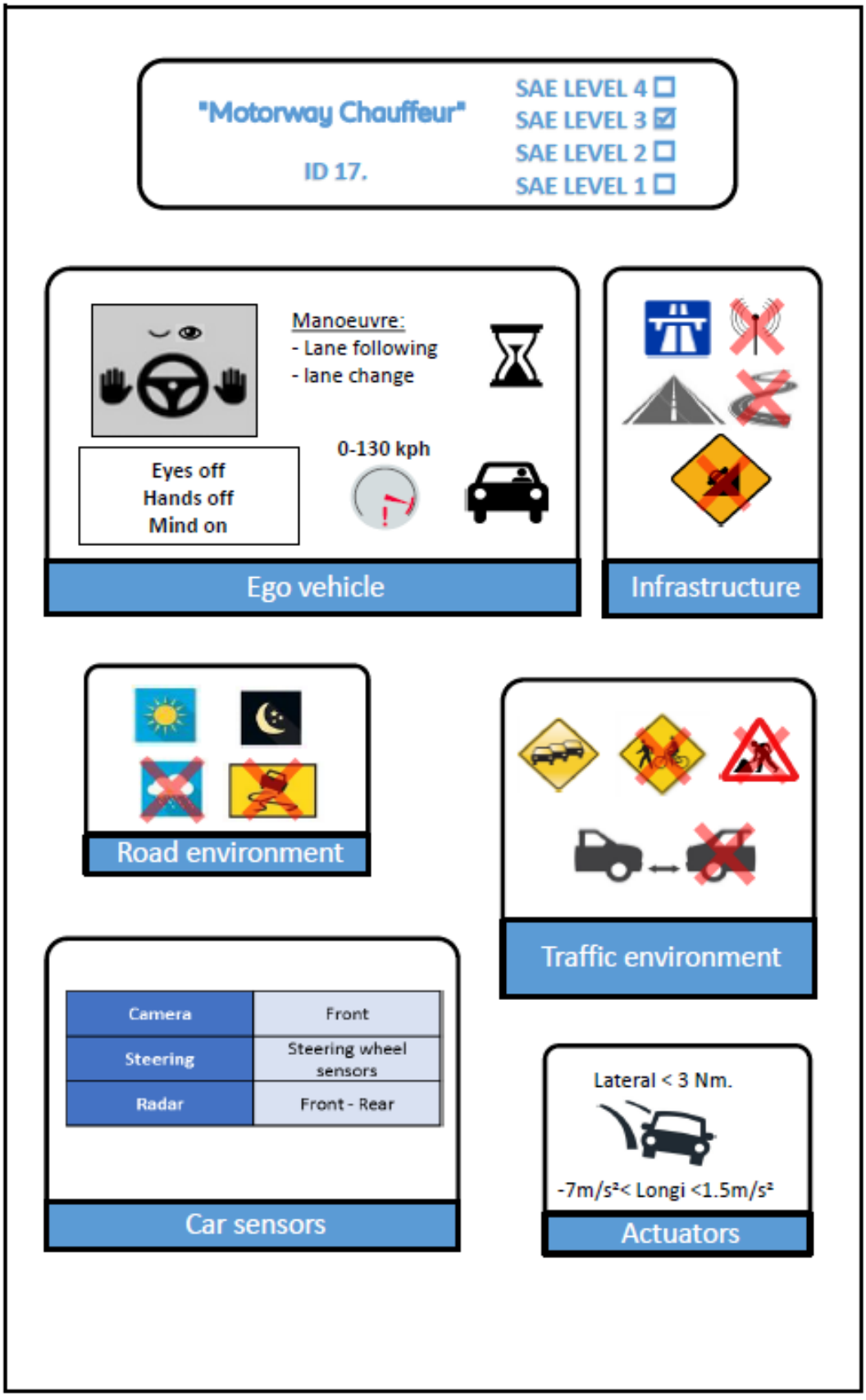

"Parking Chauffeur"
ID 12.
SAE LEVEL 4 ☑
SAE LEVEL 3 ☐
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Remote Park Level 2+ ;
Home Zone Level 4
Eyes off
Hands off
Mind on
2-10 kph
Ego vehicle
PARKING AREA
Infrastructure
Road environment
Traffic environment
Camera
Front and Surround-view
USS
Objects
Radar
Front
Lidar
(16 beams) Objects
Car sensors
Lateral < 3 Nm.
-4m/s²< Longi <1m/s²
Actuators

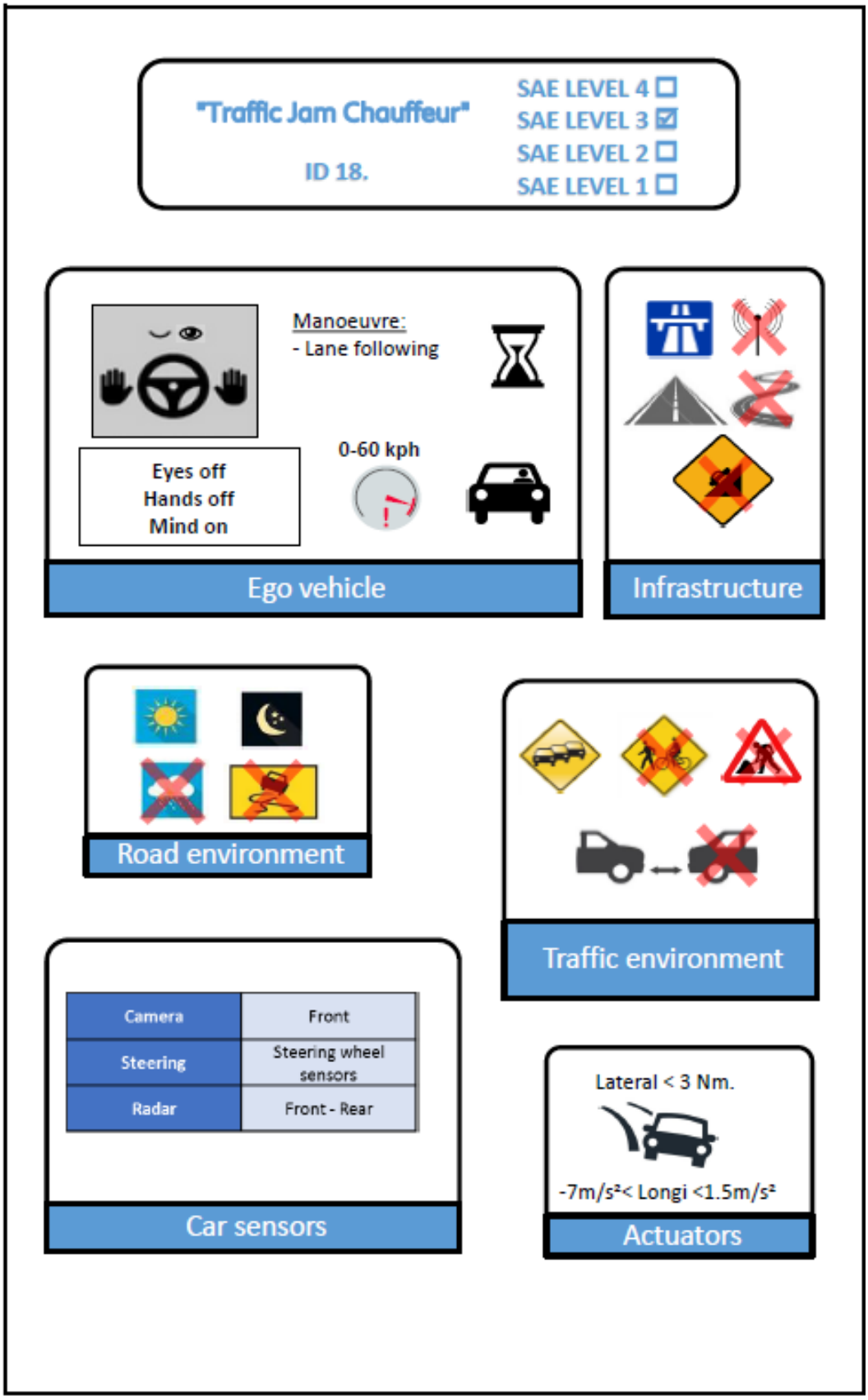

"Traffic Jam Chauffeur"
ID 13.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
Eyes off
Hands off
Mind on
0-60 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + surround + traffic
Radar
Front + surround
Lidar
Front
Steering
Driver monitoring
Ultra Sound Sensors
Objects
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators


"Parking Assist"
ID 14.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☐
SAE LEVEL 2 ☑
SAE LEVEL 1 ☐
Manoeuvre:
- Parking
- Follows learned
- Trajectory
Eyes on
Hands off
Mind on
0-3,6 kph
Ego vehicle
PARKING AREA
Infrastructure
Road environment
Traffic environment
Camera
Surround-view
Ultra Sound Sensors
Objects
Car sensors
Lateral < 3 Nm.
-4m/s²< Longi <1m/s²
Actuators


"Motorway Chauffeur"
ID 15.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Lane change
- Vehicle following (80-130 kph) & uninfluenced driving
Eyes off
Hands off
Mind off (thanks to a co-safety driver)
0-130 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front, Back & Driver Status
Ultra Sound Sensors
Objects
Radar
Front & Back & Surround
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-10m/s²< Longi <3m/s²
Actuators


"Urban Chauffeur"
ID 16.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- Intersection crossing
- Obstacle avoidance
- Lane change
Eyes off
Hands off
Mind on
0-50 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front + Surrounding + Driver
Ultra Sound Sensors
Objects
Radar
Long for Front + Short for Side/Rear objects
Lidar
Front + Surrounding
Steering
Driver monitoring
Car sensors
Lateral < 3 Nm.
-3,5m/s²< Longi <3m/s²
Actuators


"Motorway Chauffeur"
ID 17.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
- lane change
Eyes off
Hands off
Mind on
0-130 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front
Steering
Steering wheel sensors
Radar
Front - Rear
Car sensors
Lateral < 3 Nm.
-7m/s²< Longi <1.5m/s²
Actuators


"Traffic Jam Chauffeur"
ID 18.
SAE LEVEL 4 ☐
SAE LEVEL 3 ☑
SAE LEVEL 2 ☐
SAE LEVEL 1 ☐
Manoeuvre:
- Lane following
Eyes off
Hands off
Mind on
0-60 kph
Ego vehicle
Infrastructure
Road environment
Traffic environment
Camera
Front
Steering
Steering wheel sensors
Radar
Front - Rear
Car sensors
Lateral < 3 Nm.
-7m/s²< Longi <1.5m/s²
Actuators

3 Main activities conducted in SP4 (Fleet Preparation and Support)

3.1 WP4.1 and WP4.2 Management and Interactions

In the sub-project “Fleet Preparation & Support”, we aimed at:

- Providing a description and a taxonomy of automated driving functions of the L3Pilot fleet to be evaluated.
- Adapting, implementing, and pre-testing the functions in the pilot fleet vehicles.
- Providing technical support to the project.
- Considering legal issues such as compliance to laws and regulations, including data privacy and insurance.
- Considering cybersecurity recommendations.

As for the first objective (WP4.3), Deliverable D4.1 was drafted out of the responses of the questionnaire. In addition, a task force was created to propose a taxonomy (or classification) of the functions as L3Pilot was not intending to evaluate each function one by one but by groups (Motorway, Parking, Urban areas). This task force delivered two taxonomies that could be used depending on the objectives of the evaluations.

As for objective 4 and 5, the work consisted in sending a questionnaire about the regulations in place in 7 countries (France, Germany, the Netherlands, Belgium, the UK, Sweden, Italy) to conduct AD experiments. As for cybersecurity, a task force prepared a review of all aspects to be considered about cybersecurity and enhancing an approach available in the state of the art (TARA). The outcome is Deliverable D4.2, considering regulations and cyber protection.

As for objective 3, the work was included in SP6 once the experiments started.

The core of SP4 “Fleet Preparation and support” was objective 2: adapting, implementing, and pre-testing AD functions on test tracks and open roads. A table with milestones and deadlines was proposed to monitor the progress of each Pilot Leader in preparing their fleets, experimental procedures, study design, testing cars and pre-piloting. Pre-piloting means testing the whole piloting process on open roads all the way from preparing the test drivers for piloting, data collection to the analysis of first data samples.

- 8 physical general meetings (2 days) were held all over the preparation period (September 2017-May 2019) every 3 or 4 months, with all Pilot Leaders. The objectives were to monitor the progress of the preparation of the vehicles and the pre-pilots; also to generate and follow-up interactions with SP3, SP7, and SP5 for: getting prepared for the methodology, giving feedback concerning the methodology and to the evaluators about what was feasible compared to expectations and also to getting started with data loggers, data collection and data storage. Specific workshops with SP3/SP7 were organised to

look closely at study design, experimental procedures, taxonomy of AD functions and methodologies for evaluation.

- Finally, all Pilot Leaders made progress in preparing the fleets and started pre-testing their cars and data collection. Hand-over to SP6 was planned by March and was really effective by May 2019.

Results achieved:

D4.1 "Description and taxonomy of automated driving functions" was delivered in its final version in April 2019. Each of the 18 AD systems is presented in a single sheet with summarized information about how the function works.

D4.2 "Legal requirements for AD Piloting and cybersecurity analysis" was delivered in April 2019 with details on how to apply AD experiments in compliance with national regulations and recommendation on how to comply with cybersecurity issues.

The preparation status was also monitored periodically to identify best estimates of dates of piloting starting date and reasons for delay, if any. Pre-piloting started between April and November 2019 and pilots were conducted from spring 2019 to February 2021, despite several challenges (technical issues, data collection-conversion-storage issues, delay in clearance from the public authorities, availability of prototypes, changes in in-house organisation, temporary lack of resources, changes in experimental routes, pandemic, etc.).

3.2 WP4.3 AD Functions

The different AD functions tested in L3Pilot differed not only in terms of which specific type of driving they target (motorway driving, traffic jam driving, urban driving or parking) but also in the specific implementation of these functions (e.g. some functions combined motorway driving with traffic jam driving). In the type of project as L3Pilot the results of the individual functions were not reported outside the project. So, the different functions needed to be combined in such a way that still a meaningful presentation of the results was possible. In order to achieve this, a small team of partners developed a taxonomy for presenting the results. To make this taxonomy it was also necessary not only to take the number of functions in a specific category into account, but also the data that is collected by a specific test site for a specific function and whether the test site would be able to answer a specific research question as developed by SP3.

Based on the information about the different functions five different categories could be made. Motorway (or Highway) function (HW), Motorway (or Highway) function combined with Traffic Jam function (HW/TJ), only Traffic Jam (TJ), Parking function (PRK) and Urban function (URB). In Figure 3.1, the numbers indicate the number of functions being tested in L3Pilot per category.

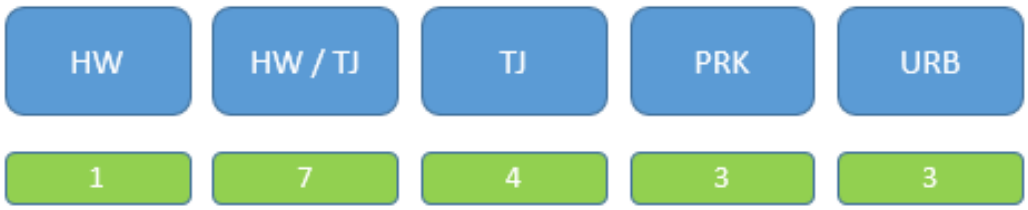


Figure 3.1: Taxonomy of functions and the number of pilot sites testing these functions.

If needed, the combined HW/TJ function could be separated based on the speed in which the individual functions operated (TJ < 60 km/h). This would lead to a higher number of HW functions and TJ functions of which the results could be combined and presented (Figure 3.2).

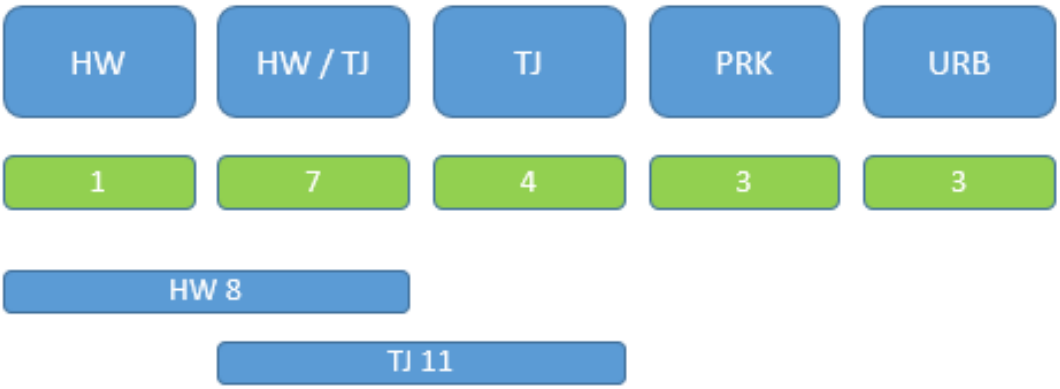


Figure 3.2: Taxonomy and numbers when combining the HW and TJ functions.

How the function operated and what the driver needed to do was highly relevant for the user and acceptance analyses. Therefore, a distinction was made between whether the driver monitored the environment, the car monitored the environment, the driver needed to be ready to take over and the car drove. Different functions were grouped along those lines (Figure 3.3).

Figure 3.3 shows that by classifying the functions along these lines for the combined HW/TJ functions and the Parking functions there is one function that fell in a single class. There could have been two solutions for presenting the results. The first solution was to combine the class with one function with one of the other classes (see the grey areas in Figure 3.3). The second solution was an option when the deviation of the results in two classes was too large to combine the results. In this case, the results of the single functions would not have been combined with any other and results would therefore not have been reported outside the project.

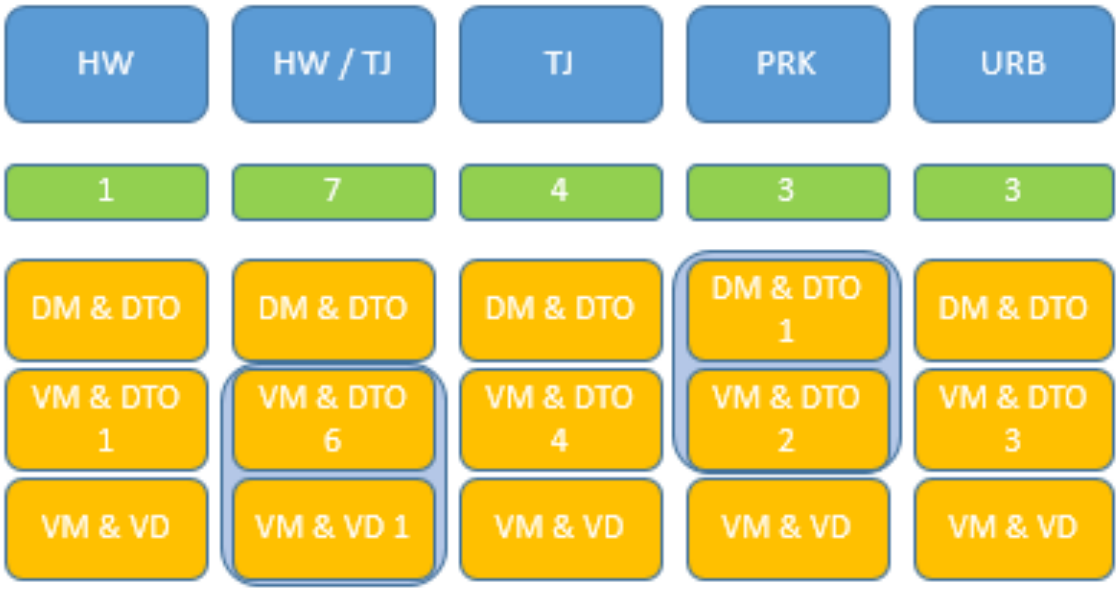


Figure 3.3: Number of different functions over different categories.

(DM = Driver Monitors, DTO = Driver take over, VM = Vehicle Monitors, VD = Vehicle Drives).

The final outcome, i.e., which of the possible taxonomies in the end have been chosen to present the results outside the project strongly depended on available data and possibilities for simulations in the evaluation part of the project (acceptance, safety, efficiency and environment, mobility). Finally, the simplest taxonomy was retained with only 3 classes: motorway (or highway), urban areas, parking (see deliverables D3.4, D7.3, D7.4).

3.3 WP4.4 Implementation of Functions

Cars that provided longitudinal and lateral control for Level 2 automated driving, were already close to market at the beginning of the project. Driver observation and system redundancy for higher automation were not yet necessary as the driver's mind was always on the task and the available redundancy (e.g., independent braking and steering) matched Functional Safety requirements for ADAS. However, vehicles with Level 3 capabilities were already in pre-development or prepared for testing on closed test tracks with professional test drivers. The legal framework did not exist yet to execute these vehicles without full supervision of the driver.

For L3Pilot, though, the focus shifted towards driving on public roads and inviting also non-professional participants to experience AD in the passenger seat or even as driver at the wheel. This required adaptation of existing vehicles and the setup of new test vehicles.

3.3.1 Working function

There are several ways to realize a given function, that is to provide a working model that takes input (sensor reading) and produces output (controlling actuators) according to rules. Virtual reality, 3D-simulator, jury-rigged prototypes, and smooth vehicles with highly integrated HMI-elements are examples for the models. These realizations are needed to test interactions with other in-vehicle systems, gather user reactions and more closely look at the boundaries of ODD. The closer the approximation to a series car the more convincing the look-and-feel of a function will be.

The need to provide rigorously checked and safety validated vehicles, ready to drive on open roads, including possibly an ordinary driver, even if only on the passenger seat, was a necessary step to gather experience. To give more people more chances to experience real automation required a real car. Therefore, the automated function needed an implementation in a car, safe and robust, that was as close as possible to the intended series product. The goal of the implementation was, therefore, to provide the real thing.

3.3.2 Vehicle

The cars, chosen for implementation, were series vehicles with extensive changes. The actuators for steering, braking etc. were either physically exchanged for the development hardware or existing actuators needed the development software that provides control pathways and additional signals that were not present in the dedicated and highly optimized series version. A computing platform was installed in the vehicle consisting of several single computers, where each one fits best to a particular task (e.g., deconvolution of fisheye cameras, collecting radar maps, running neural networks) and which allows to change software often. Extra sensors for ground truth as e.g., Lidar and cameras were needed as well and their installation outside of the car needs to withstand the expected driving speed, vibrations, and weather. The additional computing and sensors created a need for more electric power than a series generator in a car is meant to deliver, and a heavy-duty generator and extra battery were needed. Depending on the safety requirements of the use case additional controls were installed at the front passenger side of the vehicle like brake and accelerator pedal and a second steering wheel. The cost for the preparation of the prototype was usually several times higher than the base vehicle.

The vehicle model chosen for the implementation was not an indication of the series model intended for the function: after the function had been implemented in the prototype and, after further changes during testing & presentations, the blueprints and code would be handed over to the series development. Figure 3.4 gives an overview of the prototype model where each partner implemented the function.

3.3.3 Tools

Implementation of the function in the vehicle took place between the engineer's desktop workstation and the robust but often less versatile car computer or ECUs in the vehicle. Therefore, software tools were used which allow load intensive prototyping, developing and

testing at the desktop. These tools were also able to produce optimized binaries for deployment to the vehicle. In L3Pilot vehicles from 4 to 10 separate computers were needed to provide the necessary processing power in the various building blocks of the function implementations. The number of computers was not necessarily a measure of complexity but was also tied to the division of software development between internal the departments and the supplier.

With the interplay between sense-plan-act an important part of such software is the ability to collect messages from diverse sensors via CAN and UDP, provide them centrally to other compute tasks or computers (e.g., object classification, trajectory planning), collect pre-processed results and enforce a synchronization mechanism to tie parallel processes to a common time base. The software that does the collect-provide-synchronize task is often called a framework as it provides the structure to dock services on (common tools are e.g., ADTF, ROS, RTMaps, Simulink, dedicated partner software). In a typical installation the output of the framework decides the action of the vehicle. For ease of installation of cable harnesses, and robustness the actuation (i.e., controlling the vehicle via brake, steering, accelerator) is done on a single computer, that is not fast but robust. It should start in seconds and provide operating in real-time. This requirement specifies an upper bound of latency for executing a command.

For later implementation in the series vehicle the software is stripped of many debugging capabilities and optimized so that it eventually runs on few, small and dedicated ECUs – otherwise, the cost and volume of installation would be prohibitive.

Figure 3.4: Overview of prototype vehicles where the functions were implemented.

3.3.4 Hand-over

At the end of the work package “Implementation of Functions” the functions were working in the test vehicles as intended. The automated functions had been polished during intensive testing and were integrated for robust operation. The vehicle could be started and operated in the field without the need for a specialist. The data logging equipment had been installed but still needed to be assured to deliver the signals needed for later analysis.

The preparations to obtain a driving permission, although started much earlier, were extended somewhat in the next phase in some instances. The dossiers or the vehicles needed still to be presented to the road authority and some documents needed updates after that. This was understood as few previous processes for automated driving existed prior to this project.

3.4 WP4.5 Pre-Piloting

Pre-piloting mainly consisted of monitoring preparation of the fleet and preparation of the experimental design for the pilot could start with everything fixed and safe. A table was drawn up to monitor the progress of each L3Pilot site and identify blockers (Table 3.1). The table was supposed to be as comprehensive as possible in the activities to conduct while preparing the Pilots (i.e. technical readiness of prototypes, ADF installed, adapted and tested; loggers installed and tested, video installed, compliance with regulation, participant selection, readiness of the data tool chain, first data analysis done).

Table 3.1: Overview of prototype vehicles where the functions were implemented.

Activity	Planned Milestone	Status
Vehicle technically ready		
ADF adapted to the vehicle		
ADF tested and approved		
Logger installed and tested		
Video and/or eye tracking installed		
Vehicle approved for public roads		
Test subject selection and training		
Questionnaire ready		
First test trips performed		
Data upload tool implemented		
Database ready		
Signals in Common data format		
Simple data analysis performed		
Ready for piloting (first vehicles in ramp-up)		

This table was periodically updated and examined at each SP4 meeting over the period of 21 months, the time allocated for the fleet preparation. It gave a good overview of the status of the pilot sites for each activity compared to the initial planning and was a useful tool for SP6 (Piloting) to consider potential of piloting depending on pilot sites.

It of course provided the project with updated information about technical status of the fleet (Installation and testing of ADFs, data loggers and cameras) as well as information about pilots and the experimental conditions (compliance with regulation, participant recruitment, readiness of the data tool chain, data analysis).

This information was periodically shared with SP5 (Data) and SP3/SP7 (Methodology and Evaluation) so that they can plan their activities depending on date of start of pilots and expected end of data collection.

3.5 WP4.6 Legal aspects and cybersecurity

3.5.1 Legal Requirements for AD Piloting summary

WP4.6 provided a collection of regulations regarding AD experiments over seven countries. This was intended to provide a comparative overview in a variety of European countries. Some regulations were more detailed and spelled out e.g., the mileage demanded in simulation or test track driving, or they required the streets where the experiment took place. Other regulations were less specific and recommended safe practices in more general terms.

All Pilot Leaders in L3Pilot implemented internal processes regarding how to conduct experiments on public roads. These processes were based on their consolidated experience with prototypes and on the knowledge collected during the development of similar products (e.g., ADAS functionalities), with the objective of maximizing safety for all road users, not forgetting the driver/passengers of the test vehicle. Such processes included driving permits for prototype vehicles, medical tests and specific training for unexpected behaviour of the vehicle or the environment. In addition, a detailed examination of functional safety had an integral role in the process, and in this respect the system developers strived to include a large range of use cases.

3.5.2 Cybersecurity Analysis summary

One of the motivations of this work was the need for a cybersecurity assessment of AD functions being tested in the L3Pilot. In the L3Pilot context, the vehicles under analysis were prototype vehicles that were driven/piloted by a mix of professional and normal drivers under uncontrolled environment. Automated driving systems might be highly interconnected and networked cyber-physical systems and their implementations varies among pilot sites. The AD applications such as Motorway, Urban, and Parking Chauffeur were supported by different levels of automation among Pilot sites. Therefore, all threats were taken into account focusing mainly on the remote exploitation by nonusers of the vehicle. Figure 3.5 represents a generic reference architecture of an autonomous vehicle (red flash denotes vehicle attack surfaces; green flash signals denote remote attack surfaces).

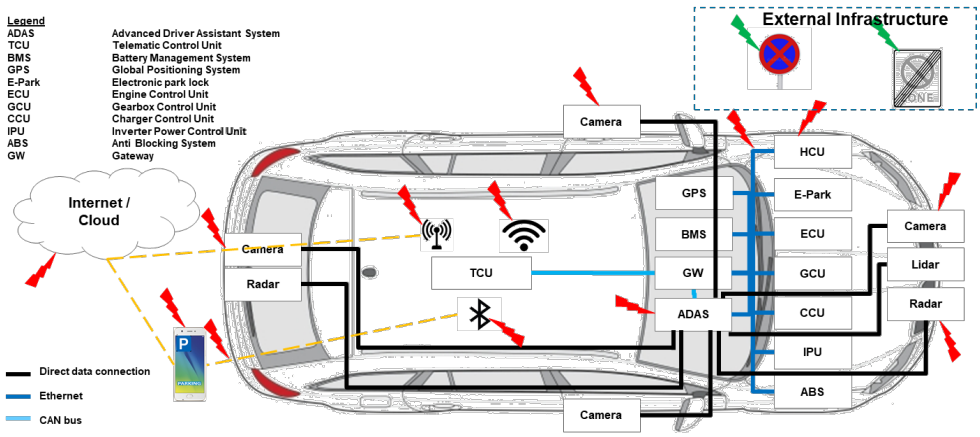


Figure 3.5: Reference Architecture for Risk Analysis.

Threat Analysis and Risk Assessment (TARA) helps identify various system vulnerabilities systematically by a categorisation for mitigating them with respective countermeasures. As technology improves and expertise becomes accessible, more sophisticated threats emerge, and an initial threat identification becomes obsolete. Therefore, there is a need to take a more flexible view of the risk, which ensures that new forms of attack can be recognised, and responded to, over the system lifetime. In this respect, these challenges were addressed by:

- Developing an application-based approach as opposed to a component-based one.
- Integrating a “controllability factor” in the risk assessment to quantify the system’s resilience during the time of the analysis (see deliverable D4.2, Table 5.1).

The approach promoted the synergy among the three well-known standards on AD systems taxonomy (SAE J3016), automotive security (SAE J3061) and functional safety (ISO 26262), and its extension (PAS SOTIF 21448). The model built is based on the Threat Analysis and Risk Assessment (TARA) framework proposed in the SAE J3061 “concept” phase. The proposed threat model is named TARA+. The contributions are:

- Quantification of the threats, based on attack potential and attack impact as defined in the SoA (Service Oriented Architecture).
- The definition of “controllability levels” for the AD system based on the principles of system availability, safety, and integrity (Bolovinou et al., 2019, Table III).
- The formation of “controllability factor” as an AD system/driver shared property (the proposed “controllability” takes into account the levels of automation from SAE J3016) and its integration in the TARA framework by modifying the attack’s impact factor.
- A modified attack impact calculation which integrates the proposed “controllability factor” (Bolovinou et al., 2019).
- A 2D risk matrix, based on attack potential and proposed modified impact.
- An attack surface analysis with the “controllability” of an attack (Bolovinou et al., 2019).

This cybersecurity work focused on the threat analysis and risk assessment of AD systems of level 3 and higher. To this end, a novel controllability definition and classification was proposed that handles both the AD system and the driver in a joint scheme. The proposed TARA+ methodology constitutes a proof of concept towards designing a controllability-aware security analysis framework of AD systems, as early as in the concept phase of their design, combining the strengths of the well-known SAE and ISO standards in the field. As AD systems progress to production stage and new applications are developed, the framework may need to be re-applied to account for new information on both the system design and the available security countermeasures. As argued in Monkhouse et al. (2017) the notion of controllability needs to be expanded to holistically consider controllability for the driver, for other road users and for the system itself. This is left for future work.

Based on the D4.2 deliverable, an additional work was done. It features a technical paper on cybersecurity analysis of a V2X assisted manoeuvre on highways by an automated vehicle. The authors of the publication cast the problem on the V2X domain focusing on the RSU side (in contrast to the AV centric analysis of the L3Pilot) and they applied the TARA+ framework for the risk analysis (Chen et al., to be submitted): the off-board information provided through V2X systems can produce a significant difference in the safety and efficiency of the higher level autonomy AD systems where the on-board sensors can be impaired by an occlusion such as V2X-assisted highway merging. However, new attack surfaces can emerge due to the wireless connectivity in V2X-assisted autonomous vehicles, which must be understood and addressed before the commercialisation of AD systems. Therefore, a generic reference architecture (RA) to model a V2X-assisted merging function that fuses off-board radar and camera sensors with the vehicle's on-board sensors was designed. The RA is used to identify the attack surfaces and analyse cybersecurity threats. The STRIDE threat classification was adopted, and the potential threat actor profiles were assessed to be able to attack the target surfaces. All these features are utilised in the TARA+ for quantifying the risk of each attack. The potential mitigation strategies were also discussed for the underlying attack surfaces within the context of the subject AD system.

As a conclusion of the D4.2 work, high-level recommendations for further use by the L3Pilot prototype vehicle owners during the project’s pilot preparation phase and beyond, were proposed for planning against cyber-attacks for the entire L3 vehicle lifecycle. For this purpose, the recommendations were based on the literature review (e.g., NHTSA, 2016), the L3Pilot OEM questionnaires/interviews, and the results of D4.2 TARA+ analysis. Technical recommendations in the form of countermeasures per attack vector as identified in our work can be found in the general analysis part of D4.2 Section 3 and in particular in Tables 3.2 to 3.4 (L3Pilot, Deliverable D4.2).

4 Conclusions and Lessons learnt

Overall, the SP4 “Fleet preparation and support” was successful in preparing the prototypes fleet for piloting (i.e., ADF implementation and testing) and in conceiving the experimental design (routes to be driven, types of participants, safety concept including safety drivers, identification of baseline, number of kilometres to be driven, etc.).

Pre-piloting started between April and November 2019 and pilots were conducted from spring 2019 to February 2021, despite several challenges (technical issues, data collection-conversion-storage issues, delay in clearance from the public authorities, availability of prototypes, changes in in-house organisation, temporary lack of resources, changes in experimental routes, pandemic, etc.). Pilots collected 200 000 kilometres of data in AD mode and 200 000 kilometres of data for baseline, mostly on motorways but also in urban areas and in parking spaces. At the end, 750 participants drove 70 prototypes, sometimes just for a few minutes, sometimes for a few hours, sometimes one shot, sometimes several rounds for each participant.

This preparation phase benefitted from past experience of the Pilot Leaders in setting large-scale experiments, either internally or in EU-funded projects such as Euro-FOT or U-Drive, but it was also the opportunity to gain additional knowledge about setting that kind of challenging experiments, noticeably because of the special and unusual size and nature of the trials: testing prototypes with high level of technology, collecting large amount of data and ensuring the highest safety of participants and surrounding traffic.

We report below the main lessons learnt during this phase of the project.

4.1 Constitution of the experimental fleet, safety, technical pre-tests and experimental design

- Build-up of a prototype vehicle for test-track use only (in advance of building up the piloting vehicles) is helpful for the validation of the AD function and technical concept as well as for the first discussions with authorities in order to save time on the approval later with the piloting vehicles.
- Test cars are usually continually updated (e.g., software modifications, sensor calibrations, etc.) or driven in different regions which demand diverse map data formats. It is therefore critical to ensure that data collected over a long period or on varied regions considers these updates/variabilities and make them consistent from the beginning to the very end.
- Pre-tests are extremely important to be able to pass on to the actual testing of the fleets. When Piloting starts, the complete data collection chain must have been validated and proven to work.

- AD piloting on public road potentially demands new safety concepts and processes. This requires additional time and technologies (e.g., special training vehicles, special trained safety drivers). A specific method to generate the safety requirements is therefore recommended, in addition to the usual one set up for open roads experiments. Many Pilot leaders (if not all) generated specific internal processes and validation requirements to make sure that safety is the highest priority, even though it is conflicting with experimental design requirements (e.g., continuous presence of safety drivers in charge of taking over control in case of whatever potential hazard even if it limits the potential to collect data on traffic conflicting situations).
- Even though the project initially allocated 18 months for the preparation of the pilots (assumed to be comfortable), it is wise starting as soon as possible since safety, technical and organisation issues take more time to be solved than it looks at first. For example:
  - having normal drivers not experienced to automated systems with the possibility of full Level 3 hands-off, eyes-off driving made a safety-driver a legal "driver of the vehicle" and fall-back driver during AD mode necessary. Subsequently, special safety-driver training and functional adjustments in the vehicle such as driving school pedals were required.

    This safety-driver training needs time and effort that should not be underestimated, e.g., to agree on the content of the training, selecting suitable drivers, the training itself and approval from authorities. Likewise, for driving school pedals.

    In some cases, a monitoring system had to be developed to inform the safety-driver or a supervisor (seated on front-passenger seat or on the back seat) on the system status, e.g., to immediately show errors. This always allowed a correct supervision of the AD system without having to see the instrument cluster in front of the driver. This system was, especially in Germany, one of the conditions for authorities to allow the concept of normal drivers as participants and safety-drivers as fall-back and this worked well during piloting.
  - Using test vehicles with AD prototype systems requires more effort for testing and bug-fixing, compared to fleet test with nearly mass production ADAS.
- Safety or professional drivers training was conducted pilot site by pilot site. It worked pretty well but Pilot leaders recognize that harmonizing a safety-driver training for all pilot sites from the start would be ideal for consistency between pilot sites and especially consistency between data collected in different regions where participants and safety drivers were given different instructions.
- It happened that the public asked questions during the trials. We therefore recommend that, in addition to available communication means such as leaflets and booklets, a Q&A sheet about the project is available in the car to answer on the road public questions.

- The placement of video cameras inside the vehicle is more challenging than expected due to compliance with crash safety. For example, in some instance it was difficult to mount a video camera in front of the driver to avoid being an obstacle in case of a collision. The camera must be mounted somewhere else, but it can hinder the human factors analysis if it is not framing the face of the actions of the driver appropriately. A compromise solution had to be found between safety and requirements for analysis.
- As for data collection and conversion to common data format (more lessons learnt are available in D5.2 “Guidelines and lessons learnt on Pilot Tools and Data”):
  - Anticipate that internal data storage may require a specific data format, different than the project format.
  - Data conversion from raw data collected in the car to “common data format” was generally more challenging than expected (e.g., correct identification and decoding of relevant signals from the bus system, algorithm to develop for conversion) and has generated more efforts and resources than initially planned. More time should be allocated to this task in the future.
  - AD function requires many sensors and video. Therefore, logging needs to enable high data rates and time synchronization issue (e.g., requires SSD RAIDs, Ethernet cameras, and stream compression).
  - Handling huge data amounts brings classical corporate IT systems to boundaries. Cloud-based approaches are preferred but it is time consuming to set up.
  - Online streaming of driving data for evaluation purposes, also enabling real-time data analytics would be a good alternative for data storage and processing in the future (on the cloud). Classical embedded automotive architectures (based on reading from CAN bus) need to be extended with a smart and secure communication gateway component responsible for supporting the vehicle data cloud-based streaming (efficient reading, publishing data from the vehicle to the cloud and back).
  - Handling big volumes of video data and their synchronization with vehicle CAN data brings requirements for smart data synchronization and compression on-board to minimize local data storage needs.
  - Early exchange of data between data engineers and Pilot leaders is necessary. Ideally, even before the pre-piloting phase to test the data suitability, transfer, and access.
  - Meta data is important for the data management and the data analysis. It should be examined with higher care in follow-up projects.

4.2 Clearance from the Public Authorities

- Generally, constituting dossiers, submitting the application, and getting the approval from Public Authorities to carry out AD experiments on open roads is very time-consuming

given all dossiers to be submitted, the duration and sometimes due to numerous intervening factors. Challenges to get clearance is even higher when clearance is requested in another country. Subsequently, the activity must get started right from the very start of such projects.

- Sometimes, the approval to experiment L3 function on public roads excluded certain situations (construction sites, difficult weather conditions …). During pre-pilots, moving construction sites on the designated test route hindered smooth vehicle testing. Therefore, excluded situations and piloting route need to be considered before first trips and for pilot planning.
- Beside the clearance from Public Authorities because of national laws and regulations regarding automated driving trials, GDPR (General Data Protection Regulation) compliance activities must also henceforth start at the very beginning of the project.
- With the expected increase of cross borders or multiple countries experiments by OEMs or other bodies, L3Pilot recommends that a jump in harmonizing / standardizing regulations relating to the automated driving experiments, at least at EU level, is done for simplifying and make requests and approval processes consistent and even unique across countries.

4.3 Cybersecurity

- Dealing with new AD functionality w.r.t cybersecurity aspects requires extension of Threat Analysis and Risk Assessment (TARA) tools to handle system-driver joined sharing of control.
- Safety and security co-engineering are very important and only recently supported in the level of technical guidelines by the new ISO 21434 standard (which introduces the Automotive Safety Integrity Levels, following the concept of the *popular ISO26262 ASIL* levels). In the L3Pilot, TARA+ framework proposed for the analysis of L3 and up AD functions, an attempt to integrate the ISO 26262 notion of driver 'controllability' in the risk analysis framework by also adding a system 'controllability' factor, has been made. More research in this is needed for the better quantification of the system 'controllability' in automated functions and its relationship with cybersecurity TARA concept design step.
- The same autonomous driving functions may be developed differently by OEMs. It may include differences in system architecture and sensors in use. It is crucial to develop a Reference Architecture, which should be sufficiently comprehensive to reveal attack surfaces and potential track of a cyber-attack, but also higher-level to cover the systems of different OEMs.
- Due to limited resources for security, the system developers need to prioritise certain threats which contain higher likelihood or impact. Risk assessment needs to be run to have insights on this.

Propositions and recommendations will certainly be taken into consideration in follow-up projects such as Hi-Drive, and other in-house initiatives. In any case L3Pilot explored new domains in setting up large-scale multi-centric experiments and adapted the FESTA approach with new challenges that were properly overcome: technical readiness of cars equipped with complex technology, experimental design with higher safety requirements, collection/conversion/storage of big amount of complex data, compliance to new regulations (AD and GDPR), and last but not least, the SARS-COV-2 pandemic. SP4 “Fleet Preparation and support” was not affected by the pandemic since it was completed by mid-2019 but SP6 “Piloting” showed that trials stopped for a while and re-started with even higher health and safety requirements.

References

AdaptIVe Project – Co-funded by the European Union under the 7th Framework Programme. Available at: www.adaptive-ip.eu [05.01.2018].

A Bolovinou, U. Atmaca, A. T. Sheik, O. Ur-Rehman, G. Wallraf and A. Amditis, "TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems," 2019 IEEE Intelligent Vehicles Symposium (IV), Paris, France, 2019

Brussels, Belgium, 2018 SAE International. AE classification of automated driving levels Available at: http://standards.sae.org/j3016_201609/ [05.01.2018].

C. Chen et. Al., Analysing Cyber Attacks and Risks inV2X-Assisted Autonomous Highway Merging, Status: to be submitted

Inagaki T, Sheridan TB. (2018), A critique of the SAE conditional driving automation definition, and analyses of options for improvement, https://link.springer.com/content/pdf/10.1007/s10111-018-0471-5.pdf.

ISO/FDIS 26262 2nd Ed., TC 22/SC32/WG08, Road Vehicles – Functional SafetyParts 1-12", Mar 2018.

J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," Black Hat Eur., pp. 1–13, 2015.

L3Pilot project, D4.1, Description and taxonomy of AD functions. Available at: https://l3pilot.eu/fileadmin/user_upload/Downloads/Deliverables/L3Pilot-SP4-D4.1-Description_and_taxonomy_of_AD_functions-v2.0_for_website.pdf

L3Pilot project, D4.2, Legal Requirements for AD Piloting and Cybersecurity Analysis. Available at : https://l3pilot.eu/fileadmin/user_upload/Downloads/Deliverables/L3Pilot-SP4-D4.2-Legal_requirements_to_AD_piloting_and_cyber_security_analysis-v1.2_for_website.pdf

H. Monkhouse et. al., Why Functional Safety Experts Worry About Automotive Systems Having Increasing Autonomy, August 2017, Conference: International Workshop on Driver and Driverless Cars: Competition or Coexistence.

National Highway Traffic Safety Administration. (2016, October). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC.

SAE J3016, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, 2018.

SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE standard, 2016.

TUV Austria, Highly Automated Driving, The new challenges for Functional Safety and Cybersecurity, White paper,, Vienna, October, 2018.

List of Abbreviations and Acronyms

Abbreviation	Meaning
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Function
AV	Automated Vehicle
DDT	Dynamic Driving Task
HC or HW	Highway Chauffeur, Motorway Chauffeur
HTJC	Highway Traffic Jam Chauffeur
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
PC or PRK	Parking Chauffeur
SoA	Service Oriented Architecture
TARA	Threat Analysis and Risk Assessment
TJC or TJ	Traffic Jam Chauffeur
V2X / V2V / V2I	Vehicle to Everything / V. to Vehicle / V. to Infrastructure