Information and technology law course

LECTURE 16 – 15 NOVEMBER 2024

FEDERICA CASAROSA – 2024/2025

Autonomous driving vehicles

Autonomous driving

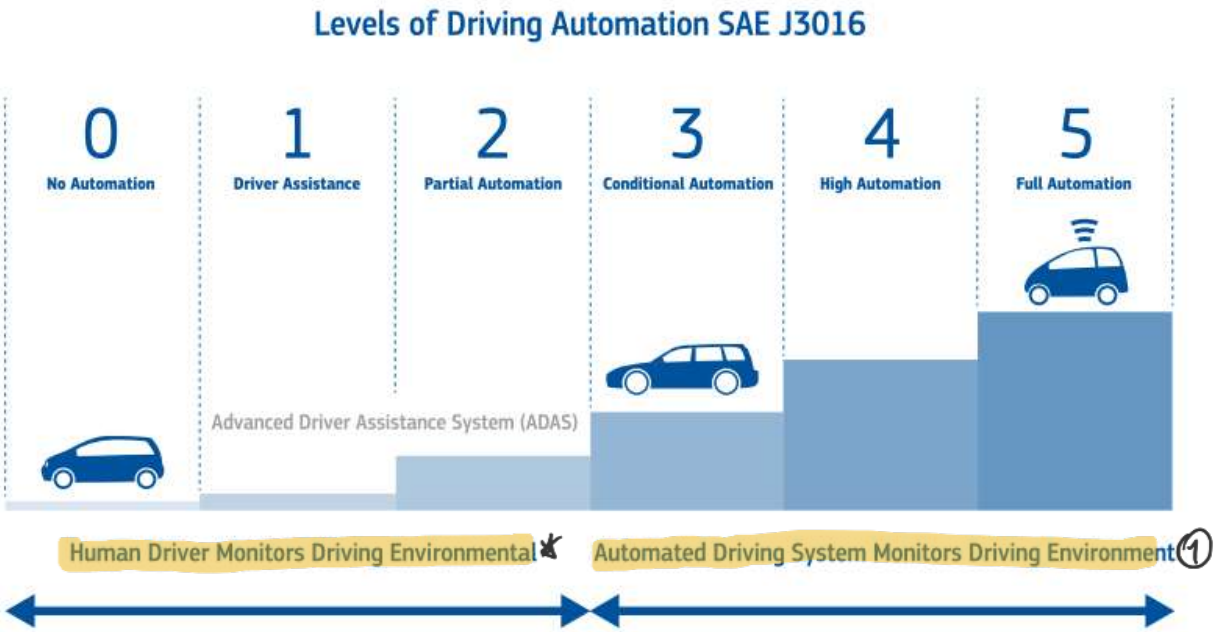

Figure 1. Vehicles automation levels as defined in SAE J3016.

2018 Taxonomy

* Facilitate some of the parts of driving activity, but not many

① Automated driving system controls the environment.

AI has opened new realm: ②

Some of the new cars are able to achieve a certain level of automation.

② High level of automation: system can learn to react to triggers. Idea is reducing mortality, congestions exc. Accidents happen because of limited level of control over the vehicle.

Connectivity

automated driving: communicate infrastr. and devices outside the cars.

- Vehicle-to-Network (V2N) = Verify what is happening: real time traffic info. Embedded in the car.
- Vehicle-to-Vehicle (V2V) = Allow each car to connect and exchange info regarding location, speed, steering wheel position *
- Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) ①
- Vehicle-to-Person (V2P) = Connect smartphones and wearable devices, so pedestrians can share data with cars.
- Vehicle-to-Device (V2D) and Vehicle-to-Everything (V2X) ②

* To coordinate cars better. There of course should be sensors to do so.

① Possible to communicate with road infrastructure, for ex. related to traffic, work activity.

② Future: allow connection with every other device available. How to improve car understanding what is going on.

Current available features of Avs

- Up to today most functions have been primarily designed to assist drivers rather than replace them by providing warnings, or taking control of the vehicles in limited situations.
- In the future, with fully developed AVs, these functions are part of the driving process and, essentially, contribute to replacing the driver

Lane Change and Blind Spot assistance, automated parking, collision avoidance systems, traffic sign recognition (w. camera sensors)

AV sensors and hardware

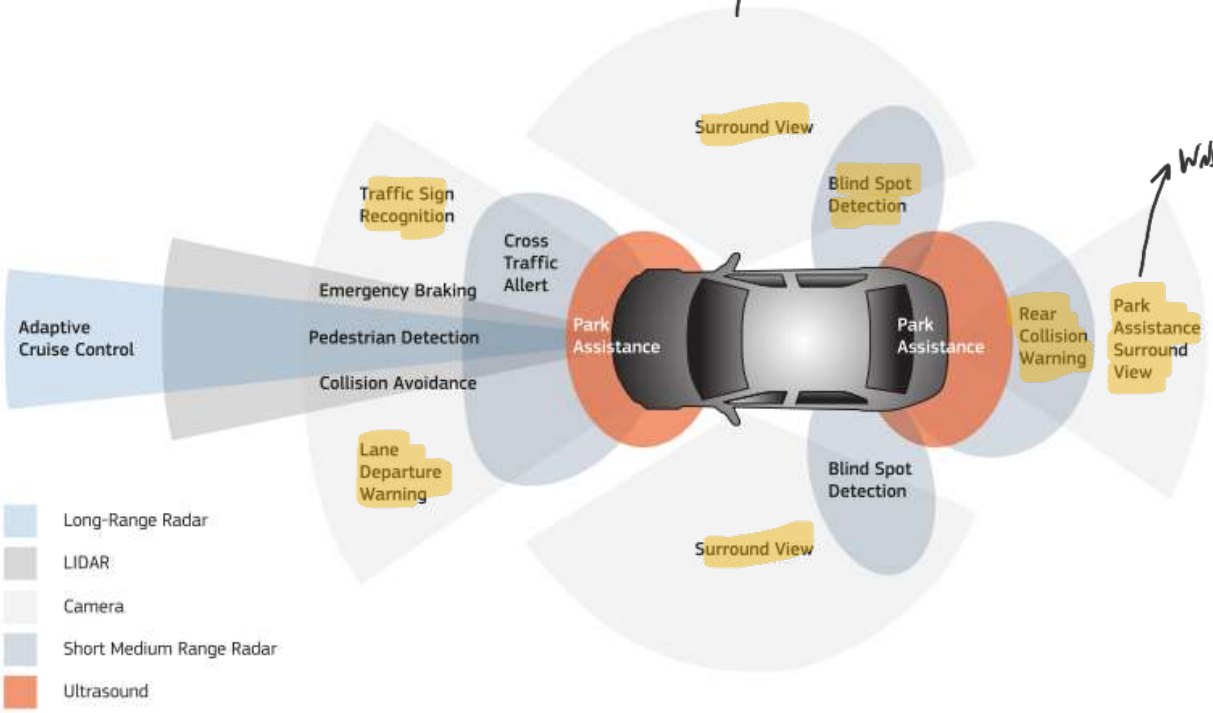

Figure 5. Localization of the sensors on the vehicle and their main uses.

Technical tools used to allow you what is around[1], understand distances[2], interpret elements to make decision (understand presence of obstacle, identify the obstacle: is it a pedestrian? A rock? A Tree?. This requires not only perception but interpretation: step forward, if I interpret it can decide how to react: Changes in the activity of the cars, change speed, trajectory (if there's a pedestrian they can move too))

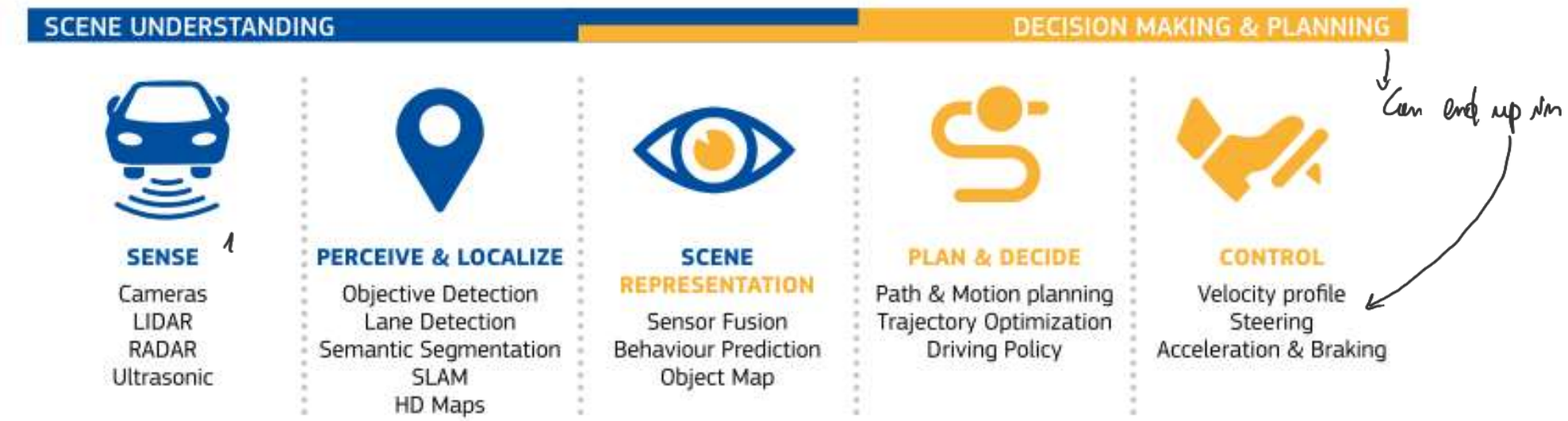

Figure 2. Typical elements of autonomous driving systems. Inputs from the environment are obtained from the sensors of the vehicle or external mapping information. They are used to perceive and understand the environment, plan the trajectory of the vehicle, and act on the vehicle's commands.

The role of AI in Autonomous vehicles

Data can be used to perceive and understand reality, processing can be used to make decisions (either by driver or AI!). AI is one of the most important techs that can be used.

AI technologies in AV

- Object recognition
  - Detecting (localization) and classifying objects in an image
- Segmentation
  - A label is assigned to each region to classify them into prescribed categories
- Vehicle localization
  - Technique used to estimate using a sequence of images captured over time by the camera mounted on the vehicle
- Tracking of objects
  - Technique used to determine the dynamics of moving objects.

= of course simplified: interpret and define patterns and rules of available data. IN AV this applies like:

⇒ Training is fundamental for this. We need to recognise things.*

↳ how is the car moving? How far/far objects are? Can other objects move? How quick? Type of reaction?

Dynamic of moving obj. is to be done with machine learning.

*Size analysis is also important, is it something far away? No? Etc. Make it possible for system to learn. Bounding is crucial.

Wrong set of data will bring biased results.

interpreting information and control

Automotive Functionality	Software Components		
	Perception	Planning	Control
Detection of roads	X		
Detection of lanes	X		
Detection of agents	X		
Traffic sign recognition	X		
Markings recognition	X		
Tracking of objects	X		
Localization	X		
Occupancy maps	X		
Routing		X	
Behaviour modelling		X	
Motion planning		X	
Trajectory execution			X
Sound event recognition	X		

AI technologies in AV

Cybersecurity issues

- Intentional threats
  - malevolent exploitation of the limitations and vulnerabilities present in AI and ML methods to cause intended offence and harm
- Unintentional threats
  - side effects of benevolent usages, due to open issues inherent in the trustworthiness, robustness, limitations and safety of current AI and ML methods

‘Old’ example

https://www.youtube.com/watch?v=MK0SrxBC1xs

User being control by an outsider. With no control of what was happening.

not possible for driver to control.

Table 1. Common cyber threats to autonomous vehicles and their impacts.

Threat Type	Description	Real-World Examples	Potential Impacts
Remote Hacking	Unauthorized access to vehicle systems via wireless communication	Jeep Cherokee hack (2015)	Vehicle control takeover, disabling functions, safety risks [18]
Sensor Manipulation	Interference with sensors like LiDAR, radar, cameras	Tesla autopilot deception (2016)	False obstacle detection, erratic behavior, collisions [19]
Data Breaches	Unauthorized access to sensitive data stored or transmitted by the vehicle	Electric vehicle manufacturer server hack (2020)	Privacy violations, identity theft, compromised decision-making [20]
DoS Attacks	Overloading vehicle's systems to disrupt normal operations	DDoS attacks on vehicle-to-infrastructure networks	Performance degradation, connectivity loss, vehicle immobilization [21]

(Saturation of the vehicle comm. channels)

Durlik, I.; Miller, T.; Kostecka, E.; Zwierzewicz, Z.; Łobodzi ´nska, A. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? Electronics 2024, 13, 2654.

① Who's the driver, real time location, driving patterns, insurance information;

Table 2. Existing countermeasures in AV cybersecurity.

Countermeasure	Description	Benefits
Intrusion Detection Systems	Monitoring network traffic for malicious activity	Real-time threat detection, anomaly identification [64]
Encryption	Securing data in transit and at rest	Protects data integrity and confidentiality [65]
Regular Updates	OTA updates for software and firmware	Addresses vulnerabilities, enhances functionality [66]
Authentication Protocols	Ensuring only authorized access to vehicle systems	Prevents unauthorized access, secures communication [12]

Durlik, I.; Miller, T.; Kostecka, E.; Zwierzewicz, Z.; Łobodzi ´nska, A. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? Electronics 2024, 13, 2654.

European interventions

1. 2016, the European Commission adopted a European Strategy on Cooperative Intelligent Transport Systems,
2. In 2016, the Member States and the European Commission launched the C-Roads Platform to link C-ITS deployment activities,
3. In 2018, the European Commission published the EU Strategy for mobility of the future (2)
4. In 2019, the European Commission has set up a Commission Expert group on cooperative, connected, automated and autonomous mobility, named "CCAM" (4)
5. In September 2020, report on Ethics of Connected and Automated Vehicles
6. Regulation 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users (Vehicle General Safety regulation)

① Was starting to launch this C-ITS, based on the idea of finding out a way to create an automated mobility system. Have a system that can allow different countries and infrastructures to speak to each other (ex. traffic signs in different countries).

② 2018: EU strategy for mobility in the future (from 2017 initiative on safety regulations in order to address road fatalities and injuries): strategy (guidelines for future years) was to focus and have a pilot on CS of infrastructures that was going to achieve a secure and trustful communication between vehicles and infrastructures for road safety and traffic management.

③ 2019 saw the setup of a commission expert group on cooperative, connected, automated and autonomous mobility, which was trying to provide advice and support commission in order to create another pilot in the direction of CS infrastructures trying to foster experience sharing and learning to create something useful, which resulted on the 2020 Report on Ethics of Connected and Automated Vehicles.

Regulation was a result of lot of discussions.

International interventions: UN Regulations No. 155 and 156

UN Regulation No. 155 on Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

- requires a Certificate of Compliance for Cyber Security Management System from a vehicle manufacturer in order to have its vehicle approved for use on public roads
  - 'a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks'
  - Such as processes used for the identification of risks to vehicle types and processes used for testing the cyber security of a vehicle type (e.g. mitigation methods of different cybersecurity risks, including measures to prevent and detect unauthorized access shall be employed).
- Objective: ensure no one can gain unauthorised access to the vehicle's system.

Before, vehicle connected. Now, software embedded, so we have different manufacturers for example.

International interventions: UN Regulations No. 155 and 156

UN Regulation No. 156 concerning Uniform provisions concerning the approval of vehicles with regards to software update and software update management Software update: ⓪

- requirements on how to update the software of the vehicle
  - Certificate of compliance for Software Update Management System.
  - It is a systematic approach defining organisational processes and procedures to comply with the requirements for delivery of software updates
  - Such as
    - a process whereby any interdependencies of the updated system with other systems can be identified
    - a process to establish the compatibility of the update with the target vehicle configuration

→ Identify dependencies that can show vulnerabilities.

① Need to verify that in case of SW inside a vehicle

Those are looking at each other at different sectors: attacks can come from vehicle but also SW.

EU legislation

Vehicle General Safety Regulation 2019/2144

- Entered into force 6 July 2022

- Objectives:
- Introduce mandatory advanced driver assistant systems to improve road safety and establishes the legal framework for the approval of automated and fully driverless vehicles in the EU.

We are aware that AV will have additional risks due to connection to external entities. We need to take into account what other measures are implemented. (UN Regulations at the time were not existed)
There was NIS, CS act almost there exc...

Vehicle general safety regulation

(26) The connectivity and automation of vehicles increase the possibility for **unauthorised remote access to in-vehicle data and the illegal modification of software over the air.** In order to take into account such risks, **UN Regulations or other regulatory acts on cyber security should be applied on a mandatory basis** as soon as possible after their entry into force.

(27) Software modifications can significantly change vehicle functionalities. Harmonised rules and technical requirements for software modifications should be established in line with the type-approval procedures. Therefore, UN Regulations or other regulatory acts regarding software update processes should be applied on a mandatory basis as soon as possible after their entry into force. However, those **security measures should not compromise the obligations of the vehicle manufacturer to provide access to comprehensive diagnostic information and in-vehicle data relevant to vehicle repair and maintenance.**

Encryption can protect data. But what if I have to take car to mechanic? There needs to be exclusion relating to maintenance.

general reg.: whatever the car

Vehicle general safety regulation

Article 4 General obligations and technical requirements for vehicles in the scope of reg.

whatever is a road vehicle

5. Manufacturers shall also ensure that vehicles, systems, components and separate technical units comply with the applicable requirements listed in Annex II with effect from the dates specified in that Annex, with the detailed technical requirements and test procedures laid down in the delegated acts and with the uniform procedures and technical specifications laid down in the implementing acts adopted pursuant to this Regulation, including the requirements relating to:

- (a) restraint systems, crash testing, fuel system integrity and high voltage electrical safety;
- (b) vulnerable road users, vision and visibility;
- (c) vehicle chassis, braking, tyres and steering;

} Traditional parts

- **(d) on-board instruments, electrical system, vehicle lighting and protection against unauthorised use including cyberattacks;**
- (e) driver and system behaviour; and
- (f) general vehicle construction and features.

Within sets of requirements could and ensure before can put on the market there should be called also the onboard systems.

Art. 6 also points to advanced vehicle systems; specific for particular systems: driver warning, black recording etc.

Additional cases for advanced systems. Out in general, even for advanced vehicles w have CS requirements. Not well defined but there at least.

In relation to AV

Vehicle general safety regulation

Article 11 Specific requirements relating to automated vehicles and fully automated vehicles

1. In addition to the other requirements of this Regulation and of the delegated acts and implementing acts adopted pursuant to it that are applicable to vehicles of the respective categories, automated vehicles and fully automated vehicles shall comply with the technical specifications set out in the implementing acts referred to in paragraph 2 that relate to:
   - (a) systems to replace the driver's control of the vehicle, including signalling, steering, accelerating and braking;
   - (b) ystems to provide the vehicle with real-time information on the state of the vehicle and the surrounding area;
   - (c) driver availability monitoring systems;
   - (d) event data recorders for automated vehicles;
   - (e) harmonised format for the exchange of data for instance for multi-brand vehicle platooning;
   - (f) systems to provide safety information to other road users.

in all these cases there should be additional req. per 2:

However, those technical specifications relating to driver availability monitoring systems, referred to in point (c) of the first subparagraph, shall not apply to fully automated vehicles.

2. The Commission shall by means of implementing acts adopt provisions concerning **uniform procedures and technical specifications for the systems and other items listed in points (a) to (f) of paragraph 1 of this Article, and for the type-approval of automated and fully automated vehicles with regard to those systems and other items in order to ensure the safe operation of automated and fully automated vehicles on public roads.**

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 13(2).

Although NOT speaking of CS in automated vehicles, there's still article 4. In general, we want for any vehicle we do not want unauthorised access to systems. NOT THAT BAD.

"In all these cases (a-f), additional requirements will be defined by the Commission (technical specifications that is gonna be used and adopted by vehicles qualified as automated or fully automated). Regulation has started to introduce notion of CS for connected vehicles.
Would have been better to specify something more for AV, but article 4 is good.