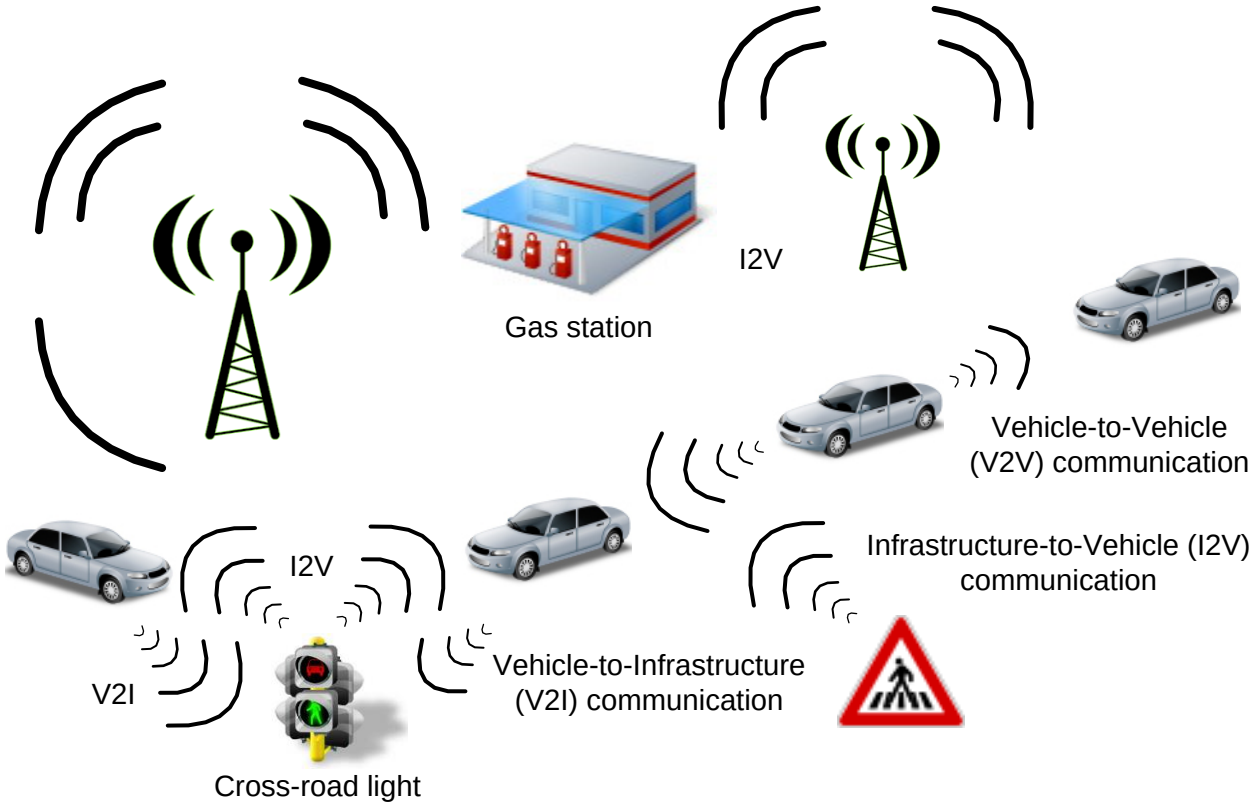
Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach

Mohamad Gharib, Paolo Lollini, Andrea Ceccarelli, and Andrea Bondavalli

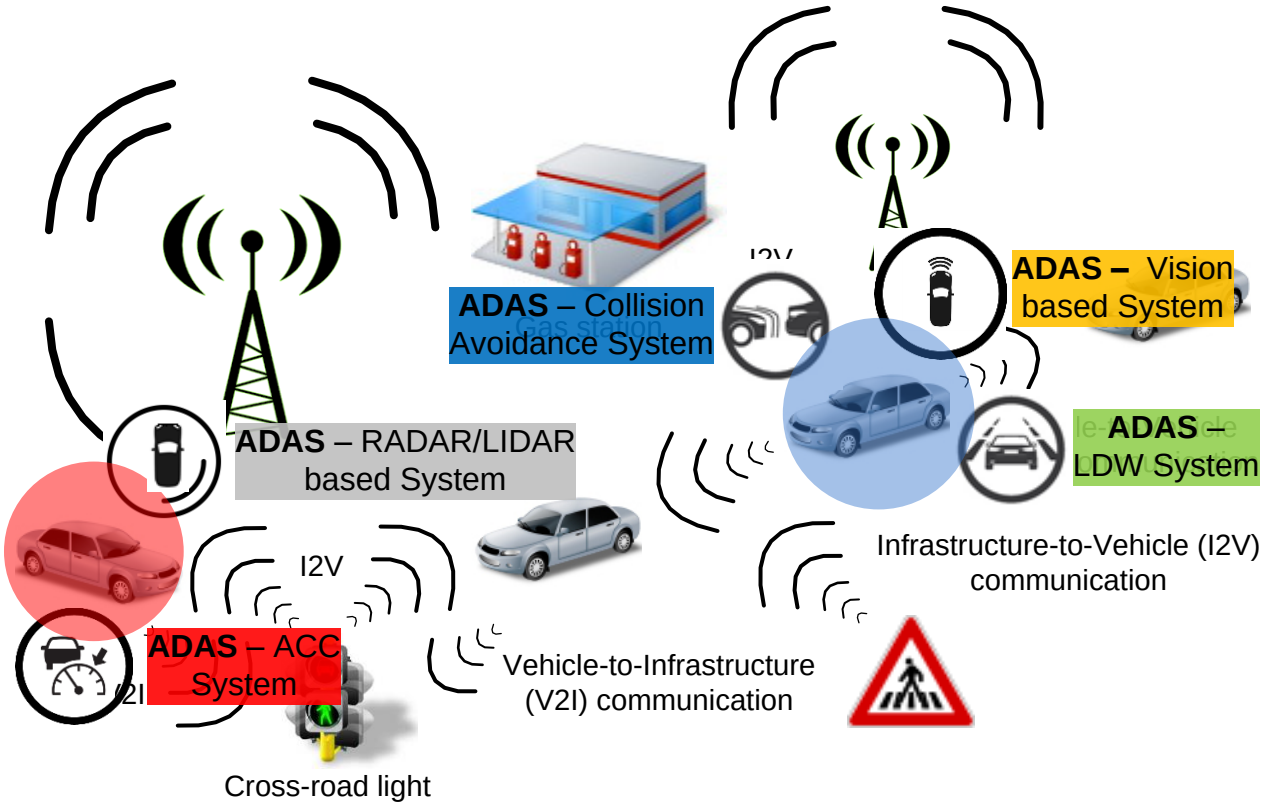
University of Florence
Department of Mathematics and Informatics
Florence, Italy

Problem statement



- Road transport system is an essential infrastructure in the world, where the majority of the population uses its facilities on a daily basis.
- That is why ensuring their safety has been always a growing concern for most authorities.

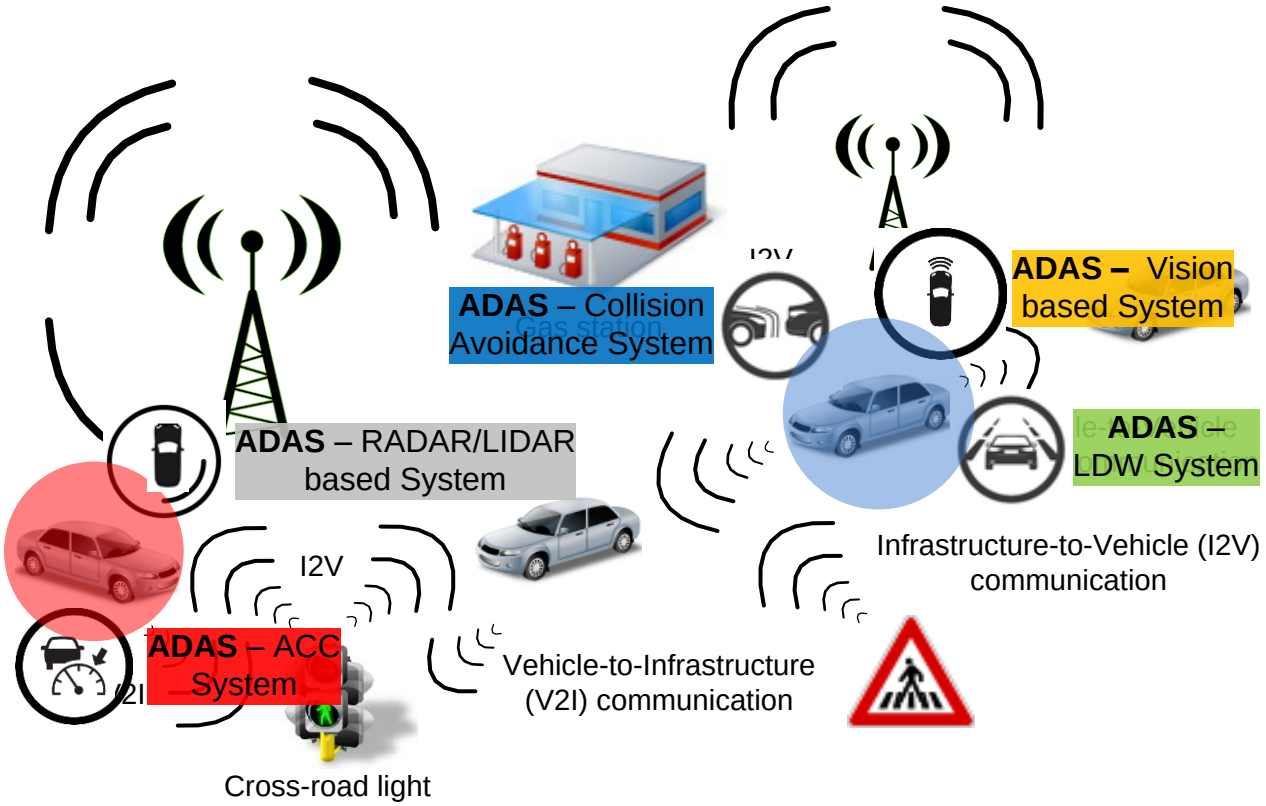
Problem statement



- The complexity of automotive systems have increased significantly in terms of their functionalities.
- The automotive industry is already aware of that, and the **ISO 26262** a standard has been developed.

ISO 26262 covers **E/E systems** of vehicles with almost no emphasis on the **driver** itself

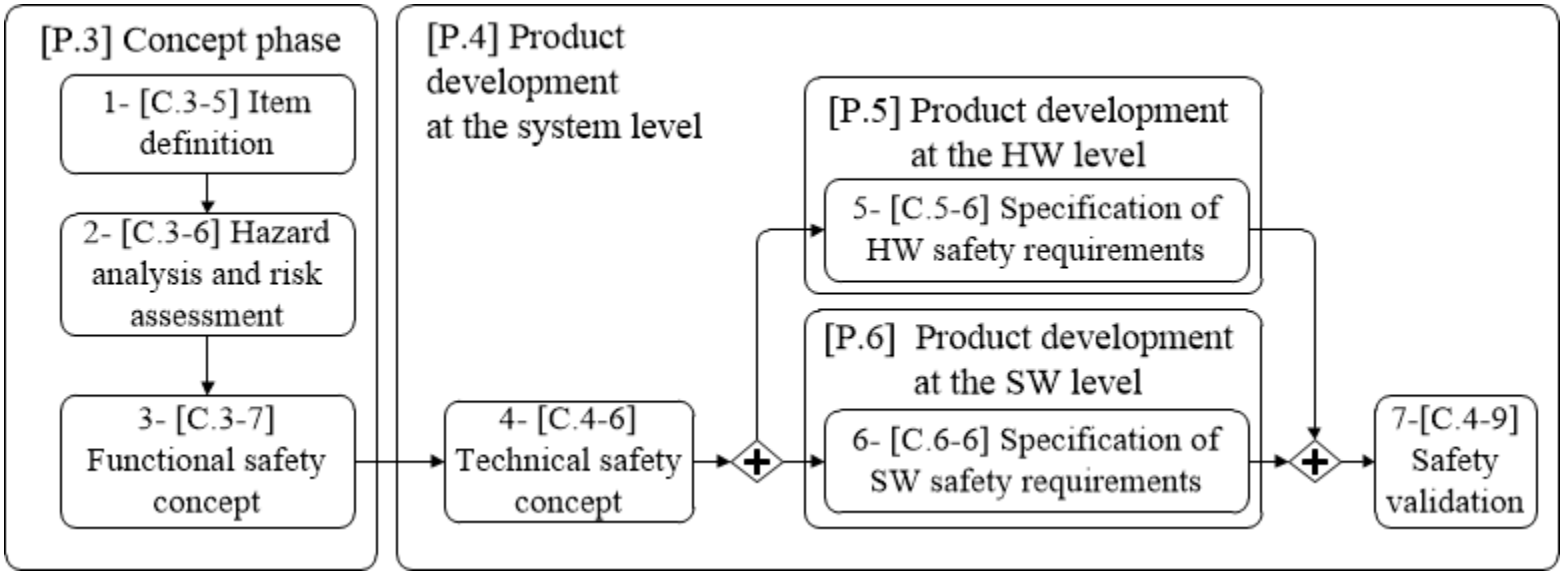
Problem statement



- The complexity of automotive systems have increased significantly in terms of their functionalities.
- The automotive industry is already aware of that, and the **ISO 26262** a standard has been developed.

  ISO 26262 covers **E/E systems** of vehicles with almost no emphasis on the **driver** itself
- Integrating **social** and **technical** components is essential for developing **safer** automotive systems.

ISO 26262



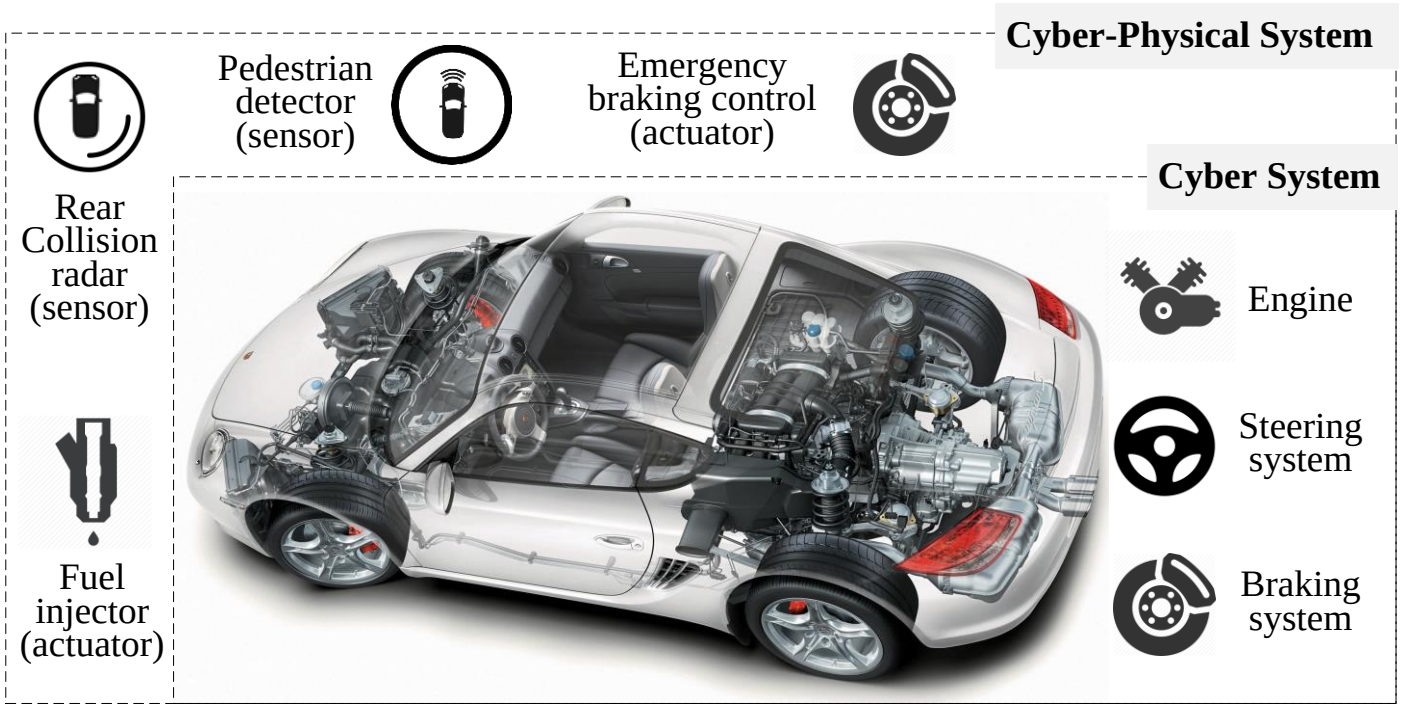
- ISO 26262 [1] is a functional safety standard applicable to all road vehicles with a weight under 3500 kg.
- ISO 26262 has been developed with a main objective to provide guidelines and best practices to increase the safety of E/E systems in vehicles.

[1] ISO: 26262: Road vehicles-Functional safety. IS ISO/FDIS 26262 (2011).

Cyber-Physical-Social Systems (CPSSs)

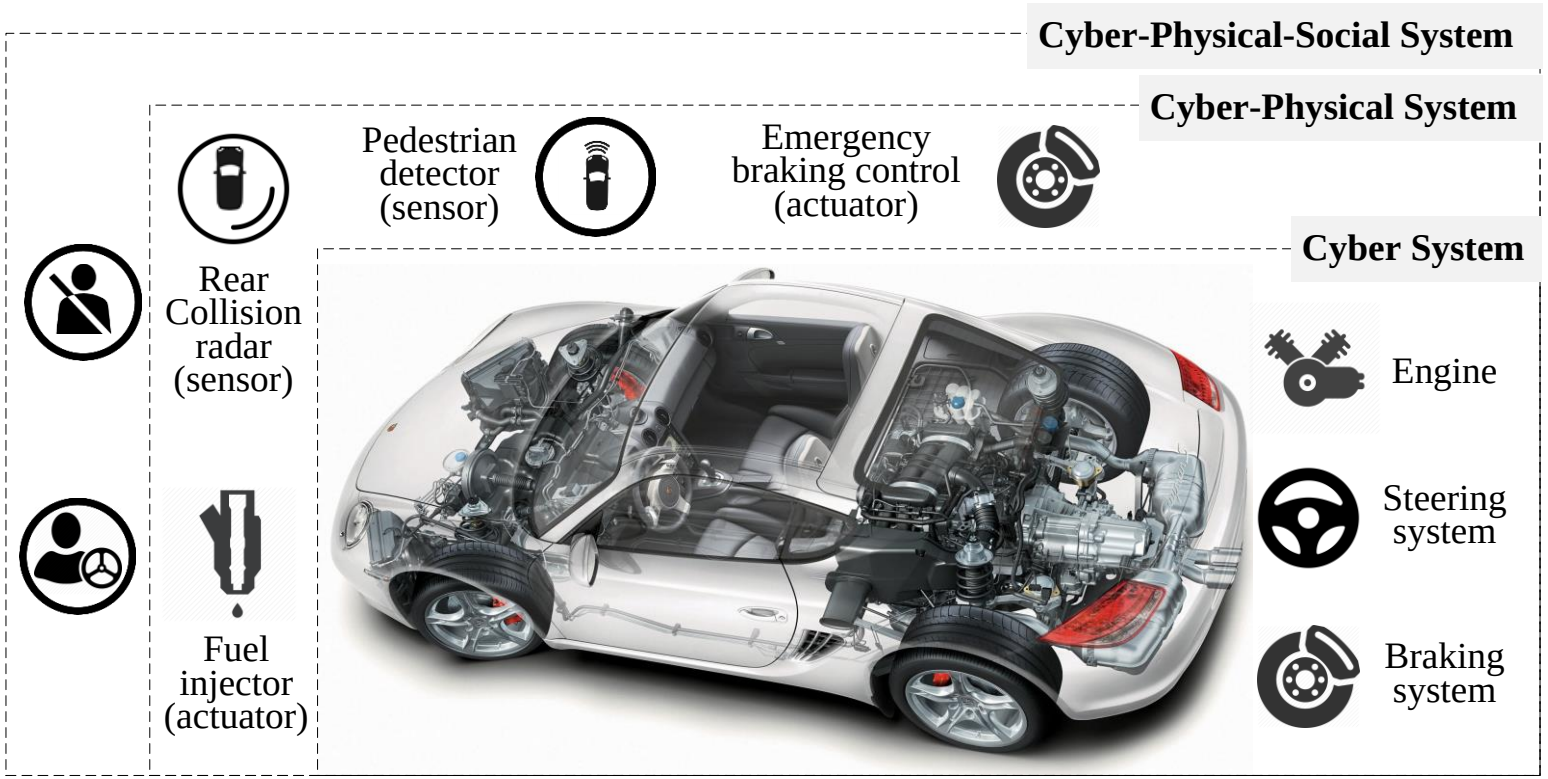
- **A Cyber system** is a system consisting only of technical components.

Cyber-Physical-Social Systems (CPSSs)



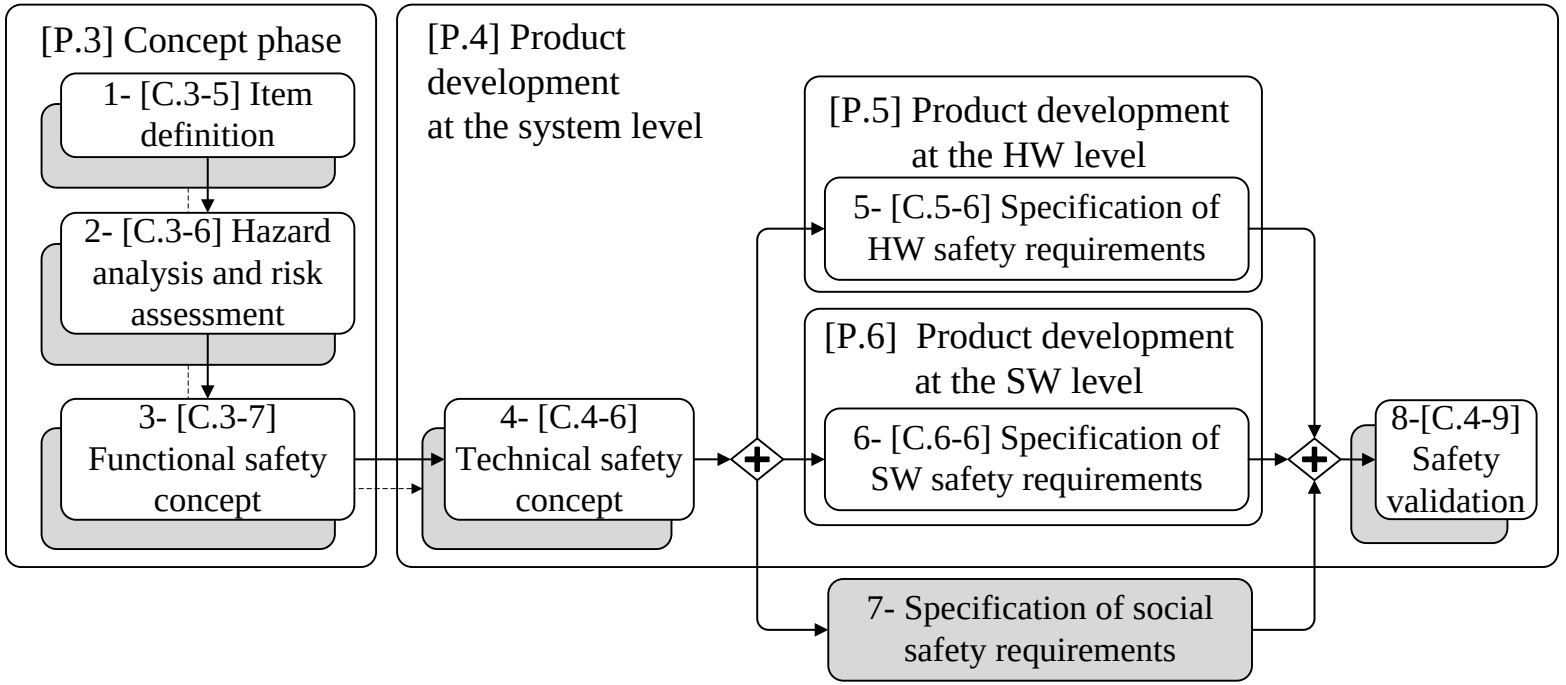
- **A Cyber system** is a system consisting only of technical components.
- **A Cyber-Physical System (CPS)** is a system consisting of cyber systems and controlled objects.

Cyber-Physical-Social Systems (CPSSs)



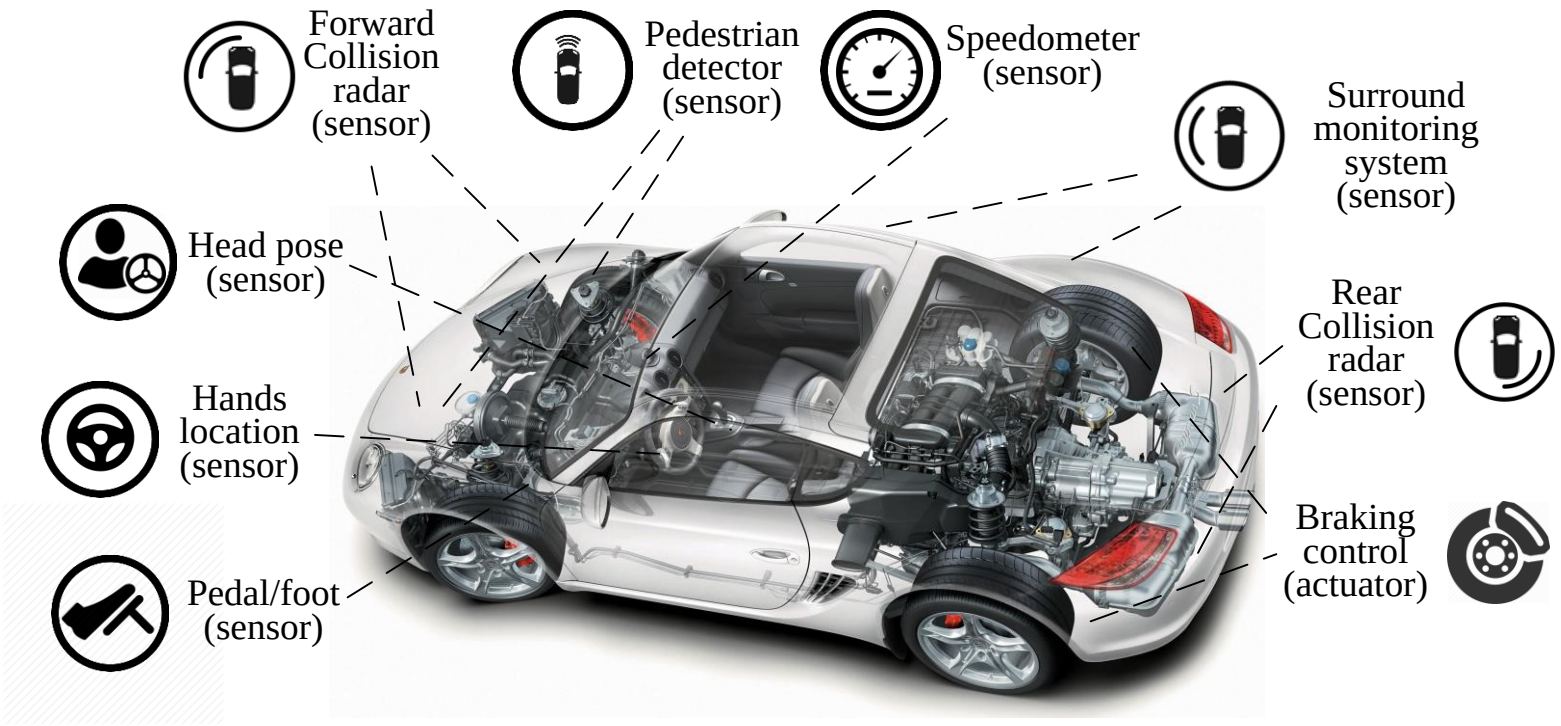
- **A Cyber system** is a system consisting only of technical components.
- **A Cyber-Physical System (CPS)** is a system consisting of cyber systems and controlled objects.
- **A Cyber-Physical-Social System (CPSS)** is a system consisting of cyber systems, controlled objects and interacting humans.

A Holistic Approach to Deal with FSR for Automotive Systems



- The process underlying our approach consists of eight main activities:
  - Activities 1, 2, 3, 4, and 8 are based on ISO 26262 clauses C.3-5, C.3-6, C.3-7, C.4-6, and C.4-9 respectively, and they have been extended to consider the driver behavior.
  - Activities 5 & 6 are based on clauses C.5-6 and C.6-6 respectively.
  - Activity 7 is a new activity that focuses mainly on the specification of social safety requirements.

Example: Maneuver Assistance System

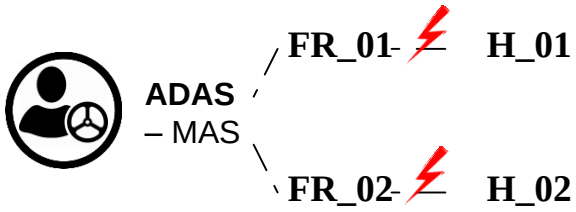


- **Maneuver Assistance System (MAS)** is expected to increase the driver's safety by monitoring its behaviour, detecting unintended maneuvers, and respond in a way that guarantees the highest possible level of driver safety.

Example: Maneuver Assistance System

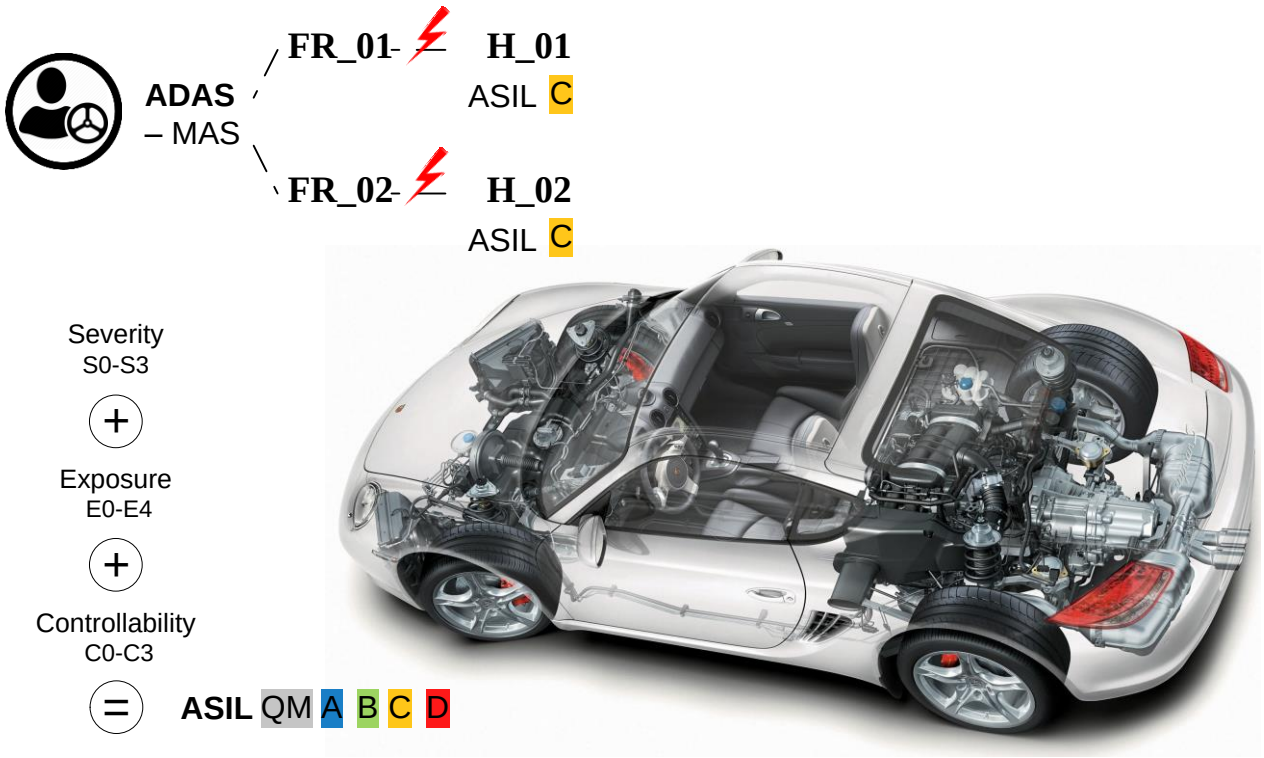
- 1. [C.3-5] **Item definition:** The main function of MAS is to allow/prevent intended/unintended drivers' tactical and operational maneuvers when the vehicle is moving faster than 50 km/h.
  - **FR_01.** Allow intended drivers' tactical/operational maneuvers when the vehicle.
  - **FR_02.** Prevent unintended drivers' tactical/operational maneuvers when the vehicle.

Example: Maneuver Assistance System



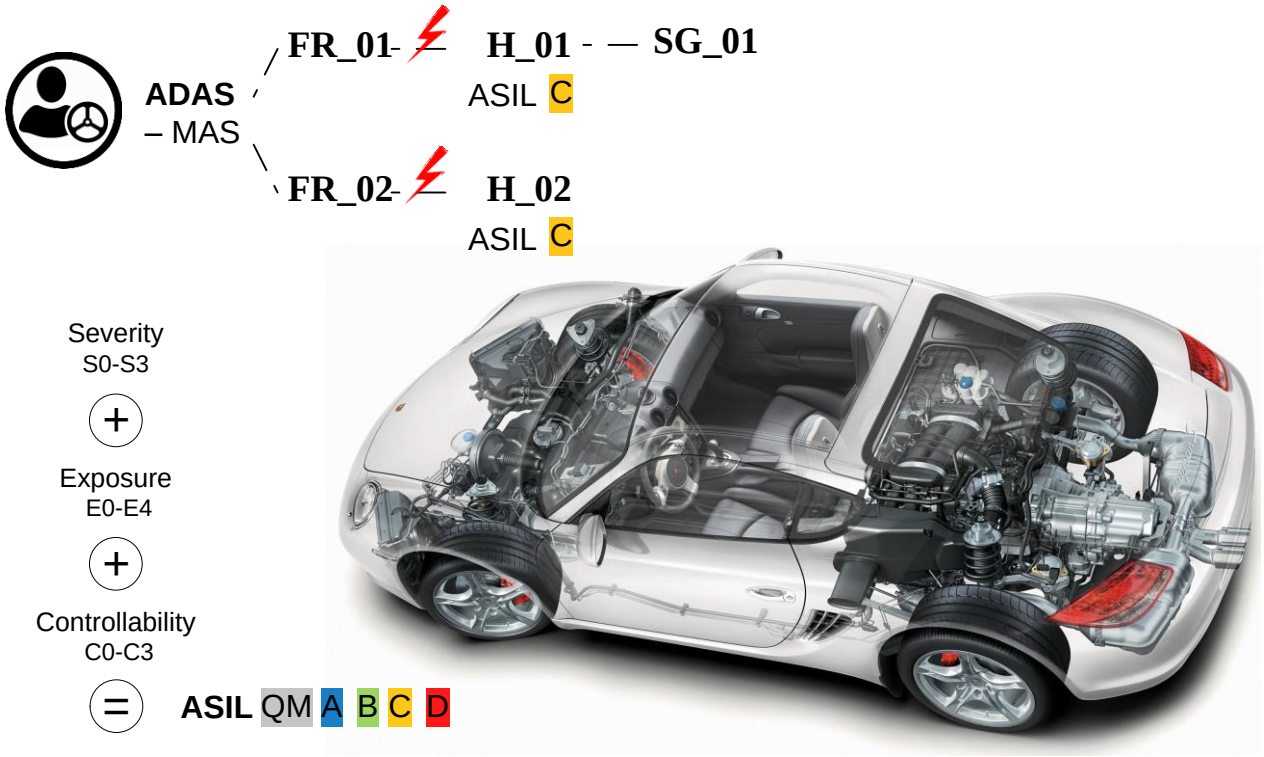
- 2. [C.3-6] **HARA: Hazard analysis and risk assessment.**
  - 2.1. **Hazard identification**
    - **H_01.** Preventing an intended maneuver when the vehicle.
    - **H_02.** Allowing an unintended maneuver to be performed.

Example: Maneuver Assistance System



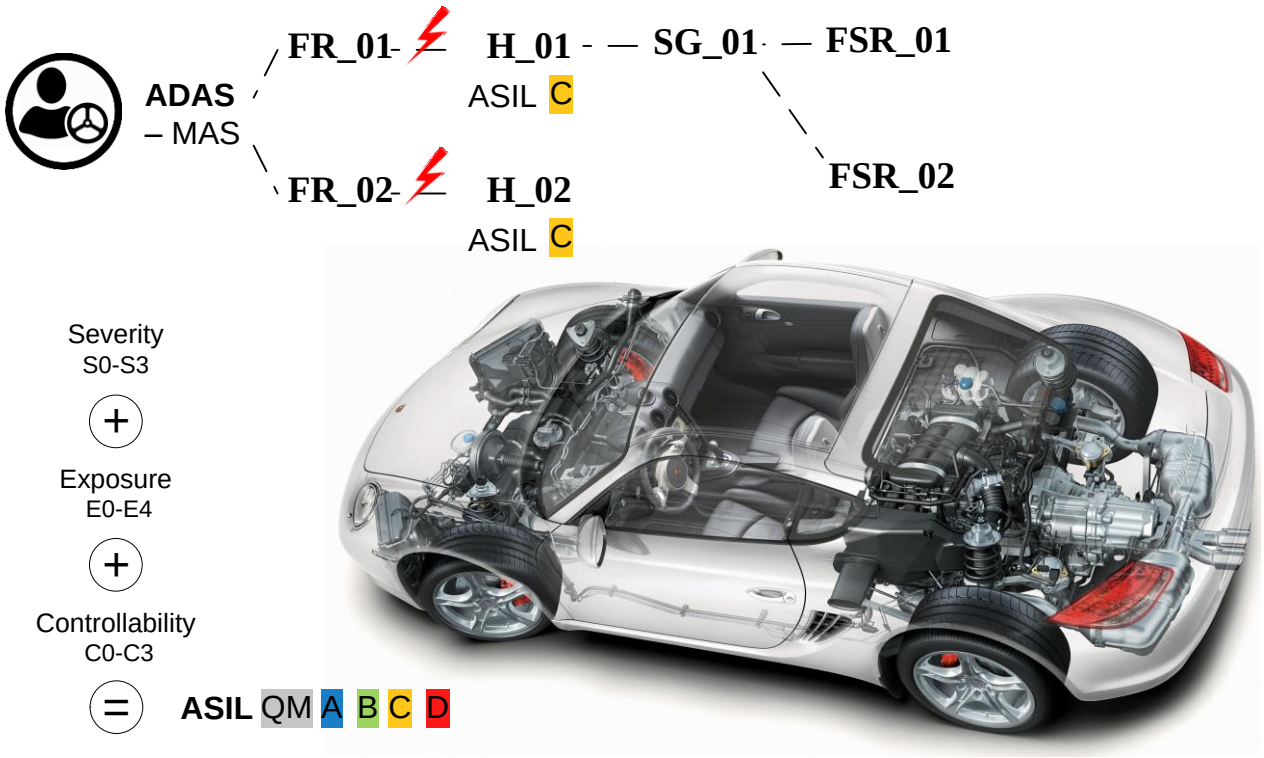
- 2. [C.3-6] **HARA: Hazard analysis and risk assessment.**
  - 2.1. **Hazard identification** & 2.2. **Risk assessment**
    - **H_01.** Preventing an intended maneuver when the vehicle.
    - **H_02.** Allowing an unintended maneuver to be performed.

Example: Maneuver Assistance System



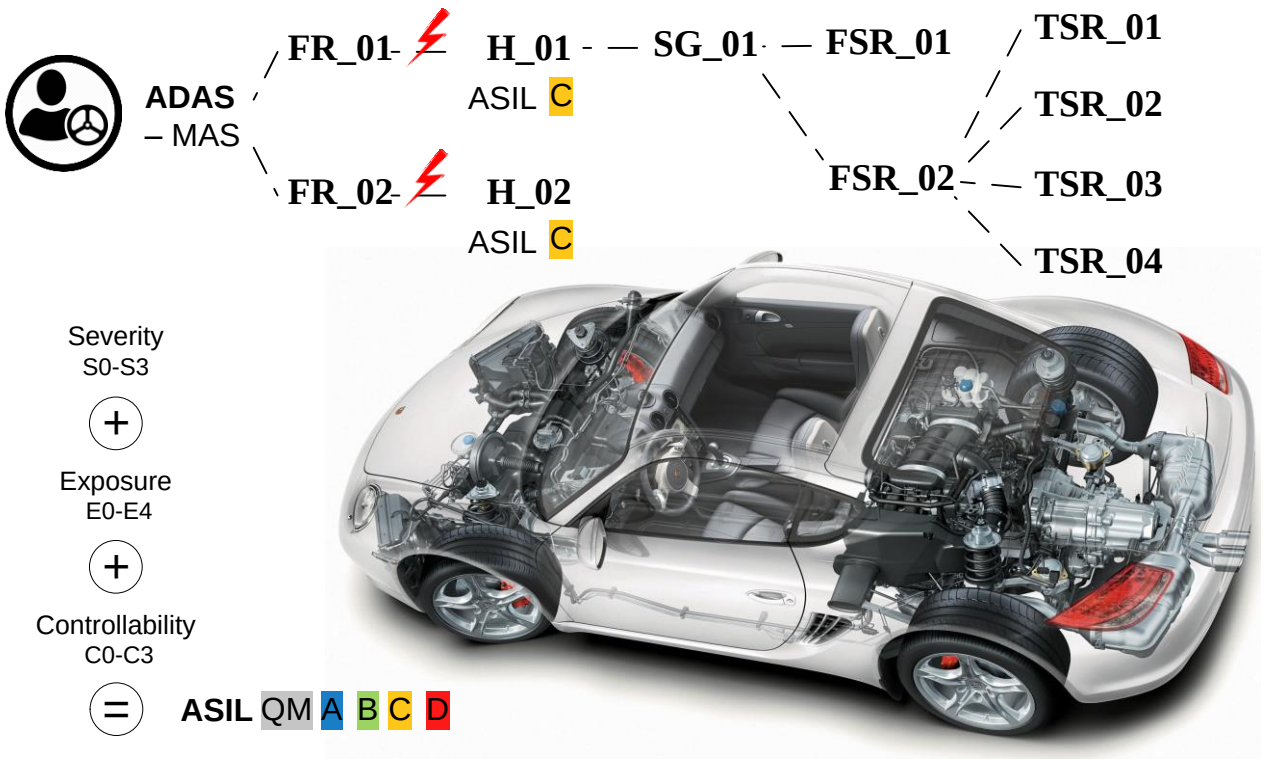
- 2. [C.3-6] **HARA: Hazard analysis and risk assessment.**
  - 2.1. **Hazard identification** & 2.2. **Risk assessment**
    - **H_01.** Preventing an intended maneuver when the vehicle.
      - **SG_01.** A driver unintended maneuver shall be prevented
    - **H_02.** Allowing an unintended maneuver to be performed.

Example: Maneuver Assistance System



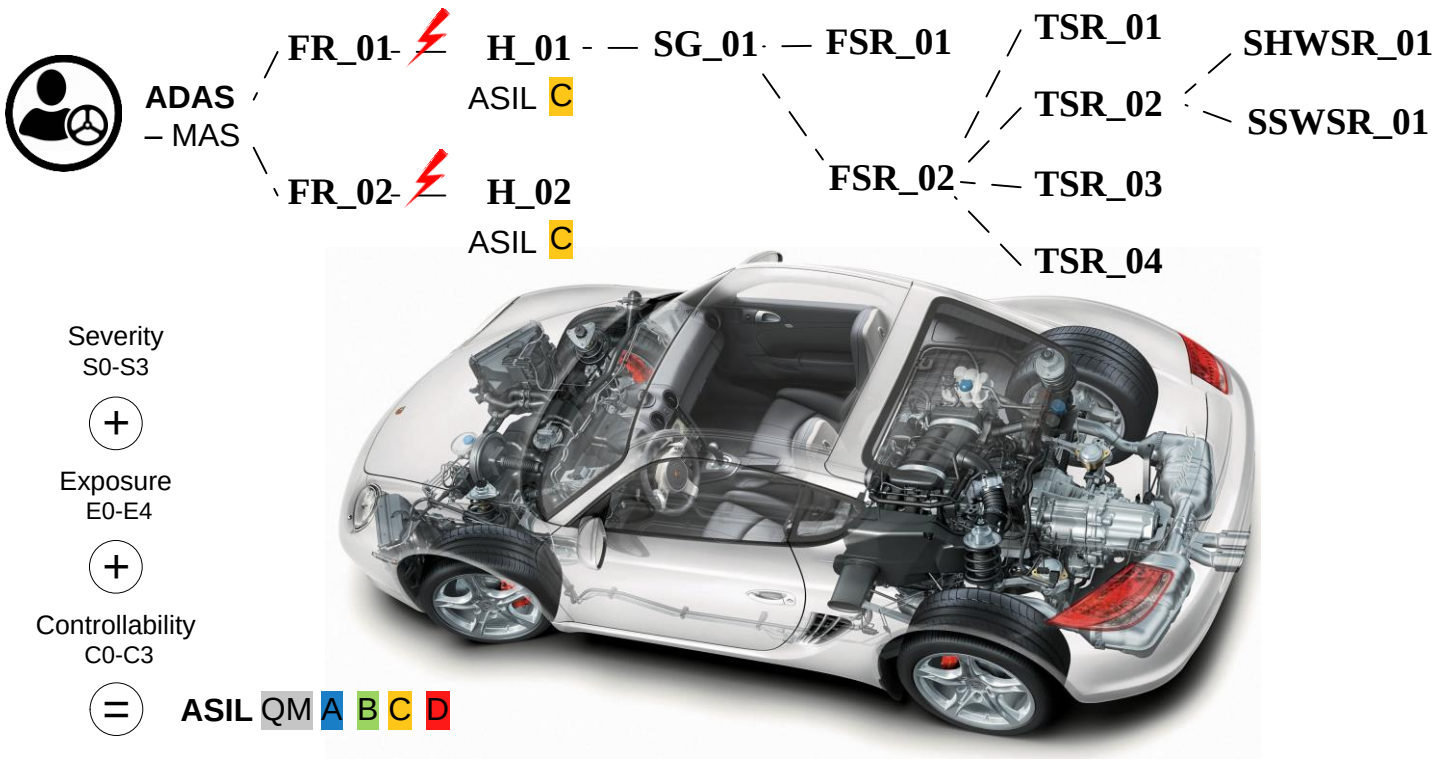
- 3. [C.3-7] **Functional safety concept** is developed by deriving functional safety requirements from safety goals.
  - **FSR_01.** MAS shall be able to verify whether the driver's maneuver is intended within an appropriate time.
  - **FSR_02.** MAS shall prevent unintended maneuvers.

Example: Maneuver Assistance System



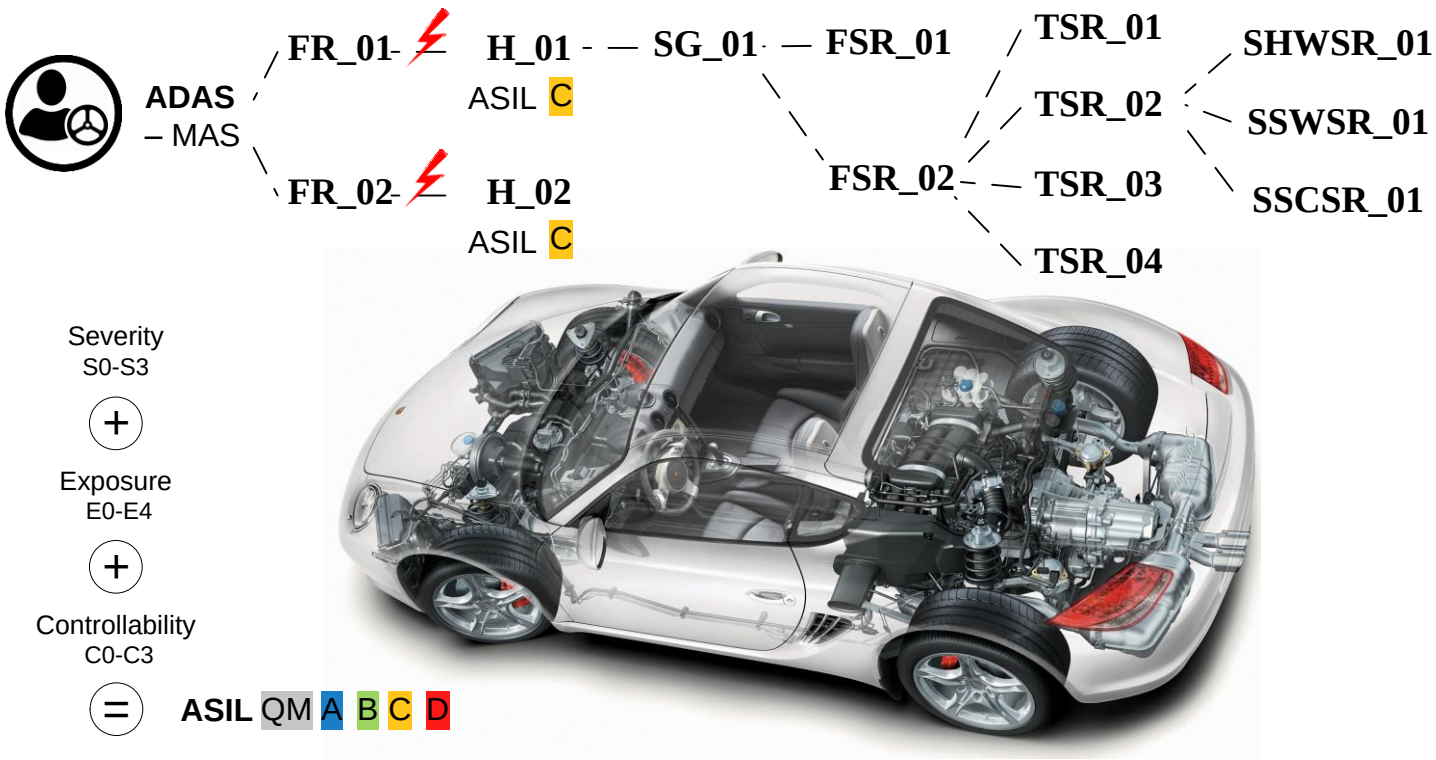
- 4. [C.3-6] **Technical safety concept** aims to specify the technical implementation of the functional safety concept.
  - **TSR_01.** MAS shall be able to verify whether the driver's operation maneuvers are needed within an appropriate time.
  - **TSR_02.** MAS shall prevent unneeded operational maneuvers.

Example: Maneuver Assistance System



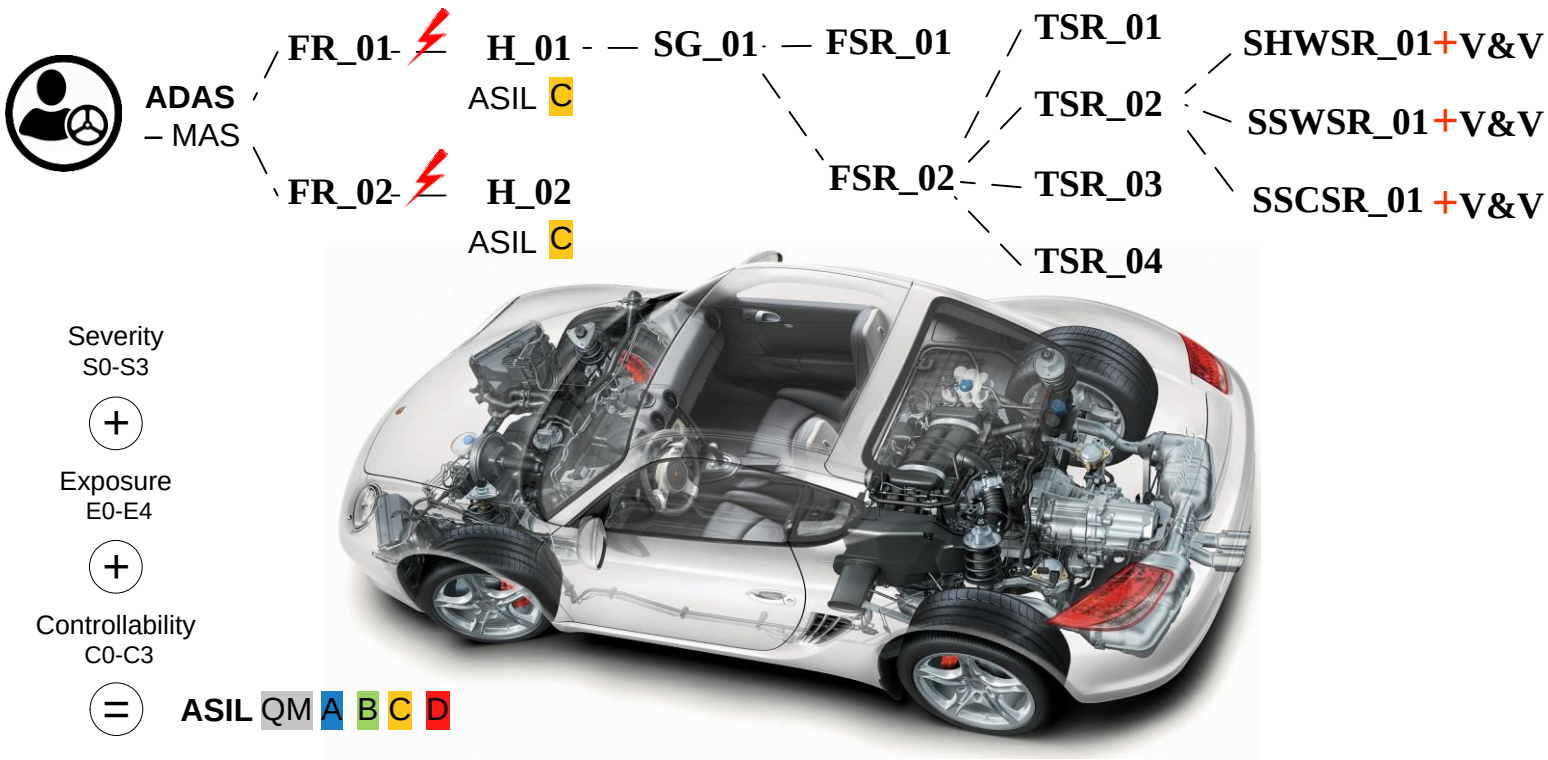
- 5. [C. 5-6]/6.[C. 6-6] **Specification of Hardware/Software/SoCial Safety Requirements (HWSRs)/(SWSRs).**
  - **SHWSR_01.** Lock actuator should be tested and verified efficient in an environment complying with the same real environmental it might function in.
  - **SSWSR_01.** Lock actuator software concerning timely response should be tested and verified efficient in an environment complying with the same real environmental it might function in.

Example: Maneuver Assistance System



- **7. Specification of SoCial Safety Requirements (SCSRs).**
  - **SSCSR_01.** MAS shall be able to fuse all available cues information to determine whether an operational maneuver is needed with respect to the driver state, vehicle and its environment within appropriate time.

Example: Maneuver Assistance System



- 8. **Safety validation.**
  - **V&V for SSCSR_01.** Each mechanism used for acquisition and fusion of cues information to determine the driver awareness, predicting and evaluating whether its operational maneuver is intended should be tested and verified efficient in an environment complying with the same real environmental it might function in.

Conclusions and Future Work

▶ Conclusions

- We discussed the limitation in the current standard (ISO 26262) for developing functional safety systems for vehicles, which mainly cover E/E systems of vehicles.
- We proposed a holistic approach built based on the ISO 26262 standard and considers both the E/E systems and the driver's behaviour.

▶ Future Work

- We intend to formalize all the previously introduced concepts and develop SysML profiles based on them, which allows for modeling FSRs, derive the TSRs, and then derive the HWSRs, SWSRs, and SCSRs from TSRs.
- We are planning to propose a set of Object Constraint Language (OCL) constraints for specifying rigorous rules for the derivation of HWSRs, SWSRs, and SCSRs from TSRs, and the derivation of TSRs from FSRs.

THANK YOU for your attention