Standards & Regulations Presentation

Team E: OuterSense

#1. ISO 26262
Road Vehicles – Functional Safety

Why we need this?

One century ago, **the Ford Model T**, which is considered the first mass-produced automobile, was powered **by an electrical system**

Today, the electrical and/or electronic (E/E) systems within automobiles are far more complex.

The **IEC 61508** series of standards specifies any electronic safety-related system

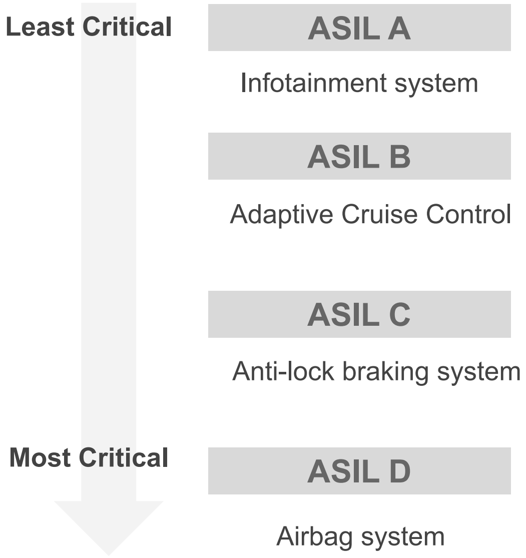
To meet the specific needs of electrical and/or electronic systems within road vehicles, ISO 26262 was adapted from the IEC 61508 series.

About

ISO 26262 is an **automotive functional safety standard for *E/E* systems** defined by the International Organization for Standardization (ISO)

- Primary objective is to prevent accidents caused by system failures in vehicles
- Provides a structured approach to managing the safety of electrical and electronic systems within automobiles for entire lifecycle
- To classify components into ASILs, one must do the Hazard Analysis and Risk Assessment (HARA).

Automotive Safety and Integrity Levels (ASIL)



Least Critical

ASIL A

Infotainment system

ASIL B

Adaptive Cruise Control

ASIL C

Anti-lock braking system

Most Critical

ASIL D

Airbag system

Application

ISO 26262 is applicable to a wide range of products and markets in the automotive industry.

- It covers road vehicles, including passenger cars, commercial vehicles, and more.
- It is relevant to various stakeholders in the automotive supply chain, including vehicle manufacturers, suppliers, and service providers.

Commercial Vehicle

Electric vehicles

Automotive supplier

Automotive software

Passenger Vehicle

ADAS

Advanced driver assistance

Automotive products and repairs

Emerging technology

Main prescriptions

The parts or sections of ISO 26262 contribute to the prescriptions

Functional Safety management

It requires the establishment of safety plans and the monitoring of safety goals throughout the development lifecycle. Project independent and project specific management activities in safety lifecycle

Concept Phase

This is the concept phase, and it features item definition, hazard analysis and risk assessment, and the functional safety concept. Leads to determination of ASIL, safety goals and requirements for each safety-critical component.

Product development

Product development at system, software and hardware level. Includes safety specification, architectural design, verification, integration and testing

Production and operations

Safety considerations extend to the production and operational phases. Processes to maintain safety during these phases are defined.

Main prescriptions

Functional Safety assessment

Supporting processes for the functional safety such as verification, validation, and functional safety assessment to confirm that safety goals are achieved and that processes are followed correctly.

Safety analysis and ASIL

Safety-oriented analyses, such as Hazard Analysis and Risk Assessment (HARA), to determine the ASIL for each component.

Documentation and traceability

Comprehensive documentation is required to demonstrate compliance with the standard. This documentation must show traceability between safety goals, requirements, and verification activities.

Guidelines

The standard provides additional guidance on implementing ISO 26262 in the form of guidelines and recommendations.

Application to OuterSense

Automotive software

Emerging technology

Safety analysis and risk assessment

- **Perception** : Ensuring robust external perception to have safe planning for vehicles. Latent perception can increase planning and control latency causing delayed response. Asses risk related to hardware and unit performance
- **Trajectory planning**: Ensure correct plans are generated and wrong decisions are not made. Planner to handle latent sensor information and dynamic environments, generate plans feasible for follower to follow.
- **Control** : Conduct sanity checks on planner and estimation output. Ensure vehicle follows plan accurately, stop the vehicle during emergencies.

System development and testing

- Develop subsystem and conduct unit testing, ensure all safety goals and requirements are met
- Conduct system level integrated testing for robustness and safety checks

#2. National Highway Traffic Safety Administration: Federal Automated Vehicles Policy

About

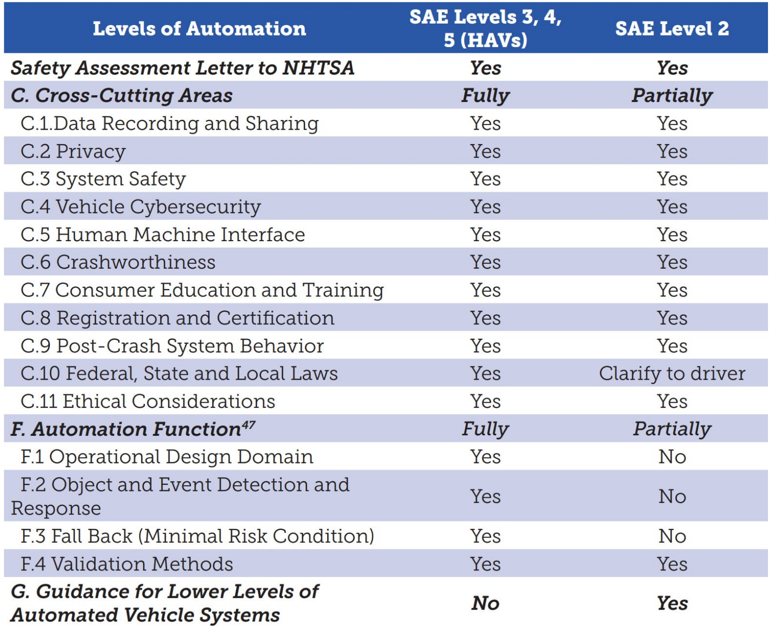
- Shapes the regulatory landscape for automated vehicles in the United States

- Policy focused on Highly Automated Vehicles (SAE L3, L4, L5)

- Four sections
  - Vehicle Performance Guidance for Automated Vehicles
  - Model State Policy
  - NHTSA’s Current Regulatory Tools
  - New Tools and Authorities

NHTSA Federal Automated Vehicles Policy

Application



Levels of Automation	SAE Levels 3, 4, 5 (HAVs)	SAE Level 2
Safety Assessment Letter to NHTSA	***Yes***	***Yes***
C. Cross-Cutting Areas	***Fully***	***Partially***
C.1.Data Recording and Sharing	Yes	Yes
C.2 Privacy	Yes	Yes
C.3 System Safety	Yes	Yes
C.4 Vehicle Cybersecurity	Yes	Yes
C.5 Human Machine Interface	Yes	Yes
C.6 Crashworthiness	Yes	Yes
C.7 Consumer Education and Training	Yes	Yes
C.8 Registration and Certification	Yes	Yes
C.9 Post-Crash System Behavior	Yes	Yes
C.10 Federal, State and Local Laws	Yes	Clarify to driver
C.11 Ethical Considerations	Yes	Yes
F. Automation Function[47]	***Fully***	***Partially***
F.1 Operational Design Domain	Yes	No
F.2 Object and Event Detection and Response	Yes	No
F.3 Fall Back (Minimal Risk Condition)	Yes	No
F.4 Validation Methods	Yes	Yes
G. Guidance for Lower Levels of Automated Vehicle Systems	***No***	***Yes***

Embark

Einride

PLusAI

Locomotion

Kodiak

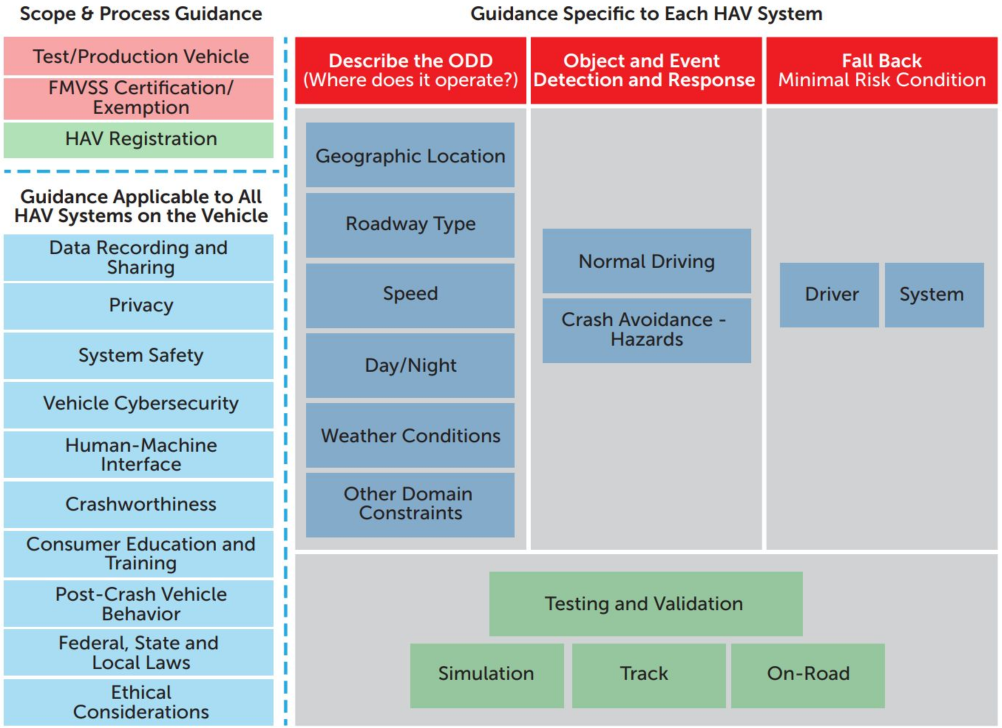
Aurora

Nuro

NHTSA Federal Automated Vehicles Policy

Main prescriptions

Vehicle Performance Guidance for Automated Vehicles



Scope & Process Guidance

- Test/Production Vehicle
- FMVSS Certification/ Exemption
- HAV Registration

Guidance Applicable to All HAV Systems on the Vehicle

- Data Recording and Sharing
- Privacy
- System Safety
- Vehicle Cybersecurity
- Human-Machine Interface
- Crashworthiness
- Consumer Education and Training
- Post-Crash Vehicle Behavior
- Federal, State and Local Laws
- Ethical Considerations

Guidance Specific to Each HAV System

Describe the ODD (Where does it operate?)

- Geographic Location
- Roadway Type
- Speed
- Day/Night
- Weather Conditions
- Other Domain Constraints

Object and Event Detection and Response

- Normal Driving
- Crash Avoidance - Hazards

Fall Back Minimal Risk Condition

- Driver
- System

Testing and Validation

- Simulation
- Track
- On-Road

NHTSA Federal Automated Vehicles Policy

Main prescriptions

Vehicle Performance Guidance for Automated Vehicles

Section F: Specifics for Automation Functions

1. Operational Design Domain	2. Object and Event Detection and Response
• Roadway types	• Other vehicles (in and out of its travel path)
• Geographic area	• Pedestrians,cyclists, animals, other objects
• Speed range	• Emergency vehicles
• Environmental conditions	• Temporary work zones
• Other domain constraints	• Other unusual conditions

Main prescriptions

Vehicle Performance Guidance for Automated Vehicles

Section F: Specifics for Automation Functions

3. Fall Back (Minimal Risk Condition)	4. Validation Methods
• Capability to detect malfunctions, degraded state, or operation outside of ODD • Fall back actions should facilitate safe operations of the vehicle and minimize erratic driving behavior	• Tests to demonstrate the performance during normal operation, crash avoidance situations, and fall back strategies. • Combination of simulation, test track, and on-road testing

Application to OuterSense

Operational Design Domain for OuterSense

- Environment spanned by overhead cameras with overlapping FOVs
- Pre-defined map with known road dimensions and traffic signs
- Well illuminated environment
- Driving speed - up to 15 miles per hour (PR4, DPR2)
- Access to a reliable wireless communication network in the environment
- A human operator monitoring simultaneously monitoring automated operations

Application to OuterSense

Object and Event Detection

- The OuterSense perception system can detect obstacles/other vehicles/actors tagged by OuterSense or Aruco markers with 95% success rate

Response

- No collisions with other controlled vehicles (PR1)
- No collisions with static and dynamic obstacles (DPR3)

Application to OuterSense

Fall Back (Minimal Risk Condition)

Identification	Action
1. Operation outside ODD	
1.1. Detect if a vehicle is outside the FOV of the infrastructure sensor	1.1 Follow the safety profile to a smooth stop if no detection in found on 0.5s
1.2. Commanded speeds higher than 15 mph	1.2 Clip to 15mph at all levels
2. Degraded performance	
2.1. Detect latency in receiving new control actions from the cloud	2.1 Follow the time-synchronized motion cues - follow the safety profile to come to a smooth stop if no new motion cues are received.

Application to OuterSense

Validation

Simulation

Use recorded data from manual drives to validate autonomy functions (perception, state estimation, planning)

Test-track

Integrated system can safely control vehicles in the ODD adhering to the requirements (Tests 1-12 outlined in the Fall Test Plan)

Thank You