KENNESAW STATE UNIVERSITY

Module 13:

Autonomous Vehicles Safety Guidelines

Dr. Maria Valero

Agenda

- Background
- Safety Elements: System Safety
- Safety Elements: Operational Design
- Object Detection
- Minimal Risk
- Human Machine Interface (HMI)
- Avoiding Crash

Background (1)

Since the Department of Transportation was established in 1966, there have been more than 2.2 million motor-vehicle-related fatalities in the United States.

After decades of decline, motor vehicle fatalities spiked by more than 7.2 percent in 2015, the largest single-year increase since 1966.

The major factor in 94 percent of all fatal crashes is human error.

Automated Driving Systems (ADSs) have the potential to significantly reduce highway fatalities by addressing the root cause of these tragic crashes.

Background (2)

In the transportation sector, where 9 out of 10 serious roadway crashes occur due to human behavior, automated vehicle technologies possess the potential to save thousands of lives, as well as reduce congestion, enhance mobility, and improve productivity.

The Federal Government wants to ensure it does not impede progress with unnecessary or unintended barriers to innovation. Safety remains the number one priority for the U.S. Department of Transportation (DOT) and is the specific focus of the National Highway Traffic Safety Administration (NHTSA).

Background (3)

Vehicles operating on public roads are subject to both Federal and State jurisdiction, and States are beginning to draft legislation to safely deploy emerging ADSs.

National Highway Traffic Safety Administration (NHTSA) offers *Section 2: Technical Assistance to States, Best Practices for Legislatures Regarding Automated Driving Systems (Best Practices)*.

The section clarifies and delineates Federal and State roles in the regulation of ADSs.

NHTSA remains responsible for regulating the safety design and performance aspects of motor vehicles and motor vehicle equipment;

States continue to be responsible for regulating the human driver and vehicle operations.

Safety Elements: System Safety

- The overall process should adopt and follow industry standards, such as the functional safety process standard for road vehicles, and collectively cover the entire operational design domain (i.e., operating parameters and limitations) of the system.
- The design and validation process should also consider including a hazard analysis and safety risk assessment for ADSs, for the overall vehicle design into which it is being integrated, and when applicable, for the broader transportation ecosystem.
- The software development process is one that should be well-planned, well-controlled, and well-documented to detect and correct unexpected results from software updates.
- Thorough and measurable software testing should complement a structured and documented software development and change management process and should be part of each software version release.

Safety Elements: Operational Design

- Entities are encouraged to define and document the Operational Design Domain (ODD) for each ADS available on their vehicle(s) as tested or deployed for use on public roadways

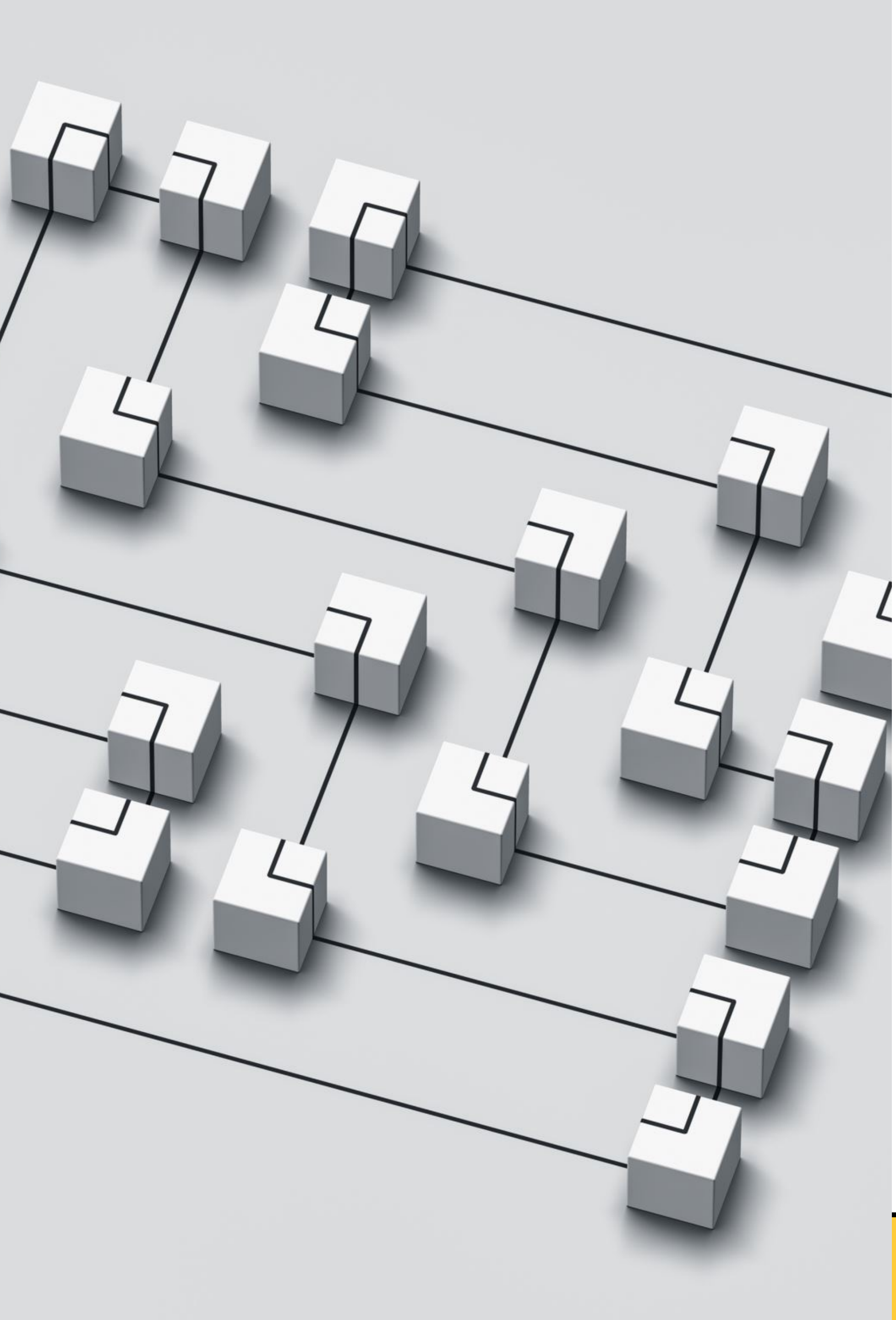
- The ODD would include the following information at a minimum to define each ADS's capability limits/boundaries:
  - Roadway types (interstate, local, etc.) on which the ADS is intended to operate safely;
  - Geographic area (city, mountain, desert, etc.);
  - Speed range;
  - Environmental conditions in which the ADS will operate (weather, daytime/nighttime, etc.); and
  - Other domain constraints.

Safety Elements: Object and Event Detection and Response (1)

Entities are encouraged to have a documented process for assessment, testing, and validation of their ADS's OEDR capabilities.

ADS's OEDR functions are expected to be able to detect and respond to other vehicles (in and out of its travel path), pedestrians, bicyclists, animals, and objects that could affect safe operation of the vehicle.

An ADS's OEDR should also include the ability to address a wide variety of foreseeable encounters, including emergency vehicles, temporary work zones, and other unusual conditions (e.g., police manually directing traffic or other first responders or construction workers controlling traffic) that may impact the safe operation of an ADS.



Safety Elements: Object and Event Detection and Response (2)

- Crash Avoidance Capabilities
  - Entities are encouraged to have a documented process for assessment, testing, and validation of their crash avoidance capabilities and design choices.
  - Based on the ODD, an ADS should be able to address applicable pre-crash scenarios16 that relate to control loss; crossing-path crashes; lane change/merge; head-on and opposite-direction travel; and rear-end, road departure, and low-speed situations such as backing and parking man

Safety Elements: Fallback (Minimal Risk Condition)

- Entities are encouraged to have a documented process for transitioning to a minimal risk condition when a problem is encountered, or the ADS cannot operate safely.
- ADSs operating on the road should be capable of detecting that the ADS has malfunctioned, is operating in a degraded state, or is operating outside of the ODD.
- ADSs should be able to notify the human driver of such events in a way that enables the driver to regain proper control of the vehicle or allows the ADS to return to a minimal risk condition independently
- Fallback actions are encouraged to be administered in a manner that will facilitate safe operation of the vehicle and minimize erratic driving behavior
- A minimal risk condition will vary according to the type and extent of a given failure, but may include automatically bringing the vehicle to a safe stop, preferably outside of an active lane of traffic

Safety Elements: Validation Method

- Tests should demonstrate the behavioral competencies an ADS would be expected to perform during normal operation, the ADS's performance during crash avoidance situations, and the performance of fallback strategies relevant to the ADS's ODD.
- To demonstrate the expected performance of an ADS for deployment on public roads, test approaches may include a combination of simulation, test track, and on-road testing

Safety Elements: Human Machine Interface (HMI)

- (HMI), has always played an important role in the automotive design process.
- The vehicle must be capable of accurately conveying information to the human driver regarding intentions and vehicle performance.
- Human drivers may be requested to perform any part of the driving task, e.g.,, in a Level 3 vehicle, the driver always must be receptive to a request by the system to take back driving responsibilities.
- However, a driver’s ability to do so is limited by their capacity to stay alert to the driving task and thus capable of quickly taking over control, while at the same time not performing the actual driving task until prompted by the vehicle.
- Entities are encouraged to consider whether it is reasonable and appropriate to incorporate driver engagement monitoring in cases where drivers could be involved in the driving task so as to assess driver awareness and readiness to perform the full driving task.

Safety Elements: Human Machine Interface (HMI)

- At a minimum
  - Functioning properly;
  - Currently engaged in ADS mode;
  - Currently “unavailable” for use;
  - Experiencing a malfunction; and/or
  - Requesting control transition from the ADS to the operator

Safety Elements: Vehicle Cybersecurity (1)

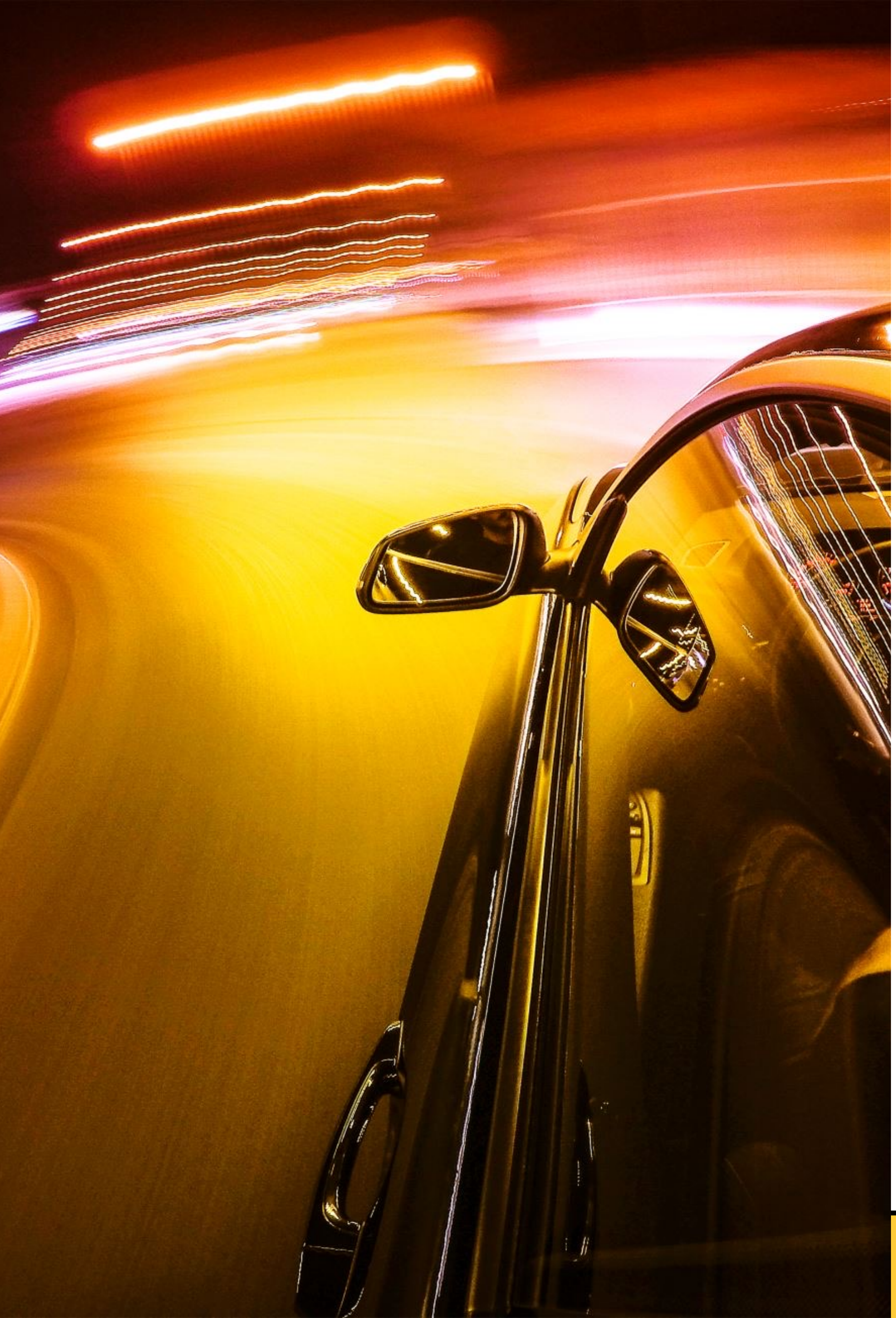
- Entities are encouraged to follow a robust product development process based on a systems engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities.
- This process should include a systematic and ongoing safety risk assessment for each ADS
- Industry sharing of information on vehicle cybersecurity facilitates collaborative learning and helps prevent industry members from experiencing the same cyber vulnerabilities

Safety Elements: Vehicle Cybersecurity (2)

NHTSA encourages entities to document how they incorporated vehicle cybersecurity considerations into ADSs, including all actions, changes, design choices, analyses, and associated testing, and ensure that data is traceable within a robust document version control environment.

Entities are encouraged to report to the Auto-ISAC all discovered incidents, exploits, threats and vulnerabilities from internal testing, consumer reporting, or external security research as soon as possible, regardless of membership.

Entities are further encouraged to establish robust cyber incident response plans and employ a systems engineering approach that considers vehicle cybersecurity in the design process



Safety Elements: Crashworthiness

- Regardless of whether the ADS is operating the vehicle or the vehicle is being driven by a human driver, the occupant protection system should maintain its intended performance level in the event of a crash.
- Entities should consider incorporating information from the advanced sensing technologies needed for ADS operation into new occupant protection systems that provide enhanced protection to occupants of all ages and sizes.
- In addition to the seating configurations evaluated in current standards, entities are encouraged to evaluate and consider additional countermeasures that will protect all occupants in any alternative planned seating or interior configurations during use

Safety Elements: Post Crash ADS Behavior

- Entities engaging in testing or deployment should consider methods of returning ADSs to a safe state immediately after being involved in a crash.
- Depending upon the severity of the crash, actions such as shutting off the fuel pump, removing motive power, moving the vehicle to a safe position off the roadway (or safest place available), disengaging electrical power, and other actions that would assist the ADSs should be considered.
- If communications with an operations center, collision notification center, or vehicle communications technology exist, relevant data is encouraged to be communicated and shared to help reduce the harm resulting from the crash
- Entities are encouraged to have documentation available that facilitates the maintenance and repair of ADSs before they can be put back in service.

Safety Elements: Data Recording

- Learning from crash data is a central component to the safety potential of ADSs.
- For example, the analysis of a crash involving a single ADS could lead to safety developments and subsequent prevention of that crash scenario in other ADSs.
- Paramount to this type of learning is proper crash reconstruction.
- Currently, no standard data elements exist for law enforcement, researchers, and others to use in determining why an ADS-enabled vehicle crashed.
- Entities engaging in testing or deployment are encouraged to establish a documented process for testing, validating, and collecting necessary data related to the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any crash.
- Data should be collected for on-road testing and use, and entities are encouraged to adopt voluntary guidance, best practices, design principles, and standards