NIST Special Publication 1900-301

Automated Driving System Safety Measurement Part I: Operating Envelope Specification

Edward Griffor
David Wollman
Christopher Greer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-301

CYBER-PHYSICAL SYSTEMS

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1900-301

Automated Driving System Safety Measurement Part 1: Operating Envelope Specification

Edward Griffor
David Wollman
Christopher Greer
Smart Connected Systems
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-301

December 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1900-301
Natl. Inst. Stand. Technol. Spec. Publ. 1900-301, 24 pages (December 2021)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-301

Abstract

The safety of Automated Driving System (ADS) equipped vehicles and reliable methods for assessing that safety are critical for public acceptance of these engineered systems. This document presents a novel approach for developing an ADS safety measurement methodology, which came from the NIST Automated Driving System Safety Measurement (ADSSM) Technical Working Group.

This document presents the concept of an Operating Envelope Specification (OES), a structured description of environmental factors or aspects that an ADS may encounter during operation and relates it to the Operational Design Domain (ODD) of ADS-equipped vehicles.

Reasoning about the operating conditions of an ADS-equipped vehicle, using OES and during relevant scenarios or other modalities of test, can be classified as relating to specific engineering concerns such as functional, communications, or trustworthiness concerns and for purposes of providing an assurance case for each concern. One such classification is provided by the NIST Framework for Cyber-Physical Systems (CPS Framework) [1]. The CPS Framework provides a set of engineering concerns that can be used to sort or classify constraints on system behaviors, such as those provided by regulation or roadway design or those determined during system development. This methodology will be presented in future work.

Key words

Automated Driving System (ADS); Automated Driving System safety measurement; cyber-physical systems; Operational Design Domain (ODD); Operating Envelope Specification (OES); vehicle safety measurement.

Table of Contents

1. Introduction ... 1
2. Background ... 1
3. ADS Safety Abstractions ... 4
3.1. ADS Logic and OES ... 7
3.2. Notional ADS (Testbed) Architecture ... 9
3.3. Relationship between ODD and OES ... 10
4. OES Case Study ... 12
4.1. Example OES Information ... 14
5. Conclusions and Summary ... 15

List of Figures

Fig. 1. SAE automation levels. ... 5
Fig. 2. ADS Logic Chart using OES. ... 8
Fig. 3. Notional ADS testbed architecture using OES ... 10
Fig. 4. ODD, OES, and the “V-model”. ... 11
Fig. 5. AVSC ODD example map. ... 13
Fig. 6. AVSC ODD description table. ... 13

1. Introduction

This document reviews the activities of the NIST Automated Driving System Safety Measurement Technical Working Group (referred to here as the ADS TWG or working group) and presents the results of its work. The document summarizes past and present efforts related to the Operational Design Domain (ODD) of ADS-equipped vehicles and offers a brief synopsis of the genesis of the NIST ADS TWG. It includes definitions for the concepts currently in use to discuss ADS-equipped vehicle safety and introduces the concept of the Operating Envelope Specification (OES) of an ADS-equipped vehicle.

ODD is the design state space of ADS-equipped vehicles that includes elements that are names for operating conditions. The ODD of an ADS-equipped vehicle is determined by ADS-equipped vehicle developers, choosing ODD elements that describe the operating conditions under which the vehicle under design is intended to function. OES is the operating state space of ADS. OES is a scientifically rigorous complement to the notion of ODD, for measuring operating conditions, including those called out in the ODD of the vehicle, toward measuring and assessing the performance of an ADS. The concepts and methods presented in this document for the development of an OES framework include a formal model of ADS operation and a model ADS testbed architecture, based on the NIST Framework for Cyber-Physical Systems (CPS) [1]. The intent is to provide a measurement resource for testing and assessing the performance of ADS-equipped vehicles.

These foundations are intended to provoke further discussion and promote a common understanding of ODD and OES and their use, as well as serve as a basis for ongoing efforts to measure and assess ADS-equipped vehicle safety performance.

2. Background

ADS-equipped vehicle safety and reliable methods for assessing safety performance of these systems are critical for building confidence in these engineered systems. The ADS community is a multi-stakeholder group comprising manufacturers, transportation providers, technology developers and innovators, government organizations, public and private sector researchers, roadway designers and customers.

Technical Note Section Highlights

Section 2. Background—summarizes the discussions of ADS-equipped vehicle safety and ODD during NIST-hosted workshops and meetings of the ADSSM TWG.

Section 3. ADS Safety Abstractions—proposes conceptual foundations for ADS-equipped vehicle safety measurement, including the ADS safety specification abstractions, ODD and OES

Section 4. OES Case Study—applies OES to example operating environment factors that may occur in the ODD of an ADS, and provides an example of OES information to demonstrate how the OES abstraction can be used in assessing ADS-equipped vehicle behavioral competence and to measure the operating environment of an ADS-equipped vehicle.

Section 5. Conclusions and Summary

During the ADSSM TWG meetings, members of the ADS community gathered to discuss concepts and goals for ADS vehicle safety assessment. Prior to the working group's formation, NIST held a workshop on the topic of ADS safety measurement at the NIST Gaithersburg campus in June 2019, titled Consensus ADS Safety Measurement Methodologies. Participants from the ADS community discussed the need for consensus-based measurement methodologies for ADS vehicle safety. A key finding of the workshop participants was that the operational design domain (ODD) of an ADS-equipped vehicle—a description of the operating conditions in which the vehicle is designed to operate—needed further analysis and elaboration.

In response to this challenge, NIST convened the working group, with many of the initial workshop participants and others and open to any interested parties, to discuss ODD and explore foundations for an ADS safety measurement methodology. The ADSSM TWG began biweekly meetings in April 2020 to prepare for a July 2020 workshop, with the goal of producing this technical document. The ADS Safety Measurement and Operational Design Domain Workshop was held July 7-8, 2020 to host deeper discussions of ADS safety measurement and ODD. During this event, thought leaders from the ADS community presented current work, including taxonomies for ODD. They also considered and discussed the role of ODD for ADS safety assessment and identified the need for additional foundational notions to support ADS safety measurement.

ADS-equipped vehicles are a combination of existing vehicle technologies and an ADS that together enables execution of all of the dynamic driving tasks (DDT). For decades, automotive experts have considered the possibility of automating the role of the human driver. Since the 1990s, with the advent of vehicle controller area network (CAN) and other networking technologies, vehicle developers have implemented various automated features and active safety functions. Over the last two decades, manufacturers have introduced and marketed automation of many electromechanical systems using on-vehicle communication networks. These automated features and active safety features range from systems that the driver directly interfaces with—first surface systems, such as instrument panel and center stack or head unit, to systems that function without direct driver input, such as engine, transmission, torque conversion and stability control, as well as features that increase a vehicle’s awareness of its operating conditions.

The process of engineering automated function in an automobile involves coordinating electromechanical functions using onboard communications technologies to allow components to exchange information. A primary concern is for the safety of the operator and passengers of the vehicle and nearby vehicles, as well as pedestrians in the operating environment. Additional concerns include functional, timing, data, and communications concerns.

In legacy vehicles, human drivers accelerate, decelerate, and steer the vehicle to navigate the road system so they can reach their destinations while avoiding harm to themselves and others. Human drivers have the ability to detect and manage risks using their senses and their understanding of how best to operate the vehicle to minimize risk based on experience and training and their grasp of the vehicle’s capabilities. Today’s vehicles included technology that augments the senses, and the responses, of the driver. These include, for example, blind spot warning, noted above, that indicate to the driver the presence of objects or obstacles outside their field of vision, and blind spot assist that invokes limited steering torque to direct the vehicle away from the detected obstacle and avoid a collision.

Increased safety and reduced injuries and fatalities are goals of vehicle automation experts. Automation of driving tasks, including onboard decision-making during their execution, brings with it new challenges such as how to assess whether the ADS-equipped vehicle is able to navigate to its destination while detecting and managing risks that arise.

In the U.S. and elsewhere, the ability to assess vehicle safety is the shared vision of researchers, technology suppliers, manufacturers, and government. Technology suppliers assess the performance of their technologies before providing them to manufacturers. Manufacturers assess their vehicles at the component, system, and full vehicle levels during development and monitor their vehicle's performance, including safety performance, in the field. When warranted, the government establishes safety standards[1] and processes for compliance with those standards and investigates reports of safety issues. Government safety standards establish minimum vehicle performance requirements and provide guidance on the associated tests that the manufacturers perform. Manufacturers are responsible for ensuring their products meet those safety standards and maintaining a record of results that can be made available to an investigator, should any issues be reported. Government testers or researchers may run tests on selected vehicles to assess adherence to the standards provided. Furthermore, regardless of whether a Federal motor vehicle safety standard (FMVSS) may have been specified for a particular performance, manufacturers have the obligation to design systems free of unreasonable safety risks; and the government has broad defect enforcement authority to administer its safety oversight responsibility.

A key finding of participants in the June 2019 NIST workshop was the need to understand in more detail the relationship between ODD and safety assessment and measurement. ODD was originally introduced by the Crash Avoidance Metrics Partnership (CAMP)[2] AVR Project as one of the results of its pre-competitive crash-avoidance research projects. Efforts to provide a common understanding and foundational concepts surrounding ODD are underway at the SAE Industry Technologies Consortia (SAE ITC) through the Automated Vehicle Safety Consortium (AVSC)[3], at the British Standards Institution (BSI)[4], and in European projects such as PEGASUS (Germany) and others. The International Organization for Standardization (ISO) is working on similar efforts based on BSI Publicly Available Specification (BSI PAS) 1883.[5] Finally, additional efforts utilizing the concept of an ODD are in progress under the direction of USDOT and NHTSA.

Though these efforts vary in their approaches, each has presented an "ODD Framework", frequently in the form of ODD taxonomies. These taxonomies comprise structured lists of elements of the operating environment that an ADS-equipped vehicle may claim to be capable of handling. The lists are structured in the sense that they proceed from higher-level categories of elements, such as *weather*, to more specific sub-categories, such as *precipitation*, to further instances of a category, such as rainfall. In some cases, these taxonomy elements include indications of how to quantify elements, such as inches or centimeters of rainfall.

[1] "NHTSA issues Federal Motor Vehicle Safety Standards (FMVSS), https://www.nhtsa.gov/laws-regulations/fmvss .

[2] https://www.campllc.org/avr/

[3] https://www.sae-itc.com/

[4] https://www.bsigroup.com/en-GB/CAV/

[5] https://www.bsigroup.com/en-GB/CAV/pas-1883/

In its efforts to foster a clear understanding of ODD, and its relationship to measuring and assessing safe operation, the ADSSM TWG developed concepts that can be used to characterize quantitatively the operating environment of an ADS-equipped vehicle.

Further, this document describes the context within which the conceptual tools are introduced, including a logic of ADS operation (ADS logic) and a notional architecture for an ADS-equipped vehicle testbed suggested by the ADS logic. These tools relate generally to a variety of autonomous systems and, in the context of ADS safety, may be useful in determining a methodology for ADS safety measurement. The next section presents these abstractions and discusses their potential for providing a foundation for ADS safety measurement.

3. ADS Safety Abstractions

The definition of ODD is included in the April 2021 version of the SAE International (SAE) J3016 document, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* [2]. This discussion of ADS safety abstractions begins with a review of that definition.

> **Definition:** Operational Design Domain (ODD) comprises the operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics. [2]

The ODD, or operating conditions under which the ADS or feature is designed to function, can be documented using a set of reference operating conditions. As mentioned earlier, there are multiple efforts underway to develop and build consensus around such a reference set in the form of taxonomies or lists of operating conditions. Given a reference set of operating conditions—an *ODD framework*—an ODD for a given ADS can then be formed and potentially compared to that of other ADS. The ODD of an ADS is thus a design artifact in that it expresses the design intent of the developer.

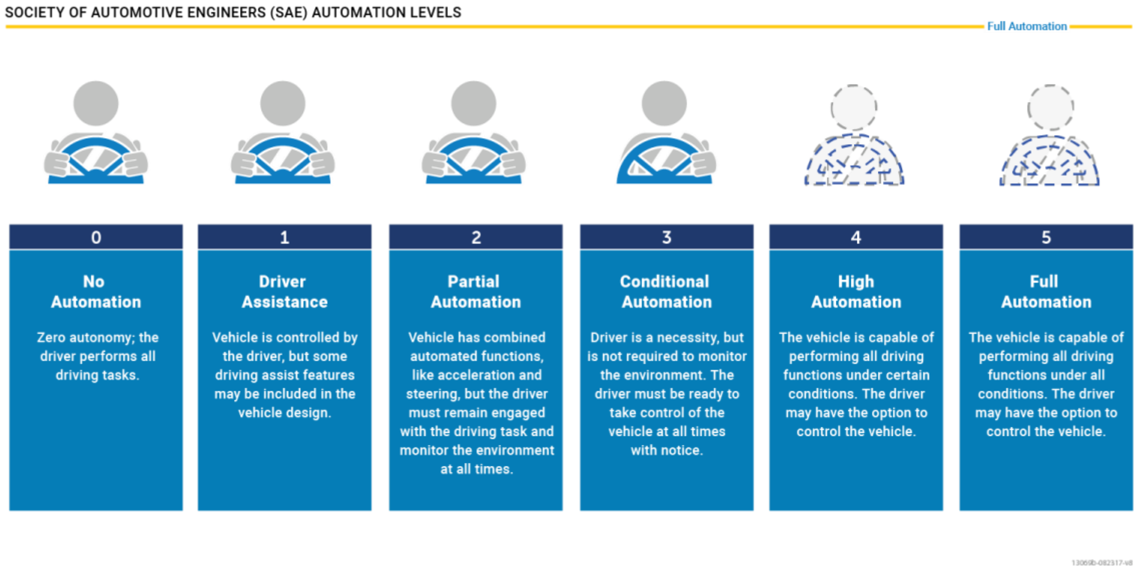
The descriptions of SAE driving automation levels 3 (L3), 4 (L4), and 5 (L5) (see Fig. 1), SAE J3016[6] use the term fallback. J3016 focuses on fallback-ready users for L3. L4 and L5 ADS-equipped vehicles can perform a fallback maneuver to achieve a minimal risk condition (MRC) on exit from its ODD or in the event of a DDT performance-relevant system failure. There are also situations where fallback is not "required" for L4/5 such as when the ADS is no longer functional, in which case J3016 suggests "a failure mitigation strategy may apply (see 3.11 and 8.6)" for some L4/5 systems.

The assessor of ADS operating behaviors and the ADS-equipped vehicle itself need to reason and perform calculations about the driving environment. To function the ADS-equipped vehicle needs to be aware of its current operating environment. Thus, there is a need for an additional safety-related abstraction that:

- describes operating conditions in a way that is measurable;

[6] DOI: https://doi.org/10.4271/J3016_202104

- relates these measurements to concerns about ADS operation; and
- supports reasoning about operating conditions both offboard for assessment of vehicle behaviors and onboard for decision-making.



No Automation: Zero autonomy; the driver performs all driving tasks.

Driver Assistance: Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.

Partial Automation: Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.

Conditional Automation: Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.

High Automation: The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.

Full Automation: The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Fig. 1. SAE automation levels.

The OES of an ADS-equipped vehicle offers a basis for reasoning formally about, or performing calculations related to, the safety of its operating behaviors and therefore serves the need of manufacturers to test their systems and the need of others to assess their safety.

The OES abstraction originated in the work of this TWG.[7] OES provides the means of measuring operating conditions of an ADS-equipped vehicles needed to assess their behavioral competencies[9]. A behavioral competency of an ADS-equipped vehicle is defined in the draft J3164 standard (WIP 2018-01-31) as “a description of an expected capability(ies) from an ADS operating a vehicle within its ODD (if any).” An example of a behavioral competency is “detect and respond to speed limits, speed zones, and speed advisories’ described as ‘adjusts and maintains an appropriate speed for traffic conditions in response to speed limits and speed advisories.”

> **Definition:** An Operating Envelope Specification (OES) is a structured description of the operating environment for driving, useable for formal reasoning (i.e., calculation-based reasoning) about that environment in testing and certification applications and in real-time driving conditions. An instance of an OES comprises the dimensions of the operational state space (whether chosen by the manufacturer, developed from a

[7] ADS Safety Measurement and Operational Design Domain. NIST TWG link: https://www.nist.gov/news-events/events/2020/07/ads-safety-measurement-and-operational-design-domain

relevant scenario set, or defined de novo) sufficient to enable formal reasoning about the state space.

In other words, OES is a structured description of environmental factors or aspects that an ADS-equipped vehicle may encounter during operation. An instance of an OES comprises a set of environmental factors, that make up a description of an operating environment together with parameters that can be reliably measured and thus support formal reasoning about ADS-equipped vehicle operating behaviors in that environment. Examples of OES usage include:

- an ADS-equipped vehicle determining whether it is currently in or outside of its ODD; and
- Designing safety measurement approaches for developers of ADS and roadway infrastructure designers, including measurement methodologies for testing scenarios.

OES builds on three types of information, OES_{Nom}, OES_{Act} and OES_{Ref}.

OES Nominal (OES_{Nom}): Nominal operating conditions, including the associated parameters and their nominal values. Content may include roadway characteristics such as roadway components and their physical dimensions and transit paths, for example.

OES_{Nom} informs product development by the OEM, design and test activities by technology suppliers, as well as independent assessment of ADS-equipped vehicle behaviors. Each of these users would begin development of their OES_{Nom} from a taxonomy for ADS operating conditions (denoted by OES_{Ref} below). An OES_{Nom}, informed by the ODD of the ADS, informs the design, realization and testing of that system by providing measurable parameters for describing each element.

Note that OES may contain elements beyond those covered in an ODD. The data and networking aspects of the ADS-equipped vehicle operating environment are generally not covered by ODD and similarly for the human aspect. This sort of analysis point to differences between OES and ODD. The ODD is targeted at things in the environment that a designer would consider. The OES is targeted at everything in the environment that an ADS would be required to consider.

The elements of an ODD are selected by a designer, who may choose what will be considered and what may not need to be addressed in the design phase. The elements of an OES must reflect the full operating environment. Once developed, say by the OEM product developer, the OES_{Nom} informs both the design of vehicle systems and their testing, verification. and validation.

OES Actual (OES_{Act}): Actual, real-time information specifying changes to OES_{Nom}. Content may include notifications of changes in nominal operating conditions, values for the associated parameters that have changed and the projected duration of the change, for example.

OES_{Act} updates each OES_{Nom} as to which operating conditions have changed with the changes to the values of defining parameters and the anticipated duration of the change. Thus, an OES_{Act} updates one or more element of an OES_{Nom}, for example, changes due to intermittent lane closures or redirections due to roadway repair. The notation $OES_{Nom/Act}$ is used below as shorthand to refer to both forms.

> **OES Reference (OES_{Ref})**: A compendium of operating condition names and parametrized definitions. Content may include, for example, guidance on inventory of roadway characteristics, geometry, angles, controls, design speeds/sight distances, markings, etc.

OES_{Ref} is any taxonomy for use by, for example, an OEM for developing its OES_{Nom} to support verification and validation or for use by infrastructure designers as a starting point in specifying roadway and traffic system design and test. OES_{Ref} is the vocabulary or language of the OES.

As noted earlier, reasoning about the operating conditions of an ADS, using OES_{Nom} and during relevant scenarios or other modalities of test, can be classified as relating to specific engineering concerns such as functional, communications, or trustworthiness concerns and for purposes of providing an assurance case for each concern. The NIST Framework for Cyber-Physical Systems (CPS Framework) [1] provides one such classification. The CPS Framework provides a set of engineering concerns that can be used to sort or classify constraints on system behaviors, such as those provided by regulation or roadway design or those determined during system development. This methodology for classifying constraints will be presented in future work.

The following sections provide examples of how an OES can be used and are presented to illustrate the importance of the OES concept for the logic of ADS-equipped vehicle operation and a notional co-simulation testbed architecture.

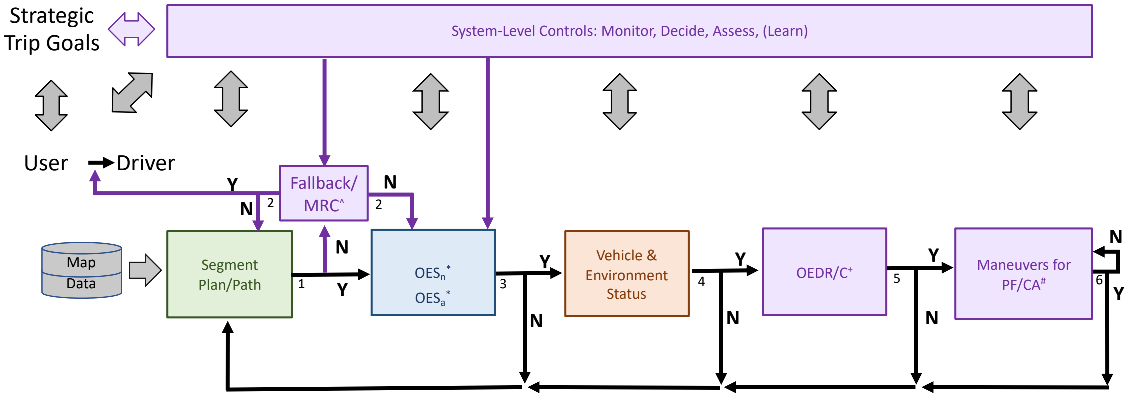
3.1. ADS Logic and OES

An ADS will need to perform the driving tasks previously performed by a human driver, such as “right turn on red” or “unprotected left turn.” Each task or maneuver includes a sequence of steering, braking, and propulsion torque requests. The decisions required for these maneuvers will require information about the current operating conditions. This document refers to such a sequence as a *driving path or segment* and a representation of a driving path as a *driving path plan* or simply a *path plan*.

Expressing constraints on vehicle behaviors is integral to ADS development. The ranges of acceptable variation in environmental aspects can be used to develop constraints on vehicle sensing, controls, and actions during operation. For the ADS itself to assess operating conditions and take action, parameters in its control logic are replaced during ADS operation with current sensor or offboard signals, and the truth-value of pre-conditions of that logic are then evaluated to determine the ADS’s responses.

To perform driving tasks, an ADS will need to be provided with a goal or destination; develop path plans consistent with that goal and nominal roadway data, and subject those plans to assessments of current or real-time roadway data, vehicle and environmental status, and object and event detection, recognition and classification; and finally execute path following (PF) and collision avoidance (CA). We refer to these steps as a series of path assessments, including system level control monitoring. To accomplish its objective, the ADS-equipped vehicle will need to access continuously generated path plans that can be subjected to these checks to help in managing system failures or unexpected obstacles or events in the vehicle path and surroundings.

Should no path plan be available that meets or satisfies these checks, the system will need access to and be able to execute a fallback maneuver, i.e., the ADS will require access to path plans that achieve a minimal risk condition (MRC). Any such fallback maneuver will need to satisfy the assessments of ADS Logic, including current operating conditions. In the case that there is a fallback-ready user, corresponding to an L3 system, the fallback may be to engage that driver to control the vehicle. ADS Logic can be represented as a diagram, referred to here as an *ADS Logic Chart* (see **Fig. 2**).



+OEDR/C: Object and event detection, recognition, and categorization

*OES: Operational envelope specification, n= nominal; a=actual

>DDT: Dynamic driving task

#PF/CA: Path following/Collision avoidance

^MRC: Minimal Risk Condition; Fallback/MRC execution via ADS is a minimal segment/path to achieve minimal risk condition

Fig. 2. ADS Logic Chart using OES.

OES_{Nom} and OES_{Act} both play roles in ADS Logic. OES_{Nom} provides nominal roadway characteristics and the associated parameters, and OES_{Act} provides actual, current information specifying changes to OES_{Nom}. The Path Plan component develops segment plans (paths) using high-resolution map data and Path Management the process of path generation. The path plans may be of arbitrary length and are sent to the vehicle for executing maneuvers. The gray bidirectional arrows in **Fig. 2** represent exchanges of information for purposes of monitoring, control, and may include learning between system-level controls and the other elements of ADS Logic.

The system-level controls of the ADS Logic Chart represent the controls of the vehicle, including DDT execution. The ADS Logic is a logical operation that builds path plans continuously, subjects them to checks, and exchanges information with system-level controls.

ADS system-level controls entirely replace the human driver and their decision-making in SAE automation levels 4 and 5 (L4 and L5) system. The only difference between L4 and L5 is that L4 has a prescribed ODD and L5 does not. The gray arrows in the chart represent bidirectional data exchange, while the unidirectional arrows represent updates.

The unidirectional transitions in the ADS Logic Chart, or checks, are labeled with Y or N and number labels. These checks are explained as the follows:

1. Can a segment plan be produced that is feasible and meets the strategic trip goals?
2. Has the user (e.g., passenger, safety driver) responded to the request to take over the DDT?
3. Does the segment plan/path conform to all OES constraints (is the system within its OES or operating constraints)?
4. Is the status of the vehicle (e.g., fault status) and the environment (e.g., visibility) suitable for the segment plan and OES?
5. Are all detected objects and events reliably identified and categorized?
6. Is the maneuvering process approaching successful completion of the segment plan?

ADS Logic suggests that the ADS function itself should also be assessed during operation. One example of such a metric is the number of viable path plans satisfying the checks of the ADS Logic that are available to the ADS during operation.

3.2. Notional ADS (Testbed) Architecture

As illustrated in Section 3.1, OES_{Nom} and OES_{Act} may be used in ADS operation to enable reasoning about ADS current operation and operating conditions. ADS Logic, and the role of OES, suggest an approach to architecting an ADS testbed for assessing ADS trustworthiness, including safety and security, and other critical concerns.

ADS Logic has implications for the design of ADS and also informs the approach to evaluating operating behaviors of ADS-equipped vehicle. One such approach to safety assessment is to realize the elements of ADS Logic in a simulation, hardware-in-the-loop (HIL) and co-simulation environment, where bidirectional arrows are realized as information exchanges between those simulation, HIL or co-simulation components.

Pursuing this use of ADS Logic, one may derive a notional architecture for an ADS-equipped vehicle testbed that includes the ADS, DDT execution, path planning and management, OES_{Nom} and OES_{Act}, and vehicle/environment functions, including vehicle physics, time and location, sensors, and communications. **Fig. 3** graphically represents such a notional ADS testbed architecture.

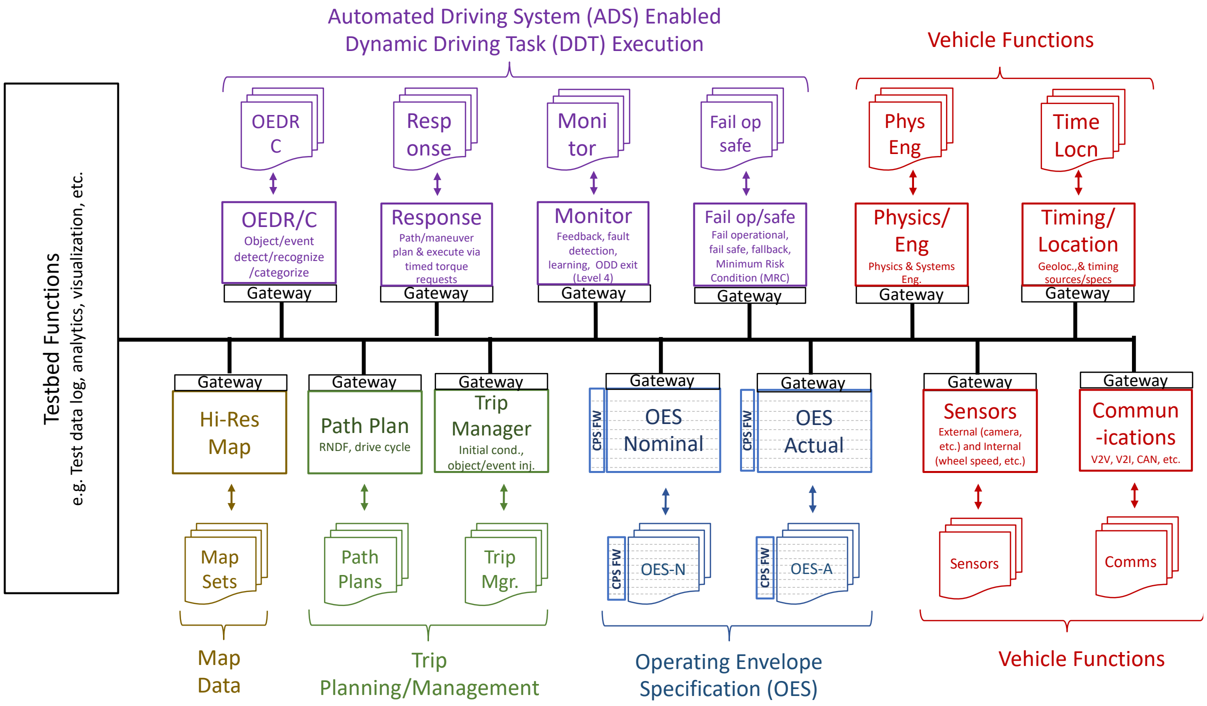

Automated Driving System (ADS) Enabled
Dynamic Driving Task (DDT) Execution
Vehicle Functions
Testbed Functions
e.g. Test data log, analytics, visualization, etc.
OEDR C
Resp onse
Moni tor
Fail op safe
Phys Eng
Time Locn
OEDR/C
Object/event detect/recognize /categorize
Response
Path/maneuver plan & execute via timed torque requests
Monitor
Feedback, fault detection, learning, ODD exit (Level 4)
Fail op/safe
Fail operational, fail safe, fallback, Minimum Risk Condition (MRC)
Physics/ Eng
Physics & Systems Eng.
Timing/ Location
Geoloc.,& timing sources/specs
Gateway
Hi-Res Map
Path Plan
RNDF, drive cycle
Trip Manager
Initial cond., object/event inj.
CPS FW
OES Nominal
OES Actual
Sensors
External (camera, etc.) and Internal (wheel speed, etc.)
Commun -ications
V2V, V2I, CAN, etc.
Map Sets
Path Plans
Trip Mgr.
OES-N
OES-A
Sensors
Comms
Map Data
Trip Planning/Management
Operating Envelope Specification (OES)
Vehicle Functions

Fig. 3. Notional ADS testbed architecture using OES.

The elements of **Fig. 3** include testbed components, indicated as blocks with bus gateways; data consumed or produced by components, indicated as stacks of documents; a testbed communication bus, indicated by a connecting line; and testbed management functions, including functions for executing a test procedure and gathering, analyzing, and visualizing test results. This Notional ADS Testbed Architecture can be realized using a variety of technologies. One such technology platform is the Universal CPS Environment for Federation (UCEF), developed at NIST for the study of CPS and Internet of Things (IoT) generally. Using ADS Logic and this notional testbed architecture, one can study how well the DDT is performed by an ADS-equipped vehicle in a partial or fully virtual environment.

3.3. Relationship between ODD and OES

ODD is a strong concept that is evolving as a result of the efforts underway in the ADS community and is suitable for use in the design specification of an ADS. In the course of developing a vehicle (i.e., conceptualization, realization, and assurance), a manufacturer determines at the outset the feature or functional content of the intended vehicle. In the case of an ADS-equipped vehicle, this functional content includes an ODD. This expression of feature content intent is then used to determine design requirements for the full vehicle system, its sub-systems and components needed to deliver that content. These component and system specifications are typically delivered to specialized suppliers, together with any applicable industry standards. Suppliers then develop the components and systems, either on their own or with a manufacturer.

These prototype components and systems are developed and tested, assembled into sub-systems and tested, and finally assembled into whole vehicle prototypes and tested. All tests are based on the design and manufacturing requirements for those systems, components, sub-systems, or the whole system. **Fig. 4** displays what is typically referred to as the "V-Model", which depicts the activities in an OEM product development process.

Each activity of this development process produces a variety of artifacts, including data associated with system and component requirements testing and validation. Together the artifacts of all these phases of development make up the body of evidence that can be used in assurance arguments, according to best practices, including assurance arguments using standards or expert opinion. Among these requirements are those added specifically for safety.

OES, and the tools it provides for measuring the ADS-equipped vehicle operating environment, is needed to support reasoning about vehicle behaviors or competencies in those environments.

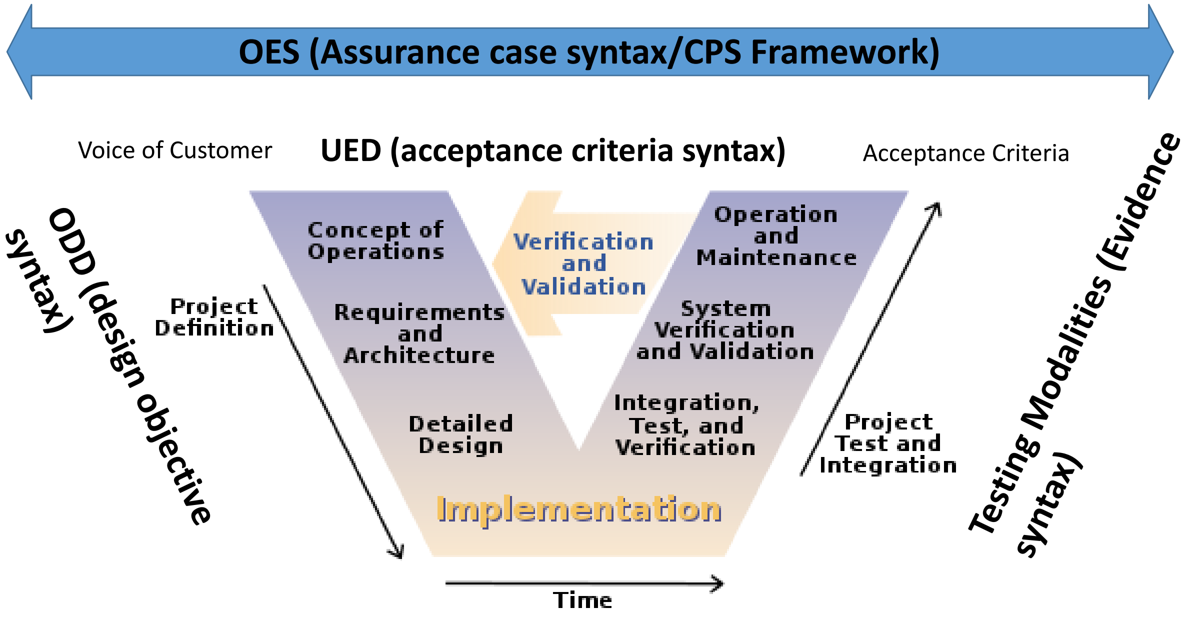

OES (Assurance case syntax/CPS Framework)
Voice of Customer
UED (acceptance criteria syntax)
Acceptance Criteria
ODD (design objective syntax)
Project Definition
Concept of Operations
Requirements and Architecture
Detailed Design
Implementation
Verification and Validation
Operation and Maintenance
System Verification and Validation
Integration, Test, and Verification
Project Test and Integration
Testing Modalities (Evidence syntax)
Time

Fig. 4. ODD, OES, and the "V-model".

The ODD as defined by SAE is intended to enable ADS design, setting out the operating conditions under which a given ADS or feature thereof is specifically designed to function. The OES is intended to enable ADS operation and testing, providing a structured description of the operating environment suitable to support formal reasoning in testing and validation applications and in real-time driving. Since both are descriptions of the operating environment, albeit expressed in different terms for distinct purposes, there is intrinsic overlap between these concepts, and they must be aligned.

For example, the ODD for a given system sets the *boundaries* for testing. For instance, it would be inappropriate to test a system in operating conditions outside its specified ODD. The $\text{OES}_{\text{Nom/Act}}$ provides the *basis* for testing and evaluating results, i.e. it enables the application of formal reasoning to structuring a test program and assessing the results for purposes of assurance. In this example, the ODD sets out limits to the relevant operating state space while $\mathrm{OES}_{\mathrm{Nom/Act}}$ specifies its full contents. (Note that $\mathrm{OES}_{\mathrm{Ref}}$ covers the operating state space relevant to any ADS while $\mathrm{OES}_{\mathrm{Nom/Act}}$ is specific to a given ADS.)

The need for aligning ODD and $\mathrm{OES}_{\mathrm{Nom/Act}}$ is evident in considering real-time operations. In performing the dynamic driving task (DDT), ADS logic (see Fig. 2) involves evaluating sensor input against information about the operating environment (i.e., $\mathrm{OES}_{\mathrm{Nom}}$ and $\mathrm{OES}_{\mathrm{Act)}}$) to develop maneuvering plans (described here as segment or path plans). For safety, the information about the environment (i.e., the OES) must be sufficiently complete to allow reliable maneuvering under all relevant conditions. SAE J3016 provides that Level 4 and 5 ADS-equipped vehicles must be capable of performing the DDT fallback to achieve a minimal risk condition upon exiting the ODD. This requires that ODD limits be included in the information about the environment that the ADS consults so that it may determine when it is approaching or leaving ODD boundaries. Thus, OES must include all ODD information (encoded in a form suitable for reasoning) as well as all other environmental information needed for safe operation.

4. OES Case Study

This section illustrates the use of OES. OES information, including $\mathrm{OES}_{\mathrm{Ref}}$, $\mathrm{OES}_{\mathrm{Nom}}$, and $\mathrm{OES}_{\mathrm{Act}}$ can be described in detail once a choice of operating conditions, including relevant ODD items, that an ADS may encounter during operation is provided. Consider, as an example of an operating environment, the ODD drawn from the recent AVSC release document [3]. This ODD is expressed there as a narrative and in tabular form, composed of ODD items from the AVSC document.

> The system is designed to operate on the road network in the urban center of Detroit, Michigan (see map in Fig. 5) on all streets with a speed limit of 35mph or less. Its boundary is constrained by I-75 to the north; I-375 to the east; M-10 to the west; and Atwater Street along the Detroit River to the south. The areas around the Detroit Police Department and Department of Public Safety are excluded from this ODD. The system is capable of operating during daylight hours when the sun is at or above the horizon. It can operate in fair weather, including wind gusts up to 35 mph, light rain, and light snow, provided the road surface is not covered by snow. It recognizes and understands all signage and traffic control devices inside this ODD. Work zones are coordinated with the local transportation department and excluded from the route network as needed [3].

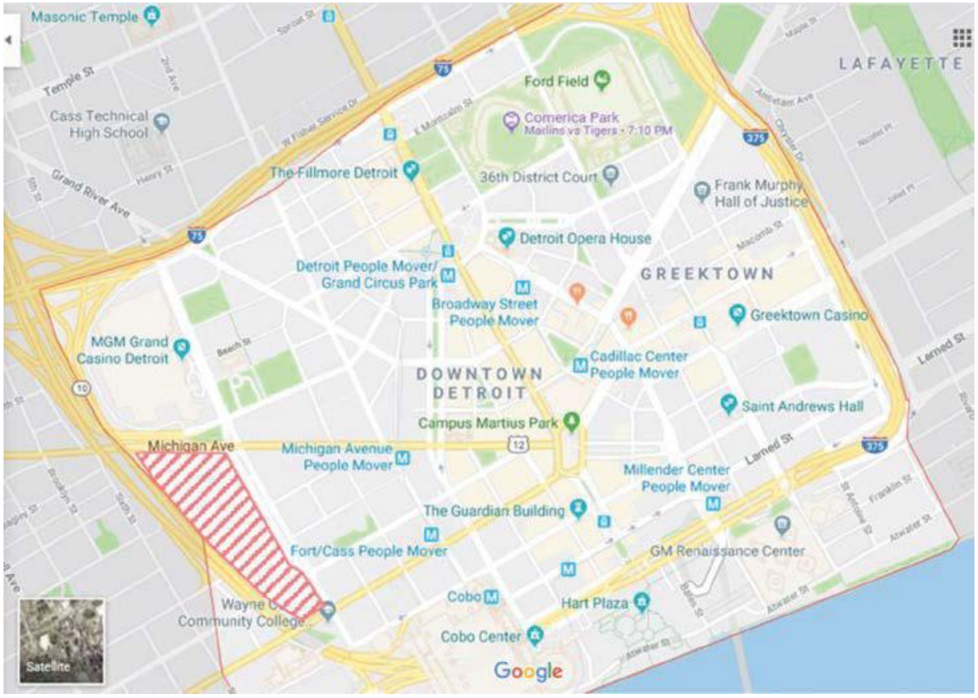
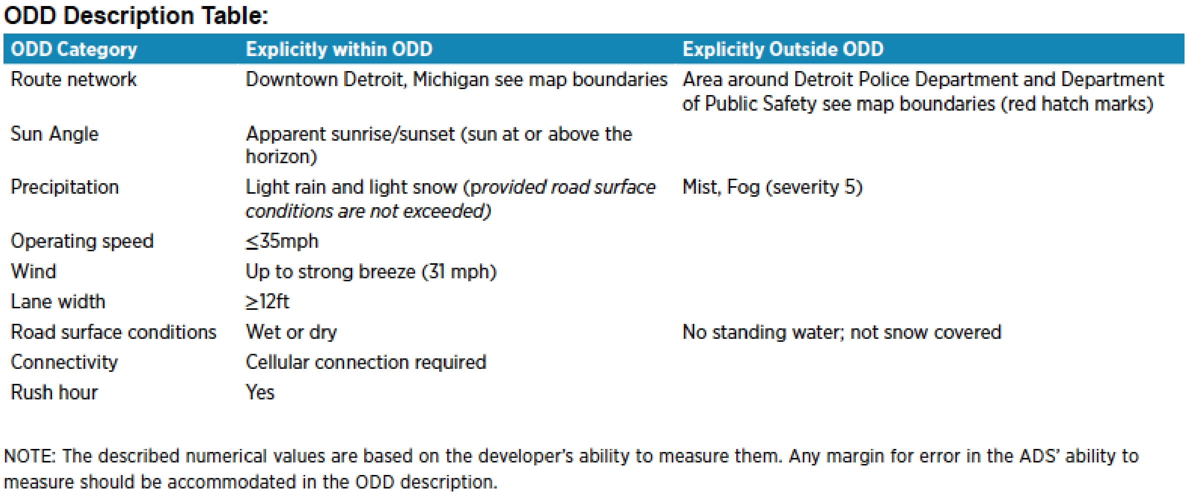


Fig. 5. AVSC ODD example map.

As noted above, this ODD narrative can also be expressed in a tabular form. **Fig. 6** shows an AVSC ODD description table from the AVSC Best Practice for Describing an ODD [3], with column headings ODD Category, Explicitly within ODD, and Explicitly Outside ODD.



ODD Description Table:

ODD Category	Explicitly within ODD	Explicitly Outside ODD
Route network	Downtown Detroit, Michigan see map boundaries	Area around Detroit Police Department and Department of Public Safety see map boundaries (red hatch marks)
Sun Angle	Apparent sunrise/sunset (sun at or above the horizon)	
Precipitation	Light rain and light snow (*provided road surface conditions are not exceeded)*	Mist, Fog (severity 5)
Operating speed	≤35mph	
Wind	Up to strong breeze (31 mph)	
Lane width	≥12ft	
Road surface conditions	Wet or dry	No standing water; not snow covered
Connectivity	Cellular connection required	
Rush hour	Yes	

NOTE: The described numerical values are based on the developer's ability to measure them. Any margin for error in the ADS' ability to measure should be accommodated in the ODD description.

Fig. 6. AVSC ODD description table.

This example illustrates how an ODD describes boundaries and sets limits on weather, lighting, lane width, and other conditions in a manner suitable for developing ADS design requirements. However, an ODD does not focus on specific features of the operating environment such as the intersection types to be encountered by the ADS during operation.

Developing the OES information for complex driving environments goes beyond the scope of this document. Instead, section 4.1 below illustrates OES_{Ref}, OES_{Nom}, and OES_{Act} for a single roadway characteristic, an intersection, and a single intersection type in the functional aspect of an OES.

4.1. Example OES Information

Below is an example of OES information for a four-way stop intersection. The terminology for roadway characteristics, including associated parameters, may be standardized. There exists a considerable literature covering past and current efforts to do just this, including federal and state documents for the U.S. and elsewhere. An example is the AASHTO Green Book [4]. In the following, we use information from the AASHTO Green Book for the OES information related to intersection configuration and from the Manual on Uniform Traffic Control Devices (MUTCD) for OES information related to traffic controls for a four-way stop intersection below.

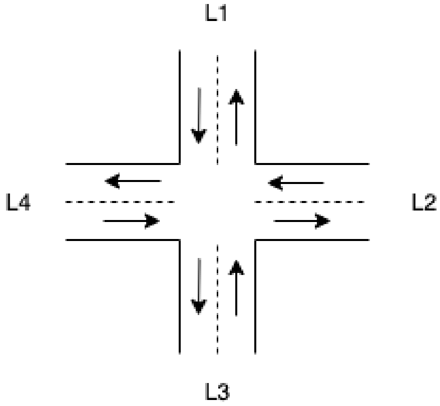
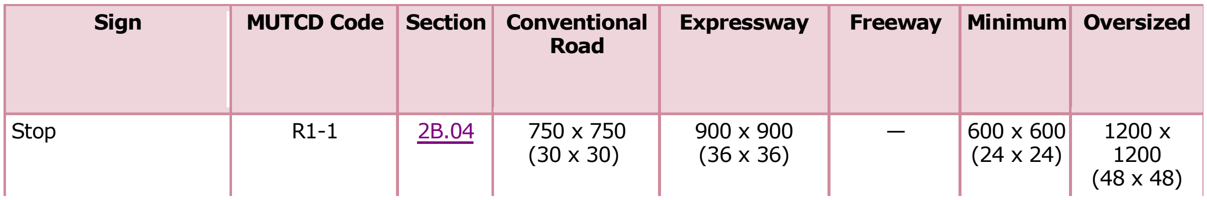


Fig. 7. Unchannelized 4-leg intersection.

- OES_{Ref}: A 4-way stop intersection is defined by:
  - Intersection type: unchannelized 4-leg intersection;
  - An enumeration of the intersecting roadway legs (a unique way of naming or numbering the legs, e.g., starting at magnetic north and proceeding clockwise);
  - Roadway leg types, including but not limited to roadway leg number (or name) together with the number of thru lanes on that leg, the number of right turn lanes and left turn lanes;
  - Adjacent roadway leg angles of 30-90 degrees, including adjacent roadway leg numbers (or names) and the angle in degrees between the named adjacent roadway legs; and
  - A configuration of intersection controls, including control type and position of stop signs or other controls.



Sign	MUTCD Code	Section	Conventional Road	Expressway	Freeway	Minimum	Oversized
Stop	R1-1	2B.04	750 x 750 (30 x 30)	900 x 900 (36 x 36)	—	600 x 600 (24 x 24)	1200 x 1200 (48 x 48)

Fig. 8 MUTCD Stop Controls Data

- etc.

- OES_{Nom}: The nearby 4-way intersection is of the following configuration:
  - Intersection legs: L_1-L_4;
  - Leg types: L_1-L_4 are two-lane surface roads;
  - Intersection geometry: 90-degree angles between intersection legs L_1-L_4;
  - Configuration of intersection controls: Stop signs of type MUTCD R1-1, positioned at the right side of each leg L_i at 45-degrees to D_i and D_{i+1} (for i=1,2,3);
  - etc.

- OES_{Act}: Notification issued, in this example, where an accident resulted in damage to the stop sign between legs L_2 and L_3. The notification lists changes to the OES_{Nom} for the intersection in question and remains in effect until further changes are made (e.g., accident is cleared, and replacement is complete):
  - Notification type: Change in Controls Configuration;
  - Valid timeframe: Two weeks from 11/1/2021 to 11/15/2021;
  - Controls Configuration changes: Temporary stop sign between leg D_2 and D_3 positioned between legs L_2 and L_3;
  - etc.

This set of example information types is not complete, nor is it fully aligned with available FHWA and individual state guidance. For ADS onboard use, OES information will need to be machine-readable to facilitate onboard reasoning and calculations. Nonetheless, this example information is indicative of the methodology for using OES in support of ADS-equipped vehicle safety assessment.

5. Conclusions and Summary

The ODD and OES abstractions serve different purposes in the development and assurance of ADS-equipped vehicles. Fig. 9 illustrates several relations between ODD, OES, and scenario-based testing. An ODD for a Level 4 ADS-equipped vehicle, as laid out in the AVSC best practice document [3], serves as guidance to manufacturers, their developers and suppliers, government, and customers, by enumerating the operating conditions under which the vehicle will operate. The ODD of an ADS-equipped vehicle is currently determined by the manufacturer. The ODD provides a means of describing the operational intent of the manufacturer but does not provide the methods and approach to reasoning formally about the operating conditions of the ADS-equipped vehicle. That is the purpose of the OES.

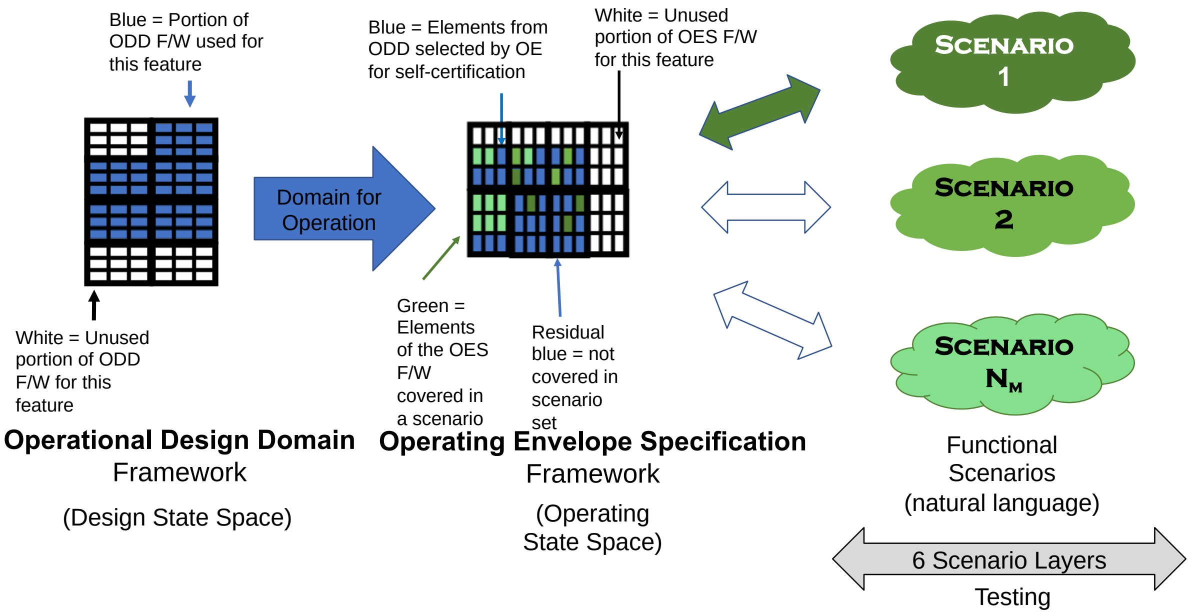

Blue = Portion of ODD F/W used for this feature
White = Unused portion of ODD F/W for this feature
Domain for Operation
Blue = Elements from ODD selected by OE for self-certification
White = Unused portion of OES F/W for this feature
Green = Elements of the OES F/W covered in a scenario
Residual blue = not covered in scenario set
Scenario 1
Scenario 2
Scenario N_M
Operational Design Domain Framework
(Design State Space)
Operating Envelope Specification Framework
(Operating State Space)
Functional Scenarios (natural language)
6 Scenario Layers
Testing

Fig. 9. Relation between ODD and OES frameworks and ADS-equipped vehicle testing.

Examples of OES users include developers, technology suppliers, infrastructure designers and other stakeholders. ADS developers use and benefits include those in designing test setup for testing determining test cases. Suppliers of ADS technology could use OES in assessing their having met performance specifications provided by developers. Infrastructure designers, owners and operators would benefit from OES in determining roadway characteristics desirable for ADS operation. Also, teleoperators of ADS would have in OES data support for teleoperation, either remote driving or remote assistance.

OES data may be created, and maintained, by public and private entities. Examples include ADS developers and their technology suppliers, infrastructure owners and operators, and map data suppliers. SAE J3131, *Automated Driving Reference Architecture*, describes the domain of static and dynamic operating condition data as a mix of public and private stakeholders, e.g., by region or state. Map data suppliers is an example of a private sector role, while managers of permanent or temporary roadway characteristics is an example of a public sector role.

An OES reference framework can inform research, ADS operation, and ADS infrastructure design, as well as testing by design engineers, local and state infrastructure designers, and government. Once defined, described, and assessed to be a comprehensive set of information, OES characterizes, and enables the measurement of, environmental operating conditions that an ADS may encounter during its operation. OES items are reliably measurable and support reasoning about ADS-equipped vehicle operating conditions. On the ADS-equipped vehicle, the parameters of OES_{Nom} appear in the pre-conditions of its system-level controls and describe the nominal envelope of its operating environment or its operating state space. The data of OES_{Act} serve to update that OES_{Nom} description of the operating environment and, in so doing, the decisions of the ADS control logic. For ADS-equipped vehicle development, vehicle behaviors can be assessed, using an OES reference framework to choose values of OES parameters consistent with the state space of the operating environment.

Acknowledgments

The members of the ADSSM TWG are acknowledged for their effort and contributions in developing the concepts described in this document. Particular thanks go to Michelle Chaka, Francesca Favaro, Siddartha Khastgir, Shawn Kimmel, Greg Leeming, Ed Straub, Jack Weast, and Barb Wendling for their comments and insights.

References

[1] Griffor E, Greer C, Wollman D, Burns M (2017) NIST Framework for Cyber-Physical Systems (CPS) (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[2] SAE International (2014) Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Surface Vehicle Recommended Practice J3016, Revised 2018-06-15. https://www.sae.org/standards/content/j3016_201806/

[3] SAE International (2020) AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon, Automated Vehicle Safety Consortium™ Best Practice AVSC00002202004. https://www.sae.org/standards/content/avsc00002202004/

[4] AASHTO (2011) A Policy on Geometric Design of Highways and Streets. The American Association of State Highway and Transportation Officials, AASHTO Green Book, Washington DC.

[5] Manual on Uniform Traffic Control Devices (MUTCD). https://mutcd.fhwa.dot.gov/

Other Documents

1. National Highway Traffic Safety Administration (2016), “Federal Automated Vehicle Policy: Accelerating the next revolution in roadway safety,” https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf .

2. National Highway Traffic Safety Administration (2017), “Automated Driving Systems 2.0: A vision for safety,” https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems

3. Thorn E., Kimmel S. and Chaka M. (2018), “A Framework for Automated Driving Systems Testable Cases and Scenarios,” National Highway Traffic Safety Administration, Publication No. DOT HS 812 623.

4. German Federal Ministry for Economic Affairs and Energy, “Project Pegasus,” [Online]. Available: https://www.pegasusprojekt.de/en/about-PEGASUS.

5. Fraade-Blanar L., Blumenthal M.S., Anderson J.M. and Kalra N. (2018), “Measuring Automated Vehicle Safety: Forging a framework,” RAND Corporation, Available: https://www.rand.org/pubs/research_reports/RR2662.html .

6. Lefler, N. (2017), “Model Inventory of Roadway Elements - MIRE 2.0,” Federal Highway Administration, Available: https://safety.fhwa.dot.gov/rsdp/mire.aspx .

7. Google Maps (2021), “Map of Detroit, Michigan,” [Online]. Available: https://www.google.com/maps/place/Detroit,+MI/@42.3523699,-

83.169275,12z/data=!4m5!3m4!1s0x8824ca0110cb1d75:0x5776864e35b9c4d2!8m2!3d42.331427!4d-83.0457538. [Accessed 13 April 2021].

8. Federal Highway Administration (2013), "Highway Functional Classification Concepts, Criteria and Procedures," U.S. Department of Transportation, https://www.fhwa.dot.gov/planning/processes/statewide/related/highway_functional_classifications/.