Formalization of Operational Domain and Operational Design Domain for Automated Vehicles

Ali Shakeri
German Aerospace Center (DLR),
Institute of Systems Engineering for Future Mobility,
Escherweg 2, 26129 Oldenburg, Germany,
ali.shakeri@dlr.de

Abstract—Specifying an Operational Design Domain (ODD) is crucial for safeguarding automated vehicle systems against conditions that exceed their capabilities. Yet, prior definitions of ODD have relied on ambiguous and unclear terms, resulting in numerous misunderstandings and misconceptions. This paper introduces a formal approach to clearly define the Operational Domain (OD) and ODD for automated vehicles. Furthermore, the absence of essential terms, such as the OD, has resulted in the creation of numerous terms that have made things more complicated and confusing. This level of complexity is unacceptable when it comes to developing safety-critical systems, where any uncertainty can lead to significant risks. This study addresses these deficiencies by providing a precise mathematical model of OD and clarifying its relationship with other terms. Also, by formalizing these terms, this work establishes a foundation for developing further concepts such as ODD specification and ODD monitoring, which are explained in this paper.

Keywords–Operational Domain; Operational Design Domain; Formal Specification; ODD Specification; ODD Monitoring

1. Introduction

Automated systems are limited by their hardware and software, meaning they cannot operate in all environments or under all conditions. As a result, it is critical to define the safe operational domain for such systems and ensure they do not exceed their capabilities. This is where the concept of Operational Design Domain (ODD) becomes significant, safeguarding the systems against the broad operational domain.

Among various automated systems, defining ODD for Automated Driving Systems (ADS) is of greater importance due to their safety-critical nature. Additionally, as the level of autonomy [1] increases, the decision-making responsibility increasingly shifts from humans to machines. Therefore, ADS must be capable of handling more unexpected things that may go wrong in the real world. Consequently, such systems shall have an accurate and consistent model of their operational domain and ODD. Otherwise, any misinterpretation in the operational domain and ODD could lead to injuries or put lives at risk [2].

Due to its importance, the topic of ODD has been a subject of considerable interest among researchers and industries. The various studies and standards that have emerged from these efforts will be discussed in more detail in Section 2. However, it is worth mentioning here that despite the efforts made so far, there is still confusion regarding fundamental concepts and their connection. This confusion leads to various issues, such as misinterpretation of terminology, development of new concepts based on misconceptions, and proliferation of terms and concepts in new research and standards. These issues can significantly delay development processes and increase costs and safety risks. In the following, we will describe each of these issues and their consequences.

SAE J3016 defines ODD as ”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” [1]. While the SAE’s definition of ODD is a useful starting point, it lacks a clear definition for terms like ”operating condition” and ”restriction”, making the definition ambiguous and opening the doors to misinterpretations. Such misinterpretation of terms could cause misunderstandings between different engineering teams, and even worse, the ambiguity could propagate to future standards. Consequently, this will increase not only costs and delays but also safety risks, which is unacceptable for safety-critical systems.

On the other hand, the lack of a clear definition of OD can lead to misconceptions. One common misconception is the use of the term ”ODD taxonomy”, while it is clear that ODD is a specific property of a vehicle system that alters with every alteration in sensor setup or system design decision. What the standardization committees, including the recent ISO 34503, refer to as the ODD taxonomy, is, in fact, a taxonomy for characterizing the operational domain attributes. This misconception may not seem significant, but it can actually affect future work. For instance, as of writing this paper, there is no known method for generating scenario descriptions based on operational domain attributes (the recent work from Zhang et al. only covers scenario generation based on ODDs [3]).

Another problem with the SAE’s definition is that it establishes no relationship between ODD and the OD. The lack of a definition for OD leads to the introduction of many other unnecessary terms with very vague definitions, such as ”Operational World Model,” ”Operational Road Environment Models,” and

”subject vehicle models” in Czarnecki work [4]. As another example, in an attempt to establish an ODD specification, Schwalb et al. [5] encountered difficulties as they tried to formalize related concepts. The absence of a clear relationship between ODD and the operational domain led to the creation of new terms in their work, including ”situation” and ”facts”, which themselves lacked proper definitions and therefore made the formalization hard to follow [5]. Besides, this proliferation of terminology adds complexity and ambiguity and can hinder research and development efforts.

Furthermore, the three primary problems discussed earlier can have further negative impacts. Due to broken relations between existing concepts, it is not easy to develop other concepts. One important concept is ODD monitoring, which ”is essential for the ADS to be able to decide on triggering the minimal risk manoeuvre (MRM) or issuing a transition demand by the ADS” [6]. Colwell et al. describe the purpose of ODD monitoring as ”to determine whether or not the ADS is in a situation that it was designed to handle safely” [7] while they do not clarify the meaning of ”situation”. Also, C. Sun et al. define ODD monitoring as ”to monitor the vehicle states and driving environment that satisfy a specific ADS function requirement” [8]. However, it is unclear what ”vehicle state” or ”function requirement” means.

To address issues, this paper will use a formal method based on notable work by Olderog [9] to clarify concepts and their relations. This study begins by defining OD as a key concept. Then, we show how this concept simplifies the development of related concepts such as ODD specification and ODD monitoring. After describing the terms, we present a formal representation of them. This final step is necessary to clarify the relationship between these concepts with less ambiguity. Finally, this work demonstrates how the new formulation enables us to create a more accurate model of OD and ODD.

It is important to note that the current work strives to avoid creating a detailed and precise ODD specification or offering a description for operational domain taxonomy. For this reason, certain concepts have been intentionally simplified to effectively convey the main message, highlighting the importance of formal methods in this domain. The novelty of the current work is establishing clear relations between essential concepts in the field of ODD for automated vehicles. Furthermore, it enables us to describe other concepts using these main ones.

This study starts with an overview of related work in Section 2. Then in Section 3 the fundamental terms are defined. Building upon this foundation, the concepts of ODD and ODD specification are also defined in Section 3. Next, the mathematical preliminaries are presented in Section 4, essential for formally representing the defined concepts. After that, a formal representation of OD in Section 5 and ODD and ODD specification in Section 6 is introduced. Also, further concepts, such as ODD monitoring, are discussed in Section 6. Finally, concluding remarks and future work are provided in Section 8.

2. Related Work

The operational domain of autonomous vehicles (AVs) consists of many different dimensions. Researchers and organizations have proposed various taxonomies to categorize these dimensions and describe the operational domain. The National Highway Traffic Safety Administration (NHTSA) identified a preliminary set of attributes categorized into six main categories [10]. Koopman and Fratrik emphasized the importance of defining the operational environment for AVs by listing critical aspects such as terrain characteristics and environmental conditions. They proposed a comprehensive list of factors relevant to describing the operational domain. Gyllenhammar et al. develop a framework to categorize and quantify the ”operating conditions” [11]. Other standardization committees have also attempted to define the operational domain for ADS by developing a taxonomy of its attributes [12], [13], [6].

The operational domain can be infinite because of the endless possibilities of traffic situations. Neurohr et al. suggest that an approach to scenario description is crucial for comprehending the operational domain of automated vehicles since it allows the organization and analysis of the infinite space [14]. Moreover, the operational domain is not a static entity and can change over time. As a result, new classes, properties, and attributes may emerge. This has been discussed by Weshhofen et al., who suggest using ontologies to formally represent both the operational domain and critical phenomena in urban traffic scenarios [15]. In another research, Erz et al. suggest an ontology to bridge the ODD, scenario-based testing, and AV architecture [16]. By leveraging this ontology, the authors seek to provide systematic guidance for defining ODDs.

Efforts have been made to develop languages that define ODD for driving systems. Irvine et al. (2021) propose a structured natural language approach to defining ODD for Automated Driving Systems (ADS), aiming to enhance understandability and accessibility for a diverse range of stakeholders, including regulators and system designers. Schwalb et al. built upon Irvine’s work, transitioning from a structured natural language format designed for clarity and accessibility towards a more formal representation aimed at programmatic execution. At the time of writing this article, the ASAM OpenODD standardization committee is actively working on developing a language to describe the ODD specification [17].

3. Terminology and Definitions

Historically, conventional vehicle systems, including cars, trucks, and motorcycles, have been designed to function within a wide range of infrastructures built on the earth’s surface. In such vehicle systems, a human driver is responsible for handling external conditions such as environmental and dynamic traffic. With the advent of AVs, depending on their level of autonomy, they will take over some or all of these responsibilities. Therefore, an AV must have a model of the environment within which it operates, referred to as the operational domain in this work.

The automated vehicle will use sensors to perceive the operational domain and actuators (e.g., braking system) to interact with it. Consequently, the vehicle's operation is primarily limited by the quality of its sensors and the response of its actuators. Also, the qualities of OD, such as infrastructure, environmental conditions, and dynamic traffic, can significantly impact the AV's performance. Accordingly, engineers, infrastructure operators, and AVs must clearly understand the operational domain and its attributes. A formal model of the operational domain is necessary, but first, a definition of it is required.

Definition 3.1 (operational domain)**.** The operational domain for vehicle systems refers to the attributes of the physical surroundings in which the vehicles navigate, including the natural terrain and human-made infrastructure, environmental phenomena, and traffic conditions.

According to the above definition, characterizing the operational domain attributes is crucial to better understanding it and creating an accurate model of it. This characterization is done through several standards that provide a taxonomy for operational domain attributes [12], [13], [6]. However, it is worth mentioning that the ODD taxonomy standards, such as the recent ISO 34503, despite their nomenclature, actually offer a taxonomy for the operational domain.

Next, it is important to acknowledge that AV systems cannot function in all environments due to hardware or software constraints. An automated vehicle - excluding those classified as SAE level 5 [1] - is not designed to function throughout the entire operational domain. Rather, it can safely operate only within a specific and restricted region of the operational domain, known as the Operational Design Domain (ODD). The ODD can be defined based on the operational domain, which is as follows:

Definition 3.2 (Operational Design Domain)**.** An Operational Design Domain (ODD) for a specific vehicle system refers to a subset of the operational domain (see Definition 3.1) within which the system is specifically designed and engineered to operate safely.

The definition given above establishes a relationship between ODD and OD; that is, ODD for a particular system is a specific region within the OD. For AV systems, it is essential to clearly and unambiguously specify this region for the system and the driver. Failure to do so could result in the vehicle encountering circumstances beyond its control or confusion in making a decision. For more detail, see completed investigation cases [18] that involved an AV crash. An ODD specification is defined as follows:

Definition 3.3 (ODD specification)**.** An ODD specification for a specific system comprises a collection of declarative statements defined over OD attributes characterized by an OD taxonomy. These statements specify the ODD (see Definition 3.2) and ODD boundaries within OD.

It is important to note that the terms "ODD" and "ODD specification" are often used interchangeably, but they actually have distinct meanings. While ODD refers to the specific domain in which a system is intended to operate, ODD specification is a term used to define and specify that specific domain. Figure 1 provides a high-level illustration of the relationship between fundamental concepts used in the current study.

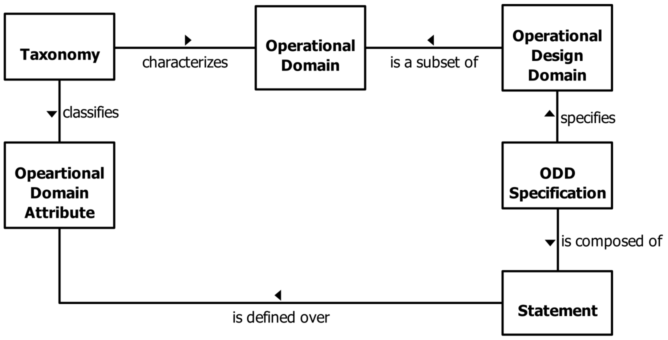

Figure 1. This illustration depicts the relationship between different concepts used in this work. The Operational Domain is characterized by a Taxonomy such as ISO 34503 [6], which also classifies the Operational Domain attributes. An Operational Design Domain is a subset of the Operational Domain, specified by an ODD specification that is composed of a collection of Statements defined over attributes.

Furthermore, it is worth noting that an ODD could be an infinite set of values that is hard to represent in computer systems. Yet, ODD specification is a finite set of declarative statements, each declaring an acceptable range of values for OD attributes based on the system's limitation.

This study intentionally employs a simplified ODD example to focus on introducing the terms, concepts, and their mathematical representation. However, this will not undermine the applicability of the formalization method to practical cases. As an example, consider the following textual specification that specifies the ODD for a specific AV system using natural language:

The system is designed and only allowed to operate

on motorways, (s_1)

where pedestrians are prohibited, (s_2)

up to speed of 60 km/h. (s_3)

The ODD specification, as described above, comprises three statements: (s_1), (s_2), and (s_3) that presume the safe operation of the system only when it operates in motorways, in the absence of pedestrians, and with the maximum operational speed of $60\,\mathrm{km/h}$.

A natural language specification could lead to ambiguities and uncertainty when specifying the ODD. Therefore, the statements containing temporal and spatial constraints shall be expressed precisely. Accordingly, they shall be formalized using a formal specification method such as the one established by E.-R. Olderog and H. Dierks [9] for real-time systems. Besides, computer systems require a machine-readable specification. This study does not have the goal of creating a specification that can be read by machines. Instead, the ASAM OpenODD standardization committee [17] is developing a language that can be used to describe OD and specify ODD. The remainder of this study focuses on formally representing OD, ODD, and ODD specifications.

4. Preliminaries

As discussed in previous section, formalization of concepts including OD, ODD, and ODD specification is necessary. This formalization is based on some preliminary definitions which is provided in this section. Here, the formal definition of attributes and statements is presented, which is the building block of other concepts.

4.1 Attributes

The operational domain can be described by a set of attributes denoted as $\mathbb{A} = \{A_1, A_2, \ldots, A_n\}$ and their corresponding set of data types $\mathbb{D} = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n\}$. Let A be an attribute with data type $\mathcal{D}$, i.e., A has a value in $\mathcal{D}$. For brevity, the notation $\mathcal{D}(A)$, is introduced to denote the data type of an attribute A.

To start with an example, consider ODD statements that were introduced in Section 3. The statement (s_1), implicitly assumes that among different "road types" the system is designed to operate on "motorway". For this statement, we can abstract "road type" as an attribute and "motorway" as a value for this attribute. For the sake of this example, let us assume that the attribute "road type", denoted by A_1, accepts three values, namely "motorway", "regional", and "rural". In the same way, the statement (s_2) can be described using the attribute "presence of pedestrian", denoted by A_2 that has a Boolean data type, i.e. it's value is "true" whenever there is a pedestrian on the road at a specific time and location and is "false" otherwise. Finally, the statement (s_3) can be described by an attribute "operational speed", denoted by A_3, that represents the speed the vehicle is allowed to reach. This attribute is described with a real number data type.

The semantic of an attribute A, is given by an interpretation, $\mathcal{I}$, at a certain time, $t \in \text{Time}$, and location, $(x, y) \in \text{Space}$. The interpretation, $\mathcal{I}$, is a mapping that assigns to each attribute A, a value in $\mathcal{D}$,

$$\mathcal{I}\colon \mathbb{A} \times \text{Time} \times \text{Space} \to \mathbb{D}. \tag{1}$$

The value of A for a specific interpretation $\mathcal{I}$ at time t, and location (x, y), is denoted by $\mathcal{I}(A)(t, x, y)$ or alternatively $\mathcal{I}_A(t, x, y)$. In relation (1), Time denotes the time domain which is a non-negative real number in $\mathbb{R}_{\geq 0}$, and Space denotes space domain as a tuple of two real numbers that are a subset of $\mathbb{R}^2$. For this a Geodetic system can be used such as WGS 84 that is being used in Global Positioning System (GPS) equipment [19].

In general, $\mathcal{I}_A(t, x, y) \in \mathcal{D}(A)$, and by considering the example, the interpretation of attributes in statements (s_1), (s_2), and (s_3) are respectively represented as

$$\mathcal{I}_{A_1}(t, x, y) \in \{\text{motorway}, \text{regional}, \text{rural}\}, \tag{2}$$

$$\mathcal{I}_{A_2}(t, x, y) \in \{\text{true}, \text{false}\}, \tag{3}$$

$$\mathcal{I}_{A_3}(t, x, y) \in \mathbb{R}. \tag{4}$$

Fig. 2 (b), (c) shows the fact that various interpretations of an attribute exists for a specific time and location. It is worth noting that representing the location (x, y), in space requires a fixed frame of reference. Choosing a frame of reference is arbitrary and there is no preferred one. Fig. 2 shows two frames of reference, one attached to the vehicle and another one attached to the road.

4.2 Statements

Statements are the building blocks of ODD specifications as they describe constraints on attributes. An ODD specification is composed of set of statements $\mathbb{S} = \{S_1, S_2, \ldots, S_n\}$. Each statement $S \in \mathbb{S}$ is defined with the syntax, $\mathcal{A} \bowtie d$, where $\mathcal{A}$ is an attribute symbol, and d belongs to data type $\mathcal{D}(A)$. Also, the $\bowtie$ symbol is one of the binary predicate symbols $\{=, <, >, \leq, \geq\}$, however, all binary predicate symbols might not be relevant for all attribute, or they may need to be defined. For instance, if the binary relation $>$ is not defined for the 'road type' attribute, then $A_1 > \text{motorway}$ has no meaning.

A statement is defined with the following syntax

$$S ::= \mathcal{A} \bowtie d \mid \neg S,$$

therefore, if S is an statement, then is $\neg S$. For instance, the following relations have the syntax of a statement

$$S_1 := \quad \big(A_1 = \text{motorway}\big), \tag{5}$$

$$S_2 := \quad \big(A_2 = \text{false}\big), \tag{6}$$

$$S_3 := \quad \big(A_3 < 60\,\mathrm{km\,h^{-1}}\big). \tag{7}$$

The semantics of a statement depend on the interpretation of its corresponding attribute. The semantics of statement S, denoted by $\mathcal{I}[\![S]\!]$, is a function returning the truth value of a statement, given an interpretation $\mathcal{I}_A$, that assigns a value to the corresponding attribute A at certain time and space,

$$\mathcal{I}[\![\,]\!]\colon \mathbb{S} \times \text{Time} \times \text{Space} \to \{\text{true}, \text{false}\}. \tag{8}$$

For statements S_1, S_2, and S_3 defined in relations (5), (6), and, (7), $\mathcal{I}[\![S_1]\!](t, x, y) = \text{true}$ whenever for $t \in \text{Time}$, and, $(x, y) \in \text{Space}$, an interpretation of A_1 is given such that $\mathcal{I}(A_1)(t, x, y) = \textit{motorway}$. In the same way, $\mathcal{I}[\![S_2]\!](t, x, y) = \text{true}$, whenever for a given interpretation, there is no pedestrian present on the road at (t, x, y), i.e., $\mathcal{I}(A_2)(t, x, y) = \text{false}$, and $\mathcal{I}[\![S_3]\!](t, x, y) = \text{true}$, whenever at (t, x, y) the speed of the vehicle is less than $60\,\mathrm{km/h}$.

5. Operational Domain (OD)

The operational domain of a system is fully realized when all its relevant attributes and their respective data types are specified. The process of identifying these relevant attributes is inherently dependent on the level of abstraction and the granularity of modeling details required for the system's operation. For instance, the specificity of attributes can vary widely based on standards and use cases; some standards might consider the 'type of asphalt' on which the vehicle operates as a relevant attribute due to its impact on vehicle handling and safety features. At the same time, others may deem this detail too granular and omit it from consideration.

Numerous standardization committees identified and classified Operational Domain (OD) attributes and their corresponding data types by providing a taxonomy of OD attributes. For instance, ISO 34503 [6] and BSI PAS 1883 [13] offered an OD taxonomy. However, it is important to highlight that they inaccurately named it an ODD taxonomy. The following section aims to remedy this confusion by formally representing an Operational Domain.

For an operational domain that is characterized by a set of attributes $\mathbb{A} = \{A_1, A_2, \ldots, A_n\}$, it can be represented mathematically as a set of tuples over data types,

$$\mathrm{OD} := \mathcal{D}_1 \times \mathcal{D}_2 \times \cdots \times \mathcal{D}_n. \tag{9}$$

For example if A_1 and A_2 are all relevant attributes of a certain system with range of possible values represented in Equations (2) and (3), then OD of such system is represented by

$$\begin{aligned}\mathrm{OD} = \{&(\mathrm{motorway}, \mathrm{true}), (\mathrm{motorway}, \mathrm{false}),\\ &(\mathrm{regional}, \mathrm{true}), (\mathrm{regional}, \mathrm{false}),\\ &(\mathrm{rural}, \mathrm{true}), (\mathrm{rural}, \mathrm{false})\}.\end{aligned}$$

The above example shows an OD defined over attributes with discrete data types. In the same way, OD for attributes with continuous data types can be defined. However, such OD forms an infinite set and an OD description is required to formally specify such an infinite OD.

A vehicle system explores different regions of the OD at various times and locations. In other words, the vehicle's sensors measure distinct values for OD attributes at multiple times and locations. To address this variability, it is useful to introduce a variable named Local Operational Domain (LOD), which is essentially an element of the OD. LOD is a tuple, given by interpretation of all measured attributes $\mathcal{I}_{A_1}, \mathcal{I}_{A_2}, \ldots \mathcal{I}_{A_n}$ at a certain time t and location (x, y):

$$\mathrm{LOD}(t, x, y) := \big(\mathcal{I}_{A_1}, \mathcal{I}_{A_2}, \ldots, \mathcal{I}_{A_n}\big). \tag{10}$$

For example, consider a simplified OD defined over A_1 and A_2. Let us assume that at time t and location (x, y), the type of road is motorway, and no pedestrian exists on the road. Then LOD would be represented as $\mathrm{LOD} = (\mathrm{motorway}, \mathrm{false})$.

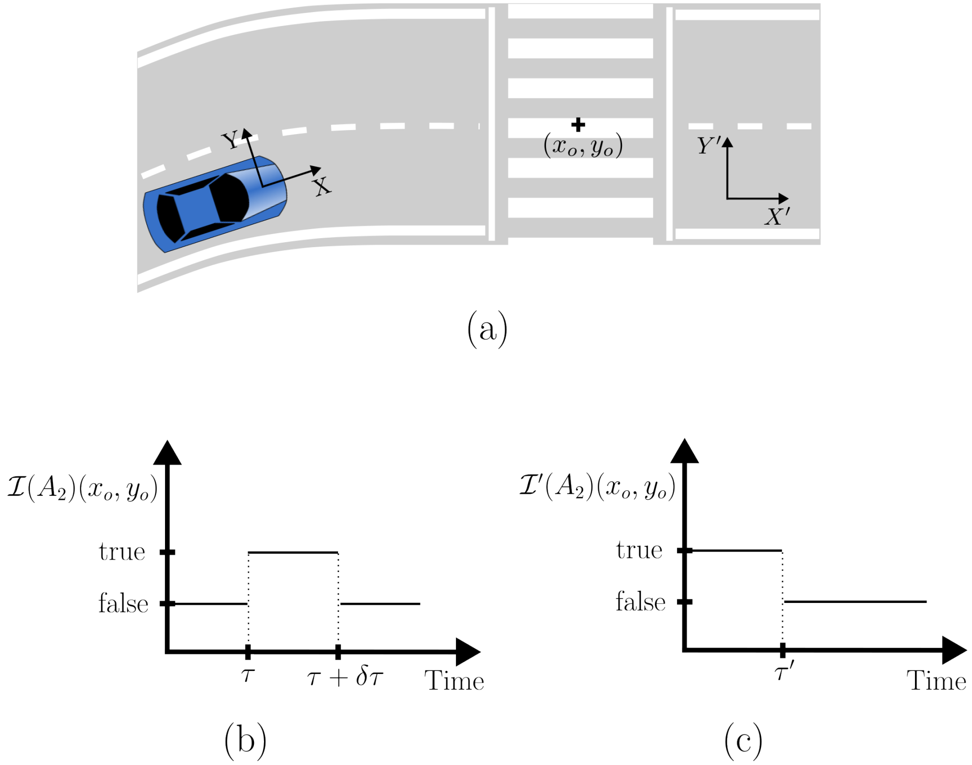

Figure 2. (a) shows a vehicle moving in a segment of a road while facing a pedestrian zone in front. A frame of reference (X, Y) is attached to the vehicle and another frame of reference (X', Y') to the road. (b), (c) show two different interpretation of attribute A_2 representing the presence of a pedestrian at a certain location, labeled with (x_o, y_o) coordinates denoted by a cross at sub-figure (a).

Defining another quantity that is very similar to LOD but has a different meaning is beneficial. This quantity will be used later when introducing the concept of ODD monitoring. The Current Operational Domain (COD) can be defined as

$$\mathrm{COD} := \mathrm{LOD}\ (t_c, x_c, y_c) \tag{11}$$

where t_c is the current time and (x_c, y_c) is the space coordinates at time t_c. The distinction between COD and LOD is that COD indicates the value of OD attributes in the current time and space, while LOD is a variable that can potentially indicate past or future of OD or value of OD at space coordinates that are different from current AV coordinates.

6. Operational Design Domain (ODD)

After understanding essential concepts and mathematical preliminaries, this section is dedicated to the formal representation of ODD. According to Definition 3.1 and Definition 3.2, it is clear that ODD is a subset of OD. However, a specification of ODD, denoted by $\mathrm{Spec.}$ is required according to Definition 3.3 to clearly specify ODD.

The formal specification of ODD denoted by $\mathrm{Spec.}$ is either a single statement (introduced in Section 4) or logical conjunction of multiple statements or specifications defined by the following syntax:

$$\mathrm{Spec.} ::= S \mid \neg\mathrm{Spec.} \mid \mathrm{Spec.}_1 \wedge \mathrm{Spec.}_2. \tag{12}$$

Using the grammar in equation (12), the statements (s_1), (s_2), and (s_3) that are introduced in section 3, can be described by (5), (6), and (7) respectively, to form an ODD specification denoted as $\mathrm{ODD\ Spec.}$:

$$\mathrm{ODD\ Spec.} = S_1 \wedge S_2 \wedge S_3. \tag{13}$$

Before moving forward, it is essential to note that an AV equipped with a set of sensors may only be able to measure some attributes of the OD. For instance, a vehicle might lack detectors for measuring smoke in the air. Additionally, a specific AV design might intentionally ignore certain OD attributes. For example, it may have a sensor setup that remains functional even in the presence of smoke. In the same way, an ODD specification can be ignorant of some OD attributes. In cases where ODD specifications have lower attribute coverage than OD attributes, additional assumptions must be made to prevent confusion when developing ODD specifications for such a system. One basic assumption that is called permissive assumption in the current study is that if the system is ignorant of particular attributes and their values, it implies that the system permits 'all' values for such attributes. For instance, if a permissive ODD specification for a specific system is silent about road types, it implies that the system can operate on all types of roads.

Other more elaborate assumptions could be made to restrict some or all attributes that are not mentioned in the ODD specifications; however, delving deeper into a specification language for ODD is beyond the scope of the current study. The interested reader is referred to the work by Schwalb et al. [5] and Irvine et al. [20] for more details on specification languages for ODD specifications.

The semantic of an ODD specification, denoted by $\mathcal{I}[\![\mathrm{Spec.}]\!]$ is a function that returns the truth value of a certain $\mathrm{Spec.}$, given the $\mathrm{LOD} \in \mathrm{OD}$ at a certain time and space for all relevant attributes:

$$\mathcal{I}[\![\mathrm{Spec.}]\!] \colon \mathrm{OD} \times \mathrm{Time} \times \mathrm{Space} \to \{\mathrm{true}, \mathrm{false}\}. \tag{14}$$

For brevity, $\mathcal{I}[\![\mathrm{Spec.}]\!]\big(\mathrm{LOD}(t,x,y)\big)$ is used to denote the function in Eq. (14).

With the definition of Eq. (14), ODD can be represented as all elements of OD that satisfy ODD specification as follows:

$$\begin{aligned}\mathrm{ODD} = \{&\mathrm{LOD}(t,x,y) \in \mathrm{OD} \mid \\ &\exists\, \mathcal{I}, t, x, y \cdot \mathcal{I}[\![\mathrm{Spec.}]\!](\mathrm{LOD}(t,x,y))\}.\end{aligned} \tag{15}$$

The procedure described above highlights the difficulty of representing ODD for a system without an appropriate definition and formal representation of OD and ODD specification.

7. Discussion

This study emphasizes the significance of formally representing ODD-related terms, particularly the operational domain (OD). As detailed in section 5, a formal representation of ODD becomes feasible only after the mathematical representation of OD is established. This approach has proven essential in providing a clear and well-defined model, which effectively eliminates the ambiguities previously associated with these terms. This section will further explore the implications of our formalization approach, discussing how it helps to define other concepts and enhances the clarity.

Expanding upon the established foundation, it is possible to construct further advanced concepts. One of these concepts that is of great importance in the development and operation phases of AVs is the monitoring of the Operational Design Domain (ODD) or simply ODD monitoring. ODD monitoring is crucial because it ensures the AV operates safely within its specified operational boundaries. Continuous monitoring of the system is essential to prevent system failures or safety breaches. This means that the system must be monitored continuously to ensure that it is functioning within the ODD. Consequently, ODD Monitoring can be defined as follows:

Definition 7.1 (ODD monitoring)**.** ODD monitoring refers to the process of ensuring whether the current operational domain (COD) measured by an AV's sensors satisfies the ODD Specification defined for that specific AV.

The relation (14) states that if $\mathcal{I}[\![\mathrm{Spec.}]\!](\mathrm{COD}) = \mathrm{true}$, for a specific AV system, it implies that the system's current operational domain (COD) is within the boundaries defined with ODD specification. Alternatively, according to relation (15), it is possible to show that

$$\mathrm{COD} \in \mathrm{ODD} \iff \mathcal{I}[\![\mathrm{Spec.}]\!](\mathrm{COD}) = \mathrm{true}.$$

In other words, ODD monitoring involves evaluating the truth value of ODD specifications in the current time and location.

The formalization approach presented here has other practical implications. This work illustrates how ODD specifications can be effectively related to OD attributes. Although the goal of current work was not to formulate a comprehensive ODD specification, it proposed a straightforward grammar of statements and ODD specifications. Additionally, it successfully demonstrated how these specifications can be evaluated with OD elements, as shown in Eq. (14).

This study intentionally used a simplified approach to explain the importance of formal methods in safeguarding automated vehicles. However, this approach has limitations, and further investigation and extension are needed.

Firstly, more detailed statements and specifications can be added while maintaining the same formal approach. For instance, conditional or time-dependent statements can be introduced specifically tailored to address various real-world scenarios automated vehicles might encounter.

Second, the measurement of the operational domain and current operational domain (COD) demands a thorough investigation due to the numerous unanswered questions concerning measurement techniques, which remain largely unstandardized. For instance, the method for accurately measuring the position of an object on the road is crucial and requires detailed consideration. Should such objects be regarded merely as points, or is it more practical to consider an effective radius that better reflects their physical presence? Such methods shall address the measurement error and provide ways to safeguard AV operations against these measurement errors.

Finally, building upon the current formalization framework, it is possible to define additional concepts, such as degraded functionalities and restricted ODD regions. By identifying specific subsets of the ODD that apply to degraded operation modes, as suggested in the literature [7], we can tailor the system's responses to various levels of functionality impairment. Exploring these ideas in future research requires the formalization approach presented in this paper.

8. Conclusion

This initial study has provided a basis for understanding the term OD and its importance in clarifying related terms such as ODD and ODD specification. By introducing precise definitions and a structured approach, we have addressed the ambiguities that previously clouded these critical terms, enhancing the clarity crucial in developing automated vehicle systems. In this regard, this work introduced a preliminary formal representation of OD and ODD and explained these notions using several examples. In addition, the current study demonstrated the procedure for creating a primary ODD specification by employing basic statements and evaluating it based on the operational domain. In the end, it shows how other concepts, such as ODD monitoring, can be built on top of the current formalization.

Despite the progress made, this study acknowledges the limitations of the current formalization and the need for extensions. In particular, there is a need to create a comprehensive language for ODD specification that addresses technical intricacies, such as the inclusion of conditional statements, which were beyond the scope of this work. Also, the temporal aspects of ODD statements (such as time intervals during which some statement is not fulfilled) need to be explored in future work. Nonetheless, future work will benefit the approach presented here, incorporating more detailed and dynamic specifications and exploring measurement techniques for real-world applications.

9. Acknowledgment

This work received support from the GAIA-X 4 PLC-AAD project, which is funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) under the funding code 19S21006K. The author is grateful to Dr. Bernd Westphal for his insightful and valuable discussions and guidance throughout the research process. Additionally, appreciation is due to Anna Austel, Ishan Saxena, and Dominik Grundt for their critical feedback on earlier drafts of this paper. Their perspectives and critiques were essential in refining the arguments and enhancing the overall quality of the manuscript.

References

[1] "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," SAE International, Standard SAE J3016 202104, April 2021.

[2] P. Koopman, *How Safe is Safe Enough?: Measuring and Predicting Autonomous Vehicle Safety*. Carnegie Mellon University, 2022.

[3] X. Zhang, S. Khastgir, J.-K. Tiele, K. Takenaka, T. Hayakawa, and P. Jennings, "Odd and behavior based scenario generation for automated driving systems," *IEEE Access*, vol. 12, pp. 10 652–10 663, 2024.

[4] K. Czarnecki, "Operational design domain for automated driving systems, taxonomy of basic terms," *Waterloo Intelligent Systems Engineering (WISE) Lab, University of Waterloo, Canada*, 2018.

[5] E. Schwalb, P. Irvine, X. Zhang, S. Khastgir, and P. Jennings, "A two-level abstraction odd definition language: Part ii," in *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2021, pp. 1669–1676.

[6] "Road vehicles — test scenarios for automated driving systems — specification for operational design domain," ISO (International Organization for Standardization), Standard ISO 34503:2023, August 2023.

[7] I. Colwell, B. Phan, S. Saleem, R. Salay, and K. Czarnecki, "An automated vehicle safety concept based on runtime restriction of the operational design domain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 1910–1917.

[8] C. Sun, Z. Deng, W. Chu, S. Li, and D. Cao, "Acclimatizing the operational design domain for autonomous driving systems," *IEEE Intelligent Transportation Systems Magazine*, vol. 14, no. 2, pp. 10–24, 2021.

[9] E.-R. Olderog and H. Dierks, *Real-time systems: formal specification and automatic verification*. Cambridge University Press, 2008.

[10] E. Thorn, S. C. Kimmel, M. Chaka, B. A. Hamilton *et al.*, "A framework for automated driving system testable cases and scenarios," United States. Department of Transportation. National Highway Traffic Safety Administration, Standard DOT HS 812 623, 2018.

[11] M. Gyllenhammar, R. Johansson, F. Warg, D. Chen, H.-M. Heyn, M. Sanfridson, J. Söderberg, A. Thorsén, and S. Ursing, "Towards an operational design domain that supports the safety argumentation of an automated driving system," in *10th European Congress on Embedded Real Time Systems (ERTS 2020)*, 2020.

[12] "AVSC best practice for describing an operational design domain: Conceptual framework and lexicon," Automated Vehicle Safety Consortium (AVSC), Standard AVSC00002202004, April 2020.

[13] "Operational design domain (odd) taxonomy for an automated driving system (ads) – specification," The British Standards Institution (BSI), Standard PAS 1883:2020, August 2020.

[14] C. Neurohr, L. Westhofen, M. Butz, M. H. Bollmann, U. Eberle, and R. Galbas, "Criticality analysis for the verification and validation of automated vehicles," *IEEE Access*, vol. 9, pp. 18 016–18 041, 2021.

[15] L. Westhofen, C. Neurohr, M. Butz, M. Scholtes, and M. Schuldes, "Using ontologies for the formalization and recognition of criticality for automated driving," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 3, pp. 519–538, 2022.

[16] J. Erz, B. Schütt, T. Braun, H. Guissouma, and E. Sax, "Towards an ontology that reconciles the operational design domain, scenario-based testing, and automated vehicle architectures," in *2022 IEEE international systems conference (SYSCON)*. IEEE, 2022, pp. 1–8.

[17] "ASAM OpenODD," Association for Standardization of Automation and Measuring Systems (ASAM), Standard ASAM OpenODD V1.0.0, October 2021.

[18] National Transportation Safety Board. (NTSB), "Automated vehicles - investigations," https://www.ntsb.gov/Advocacy/safety-topics/Pages/automated-vehicles-investigations.aspx, accessed: 11.04.2024.

[19] J. A. Slater and S. Malys, "Wgs 84—past, present and future," in *Advances in Positioning and Reference Frames: IAG Scientific Assembly Rio de Janeiro, Brazil, September 3–9, 1997*. Springer, 1998, pp. 1–7.

[20] P. Irvine, X. Zhang, S. Khastgir, E. Schwalb, and P. Jennings, "A two-level abstraction odd definition language: Part i," in *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2021, pp. 2614–2621.