
Ru Niu
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, China. E-mail: rniu@bjtu.edu.cn

Sifan You
School of Electronics and Information Engineering, Beijing Jiaotong University, China. E-mail: 19120268@bjtu.edu.cn

Shijie Zhang
School of Electronics and Information Engineering, Beijing Jiaotong University, China. E-mail: sjzhang@bjtu.edu.cn

Yige Lei
School of Electronics and Information Engineering, Beijing Jiaotong University, China. E-mail: 18211011@bjtu.edu.cn

In recent years, the research of next-generation railway focuses on enhancing the autonomy of unmanned train with AI techniques to identify, analyze and safely handle uncertain environments and emergencies. Due to the limitation of sensors and machine learning algorithms, it is essential to clearly and completely specify the operation condition under which the train control system is designed to work and ensure trains are always safely operating in this domain. This domain is well-defined as operational design domain (ODD) for autonomous vehicles firstly, but is often limited by the uncontrolled environment and the complicated traffic situation. In the field of urban rail transit, a clear definition can be assured by the closed operating environment and organized operation. Thus, this article gives the definition and structure of the ODD of rail transit to describe the safety constrains and assumptions. The factors that are relevant to the identification of ODD have been described and a framework for defining hazardous scenario of train operation based on ODD semantic is proposed. Further, a case of ODD identification and analysis for the typical scenario in unmanned train control system is used to demonstrate its contribution to safety assurance.

Keywords: Operational Design Domain (ODD), scenario generation, risk defense model, autonomous train, unmanned system.

1. Introduction
With the development of urban rail transit entering its golden age, many emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and robotics have been introduced into the train control system (European Commission 2020). They create new opportunities and benefits for the unmanned system. At present, in the urban rail system, a fully automatic operation system can be applied under the GoA 4 (Grade of Automation 4), which means no driver onboard, but can only operate under strict safety application conditions. Traditional external supervision, emergency treatment, confirmation of physical isolation and so on are manually achieved. With the advance of unmanned systems, these manual works will be further reduced in the near future. Even experience-intensive tasks, such as risk situation awareness and safety decision making traditionally undertaken by humans, will also gradually be handed over to machines. Unlike highly repetitive and rule-based works that have already been automatic, these tasks are highly uncertain and safety-critical at the same time, so artificial intelligent (AI) technology is introduced to enhance the environment perception and decision-making ability of unmanned trains. However, it has to admitted that AI itself has not been fully understood and controlled by human being. The model is hard to explained and the outputs are much less predictable. Moreover, disparate development process, such as dataset specification, highly integrated system architecture, and automatic coding, challenges the widely used process-based safety assessment standards represented by EN5012X. Therefore, in order to validate the safety of AI equipment and supervise the behavior of autonomous train, it is necessary to specify and model the safe constrains and assumption of various train operation scenarios, and then risk situation can be assessed by monitoring the changes and violations of the safe restrictions.

Similar researches are underway in other autonomous transportation fields. Operational Design Domain (ODD), a very popular concept in unmanned vehicles area, is used to describe the expected working environment and functional boundary of the system. ODD was first proposed in the field of autopilot (SAE J3016 2018), which is used to specify the conditions for safe operation of smart cars. Since then, ODD is regarded as an important part and widely used in the design process and online supervision of Autonomous Vehicles (AVs). (Colwell 2018) achieve maximum functionality in the case of system failures through modifying a runtime representation of the ODD based on current system capabilities. In (Koopman et al. 2019), ODD can define all safety operation scenarios, specify all restrict operations in unsafe situations. Ensuring that all aspects of the ODD have been addressed either by ensuring safe system operation or by ensuring that the system can recognize and mitigate an excursion beyond the defined ODD could ensure the functions of AI are complete. (Farah...
et al. 2020) developed ODD assessment method for the vehicles with the lane-keeping system, in order to address the problem that the operator's ability and actions perceived by designers do not match the real situation. In the field of railway, (Meng et al. 2021) proposed an ODD structure of ATO (Automatic Train Operation) system for the high-speed railway to describe its normal working condition. However, as the ATO runs under the protection of ATP (Automatic Train Protection), this study didn’t consider safety application restrictions and safety responsibility of each objects, and can only be used to describe the normal operation process of the ATO.

In this paper, we define the ODD of urban train operation control system from the perspective of risk control. A new ODD structure is proposed to describe the supervision and enforcement mechanism of safety constrains, and the preconditions for this mechanism to be effective. The rest of this paper is organized as follows. Discussion of existing ODD definition and structure is presented in Section 2. ODD structure and the scenario description framework are proposed in Section 3. A case study of the process of entering and leaving a station are presented in Section 2. ODD structure and the scenario description framework are proposed in Section 3. A case study of the process of entering and leaving a station are described in section 4. The conclusion is in Section 5.

2. Background

2.1. The definition of ODD

The concept of ODD is derived from the field of AVs. Technology companies and automotive manufacturers often use the idea of ODD to indicate where, when, and how their AV can operate safely. (Lee 2020)

The term defines all conceivable overlapping conditions, use cases, restrictions, and scenarios that an AV might encounter, even the most esoteric edge cases, (Berman 2019). In (SAE J3016 2018), ODD is defined as “Operating conditions (OCs) 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”. (Shuo et al. 2020) considered that an ODD is defined by where (such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an AV is designed to operate. All of these definitions essentially provide static parameters and a feasible set of dynamic parameters for AV.

2.2. The structure of ODD

The definition of an ODD only clarifies the objective and general scope of this definition. Different developers would design different structures and constitutions based on their specific target. (Hillen et al. 2020) proposed a comprehensive conclusion of ODD structure. In his structure, the ODD is divided into three main layers. They are feature situation space, critical situation, and restrict operation respectively. In addition, (Czarnecki 2018) divides the structure of ODD into operational world models and the terms of driving scenarios and their attributes. He explained twelve terms in detail in his work. (Imai 2019) summarized the composition of the conditions of use by the Ministry of Land, Infrastructure, Transport, and Tourism. The constituents of ODD are driving environment conditions which include road conditions, geographic conditions, natural environmental conditions, and other conditions.

2.3. The applicability of ODD in railways

In road traffic, ODD is introduced to all situations, where the AV with different SAE (Society of Automotive Engineers) levels can operate safely. This is because, in ISO 26262 and ISO 21448, there is a lack of description for safety conditions for vehicles in different SAE levels. While in railway, as the operators and equipment suppliers have been considered to be the preliminary risk owner, a relatively complete risk defense mechanism has already been established through hundreds of years of evolution. In the past system upgrades, whether it is speed improvement or automation level improvement, certified protection function and degrade mode of signaling system need to be determined firstly. However, because the railway system has strong customization characteristics, it is necessary to determine the safety constraints and operating assumptions of the risk defense system according to the design parameters and service requirements of the specific line. Therefore, the contents of railway ODD should focus on the description of safety constrains and assumptions, although it is also used to delineate the safe boundary similar to road traffic.

Unlike road traffic in which each vehicle has independent sensing and control functions, railway is an kind of organized transport. Especially for the subway, every vehicle runs in accordance with the predetermined plan again and again, and performs the same operation task in the same position several times a day. Therefore, the task scenarios are limited and predetermined. Moreover, railways are designed with an active protection system, the signaling system. The trackside center is responsible for sensing the transit area of the network and calculation the safe distance to go for each train, and the onboard equipment only limits the speed of the train along the rails based on trackside orders and infrastructure constrains. In this way, the uncertainty brought by moving obstacles on the line (mainly other trains) to operation safety is reduced to a minimum. Therefore, the dynamic characteristics of other trains are not as important as those of road traffic in existing railway systems and the operation scenarios are also limited. It is possible to define ODD model for each operating scenario to specify the action of train operation system.

3. Methods

3.1. The definition of railway ODD

ODD is used to describe the enforcement process of safety constrains (SCs) and its preconditions which is often referred to as operation assumption (OA) in development projects. For railway, this enforcement process is performed by the prerequisite equipment and facilities for train running and the active safety protection system (signaling) to avoid collisions between moving trains and hold main operation.
constrains. Thus, we specify SC as the functional and timeliness requirements for actions of signaling equipment to prevent the train from hazardous situation. For example, onboard signaling should give out emergency brake order when the speed of a train closes to the line speed limit. And, OA is defined as the prerequisites to ensure that the related SCs can deduce the safety of train running. In other words, OA contains the basic conditions provided by equipment and facilities outside signaling boundary for safe operation, such as regularity of track, availability of locomotive, isolation of track zone. Thus, the ODD can clearly express the expected operating condition in the identified scenario.

The process of inferring the ODD structure step by step is shown in Fig.1. From the perspective of train operation safety assurance, there are SCs and OA, which are the manifestation of ODD at the top level. From the perspective of railway risk defense, ODD is formed as the expected behavior of a signaling subject in certain context with various assumption conditions, including the assumption on interaction on inner components, the assumption on external risk owners, the assumption on working environment and the assumption on service users (passengers). External risk owner includes all the equipment, facilities, and railway staff who own safety-related functions or responsibilities. From presentation perspective, we concentrate on the presentation of specific railway safety defense mechanisms. Based on ontology theory, four ontologies and their attributes are abstracted, which are Signaling Elements, Requisite Objects, Operational Constrains and Environmental Factors. Signaling behavior and interaction between signaling elements can be described as the safety-related functions, elements state and connections relationship. External risk owners are modeled as Requisite Objects with the attribution of safety-related responsibilities, self-representation and effects of state changes. Environment and user assumption are classified as Environmental Factors. Operational Constrains mainly referred to requirements and orders come from operational management, including permanent and temporal constrains. These constrains are supervised by signaling and staff. As operational constrain is the higher level control actions, we make it a separate class. The context in risk defense layer can be stated by concerned changes in the ODD before and after a certain moment.

The components for ODD framework is shown in Fig.2. As the active protective barrier of train operation, Signaling Category refers to the onboard and trackside signaling devices and interfaces, such as VOBC, ZC, CI, etc. They are originator of risk control behaviors and the connection between these components should be detailed described. The second category is object, which is mainly compose of the risk owners except signaling, including route infrastructure that are related to operation and protection (for example, the track, cable), trackside equipment and facilities, and also operation and maintenance staff. Signaling and object categories describe the whole protection system of railway operation risk. The third is environment, which include weather, environmental factors (ambient temperature and humidity), electromagnetic interference, and vibration, geographic location. The OAs of almost all systems involve these environmental factors, and the changes of environment items may cause OA violation and eventually evolved into huge challenges for operation safety. The last category is operational constraint, including speed limit, operation plan, zone block, etc. Such constrains can be seen as guiding rules or orders at operation level. With above four categories, ODD can show the pre-organized risk control system of railway, and also the resources, preconditions and constrains required for the system to operate safely.

3.2. Scene modelling based on the ODD

The components of an ODD can be considered as a terminological knowledge base. Based on the systematic accident causation theory, these components are combined together to form a scene, as shown in Fig.3. Operational constrains and signaling constitute a hierarchical control system. Operational constrains set temporary and long-term requirements and targets of train running safety for the signaling, and the signaling equipment implement active safety protection actions when necessary. Requisite Objects are modeled as the resources for signaling, which are mainly perform some information detection, low-level control and actor tasks in the train safety protection. Assigning values to the attributes of all objects in Fig.1 is intended to specify their function scopes and connection relationships. For objects and signaling, it is important to monitor whether their functions are realized correctly and timely. Environmental factors are the assumed working condition of the whole system and usually have the predefined value intervals. These preset values need to be ensured by the maintenance staff during operation. The fluctuation of environmental factors could threat the operation of signaling and objects, and these events should be considered as the context of risk control behavior. Therefore, a scene of risk defense mechanism is formed by associating the related
elements in the ODD through assigning values to them at a certain moment.

![Fig. 3. The definition of a scene based on ODD](image)

**3.3. Scenario description based on ODD**

A scenario is a collection of scenes that are functionally related. For railway, the trains often perform a bunch of operation tasks in similar time and space over and over again in accordance with the established plan, so a scenario can also be defined as the process of completing a certain pre-set task, such pull-in, pull-out, exit stabilizing and return to stabilizing etc. Every step of this process can be seen as a scene and described with ODD, as shown in Fig.4. The formation of each scene is driven by the goal of each step to be achieved, selecting elements from the ODD and building them according to the goal. The behaviors of signaling and requisite objects follow the different operational constraints evolved from different scenario goals. One scene switches to another driven by Trigger Events (TEs). TEs and ODD from previous scene can show the context of the defense behavior of the moment.

TEs in fig. 4 could be the initiator of next step, or deviation of ODD components that can lead to a response of risk defense system, e.g. equipment failure and snowy weather. In the first case, all equipment and facilities work as planned, and the assumptions and constraints are the same. These are the most common situations, and called normal scenarios. In the other case, the fail-safe mechanism of the signaling system is activated by the deviation of ODD parts. The risk defense system goes into another predesigned ODD, which is still safe for the train operation. If some OAs change or the state of requisite objects change, the signaling system may enable special functions, such as rain and snow mode or disaster response. If the signaling equipment fails, the system goes into degrade mode and bypass failed elements, so the members of ODD change. In this way, ODD can describe organized scenarios and the handling scenarios of known exception.

Of course, fail-safe doesn’t mean absolute safe. If the ODD change is not detected, or there is some unknown ODD change, or there is a problem in the ODD migration process, the railway system operates out of all the organized and exception handling ODDs. The risk defense is invalidated, the train runs without any protection, and there is a very high probability of accidents. These are what are called hazardous scenarios.

**4. Case study**

In this section, we take the process of train entering and leaving a station of Fully Automatic System (FAO) as an example to illustrate the ODD structure and scenario description. The ODD is recorded with state machine, and scenario can be automatically generated by UPPAAL.

A typical accident in this process is a passenger caught between the train door and the screen door. We show the violation of ODD when this kind of hazard occurs, and UPPAAL results can also deduce the hazardous scenario.

**4.1. ODD structure of the train parking process**

FAO system is the existing unmanned train operation system, consisting of CI (Computerized Interlocking), VOBC (Vital On-board Controller), ZC (Zone Controller) and TIAS (Traffic Integrated Automation System). On the basis of traditional CBTC (Communication Based Train Control), FAO system enhanced remote monitoring and control to achieve the unmanned control in whole operation process, including entering and leaving the stations and depots. In the process of entering and leaving a station, CI and VOBC cooperate to complete the function of signalling. CI is responsible to check the clearance of station area (OA) and communicate with PSD (requisite object). And, VOBC is responsible to control the train speed and train doors accordingly.

The description of ODD components related to this process are listed in Table 1, and the attributes of each element are specified. Based on the ODD details, we regard the execution of each function as a state of the signalling and requisite objects, model the connections among them as the message on the transition, and take the OAs as the transition guards. Therefore, ODD can be transformed into state transition models, shown as Fig 5 a) to d).

**4.2. Normal scenario construction**

The process of entering and leaving station is divided into 4 steps, as shown in Table 2. Step 1: interlock checking and entering the station. If the station area is not occupied and the switches related are in correct position, VOBC will control the vehicle to part inside the designed window (within 0.5 meters before and after the parking point). Step 2: opening doors. After the train stop event occurs, the operation goal changes from parking to open the doors. The VOBC open the train door and CI open the PSD synchronously. Step 3: passengers boarding and landing. In this scene, OA is that the passenger completes the boarding safely. When boarding may not be possible, passengers...
won’t linger around the doors and return to the platform. This scene continues until the end of the countdown timer, which is an operation constrain. Step 4: Closing Doors and departure. In this scene, the goal is to examine whether the door and PSD condition are all closed. OA is CI is fully aware of the situation of the PSD and the door. The process of this operation task is also transferred to a state transition model, shown as Fig 5 e).

Using the simulator of UPPAAL, the sequence chart of the process of entering and leaving a station can be generated from the ODD automata above, as shown in Fig. 6. As no exception are considered, this model shows the normal scenario of this process.

Table 1. ODD component in train parking scenario

<table>
<thead>
<tr>
<th>ODD categories</th>
<th>VOBC</th>
<th>CI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety-related function</td>
<td>Offer inbound control command; control doors open; countdown boarding time; control the doors close; control train depart.</td>
<td>Check infrastructure and station environment initial condition.</td>
</tr>
<tr>
<td>Connection</td>
<td>Receive initial condition from CI; send train departure condition check command to CI.</td>
<td>Send initial condition to VOBC; receive train departure condition check command from VOBC.</td>
</tr>
<tr>
<td>State</td>
<td>Operate in interval; receive CI message; extend MA into station; send door open command; sync PSD open command; count down start; count down; count down end; depart</td>
<td>Check station initial condition; send condition message; send door and PSD state</td>
</tr>
</tbody>
</table>

Table 2 The process of entering and leaving station

<table>
<thead>
<tr>
<th>Process</th>
<th>TE ID</th>
<th>TE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step1</td>
<td>Interlock checking</td>
<td>Train_stops</td>
</tr>
<tr>
<td>Step2</td>
<td>Opening doors</td>
<td>Countdown_starts</td>
</tr>
<tr>
<td>Step3</td>
<td>Passengers boarding and landing</td>
<td>Countdown_ends</td>
</tr>
<tr>
<td>Step4</td>
<td>Closing Doors and departure</td>
<td>Train_depands</td>
</tr>
</tbody>
</table>

Table 2 a). PSD automata

Fig. 5 b). Vehicle automata
4.3. Hazardous scenario analysis

When the OAs or SCs are violated, hazardous scenarios will happen. A typical accident in this process is a passenger caught between the train door and the screen door. From the view of ODD, this accident relates to two OAs. The first is the passenger OA, which assumes passengers will safely board or stay on the platform and never rush up and down when boarding. The second is on-board passenger OA, which assumes passenger inside the train will press the emergency brake button when see someone caught between the door and the PSD. If we delete these two guard from the automata of VOBC, the sequence chart will lead to the injury, as shown in Fig. 7.

5. Conclusion

In this paper, according to the characteristics of rail transit, we define the railway ODD as the expected operating conditions for the safe operation of trains, which is comprised of safety constraints and the operating assumptions. We propose an ODD structure for the autonomous train to clarify the operation scenarios. In presentation perspective, the key is building the relation among operation constraints, signalling elements, requisite objects and environment. We also proposed a framework of scenario generation by scenes driven by external events. Each scene can be described by assigning attributes to the ODD model. The case study of the train parking process is shown as an example for scenario description.

From the result, it can be seen that the ODD scenario description method proposed can effectively complete the description of the station parking scenario. An analysis of a passenger injury incident shows the necessity of using an ODD to define a scenario. By defining the expected conditions and assumption in the ODD, we can intuitively find the reason for the SC violation. It can be seen that the introduction of the ODD concept in the railway is of great significance to the daily maintenance and operation work of autonomous trains. It can also help to find the weak point of the design of autonomous train control systems.
Fig. 6. Train safety inbound and outbound scenario
Acknowledgement
Supported by National Natural Science Foundation of China (U1934219), Beijing Natural Science Foundation (L181006), Beijing Laboratory of Urban Rail Transit and College Students’ Innovative Entrepreneurial Training Plan.

References


Berman, B. (2019). The key to autonomous vehicle safety is ODD. SAE International.


Road vehicles—safety of the intended functionality. ISO. ISO/CD 21448.