Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P461-cd

New definition and specification of Operational Design Condition for autonomous railway system

Rim LOUHICHI

IRT Railenium, 180 rue Joseph-Louis Lagrange, F-59300 Famars, France. E-mail: rim.louhichi@railenium.eu

Insaf SASSI

IRT Railenium, 180 rue Joseph-Louis Lagrange, F-59300 Famars, France. E-mail: insaf.sassi@railenium.eu

Railway market is undergoing a major change with the incoming of driving automated systems and autonomous trains in open environment. Due to the strict railway regulations and the complexity of rail technology, defining and specifying the operational design domain that describes the environmental conditions within which the autonomous system is designed to operate safely is primordial for establishing a safety demonstration for autonomous trains. In this paper, we describe a methodology for specifying the operational design domain during all the life cycle phases of the railway system as described by the safety norm EN-50126: starting from high-level definition of the operational design domain from the operational context, hazard and risk analysis until the derivation of safety requirements encapsulated by the operational design domain. We tackle, in a second part, a new concept called the operational design condition that encapsulates both the operational design domain and the real time system and human capabilities. Similarly, we explain how the operational design condition can be specified, step by step, in each phase of the railway system life cycle.

Keywords: operational design domain, operational design condition, automation, autonomous systems, safety, risk assessment, railways

1. Introduction

Autonomous driving is widely impacting the transportation sector, mainly the railway sector, due to its expected benefits. In fact, autonomous driving contributes to more safety by eliminating adverse effects of driver inattention or distraction, a significant factor of railway incidents. It contributes to more flexible operations as it reduces dwell time, obstacle detection and obstacle avoidance time. Besides, it leads to reduced overall costs, if well deployed.

However, new challenges have emerged, due to the introduction of automated systems in railway: the complexity of development and integration of automated systems present a considerable challenge. Besides, as automated systems in railway may require to operate for long periods without human intervention, a high level of safety should be proven for system acceptance and market release. The validation tests to prove the safety of a railway system should cover all the relevant Operational Conditions (OCs) in which the automated driving system is designed to operate. That approach to limiting the OCs of the system is known as adopting an Operational Design Domain (ODD) (Koopman and Fratrik (2019); NHTSA (2017)). The ODD can take the form of a taxonomy which is a set of rules or principles applied to classify concepts in a specific knowledge field (Ramírez et al. (2022)). These concepts, generally called attributes in the context of ODD, can be evaluated qualitatively or quantitatively, or can be further split into more detailed attributes. In this paper, we present the ODD as a tool to support safety argumentation of automated systems in railway and we explain why the ODD is not enough to support the safety argumentation and why it is important to include also the human operator/driver's state and system's state as part of OCs. This lead us to tackle the Operational Design Condition (ODC) as a super set of ODD. Besides, we explain how the ODD and ODC are specified in the different phases of the railway system life cycle.

This study will be applied in the case of Draisy, a frugal railway solution aiming at transporting passengers in rural areas and tending towards high levels of automation in the future.

In this paper, we start with presenting in section 2 a background on autonomy in different fields. Section 3 describes our view on how the ODD should be specified in the life cycle of a railway system and section 4 is devoted to detail our view on ODC as a new concept including ODD, human capabilities and system capabilities and how it should be specified. Conclusions and perspectives are given in section 5.

2. Background: Autonomy in different transport fields

Autonomy is a measure to indicate what a system can do without human involvement (Theunissen and Veerman (2018)). Automation is a way to achieve autonomy and most of the existing transport systems nowadays are not autonomous as they do not operate independently; they operate rather on the basis of algorithms and user commands (Sheridan and Parasuraman (2005); SAE (2018)). The willingness to achieve highly automated systems by public and private transport sectors can be explained by the benefits of automation as it allows drivers to focus more on non-driving related activities and reduce the unwanted effort of the driving task Lehtonen et al. (2022).

In automotive industry, Automated Driving Systems (ADS) *"are the hardware and software that are collectively capable of performing the entire Dynamic Driving Task (DDT) on a sustained basis, regardless of whether it is limited to a specific ODD; this term is used specifically to describe a Level 3, 4, or 5 driving automation system"* SAE (2018). The DDT represents all the operational and tactical functions required to operate a vehicle such as lateral and longitudinal control or object detection SAE (2018). In this sense, ODD is defined at design level as the operating environment within which an ADS can perform the DDT safely SAE (2018); NHTSA (2017). When the ADS no longer operates within its predefined ODD or when the ADS witnesses a failure, a fallback action shall be performed. A fallback response must be performed in time in order to either perform the dynamic driving task or achieve a minimal risk (SAE (2018)). In maritime, ship autonomy is defined as *"the combination of automation and the approved absence of operators"* according to (Rødseth et al. (2021)). Because autonomous ships will always use a combination of human and automation control, we do not use the concept of ODD in maritime but rather the concept of Operational Envelope (OE) which is the set of conditions and related operator control modes under which the automated system is designed to operate. In other terms, OE represents the states where human and/or automation can maintain full control of the system while the fallback defines the states where full control is no longer possible (Rødseth et al. (2021)).

Due to the specificity of the railway field (heaviness of regulations, level of required safety), attempts to introduce autonomy in open rail networks remain conservative, contrary to the urban metros, operating in closed environment. These latter have been automated for more than 50 years (Ramírez et al. (2022)). In fact, trains operating in open environment are more likely to face hazards such as obstacle present on the tracks, visibility reduced due to rough environmental conditions, etc...In order to validate the safety of automated trains in open environment, all the relevant OCs should be determined to confine the scope of verification Gyllenhammar et al. (2020). This is why it is important to specify ODD for automated trains in open environment. Recent works have tried to define the ODD in railway. We mention for example the work of Peleska et al. (2022) that introduces four sub-divisions for ODD in railway: autonomous normal operation, autonomous degraded operation, non autonomous control-remote control and non autonomous control-manual control. We mention also the work of Tonk et al. (2021) which presents a methodology for ODD specification for a safe remote control of trains.

Although there are few attempts to define ODD in railway, we think that there is a lack of a structured methodology to specify ODD during all the life cycle phases of the railway system as described in EN-50126 (2017a). We also think that there is a need to define a more global concept than ODD which is able to encapsulate both system in degraded situations and human role in the loop. Therefore, in this paper, we give a proposal for defining and specifying the ODC that has been introduced by Khastgir (2020). According to Khastgir (2020), the ODC should integrate both ODD, system capabilities and human capabilities.

3. Specification of the Operational Design Domain

In this section, we describe how the ODD is constructed in each life cycle phase of the railway system (see Figure 1). The norm EN-50126 as well as the work of (Tonk et al. (2021)) are the main references for conducting our methodology for ODD specification. We also explain the role of ODD mainly in confining the Hazard Analysis and Risk Assessment and supporting the system acceptance (Gyllenhammar et al. (2020).

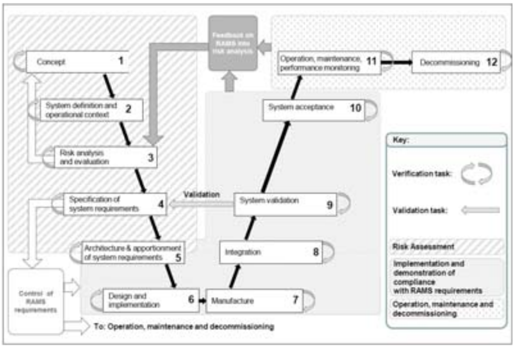
Feedback on RAMS into risk analysis
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
Control of RAMS requirements
To: Operation, maintenance and decommissioning
Key:
Verification task:
Validation task:
Risk Assessment
Implementation and demonstration of compliance with RAMS requirements
Operation, maintenance and decommissioning

Fig. 1. Life cycle of railway system EN-50126 (2017a)

3.1. *Phases 1-2: Concept, system definition and operational context*

From phase 1 to 2, we define the relevant taxonomy for the driving tasks in railway. This will help defining the high level of ODD. This taxonomy for high level ODD definition is largely documented in literature. The attributes relevant to the considered railway system in its operational context can be derived at this stage (see Figure 2).

3.2. *Phase 3: Risk analysis and evaluation*

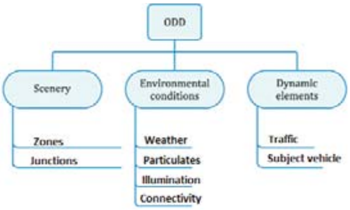

Fig. 2. Example of high level ODD definition (adapted from SAE (2018))

In this stage, we identify hazards at the railway system level. A risk assessment is conducted and is comprised of:

- Risk analysis to identify hazards and related potential losses
- Risk evaluation to derive the safety targets in terms of tolerable hazard rate (THR)

3.2.1. *Case 1: the risk is acceptable*

If the risk analysis identifies cases with risk ”broadly acceptable”, there is no need to specify further requirements for those cases (EN-50126 (2017a)). The safety requirements at system level are derived, which corresponds to phase 4 of the system life cycle. The ODD that encapsulates all the OCs to control the hazard resulting in an acceptable risk is defined.

3.2.2. *Case 2: the risk is not acceptable*

In case the risk analysis concludes that a risk is not ”broadly acceptable”, the risk analysis activity shall be continued by choosing and applying a risk acceptance principle (RAP): use of code of practice, comparison with a similar system as reference and explicit risk estimation. External barriers and mitigations shall be identified in order to reduce the severity or the frequency of the hazard. Then, the THR values are derived to ensure an acceptable risk. If the set of measures are enough to meet the RAP, then safety requirements are derived and the ODD is specified accordingly. If the risk remains unacceptable, a sub-ODD is defined at this level that encapsulates the OCs related to the hazards leading to this risk. A process of hazard control refining is performed leading us directly to the phase 5.

3.3. *Phase 4: Specification of system requirement*

A list of safety requirements at system level with their corresponding ODDs is obtained thanks to phase 3. They are translated into functional and non functional requirements. However, in order to make sure that all the obtained ODDs encapsulate the different OCs guaranteeing an acceptable risk, a bottom-up approach should be performed to validate the system safety requirements against the risk assessment process conducted in phase 3 as described in sub-section 3.2. A hazard analysis starting from the specified ODD and the safety related functions failure modes is performed. If within an ODD, all the identified hazards leads to acceptable risk, then we check if the ODD encapsulates the OCs, else, another ODD should be defined and new safety requirements are derived. If within an ODD, the identified hazard is leading to unacceptable risk, then the ODD becomes a sub-ODD and the hazard undergoes a hazard control refining process.

3.4. *Phase 5: Architecture and apportionment of system requirement*

The hazard control refining process starts in this phase. The system architecture is used in order to derive hazards and allocate safety requirements at the subsystem and component level. Concerning the allocation of quantitative safety requirements, the apportionment of THR is done using several methods such as causal analysis, fault tree analysis, etc as depicted in Figure 3.
A hazard that is quantified by a THR is linked to a specific functional composition defined by the system architecture and therefore apportioned into Tolerable Functional Failure Rate TFFR for the functions taking into account the logic inter dependencies between functions. At the lowest level of the apportionment process, where independence among functions can be proven, a Safety Integrity Level (SIL) can be allocated. This SIL is then applied to the lower levels, and cannot be apportioned. The TFFR is further apportioned resulting in failure rates for components/equipment as shown in Figure 3 (EN-50126 (2017b)).

In this phase, new technical hazards can be arising from the architecture, requirements to control these hazards shall be derived from the new hazards and allocated to the related subsystems and/or components. A hazard identified at subsystem level shall be analyzed to assess the resulted risk leading either to an ODD with safety requirements at the subsystem/interfaces level or to a sub-ODD if the associated risk in unacceptable. In this case, the process of hazard control refining should be iterated. In case the cause is at component level, a mitigation should be defined in order to reduce the failure rate at component level, to satisfy the THR of the top level event (see Figure 3). This can take, for example, the form of function/component redundancy, preventive repair time planning, etc. The system architecture may be modified according to the adopted mitigations and new technical measures and an ODD that encapsulates the OCs is defined. For instance, we need to check if the OCs defined by the ODD at system level are compliant with the OCs of components. For example, if the ODD at system level contains rain and weather conditions, we need to check that components are still able to operate in the same rain and weather conditions with respect to the predefined TFFR.
Finally, all Sub-ODDs relevant to a particular hazard combine together to provide maximum restriction and modify the high level operational context through a feedback loop (Tonk et al. (2021)).

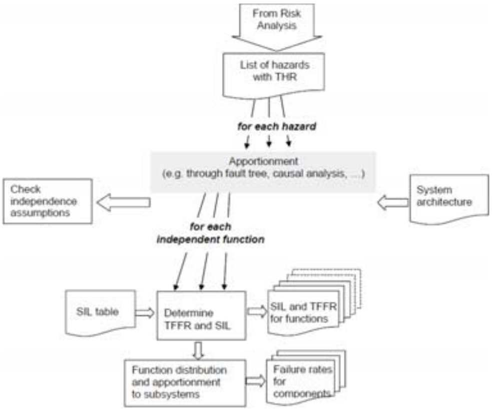
From Risk Analysis
List of hazards with THR
for each hazard
Apportionment (e.g. through fault tree, causal analysis, ...)
Check independence assumptions
System architecture
for each independent function
SIL table
Determine TFFR and SIL
SIL and TFFR for functions
Function distribution and apportionment to subsystems
Failure rates for components

Fig. 3. Apportionment of safety requirement EN-50126 (2017b)

3.5. *Phases 6-9: Design and implementation, manufacture, integration and system validation*

New hazards may emerge during phases 6-9 that can cause potential harm to people, in particular, if the system is new. This can be caused for example by design, manufacture or integration errors due to a lack of knowledge or experience, or mistakes due to inadequate specification. In this case, we need to reiterate the process of hazard analysis and risk evaluation in order to control these additional hazards. This will lead us potentially to define new ODDs. Given an ODD, challenges from phases 6-8 may appear as for example: we may not be able to handle sun blinding the sensor during a certain incidence angle if there is rain on the road (Gyllenhammar et al. (2020)). Besides, the ODD can be deployed to generate test cases for phase 9 with the objective to cover all the possible scenarios. For instance, the ODD gives the OCs where the ADS needs to be tested in real life. This implies to define test scenarios on the basis of these OCs.

3.6. *Phase 10: System acceptance*

In this stage, the ODD serves as a support for safety argumentation, in order to confirm or update the safety case for the system under study.

3.7. *Phase 11: Operation, maintenance and performance monitoring*

During phase 11, we need to have a run-time monitoring of the ODD. Colwell (2018) have introduced the concept of Restricted ODD (ROD), defined as *"the specific conditions under which a giving driving automation system or feature thereof is currently able to function, including, but not limited, to driving modes"*. While the ODD is considered as static during operation, the ROD change depending on the degraded/restricted operation mode of the system. The ROD serves as an input for refining the ODD specification in degraded mode. In fact, new hazards may appear during system operation that lead to ROD violation. These hazards need to be controlled through a feedback loop leading us to the phases 3-4 according to whether the hazard is at the railway system level or at the subsystem and component level.

A recap of the process of ODD specification is given in Figure 4.

4. Specification of the Operational Design Condition

The specification of the ODD, as summarized in Figure 4, does not guarantee the safety of use of the autonomous train. In fact, several safety issues may be encountered while using the system that need to be considered upstream of manufacturing. For example, a potential inability of perceiving the environment by the system or human misunderstanding of the system can lead potentially to harmful hazards, even when operating within its specified ODD. Therefore, there is a need to introduce in railway a concept that is more able to encapsulate both ODD, system capabilities and human capabilities. This concept introduced by Khastgir (2020) is called the ODC. We propose the following definition for the ODC:

"OCs under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited, ***system capabilities and human capabilities****."*

System and human capabilities are specified in the design phase on the basis of predefined scenarios for the purpose of completeness, in the sense that completeness of scenarios is required. The system (respectively human) capabilities refer to the abilities of the system (respectively human) *"to create a sufficiently accurate environment model, make the right decisions, derive the correct control actions based on the environmental model and execute the control actions."* (ISO-21448 (2022)). Even if we think that high level ODC can be defined in early life cycle phase (risk analysis and evaluation), the process of refining system capabilities and human capabilities is mainly performed starting from the phase of design, as the specification and design provide an appropriate understanding of the system, its elements, its functionality and its performance targets (ISO-21448 (2022)).

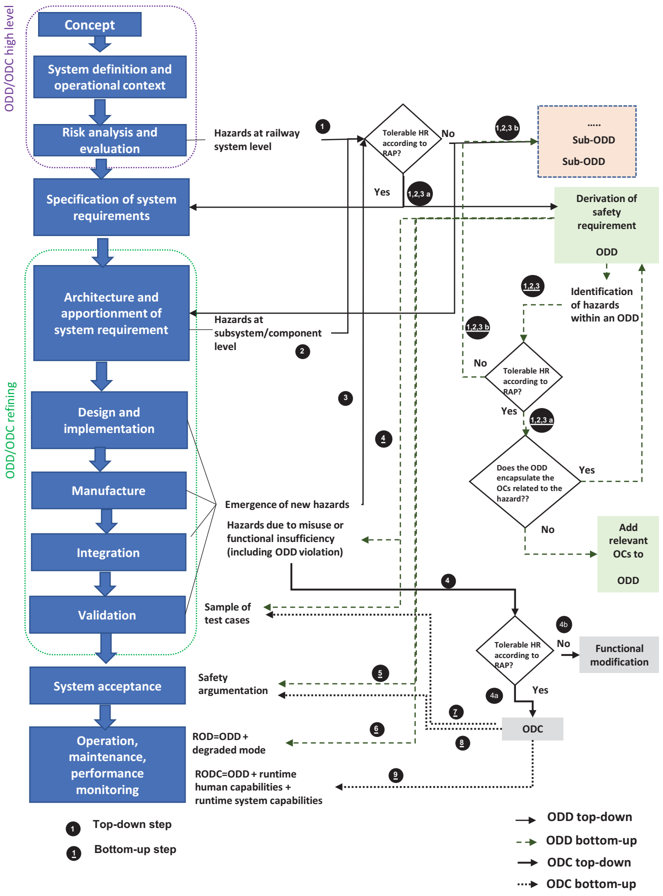
ODD/ODC high level
Concept
System definition and operational context
Risk analysis and evaluation
Specification of system requirements
ODD/ODC refining
Architecture and apportionment of system requirement
Design and implementation
Manufacture
Integration
Validation
System acceptance
Operation, maintenance, performance monitoring
Hazards at railway system level
1
Tolerable HR according to RAP?
No
1,2,3 b
.....
Sub-ODD
Sub-ODD
Yes
1,2,3 a
Derivation of safety requirement
ODD
1,2,3
Identification of hazards within an ODD
1,2,3 b
No
Tolerable HR according to RAP?
Yes
1,2,3 a
Does the ODD encapsulate the OCs related to the hazard??
Yes
No
Add relevant OCs to
ODD
Hazards at subsystem/component level
2
3
4
Emergence of new hazards
Hazards due to misuse or functional insufficiency (including ODD violation)
4
Sample of test cases
4b
Tolerable HR according to RAP?
No
Functional modification
4a
Yes
7
ODC
8
Safety argumentation
5
ROD=ODD + degraded mode
6
RODC=ODD + runtime human capabilities + runtime system capabilities
9
1 Top-down step
1 Bottom-up step
ODD top-down
ODD bottom-up
ODC top-down
ODC bottom-up

Fig. 4. ODD and ODC in the railway system life cycle

4.1. *Phases 6-8: Design and implementation, manufacture and integration*

Specifying the TFFR at functional level as described in section 3.4 is a first layer towards specifying system capabilities within an ODD. Unfortunately, this is not enough as hazards may arise from a misuse of the system or from functional insufficiency as for example: sensors unable to operate correctly due to fog. Within an ODD, hazards arising from misuse or functional insufficiency are derived, as well as hazards arising from ODD violation. We recommend the use of a structured method to derive misuse and functional insufficiency hazards as depicted in Figure 5. If these hazards can lead to severe consequences

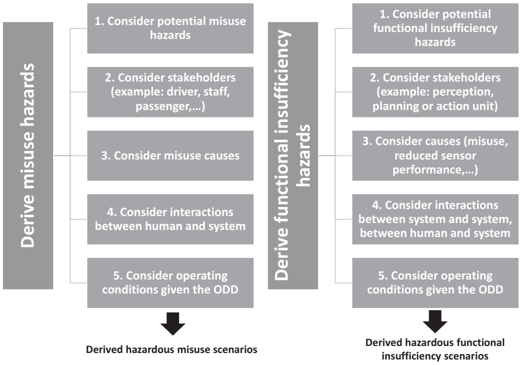
Derive misuse hazards
1. Consider potential misuse hazards
2. Consider stakeholders (example: driver, staff, passenger,...)
3. Consider misuse causes
4. Consider interactions between human and system
5. Consider operating conditions given the ODD
Derived hazardous misuse scenarios
Derive functional insufficiency hazards
1. Consider potential functional insufficiency hazards
2. Consider stakeholders (example: perception, planning or action unit)
3. Consider causes (misuse, reduced sensor performance,...)
4. Consider interactions between system and system, between human and system
5. Consider operating conditions given the ODD
Derived hazardous functional insufficiency scenarios

Fig. 5. Example of structured method for derivation of hazardous misuse and functional insufficiency scenario (adapted from ISO-21448 (2022))

especially when combined with some conditions, then the risks resulted from these hazards should be evaluated and confronted with risk acceptance principle as stated in section 3.2. If the residual risk after introducing mitigation measures is acceptable then, the hazard is deemed to be acceptable and human/system capabilities are derived, otherwise functional modifications should be brought to the system to mitigate the harm. These functional modifications can have impact on system architecture, system design and implementation or even system manufacture and integration. A high level of taxonomy describing human and system capabilities can be simply: recognition, judgment and action. We refer for example to the use of a cognitive model to represent human capabilities such as the IDAC (Information, Decision, and Action) model for human reliability analysis to predict the human response in presence of abnormal OCs Chang and Mosleh (2007).

The attributes describing human and system capabilities can later be dispatched according to this high level taxonomy (See Figure 6)

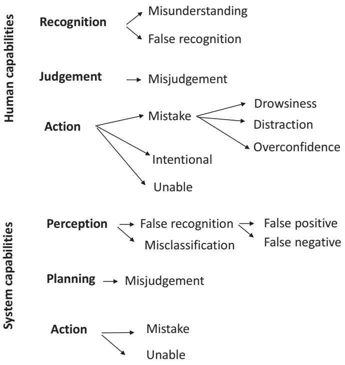

Fig. 6. Example of taxonomy for human capabilities and system capabilities

4.2. *Phase 9: System validation*

The ODC gives several combinations to derive test cases (for simulation, on-field testing,...) by matching ODD with human capabilities and system capabilities and by pushing the tests to the boundaries of system operation (ODD violation, false recognition,...). The objective of the system validation is to ensure that the known hazardous scenarios meet the acceptance criteria and to ensure a maximum coverage of hazardous scenarios. This later can be proved, for example, if the number of encountered unknown hazardous scenarios, for a set of test scenarios, is lower than a predefined target value (ISO-21448 (2022)).

4.3. *Phase 10: System acceptance*

The ODC provides a better support for safety argumentation than ODD, as it takes in consideration system limitations, human errors and how they are both mitigated, to better model the complexity of real world.

4.4. *Phase 11: Operation, maintenance, performance monitoring*

On-board monitoring is necessary to ensure the respect of ODC during operation. Similarly to ROD, Restricted ODC (RODC) can be determined in time on the basis of ROD, instantaneous human and system capabilities. Unknown hazardous scenarios may emerge during operation due for example to regulation evolution, or infrastructure modification or even due to a poor anticipation of system behavior or human behavior. These hazards should be controlled through a feedback process.

We refer to Figure 4 where we recap the whole approach for ODD and ODC specification in the railway system life cycle.

5. Conclusion

Finding the suitable concepts for the deployment of automated/autonomous trains is not an easy exercise due the complexity and the normative constraints. In this paper, we have introduced our vision on what can be an ODD, a concept adapted from the automotive domain for the automated driving systems. A methodology on how we think the ODD should be specified in the different life cycle phases, its role as a support for safety argumentation and risk assessment. However, as we think that ODD is not enough to support safety argumentation, we have tackled a new concept, the ODC that encapsulates the ODD, human capabilities and system capabilities. After defining this concept, we have explained, similarly, how we think the ODC should be specified during the different phases of the system life cycle. Besides, we have tackled the ROD and the RODC, during operation phase, that give a temporal dimension, respectively, to ODD and ODC. Future work will be carried out to deepen the concept of ODC, mainly constructing an appropriate taxonomy to model human and system capabilities, and applying it on a real railway system. Besides, we will give a particular attention to how the ROD is constructed on the basis of instantaneous human and system capabilities.

Acknowledgement

”This research work contributes to the French collaborative project DRAISY. It was funded by the French government within the Program “Investissements d’Avenir” and the framework of France 2030 operated by ADEME. We would like to thank our project’s partners SNCF, Lohr, GCK and Stations-e.”

References

Chang, Y. and A. Mosleh (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 1: Overview of the idac model. *Reliability Engineering & System Safety 92*(8), 997–1013.

Colwell, I. (2018). Runtime restriction of the operational design domain: A safety concept for automated vehicles. Master’s thesis, University of Waterloo.

EN-50126 (2017a). The specification and demonstration of reliability, availability, maintainability and safety (rams) - part 1: Generic rams process. European Norm.

EN-50126 (2017b). The specification and demonstration of reliability, availability, maintainability and safety (rams) - part 2: Generic rams process. European Norm.

Gyllenhammar, M., R. Johansson, F. Warg, D. Chen, H.-M. Heyn, M. Sanfridson, J. Söderberg, A. Thorsén, and S. Ursing (2020). 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)*.

ISO-21448 (2022). Road vehicles-safety of the intended functionality. International Standard.

Khastgir, S. (2020). The curious case of operational design domain: What it is and is not?

Koopman, P. and F. Fratrik (2019). How many operational design domains, objects, and events? *Safeai@ aaai 4*.

Lehtonen, E., F. Malin, T. Louw, Y. M. Lee, T. Itkonen, and S. Innamaa (2022). Why would people want to travel more with automated cars? *Transportation research part F: traffic psychology and behaviour 89*, 143–154.

NHTSA (2017). Automated driving systems 2.0: A vision for safety. *Washington, DC: US Department of Transportation, DOT HS 812*, 442.

Peleska, J., A. E. Haxthausen, and T. Lecomte (2022). Standardisation considerations for autonomous train control. In *Leveraging Applications of Formal Methods, Verification and Validation. Practice: 11th International Symposium, ISoLA 2022, Rhodes, Greece, October 22–30, 2022, Proceedings, Part IV*, pp. 286–307. Springer.

Ramírez, R. C., I. Adin, J. Goya, U. Alvarado, A. Brazalez, and J. Mendizabal (2022). Freight train in the age of self-driving vehicles. a taxonomy review. *IEEE Access 10*, 9750–9762.

Rødseth, Ø. J., H. Nordahl, L. A. L. Wennersberg, B. Myhre, and P. Petersen (2021). Operational design domain for cars versus operational envelope for ships: Handling human capabilities and fallbacks. In *Proceedings of the 31st European Safety and Reliability Conference*.

SAE, O.-R. A. V. S. C. (2018). Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *SAE International: Warrendale, PA, USA*.

Sheridan, T. B. and R. Parasuraman (2005). Human-automation interaction. *Reviews of human factors and ergonomics 1*(1), 89–129.

Theunissen, E. and T. H. Veerman (2018). Automated detect and avoid: Autonomy and ethics. In *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, pp. 2A1–1. IEEE.

Tonk, A., A. Boussif, J. Beugin, and S. Collart-Dutilleul (2021). Towards a specified operational design domain for a safe remote driving of trains. In *Proceedings of the 31st European Safety and Reliability Conference, Angers, France*, pp. 19–23.