Definition And Characterization Of An Electromagnetic Operational Domain Model

Mohammad Tishehzan
Department of Computer Science
University of York
York, United Kingdom
mohammad.tishehzan@york.ac.uk

Mark Nicholson
Department of Computer Science
University of York
York, United Kingdom
mark.nicholson@york.ac.uk

John F. Dawson
School of Physics, Engineering and Technology
University of York
York, United Kingdom
john.dawson@york.ac.uk

***Abstract*—The increasing use of autonomy and complexity of systems has identified the need for explicit specification of operational conditions for systems such that the properties of a system can be assured against these conditions. Although the EE (Electromagnetic Environment) within which a system can safely operate should be considered as part of operational conditions, it has not previously been represented in taxonomies of ODMs (Operational Domain Models). In this paper, the concept of EODM (Electromagnetic Operational Domain Model) is introduced which facilitates the development and safe operation of a system against the safety risks emerging from EMI (Electromagnetic Interference). Furthermore, a process for defining the EODM during development of a system is presented, and an appropriate process for considering EODM's contribution during operation is proposed.**

***Index Terms*—Electromagnetic Environment, Electromagnetic Operational Domain Model, Safety risk, Operational Conditions, Electromagnetic Interference**

I. Introduction

The development of new engineering concepts and the increasing complexity of systems have introduced new safety concerns and intensified some existing ones. One of these safety concerns is rooted in new challenges regarding the interactions and engagement of various electrical, electronic, and programmable electronics in numerous states and configurations. Threats may emerge from these safety concerns in the form of the impact of Electromagnetic Interference (EMI) phenomena on device interactions and hence the observed behavior of a system. Traditionally, functional threats that arise from EMI have been managed by following prescriptive requirements of Electromagnetic Compatibility (EMC) standards. While this EMC approach, known as the rule-based approach, may assure the performance and availability of the system, it is by no means certain that safety assurance can be achieved.

Assurance is a "positive declaration intended to give confidence"; thus, an assurance case is defined as "a reasoned, auditable artefact that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation, its underlying evidence, and explicit assumptions that support the claim(s)" [1].

The disadvantages of the rule-based approach regarding safety include the limited number of tested scenarios, high uncertainty in the effectiveness of mitigation techniques and the lag of EMC standards compared to new technologies and relevant EMI threats [2]. Those limitations necessitate replacing the rule-based approach with more effective risk-based approaches to assure the safety and availability of the system in regard to EMI threats [3]. Applying a risk-based approach alongside increasing EM resilience of the system necessitates considering EMI as a cause of system failure from the earliest phases of the system engineering lifecycle. In other words, it is essential to have a comprehensive procedure to ensure that EMI issues have been considered during each system lifecycle stage to ensure that related safety risks are identified and mitigated to an acceptable degree.

To determine activities that need to be undertaken in each stage of development, an acceptable and adequate understanding of the EE (Electromagnetic Environment) that the system is intended to operate in, is required. Furthermore, to achieve safety assurance, knowledge of the capabilities of the system in regard to maintaining safe operation while the system is exposed to EMI threats is required. Therefore, the operational conditions in which the safe operation of the system is to be assured should be identified.

To capture the operational scope of a system in which safe operation can be demonstrated, the concept of an Operational Domain Model (ODM) has been defined [4]. An ODM is defined to facilitate the elicitation of system safety requirements as part of system development by providing assumptions about the capabilities of the system in the foreseeable environment in which the system is supposed to operate in. In the automotive industry, the concept of the Operational Design Domain (ODD) represents the ODM concept. It is defined by the Society of Automotive Engineers (SAE) 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-

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 812790 (MSCA-ETN PETER). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

979-8-3503-2400-6/23/$31.00 ©2023 IEEE

day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics" [5].

The definitions of ODM and ODD imply that any environmental condition that could impact the safe operation of the system should be considered. Therefore, the operational condition with regard to the EE should be addressed. This requires a process for the definition and characterisation of the ODM in order to be used as an artefact in the development process and during operation. To the best knowledge of the authors, no process for defining and characterising the EE as part of operational conditions has been reported.

In this paper, an approach for defining and specifying the EE as operational conditions is introduced. The Electromagnetic Operational Domain Model (EODM) models the EE in which the safe operation of the system is assured and includes all EE conditions under which the system can operate safely. It is essential to identify the boundary of EODM as this determines the permitted conditions and modes of operation of the system and consequently impacts a system's design and operational requirements. Moreover, it establishes the scope of the assurance case that should be maintained during operation. Using the concept of EODM facilitates the employment of risk-based EMC techniques and measures during the development of the system and enables the monitoring of the system and maintaining safety assurance during operation.

An EODM enables developers to define appropriate EM safety requirements and consequently demonstrate the assurance of safety by complying with those requirements. Although there is no unique framework to develop an EMI-aware assurance case, the main principles that should be followed are introduced in [6]. These principles have been defined as follows:

- **Principle 1**: EM Safety risk requirements shall be defined to address the contribution of EMDs to system hazards.
- **Principle 2:** The intent of the EM safety risk requirements shall be maintained throughout requirements decomposition.
- **Principle 3:** EM safety risk requirements shall be satisfied.
- **Principle 4:** Emergent hazardous behavior of the system due to EMDs shall be identified and mitigated.
- **Principle 4+1:** The confidence established in addressing the EM safety risk principles shall be commensurate to the contribution of the EMD to the system safety risk.

In [7] these principles are presented using the Goal Structuring Notation (GSN), a conventional graphical method for argumentation. In [7] determining the operational conditions with respect to the EE is considered as a necessary contextual information to define appropriate EM safety requirements.

In Section II of this paper, the background to the specification of the EM environment as part of the operational condition is provided and discussed. In Section III, the concept of EODM and its development is discussed, and in Section IV, the impact of EODM on operation is explained.

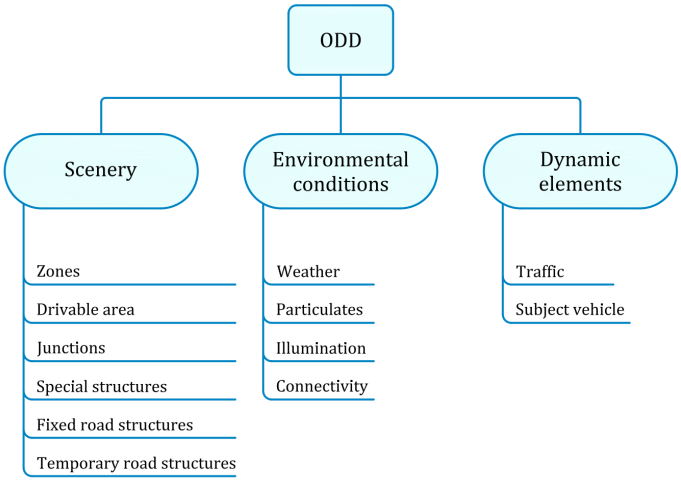

Fig. 1. ODD Taxonomy described in [8]

II. Specification of EE as Operational Condition

The safe operation and assurance of a system are dependent on the accurate identification of the boundaries of its safe operational conditions. In the autonomous vehicle industry, these boundaries are identified by ODD and include the physical scenery, environmental conditions and dynamic elements in the surrounding area of the system according to the taxonomy introduced in [8] (see Fig. 1). None of the proposed ODD taxonomies has addressed an EE. In [8], the need to consider the impact of EMI on the connectivity attribute of the system is identified, but it does not provide any approach to characterize EE as an attribute of the operational conditions of the system.

Therefore, the question is what is the current understanding of electromagnetic operational conditions which is applied in the development and certification processes of a system and addresses the assurance of it in regard to reliability, safety, etc.

Demonstration of compliance with current EMC standards by passing the prescribed tests provides an implicit interpretation of the assumed operational conditions in which the system is designed to operate. In other words, one can say that the operational conditions of the system with regard to EE are equivalent to the set of scenarios and their corresponding test attributes, which the system has successfully gone through (see Fig. 2). These attributes comprise all of the test specifications, such as frequency, amplitude, modulation, etc. The implicit aspect of this interpretation lies in the fact that designers often do not provide information on appropriate conditions of EE, and consumers can only infer the conditions addressed based on the demonstrated compliance with EMC standards.

Since the boundaries of current EMC test levels are mainly determined by the description of the EE, provided in IEC TR 61000-2-5 [9], the boundaries of the implicit interpretation of operational conditions eventually are defined by test limits and ranges determined by [9] methodology. In [9] the EE is classified into a limited number of defined environments based on potential sources that might exist in those environments (e.g. industrial, domestic, etc.).

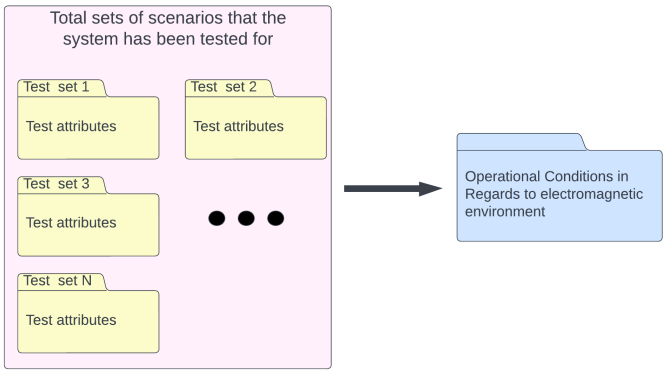

Fig. 2. Implicit Interpretation of Operational Conditions in regards to EE

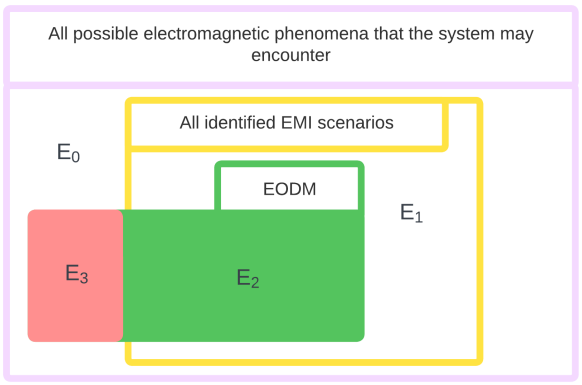

Fig. 3. Conceptual Diagram of EODM

Although this methodology might provide a rough estimation of existing electromagnetic disturbance levels in the environment, the provided information is not adequate for assuring the safe operation of the system against EMI. For instance, the rise of EMI events with potential safety hazard consequences in medical devices [10] shows that the test limits and levels of EMC standards do not represent actual clinical EE [11] and consequently complying with them is not adequate to be employed as the sole argument for safety assurance against EMI.

To determine the assured operational conditions of the system, performing adequate risk analysis on the EM resilience capabilities of the system is required. The current implicit approach lacks this information and only considers the EE to define operational conditions. Furthermore, the test levels required by EMC standards are often compromised with non-technical aspects such as economic considerations and the required rigour for assuring safety is not reflected in determining test levels. In other words, there is no proportionality of testing effort relative to the contribution of EE to safety risk.

Apart from that, variations in the EE during the system's lifecycle due to the introduction of new sources and the aging of existing devices indicate that the operational conditions of the system are changeable. Therefore, an approach which detects changes in the environment and carries out appropriate measures to update the defined operational condition of the system is essential.

III. EODM Concept and Development

A. EODM Definition

In this paper, the Electromagnetic Operational Domain Model (EODM) is defined as the "***Model of operating conditions under which a given system or feature thereof is specifically designed to function, with respect to the EE it is exposed to***".

According to this definition, the EODM of a system is based on two contributing factors. First, the EM environment in which the system is designed to operate and second, the degree of assured resilience provided by both the system capabilities and the use of appropriate techniques and measures against EMI.

The main aim of defining the EODM is to determine the boundaries of the EE within which the system will operate safely. In other words, the safe operation of the system outside of the defined EODM boundaries is not assured and the system should not operate when it is exposed to the EE which has not been included in the EODM. Note that the EODM does not present risk-free operational conditions, but it presents the operational conditions in which the safety risk emerging from EMI is acceptable.

A diagram of the EODM concept is illustrated in Fig. 3. It shows different EE domains that we consider. The domain E_0 includes all possible electromagnetic phenomena in the defined scope (for instance, a range of radiated electromagnetic disturbance) that the system may be exposed to. It comprises both foreseeable and unforeseeable phenomena. During the development of the system and by undertaking an appropriate risk assessment, the EMI scenarios to which the system might be exposed to, are identified. Based on this model, the E_1 domain includes all identified EM phenomena that are initiating EMI scenarios. Here, the EMI scenario is defined as a sequence of scenes initiated by a specific EM disturbance phenomenon that might contribute to the emergence of safety hazards. It is noted that the E_1 domain includes phenomena which might or might not contribute to safety hazards. In other words, it includes all foreseeable EM phenomena that have been identified.

The E_2 domain ($E_2 \subset E_1$) comprises EM phenomena identified during risk assessment and the system can be assured to operate while exposed to them (unlike the $E_1 - E_2$ domain which assurance cannot be achieved). On the other hand, the E_3 domain ($E_3 \subset E_0$) includes the EM phenomena that have not been identified and consequently has not been assured satisfactorily. However, in practice, due to deficiencies in environment identification, risk assessment activities, or inadequate argumentation for providing assurance for the system against those EM phenomena, both the E_2 and E_3 domains make up the EODM that are considered as conditions in which safe

operation is possible and an assurance case are made for. So the EODM might be expressed as:

$$\text{EODM} = E_2 + E_3 \tag{1}$$

The ideal situation is where the entire identified EM phenomena are assured and the EODM does not include any unforeseeable EM phenomena that may contribute to a safety risk, where the ideal EODM might be expressed as:

$$\text{EODM}_{\text{Ideal}} = E_1 = E_2 \tag{2}$$

and $E_3 = \varnothing$.

However, in reality, the entire domain of the identified EM phenomena (E_1) cannot be assured and classified as part of EODM. Though the developers should aim to maximize the EODM to cover all identified EM phenomena and minimize the situations which are not identified properly and the system is not assured against them but have been classified as part of the EODM.

Alternatively, the operational environment of the system (EODM) should not be extended beyond the boundary of the E_1 domain, since the EODM can not be assured of safety due to the lack of adequate identification of the environment. Knowing the boundaries of the assured EE is one of the fundamental arguments for safety assurance related to EMI and EMD (Electromagnetic Disturbances). Although this limitation might reduce the availability of the system in certain situations, it reduces the likelihood of emerging hazardous behavior when the system operates outside of the EODM in an unsafe way.

B. Development of EODM

The two factors that affect the limits of EODM are the environment where the system is intended to operate and the capabilities of the system to maintain safe operation in the presence of EMI. These assumptions led us to a process for developing an EODM, which is both top-down and bottom-up.

Fig. 4 illustrates the process of defining EODM in the early stages of system development. The top-down approach starts by identifying the foreseeable EE in which the system is supposed to operate. Another aspect that should be considered in the top-down approach is the impact of system safety requirements. These requirements are often defined in the early stages of development using techniques such as functional hazard analysis of the system based on the system's architecture and functional requirements. These safety requirements determine which equipment and subsystems should be considered in the scope of the EODM definition process. In other words, by analysing these system safety requirements the system or part of the system that requires safety assurance in regard to EMI is identified. By identifying the foreseeable environment and determining the subsystems and components that must work in the EODM, the ideal EODM is defined.

The ideal EODM presents all the operational conditions in an ideal world without considering the susceptibilities of the components. However, in reality, EMI-susceptible components limit the operating conditions of the system. To take this into account, the bottom-up part of the process is defined. The

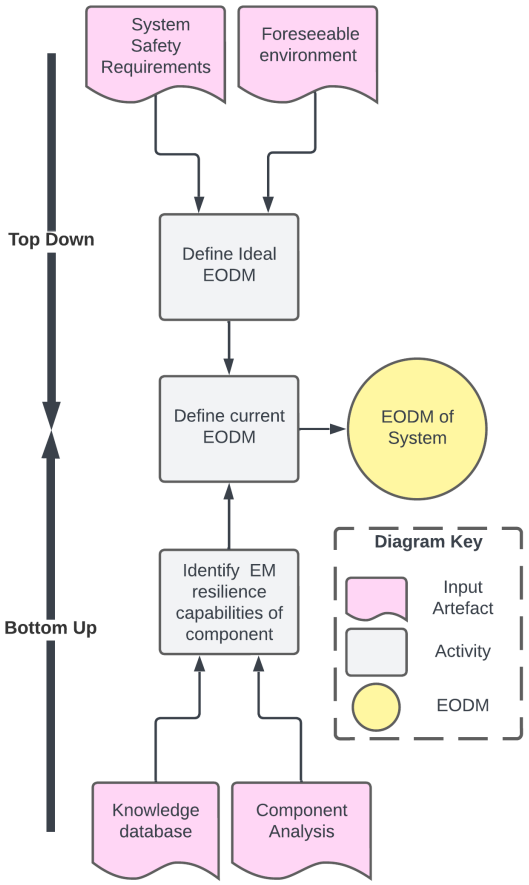

Fig. 4. Defining process of EODM in early stages of system development

component capabilities of the system can be determined by analyzing components and considering the information resulting from previous experiences of the component's behavior when it is exposed to the conditions defined in the ideal EODM.

By taking into account each component's capabilities and identifying the conditions under which the component's operation cannot be assured, some conditions can be omitted from the ideal EODM. The output of the process is the initial EODM of the system or sub-system based on the defined scope of development.

It should be noted that the result of this process is the first version of EODM. Once the first version of EODM is defined, it can be used to define EM safety requirements. Meeting these requirements can ensure safety while the system operates inside the defined EODM. This set of the operational condition can also be assured by appropriate evidence.

The development of EODM is an iterative process. During the development of the system, various techniques and measures may be applied to the system which impact on the capabilities of the system to maintain its safe operation when exposed to certain situations that have not been included in the EODM in earlier phases. For instance, [12] provides a set of techniques and measures for increasing the resilience of the

system against EMI which are derived from techniques and measures defined in [13].

IV. EODM Process in Operation

A key part of the EODM concept is the capability of the system to respond to changes in the EE in order to maintain safety. The environment and the operation of the system should be monitored so that the most appropriate response to environmental changes be considered. In other words, the system should be monitored during operation to make sure the system operates within the operational conditions defined by the EODM. Any violation of EODM may increase the risk of safety violations to an unacceptable level, making the system unsafe to operate. Therefore, designers should define the proper actions to be taken so that the system returns to a safety-assured operational condition.

In reality, there are four states of a system in regard to functionality and EODM. These states are originally driven from ODM states defined in [4] and can be presented as follow:

- State 1: Operating full functionality inside of EODM
- State 2: Operating full functionality outside of EODM
- State 3: Operating a fallback functionality inside of EODM
- State 4: Operating a fallback functionality outside of EODM

According to the concept of EODM, state 1 is the most desirable state since the system operates to its full functionality while its safety is assured. On the other hand, state 2 is the unsafe state of the system and should be avoided. State 3 is where a fallback action is triggered wrongly while the system is still inside of EODM. State 4 represents the scenarios when the system identifies an EODM violation and triggers fallback action. Therefore, a beneficial EODM process should facilitate the transition between states 1 to 4 and back again.

Fig. 5 illustrates the architecture proposed for the EODM process for transition between states 1 and 4 during operation. It is considered that EODMs are defined for the set of subsystems that have safety requirements associated with them. During operation, the subsystems should be monitored to identify any changes in their normal behavior due to EMI (e.g. detection of EMI by an EMI detector). Moreover, the EE should also be monitored. This information can be obtained in various ways. For instance, it can be achieved by the installed sensors which screen the EE or by receiving information from external providers (e.g. receiving data about the existence of certain electromagnetic sources in roads). This information increases the situational awareness of the system in regard to its EE.

Once the appropriate information about the actual EE of the system is provided, this information should be examined against the defined EODM. Therefore, the EODM monitor unit compares the current EE of the system with the EODM to ensure that the system operates within the boundaries of the EODM.

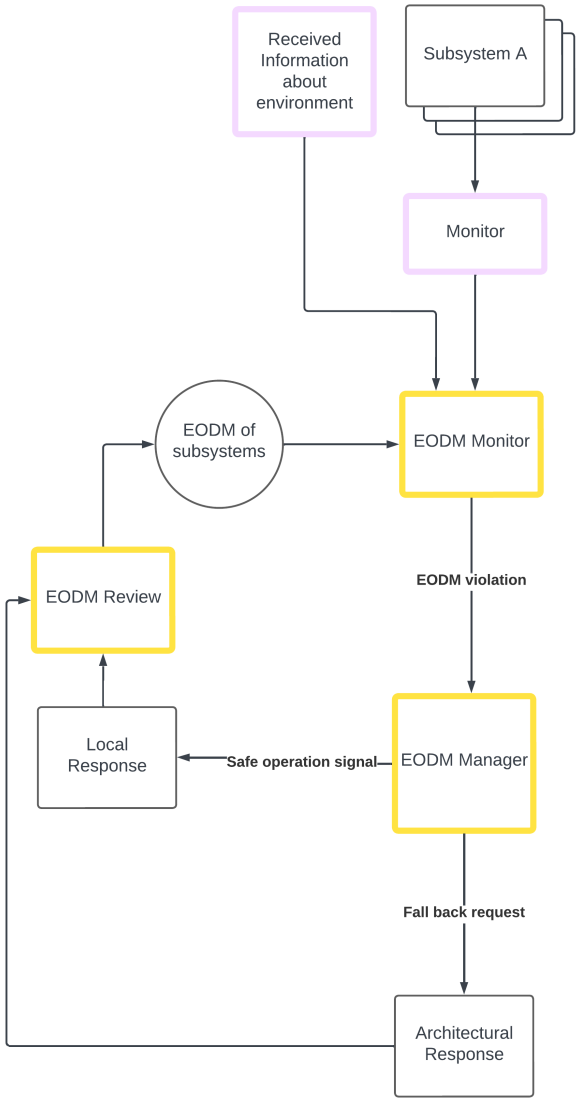

Fig. 5. Proposed Architecture for EODM process in operation

Once the EODM monitor identifies any violation of the EODM, it means that the system is operating in unsafe operating conditions. Therefore, the EODM Manager unit should decide the most appropriate response to the EODM violation. The first approach is the local approach, which is achieved by correcting any changes in the functional behavior of the system or the data it is handling due to exposure to electromagnetic disturbance. An example of this kind of response is Error Detection and Correction Codes [12]. The other approach is to request fallback actions that are considered an architectural response to a violation of EODM (e.g fail-safe). This approach should be taken once the system and the applied techniques and measures for increasing the resilience of the system are not capable of correcting the impact of interference due to the extent of EODM violation. The way the EODM Manager unit decides should be designed during the development of the

system.

Once either of these approaches is followed, an important step of the process is to review the EODM. Any violation of EODM may mean that the current EODM is not defined sufficiently, and there are certain operational conditions which are not assured for their safety risk properties. In other words, there are operational conditions which are not appropriately identified or the capability of the system to withstand the defined operational conditions are not assessed adequately. Moreover, it could be the result of changes in EE due to new sources in the environment or aging of devices in the environment. Therefore, EODM should be placed under formal safety management and a process for ensuring that the deficiencies are addressed should be employed to minimise cumulative risks. Depending on the extent of EODM violation and how the system responded to the violation, the required changes could be a range of actions from slight updates in the EODM to redesign of the system.

V. Conclusion

In this paper, we outline the necessity of defining the operational conditions of the EE in an explicit way in order to enable safety assurance in regard to EMI and EMD. The current state of defining EE is implicit and derived from complying with EMC standards and its shortcomings are discussed. To overcome the stated problems, the concept of EODM is introduced which defines the operational conditions explicitly. The process for defining EODM during the system's development is explained. Furthermore, monitoring the proposed architecture of the EODM process during operation to overcome variations in EE during the lifecycle of the system is discussed and the link to safety management is explored. In the next steps of this research, the contribution of EODM in an EMI-aware safety assurance workflow which has been designed to be integrated into system development processes will be investigated and appropriate case studies will be identified to evaluate the process against them.

References

[1] "IOS/IEC 15026-1: 2019; Systems and Software Engineering - Systems and Software Assurance Part 1: Concepts and vocabulary," 2019.

[2] E. K. Armstrong, "Introduction to EMC for functional safety," 2004, event-place: Newbury, UK.

[3] D. Pissoort, A. Degraeve, and K. Armstrong, "EMI Risk Management: A necessity for safe and reliable electronic systems," in *2015 IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*. IEEE, Sep. 2015, pp. 208–210.

[4] R. Hawkins, M. Osborne, M. Parsons, M. Nicholson, J. McDermid, and I. Habli, "Guidance on the Safety Assurance of Autonomous Systems in Complex Environments (SACE)," Aug. 2022, arXiv:2208.00853 [cs, eess]. [Online]. Available: http://arxiv.org/abs/2208.00853

[5] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International*. Society for Automotive Engineering, 2021. [Online]. Available: https://www.sae.org/standards/content/j3016-202104/

[6] D. Pissoort and M. Nicholson, "The 4+1 Principles for EM Risk Management," in *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, Jul. 2021, pp. 1030–1030.

[7] M. Tishehzan, M. Nicholson, J. F. Dawson, and D. Pissoort, "Providing Assurance that Risks Associated with Electromagnetic Disturbances are Sufficiently Managed," in *2022 International Symposium on Electromagnetic Compatibility – EMC Europe*, Sep. 2022, pp. 163–167, iSSN: 2325-0364.

[8] "PAS 1883: Operational Design Domain (ODD) taxonomy for an Automated Driving System (ADS) – Specification," 2020. [Online]. Available: https://www.bsigroup.com/en-GB/CAV/pas-1883/

[9] "IEC TR 61000-2-5, Electromagnetic compatibility (EMC) - Part 2-5: Environment - Description and classification of electromagnetic environments," 2017.

[10] J. L. Silberberg, "An FDA Perspective on Medical Device EMC and Wireless WED-PM-4," in *2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI PI)*, Jul. 2018, pp. 1–84.

[11] N. Senevirathna, R. Kleihorst, and A. Roc'h, "A Review On Links Between Different EMC Test Environments in Medical Technologies," in *2022 International Symposium on Electromagnetic Compatibility – EMC Europe*, Sep. 2022, pp. 834–839, iSSN: 2325-0364.

[12] "IEEE 1848 - IEEE Standard for Techniques and Measurement to Manage Functional Safety and Other Risks with Regards to Electromagnetic Disturbances," 2021.

[13] "IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems," 2010.