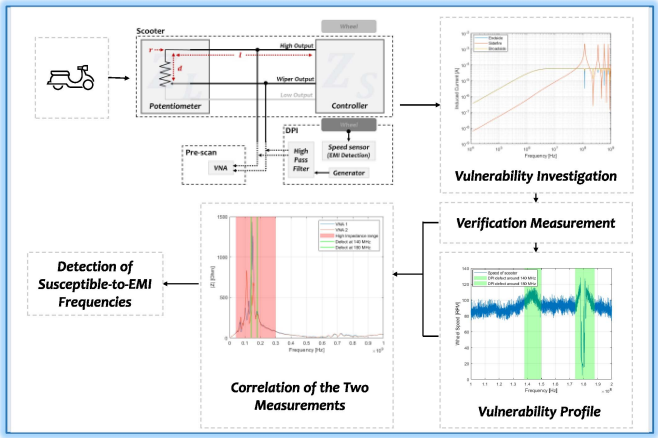
Fast and Curious: Exposure of EMI Vulnerability of an Electric Scooter for a Risk-Based EMC Approach

Vasiliki Gkatsi, *Graduate Student Member, IEEE*, Robert Vogt-Ardatjew, *Member, IEEE*, and Frank Leferink, *Fellow, IEEE*

***Abstract*—Compliance of lone equipment with the electromagnetic compatibility (EMC) standards does not directly result in proper operation when used on the system level, especially in large and complex structures. A more robust way to incorporate possible unwanted behaviors and unpredicted scenarios is to expand the EMC testing by adopting the risk-based EMC approach. This letter addresses an electromagnetic interference (EMI) case caused by a differential mode voltage excitation on a cable harness of an electric scooter focusing on the first step of an EMC assessment procedure, which is the EMI vulnerability investigation. The objective of this research is to detect and expose the vulnerability of a real case study caused by an uncommon cause. This is done by a vector network analyzer measurement and the direct power injection method. The goal of this research is to demonstrate the importance of adopting a risk-based EMC approach while performing EMC testing.**

***Index Terms*—Differential mode voltage (DM), direct power injection (DPI), electric scooter, vector network analyzer (VNA).**



I. Introduction

ELECTROMAGNETIC compatibility (EMC) compliance testing is usually performed in laboratories in accordance with governing standards. These regulations aim to establish proper EMC operation of any electronic component, device, or system in its intended operational environment [1]. Even though such methodologies are used in all types of apparatus, they fall short when it comes to large and complex installations, such as ships [2] and vehicles [3]. Over the last few years, more discussion has taken place regarding incorporating risk management procedures into EMC testing [4] and references on a risk-based EMC approach are already made in the Blue guide [5], Red Guide [6], and Guide for the EMC directive (EMCD) [7]. More specifically, EMCD proposes the application of an EMC assessment, which "is considered to be an adequate analysis and assessment of the risk(s)" [7]. It also proposes that the manufacturer "is fully responsible for applying the appropriate method of assessment," which "shall include an adequate analysis and assessment of the risk(s)" [7]. A risk-based EMC approach has already been applied in the navy as shown in [8], in contrast to the conventional way of rule/standard-based EMC testing. Therefore, so far, risk-based EMC has been proven to be a key tool when it comes to assessing systems in their real intended environment [9] and it proposes methods for exploratory and iterative testing [10].

To understand, evaluate, and foresee the behavior of a complex structure in a real dynamic complex electromagnetic environment (EME), EMC assessment should be applied beforehand as proposed by the EMCD. It can be beneficial in exposing potential susceptible behaviors [11]—that might have not been detected with traditional EMC testing—as it will

Take-Home Messages:

- Even though the individual components of a complex structure might satisfy the respective EMC standards, complete EMC compliance of the system is not necessarily assured.
- Less-common differential mode coupling can be crucial for proper operation of a complex structure and needs to be evaluated too.
- Assessment of the risk(s) is necessary so that unforeseen, dangerous EMI scenarios can be detected and overcome.

Manuscript received 6 March 2023; revised 30 April 2023; accepted 25 May 2023. Date of publication 8 June 2023; date of current version 22 September 2023. This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Sklodowska-Curie Grant under Agreement 812790 (MSCA-ETN PETER). *(Corresponding author: Vasiliki Gkatsi.)*

Vasiliki Gkatsi and Robert Vogt-Ardatjew are with the Department of EEMCS, University of Twente, 7522 NB Enschede, The Netherlands (e-mail: vasso.gkatsi@utwente.nl; r.a.vogtardatjew@utwente.nl).

Frank Leferink is with the Department of EEMCS, University of Twente, 7522 NB Enschede, The Netherlands, and also with Thales Nederland B.V., 7554 RR Hengelo, The Netherlands (e-mail: frank.leferink@utwente.nl).

Digital Object Identifier 10.1109/LEMCPA.2023.3284232

also be shown in this letter. In terms of risk management [12], the first step of an EMC assessment within the risk-based EMC approach is the risk identification. Before identifying the risk(s), though the vulnerability of the equipment under test (EUT) needs to be investigated. As discussed in [13], differential mode voltages (DM) seem to cause a malfunction in the real case of an electric scooter. In this letter, the same case study as in [13] is further investigated by following a series of steps for exposing its vulnerability. Scooters as well as wheelchairs have already been proven to be vulnerable to electromagnetic interference (EMI) as shown in [14]. The applied case here has fulfilled the EMC standards. However, as it will be shown, that does not conclude to complete robustness of the system. In this case, the controller of the scooter is operating based on the received dc voltage from the potentiometer. However, a high-frequency field that might couple on to the wires from an external illuminating field, can be rectified and seen as an input dc voltage at the site of the controller, causing unforeseen operation [13]. Usually, the expected coupling of an external field onto the vulnerable components of a scooter concerns common mode (CM). However, here, the uncommon differential coupling is tested, based on the controller's susceptibility. Since full analytical EMC tests are time consuming and costly, there is a need for a risk-based EMC approach that can narrow down the potential occurring issues. In the context of EMC assessment proposed by the EMCD and risk management as stated in [12], this can be achieved by first investigating the vulnerability of the EUT.

In this letter, a vulnerability investigation on an electric scooter is performed. This investigation can serve as the "first step" in an EMC assessment procedure, which can later be used for identifying, analyzing, evaluating, monitoring, and controlling the risk(s). After a theoretical study based on the transmission line (TL) theory, a quick measurement using a vector network analyzer (VNA) extends the investigation and hypothesis with a practical measurement and hints the potential susceptible-to-EMI frequencies for the applied case study. Afterward, following the setup of the MIL-STD 461C CS02 [15] method for testing the DM coupling directly and controllably, DM voltages are directly injected to the input of the controller of the scooter at the suspicious frequency band(s) obtained from the VNA measurement for improved susceptibility tests. This is called direct power injection (DPI). Based on the vulnerability profile of the scooter, a correlation between the DPI method and the VNA prescan measurement is indicated, validating the vulnerability investigation. It is also proven that the robustness of the system is not ensured, even though the scooter has satisfied the respective EMC standards. Finally, the necessity of incorporating a risk-based EMC approach in EMC testing is shown.

II. Case Study

The EUT investigated in this letter is an electric scooter. Scooters can be easily characterized as complex structures taking into consideration their complicated chassis geometry as well as the interactions between their electronic components. Even though their design, materials, and overall architecture might vary, they usually seem to follow a similar hardware configuration. In the case examined in this letter, there are three main sensitive electronic parts of the EUT that are directly related to the scooter's fundamental functionality—movement of the wheels. These are: a 5-kΩ potentiometer, a long cable harness, and a controller. The potentiometer is an adjustable resistive voltage divider that is directly connected to the steering wheel of the scooter. Due to its variable resistance between its outputs (wiper output to low/high output), it can change the dc voltage levels seen across an unshielded cable harness reaching the controller. The cable harness, in this case, consists of a bundle of wires supplying various functions of the scooter, such as braking, reverse gear, horn, etc. The wires follow a loose configuration, which makes it possible for loops to be created as it is shown also later in this letter.

III. Vulnerability Investigation

Before investigating the vulnerability of the scooter in practice—as it would have been performed by a typical EMC test plan procedure and by following the existing standards—an EMC assessment of the scooter needs to be performed based on simple observations of its structure and general configuration. The case study applied in this letter follows a loose cable configuration over its structure, the controller is placed inside a nonshielded box, and there are no filters protecting the controller from a potentially crucial dc signal component. According to the documentation of the controller, the product has been tested according to ISO 7176-21 [16] concerning EMC compliance, ensuring therefore proper operation of the product. However, as it will be shown later in this letter, EMC compliance is not necessarily confirmed, and the vulnerability investigation can play a significant role in that.

Taking into account the lack of a protective filter at the input of the controller as well as its potential vulnerability to unwanted significant dc voltages caused by an illuminating field, it is of interest to perform a brief vulnerability investigation with some basic rule-of-thumb considerations. Therefore, an investigation of a potential incident plane wave on the scooter—which can cause significant voltage levels—at the site of the controller is performed following TL theory. Modeling procedures of cable harnesses in avionics have also proposed solutions by applying numerical models following the field-to-TL models [17]. Therefore, to address the occurrence of significant levels of voltages across the wires between the potentiometer and the controller of the scooter, the three types of incident field illumination (endfire, sidefire, and broadside) onto the wires are investigated [18]. Both the potentiometer as well as the controller are modeled as resistive loads. The potentiometer is known to be $Z_L = 5$ kΩ and the impedance of the controller is $Z_S = 10$ kΩ, as indicated by the manufacturer. The remaining parameters are set based on the physical dimensions of the scooter. Thus, $l = 1.3$ m, $r = 0.001$ m, and $d = 0.1$ m, where l is the length of the cable harness, r is the radius of the wires, and d is the wire separation distance.

In Fig. 1, the induced voltages at the input of the controller are calculated in MATLAB for the three cases of a

30-V/m incident field. As it can be observed, especially in the case of sidefire illumination above 100 MHz, there are strong voltage peaks, hinting potential vulnerable points. The model here follows an ideal case of perfect geometry. It is important to mention that the real case is different, and deviations are expected from the results. However, the occurrence of voltage peaks in this simplified case already hints about the existence of multiple critical frequency points that require further investigation for possible detection of the scooter vulnerability, as it will be shown in the following sections. Note that this analysis is a pure DM case, which is nearly not covered in standards nor is it considered in basic rule-of-thumb analyses, as these assume CM only.

IV. Measurement Procedure for Detecting Potential Vulnerability

A. Verification Measurement Using a VNA

After performing the vulnerability investigation using the TL theory as explained in Section III, a VNA measurement is performed to create a link to the theoretical study. The aim of this VNA measurement is to describe the behavior of the EUT with respect to the system input impedance and, thus, identify the suspicious frequency points that can cause an unwanted behavior of the scooter, as hinted in the vulnerability investigation. The hypothesis of this measurement is that the significant voltage magnitudes received at the site of the controller can be detected based on the high impedance values measured with the VNA. This information can be later used as described in [19] to correlate the injected power to the external field. The connection between the potentiometer and the controller of the scooter according to the latter documentation is to be seen along with the equipment used for the VNA measurement in Fig. 2. To perform the prescan measurement and address the resonant frequencies and, thus, the significant voltages, a VNA is connected between two cables coming from the potentiometer (wiper out, high out) close to the controller. Then, an S_{11} sweep is performed in the broad frequency range of 1 MHz–1 GHz. The measurement is performed for a set, constant speed of the scooter, related to the potentiometer resistance used in Section III, measured with a speed sensor.

B. Vulnerability Profile of the EUT Using the DPI Method

After detecting the potential vulnerable frequency bands with the VNA measurement, the DPI method is applied for the validation of the vulnerability profile of the scooter by implementing a DM signal directly to the input of the controller. Fig. 2 also shows the measurement setup used to perform the injection measurements emphasizing that the two setups were placed at the same position one after the other. To detect the vulnerability of the scooter, the injection method is applied following the setup of MIL-STD 461C CS02. As can also be seen from Fig. 2, a signal generator along with a high-pass filter are directly connected to the two ends of the potentiometer cable harness (wiper output, high output) of the EUT. The high-pass filter is the same as that used for the CS02 testing procedure. A continuous wave (CW) signal is generated around the

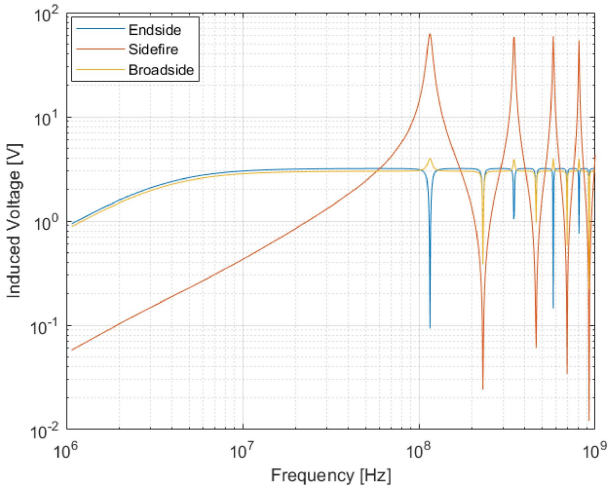


Fig. 1. Induced voltages on the cable harness at the side of the controller for the three incident field orientations based on the TL theory (endside, sidefire, and broadside).

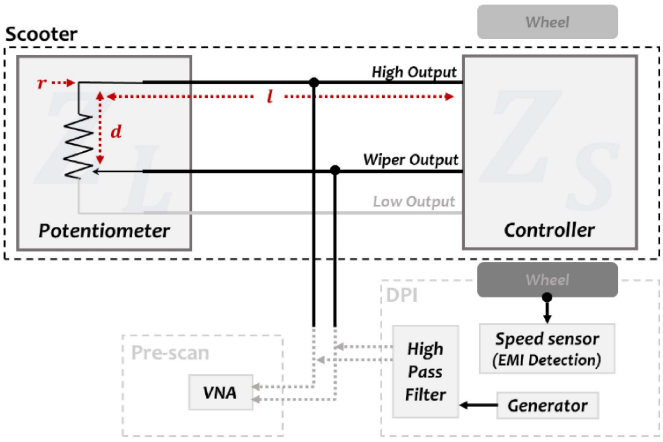


Fig. 2. Schematic of the configuration of the scooter in the two measurement procedures. The prescan measurement using a VNA: Connecting a VNA to two wires between the potentiometer and the controller of the scooter, and the DPI method: Connecting a generator with a high-pass filter at the same position as the VNA measurement. It should be noted that the two measurement procedures are not taken at the same time, but at the same point, a few centimeters from the controller, i.e., as short as possible. First, the prescan measurement using a VNA takes place, and then the DPI method is performed.

frequency bands indicated by the VNA measurement to validate the hypothesis that an EMI issue lies there. The wheel speed was tracked down by a speed sensor placed on one of the wheels counting the revolutions per minute (RPMs).

V. Result and Discussion

Following the measuring procedures as described in Section IV for both the VNA and DPI measurements, both of the results can be seen in Fig. 3. The impedance measured with two different VNAs is depicted along with two cases of EMI caused by applying the DPI method. The two VNAs are from different manufacturers to observe if there is any difference in their response regarding the measured impedance. From the figure, it can be easily noticed that for both VNAs, the highest input impedance values are detected around the frequency range of 50–300 MHz while the scooter is running at that certain speed. Therefore, applying the DPI

method in the frequency range of 50–300 MHz, alterations to the speed of the scooter take place as can be seen in Fig. 4. The power level of the DPI, where a malfunction was detected, was between 22 and 25 dBm from the signal generator. The figure shows the changes of RPMs of the scooter measured with a speed sensor. As it can be observed, a small acceleration and deceleration is detected at around 140 MHz and a more significant change of speed is detected at around 180 MHz, where the scooter is almost stopped. During the measurement campaign, various abnormal behaviors of the scooter speed were detected as, e.g., kicking of the wheel, going in reverse, complete stop, etc.

Combining the results from the two procedures in Fig. 3, it is easily shown that the vulnerability of the scooter occurs indeed in the suspicious frequency band detected with the VNA. By following a step-by-step vulnerability investigation based on the basic TL theory and simple measurements, the vulnerability of the scooter can easily be exposed as demonstrated here. It is proven that even though the components of the EUT have separately satisfied the EMC standards and have been applied to the final product that reached the market, the complete robustness of the system is not ensured, especially when placed in real dynamic complex environments. In the case applied, the product is vulnerable to the usually less-tested DM sources. This behavior is also indicating that exposure to outside fields can be crucial, and the DM components of a plane-wave coupling to the wiring of the scooter can cause a significant voltage at the side of the controller and consecutively change the speed resulting in unforeseen dangerous scenarios. The correlation between the DPI and the field that is coupled to the scooter is to be investigated in a future publication. In this letter, as it is shown from the TL theory, an illuminating field of 30 V/m can cause a significant voltage on the line (Fig. 1), already indicating the need for investigating the field coupling mechanism and the potential vulnerability of the scooter.

Vulnerability investigation applied beforehand, as shown, can hint at such abnormal behaviors. Therefore, assessing the EUT for its lack of proper EMC measures—which might be associated with high risk—before following attentively the EMC standardized procedures, is strongly recommended. Following a risk-based EMC investigation before following strict fixed laboratory requirements can help to avoid potentially unforeseen EMI issues and further make it easier to understand these complex systems and the interactions with their operational environment. Finally, EMC testing can be more robust and reliable covering more eventual scenarios.

VI. Conclusion

The aim of this letter is to demonstrate the importance of adopting a risk-based EMC approach into EMC testing. This is achieved with a vulnerability investigation acting as a "first step" toward EMC assessment, as proposed by the EMCD. The brief investigation performed here assesses a real case and easily exposes its vulnerability with no time-consuming measuring procedures while also setting the field for further research in the implementation of risk management

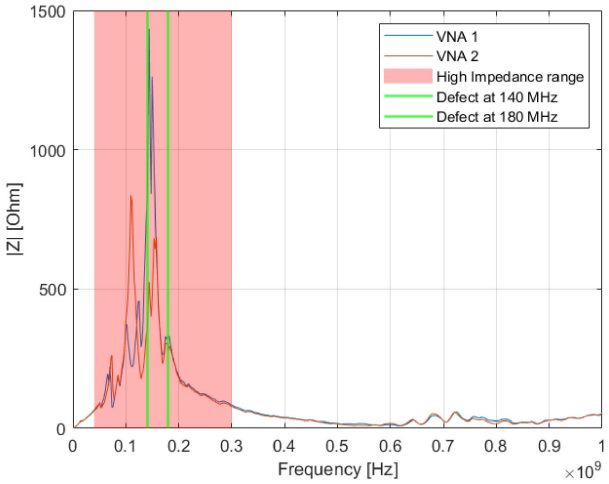


Fig. 3. Input impedance measured a few centimeters, i.e., as short as possible away from the controller of an electrical scooter in the frequency range of 1 MHz–1 GHz.

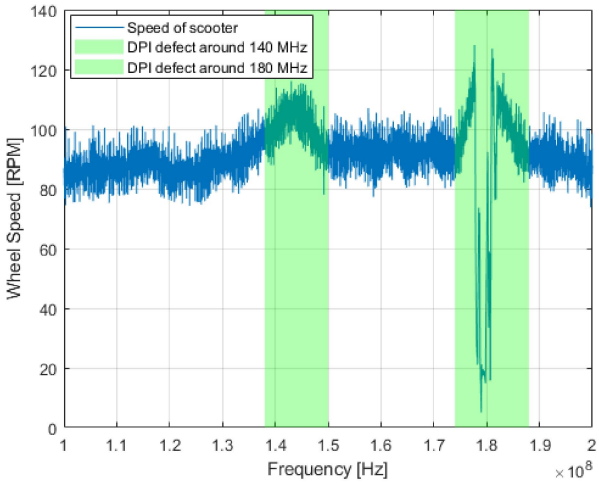


Fig. 4. Speed alteration of the scooter while applying the DPI method. Significant changes are detected at around 140 and 180 MHz.

procedures in the so-far applied EMC standardized techniques. Future work aims at assessing the behavior of the scooter in field illumination inside a semianechoic chamber (SAC) as well as inside a reverberation chamber (RC) and creating a link between the induced values from the DPI method to the field illumination.

Acknowledgment

This publication reflects only the authors' view, exempting the European Union from any liability. Project website: http://etn-peter.eu/.

References

[1] "Directive 2007/46/EC of The European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (framework directive) (text with EEA relevance)," Off. J. Eur. Union, Brussels, Belgium, document 32007L0046, Oct. 2007.

[2] F. Leferink, J.-K. van der Ven, H. Bergsma, and B. van Leersum, "Risk based EMC for complex systems," in *Proc. 33rd General Assembly Sci. Symp. Int. Union Radio Sci. (URSI GASS)*, Montreal, QC, Canada, Aug. 2017, pp. 1–4.

[3] K. Pliakostathis, M. Zanni, G. Trentadue, and H. Scholz, "Assessment of a vehicle's electromagnetic emissions under dynamic drive conditions," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 6, pp. 2411–2422, Dec. 2020.

[4] F. Leferink, "Risk-based vs rule-based electromagnetic compatibility in large installations," in *Proc. IEEE 4th Global Electromagn. Compat. Conf. (GEMCCON)*, Stellenbosch, South Africa, Nov. 2018, pp. 1–4.

[5] "The 'blue guide' on the implementation of EU products rules 2016," Off. J. Eur. Union, Brussels, Belgium, Doc. 2016/C 272/01 Commission Notice, Jul. 2016.

[6] "The RED guide." 2018. [Online]. Available: https://ec.europa.eu/docsroom/documents/29782

[7] "Guide for the EMC directive." 2019. [Online]. Available: https://ec.europa.eu/docsroom/documents/28323

[8] J.-K. van der Ven, B. van Leersum, M. van Rij, and F. Leferink, "Cost-effective electromagnetic compatible installation on ships using a risk based approach," in *Proc. Int. Symp. Electromagn. Compat. (EMC Eur.)*, Angers, France, Sep. 2017, pp. 1–6.

[9] V. Gkatsi, R. Vogt-Ardatjew, and F. Leferink, "On-site automotive environment measurements for a risk-based EMC approach," in *Proc. IEEE Int. Symp. Electromagn. Compat. Signal Power Integrity (EMCSI)*, Spokane, WA, USA, Aug. 2022, pp. 443–448.

[10] P. T. Jensen, "Using EMC HALT for risk-and fault assessment: Using accelerated EMC tests for unveiling and identification of failure mechanisms in electronics provides a useful tool for risk assessment," in *Proc. Int. Symp. Electromagn. Compat.*, Brugge, Belgium, Sep. 2013, pp. 6–9.

[11] V. Gkatsi, R. Vogt-Ardatjew, and F. Leferink, "Risk-based EMC system analysis platform of automotive environments," in *Proc. IEEE Int. Joint EMC/SI/PI EMC Eur. Symp.*, Raleigh, NC, USA, Jul./Aug. 2021, pp. 749–754.

[12] *Risk Management—Guidelines*, ISO Standard 31000:2018, 2018.

[13] V. Gkatsi, R. Vogt-Ardatjew, and F. Leferink, "Detection of EMI issues caused by differential-mode voltages on an electric scooter," in *Proc. 7th IEEE Global EMC Conf. (GEMCCon)*, Bali, Indonesia, Jan. 2023, pp. 44–45.

[14] D. M. Witters and P. S. Ruggera, "Electromagnetic compatibility (EMC) of powered wheelchairs and scooters," in *Proc. 16th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Baltimore, MD, USA, Nov. 1994, pp. 894–895.

[15] *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, Standard MIL-STD-461C CS02, Aug. 1986.

[16] *Wheelchairs—Part 21: Requirements and Test Methods for Electromagnetic Compatibility of Electrically Powered Wheelchairs and Scooters, and Battery Chargers*, ISO Standard 7176-21:2009, 2009.

[17] S. Arianos et al., "Evaluation of the modeling of an EM illumination on an aircraft cable harness," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 4, pp. 844–853, Aug. 2014.

[18] C. R. Paul, *Analysis of Multiconductor Transmission Lines*, 2nd ed. Hoboken, NJ, USA: Wiley, 2007, pp. 602–610.

[19] V. Gkatsi, I. Struzhko, R. Vogt-Ardatjew, and F. Leferink, "Study of random field coupling onto a scooter following the risk-based EMC approach," in *Proc. Int. Symp. Electromagn. Compat. (EMC Europe)*, Gothenburg, Sweden, Sep. 2022, pp. 799–804.