Vulnerability of Smart Grid-based Protection Systems to Ultra-Wide Band IEMI Sources

Fernando Arduini
Electromagnetic Effects and Threats
Fraunhofer Institute for Technological Trend Analysis INT
Euskirchen, Germany
fernando.ribeiro.arduini@int.fraunhofer.de

Michael Suhrke
Electromagnetic Effects and Threats
Fraunhofer Institute for Technological Trend Analysis INT
Euskirchen, Germany
michael.suhrke@int.fraunhofer.de

Thorsten Pusch
Electromagnetic Effects and Threats
Fraunhofer Institute for Technological Trend Analysis INT
Euskirchen, Germany
thorsten.pusch@int.fraunhofer.de

Heyno Garbe
Electrical Engineering and Measurement Technology
Leibniz University Hannover
Hannover, Germany
garbe@geml.uni-hannover.de

***Abstract*—The threat of IEMI to power infrastructures has been growing in concern by experts and authorities worldwide. This is due to the increased integration of smart electronic devices (SEDs), whose microprocessor systems may be vulnerable to high-power electromagnetic interference. One possible gateway for such attacks is the digital protection relays employed to protect power substations. The malfunctioning of these devices could lead to equipment damage (e.g., power transformers) and cascading of blackout events. This paper presents a vulnerability study of a protection system with three different cable topologies subjected to a high-power radiated interfering source. The results showed that variations in the wiring topology would affect the protection system's incidence rate of critical failures when exposed to Ultra Wide Band (UWB) pulses.**

***Index Terms*—IEMI. Smart Grid. Power Systems. Protection System. Ultra-Wide Band Source. Wiring Topology. System-Based Risk Assessment.**

I. Introduction

There is an increasing concern about electromagnetic threats to infrastructures necessary to maintain the vital functioning of society. At the 1999 URSI General Assembly held in Toronto, the use of electromagnetic weapons was no longer deemed to be solely limited to military purposes and was termed Intentional Electromagnetic Interference (IEMI). On that occasion, this term was defined as "*intentional malicious generation of electromagnetic energy by introducing noise or signals into electrical and electronic systems, disrupting, confusing or damaging these systems for terrorist or criminal purposes*." From that point on, several European and other nations included IEMI attacks as one of the emerging threats to critical infrastructures.

One of the most critical infrastructures endangered by IEMI is the power system since the operation of all societal segments depends on the continuous supply of electricity. Even though critical infrastructures such as industries, water management systems, and hospitals usually have backup generators, they cannot handle long outages of the main supply in case of power interruption. In addition, modern power systems rely heavily on automation, centralized equipment control, and high-speed communications due to the increasing integration of Smart Electronic Devices (SEDs). However, despite the advantages of such modernization, including the system's enhanced robustness, efficiency, and flexibility, recent studies have shown that SEDs can be vulnerable to high-power electromagnetic interference sources [1].

For the IEMI risk assessment of critical power infrastructure, empirical laboratory data concerning the susceptibility of SEDs is essential for baseline estimations. In recent studies, smart meters have demonstrated high susceptibility to radiated and conducted narrowband sources at operating frequencies from 150 MHz to 7.5 GHz [2]. Likewise, IEMI susceptibility tests for eight SEDs employed in power substations as part of the Supervisory Control and Data Acquisition (SCADA) system were presented in [3]. These devices comprised telecontrol units and protection relays of different models, manufacturers, and generations. The results showed susceptibility to radiated and conducted high-power narrowband signals in the frequency range between 10 MHz and 3400 MHz for all tested devices. The observed effects ranged from display screen deviation, communication channel interruption, and mission-critical failures, which could lead to extensive impacts on the power system.

The mentioned papers and others involving applications beyond the scope of smart grids have already demonstrated the failure patterns of electronic devices for different IEMI sources and different communication and power cable technologies [4]–[6]. However, there is no scientific literature evidence whether small variations in the cabling layout belonging to critical SEDs influence the incidence of IEMI failures.

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/.

Furthermore, previous IEMI vulnerability studies with SEDs have employed high-power narrowband pulses as source of disturbances. However, tests with other sources are needed to feed IEMI risk analyses of power infrastructures. Therefore, this paper presents a study where the same protection system setup test considering different cable topologies is subjected to a high-power Ultra-Wide Band source. For this purpose, different parameters of this source are considered, including different field strengths, attack duration, and Pulse Repetition Rate (PRR) values.

The paper is organized as follows: Section II introduces the risk analysis steps regarding the IEMI threat. Section III describes the impact of different IEMI sources on electronic devices. The methodology of the test campaign, including the system under test, the monitoring system for fault diagnosis, and the HPEM test environment employed, are described in Section IV. The results are discussed in Section V. Section VI outlines the main conclusions and future work.

II. IEMI Risk Management Process

To ensure acceptable levels of security for CIs, systematic IEMI management processes should also be carried out. According to ISO 31000:2009, a generic risk management process should follow a set of activities as shown in Fig. 1 [7].

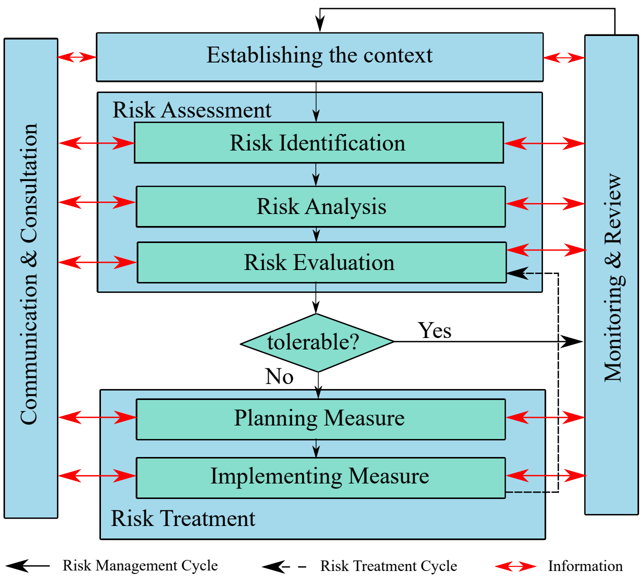


Fig. 1. Risk Management Process [7].

The *Risk Management* process involves three sequential steps represented by *Establishing the context*, *Risk assessment* and *Risk Treatment*. In the first step, represented by *Establishing the context*, the external parameters when managing the risk are defined. Furthermore, scope and risk criteria are defined (e.g. the terms of reference against which the significance of a risk is evaluated).

The subsequent step, represented by the *Risk assessment*, consists of three sub-steps, namely *Risk identification*, *Risk analysis* and *Risk evaluation*. *Risk identification* is the process of identifying, recognising and describing possible risks. In *Risk Analysis*, the nature of the risk is understood and its likelihood and magnitude are determined. *Risk Evaluation* is defined as the process of comparing the results of the risk analysis against the criteria defined in the establishing the context step to find out if the risk is acceptable.

If the risk is not acceptable, the *Risk Treatment* step is performed. In this step, measures are applied to reduce the risk to acceptable levels. All these steps are communicated with the *Monitoring and review* and *Communication and Consultation* steps, which take place during the whole risk management process. On the one hand, *Monitoring and Review* is necessary to periodically ensure that risk management policies and plans are still appropriate. On the other hand, *Communication and Consultation* serves to ensure that those responsible for implementing the risk management process understand the basis for decisions taken.

III. Ultra-Wide Band sources employed for IEMI

The risk identification process involves vulnerability tests to verify a Device Under Test (DUT) behavior when subjected to intentional interfering signals. The IEMI sources can be classified according to their primary coupling scheme, being qualified as radiated or conducted. In the first type, the disturbance signal is radiated over the air to reach the internal electronics of a target system, while in the second, the propagation of the disturbance signal is carried out through conductors connected to the target. Besides the coupling scheme, the IEMI sources can also be classified according to frequency range, waveform, peak voltage (for conducted sources) or peak field (for radiated sources), mobility, and technological challenge. From this perspective, in 2014, 76 different IEMI sources were identified, of which 21 were primarily conducted, and 55 were radiated [8].

The waveform of IEMI sources can have various shapes. The most common types are represented by narrowband and ultra-wideband. The narrowband sources are formed by high-power microwave (HPM) pulses and concentrate the energy at designated frequencies. Therefore, this type of source must be ”tuned” to the vulnerable frequencies of the target system to affect it. The Ultra-Wideband (UWB) sources, on the other hand, are formed by repetitive high voltage transient pulses and concentrate the energy over a large bandwidth [9]. Unlike narrowband sources, UWB sources do not need to be tuned to interfere with the target system since each spectral frequency carries a portion of energy. Hence, these can be used by offenders in attack attempts where the critical frequencies of the target system are unknown.

Several susceptibility studies with UWB sources have been presented. [10] and [11] present a study where IT network systems are subjected to high-power radiated UWB signals. Both showed that these pulses could cause large amounts of errors and total system breakdown, especially for high repetition rate pulses. Similarly, a vulnerability study including several pieces of electronic equipment for general and industrial purposes is introduced in [12]. In the latter, the observed effects intensified with increased field strength levels. On the one hand, a

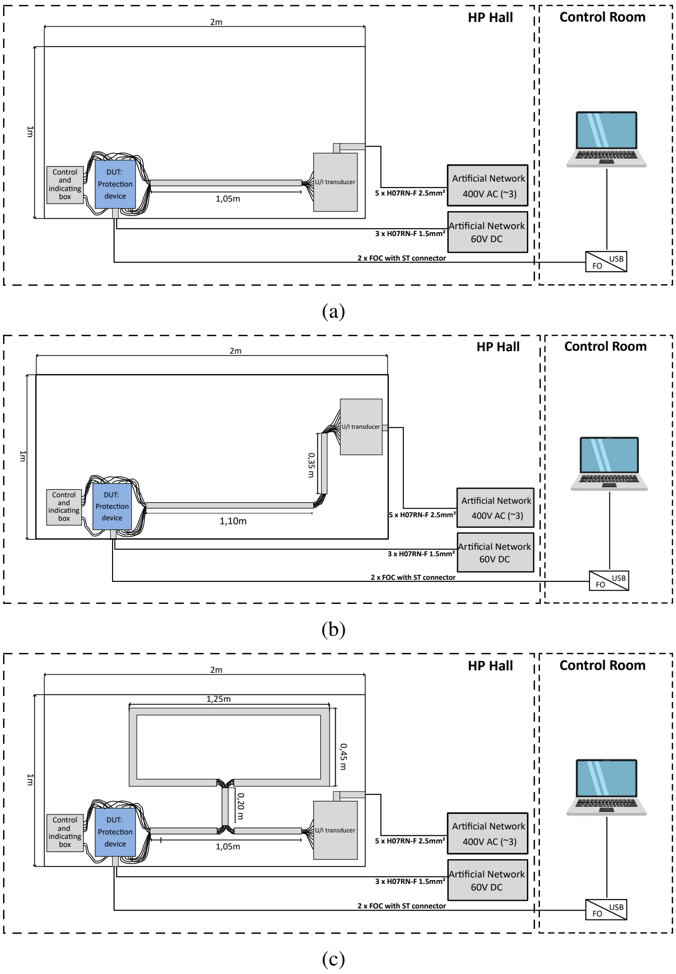


Fig. 2. Test Setups: (a) Flat (b) Angle (c) Loop.

reduction was observed in the speed of data transmission rates of some devices at relatively high exposure levels. On the other hand, both loss and distortion of received information and equipment breakdowns were registered at higher exposure levels. Differently, [13] presents a study focused not on a specific electronic device but on low-voltage installation power cables. The results revealed that subnanosecond rise time UWB voltage transients can propagate over long distances in these cables and may threaten sensitive equipment inside buildings.

IV. Measurement Setup

A. DUT description

Three test setups were proposed to investigate the influence of the cabling topology on the vulnerability of a Device Under Test (DUT). They all have the same DUT and auxiliary equipment for their operation, but different wiring topologies as shown in Fig. 2.

All components are installed on a rigid foam base plate 50 mm thick and 1 m x 2 m in size. The DUT is arranged on the lower left side of the plate. It is represented by a digital protection relay that protects substation switch-bays. For this purpose, the device is configured with an overcurrent function. In this scheme, a trip is performed as long as one of the measured three-phase currents exceeds a threshold current defined as 90% higher than the rated current.

On the right side of the plate, a transducer is installed to emulate the three-phase current and voltage signals typical of secondary substation systems. The current and voltage ratings are 80 A and 25 kV. These signals are measured by the protection relay through a copper wire bundle with a cross-section of 2.5 mm^2.

Next to the DUT, an auxiliary control and indication box is installed to monitor the status of the protection relay. The red and green LEDs of such a box are connected to the relay output, representing the power switch's terminal interface. Under the proposed wiring scheme, the green LED states that the power switch is ”On” and red that it is ”Off”. In case the indicators change from green to red, it means there was an electric signal generated by the protection relay for tripping.

Both DUT and grid emulator power supplies are copper wire-based and are connected to artificial networks and filters outside the waveguide. The 60 V DC lines supply the DUT and are brought from the left side of the test setup, while the 400 V AC lines for powering the grid emulator come from the right side.

The first test setup, represented by Fig. 2(a), is named *Flat*. For this setup, the wire bundle from the transducer box to the protection relay has a straight route. In the case of the second test setup, designated as *Angle* and represented by Fig. 2(b), the same connection has a 90-degree bend nearby the transducer box. The third test setup, represented by Fig. 2(c), is referred to as *Loop* as the wire bundle has a loop layout at the top of the plate.

B. Monitoring system

A two-part monitoring system is employed for fault diagnosis. The first part consists of a set of HPEM hardened cameras to monitor the DUT display and the LEDs of the control and indication box. The second part is an external laptop to track the output communication link of the digital relay, which is connected to a fibre optic converter positioned outside the used test environment. For this purpose, a software in Python has been developed using the IEC 60870-5-103 standard, which defines a protocol for power system control and associated communications [14].

C. HPEM test methodology

An Ultra-Wide Band (UWB) pulse generator was used as an interference source. The pulse generator emits double exponential pulses with a maximum amplitude of 45 kV, a rise time of 120 ps, and a pulse duration width of 2 ns. The TEM waveguide was employed as the radiation medium for the interference signals. Under this test environment, the test setup plate was positioned in such a way that the vertical wire segments were parallel to the electric field and that full illumination of the System Under Test (SUT) was achieved within the TEM waveguide (See Fig. 3).

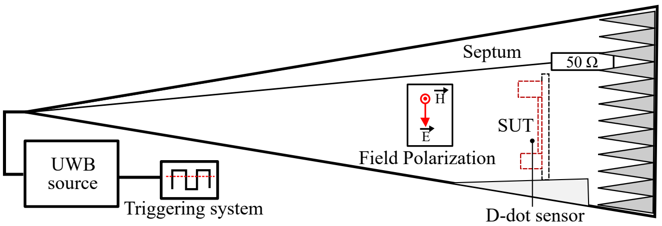


Fig. 3. Measurement scheme based on a UWB source feeding a TEM waveguide.

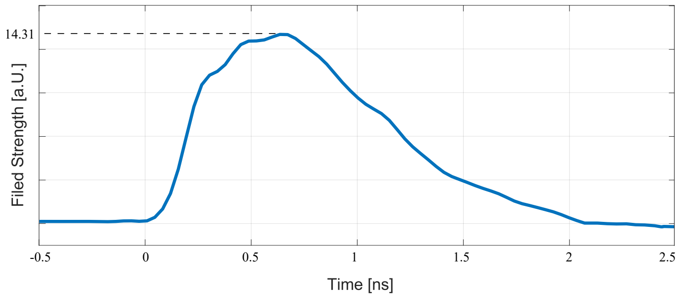


Fig. 4. UWB waveform.

By using a triggering system, several parameters of the UWB source were varied in the test campaign. These parameters were represented by three field strength levels, eight Pulse Repetition Rate (PRR) conditions and four attack durations.

The field strength was measured with a D-dot sensor positioned nearby the SUT. The complete measurement chain consisted of a D-dot probe connected to the oscilloscope input by coaxial cables, optical transmission systems, and attenuators. According to the methodology outlined in [15], the signal sampled by the sensor was integrated and corrected with a factor to obtain the field strength waveform. The resulting pulse can be seen in Fig. 4.

V. Susceptibilities of the Test Setups

Different types of DUT failures were observed for the same test conditions. Such behavior is related to the operational state of the DUT at the moment its internal microprocessor is hit by the UWB pulses. In order to determine an incidence rate for each type of failure considering the three test setups, an extensive amount of experiments would be necessary. In order to present a preliminary idea of the share of failures, five experiments were conducted for each test condition.

Table I describes the failures reported during the measurements campaign. These ranged from failures that do not affect the main function of the DUT, such as display deviation alone, to false trips of the protection relay, which can trigger power system management problems. Several categories of DUT shutdown failures were identified, varying in severity. On the one hand, in the least critical case of shutdown, the relay would be out of operation for approximately one minute (automatic restart required time) after being hit. On the other hand, in the worst-case scenario, the device would not perform

TABLE I
Failure Description.

Failure Identification	**Description**	
B	Secondary functions affected (e.g. protection display flashing)	
C	Protection relay shutdown	The system self-recovers without operator intervention
D		Operator intervention to resume system's secondary function
E		Operator intervention to resume system's primary function
F		Operator intervention to resume system's primary and secondary functions
G	Protection relay false trip	

its primary protective function until the operator realizes the problem and manually restores it.

Fig. 5 shows the share of failures identified for the three field strengths given in arbitrary units (a.U.). For this case, the PRR and the attack duration were set to 500 Hz and 2 s, respectively. In contrast to the *Flat* and *Angle* test setups, for a field strength of 3.91 a.U., failures were recorded exclusively for the *Loop* topology. Furthermore, as the field strength increases, although failures were also recorded for the *Flat* and *Angle* layouts, more critical failures, represented by the more intense tones, were identified for the *Loop* topology. Under the 14.31 a.U. field strength condition, for example, these failures included the worst-case shutdown failures *e* and *f*, and false trips.

In order to further investigate the incidence of critical failures, all shutdown (C, D, E and F) and false trip (G) failures were merged into a single group to demonstrate the following results. The next subsections outline the influence of the cabling topology on the incidence of critical failures for different values of attack duration and PRR.

A. Attack Duration

Fixing the PRR at 50 Hz, the charts represented in Fig. 6 show the percentage of success in causing a critical failure for the three field strength conditions considering increasing attack durations of 2, 4, 6 and 10 seconds. It can be verified that the longer the attack duration (T_a), the higher the incidence of shutdown failures since longer exposure time increases the probability of the DUT being hit at vulnerable operational conditions. Moreover, it is noticeable that the *Flat* wiring layout is less critical than the *Loop* and *Angle* ones in terms of successful attacks.

B. Pulse Repetition Rate

Fixing the attack duration at 6 s, the charts in Fig. 7 depict the incidence of critical failures for PRR of 5 Hz, 10 Hz, 50 Hz, 100 Hz, 200 Hz, 300 Hz, 400 Hz and 500 Hz. As in the case of increasing attack duration, the increase in PRR leads to more successful attacks for all test setups. Similarly, the *Loop* wiring layout suffers more failures than the *Angle* and *Flat* layout. As an example, it is noticed that only the *Loop* cabling topology was affected in the test campaign concerning

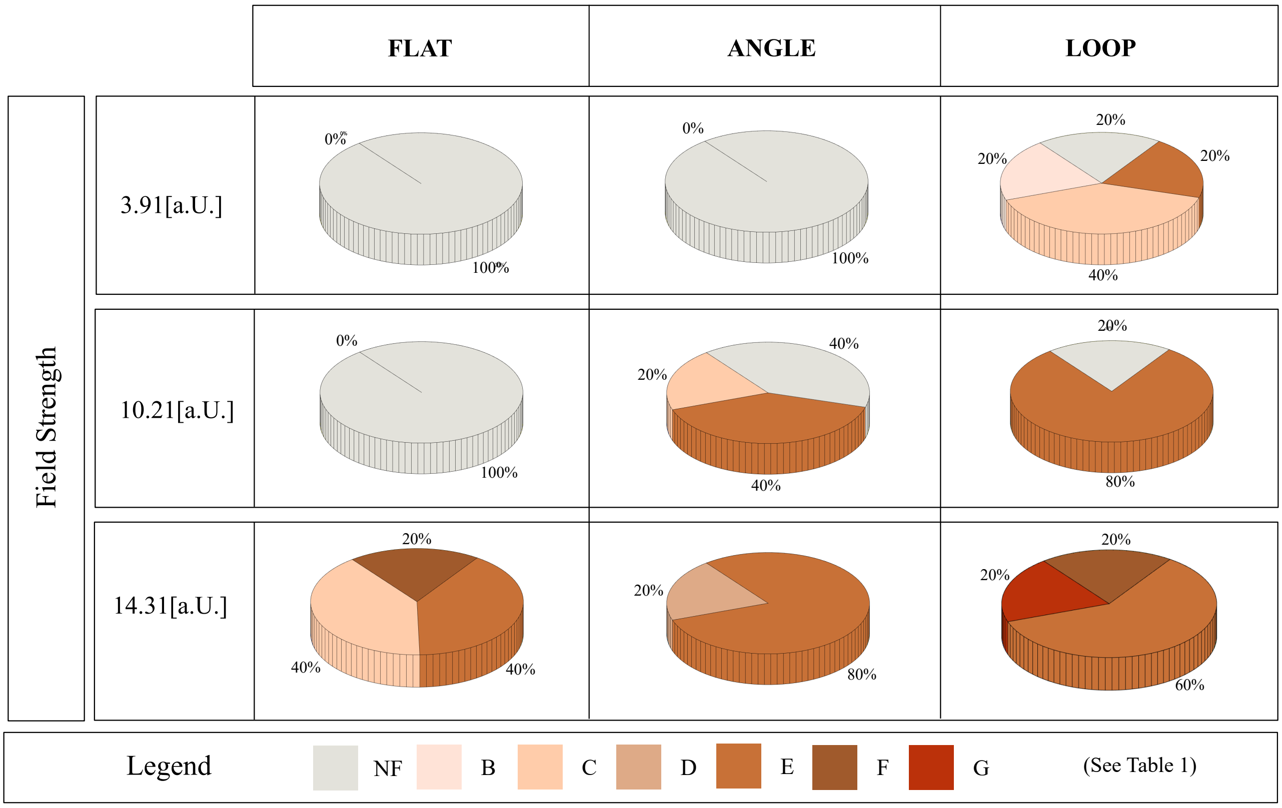
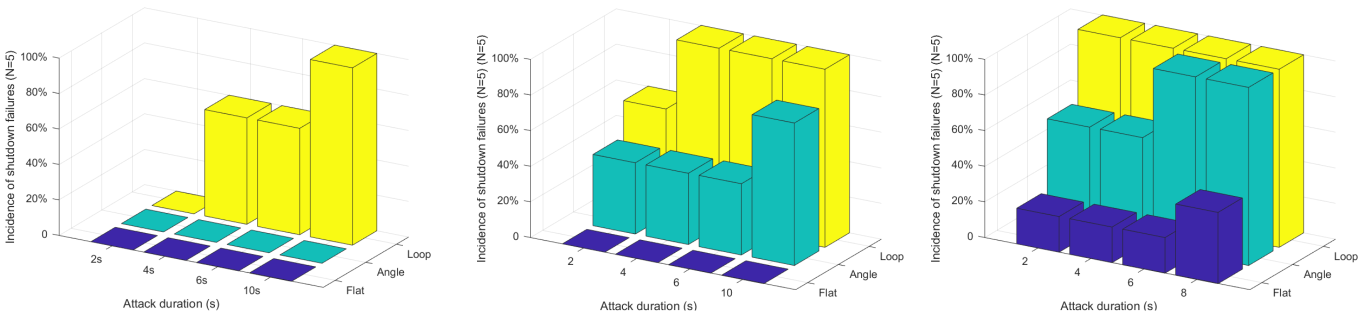


Fig. 5. Failure share (PRR = 500 Hz and T_a = 2 s).



(a) (b) (c)

Fig. 6. Incidence of shutdown failures according to the attack duration increase (PRR = 50 Hz): (a) 3.91 [a.U.] (b) 10.21 [a.U.] (c) 14.31 [a.U.].

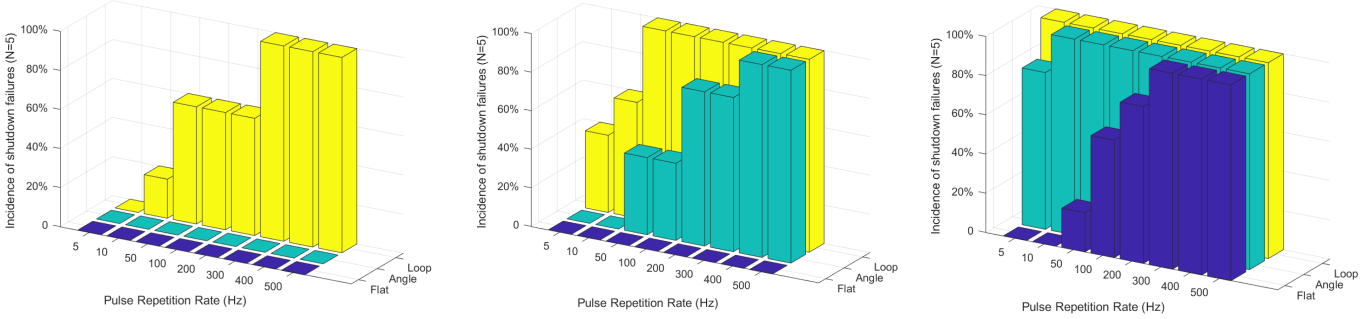
the field strength of 3.91 a.U.. It indicates that the sole fact that the cable topology is different would dictate whether the protection unit would be affected or not.

VI. Conclusion

IEMI sources of UWB characteristic have the spectral content spread in the frequency spectrum, facilitating the coupling in the target system. Unlike narrowband sources, the use of UWB sources does not require knowledge of the critical frequencies of the target device. Thus, these sources can be used by criminals in attempts to affect critical infrastructures in which knowledge of the target system is limited.

This paper presented a vulnerability study involving a digital protection relay enabled for smart grids applications. Three test setups were proposed, where only the cable topologies were different. The results showed that the simple fact of the cable topology being different would dictate if the protection system would be affected when exposed to UWB sources. The topology in which the cabling harness forms a loop, followed by the topology where the cabling has an 90° bend, presented higher incidences of failures. The pattern of failures ranged from non-critical failures, such as deviation of the protection device display, to critical failures, like shutdown with operator intervention needed and false trips.

It is still unknown whether the failure patterns of protection SEDs vary from source to source. Therefore, future investigations include the same vulnerability tests but considering other IEMI source technologies. The next step aims at investigating



(a) (b) (c)

Fig. 7. Incidence of shutdown failures according to the PRR increase (T_a = 6 s): (a) 3.91 [a.U.] (b) 10.21 [a.U.] (c) 14.31 [a.U.].

whether the failure incidence of DUT to high-power narrowband pulses, whose spectral content is concentrated at specific frequencies, is influenced by different cable topologies.

Acknowledgment

The authors would like to thank André Bausen and Jörg Radunz for the assistance provided during the measurement campaign at the Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS), Germany.

References

[1] M. Lanzrath, M. Suhrke, and H. Hirsch, "HPEM-based risk assessment of substations enabled for the smart grid," *IEEE Transactions on Electromagnetic Compatibility*, vol. 62, no. 1, pp. 173–185, 2020.

[2] M. Lanzrath, T. Pusch, M. Jöster, and M. Suhrke, "HPEM-Empfindlichkeit von intelligenten Stromzählern als Komponenten des Smart Grid," in *Internationale Fachmesse und Kongress für Elektromagnetische Verträglichkeit*. Aachen: Apprimus, 2016, pp. 11–18.

[3] M. Lanzrath, M. Suhrke, and H. Hirsch, "HPEM vulnerability of smart grid substation secondary systems," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, 2018, pp. 799–804, doi:10.1109/EMCEurope.2018.8485138.

[4] L. C. Lavau, M. Suhrke, and P. Knott, "Susceptibility of sensors to IEMI attacks," in *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, 2021, pp. 533–537, doi:10.1109/EMC/SI/PI/EMCEurope52599.2021.9559197.

[5] C. Adami, W. Berky, M. Jöster, T. Pusch, and M. Suhrke, "HPEM vulnerability of radiation meters used in security relevant scenarios," in *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, 2015, pp. 1068–1072, doi: 10.1109/ISEMC.2015.7256316.

[6] D. Mansson, R. Thottappillil, M. Backstrom, and O. Lunden, "Vulnerability of european rail traffic management system to radiated intentional EMI," *IEEE Transactions on Electromagnetic Compatibility*, vol. 50, no. 1, pp. 101–109, 2008, doi:10.1109/TEMC.2007.915281.

[7] F. Sabath, "A systematic approach for electromagnetic interference risk management," *IEEE Electromagnetic Compatibility Magazine*, vol. 6, no. 4, pp. 99–106, 2017, doi:10.1109/MEMC.0.8272296.

[8] N. Mora, F. Vega, G. Lugrin, F. Rachidi, and M. Rubinstein, "Study and classification of potential IEMI sources," *System design and assessment notes*, vol. 41, no. ARTICLE, 2014.

[9] R. Doma and A. Syed, "A comprehensive review of high voltage wideband and ultra-wide band antennas for IEMI applications," *Engineering Research Express*, January 2021, doi:10.1088/2631-8695/abd873.

[10] F. Brauer, F. Sabath, and J. L. ter Haseborg, "Susceptibility of IT network systems to interferences by HPEM," in *2009 IEEE International Symposium on Electromagnetic Compatibility*, 2009, pp. 237–242, doi:10.1109/ISEMC.2009.5284569.

[11] R. T. Tientcheu and D. Pouhè, "Susceptibility of generic it-networks," in *2015 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, 2015, pp. 1357–1360, doi:10.1109/ICEAA.2015.7297339.

[12] D. Tsyanenka, V. Mordachev, E. Sinkevich, A. Galenko, X. Ma, and W.-Q. Guo, "UWB EMP susceptibility testing of general-purpose electronic, radio communication, and industrial equipment," in *2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, 2021, pp. 1–4, doi:10.1109/APEMC49932.2021.9597130.

[13] D. Mansson, T. Nilsson, R. Thottappillil, and M. Backstrom, "Propagation of UWB transients in low-voltage installation power cables," *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, no. 3, pp. 585–592, 2007, doi:10.1109/TEMC.2007.902186.

[14] "Telecontrol equipment and systems – part 5-103: Transmission protocols – companion standard for the informative interface of protection equipment," IEC, Standard, Dec. 1997.

[15] M. Kreitlow, G. Schmidt, and F. Sabath, "The uncertainty of measurement in NEMP testing," in *2016 European Electromagnetics Symposium*, July 2016.