IEMI Vulnerability Analysis for Different Smart Grid-enabled Devices

Msc. Fernando Arduini, Fraunhofer Institute for Technological Trend Analysis, Germany.
MEng. Arash Nateghi, Bundeswehr Research Institute for Protective Technologies and NBC Protection, Germany.
Dr. Martin Schaarschmidt, Bundeswehr Research Institute for Protective Technologies and NBC Protection, Germany.
Dr. Marian Lanzrath, Fraunhofer Institute for Technological Trend Analysis, Germany.
Dr. Michael Suhrke, Fraunhofer Institute for Technological Trend Analysis, Germany.

1 Introduction

The smart grid concept aims to improve power systems' robustness, efficiency, and reliability. The transition from conventional power grids to smart grids has been achieved mainly by integrating Smart Electronic Devices (SEDs) and advanced automatic control and communication systems. On the one hand, electronic devices have been integrated to make the system more decentralised from the national electrical grid. On the other hand, from the point of view of protection and control equipment, there is a growing tendency to replace arrays of analog devices with single digital units that perform multiple functions in a more integrated and efficient way. Despite the perceived benefits of such modernisation, security issues have arisen with substantial concern as electronic devices can be susceptible to Intentional Electromagnetic Interference (IEMI) [2].

The number of IEMI sources has grown significantly in recent decades. In 2014, 76 different types were reported, in which 21 sources were conducted, and 55 were irradiated. From a technical perspective, they can present different features, including band type, average / centre frequency, peak voltage (for conducted sources), or peak field (for irradiated sources) [4]. These sources also differ in technology level, associated cost, and mobility in approaching the target system. Therefore, they can be characterized by the easiness of occurrence in a given scenario and the increased probability of successful attacks on a target system. Under this perspective, a self-built jammer built with off-the-shelf components is more likely to be employed by an offender than a High-Power Electromagnetic (HPEM) source. On the other hand, despite being less probable on account of higher technological level, cost and mobility, a HPEM source may have a higher success rate to affect the target system than the self-built jammer. Coupled with this, based on the different characteristics of the IEMI sources, the electronic devices may present distinct effects, which may trigger severe impacts on a smart grid at a higher level [8].

Therefore, this study compares the IEMI vulnerability of three devices used in smart grid applications. The first device is a Wi-Fi-based smart home meter. It can read voltage and current signals of consumer units and remotely display real power, reactive power, and power factor. These measurements can be used in-house or transmitted to a Supervisory Control and Data Acquisition (SCADA) system from Distribution System Operators (DSOs). The second device is a Power Line Communication (PLC) unit, which enables data to be carried over conductors intended primarily for electrical power transmission. This technology is used in buildings to reduce the communication network's material and installation costs and provide flexibility and faster data communication. The final device considered is a digital protection relay designed to trip circuit breakers when faults are detected. The latest digital relay units feature many protection functionalities, including overload and under-voltage/over-voltage protection, temperature monitoring, fault location, self-reclosure, among others. The three devices are subjected to self-built low-power jamming signals. As an extension, the protection relay is also subjected to a narrowband High Power Electromagnetic (HPEM) source.

2 Smart Electronic Devices

The SEDs are made possible by bidirectional communication technologies, control systems, and computer processing. The integration of these devices is expanding throughout the energy infrastructure, from power plants to final consumers. This study encompasses three Devices Under Test (DUTs) that perform different applications in smart grids. They are represented by a smart meter, a Power Line Communication (PLC), and a digital protection relay. The following subsections detail the power system application of each one, as well as their proposed setups for the test campaigns.

2.1 Smart meter

Smart meters are key devices for systematic management of energy systems in the smart grid with automated integration of commercial and domestic infrastructures to intelligently and efficiently coordinate decentralised energy suppliers. Apart from hardware and software components that apply the required functionalities, such as accurate measurement and calibration, smart meters have to be able to communicate to local SCADA systems via communication channels [1]. A loss of communication between smart meters and data concentrators, which support the SCADA system for important decisions, could have catastrophic consequences. These consequences include accidentally tripping circuit breakers, overloading the distribution lines, and increasing the risk of scalable power outages. Due to the positioning of the power distribution board, where the smart meter needs to be installed, Wi-Fi is used as a data transmission method more frequently.

In addition to voltage, current, and phase measurement, smart meters can be wirelessly connected to smartphones via mobile phone applications to support demand-side management. The mobile application can provide power usage transparency that can be used to compare supplier fees by the amount of power usage and government-mandated power factor reporting of commercial and large residential buildings to improve power quality. In [6], the susceptibility of wireless smart meters to an IEMI jamming signal is evaluated. From the experimental results, wireless communication was easily disturbed by radiated interfering signals. The interference effects varied, and the maximum impact occurred when the EMI disturbed signal hit the right frequency interval of the WLAN Orthogonal Frequency-Division Multiplexing (OFDM) physical layer (PHY). The test setup used in the test campaign is illustrated in Image 1.

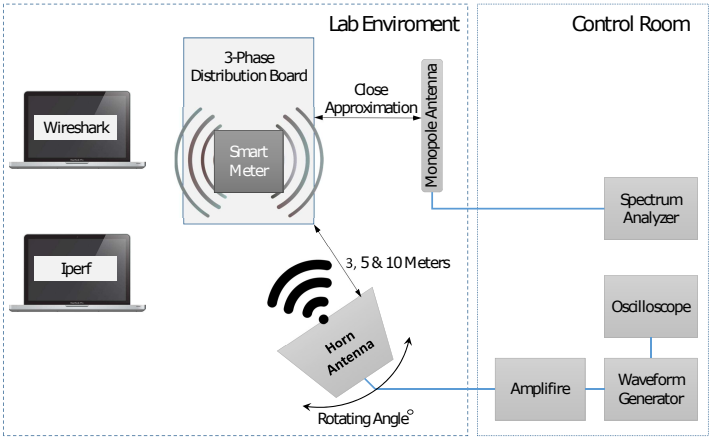


Image 1: Jamming signal radiation into W-LAN communication of smart meter [6].

2.2 PLC

Cost-effective decentralisation of the power grid requires existing assets and the interconnection of the necessary subsystems to improve operability and power flow diversity. In smart grid communication systems, where infrastructure costs need to be reduced, Power Line Communication (PLC) can be an optimal solution for transmitting the data of power system nodes, including demand side, generation points, and substations. In addition, PLC is used in commercial and residential buildings to facilitate data transmission to different property locations and improve Internet service where there are no data-link connections, especially in existing buildings. PLC can operate in Ultra-Narrowband frequencies below 3 kHz (UNB-PLC), Narrowband frequencies from 3 kHz to 500 kHz (NB-PLC), and Broadband frequencies above 1.8 MHz (BB-PLC) [3]. The test setups from previous work [5] for conducted and radiated jamming-based signals are given below in Image 2.

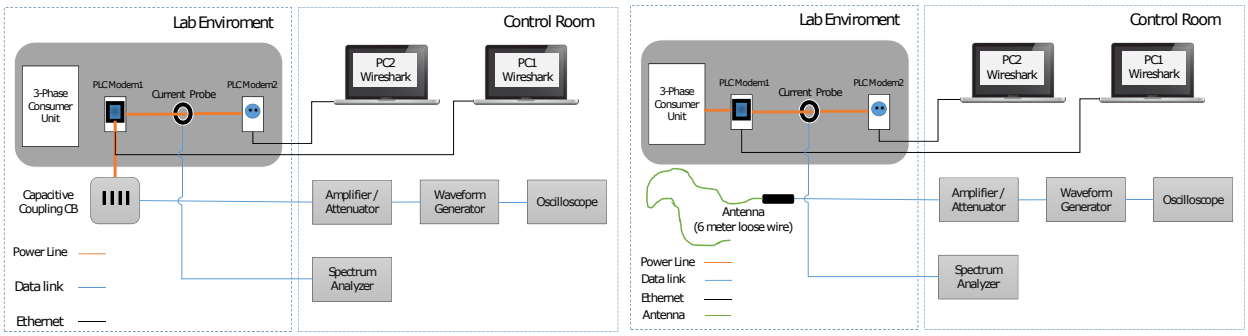


Image 2: Conducted and Radiated EMI signal into PLC. (a) Conducted (b) Radiated [5].

2.3 Digital Protection relay

The final device considered is a protection relay used in power distribution and transmission substations. It is intended to remove any element of the electrical system (e.g., transformers, lines, switchgear bays) immediately when short-circuit conditions or any abnormality that might interfere with the system's effective operation is identified. A power substation usually contains multiple protection relays mounted in racks located in control rooms. In this sense, each unit present is responsible for protecting a certain infrastructure element. In recent decades, digital protective relays have been replacing electromechanical units due to several advantages, including compactness, fast speed of response, and the ability to communicate with a SCADA system. In many circumstances, a single digital relay provides functions that would be required for multiple electromechanical units. These functions can include overload and undervoltage / overvoltage protection, temperature monitoring, fault location, auto-reveal, etc. The failure of such devices could cause several consequences to the power system. These consequences range from damage to high voltage equipment to the triggering of blackout events.

For the purposes of this study, a digital protective relay and the auxiliary equipment for its operation were mounted on a 50 mm thick rigid foam base plate. The device was configured with an overcurrent function, in which tripping occurs as long as one of the measured three-phase currents exceeds a threshold current defined as approximately 80 % greater than the nominal current. On the bottom right side of the board, a transducer is installed to emulate the three-phase current and voltage signals typical of secondary substation systems. The nominal currents and voltages are 80 A and 25 kV. These signals are measured by the protection relay by means of a bundle of copper wires 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. If the indicators change from green to red, it means that the protection relay has

generated an electrical signal for tripping. Both the DUT and the power supplies of the network emulator are copper wire-based and are connected to artificial networks and filters outside the waveguide. The protection relay communicates with an external laptop placed in the control room through a fiber optic cable. A software was developed in Python to display the three-phase current and voltage measurements in real-time. Moreover, such software displays alert messages whenever there is any information transmission breakdown to the external laptop.

For the purposes of the investigation, the protective relay is directly irradiated with a horn antenna placed three meters away. In addition to the exposure to jamming signals as performed for the smart meter and PLC devices, the protection relay is irradiated with an HPEM narrowband source, which will be detailed in Section 3.2

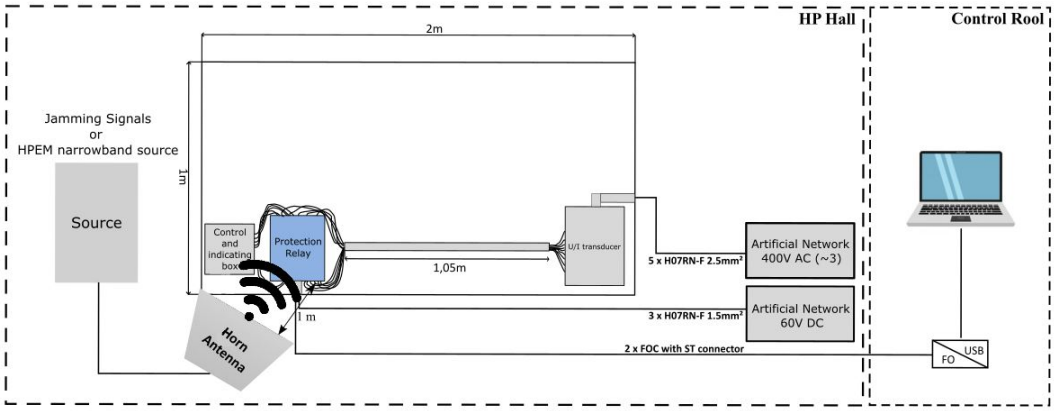


Image 3: Protection relay-based test setup.

3 IEMI Sources

The three smart grid devices were exposed to a low-power jamming weapon as the IEMI-generating source. As a complement to the investigations, the protection relay was further exposed to a higher power interference source, representing a higher degree of threat but a lower probability of usage. The subsections below detail the sources employed in the test campaigns.

3.1 Jamming Signals

The jamming signals can interfere with most communication links considering their frequency bandwidth [7]. For the previous works carried out in [6] and [5], the jamming signal was defined using MATLAB and then fed into a Programmable Arbitrary Wave Generator (PAWG) before being radiated or conducted to disturb the PHY layer of the communication link under test.

The Sweep Period (SP) jamming signal that provides the required frequency band is defined and plotted in MATLAB employing the following Equations 1 and 2.

$$i(t) = I\ cos(2\pi\ f(t)\ t),\ \ 0 < t < SP \tag{1}$$

$$f_i(t) = \frac{\mathrm{d}}{\mathrm{d}t}[f(t)\ t)] = \frac{f_2 - f_1}{SP}t + f_1 \tag{2}$$

where f_1 is the start frequency, f_2 is the stop frequency, and SP is the sweep period.

The frequency band for jamming the Wi-Fi signal ranges from f_1 = 2.4 GHz to f_2 = 2.5 GHz and the SP value is set up to 10 µs. However, the frequency band and SP value of the jamming signal can

be varied in Equation 1 and 2 to also target the PHY layer of the PLC and the data communication of the protection relay. To determine the required frequency bandwidth of the communication link, a spectrum analyser in connection with current probes are used, and the associated power spectrum versus frequency of all three communication links are given in Images 4, 5 and 6, respectively.

The Interference-to-Signal Ratio (ISR) represents the percentage of the interference signal (jamming signal) covering over the actual signal transmitted in the associated propagation channel. Having the quantities M1 and M2 from Images 4, 5 and 6, the ISR can be calculated using Equation 3:

$$ISR = 100\ (\frac{2M_1 - M_2}{M_2})\ \% \tag{3}$$

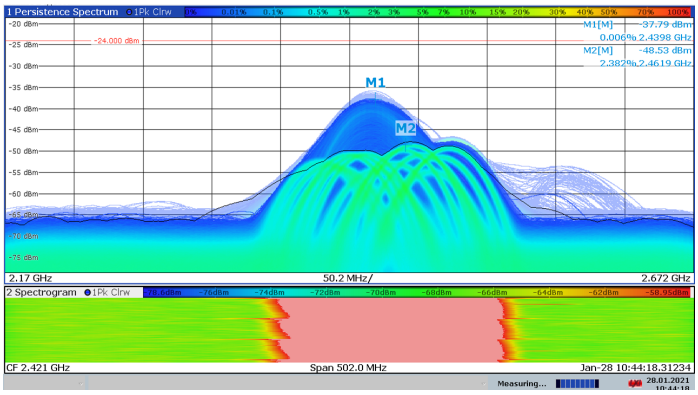
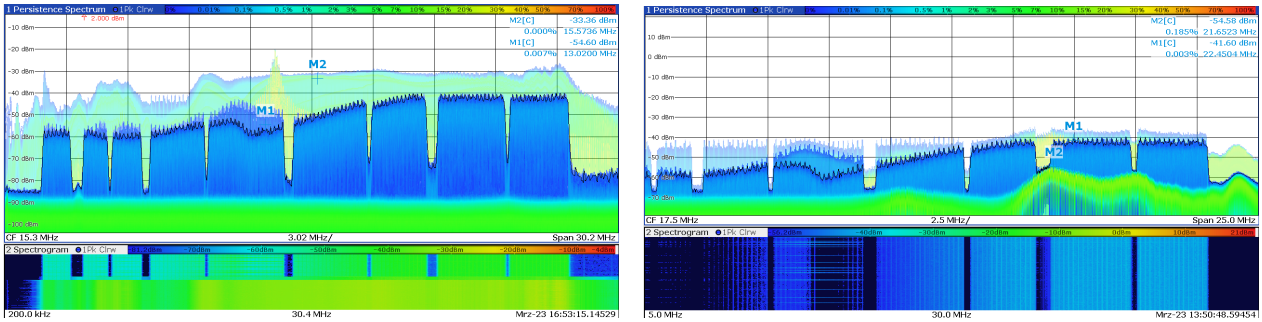


Image 4: SP jamming signal radiated into the Wi-Fi signal [6].



(a) (b)

Image 5: Jamming signal into the PLC PHY layer. (a) Conducted (b) Radiated. [5]

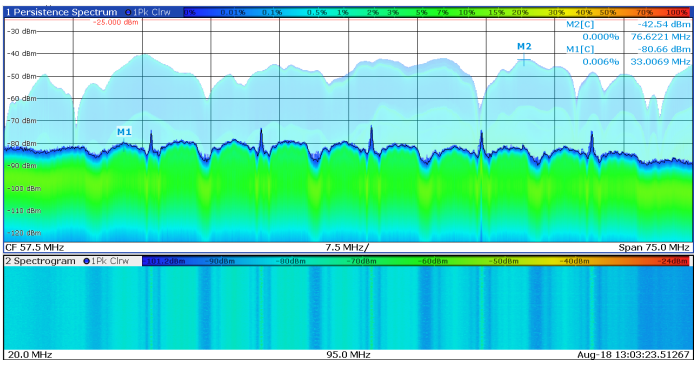


Image 6: Jamming signal radiated into the protection-relay communication link.

3.2 High-Power Narrowband Source

The high-power source employed is represented by narrowband signals with strengths well above typical EMC requirements (above 10 V/m). This type of source is formed by high power microwave pulses (HPM) and concentrates energy at designated frequencies. A high power HPM oscillator covering the frequency range from 480 MHz to 3400 MHz is used as the power source for a horn antenna placed 1 meter away from the test equipment. The frequency steps for the ranges of 480 MHz - 1 GHz, 1 GHz - 2 GHz, and 2 GHz - 3.4 GHz were 10 Hz, 20 Hz and 50 Hz, respectively. The waveform of the applied pulse is shown in Image 2(a). It represents a typical narrowband or radar signal with pulse width of 1 µs and repetition rate of 1 kHz. For the identification of fault thresholds, the output power follows a ramp function with a 20 second duration. The power starts with a minimum value, as the HPM oscillator requires some excitation for steady operation, and ends at the maximum achievable value (see Image 2(b)).

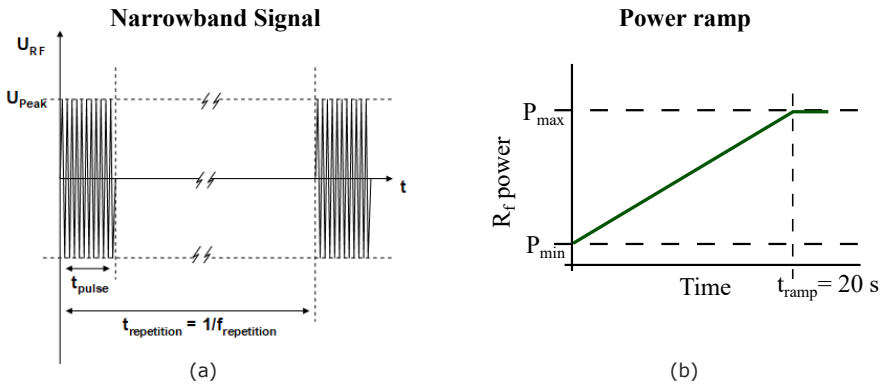


Image 7: HPEM Test Environment: (a) Narrowband signal waveform (b) Power ramp.

4 Results

The results of applying the jamming signal in Wi-Fi-based smart meter, PLC and protection relay communication channels, and the HPEM signal in the protection relay is described in the following sections.

4.1 Jamming Signals

The communication link of Wi-Fi is attacked by the radiated jamming signal defined in the previous sections, which uses a horn antenna with the associated frequency band. The jamming signal in the frequency range of several tens of MHz is radiated to the protection relay via an in-house developed horn antenna. Due to the complex design of the transmitting antenna for the frequency range of a few MHz, a six meter long single wire is used to radiate the interference jamming signal. However, the efficiency of the radiated signal is low with a single wire antenna, and the conducted jamming signal is also applied to disturb the PHY layer of the PLC channel.

Table 1 shows the characteristics of the applied Jamming signal and the calculated ISR for all three types of communication links discussed in the previous sections. As it can be observed, the jamming signal has more disruptive effects when physically coupled into the PLC channel than when radiated into the environment where PLC equipment is present. In addition, the radiated jamming signal in Wi-Fi communication can cause a much higher ISR percentage than the protection relay and PLC due to the nature of WLAN communication medium air. The case material used for more sensitive materials such as protection relays makes them more resilient to radiated EMI jamming signals compared to PLC modems and smart meters used for this work. The jamming signal radiated to all three DUTs from a distance of three meters. In addition to power amplification,

organisational measures such as accessibility and technical measures such as distance between source and victim could change the ISR ratio.

Table 1: Jamming signal applied to the smart meter, PLC and protection relay.

Device Under Test	Type of propagation	Start Freq. (f_1)	Stop Freq. (f_2)	SP (μs)	Power Amplified (W)	ISR (%)
Smart Meter (Wi-Fi)	Radiated (horn antenna)	2.4 GHz	2.5 GHz	10	50	71.5
PLC	Radiated (single wire)	20 MHz	28 MHz	10	50	25
PLC	Conducted (capacitive coupling board)	20 MHz	28 MHz	10	50	61
Protection Relay	Radiated (Horn Antenna)	20 MHz	100 MHz	10	50	10

4.2 HPEM source

The only device that did not suffer interference with the low power jamming signals was subjected to a high-power narrowband source. Image 8 shows the DUT vulnerability plot for the vertical field polarization when the protection relay is directly illuminated with a high-power narrowband source. The frequency is plotted on the horizontal axis and the electric field strength in arbitrary units (a.u.) on the vertical axis. The red area represents the field strengths applied for each frequency condition. The markers represent the individual failures observed during the power ramp at a given test frequency.

From Image 8, several failures along the frequency spectrum can be observed. Most of them are communication-related, where the external laptop temporarily stops communicating with the DUT. Under this condition, the performance of a SCADA system could be impaired since data reception and transmission would be temporarily ceased. Furthermore, three types of shutdown failures were recorded. In the first case, the protection relay is deactivated but automatically resumes itself after 40 seconds. In the second case, the device also auto recovers similarly, but the display is disturbed, meaning that the current and voltage readings are not possible until an operator intervenes. In the third case, the main protection relay functionality is removed from service until an operator restores the device.

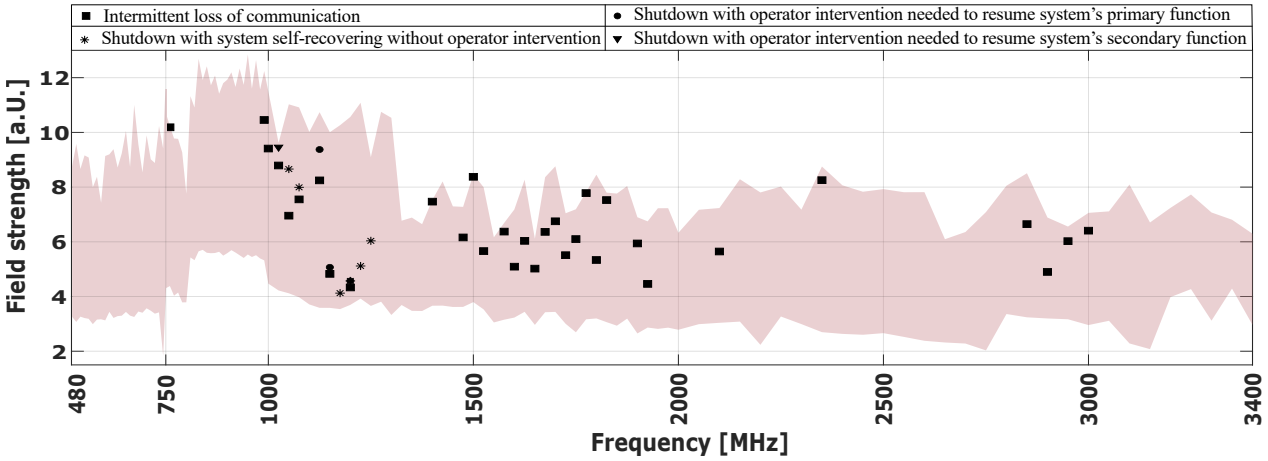


Image 8: Illumination of the DUT with a narrowband HPEM source.

5 Conclusions

The results show that the vulnerability of IEMI sources varies according to the technology type of smart grid devices. Low power interference signals disrupted the communication of smart meters and PLC devices. On the other hand, this type of interference did not affect the communication channel of the tested digital protection relay due to proper shielding and use of fiber optic communication link. Although not affected by jamming signals, the communication channel of the protection relay and its general operation were compromised with a higher power IEMI source, represented by a narrow-band HPM source.

In addition, the susceptibility of the smart grid devices to IEMI sources such as jamming signal, which requires little expertise to design, depends on the number of elements that play an important role in changing the ISR ratio. These elements are; a possible coupling path, the accessibility of the site where device is installed, the mobility of the IEMI source, the strength of the IEMI signal amplitude and the distance to the target system. The next step is to set up a complex smart grid system to intentionally apply EMI to it and assess the vulnerability of the parent system when a subsystem such as communication links is intentionally attacked by electromagnetic interference.

Acknowledgements

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/.

References

[1] BARAI, Gouri R. ; KRISHNAN, Sridhar ; VENKATESH, Bala: Smart metering and functionalities of smart meters in smart grid - a review. In: *2015 IEEE Electrical Power and Energy Conference (EPEC)*, 2015, S. 138–145

[2] LANZRATH, Marian ; SUHRKE, Michael ; HIRSCH, Holger: HPEM-Based Risk Assessment of Substations Enabled for the Smart Grid. In: *IEEE Transactions on Electromagnetic Compatibility* 62 (2020), Nr. 1, S. 173–185. http://dx.doi.org/10.1109/TEMC.2019.2893937. – DOI 10.1109/TEMC.2019.2893937

[3] LÓPEZ, Gregorio ; MATANZA, Javier ; DE LA VEGA, David ; CASTRO, Marta ; ARRINDA, Amaia ; MORENO, José I. ; SENDIN, Alberto: The Role of Power Line Communications in the Smart Grid Revisited: Applications, Challenges, and Research Initiatives. In: *IEEE Access* 7 (2019), S. 117346–117368. http://dx.doi.org/10.1109/ACCESS.2019.2928391. – DOI 10.1109/ACCESS.2019.2928391

[4] MORA, Nicolas ; VEGA, Felix ; LUGRIN, Gaspard ; RACHIDI, Farhad ; RUBINSTEIN, Marcos: Study and classification of potential IEMI sources. In: *System design and assessment notes* 41 (2014), Nr. ARTICLE

[5] NATEGHI, Arash ; SCHAARSCHMIDT, Martin ; FISAHN, Sven ; GARBE, Heyno: Susceptibility of Power Line Communication (PLC) Channel to DS, AM and Jamming Intentional Electromagnetic Interferences. In: *2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, 2021, S. 1–4

[6] NATEGHI, Arash ; SCHAARSCHMIDT, Martin ; FISAHN, Sven ; GARBE, Heyno: Vulnerability of Wireless Smart Meter to Electromagnetic Interference Sweep Frequency Jamming Signals. In: *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, 2021, S. 755–759

[7] ROMERO, Grecia ; DENIAU, Virginie ; STIENNE, Olivier: LTE Physical layer vulnerability test to different types of jamming signals. In: *2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE* IEEE, 2019, S. 1138–1143

[8] SABATH, Frank: Classification of electromagnetic effects at system level. In: *Ultra-Wideband, Short Pulse Electromagnetics 9*. Springer, 2010, S. 325–333