IEMI Risk Analysis for different smart grid-enabled devices

Speaker: Msc., Fernando, Arduini, Fraunhofer Institute for Technological Trend Analysis, Germany

Co-authors: Msc., 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., Michael, Suhrke, Fraunhofer Institute for Technological Trend Analysis, Germany.

1 Introduction (NOT READY)

The electricity sector has been undergoing transformations towards the smart grid concept, which aims to improve the robustness, efficiency, and flexibility of the power system. This transition has been achieved by the introduction of smart electronic devices (SEDs) and advanced automatic control and communication systems. One of the essential aspects of smart grid infrastructure is to include a system that is decentralized from the national power grid to work independently and that can also communicate with other decentralized local grids. In addition, from the point of view of power substations, there is a trend to replace analogue device sets with single digital units that perform multiple functions.

Despite the benefits of such modernization, safety issues have emerged with significant concern by experts and entities worldwide. One of these issues is known as Intentional Electromagnetic Interference (IEMI), where offenders employ electromagnetic sources to maliciously disrupt or damage electronic devices. Compared to a physical act of terrorism (e.g., involving the use of explosives) intended to disrupt critical infrastructure, an IEMI attack can easily occur unnoticed and remote from the target system. Conversely, in contrast to a cyber-attack, in which a hacker may trigger alarms while attempting to bypass a system's firewall, exposure to IEMI usually does not leave a trace on the affected system.

The vast number of existing IEM-generating sources range from self-made jammers built with off-the-shelf components to High Power Microwave (HPM) sources used for military purposes. They represent different characteristics, including band type, average/central frequency, peak voltage (for conducted sources) or peak field (for radiated sources). In addition, they can have different non-technical features. The later are represented by the level of technology required to assemble and deploy the source, the associated cost, and the mobility in approaching the target system.

The vast number of existing IEM-generating sources range from self-made jammers built with off-the-shelf components to High Power Microwave (HPM) sources used for military purposes. They represent different characteristics, including band type, average/central frequency, peak voltage (for conducted sources) or peak field (for radiated sources). In addition, they can have different non-technical features. The later are represented by the level of technology required to assemble and deploy the source, the associated cost, and the mobility in approaching the target system.

In view of this, this study presents a comparison of the IEMI vulnerability for three different devices used in smart grid applications, considering mainly a low-power jamming weapon as the IEMI-generating source. The first device considered is a smart home meter. It can read voltage and current signals of each phase of a three-phase consumer unit and then remotely display real power, reactive power and power factor. These measurements can be used internally or sent to a supervisory control and data acquisition (SCADA) engineer at the local distribution system operator (DSO) to operate the smart grid system more efficiently. Other features of these smart meters are their switching capabilities, which can be done remotely via smartphone applications. The second

device is a PLC device, which can employ the latest technology from providers of smart grid communication solutions for data transmission. This can be done by means of overhead or underground lines with variable

2 Devices Under Test

The Devices Under Test (DUTs) are represented by different smart grid devices. They comprise 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 the systematic management of energy systems in the smart grid with automated integration of commercial and domestic infrastructures in order to intelligently and efficiently coordinate decentralized 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 a circuit breaker, overloading the distribution line, increasing the risk of a scalable power outage. 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 the demand side management. The mobile application can provide power usage transparency that can be used to compare supplier fees by amount of power usage and government-mandated power factor reporting of commercial and large residential buildings to improve power quality. In [4], the susceptibility of wireless smart meters to an IEMI jamming signal is evaluated. From the experimental results, wireless communication was easily disturbed by interfering signal radiation into the air as the signal propagation medium. 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.

2.2 PLC

Cost-effective decentralization of the power grid requires the use of 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 locations of the property 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) [2]. The test setup from previous work [3] for Conducted EMI signal and Radiated EMI signal are given bellow, respectively, Image 2 and Image 3 .

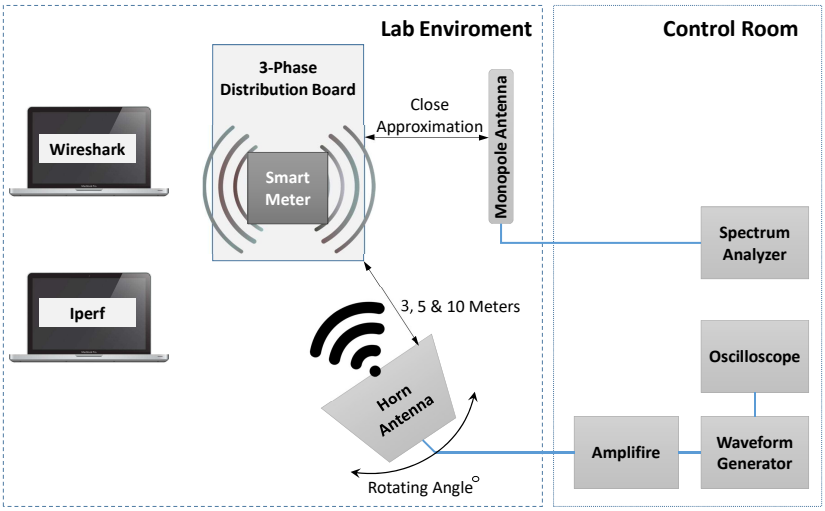

Image 1: Jamming signal radiation into W-LAN communication of smart meter [4].

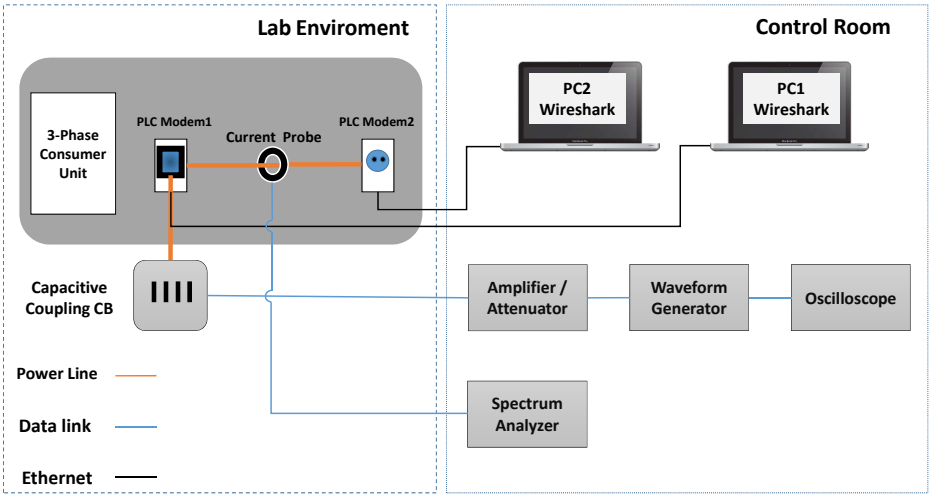

Image 2: Conducted EMI signal into PLC [3].

2.3 Digital Protection relay

The final device considered is a protection relay used in power distribution and transmission substations. It is intended to immediately remove any element of the electrical system (e.g. transformers, lines, switchgear bays) when short-circuit conditions or any abnormality that might interfere the effective operation of the system is identified. A power substation usually contains multiple protection relays that are mounted in racks located in control rooms. In this sense, each unit present is responsible for protecting a certain element of the infrastructure. In recent decades, digital protective relays have been replacing electromechanical units due to a number of advantages including compactness, fast speed of response and the ability to communicate with a SCAD system. In

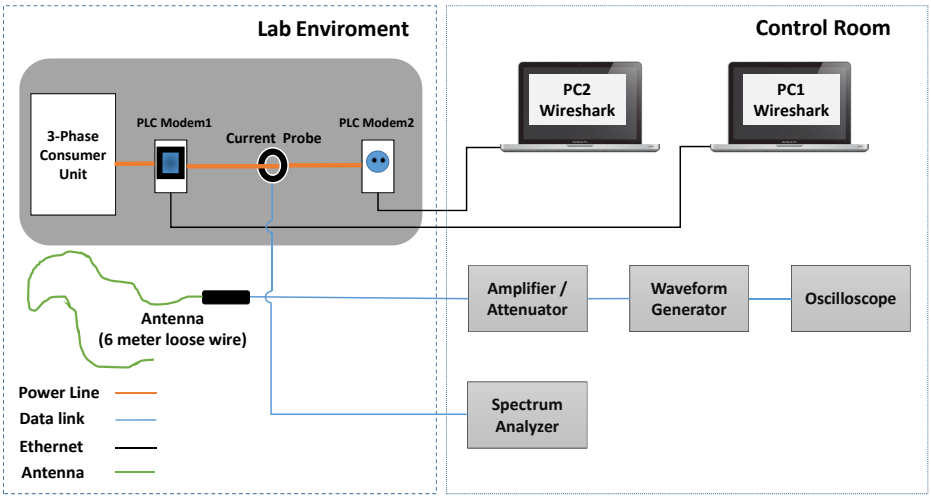

Image 3: Radiated EMI signal into PLC [3].

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, and more. The failure of these devices can 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 as well as 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 a 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. The red and green LEDs of such a box are connected to the output of the relay, which represents the terminal interface to the power switch. Under the proposed wiring scheme, the green LED indicates that the power switch is "On" and the red one that it is "Off". If the indicators change from green to red, it means that there has been an electrical signal generated by the tripping protection relay. 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 60 V DC power lines to the SUT are brought from the left side of the test setup, while the 400 V AC lines to power the network emulator come from the right side.

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 also exposed to a higher power interference source, which represents a higher technological level. The subsections below detail the sources employed in the test campaigns.

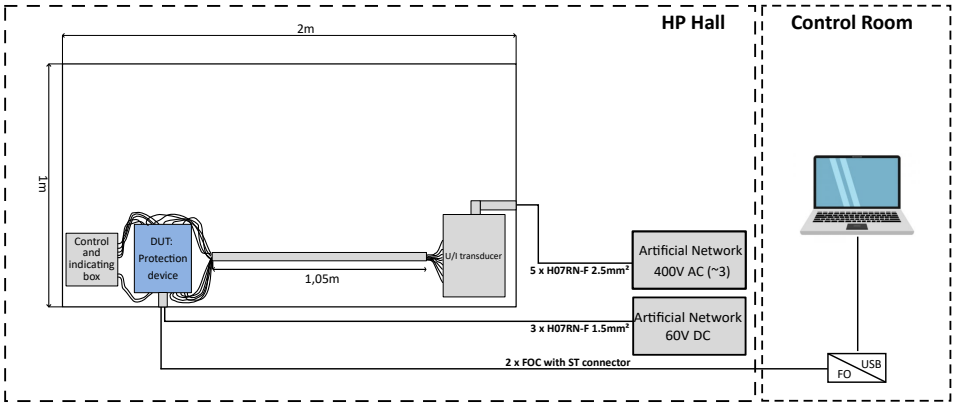

Image 4: Protection relay-based test setup

3.1 Jamming Signals

The jamming signal that can be used by signal jammier devices can interfere with most communication links considering their frequency bandwidth [5]. For the previous works carried out in [4] and [3], 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.

As it can be seen in Image 6, the frequency band for this jamming signal ranges from f_1 = 2.4 GHz to f_2 = 2.5 GHz, which is used for Wi-Fi signals, and SP value is set up to 10 µs. However, the frequency band and SP value of jamming signal can be varied in Equation 1 and 2 to target the PHY layer of the PLC and 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 5, 6 and 7, respectively.

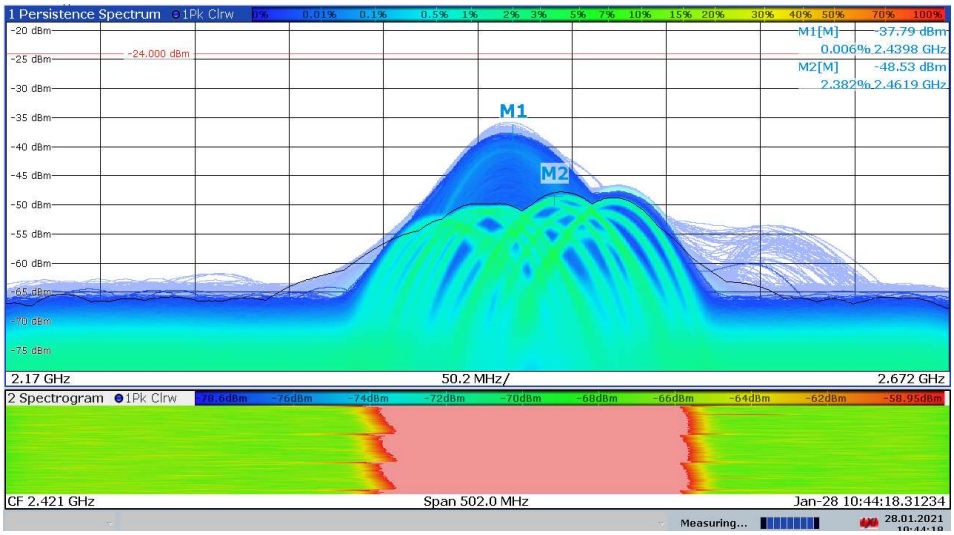

Image 5: SP jamming signal radiated into the Wi-Fi signal [4].(CHANGE FIGURE)

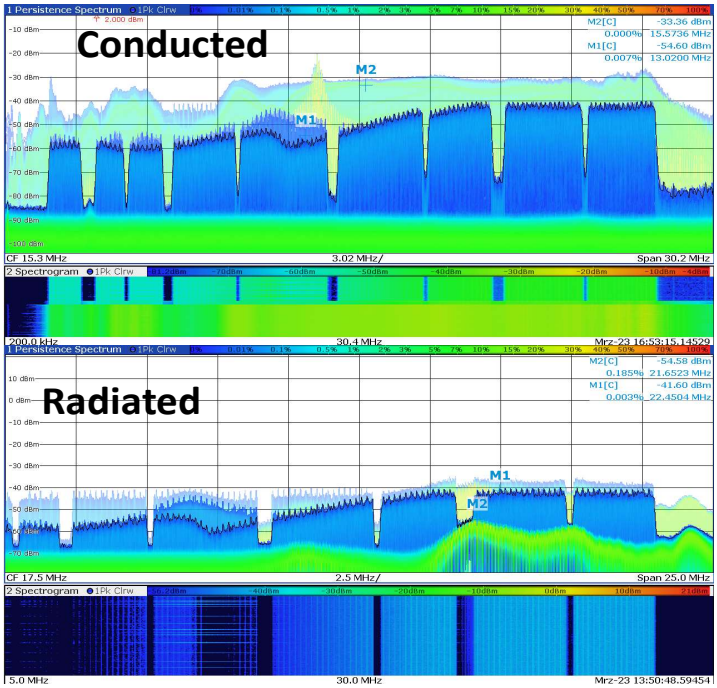

Image 6: Jamming signal conducted and radiated into the PLC PHY layer [3] (CHANGE FIGURE).

Having the quantities M1 and M2 from Images 5, 6 and 7, the Interference to Signal Power Ratio (ISR) can be calculated using Equation 3:

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

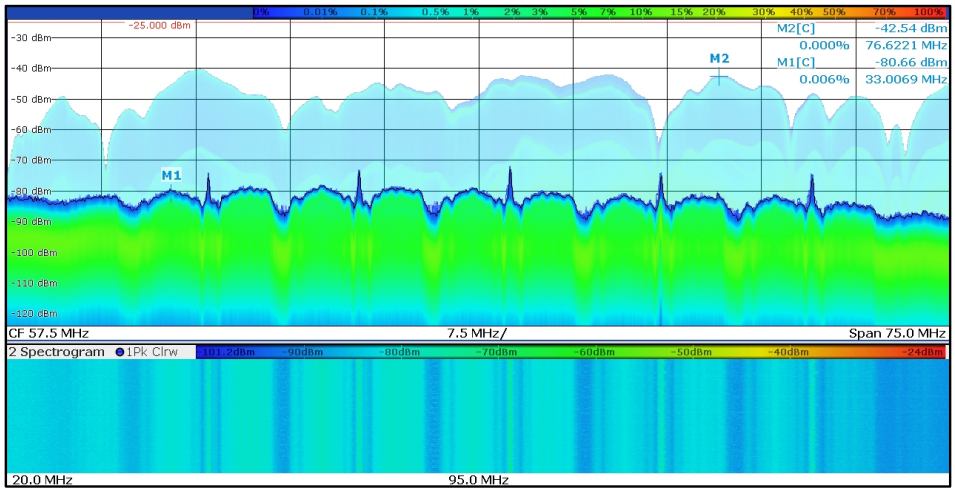

Image 7: Jamming signal radiated into the protection-relay communication link.

3.2 High-Power Narrowband Source

The high-power source employed was represented by narrow-band 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 140 MHz to 3400 MHz was used as the power source for a horn antenna placed 2 meters away from the test equipment. The waveform of the applied pulse is shown in Fig. 2(a). It represents a typical narrowband or radar signal with pulse width of 1 s 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 Fig. 2(b)).

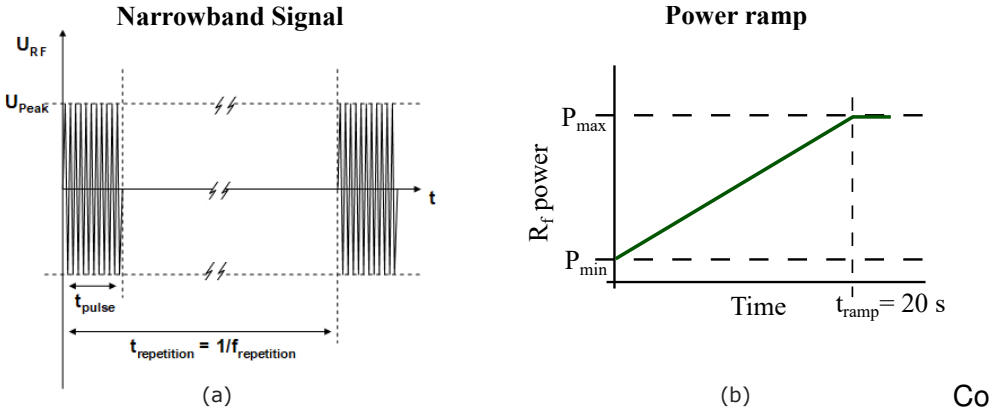

Image 8: HPEM Test Environment: (a) Narrowband signal waveform (b) Power ramp.

4 Results

4.1 Jamming

The communication link of Wi-Fi and protection relays is attacked by radiated jamming signal defined in previous sections using horn antenna with related frequency band. Due to the complexity of the design of the transmitting antenna for frequency range of few MHz, a six-meter long single wire is used to radiate the jamming signal. However, the efficiency of the radiated signal is low with single wire antenna and the conducted jamming signal is also applied to disturb the PHY layer of the PLC. The table (See Table I) explains more about the characteristics of the applied Jamming

signal and the calculated ISR for all three types of communication links discussed in the previous sections.

Table I. Jamming signal applied to Wi-Fi, PLC and protection relay communication links.

Communication type	Type of propagation	Start frequency (f_1)	Start frequency (f_2)	SP (µs)	Power amplified (%)	ISR (%)
Wi-Fi	Radiated (using horn antenna)	2.4 GHz	2.5 GHz	10	50	71
PLC	Radiate (single wire)	20 MHz	28 MHz	10	50	20
PLC	Conducted (using capacitive coupling board)	20 MHz	28 MHz	10	50	80
Protection Relay	Radiated (using horn antenna)	20 MHz	100 MHz	10	50	15

Image [**?**] xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx

xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

5 Conclusions

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx xxxxx xxxxxxx xxxxx xxxxx xxxx xx

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] 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

[3] 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

[4] 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

[5] 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