HPEM Vulnerability of Smart Grid Substation Secondary Systems

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

Holger Hirsch
Institute of Electrical Power Transmission
University Duisburg Essen
Duisburg, Germany
info@ets.uni-due.de

***Abstract*—This paper presents the results of a test campaign with focus on identifying HPEM susceptibilities for eight different secondary systems used in smart grid substations as part of the SCADA (Supervisory Control and Data Acquisition) system. The devices were tested against conducted threats in a bulk current injection (BCI) setup and radiated threats inside a TEM waveguide. Testing multiple devices of each type from different manufacturers and generations is necessary to acquire a representative overview of typical HPEM (High Power Electromagnetics) susceptibility thresholds of such systems. The tests were performed at frequencies ranging from 10 MHz to 3400 MHz whereas the failure behaviour of the tested devices strongly depends on frequency, polarization of the electromagnetic (EM) field and device type.**

***Index Terms*—High Power Electromagnetics (HPEM), High Power Microwaves (HPM), Intentional Electromagnetic Interference (IEMI), Power Grid, Smart Grid, SCADA, Substation, Secondary Systems**

I. Introduction

The power grid nowadays is one of the most important critical infrastructure for society. The steadily increasing amount of decentralised renewable energy sources presents the grid management with some challenges. An instrument for ensuring a reliable energy supply is the enhancement of the grid and the adjacent grid management system by transforming it into a system with increased intelligence - the smart grid. For the implementation of the smart grid it is essential to integrate more and more electronic control and communication devices which are all connected to the SCADA system. In this paper, we focus on the secondary system devices which are typically installed in substations as part of the SCADA system. Such electronic devices can be potential gateways for EMI (Electromagnetic Interference) and IEMI (Intentional Electromagnetic Interference) [1], [2]. For evaluations of special threat scenarios and for the risk assessment of HPEM threats to power grid substations as well as for the design of suitable countermeasures, it is necessary to gather information about the following aspects:

- HPEM susceptibilities of the SUT (System Under Test) or single DUT (Device Under Test) as part of the SUT.
- Coupling paths into the SUT or DUT for radiated and conducted disturbances.
- Likelihood of a power source being used by perpetrators which is suitable to generate the field strength and signal modulation required for malfunctions.
- Shielding effects of the respective environment.

In the past, we performed first susceptibility tests with focus on easily accessible grid components by investigating smart meters [3]. These devices possess a high susceptibility to HPEM, even though the failure of single such devices or even bigger clusters will have no influence on the integrity of the power grid. In further investigations initial HPEM susceptibility tests of secondary systems, in detail one telecontrol and one protection device, were performed [4]. A generic laboratory setup provided a defined wiring layout and test object arrangement. The tests yielded generally a higher rf (radio frequency) immunity than the smart meter devices, but nevertheless the recorded malfunctions could have a greater impact on the grid management and the power grid itself. After gaining these insights, the same generic laboratory test setup has been investigated in more detail with focus on coupling paths into the System [5]. The dominating coupling path for frequencies below 450 MHz has been determined to be the ethernet cable connected to the telecontrol device as well as the DC supply line feeding the system. Above 800 MHz, the dominating coupling has been determined to be radiated coupling directly into the DUT.

In the present paper, a modified version of the basic laboratory test setup used in [5] is presented which features a new DUT arrangement as well as an optimized wiring layout to reduce the parasitic field coupling into feed lines and ethernet cables connected to the DUT. By using the modified laboratory setup, the HPEM susceptibility of three additional protection devices with varying manufacturer, type and generation as well as one additional next generation telecontrol device have been tested. This widespread DUT portfolio of typically installed secondary systems extended by the DUT tested in [5] provides a solid base for a reliable HPEM vulnerability analysis of smart grid substations. Based on the lessons learned from [5] and the test requirements requested in the IEC 61000-4-36 standard [6], the susceptibility tests performed in this paper focus on:

- Irradiation of a single DUT arranged in 3 different

978-1-4673-9698-1/18/$31.00 ©2018 IEEE

orientations inside the TEM waveguide.
- Bulk Current Injection (BCI) into a wiring harness with supply and communication cabling as part of the SUT at 3 different coupling positions.
- Irradiation of the overall SUT arranged in 3 different orientations inside a TEM waveguide.

The paper is organized as follows. Chapter II introduces the investigated DUT/ SUT as well as the HPEM test environment and HPEM test methodology. The test results are presented and discussed in Chapter III. Chapter IV gives a summary and conclusion.

II. Measurement Setup

A. DUT/ SUT description

The SUT investigated in this paper consists of two different DUT, one protection device in combination with a telecontrol unit. Further elements of the SUT are the required auxiliary equipment to run the DUT in a defined operation mode and a defined interconnecting wiring harness with supply and ethernet cabling connecting the DUT with the auxiliary equipment (see Fig. 1). The arrangement of the SUT is based on the automotive EMC immunity standard ISO 11452-2, which describes test setups suitable for both the intended BCI and TEM waveguide tests. All parts of the SUT are installed on a rigid foam base plate. In Fig. 1, the dimensions of the 50 mm thick base plate are 1 m x 2 m, the wiring harness has one 1.5 m part (long section) and one 0.25 m part (short section), bending in an 90°angle from the long section. The predefined BCI injection setups are at 15 cm (BCI1), 85 cm (BCI2) and 155 cm (BCI3) distance as measured from the closest DUT enclosure.

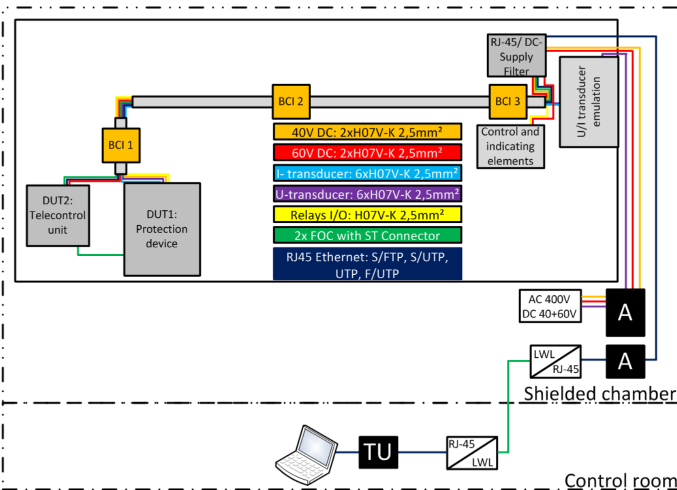

Fig. 1. Overview of the modified SUT structure with A=Artifical network and TU=Telecontrol Unit

All DUT tested in this paper are part of medium and high voltage substation secondary systems. The secondary systems are used to supervise the primary systems and connect them to the SCADA system. Primary systems are the energy-related components in substations, for example power switches, transducers, busbars or transformers. DUT1 are protection devices - programmable logical controller (PLC) which are used to supervise and protect the dedicated primary systems (listed as SG in table I) , and DUT2 are telecontrol units - the interfaces between the SCADA system and the protection devices (listed as FW in table I). Both DUT are arranged on the left side of the SUT with all supply cables connecting the auxiliary equipment arranged on the right side of the SUT with the DUT beeing packed in a defined wiring harness. The aforementioned auxiliary equipment consists of a rf filtered terminal box to reduce the parasitic coupling to the feed lines leaving the SUT, voltage and current transducers and a power switch emulation box. The DC supply for both DUT as well as the Cat. 6 S/FTP (screened foiled twisted pair) Ethernet cable of DUT2 are connected to the terminal box whereas the I/O ports of the protection devices are directly connected to the power switch emulation box and the transducers. The communication between DUT1 and DUT2 is based on a fibreoptic link using the IEC 60870-5-103 protocol. Another major difference between the basic setup used in [5] and the modified setup for this paper is the new ground connection suitable for rf of DUT1 and DUT2. This change is based on typical installation locations for the devices inside switchbays or metal cabinets, both featuring a solid ground connection.

The following table I gives an overview of all investigated DUT and their SUT association, which are either part of the investigations in this paper or which have been tested in [5]:

TABLE I
DUT Overview with SG=protection device and FW=telecontrol unit

DUT	Device Type	Manufac.	SUT	SUT config.
FW1	Telecontrol unit	1	SYS0	basic
FW2	Telecontrol unit	1	SYS1,2,3	modified
SG1	Multi func. prot.	2	SYS0	basic
SG2	Line diff. prot.	2	SYS1	modified
SG3	Distance prot.	2	SYS2	modified
SG4	Distance prot.	3	SYS3	modified

B. HPEM test environment

The following test environments have been used:

- BCI (Clamp Injection) according to IEC 61000-4-6:2007.
- TEM waveguide according to IEC 61000-4-20:2010.

The rf current injection tests are performed using two BCI injection clamps with different frequency responses and the SUT installed on a suitable ground plate. Inside the TEM waveguide the tests have been performed at three different measurement points (MP). The direct coupling tests with the single DUT are performed at MP 7 or MP 8 depending on the dimensions of the DUT. These MP are located in the front section of the waveguide close to the power feed, this section is characterized by a relatively small test volume but high field strength. The investigations of the SUT as a whole were made at MP 2 located in the rear section of the waveguide featuring a larger operating volume but with moderate field strength as a trade-off. As power source for the BCI and TEM waveguide

tests, an HPM oscillator with a maximum power output of 35 kW operating in the frequency range 140–3400 MHz was used. For BCI tests in the frequency range 10–140 MHz a solid state amplifier with 5 kW maximum output power was used. The applied disturbance signal is a pulse modulated cw signal which is typical for narrowband or radar signals with a pulse width of 1 µs and a repetition rate of 1 kHz. The output power follows a ramp function with a runtime of t_r= 20 s, starting at a minimum value as the HPM oscillator needs some excitation for stable operation and ending at the attainable maximum. The same procedure is transferred to the solid state amplifier using a signal generator performing a power sweep. The applied IEMI stress level for all excitation setups was well above typical EMC requirements of 10 V/m. Another important aspect of the tests was a suitable monitoring system. In our case, several cameras were used to observe led indicators and device displays. For communication monitoring, a commercial control software was used which logs the SUT data bus.

C. HPEM test methodology

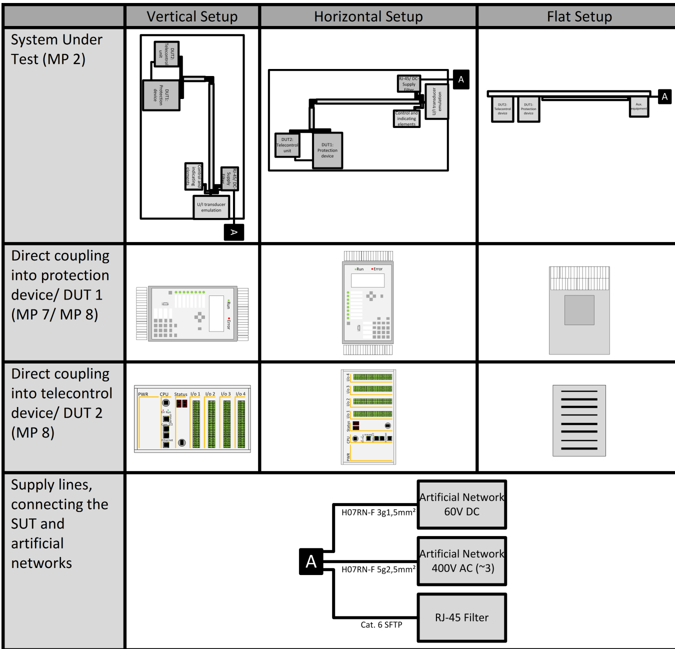

Fig. 2. SUT and DUT orientations for laboratory tests

According to [6] the investigation of different e-field polarizations is required for IEMI testing. Since the perpendicular e-field inside the TEM waveguide is fixed the test sample has to be rotated during the tests. Referring to the tests performed in [5] the DUT and SUT tests in this paper are performed using the same orientations inside the TEM waveguide to ensure the comparability of the results (see Fig. 2). In detail, the following measurements have been conducted with the three orientations for each DUT and SUT as shown in Fig. 2:

1) BCI tests (conducted coupling) of the SUT in the frequency range 10–1000 MHz, with the injection clamps installed at three different positions on the wiring harness (see Fig. 1).
2) Overall SUT tests at MP 2 in the waveguide in the frequency range 140–3400 MHz, illuminating the SUT as whole. (These tests are only performed if the susceptibility threshold limits for the direct coupling tests provide appropriate results with effects caused by moderate field strengths)
3) Tests of direct coupling into DUT1 and DUT2 at MP 7 or MP 8 in the frequency range 140–3400 MHz.

III. Results

The figures in this paper are structured as follows. The frequency is plotted on the x-axis, the electrical field strength or induced current in arbitrary units (a.u.) are plotted on the y-axis, using the same scaling for all TEM waveguide or BCI tests respectively. Small vertical lines above the x-axis indicate the test frequencies. The markers represent the individual failures observed at a given test frequency during the power ramp with the description and affiliation given in table II.

TABLE II
Plot Legend

Marker	Failure description	
▲	Commuication device temporarily disturbed	
●	Communication device disturbed until restart	
△	Protection device temporarily disturbed	
○	Protection device slightly disturbed, automatic restart	
□	Protection device heavily disturbed, manual restart required or power switch trip recorded	
☆	Protection device out of order or significant data lost	
Colour	**BCI-Plot**	**TEM-Plot**
green	BCI1	Vertical
red	BCI2	Horizontal
blue	BCI3	Flat

A. Bulk Current Injection (BCI)

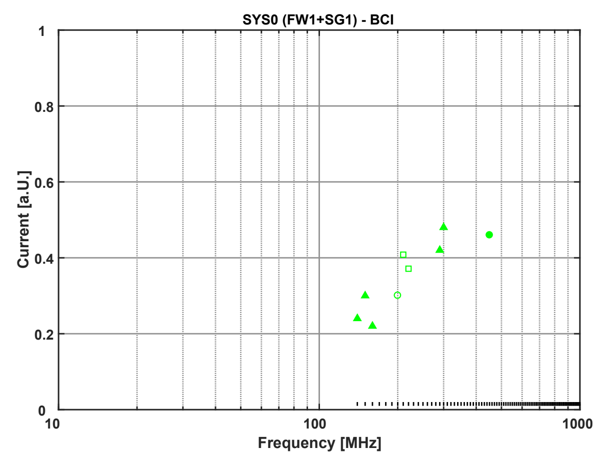

Fig. 3. SYS0 (FW1+SG1) - BCI at one position next to the protection device

In Fig. 3 the results for BCI injection into combined system SYS0 as mentioned in table I, consisting of FW1 and SG1 is shown. The tests were performed in the frequency range

f= 140–1000 MHz, with only few failures of FW1 and SG1 occuring between 140 MHz and 450 MHz.

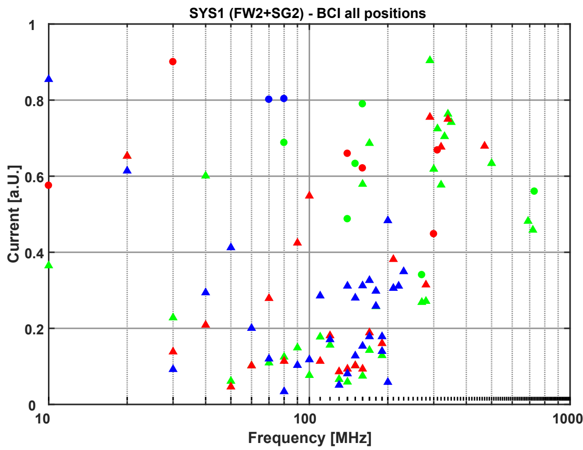

Fig. 4. SYS1 (FW2+SG2) - BCI at three positions

The BCI excitation of SYS1 shown in Fig. 4 resulted in failures recorded for frequencies between 10 MHz and 750 MHz almost for all excitation positions. All failures recorded were caused on the telecontrol unit FW2 with the highest susceptibilities between 30 MHz and 200 MHz, whereas SG2 showed no malfunction at all. Most of the failures recorded for FW2 were minor ones ranging from communication disturbance to signaled malfunctions of I/O ports. Only a few critical failures with device crashes resulting in device restarts occured.

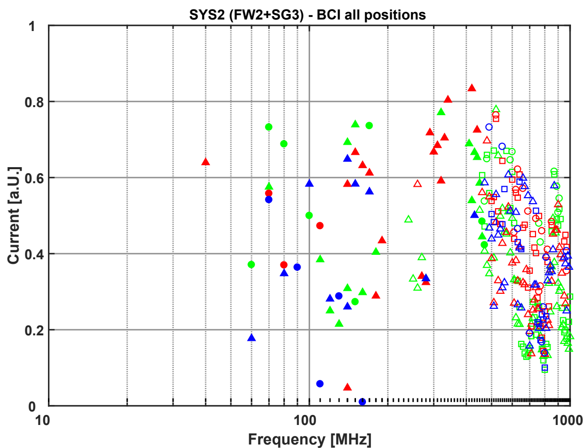

Fig. 5. SYS2 (FW2+SG3) - BCI at three positions

The last BCI excitation tests were performed with SYS2, the results are shown in Fig. 5. FW2 was effected for frequencies below 500 MHz with the highest susceptibilities between 60 MHz and 200 MHz. Effects caused on SG3 were recorded for the frequency range 250-1000 MHz with the highest susceptibilities of all tests above 600 MHz. Unlike the expectations raised on SYS0 and SYS1, the investigation of SYS2 resulted in many very critical failures caused on the protection device SG3 with a noticeable accumulation above 400 MHz. The most critical failures were power switch trips and ongoing malfunctions of the device until it is manually restarted. During this time, the device does not operate and has no protection functionality.

SYS3 could not be tested against conducted disturbances using the BCI injection method because SG4 was damaged in previous direct coupling tests (see Fig. 9).

B. *TEM waveguide direct coupling test of protection devices*

In this section, results are presented for excitation of individual DUT with high field strength in the TEM waveguide.

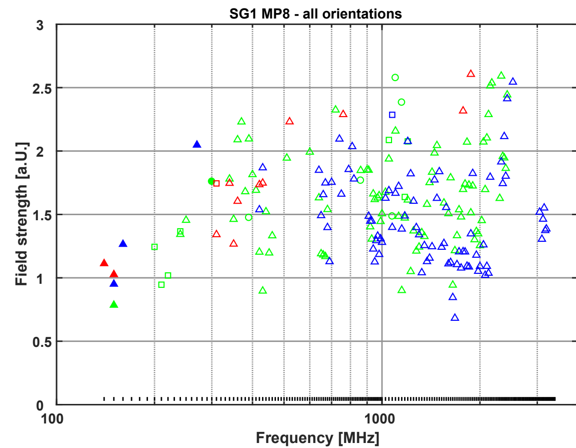

Fig. 6. SG1 - TEM direct coupling with three different orientations

The test results for direct coupling into SG1 are shown in Fig. 6. The tests were performed in the frequency range 140–3400 MHz. The failures were caused on SG1 for frequencies above 200 MHz with a few critical failures occuring between 200 MHz and 1.5 GHz. Most of the failures recorded are temporary display failures or interferences resulting in measurement deviations. There are a few failures recorded for FW1 which has been positioned 2 m apart from the waveguide, in this case the parasitic field of the TEM waveguide suffices to cause failures to the device.

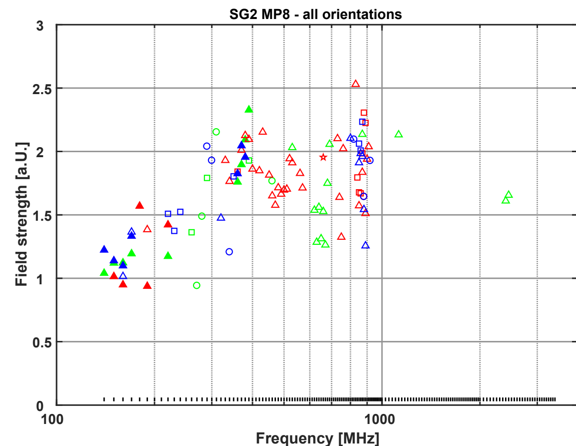

Fig. 7. SG2 - TEM direct coupling with three different orientations

Fig. 7 shows the results for individual excitation of SG2 using direct coupling. Compared to SG1, the threshold limit is slightly higher, which means that the device has a higher immunity to IEMI. Furthermore, most of the failures were

recorded for frequencies between 200–900 MHz and only a couple of failures were recorded for frequencies above 1 GHz. The amount of critical failures compared to SG1 was approximately equal, the greatest difference was one damage recorded for SG2. The device had lost significant system data which had to be uploaded again by the user to reuse the device, in the meantime the device had no functionality and was running in a fallback mode.

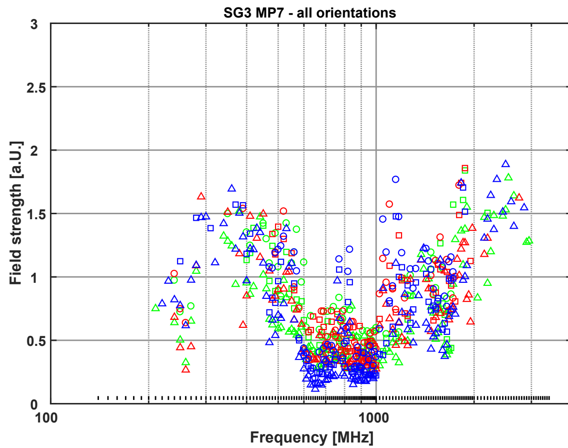

Fig. 8. SG3 - TEM direct coupling with three different orientations

The susceptibility investigation of SG3 against direct coupling is shown in Fig. 8, resulting in large number of failures occuring in the tested frequency range up to 3 GHz, with the highest susceptibility of all tested devices in line with the BCI results. Attention should be paid to the frequency range 600–1000 MHz, featuring the lowest threshold limits and the severest failures. As in the BCI tests, there were a lot of critical effects resulting in power switch trips and malfunctions requiring restart recorded for frequencies below 2 GHz.

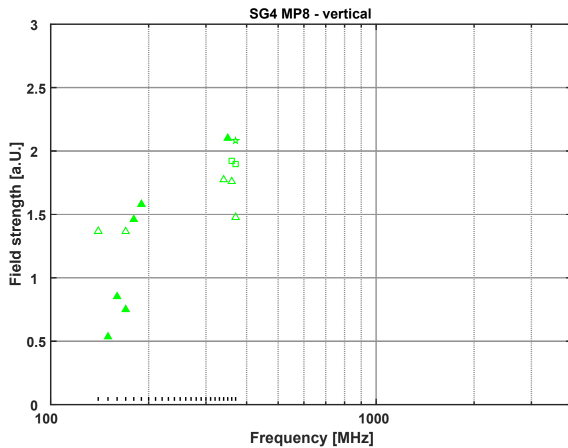

Fig. 9. SG4 - TEM direct coupling with one orientation

SG4 was tested between 140–370 MHz with one device orientation resulting in a broken device (see Fig. 9). The ongoing malfunction has been identified as a hardware error occuring during the selftest routine which is automatically performed by the device when powering up.

C. TEM waveguide direct coupling test of telecontrol devices

In Fig. 10 and Fig. 11 the test results for both telecontrol devices against direct coupled disturbances are presented. FW1 shows failures in the whole tested frequency range between 140 MHz and 3400 MHz, whereas FW2 showed most effects between 300 MHz and 1.8 GHz. The highest susceptibilities of FW1 were recorded for frequencies at 300 MHz and between 1 GHz and 1.5 GHz. FW2 by contrast showed a nearly constant threshold limit for the single device orientation tested so far. The failures recorded for both devices were typically temporary disturbances with communication disruption or I/O port failures, comparable to the results of the BCI tests. Only a few serious failures were recorded, those were manual or automatic restarts of the device.

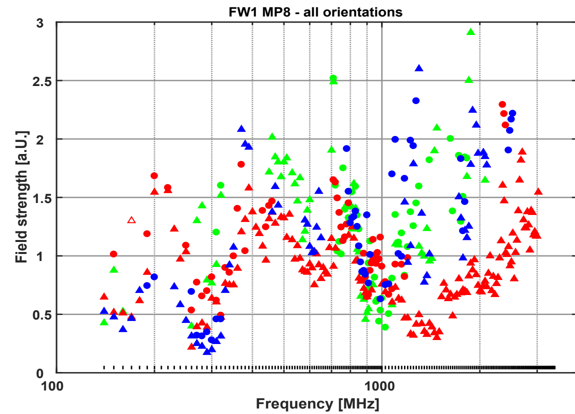

Fig. 10. FW1 - TEM direct coupling with three different orientations

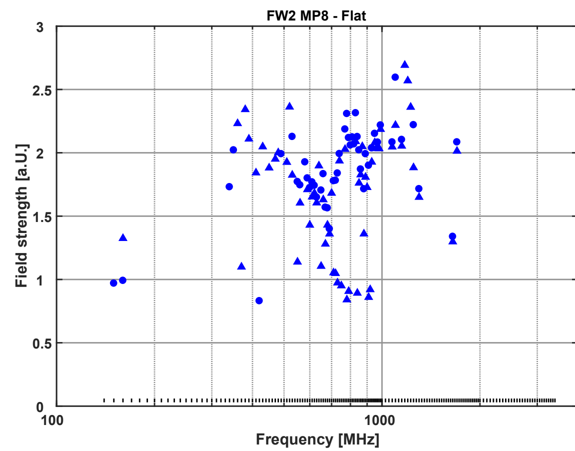

Fig. 11. FW2 - TEM direct coupling with one orientation

D. TEM waveguide system coupling tests

After performing tests on single devices, the susceptibility in a system context was investigated. The global excitation tests with lower field strength were performed for SYS0 and SYS2 inside the TEM waveguide, the results are shown in Fig. 12 and Fig. 13. As expected SYS0 with SG1 and FW1 resulted in failures occuring only for FW1 in the whole tested

frequency range, whereas the field strength did not suffice to cause failures to SG1. The high vulnerability of SG3 has been proven by the tests with SYS2. In line with the results for the BCI and direct coupling tests, SG3 has been massively disturbed again resulting in critical failures for frequencies between 600 MHz and 1900 MHz.

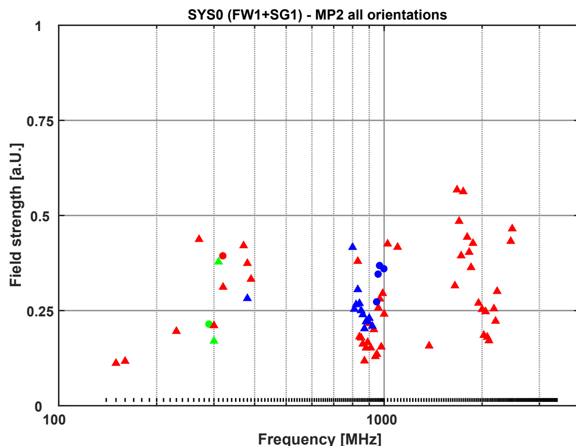

Fig. 12. Sys0 (FW1+SG1) - TEM coupling into the SUT with three different orientations

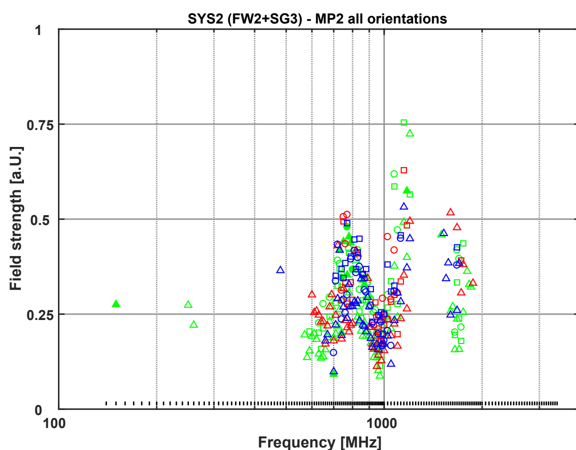

Fig. 13. Sys2 (FW2+SG3) - TEM coupling into the SUT with three different orientations

IV. Conclusion

Altogether a number of 8 different secondary systems used in power grid substations as part of the SCADA system were tested with respect to their susceptibility to HPEM and IEMI threats. All tested devices have shown a susceptibility to HPEM signals in the frequency range between 10 MHz and 3400 MHz. A few critical failures were recorded for the protection devices SG1, SG2 and SG4 in the frequency range 200–1000 MHz. Whereas for SG3 a vast amount of critical failures were recorded for frequencies between 300 MHz and 2 GHz. The investigation with different excitation methods utilizing different coupling paths into the DUT or SUT resulted in similar failure behaviours of each DUT for the various tests performed. The devices feature susceptibilities for both radiated and conducted threats, while the radiated threat has been analyzed by direct coupling into the devices and the conducted threat was simulated by directly injecting the HPEM signal on the wires connected to the DUT.

The recorded failures of the protection devices (SG) range from simple display deviations up to very critical failures affecting the assigned functionality, e.g. power switch trips, malfunctions requiring manual restart or damaged hardware causing a total breakdown. For the telecontrol devices (FW), communication suppression or disruptions as well as ongoing malfunctions until the device has been restarted were recorded. Considering the functionality within the power grid of both tested device types, the malfunctions recorded for the telecontrol devices have a smaller impact on the power grid and the grid management compared to the failures recorded for the protection devices. The failure of telecontrol devices prevents the control center of having access to the connected sensors, surveillance systems and devices, but this information is not essential to operate the grid. The critical malfunctions recorded for the protection devices with power switch trips or loss of the assigned protection functionality until the device is manually restarted or even the total breakdown of such a device could have a massive impact on the power grid. Specifically with regard to the power switch trips which have a direct impact since the attached cables will be cut off from the grid.

So far, only single devices of each category and type were tested. Further tests have to be performed testing additional samples to verify the recorded susceptibility of the protection devices, especially SG3 and SG4.

The determined high vulnerability of secondary systems used in power grid substations is precarious, due to the fact that suitable rf power sources can generate the required field strength from distances beyond some tens of meters. The EMC requirements for these kind of substation devices of 10 V/m or 35 V/m are barely sufficient to protect one of the most important critical infrastructures against HPEM and IEMI threats.

References

[1] D. Nitsch, M. Camp, F. Sabath, J.L. ter Haseborg, and H. Garbe, “Susceptibility of some electronic equipment to HPEM threats“, IEEE Transactions on EMC, vol. 46, no. 3, pp. 380-388, Aug. 2004.

[2] W. A. Radasky, R. Hoad, “An Overview of the Impacts of Three High Power Electromagnetic (HPEM) Threats on Smart Grids“, EMC Europe 2012, Sept. 17-21.2012, ISBN: 978-1-4673-0717-8.

[3] M. Lanzrath, T. Pusch, M. Jöster, M. Suhrke, “HPEM-Empfindlichkeit von intelligenten Stromzählern als Komponenten des Smart Grid“, EMV Düsseldorf 2016, 23.-25.02.2016, VDE-Verlag, ISBN: 978-3-86359-396-4, pp. 11-17.

[4] M. Lanzrath, T. Pusch, M. Jöster, M. Suhrke, Ch. Adami, “HPEM Vulnerability of Substation Control Systems as Components of the Smart Grid“, Future Security 2016, Berlin, 13.-14.09.2016, Fraunhofer Verlag, ISBN: 978-3-8396-1011-4, pp. 123-130.

[5] M. Lanzrath, T. Pusch, M. Jöster, M. Suhrke, C. Adami, B. Jörres, G. Lubkowski, “HPEM Vulnerability of Smart Grid Substations - Coupling paths into typical SCADA devices“, EMC Europe 2017, Angers, 04.-09.09.2017, ISBN:978-1-5386-0689-6.

[6] IEC 61000-4-36:2014, “Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques - IEMI immunity test methods for equipment and systems“.