HPEM Vulnerability of Smart Grid Substations

Coupling paths into typical SCADA devices

M. Lanzrath, C. Adami, B. Joerres, G. Lubkowski, M. Joester, M. Suhrke, T. Pusch
Electromagnetic Effects and Threats
Fraunhofer INT
Euskirchen, Germany
Marian.Lanzrath@int.fraunhofer.de

***Abstract*—This paper presents the results of a test campaign meant to determine coupling paths into a laboratory test setup of typical power grid substation electronics. The devices were tested against conducted threats in a bulk current injection (BCI) setup and radiated threats inside a transverse electromagnetic (TEM) waveguide as well as with a near-field TEM horn antenna. The various excitation methods and different test setups offer the possibility to trace back the observed effects to coupling paths into the tested system. For frequencies below 300 MHz the dominating coupling path to the system under test (SUT) was determined to be the Ethernet cable connected to the telecontrol device. Above 800 MHz direct radiated coupling into the test devices was identified to be dominating. The conducted coupling via a predefined wiring harness with supply cabling was less relevant for both selected substation devices.**

Keywords—Intentional Electromagnetic Interference (IEMI); High Power Electromagnetics (HPEM); Coupling Path; High Power Microwaves (HPM); Smart Grid; SCADA

I. Introduction

The power grid, enhanced to be a Smart Grid in the future, is one of the most important critical infrastructures for society. The additional varying decentralized feed-in of renewable energies complicates regulation and management of the grid. As a consequence, more and more electronic control and communication systems (Supervisory Control and Data Acquisition System, SCADA) are integrated to support the grid management. These devices can be considered as gateways for EMI (Electromagnetic Interference) and IEMI (Intentional Electromagnetic Interference) [1], [2]. Initial investigations of smart meter devices showed their high susceptibility to HPEM [3]. On the other hand, the failure of single such devices or even clusters has no effect on the power grid as a whole [3]. The tests of smart meters [3] provided first predictions of coupling paths into systems realized with these components together with a generic wiring similar as in earlier tests of media converters [2]. The results of studies concerning coupling paths into a generic office wiring setup showed that the direct coupling through device housing apertures becomes dominant for frequencies above 2 GHz [4]. For the smart meter tests, the cross over frequency between direct and cable coupling domination was noticed to be slightly above 1 GHz [3]. For the media converters a comparable frequency range for direct and cable coupling has been determined [2].

As subjects to further investigations concerning the power grid and coupling paths into a generic system model, important power grid components were focussed upon which are typically installed in substations. Initial individual susceptibility tests of the substation electronics [5] showed generally a higher rf (radio frequency) immunity than the smart meter tests. However, the recorded malfunctions of these devices could have a greater impact on the power grid management as they are part of a power grid distribution node.

Aspects relevant for the assessment of HPEM threat scenarios as well as for the design of suitable countermeasures are the following:

- HPEM susceptibilities of the SUT 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

This paper presents investigations intended to provide a better insight into potential coupling paths into a generic SUT designed to mimic a real setup but nevertheless arranged for laboratory IEMI tests. Typically, coupling paths are classified into front- and backdoor coupling. Frontdoor coupling of EM (Electromagnetic) waves takes place at antennas of the DUT e. g. for communication services. On the other hand, backdoor coupling is related to EM waves interacting with attached supply or communication cables or coupling directly into internal circuits through apertures in the DUT casing. The investigated SUT in this paper consists of substation protection and telecontrol units connected by appropriate cabling as discussed in [5]. The investigations comprise testing of various excitation setups differing in dominant coupling paths, namely

- Irradiation of the overall SUT in different orientations inside a TEM waveguide,

- Irradiation of a single DUT in different orientations inside the TEM waveguide,
- Bulk Current Injection (BCI) into a wiring harness with supply cabling as part of the SUT as well as single cables connected to the DUTs,
- Local irradiation of parts of the SUT with a near-field TEM horn antenna,
- Irradiation of the overall SUT inside the TEM waveguide after setup changes and focussed EMI countermeasure deployment.

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

II. Measurement setup

A. DUT/ SUT description

The investigated SUT consists of two different DUT, the auxiliary equipment to run the DUT in a normal operation mode and a defined interconnecting wiring harness with supply cabling (see Fig. 1). The arrangement of the SUT is based on the standard ISO 11452-2. The test setup described in this automotive EMC immunity test standard is suitable for both the intended BCI and TEM waveguide tests. All parts 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 1.5m part (long section) and two 0.25m parts (short sections), bending in a 90° angle from the long section.

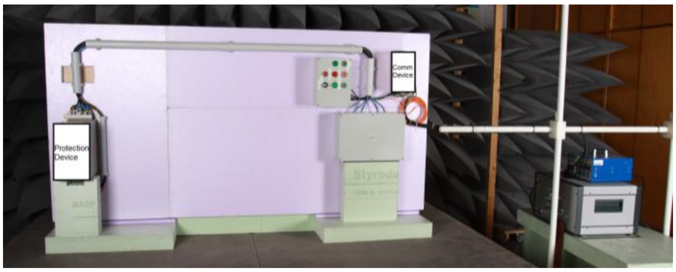

Fig. 1: Investigated SUT structure installed at MP 2

The DUT 1 arranged on the left side of the SUT is a PLC (programmable logical controller) which operates as a protection device in the substation, with the purpose to protect the controlled power switch. The DUT 2 is placed on the right side of the SUT, this device is a telecontrol unit which allows the control centre to receive measurement data and to send switching commands to the protection device. Furthermore, these devices offer the possibility to attach certain sensor contacts, e. g. switched off fuses or access controls. The control elements and indicators as well as the emulated voltage and current transducers are installed on the right-hand side of the SUT next to the telecontrol device (DUT 2). This setup is meant to emulate the physical separation of the protection device, the sensors and the actuators inside the switch bay. All necessary wire connections are realized with single PVC (Polyvinyl Chloride) coated copper wires having a 2.5 mm² cross-section. The telecontrol units are typically installed in separately located racks and connected via FOC (fibre optical cable) to the protection devices. The only copper wire connections between DUT 1 and DUT 2 are the supply voltage lines (60 V DC), this setup being an emulation of a realistic scenario where both units are connected to an UPS (Uninterruptible Power Supply). The supply lines for the SUT are brought in from the right side and are connected to artificial networks and filters outside the waveguide. The wires consist of one 400 V AC feedline for the transducer box and one feedline for the 60 V DC grid on the SUT. The last wire is a Cat. 6 S/FTP (screened foiled twisted pair) cable connecting DUT 2 to a fibre optic converter positioned outside the waveguide. This Ethernet connection is used to control and monitor the SUT from outside the shielded enclosure.

B. HPEM test environment and DUT monitoring

The following test environments have been used:

- BCI workstation according to IEC 61000-4-6:2007
- TEM waveguide according to IEC 61000-4-20:2010 with a field homogeneity according to IEC 61000-4-3:2006
- Near-field TEM horn antenna for the homogenous illumination of a small, defined area.

Inside the TEM waveguide the tests are realized at two different measurement points (MP). The investigations of the complete SUT are made at MP 2, in the rear section of the waveguide featuring a larger operating volume, with moderate field strength as a trade-off. The direct coupling tests with the single DUT are performed at MP 8, in the front section of the waveguide close to the power feed. This measurement point is characterized by a relatively small test volume but higher field strengths than MP 2. The investigations with the near-field antenna are performed in front of an anechoic wall. 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 MHz - 3400 MHz is used. The applied pulse modulated signal represents a typical narrowband or radar signal 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 a stable operation and ending at the attainable maximum. For the near-field antenna tests TWT (Travelling Wave Tube) power amplifiers are used as a power source, generating the same signal form as the HPM oscillator and field strengths similar to those obtained in the waveguide.

Another important aspect of the tests is a suitable monitoring system. In our case, several cameras are used to observe led indicators and device displays. For communication monitoring, a commercial control software is used which logs the SUT data bus.

C. Test methodology

For the HPEM tests of the SUT inside the TEM waveguide at MP 2 three different general setups were defined (see Fig. 2). The leading criterion was the orientation of the wiring harness with respect to the main EM field component inside the TEM waveguide. According to the IEC 61000-4-36:2014 standard, the various wire sections of the wiring harness are characterized by the optimum coupling at different frequency ranges with c_0 being the speed of light, f_h the upper cut-off frequency and f_L being the lower cut-off frequency:

$$f_L \approx c_0/4L < f_{res} < f_h \approx 5c_0/L \tag{1}$$

For low frequencies the coupling diminishes as the cable becomes electrically short. For high frequencies, it becomes less important due to the rising frequency dependent attenuation of the applied low voltage power cable.

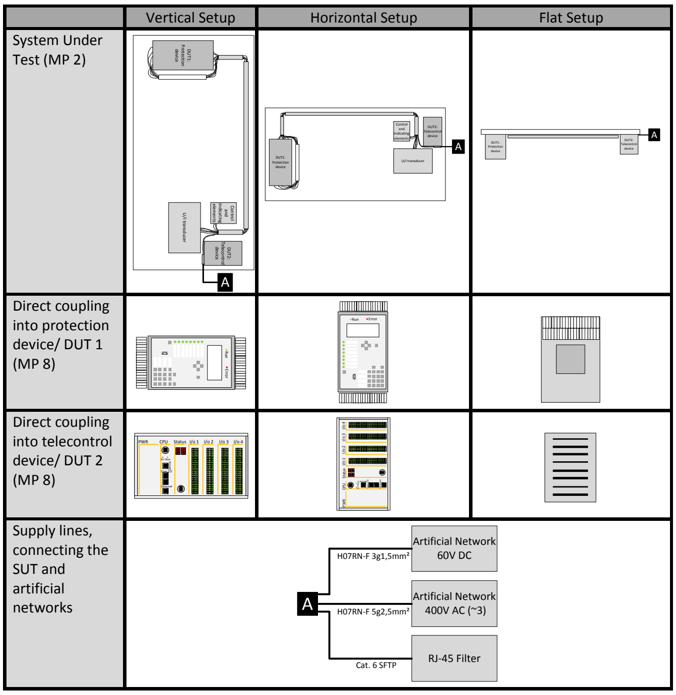
Vertical Setup
Horizontal Setup
Flat Setup
System Under Test (MP 2)
Direct coupling into protection device/ DUT 1 (MP 8)
Direct coupling into telecontrol device/ DUT 2 (MP 8)
Supply lines, connecting the SUT and artificial networks
A
H07RN-F 3g1,5mm²
Artificial Network 60V DC
H07RN-F 5g2,5mm²
Artificial Network 400V AC (~3)
Cat. 6 SFTP
RJ-45 Filter

Fig. 2: Investigated system and device orientations

Based on the effective coupling frequency range and different coupling strengths of low voltage power cables inside the waveguide depending on the cable arrangement [6], three different orientations of the SUT were chosen:

- **Vertical orientation**: long wire section parallel to the main EM-field component inside the waveguide. According to (1) the resonance effects are expected in the frequency range 50 MHz - 1 GHz.
- **Horizontal orientation**: short wire section parallel to the main EM-field component inside the waveguide. According to (1) the resonance effects are expectable in the frequency range 300 MHz - 6 GHz.
- **Flat orientation**: no wire section parallel to the main EM-field component inside the waveguide.

The same device orientation assignment is used in the study of the direct coupling to DUT 1 and DUT 2 at MP 8 (see Fig. 2). The following measurements have been conducted for the three orientation setups shown in Figure 2:

(1) Transfer function measurements for the SUT at MP 2 in the waveguide, in the frequency range 10 MHz - 2500 MHz. The rf current has been measured with a probe positioned on the wiring harness 5 cm next to DUT 1.

(2) BCI tests (conducted coupling) of the SUT in the frequency range 140 MHz - 1000 MHz.

(3) Overall SUT tests at MP 2 in the waveguide, with the focus on the field coupling to the wiring harness in the frequency range 140 MHz - 3400 MHz.

(4) Tests of direct coupling into DUT 1 and DUT 2 at MP 8 in the frequency range 140 MHz - 3400 MHz.

(5) Illumination of parts of the SUT with the near-field TEM horn antenna [7]. The illuminated area is approximately 20 cm x 20 cm and the dominating field component is parallel to the one in the TEM waveguide. The tests were performed in the frequency range 800 MHz - 6000 MHz at a total of 15 illumination positions distributed over DUT 1, DUT 2 and the wiring harness (see Fig. 3).

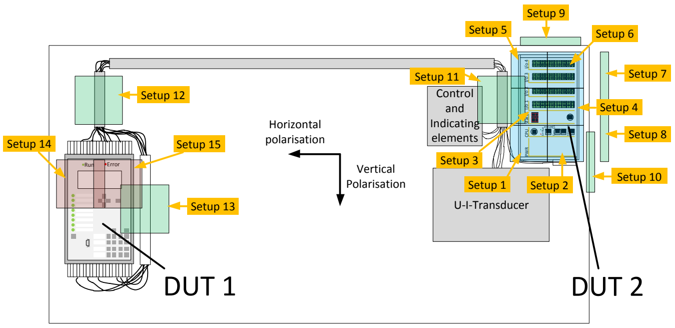

Fig. 3: Test setups for near-field antenna tests

In addition to the above mentioned tests some extra investigations have been performed for the most interesting frequency ranges or setups. One example for additional tests is the layout variation of the wiring harness with fixed DUT positions in combination with single DUT rotations at MP 2. Furthermore, tests were done with integration of ferrite sheath current filters to the RJ-45 Ethernet communication cable connected to DUT 2.

III. Results

A. Transfer functions

Fig. 4 shows the results of transfer function measurements for all three orientations at MP 2. The coupling into the SUT shows no trend up to 300 MHz, followed by a steady decrease till 2.5 GHz. A variety of resonance frequencies corresponding to the different wiring harness sections are identifiable and in compliance with calculated frequencies.

There is no difference in the order of magnitude of the induced current for the three experimental configurations. As expected, the flat setup shows the lowest coupling over nearly the whole tested frequency band. The best coupling to the EM field inside the waveguide is found in the horizontal setup. The results show that the estimation for optimum coupling for isolated cables represented by Eq. (1) is too simplified to be applicable to our test setup. The order of magnitude of the transfer functions allows an explicit comparison of the coupling magnitudes of radiated and conducted disturbances, a current of 1 a.u. corresponding roughly to a field strength of 5 a.u. An additional cause for the observed relative magnitudes of the transfer functions and in particular for the prevalence of the horizontal over the perpendicular setup is the difference in coupling efficiency between the short section (primary cable part) and the long section (secondary cable part) seen from the device (cf. [8]).

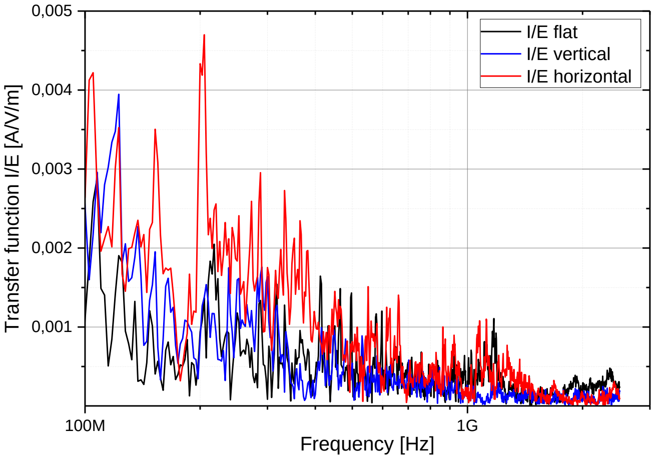

Fig. 4: Transfer functions at MP 2 for all setups

B. *BCI tests*

In the following figures 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. The small vertical lines above the X-axis indicate the tested frequencies. The shaded area represents the tested range of field strengths for each frequency. The markers indicate the individual failures observed at a given test frequency during the power ramp.

The BCI excitation of the wiring harness with the clamp positioned 15 cm next to DUT 1 and of a 2 m generic Ethernet cable connected to DUT 2 with the clamp positioned 0.9 m (Fig. 5 Pos1) and 1.1 m (Fig. 5 Pos2) next to DUT 2 resulted in failures of DUT 2 concentrating on frequencies below 450 MHz (see Fig. 5). However, the direct injection into a generic 0.6 m DC supply line connected to DUT 2 with the clamp positioned 15 cm next to the DUT resulted in failures occurring in the whole tested frequency range. With respect to the deviations between the test results for generic DC supply line and wiring harness note, that the two arrangements own different configurations e.g. of wiring layout, of junctions as well as of connected devices. Regarding DUT 2 a significant susceptibility against conducted disturbances is observable for frequencies below 450 MHz. DUT 1 shows failures, however, only for frequencies in the region of 200 MHz together with higher failure threshold levels compared to DUT 2.

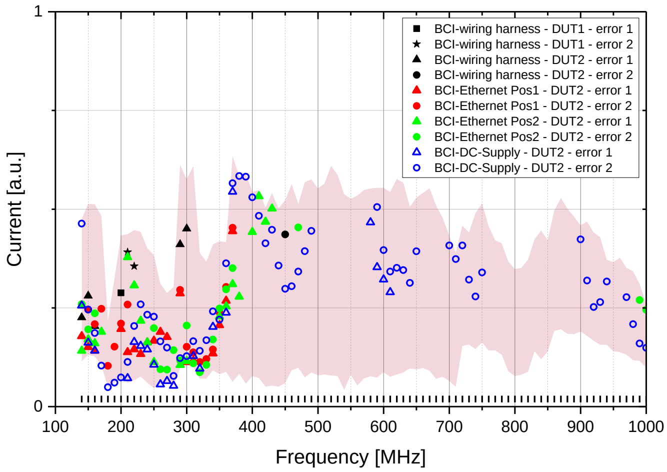

Fig. 5: BCI test results

C. *TEM waveguide tests*

Fig. 6 shows the test results of the overall SUT for all three orientations at MP 2 inside the waveguide. The marker colors in this plot correspond to the colors of the transfer functions for the respective orientations presented in Fig. 4.

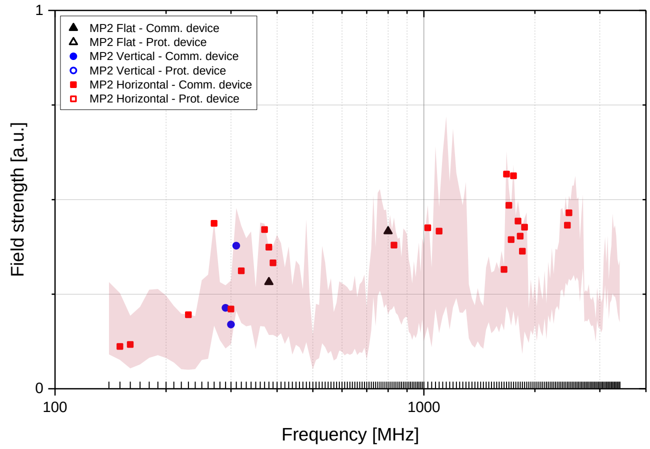

Fig. 6: MP 2 all SUT setups

All failures recorded during the tests at MP 2 are related to the telecontrol device (DUT 2). The protection device (DUT 1) shows no malfunctions. An interesting observation is that the vertical setup and the flat setup only show a few disturbances for the SUT. In contrast, the horizontal setup results in most of the failures, being spread nearly over the whole tested frequency range.

The initial tests of the SUT with BCI and field coupling tests at MP 2 inside the TEM waveguide showed a marked susceptibility of both DUT for low frequencies. As a next step for the determination of coupling paths into the SUT, each single DUT has been tested for direct coupling at MP 8 inside the TEM waveguide revealing failures for both DUT in the whole investigated frequency range. In particular, DUT 2 features some sensitive frequency ranges, depending on orientation. Fig. 7 gives an example for the horizontal orientation of the SUT at MP 2 and the appropriate orientation of DUT 2 at MP 8 together with the tested power range for

MP 2 (shaded red) and MP 8 (shaded blue). One can recognize comparable test results for threshold values and error patterns in regions with overlapping test parameters. DUT 2 is most susceptible at low frequencies between 150 MHz and 300 MHz (coupling via Cat. 6 Ethernet cable, see Section III.E) and between 1 GHz and 1.2 GHz.

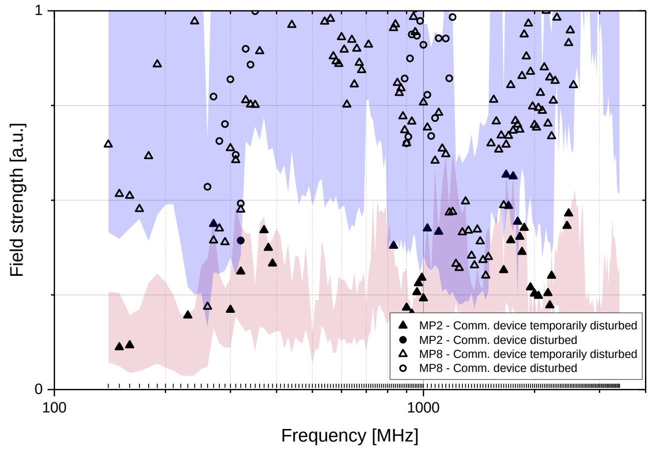

Fig. 7: Telecontrol device horizontal setup at MP 2 (shaded red) and MP 8 (shaded blue)

Direct coupling tests with DUT 1 at MP 8 (results shown in [5]) indicate a high immunity of the device, with failures occurring only in the last quarter of the power ramp. Correspondingly, the field amplitudes at MP 2 do not suffice to cause failures to DUT 1 - neither by coupling into the wiring harness nor by direct coupling into the device.

D. Near-field TEM horn antenna tests

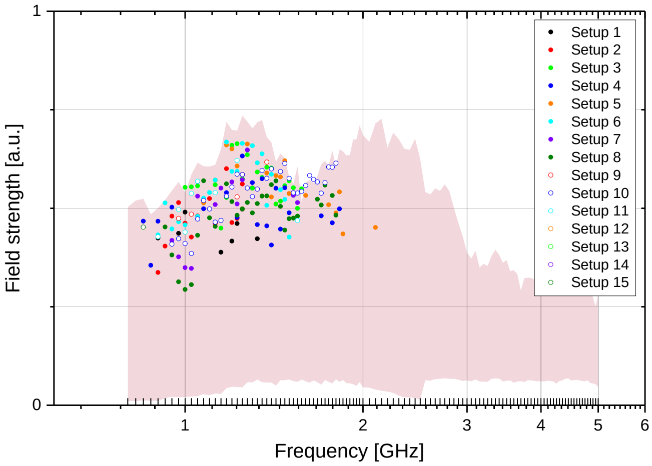

Fig. 8: Near-field antenna tests. For setups see Fig. 3

Fig. 8 shows the test results for all near field TEM horn antenna measurements without distinction between different EM field polarizations and error patterns. All of the recorded failures are captured in the frequency range 900 MHz - 1900 MHz. The determined threshold levels are comparable to the levels collected for the tests at MPs 8 and 2 (Fig. 6 and Fig. 7). The distribution of failures is roughly similar for setup 1-11 (see Fig. 3), varying slightly in amplitude and frequency range.

The analysis of test setup 1-6 with focus on the EM field polarization shows a preferred orientation for disturbances of the telecontrol device for a polarization equal to the horizontal SUT orientation in the TEM waveguide. An example is given by the test result for Setup 4 in Fig. 9. The plot shows the DUT reacting in a wider frequency range to the disturbance signal with the DUT illuminated comparable to the horizontal SUT setup in the TEM waveguide.

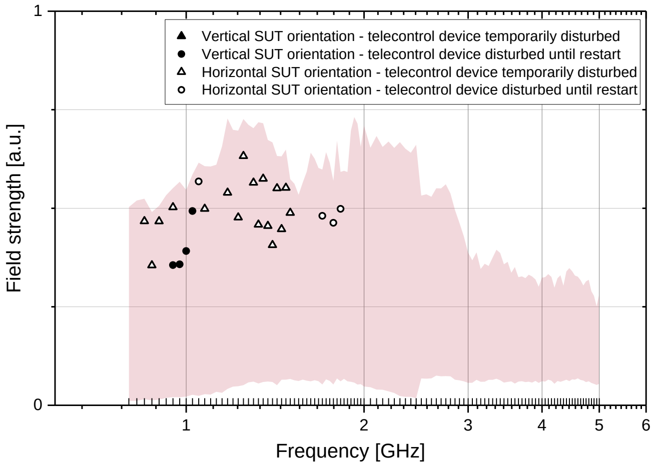

Fig. 9: Near field antenna test - Setup 4

The local coupling to both devices with the near field antenna yields the same results with similar susceptibilities as for global coupling in the TEM waveguide for frequencies above 800 MHz.

An interesting effect observed during the near field antenna tests was the possibility to test the failure mechanism of the DUT. These are typically seen to be related to either the incorporated rf energy, the amplitude of the EM field or the parameters of an applied signal modulation. With setup 14, the DUT 1 showed no effects with the pulse modulated signal (duty cycle 0.1 %). The change to a cw (continuous wave) signal exposed a high susceptibility for frequencies up to 1500 MHz with low threshold values below 1 GHz. This implies that the failures are not caused by the pulse modulation parameters but through the incorporated rf energy.

E. Additional detailed investigations

Conclusive information on the coupling paths can be derived from additional investigations of the SUT, for instance from tests with different wiring harness orientations and fixed DUT positions. Another option is the deployment of ferrite sheath current filters to the Cat. 6 S/FTP Ethernet cable connecting DUT 2 to the media converter outside of the waveguide.

The results for the test series focussed on changing only a single parameter at a time in the horizontal setup at MP 2 are shown in Fig. 10. The two plots on the left-hand side show the difference between changing the orientation of the wiring loom with the rest of the SUT remaining fixed. The upper left plot shows the normal configuration as initially tested, the lower left plot shows the result for the wiring harness turned by an angle of 90° into the same orientation as for the flat setup. The recorded failure thresholds are comparable to the results of the SUT tests at MP 2 (see Fig. 7), the change of the wiring harness resulting in no remarkable differences. On the other hand, the two plots on the right-hand side indicate a significant difference to the plots on the left-hand side. These two plots show the test result for DUT 2 rotated by an angle of 90° retaining the wiring harness configurations from the left-hand side. It is obvious that the failures are connected to DUT 2. The coupling path does not seem to be direct coupling into the device as the threshold levels for a direct coupled disturbance tend to be higher than the levels recorded for the SUT tests at MP 2 or the results given in Fig. 10.

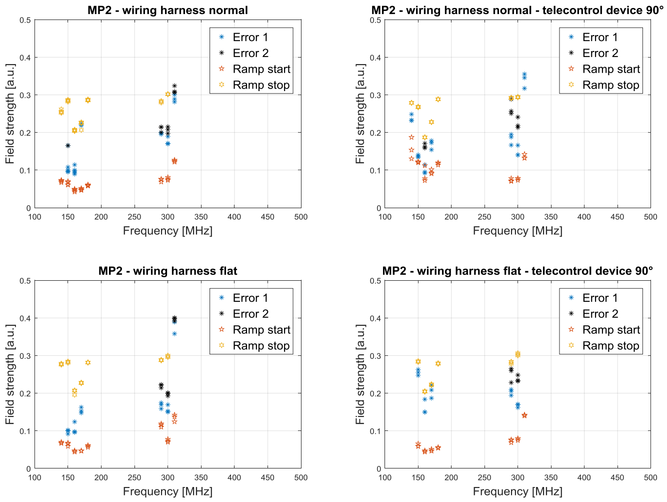

Fig. 10: Impact of sole change of cable orientation for MP 2 horizontal setup

As both Ethernet and DC supply cables are potential coupling paths for lower frequencies, further tests are performed with focus on implementing countermeasures inside these paths in order to make a clear distinction. The sheath current filters deployed at the Cat. 6 Ethernet cable completely eliminates the failures occurring in this frequency range. This failure behavior implies that the coupling to the tested system configuration happens via the Ethernet cable connecting DUT 2 to the media converter outside the waveguide. The recorded failures during the system tests manifested a high sensitivity for frequencies below 300 MHz depending strongly on the specific wiring layout of the Ethernet cable with minor changes resulting in a large impact on the failure threshold level.

IV. Conclusion

Different rf illumination methods of a test setup of typical substation devices of the Smart Grid have been used in order to identify coupling paths into the overall system. The protection device (DUT 1) showed a high immunity to conducted and radiated disturbance signals. In contrast, the telecontrol device (DUT 2) is particularly susceptible to direct coupling into the housing and via cables connected to the device. The high susceptibility of the telecontrol device is remarkable in so far as these devices are an integral part of the Smart Grid concept. Compared to the smart meter devices [3], the substation electronics in general possess a higher resilience to IEMI. Unlike the former, no substation device showed permanent failures after testing and higher field strengths are needed for inducing failures at all.

The conducted coupling via the predefined wiring harness with supply cabling is less relevant for both chosen substation devices. In comparison with the global illumination of the setup in the TEM waveguide, the tests of both devices alone with the near-field TEM horn antenna show that the coupling is predominantly local. Furthermore, it is possible to evaluate polarization dependencies of a DUT as for the performed tests the telecontrol device shows malfunctions strongly depending on the applied EM field polarization. For frequencies below 450 MHz the dominating coupling path has been identified as the Ethernet and DC supply cables connected to the telecontrol device. The dominating coupling path for frequencies above 800 MHz has been determined to be direct coupling into the telecontrol device.

In summary, Smart Grid substation control units have been shown to be remarkably susceptible to IEMI. It could be seen, however, that well-implemented protection measures help to reduce this susceptibility and with that the IEMI vulnerability of the Smart Grid.

Acknowledgement

The authors would like to thank Dr. R. Heinrich (Teseq Company) for providing the near-field antenna for this test campaign.

References

[1] 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.

[2] C. Adami, C. Braun, P. Clemens, M. Jöster, M. Suhrke, H.-J. Tänzer, "High Power Microwave Tests of Media converters" EMC-Europe 2012 Rome, ISBN: 978-1-4673-0718-5.

[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] N. Mora, I. D. Flintoft, L. Dawson, J. F. Dawson, F. Rachidi, M. Rubinstein, A. C. Marvin, P. Bertholet, M. Nyffeler: "Experimental Characterization of the Response of an Electrical and Communication Raceway to IEMI" IEEE Transactions on Electromagnetic Compatibility, Vol. 58, No. 2, April 2016, pp. 494- 505

[5] 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.

[6] R. Kichouliya, M.J. Thomas: "Interaction of High Power Electromagnetic Pulses with Power Cables and Electronic Systems", IEEE 2016, ISBN: 970-1-5090-1442-2

[7] R. Heinrich, H. Hirsch: "*Untersuchung zu TEM Hornantennen für Störfestigkeitsprüfungen im Nahbereich*", EMV Düsseldorf 2016, 23.-25.02.2016, VDE-Verlag, ISBN: 978-3-86359-396-4, pp. 87-94

[8] D. Zamow, D. Hamann, E. Genender, H. Garbe: „*On Estimating the Directivity of Electrically Large Cable Dominated Desktop Systems*", EMC Europe 2011, York, UK, September 26-30.2011, pp. 482-487