High Power Microwave Susceptibility of IT Network Components

C. Adami, C. Braun, P. Clemens, H.-U. Schmidt, M. Suhrke, H.-J. Taenzer, U. Weber
Fraunhofer INT, Appelsgarten 2, 53879 Euskirchen, Germany

1. Abstract

As an illustration of the threat of high power microwaves (HPM) to critical civil infrastructure we show electromagnetic susceptibility tests of commercial IT network components with HPM pulses in the frequency range between 150 MHz and 3.4 GHz. In our facility electric field strengths up to 1 kV/m can be achieved at the position of the test objects for pulse lengths between 250 ns and 15 µs and pulse repetition rates between 1 Hz and 10 kHz. The test setup consists of two PCs connected with twisted pair cable over a hub or a switch as typical IT network components. Network traffic is realized by file transfer between both PCs. As an option, a part of the data connection is implemented with fibre optic cable and media converters. The main coupling of fields to network components takes place via attached cabling and is most effective for the lowest frequencies. For the majority of the tested equipment failures can be induced already at fields of some 100 V/m for frequencies above 200 MHz and at some 10 V/m below 200 MHz. The use of shielded cables clearly reduces the malfunctions. The media converter can be identified as another important source of failure. Our results give hints on protection measures of IT infrastructure against the HPM threat.

2. Introduction

The HPM threat as a part of the so-called Intentional Electromagnetic Interference (IEMI) to critical civil infrastructure by terrorism or crime is getting more and more dangerous with ongoing technological development and with the worldwide spread of knowledge and technology. On one side increasingly powerful HPM sources become commercially available and on the other side potential targets become more vulnerable due to the growing dependence of our modern society on electronics which in its current digital variant is inherently more susceptible to HPM than older analogue electronics. Though the commercial-of-the-shelf (COTS) electronic equipment usually obeys the electromagnetic compatibility (EMC) regulations it is generally not hardened against the much higher electromagnetic fields which are subject of the HPM threat. Possible threat scenarios range from blackmail and cause of economic losses over obstruction of security agencies and public authorities to creation of panic and mass hysteria. Covert operations are possible since usually there are no means for detection of this threat. The openness of our civil society makes such attacks even easier.

As an important example for critical infrastructures we chose IT networks used now in many places for communication and control. We concentrate on commercial network devices as key components of those networks. From our test results on their susceptibility one can draw conclusions for HPM protection of the IT infrastructure.

In addition to microwave susceptibility tests of stand-alone PCs (see e. g. [1,2]), increasing attention has been paid to computer network equipment recently [2-6]. A computer network is characterized by the hardware as well as which connection method is used. A local area network (LAN) generally is composed of more than two computers linked together by twisted pair cables over a switch or hub operated with the Ethernet standard.

Twisted pair (TP) cabling uses eight conductors which are wound together in pairs for the purpose of cancelling out electromagnetic interference from external sources and crosstalk from adjacent wires. A significant feature is the kind of screening of the cable pairs or the whole cable to enable additional shielding against external fields. The elementary components of a network are hubs and switches. Sometimes media converters are used between electrical and optical interfaces.

In general, susceptibility tests are carried out to determine whether or not a device or system is capable of functioning without degradation of performance in the presence of disturbing external influences. The experiments have been carried out in our TEM waveguide. It can be used to determine transfer functions of a system if fed in by a continuous wave (CW) source. Connected to our high power pulsed signal source we are able to conduct susceptibility measurements with pulse lengths and repetition rates (PRF) of 0.25-15 µs and 1-10000 Hz, respectively.

By means of the susceptibility tests answers should be obtained to the following issues:

- Dependence on cabling and cable type
- Dependence on disturbing field parameters
- Induced cable currents
- Dependence on network component and data transfer rate.

It is difficult to assess the susceptibility of network components in a computer network, because the vulnerability of the computer is in the same order as of the device under test (DUT). Whenever an effect is observed it will be determined if it is self-correcting or requires manual intervention:

- Interference: effect only present during illumination
- Disturbance: during illumination and short time after
- Upset: requires manual intervention to correct.

At damage the hardware must be replaced or the software must be reloaded.

3. Test Setup

Based on a simple LAN we developed the test setup shown in Fig.1. It consists of two computers linked together via twisted pair cables and the network component to be tested. The cables form a loop with a circumferential length of about 4 m (3m+1m) and an effective loop area of 1.4 x 0.3 m^2. Only this loop with the connected DUT is irradiated with the interference field whereas the remaining parts and the computers are outside the illumination area.

As network components we selected one hub, five switches and one media converter. The power cords of these devices were in each case aligned perpendicular to the electric field to minimize radiative coupling to these cables. In the following the tested devices are specified:

- Hub: 10 Mbit/s hp J3188A (16-port)
- Switches:
    - 10 Mbit/s Cisco Catalyst3000 (16-port)
    - 10/100 Mbit/s Cisco Catalyst2900XL (22-port)
    - 10/100 Mbit/s Netgear FS-105 (5-port)
    - 10/100/1000 Mbit/s level1 GSW-0502T (5-port)
    - 10/100/1000 Mbit/s Netgear GS-608 (5-port)
- Media converter: 10/100 Mbit/s Lindy MMF (1-port).

For the connecting TP cables we used the following types:

- U/UTP-Cat.5e (unshielded)
- U/UTP-Cat.6 (unshielded, but spacer between pairs)
- F/UTP-Cat.5e (shielded with foil around pairs)
- S/FTP-Cat.6 (braided screen and foil around each pair).

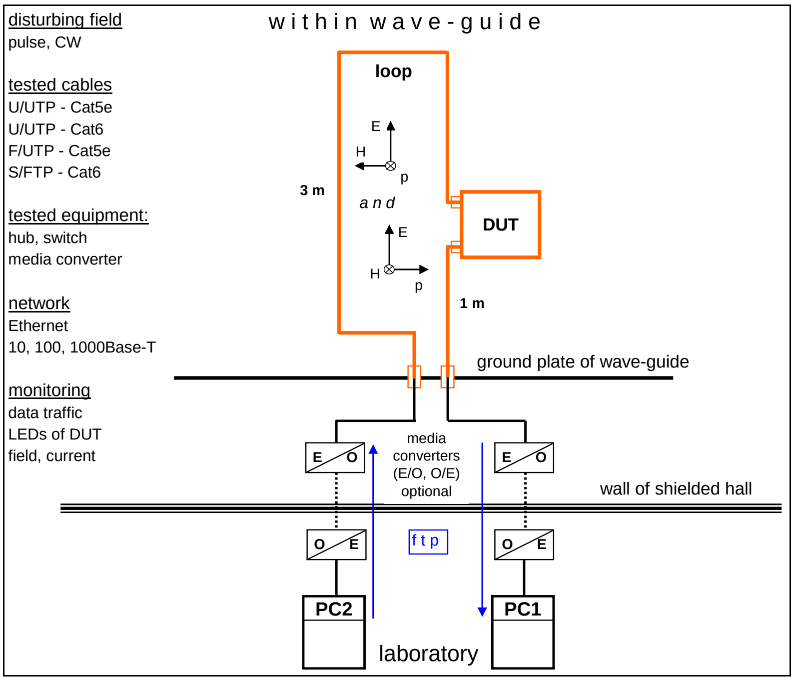

Figure1: Schematic test setup.

The connection from the loop to the PCs first was accomplished by fibre optic media converters to electrically separate the loop from the equipment in the laboratory. But during the tests it turned out, that these converters are sensitive to the induced currents on the loop cables in the same order as the hubs and switches themselves. So for the further measurements the loop was connected directly via long S/FTP cables to the PCs in the laboratory.

To generate data traffic between the two computers data samples with 10 MB, 100 MB or 1GB were sent from PC2 to PC1. The proper working of the data traffic between the computers is monitored by using network diagnostics software (Task-Manager and PING) and cameras looking at the system LEDs of the DUT.

4. Measurement Setup and Procedure

The experiments have been carried out in our field coupling facility. First, transfer functions were measured in order to estimate the resonance frequencies of the loop. But the main part of the measurements deals with the determination of the susceptibility thresholds of the network components, referring to the disturbing field or the loop current.

4.1 Waveguide

The INT test facility consists of a waveguide built as an open pyramidal asymmetric three-plate TEM transmission line which is located within a shielded hall (Fig.2). It consists of a source, a launcher and a long pyramidal shaped section of transmission line. This section includes the test volume. At a short region at the end resistors and absorbers are placed. The maximum cross sectional area is about 2.7 x 3.5 m^2 (h x w).

Figure 2: Photo of INT waveguide with pulse generator and DUT.

4.2 Measurement Setup for Transfer-Function and Susceptibility Measurements

The transfer-functions between 1-2500 MHz will be determined by CW measurements. Digital tuneable sweep generators followed by power amplifiers are used to produce maximum field levels of approximately 20 V/m. A vector network analyzer is used as receiver.

The susceptibility tests are carried out with the High Power Pulsed Signal Generator PH40KB from the former LUCAS-EPSCO company. The features of this generator are as follows:

- P_{max}: 35 kW
- Frequency range: 150 – 3425 MHz
- Pulse width: 0.25 – 15 µs
- Rise / fall time: approximately 0.1µs

- Pulse repetition frequency: single shot, 1 Hz – 10 kHz
- Duty cycle: 0.001 – 0.003.

The objective of the investigations is the determination of failure thresholds due to the disturbing field. Therefore, at a given frequency alternatively the field strength, the pulse width or the pulse repetition rate is modified, until at the DUT interference occurs. In case of a malfunction the parameters of the incident fields are manually noticed.

5. Measurements and Results

5.1 General

The test setup with the 4 m loop shown in Fig.1 shall simulate a basic network with one switch and two PCs linked together by twisted pair cables, typically for a usual workplace in an office. The cables are folded to a loop for maximum field coupling. With the measurement of the transfer functions $I_{loop}(f)/E_{ext}(f)$ the behaviour of the loop and its resonance frequencies can be estimated. These results also provide indications to possible frequencies the connected DUT may be vulnerable to.

With the susceptibility measurements we determine the failure thresholds $E_{fail}(f)$ due to the disturbing fields. But these values are dependent not only on the device under test but also on the loop characteristics. To get failure levels independent of the loop properties in some cases we also measured simultaneously the amount of the loop currents $I_{fail}(f)$ responsible for the malfunctions of the DUT.

5.2 Transfer-Function Measurements

These measurements have been done mainly in the frequency range between 1–2500 MHz with field strengths of about 20 V/m at the loop. The components of the network were in the majority of cases connected to the power supply whereas normally no data traffic took place. The position of the current probe was near the connector of the longer cable (see Fig.1). The probe measures the induced sum current on the four wire pairs or the current on the cable shield, depending on the kind of the cable.

At first the unshielded U/UTP-Cat.5e loop without switch as DUT was illuminated to assess the properties of the loop without the influence of other components. The transfer function $I_{loop}(f)/E_{ext}(f)$ is shown in Fig.3. As can be seen in the upper diagram the current decreases very fast with increasing frequency. Up to 500 MHz the degression is about 30 dB and 40 dB up to 1000 MHz, related to the maximum. The main resonances are around 37.5, 112.5 and 175 MHz and attain maximum values up to 0.008 A/(V/m). The red curve stands for maximum field coupling (E, H) whereas the black one is for only E-field coupling (E). Besides the first resonance no definite dependence on the field orientation can be observed.

Next we connected the loop consecutively to two different switches. Now the maxima are indeed in the same frequency ranges, but there appear more resonances. Again no definite dependence on the field orientation could be observed.

The results of the measurements with the shielded S/FTP-Cat.6 cable show sharper resonances in the same frequency range independent of whether a switch is connected or it is short circuited by a jumper. At these cables the shield is connected to the metal plug shell, so the disturbing current can flow over the metallic casing of the DUT.

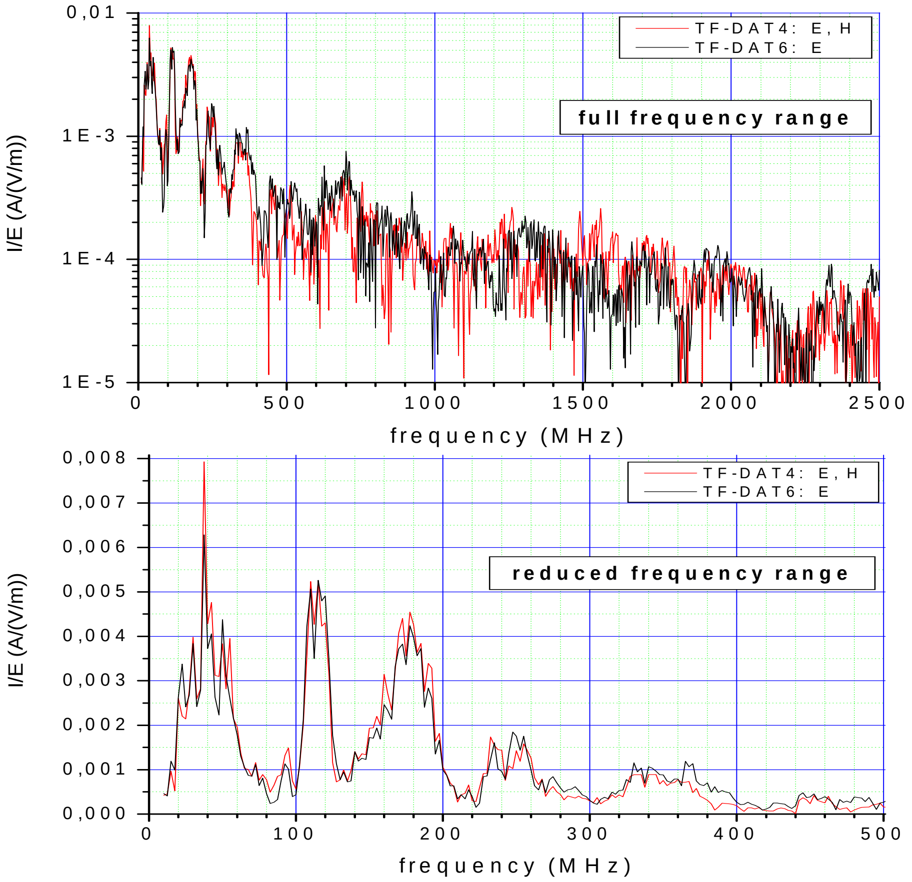

Figure 3: Transfer function I_{loop}/E for U/UTP-Cat5e loop without DUT.

The results of the transfer function measurements suggest the prediction that most of the disturbing effects on the DUT will occur below 200 MHz at lower field levels than in the following frequency region up to 1000 MHz.

5.3 Susceptibility Measurements (via Media Converter)

The susceptibility tests are carried out with our pulsed signal generator. To separate the setup electrically from the equipment in the laboratory media converters have been used. In computer networks these converters typically are used to avoid the 100 m limitation of Ethernet cables.

The chosen frequency range of the pulsed fields is between 150–3400 MHz, depending on frequency maximum field strengths of about 300–900 V/m are obtained at the loop. At each illumination the field increases within 30 s from a minimum to the maximum value. The selected pulse parameters of 1 µs width and 1 kHz repetition rate have been turned out empirically as a good compromise for susceptibility testing. Even though the previous transfer function tests show that only at frequencies lower than 1000 MHz the induced loop currents should be high enough to cause malfunction in the DUTs, at first we examined the whole frequency range. In this way among others we can look after disturbances due to bad enclosure shielding of the DUT.

For the first series of tests we chose two 10/100 Mbit/s switches. The main intention was to investigate the dependence of the susceptibility on the type of the used TP cables.

The following diagrams show the failure thresholds for the Netgear switch with the connected loop oriented to maximum field coupling. The black points mark the maximum electric field at the loop whereas the grey ones denote the minimum field level. The squares and rhombi indicate the intensity of the malfunctions as explained in Chapter I. The upper diagram in Fig.4 outlines the behaviour of the illuminated switch with the unshielded U/UPT-Cat.5e cable.

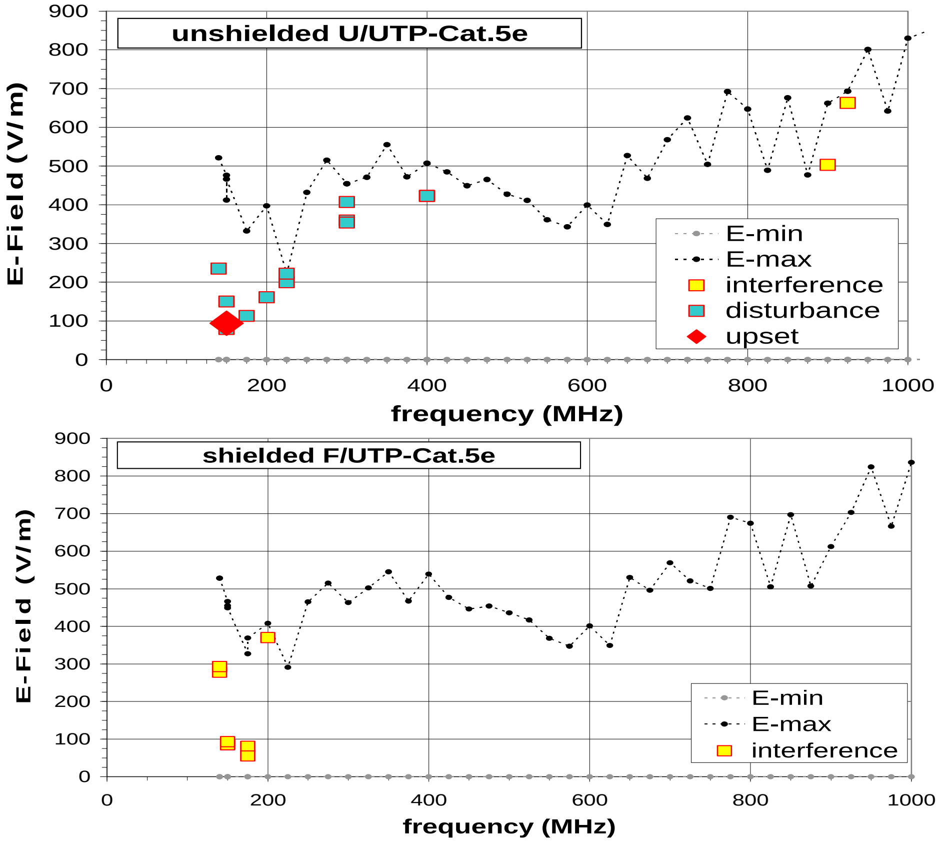

Figure 4: Failure thresholds of Netgear switch due to E-Field.

The use of U/UTP-Cat.6 cable leads to a noticeable reduction of the number and the intensity of the effects. A further reduction of the effects is obtained by screening the cable with a circumferential foil (F/UTP-Cat.5e, lower diagram). With the S/FTP-Cat.6 cable no effects appeared in the whole frequency range. The absence of any effects with this cable in addition indicates that there is no field coupling through the metal case and no influence due to the horizontally installed power cord. However, effects occurred if the power cord is oriented parallel to the electric field.

The induced currents in the loop not only influence the switch in the test setup but also the media converters below the ground plate via the ends of the loop cables.

Measurements without a switch show that the susceptibility of the media converter is slightly lower but there are also effects at frequencies not observed at the switch.

The conclusion of these previous measurements is that we have determined the susceptibility of the whole setup including the media converters and not the susceptibility of the illuminated switch alone. This configuration is typical for networks using media converters to avoid the 100 m limitation of Ethernet cabling. Nevertheless the general statements concerning the influence of the different TP cables, the power cords and the conducted effects (only via cable because of good shielding of cases) are correct further on.

5.4 Susceptibility Measurements (without Media Converter)

Because of the high susceptibility of the media converters the following measurements have been performed without them by connecting the loop directly to the PCs.

The measurement procedure was basically as before. The main difference lies in the fact that now a reference measurement with the bridged loop has to be done, that means, the data traffic between the PCs via the loop without DUT has to be monitored at first. If there are no effects during the illumination, the PCs are unaffected. If there are effects after the insertion of the DUT to the loop, these effects are due to the DUT. In this manner the setup is applicable for determining the susceptibility thresholds of devices.

The first measurements have been carried out on three switches and one hub. The results are shown in the two diagrams of Fig.5. The most susceptible switch was the FS-105 with affected frequencies at 200 and 300 MHz at a lowest field level of 140 V/m. The Catalyst2900 shows only interferences at 200 MHz and 300 V/m, whereas the 10 Mbit/s switch Catalyst3000 was unaffected. The 10 Mbit/s hub was not examined below 250 MHz, but it was still the most susceptible device. The effects between 250-400 MHz appeared as interferences and disturbances and at 275 and 300 MHz at field levels around 400 V/m even as upsets.

To assess a potential dependency of network components on different pulse parameters in a couple of measurements the pulse lengths have been varied between 0.25–10 µs and the repetition frequency between 1-4000 Hz, respectively.

At constant pulse width the increase of PRF leads to increasing disturbances of the ftp traffic. Increasing effects for increasing pulse width at constant PRF can not always be observed. Concerning the failure thresholds increasing PRF means decreasing threshold levels, the lengthening of the pulses only slightly attenuate these thresholds. The Catalyst3000 again could not be affected.

As could be seen from the transfer functions I_{loop}/E_{ext} in Fig.3 the main resonances are between 20-200 MHz. The measurements in this most sensitive frequency range have been done with a low power source generating fields up to 60 V/m. The FS-105 shows interferences with thresholds between 30-60 V/m. The Catalyst2900 appears to be more sensitive in a smaller frequency range. Interferences occurred between 20-60 V/m.

For the last measurements with Gigabit Ethernet switches the PCs had to be equipped with an appropriate network card. At the reference measurements with the bridged loop the new network adapter appears to be sensitive in a larger frequency range than the built-in Fast Ethernet adapter.

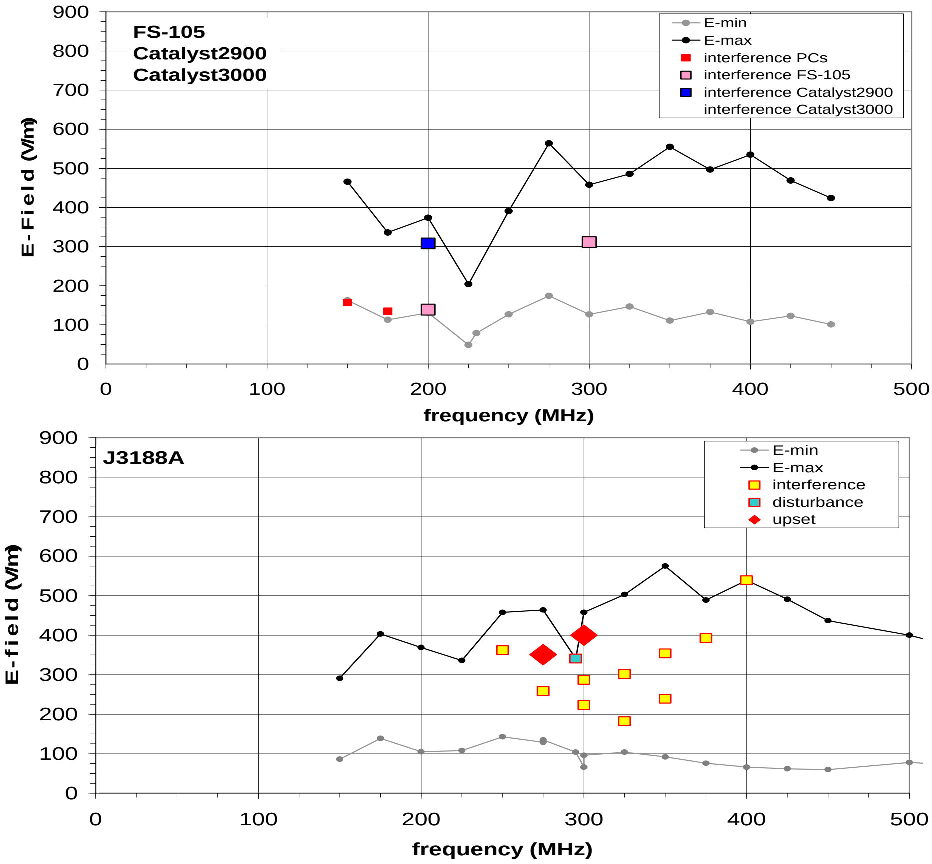

Figure 5: Failure thresholds of network components due to E-Field.

The GSW-0502 is vulnerable between 150-650 MHz with increasing thresholds at rising frequencies; interferences appeared between 100-500 V/m. The GS-608 shows only small interferences at the lower frequencies, but from 750 up to 975 MHz upsets occurred, partly with very low thresholds down to 170 V/m at 900 MHz. The great number of upsets in this frequency range may depend on the fact that the GS-608 is the only tested device with a plastic case. The 10 Mbit/s Catalyst3000 operated in the Gigabit Ethernet again shows no effects, whereas the 10/100 Mbit/s FS-105 was affected at more frequencies as in the Fast Ethernet. Furthermore the effects were more severe, so at 175 MHz upsets occurred. At a first glance these results suggest that the susceptibility of the switches depend on the network card of the connected PC, even if the data traffic is not affected at these frequencies at the reference measurements. But it may be also due to different transfer protocols and coding techniques of the different Ethernet standards.

6. Conclusion

The measurements show that the application of the widely used unshielded twisted pair cables in computer networks causes problems if operated in areas with electromagnetic disturbing fields because the cabling represents an important coupling path to the network equipment. This conclusion applies even more to IEMI and to the HPM threat. Note further that an attacker can also do serious harm by injection of conducted transients into the power or data networks of an infrastructure facility via freely accessible sockets. Failures in the investigated setup of an IT network occurred already for electric fields above 20 V/m at frequencies below 200 MHz and above 150 V/m for higher frequencies between 200 and 700 MHz. Such field levels can be easily achieved by an attacker at medium distances. The susceptibility thresholds depend strongly on the used network component and to some extent on the used Ethernet standard and of course on the setup of the test object. Shielded twisted pair cables largely avoid these problems. Contrary to expectations the use of fibre optic connections can be unfavourable due to the susceptibility of media converters. The weakness can be resolved by electromagnetic hardening of the latter if a fibre optic connection is required. This objective could be accomplished e. g. by putting each of the critical network devices into a shielded box with hardened connectors. In conclusion we strongly recommend the development of a strategy to reduce the HPM threat to critical civil infrastructure.

7. References

[1] D. Nitsch, F. Sabath, Ch. Braun, and H.-U. Schmidt, “Comparison of the HPM and the UWB susceptibility of microprocessor boards”, AMEREM 2002, 2-7 June 2002, Annapolis, MD, USA.

[2] 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.

[3] R. Hoad, A. Lambourne, and A. Wraight, “HPEM and HEMP susceptibility assessment of computer equipment”, 17th International Zurich Symposium on EMC, 27 February - 3 March 2006, Singapore.

[4] E. Savage, W. Radasky, K. Smith, and M. Madrid, “Pulse testing of network interface cards for upset and damage”, 19th International Zurich Symposium on EMC, 19-22 May 2008, Singapore.

[5] Ch. Braun, P. Clemens, H.-U. Schmidt, M. Suhrke, and H.-J. Taenzer, “Transfer function measurements and low power microwave susceptibility tests of a complex communication network”, EUROEM 2008, 21-25 July 2008, Lausanne, CH.

[6] Ch. Braun, P. Clemens, H.-U. Schmidt, M. Suhrke, and A. Taenzer, “Susceptibility of network components to pulsed medium power microwave fields”, 20th International Zurich Symposium on EMC, 12-16 January 2009, Zurich, CH.