HPEM Susceptibility Test on IT-Networks and their Components

Frank Sabath[1]

[1] Bundeswehr Research Institute for Protective Technologies and NBC-Protection (WIS), P.O.Box 1142, D-29623 Munster, Germany, Email: FrankSabath@bwb.org

Abstract

This paper presents effects of high-power electromagnetic environments on components of IT-networks. The narrowband environment was generated by the high-power microwave (HPM) test facility of WIS. An UWB test setup, consisting of a semiconductor based pulse generator and impulse radiating antennas, was employed to investigate UWB effects. The paper reports normalized thresholds of susceptibilities as well as observed tendencies.

1. Introduction

Studies indicate that while **H**igh **P**ower **E**lectro**m**agnetic (HPEM) sources are becoming more powerful, electronic equipment is becoming more susceptible to potential HPM attacks. With HPEM research being conducted worldwide, there is an increasing threat to NATO military equipment and critical infrastructure. Damaging terrorist attacks by low-cost, low-tech devices could disrupt or destroy the electronic circuitry of key nodes in an IT network, with potential catastrophic effects.

Due to its strong dependency on reliable network services, the implementation of the military doctrine of **n**etwork **c**entric **o**perations (NCO), or **n**etwork **e**nabled **c**apabilities (NEC), puts additional burden on electronic systems in IT infrastructure and communication equipment. NCO/NEC seek to translate an information advantage, enabled in part by information technology, into a competitive war fighting advantage through the robust networking of well informed, geographically dispersed forces. The operative goal of NCO/NEC is to permit entities that are conducting military missions (commanding officers) to obtain needed information from data bases and other repositories by employing modern information technology and sharing of information within operative forces. As NCO/NEC focus so much on distributing and sharing of information, one has to be wary of the effect of false information entering the system, a major reduction of network performance a total breakdown for a limited period of time. As those effects have the potential to neutralize the operational efficiency gained by NCO/NEC, the susceptibility of the communication network and especially of critical components of the IT-infrastructure is of vital interest.

One of the objectives of the research work performed at WIS has been investigation of the susceptibility of a complete military **C**ommand, **C**ontrol, **C**ommunication, **C**omputer and **I**ntelligence (C4I) network. This paper presents results of HPM and UWB investigations on a C4I system. The paper starts with a brief introduction on the HPEM test environment and the target system. The main part of the paper focuses on a discussion of observed effects and the identification of general tendencies.

2 System Description

2.1 HPEM Environment

2.1.2 HPM Simulator

The High-Power-Microwave (HPM) test facility of WIS in Munster was set up in the year 2002 [1]. Basically, the HPM-generator-system consists of a Thyratron-triggered, repetitive 1.4 Megavolt PFN-Marx generator and one set of 4 High-Peak-Power Super Reltron tubes, each equipped with motor controls for frequency- and output power-tuning. The frequency coverage extends from 675 MHz to 1.44 GHz with no gaps in coverage. The repetition rate is adjustable and extends from single shot up to 10 pulses per second. A maximum of 100 pulses can be contained in one burst. The pulses contain at least 300 cycles (Fig. 1). The microwaves are radiated into a 20 m long, anechoic chamber mainly furnished with non-combustible, pyramidal absorbers. From a shielded control room, and via optical fibers, the whole system is remote-controlled by a computer.

During the test the **e**quipment **u**nder **t**est (EUT) was exposed to bursts of 5 wave packets with various pulse repetition rates (PRF) and a duration of 100 cycles per packet. For each set of parameters (PRF, amplitude, polarization) the burst illumination was repeated three times. After a field exposure a “no field” period of at least 10 s was applied. In any case the field exposure started only after 10 s of stable and normal operation of the EUT.

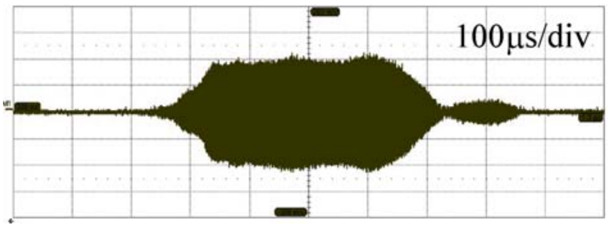


Figure 1: Typical waveform (wave packet) of the HPM simulator.

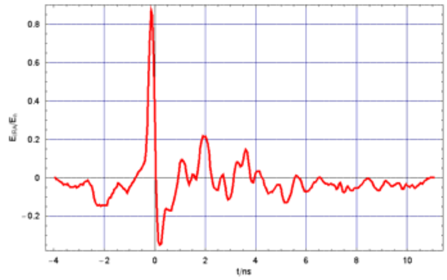


Figure 2: Typical waveform of the UWB test setup.

2.1.2 UWB Simulator

The UWB test facility at WIS consists of a Kentech PBG 7 pulse generator that feeding either a TEM horn type antenna or a 90 cm IRA type antenna. The field in the test area was measured in the absence of the EUT (Fig. 2). During the test the current field signal was monitored via a field probe in the ambient of the EUT. Due to security reasons the measured electric field strength was normalized with a normalisation factor E_n. The UWB tests were performed inside the anechoic chamber of the HPM simulator, to ensure well defined environmental conditions without reflections or disturbances form outside sources. During the test the EUT was exposed to bursts of UWB field impulses with various pulse repetition rates (PRF) and a fixed duration of 10 s. For each set of parameters (PRF, amplitude, polarization) the burst illumination was repeated three times. After a field exposure a “no field” period of at least 10 s was applied. In any case the field exposure started only after 10 s of stable and normal operation of the EUT.

2.2 Target System

HPEM investigations were performed on a large, configurable IT-network system that provides communication and network services to user, which are spread over several kilometers or more. The core element of the target system is a **l**ocal-**a**rea **n**etwork (LAN) composed of several LAN boxes that are connected via fiber optic lines or copper LAN cables (e.g. SFTP cables) to a ring type topology. Connections of the LAN to the outside world, such as ISDN lines and satellite communication, are made through the **w**ide-**a**rea **n**etwork (WAN) box. Usually, individual computers of various staff divisions and task groups are linked to the LAN ring utilizing HUB boxes. If needed, servers can be connected to the LAN.

Usually, various components of the network are located in shelters (like buildings), which provide some kind of electromagnetic shield. In a real life scenario the sources of an electromagnetic threat are mainly located outside the shelter. Therefore the electromagnetic environment in the ambient of network components depends on the shielding effectiveness of the shelter. As the HPM and UWB test focuses on the vulnerability of IT equipment the shielding by shelters has not been considered. The philosophy of the tests at WIS pays respect to the facts that (1) the test environment represents the environment inside a single shelter, (2) fluctuations of quality of service and data transmission appear during normal operation of a C4I network and (3) the reaction (and effect) of a C4I equipment depends on the operating status.

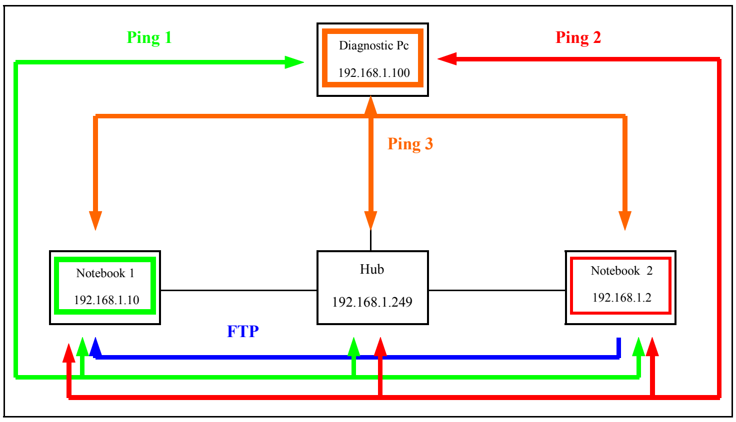


Figure 3: Test configuration of the HUB box.

Consequently, investigations focused on the core elements HUB box (Set-Up 1), LAN box (Set-Up 2), WAN box (Set-Up 4) and server (Set-Up 3). Each of these core elements was illuminated together with its typical periphery equipment and in a representative configuration. The quality of network service was measured by data traffic and retransmission rate. In the following this paper will provide results of tests on the HUB box (Fig. 3).

3. Results

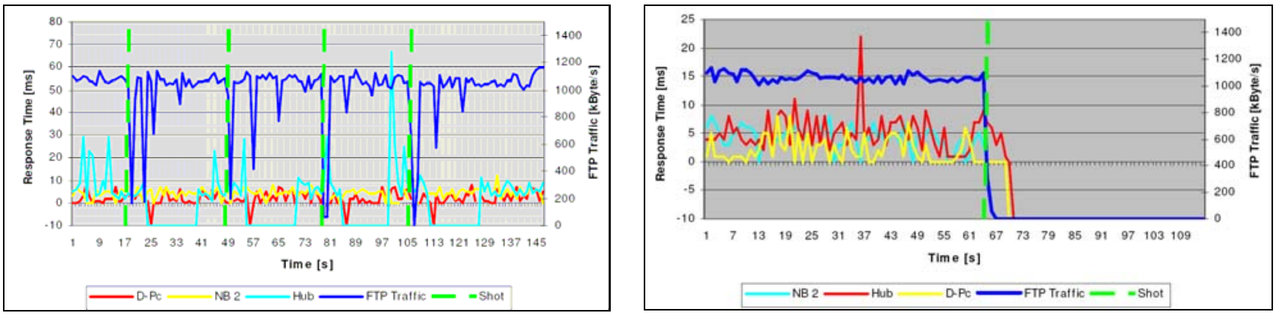
HPEM test on the HUB box resulted into three types of observable effects:

- Ping effects: Ping failure or delay of ping response (prolongation of ping response time),
- Data traffic effects: Lost of FTP data, increase of retransmission rate, decrease of data throughput and shutdown of data transmission and
- System breakdown: Reboot of the HUB box, other breakdown of HUB box or its components.

In addition to the measurable parameter, the effects were assessed in regard to the operational impact and the functionality of the system. A combined classification scheme, which has been introduced in [6], was employed to categorize the effects. The classification provides the essential information on the functionality (criticality) as well as on the duration of the effect.

3.1 HPM Experiments

A typical system behavior for an effect of level II-T (degradation for a period of time after exposure) is shown in figure 4.a. Immediately after the HPEM exposure (indicated by dashed green lines) the FTP traffic fluctuates for a few seconds and the Hub does not respond to Ping request. Furthermore, there is one Time Out per burst from notebook 1 (NB1) to the diagnostic PC (D-PC). The data traffic fluctuates for a short period, but is never interrupted.



(a) (b)

Figure 4: Example for a level II.T (a) and level III.H (b) effect

The determined normalized threshold of level II.T effects as a function of the carrier frequency is depicted in figure 5. Generally, the threshold values are in the range 1,5 to 2,5. In the lower half of the frequency range (675 – 725 MHz) the normalized threshold is approximately constant at 1,5 MHz.

Figure 4.b shows an example for an effect of level III.H (loss of main function till human intervention). The HPEM exposure results in a total break down of the FTP traffic. A few seconds after the breakdown of the FTP traffic, a loss of all Pings can be observed. The effect is critical for any kind of user, as the recovery of the function requires a manual restart of the HUB box by an operator.

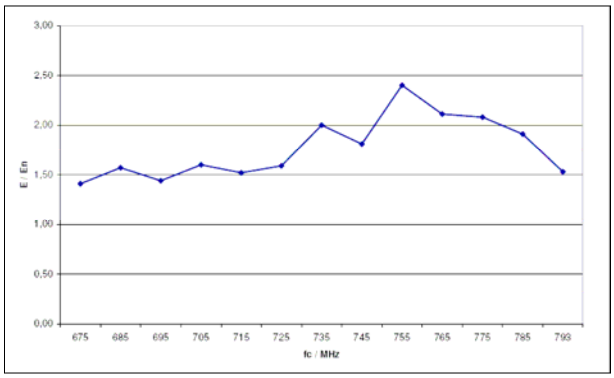


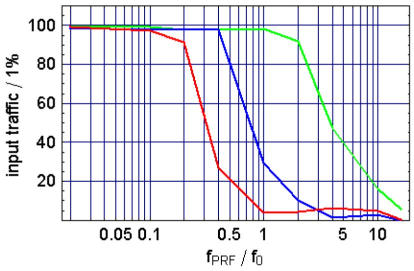
Figure 5: Threshold of level II.T effects.

3.2 UWB Experiments

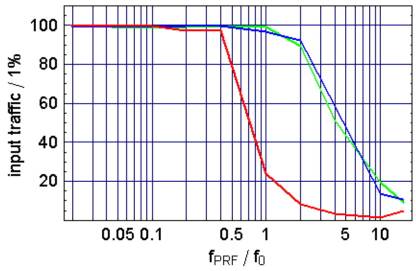
In this part of the paper we will present and discuss the results of the UWB test series on the HUB box utilizing a susceptibility diagram (Fig. 6). The diagram shows for each threshold the degree of incoming FTP traffic in percent. The percentage value bases on a representative extract of thirty recorded values of uninfluenced data throughput, which marks the base value for the benchmark of traffic performance. The incoming traffic rate has been chosen as a measure for the performance of the HUB box as other characteristic parameter, like outgoing traffic rate or retransmission rate, are in good correlation with the incoming traffic rate.

Generally, all curves are showing the typical S-shaped progression. They differ in the location (repetition rate) and steepness of the falling edge, i.e. fading of system performance. These curves can be characterized by the 80% value, where the performance starts to decline, and the 20 % value, the beginning of the total break down of data traffic.

When exposed to a vertical polarized electric field (Fig. 6, left side) with a threat level of E/E_n = 0.48 the performance dropps down to 80% at a normalized repetition rate of f_{PRF}/f_0 = 2,5 and to 20 % at f_{PRF}/f_0 = 9. Increasing the threat level to E/E_n = 0.6 results in f_{PRF}/f_0 = 0,5 for the 80% performance and f_{PRF}/f_0 = 1,5 for the 20% performance. Therefore doubling of the amplitude results in a decrease of the characteristic repetition rates by a factor of 5 to 6. Additional increase of the threat level to E/E_n = 0.9 reduced the characteristic repetition rates to f_{PRF}/f_0 = 0,225 (80%) and f_{PRF}/f_0 = 0,5 (20%), respectively.



red: E=0,9 En, blue: E=0,6 En, green: E=0.48 En



red: E=1,6 En, blue: E=1,2 En, green: E=1.0 En

Figure 6: Input data traffic rate during exposure to vertical (left) and horizontal (right) polarized UWB field.

The comparison of exposure to horizontal electric field (Fig. 6, right side) with exposure to vertical polarized field (Fig. 6, right side) indicates that the HUB box is more susceptible to a vertical than to an horizontal polarized threat. The horizontal threat needed approximately 2 times more field strength to provoke similar effects (see table 1).

Table 1: Parameter of a threat, that causes a 50% traffic degradation.

vertical polarized field				horizontal polarized field			
Effect Level	E / E_n	f_{PRF} / f_0	Burst Length	Effect Level	E / E_n	f_{PRF} / f_0	Burst Length
II-T	0,4	4,0	10 s	II-T	1,0	4,5	10 s
II-T	0,6	0,7	10 s	II-T	1,2	4,5	10 s
II-T	0,9	0,3	10 s	II-T	1,6	0,7	10 s

4. Conclusion

This paper presented effects of high-power electromagnetic environments on components of IT-networks. It discussed mainly results gained from narrowband HPM and UWB tests on a HUB box. Certain minimum thresholds were required to cause any effects, independent of the applied repetition rate. If the minimum critical field strength level was applied, a correlation between effect level and repetition rate could be recognized. A comparison between narrowband and wideband tests showed that similar threat levels were needed to cause the same loss of performance.

References

1. M. W. Wik, R. L. Gardner and W. A. Radasky, Electromagnetic terrorism and adverse effects of high power electromagnetic environments, Supplement to proceedings of the 13th International Zürich Symposium on EMC, Zürich (CH), 13, 1999.
3. F. Sabath, M. Bäckström, B. Nordström, D. Sérafin, A. Kaiser, B. A. Kerr and D. Nitsch, Overview of Four European High-Power Microwave Narrow-Band Test Facilities, IEEE Trans. EMC, vol. 46 (3), pp. 329-334, August 2004.
4. W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath and D. Nitsch, Survey of Worldwide Wideband Capabilities , IEEE Trans. EMC, vol. 46 (3), pp. 335-344, August 2004.
5. IEC 61000-4-35: Electromagnetic compatibility (EMC) – Part 5: Testing and measurement techniques – Section 35: HPEM simulator compendium.
6. F. Sabath, System oriented view on High-Power Electromagnetic (HPEM) Effects and Intentional Electromagnetic Interference (IEMI), Proceedings of the XXIX URSI General Assembly.