

High Power Microwave Effects on Computer Networks – Sensitive Parts and Comparisons

Libor Palisek^{1,*}, Lubos Suchy²

VOP-026 Sternberk, s.p. Sternberk, Czech Republic

Abstract Electromagnetic threat due to Intentional Electromagnetic Interference (IEMI) is shortly introduced at the beginning of this paper. High Power Microwave (HPM) as well as Ultra Wide Bandwidth (UWB) signals as a part of IEMI are described and compared with other electromagnetic threats. The main part of this paper is focused on data networks equipment and their electromagnetic immunity where unique testing facilities are used. Data networks are considered as a possible vulnerable part of infrastructures. HPM and UWB immunity testing of data networks is presented and discussed. Finally the most sensitive parts of data networks are discussed as well as relevant immunity comparisons.

Keywords Data, Electromagnetic, EMC; HPM, IEMI, Immunity, Networks, Susceptibility, Testing, UWB

1. Introduction

Many recent systems need reliable computer network to work properly. Especially computer networks within the infrastructure should be considered as a very important part of electronic systems. It is well known electronic equipment are sensitive to electromagnetic irradiation and computer networks are not exceptions of course. All equipment including network components has to withstand electromagnetic fields according to regular EMC (Electromagnetic Compatibility) standards but higher level of electromagnetic fields can affect electronics significantly.

High power electromagnetic fields are not normally a part of regular EMC environment but it should be considered as a possible potential threat for civilian infrastructure. Shortcuts like IEMI (Intentional Electromagnetic Interference) and HPEM (High Power Electromagnetics) are used in this area where high power electromagnetic fields are generated intentionally to affect (to attack) vulnerable electronic systems.

Other widely used and useful shortcuts in this area are HPM (High Power Microwave) and UWB (Ultra Wide Bandwidth) which are considered as a part of IEMI.

IEMI can be generated by relevant power technologies and focused (directed) towards the point of interest (target) with electronics.

HPM and UWB signals as an IEMI are shown in Fig. 1 and briefly defined:

- HPM: High Power Microwave, narrowband signals in frequency range 100's MHz up to several GHz, electro

magnetic strength at the place of target typically up to 10's kV/m (strong dependence on range).

- UWB: Ultra Wide Bandwidth, pulses with rise time typically 100's picoseconds and with duration several nanoseconds, electromagnetic strength at the place of target typically up to 10's kV/m (strong dependence on range). HPM and UWB technologies are suitable to use as a directed energy systems due to frequency range.

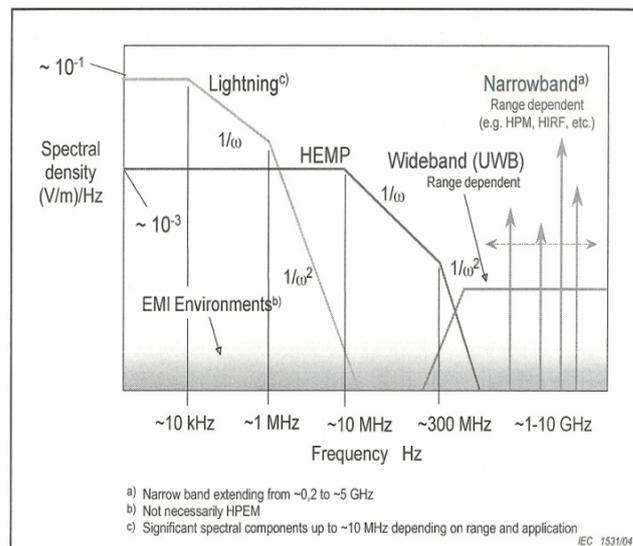


Figure 1. HPM and UWB comparison with other electromagnetic threats[1]

Many experiments regarding electromagnetic immunity of information technology (IT) equipment (mainly personal computers and some data network equipment) were carried out and published in the past[2-6]. The aim of our experiments was to find immunity of various equipment used in data networks and to make comparison of their immunities.

* Corresponding author:

palisek.l@vop.cz (Libor Palisek)

Published online at <http://journal.sapub.org/ijea>

Copyright © 2012 Scientific & Academic Publishing. All Rights Reserved

2. Experimental Measurements

HPM and UWB signals were used for experimental susceptibility measurements. As equipment under test were used typical parts of data networks i.e. data switches, routers, media converters and WiFi components.

Overall setup for HPM and UWB testing is shown in Fig. 2.

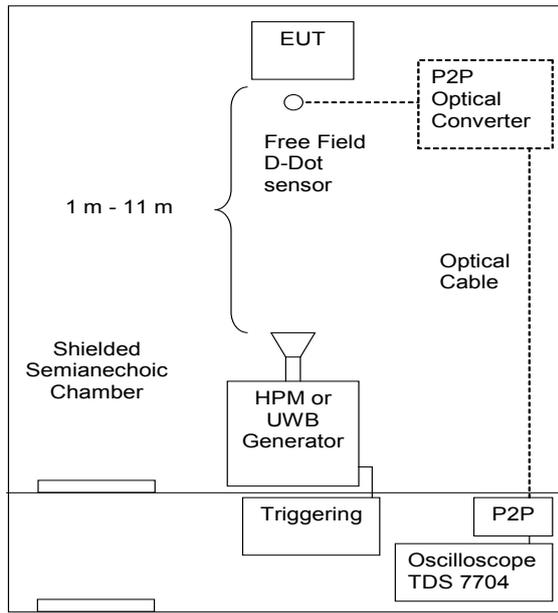


Figure 2. Test setups in semianechoic chamber for HPM and UWB testing

3.1. Configurations

Each setup was irradiated separately. Duration of irradiation was 3 seconds for HPM testing and for UWB testing the procedure was as follows: first of all single shot measurement was done and after that 10 pulses with repetition rate 10 Hz were applied (i.e. 1 second irradiation).

For both HPM and UWB testing the electromagnetic strength was increased by shortening the distance of tested equipment from HPM or UWB generator (see Fig. 2).

All tested setups were normally irradiated from 3 different positions (front, side and back) not to avoid side with connections as Ethernet connections and power supply cables.

Sensitivity of setups with regular UTP (Unshielded Twisted Pair) cables was compared with SFTP (Shielded Foil Twisted Pair) cables setups. As a default SFTP cables were used. As a diagnostic tool during testing the software Colasoft Ping Tool[7] and Jperf[8] were used to monitor traffic via network and to load the network to the maximum level.

3.2. Performance criteria

Regular performance criteria which are widely used for EMC immunity evaluation were signed *A*, *B*, *C* and *D* as follows:

A - normal performance within the specification limits,

B - temporary loss or degradation of function (self - recoverable),

C - temporary loss or degradation of function, which requires operator intervention or resetting,

D - degradation or loss of function which is not recoverable due to damage of equipment (effect that damages hardware to the point it must be replaced or software to the point it must be reloaded).

3.3. HPM signal parameters

HPM generators 3 GHz, 6 GHz and 9 GHz were used to irradiate tested setups. Pulse power, pulse width and repetition rate of all used HPM generators are mentioned in Table 1.

Table 1. Parameters of HPM Generators

	Pulse power [kW]	Pulse width [μs]	Repetition rate [Hz]
3 GHz	500	2.5	400
6 GHz	500	1.75	400
9 GHz	200	0.5	2000

Idealized shape of HPM signal is shown in Fig. 3 and measured time derivation of electromagnetic field with D-Dot sensor is shown in Fig. 4. Results from HPM testing are shown in Fig. 6 – Fig. 8, Fig. 10 and Fig. 11.

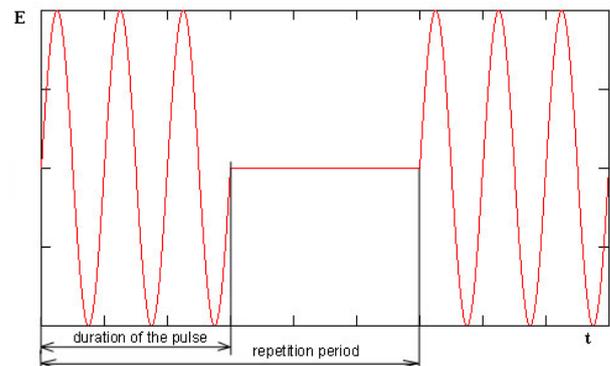


Figure 3. Idealized shape of HPM testing signal

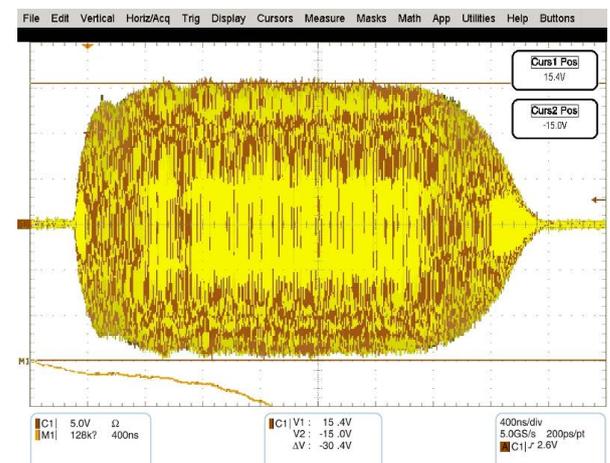


Figure 4. HPM 3 GHz, repetition rate 400 Hz - Time derivation of electromagnetic field

3.4. UWB signal parameters

UWB signal with rise time 0.5 ns (10% - 90 % of amplitude) and duration 2 ns was used (see Fig. 5) to irradiate tested setups.

Results from testing related to UWB are shown in Fig. 9 – Fig. 11.

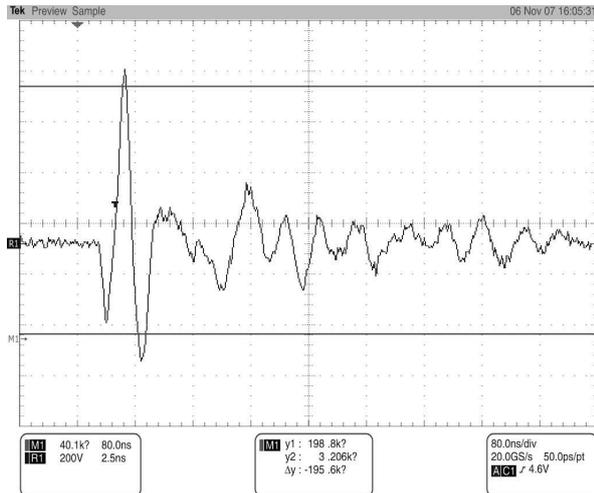


Figure 5. UWB pulse measured in distance 11 m far from UWB generator antenna

3.5. HPM and UWB Results

Results from susceptibility measurements are shown in Fig. 6 – Fig. 11. All results are shown in normalized form. From Fig. 6 it is obvious that temporary failures (B) occur almost for the same levels of electromagnetic fields for all considered media converters. Some of them were more sensitive and other effects (C or even D) occurred for higher levels. Media converters (MC1 – MC9) were extremely sensitive to electromagnetic field considering temporary failures (B).

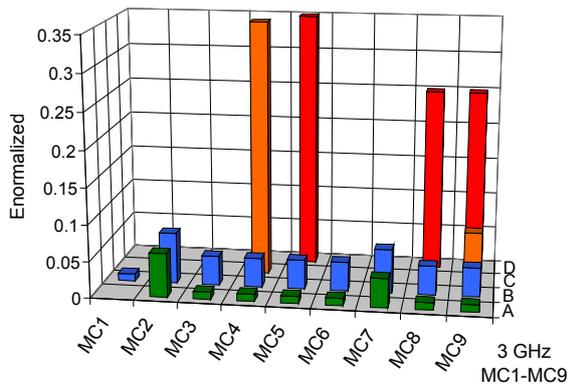


Figure 6. Susceptibilities of media converters (HPM 3 GHz)

Next Fig. 7 shows susceptibilities of tested WiFi setups for HPM 6 GHz. Communication according to standards IEEE 802.11b (11 MB/s) and newer IEEE 802.11g (54 MB/s) were established and relevant immunities were compared. Usually immunity of communication with newer standard IEEE 802.11g (54 MB/s) was higher. When only antenna connected to antenna port was irradiated (W1-g (A) or W1-g (A))

see Fig. 7), observed immunity was much higher so antenna input was not the most sensitive part during testing (all tests which were carried out can be classified as “out of band testing”).

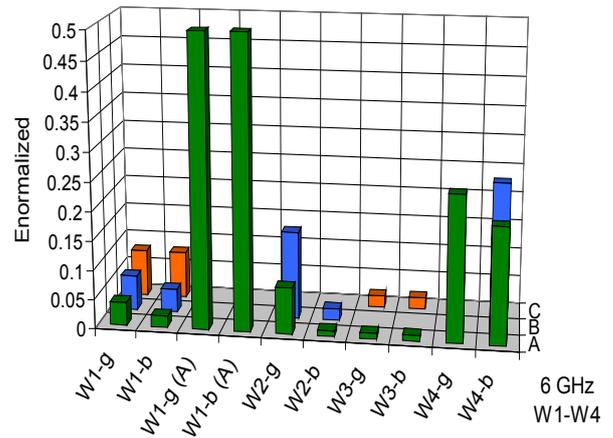


Figure 7. Susceptibilities of WiFi setups (HPM 6 GHz)

During testing of routers (R1 – R3) it was observed the most sensitive part of routers is WAN part. If routers were working in data switch mode their immunities were higher (see fig. 8).

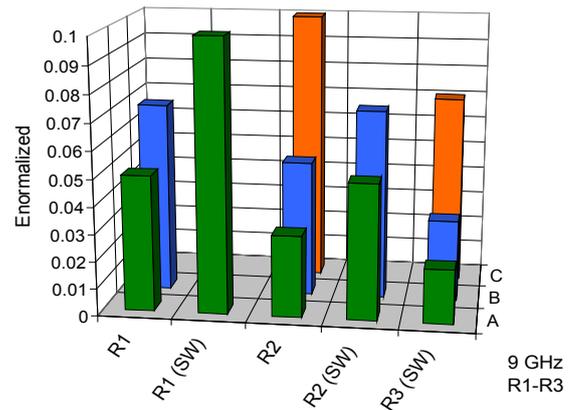


Figure 8. Susceptibilities of routers (HPM 9 GHz)

Very big differences between immunities of various kinds of data switches (SW1 – SW10) were observed during testing (see Fig. 9).

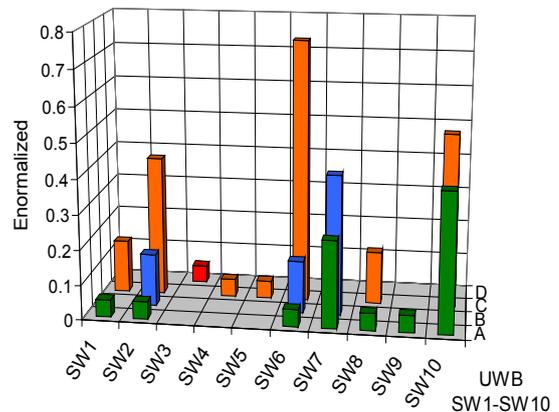


Figure 9. Susceptibilities of data switches (UWB)

Some comparisons of router and data switch sensitivities are shown in Fig. 10 and Fig. 11.

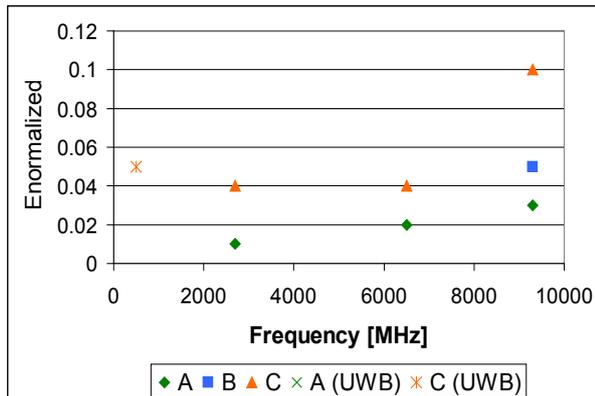


Figure 10. Susceptibilities of chosen router - comparison

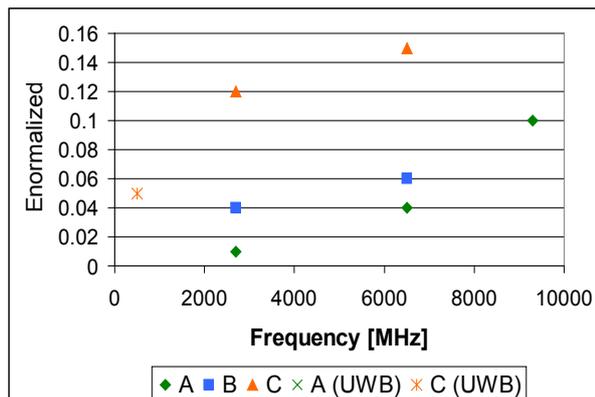


Figure 11. Susceptibilities of chosen data switch - comparison

3. Summary

It was discussed and shown network equipment are sensitive to HPM and UWB irradiation. In some cases very big differences between immunities of various tested equipment were observed so proper choose of more immune equipment can increase immunity of the system. The most sensitive part of data networks seems to be media convertors which allow us to use fiber optics instead of metal cables. Fiber optic cables can not be affected by electromagnetic field but media convertors can reduce overall immunity of network system significantly. Special attention should be taken in to account in case of vulnerability assessment of crucial systems.

Immunity of WiFi setups and router setups in different modes were found, compared and discussed.

Influence of SFTP cables use in comparison with UTP cables use was observed only seldom and only for lower HPM frequencies. Nowadays equipment are usually equipped with Ethernet connectors without shielding or shielding is not connected properly so in most cases there is no sense to install shielded SFTP cables instead of cheaper

UTP cables.

Typical dependence of immunity on frequency was observed during HPM and UWB testing. Immunity was becoming higher for higher frequencies due to less effective coupling of radiated signal to electronic structures. Some exception could be observed for frequency 500 MHz which corresponded to maximum energy of used UWB signal but due to UWB pulse length these UWB results are not fully comparable with HPM results considering only frequency influence. For accurate sensitivity comparisons considering only frequency influence the pulse lengths of all used signals has to be the same or at least comparable. This kind of measurements will be done with reverberation chamber use during year 2011.

ACKNOWLEDGMENTS

This work was supported by Ministry of Defence, Czech Republic (The project "Defence capabilities against DEW - Vulnerability assessment of weapon systems and infrastructure C2, OSPROZ-DEW1").

REFERENCES

- [1] IEC 61000-2-13, First edition, 2005-03, Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted
- [2] HOAD, R, CARTER, N. J, HERKE, D, WATKINS, S. P. Trends in EM susceptibility of IT Equipment. IEEE Trans. on Electromagnetic Compatibility, 2004, vol. 46, p. 390-395. ISSN 0018-9375.
- [3] WRAIGHT, A, HOAD, R, LAMBOURNE, A. J. HPEM and HEMP Susceptibility Assessments of Computer Equipment. Proc. American Electromagnetics Conf. (AMEREM), Albuquerque, USA, 2006, ISBN 1-4244-0123-2
- [4] SABATH, F, RÖMER, B. Susceptibility of IT-Networks to HPM and UWB Threats. Proc. European Electromagnetics Conf. (EUROEM), Lausanne, Switzerland, 2008
- [5] SAVAGE, E. B, RADASKY, W. A, SMITH, K. S, MADRID, M. J. Susceptibility of Network Interface Cards to High-Level Conducted Pulses. Proc. European Electromagnetics Conf. (EUROEM), Lausanne, Switzerland, 2008
- [6] PALISEK, L, KUSALA, J, VRANA, L, MIKSIK, R. Electromagnetic Threats to PCs. Proc. European Electromagnetics Conf. (EUROEM), Lausanne, Switzerland, 2008
- [7] Colasoft[online].[cited 2011-01-10]. Available from: <http://www.colasoft.com/ping_tool/>
- [8] JPERF[online].[cited 2011-01-10]. Available from: <<http://openmaniak.com/iperf.php>>