Marek DRAS[1], Marek KAŁUSKI[1], Monika SZAFRAŃSKA[2]

Radiotechnika Marketing sp. z o. o. (1), National Institute of Telecommunications (2)

doi:10.15199/48.2016.02.06

Introduction to High Power Microwave as a source of disturbances

***Abstract**. This paper presents some basic information about HPM pulses. It was shown how HPM pulses could interact with the electronic equipment and how dangerous it is. The authors point out that the addition of new special filters to the existing protection of military equipment is needed to offer new protection against HPM pulses.*

***Streszczenie.** W artykule zostały przedstawione podstawowe informacje o impulsach HPM. Pokazano, że impulsy HPM mogą oddziaływać na urządzenia elektroniczne a także pokazano jak groźne może być takie oddziaływanie. Autorzy wskazali jak istotna jest dodatkowa, poza już istniejącą, filtracja pozwalająca na zabezpieczenie przed działaniem impulsów HPM. (**Wprowadzenie do HPM jako źródła zaburzeń**).*

Keywords: HPM pulses, HPM filters, directed energy.
Słowa kluczowe: impulsy HPM, filtry HPM, energia skierowana.

Introduction

Research on HPM technology is one of the newest areas of interest in relation to the new generation weapons. These kinds of impulses are extremely powerful and dangerous for electronic equipment. Some projects and research considering HPM as a weapon were performed by NATO but most of the results are top secret. Radiotechnika Marketing is one of the participants of a project commissioned by Polish Ministry of Defence. One of the main subjects of the project is filtration and protection of electronic systems against HPM. In Poland, so far, there has only been one project dedicated to solving problems of protection against HPM and some results of Radiotechnika's previous research (based on that project) will be shown in this article [1]. The authors want to introduce the most important information about HPM technology and show how powerful a source of disturbances it (HPM) can be.

Taking into account that the HPM pulses could be used as a new generation weapon, authors want to show how this kind of pulses could interact with the electronic equipment and how dangerous it is. Effects of HPM's can be more dangerous than previous weapons based on electromagnetic pulses. Moreover, the HPM sources may exist in different versions. Given the fact that the source of HPM are weapons of mass destruction, non-killing, non-selective, double-edged, acting on the attackers and attacked - there is no possibility of avoiding the front of it. Practical operating range of this weapon is local at a distance of approx. 1500 m from the source of HPM [2, 3]. Protection against HPM is a common issue concerning all electronic devices on the battlefield, regardless of their level of complexity.

The authors point out that the addition of new special filters (to the existing protection of military equipment, for example against electromagnetic exposures such as lightning, sparks) is needed to ensure additional protection against HPM pulses. It should be taken into account that typical filters (such as the ones previously used in military equipment) are not able to provide effective protection against HPM.

HPM pulses

HPM pulses could generate very high currents on systems exposed to them. The effects of such pulses lead to the total destruction, disruption of work or a software crash of most of the currently used semiconductor systems. This kind of pulses could transfer huge power and generate high risk for modern systems.

As mentioned in the introduction, for over 20 years some works have been performed by NATO in the area of securing facilities against electromagnetic weapons in particular against pulsed electromagnetic fields. For many years, substantial financial costs have been borne on research in the field of defence and protection from the effects of HPM, resulting in their possible application. In particular, the results of several RTO NATO and NATO-SCI grants in the field of HPM are a rich source of knowledge (which, unfortunately, remains mostly confidential) of observed examples of protection system reactions towards HPM in military hardware.

The frequency spectrum and the energy levels generated by this kind of disturbances have been classified and can be described in such a way, as it is illustratively presented in Figure 1.

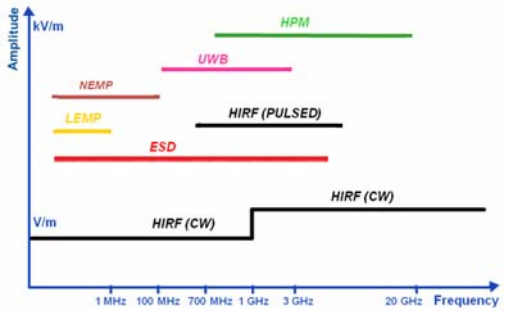

Fig.1. Frequency range and levels of pulse disturbances

Firstly, two types of apparatus generating electromagnetic disturbances need to be distinguished: the apparatus used to test the HPM and the group of some devices that produce very strong HPM pulses for tactical or terrorist use. Apparatus which can be used in the laboratory for testing immunity of phenomena of these pulses typically generate continuous, repeatable and adjustable and relatively weak HPM pulses. Large systems and equipment for tactical purposes usually produce very strong, unregulated, single or small quantity pulses meant to destroy the attacked facilities. Typically, such devices are mounted on military vehicles and airplanes, and are designed to act as a weapon and not as a device which can repeatedly generate disturbance. For example Boeing company in October 2013, in the CHAMP program of unmanned aircraft, destroyed computer networks, alarm systems and power supply in the whole complex of buildings by generating HPM pulses [4].

Polish experience in HPM pulses

Some first steps in the field of HPM pulse generation have also been made in Poland, i.a. by Radiotechnika. Commissioned by Ministry of Internal Affairs, a grant related

to this subject has been realized. Figure 2 presents a suitcase device for generating pulse disturbances used during the implementation of the grant. This device is relatively weak of only 0.2 J.

Fig.2. Suitcase system for generation pulses Diehl DS110F

Please note that due to the different types and nature of HPM pulses used by a potential attacker, each of them has different disruptive or destructive properties when affecting the device or its circuitry. Therefore, trying to prepare protection against all kinds of pulses, adequate laboratory equipment needs to be used or the existing machinery producing HPM pulses adjusted to be able to cover the broadest possible range and complexity of the exposures that occur in the reality of HPM. Radiotechnika Marketing, performing some own works on the implementation of the NCBiR grant (New weapons systems and defence in the field of directed energy), prepared the special test set-ups which allow to generate HPM pulses both in the form of continuous radio waves and those generating a series of HPM pulses. As mentioned above, laboratory devices are not intended to produce multi-megawatt pulses, but their purpose is to generate repeatable signals of similar nature (shape and method of oscillation).

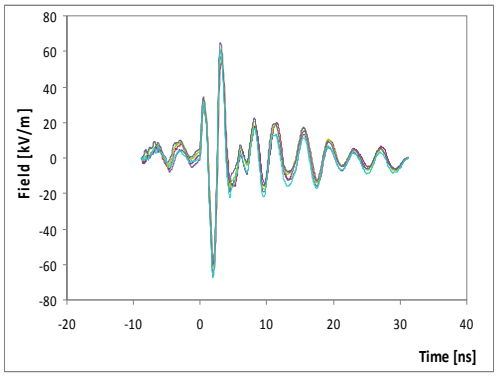

Fig.3. Test pulse generated using Diehl DS110F (time domain) – distance between source and probe 1 m

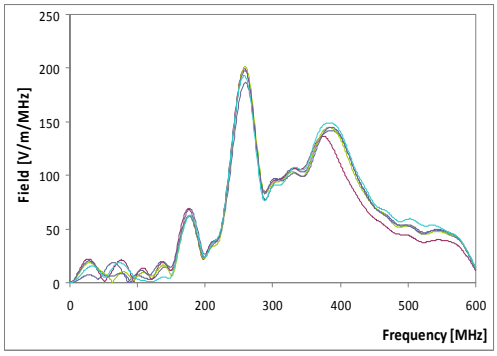

Fig.4. Test pulse generated using Diehl DS110F (frequency domain) – distance between source and probe 1 m

Figure 3 (time domain) and Figure 4 (frequency domain) below show laboratory impulses coming from the Marx's generator (suitcase system as shown in Fig. 2).

In addition, the special test set-ups based on properly configured generator systems were prepared by Radiotechnika. The example of test set-up and pulse generated in this set-up are presented in Figures 5 and 6. These pulses are used to test filtration systems that will be the target solution for protection against HPM weapons. Laboratory simulations allow multiple attempts to study how to penetrate pulses through protection without the threat of permanent damage to the equipment used during the test.

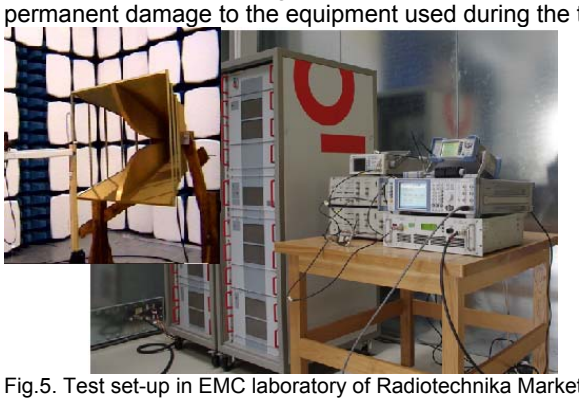

Fig.5. Test set-up in EMC laboratory of Radiotechnika Marketing

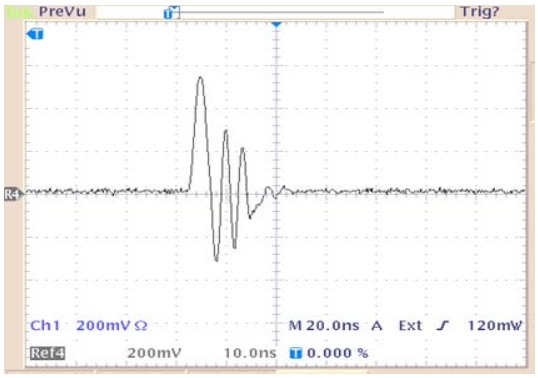

Fig.6. Pulse generated in laboratory test set-up in Radiotechnika Marketing

Preliminary measurements of conducted disturbances generated by HPM pulses

During the grant commissioned by Ministry of Internal Affairs, a series of measurements was performed in order to recognize voltage levels in various types of cable bunches. The task was to determine the safe and dangerous levels from the point of view of electronic and telecommunication devices such as network cards, power supplies and more, through a series of conducted measurements with pulsed electromagnetic field exposure.

Fig. 7 – 9 show test results of conducted disturbances measured for various Ethernet cables: shielded (on both or one ends) and unshielded. Source of disturbances was located in 1m distance from victim cable [5, 6].

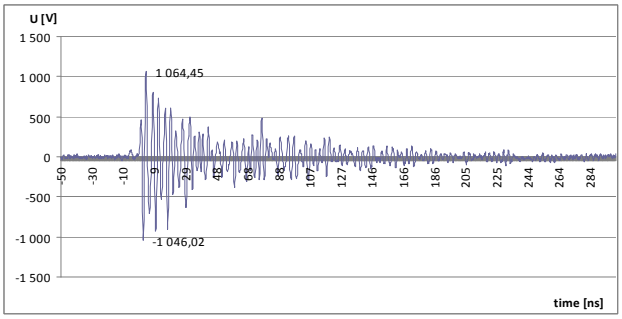

Fig.7. Conducted disturbances measured on cable without shield

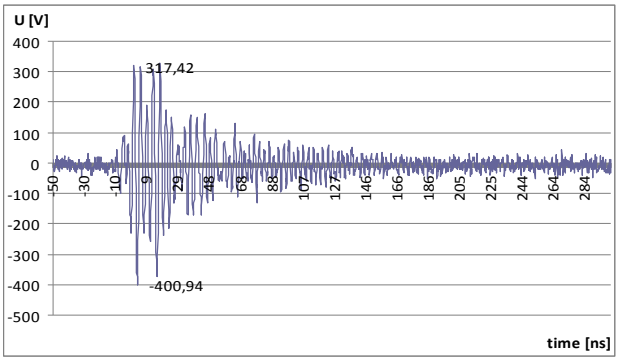

Fig.8. Conducted disturbances measured on cable with shield mounted on one site

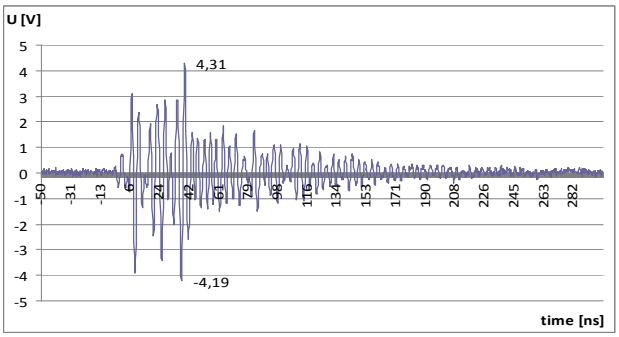

Fig.9. Conducted disturbances measured on cable with shield mounted on both sites

Note that the results presented above are derived from the exposure of a relatively weak source (as shown in Figure 2). Actual exposure coming from the weapons can transmit pulses of several hundred times higher.

Filtering of HPM pulses

Due to their construction, all currently used electronic devices are susceptible to the effects of HPM pulses. If the cables are set between distant points, they act as long receiving antennas for these impulses and lead them into all electronic systems. As an example, it can be selected parts of cable connections of power and transmission lines between containers for typical tactical command post of military C4I systems that have been tested under the NATO RTO SCI-132 grant. Also active equipment attached to such cables was subjected to testing. The susceptibility of such devices shows not only the need to protect the electronic input / output, but also the need for appropriate filtration (in particular shielding) starting from wires or cable bunches connecting the potentially sensitive components.

It should also be mentioned, as it can be seen from the results presented in the previous section, that the method of shielding of cables in a conventional manner is not sufficient to protect against the HPM pulses. The use of multi-layer shields causes a stiffening of the cables, they are not fit to virtually expand and collapse. Therefore, attention should be paid to the need to design, build and test cables with other internal conduction and preventing the propagation of the pulses caused by HPM signals.

It must be mentioned, that both AC and DC power supplies, being essential elements of operation of any electrical device, should be adequately protected against HPM.

It is well known that power supply systems which are the most external part of systems, as well as the main buffer for them, are the most exposed ones to any disturbances. Therefore, it is important to pay particular attention to these elements. Moreover, according to the grant of the work carried out for the Ministry of Internal Affairs and some works of the NATO-RTO, power supplies containing converters (practically every one of them) are very easily damaged, both from 230V mains input and the output side of DC 24V, at the time of their exposure to pulses. Reliable supply systems, including UPS, are fundamental and indispensable elements of any operation of electronic devices, in particular the military ones.

Somewhat surprising may be the need for protection against the HPM effects of optic connections. The optical fibres are theoretically resistant to the effects of electromagnetic waves. This is partly true. Same fibre-optic cables are immune, but with connections, fibre optic connectors and fibre optic systems with attached converter are, according to research carried out in NATO-RTO, the most susceptible to HPM exposure part of the C4I computer network systems. This information was kept secret by NATO for several years, and is very important for the safety of the operation of the data in centres of command.

Summary

Currently in Poland there are no pulse generators for the generation of HPM. Generators for research applications are apparatus with relatively low power and their impact on the exposed equipment is relatively weak, but they cause interference with these devices.

Results of laboratory tests for different exposures show the importance of proper filtration not only through the use of conventional protection, but also those requiring special solutions. It should be noted that if adequate dedicated sources of HPM pulses were available, interaction effects would be up to hundreds of times stronger and generated from long distances - hundreds of meters.

***Authors**: mgr inż. Marek Dras, Radiotechnika Marketing sp. z o. o., ul. Fabryczna 20, Pietrzykowice, 55-080 Kąty Wrocławskie, E-mail: mdras@radiotechnika.com.pl; mgr inż. Marek Kałuski, Radiotechnika Marketing sp. z o. o., ul. Fabryczna 20, Pietrzykowice, 55-080 Kąty Wrocławskie, E-mail: mkaluski@radiotechnika.com.pl; mgr inż. Monika Szafrańska, National Institute of Telecommunications, EMC Department, ul. Swojczycka 38, 51-501 Wrocław, E-mail: M.Szafranska@itl.waw.pl*

REFERENCES

[1] „Opracowanie technologii i demonstratora zabezpieczenia systemów teleinformatycznych służb porządku publicznego w aspekcie narażenia na terrorystyczne działanie silnych impulsów elektromagnetycznych", report from grant ordered by Home Office (NCBiR no 0R00006311, made in 2010-2012 by WAT, RM i CTM

[2] publication of NATO-RTO SCI-132, NATO-RTO SCI-119, NATO-RTO SCI-198

[3] Bendord J., Swegle J.A., Schamiloglu E., High Power Microwaves, ISBN 0-7503-0706-4

[4] Kuchta M., Kubacki R., Nowosielski L., Dras M., Wierny K., Namiotko R., Standardy bezpieczeństwa dla urządzeń teleinformatycznych zabezpieczające przed terroryzmem elektromagnetycznym, Przegląd Elektrotechniczny, no 12, 2012

[5] Wierny K., Wpływ impulsów elektromagnetycznych dużej mocy na elementy systemy teleinformatycznego, report of Radiotechnika Marketing sp. z o.o.

[6] Dras M., Odporność wojskowych urządzeń elektronicznych na narażenia elektromagnetyczne o wysokiej energii (HPM), III Communication Konference, Sieradz, March of 2012