IS HPM A THREAT AGAINST THE CIVIL SOCIETY?

Mats Bäckström[(1)], Barbro Nordström[(2)], Karl G. Lövstrand[(3)]

[(1)] Swedish Defence Research Agency FOI, Box 1165, SE-581 11 Linköping, Sweden, E-mail: mats@foi.se

[(2)] Swedish Defence Materiel Administration (FMV), Testing Directorate, Box 13400, SE-580 13 Linköping, Sweden, E-mail: barbro.nordstrom@fmv.se

[(3)] Swedish Defence Materiel Administration (FMV), Joint Materiel Command, SE-115 88 Stockholm, Sweden, E-mail: karl-gunnar.lovstrand@fmv.se

ABSTRACT

From HPM susceptibility testing of typical civil electronics, such as cars, computers and telecom equipment, it is concluded that the distance for HPM sabotage can reach a kilometre. Such a distance requires a very powerful radar transmitter but not a military HPM weapon. For back-door coupling at this distance upset is expected to occur, while for in-band front-door coupling permanent damage may also occur. Most civil systems lack protection against HPM, although some may be rather well protected due to their installation. Susceptibility of important systems should be investigated, methods for analysis and protection should be developed and evaluated.

INTRODUCTION

In later years a growing attention has been paid to the threat posed by HPM (High Power Microwaves), and other kind of high intensity electromagnetic radiation, against the function of important electronic systems of the civil infrastructure. Targets, conceivable for a terrorist attack, could be telecom, radio/television and power networks or traffic control, financial systems, computer networks etc, see Fig. 1. While this type of threat has been recognised for rather a long time by the military, the threat against civil systems, private as well as public, has started to gain wider attention only during the last five years or so. Special sessions on *EM terrorism* or *Intentional EMI*, have been arranged at several EMC conferences, see e.g. [1, 2].

There are several reasons why the threat against civil systems has to bee taken with great seriousness. One is, of course, the seemingly never-ending increase of electronics in all types of systems, including mission- and safety-critical systems such as aircraft flight control systems and anti-locking braking systems of modern cars. Another reason is that in many cases, contrary to the military scenario, it is possible for the perpetrator to come close to the system under attack. This means that the terrorist need not to have access to military HPM weapons, it will suffice to get hold of e.g. a radar transmitter or even (if the distance is very short) simple “home-built” devices. Finally, another very important reason for the concern is the fact that most civil equipment essentially lack immunity requirements against this type of threat. At microwave frequencies the legal EMC requirements, e.g. the CE requirements in the European Union, usually stop at 2 GHz, and below that frequency the required immunity levels are very modest, of the order of some tens Volts/meter. There is, to the authors knowledge, only one major exemption to this, namely civil aircraft and helicopters, which are designed to withstand the very harsh radar environments at airports.

The effects of HPM on electronics may result in upset or, at high levels of irradiation, even permanent physical damage. Upset (i.e. interference or disturbance) is caused by false in-band signals originating from envelope detection of the HPM due to non-linear effects in the electronic components. The upset may be temporary, i.e. the equipment returns spontaneously to full function after the irradiation, or it may cause permanent failure of the function, i.e. the equipment will require a manual restart or reset. Permanent damage is caused by thermal effects or electrical breakdown in the circuits. In this case the damaged component or equipment has to be repaired or replaced.

This paper presents some results from investigations on HPM susceptibility of unprotected (unshielded) “civil” electronics carried out in Sweden during the last decade. It also discusses ways of mitigation and recommendations for future activities. It should be pointed out that it exists also other electromagnetic threats than HPM against civil systems, see e.g. [1,2].

INVESTIGATIONS ON SYSTEM SUSCEPTIBILITY

Research on HPM effects, as well as other electromagnetic effects such as lightning and NEMP, has been carried out by the Swedish Defence Research Agency, FOI (formerly FOA), the Swedish Defence Material Administration, FMV, and Swedish defence industries during the last decades. A rather comprehensive knowledge has been gained from HPM-testing of systems and components. This shows some very general trends for unshielded equipment (civil equipment and military equipment for which the shield, if available, has been removed) concerning failure levels for upset and for permanent damage, and their frequency dependence, dependence of angle of incidence etc. The testing has been carried out using low level coupling measurements as well as immunity testing at intermediate and high levels. The immunity testing at intermediate level has been made in semi-anechoic rooms and in reverberation chambers. The high level testing has in most cases been carried out using the MTF, the Microwave Test Facility, located at the Saab Aircraft facility in Linköping, Sweden [3], see Fig. 2. The MTF is owned by FMV and operated by Saab Avionics AB. Testing can be performed at five spot frequencies: 1.3 GHz (L-band), 2.86 GHz (S-band), 5.71 GHz (C-band, 9.30 GHz (X-band) and 15.0 GHz (K_u-band). The maximum peak power is 25 MW (L-band), 20 MW (S-band), 5 MW (C-band), 1 MW (X-band) and 0.25 MW (K_u-band). This gives the following peak field strengths at 15 meters test distance: 30 Kv/m (L-band), 34 kV/m (S-band), 17 kV/m (C-band), 11 kV/m (X-band) and 6.1 kV/m (K_u-band). The pulse length can be varied between 0.5 and 5.6 μs. The pulse repetition frequency (prf) can be varied from single shot up to 1 kHz (2.1 kHz for the K_u-band). For the S-band there is a pulse compressor unit available by which the maximum peak power can be increased to 140 MW (at the expense of a shortening of the pulse length down to 0.4 μs). A comprehensive description of the MTF will be given in session E3 “High-Power Electromagnetics”.

The results of the test of unshielded electronics can be summarised as follows:

- Interference effects are much more prominent at low frequencies (L- and S-band) compared to high frequencies.
- Upset starts to occur (L- and S-band) typically around a few hundred volts per meter (rms peak field strength).
- Permanent damage occurs starting from 15-25 kV/m (seen only for L- and S-band)
- Permanent damage can occur also with the equipment turned off.

The pronounced frequency dependence can be explained by the fact that field to cable coupling decreases (as a trend) by the square of the wavelength. Furthermore, measurements of component susceptibility show a similar dependence versus frequency. The typical upset level of a few hundred V/m is consistent with measured data of the receiving cross section of wires together with data from measurements of component susceptibility [4,5]. The level of 15 – 25 kV/m for permanent damage is also typical although the data base for damage is much smaller than for upset. An exception from this level has been reported to occur for a PC flat screen at a level as low as 100 V/m, at a pulse repetition frequency of 1 kHz and a frequency of 140 MHz. However, the modulation was 50% i.e. the pulse length was as large as 0.5 ms.

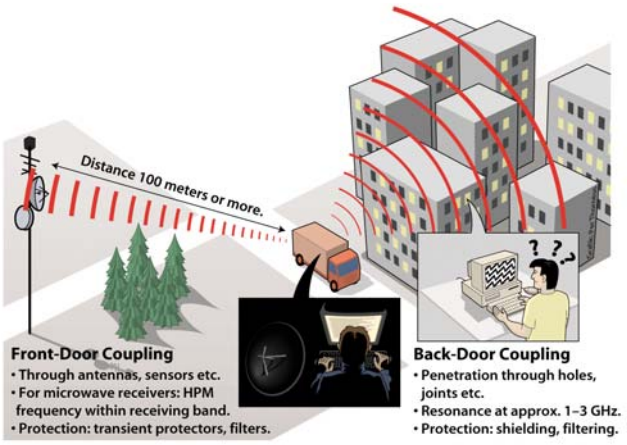

Fig. 1. *Intentional EMI*. The coupling of the HPM radiation can occur either via antennas and sensors, denoted *front-door* coupling, or as *back-door* coupling, i.e. through imperfect shields of enclosures or cables.

Fig. 2. The Swedish *Microwave Test Facility* (MTF). Photo: Saab Avionics, Linköping, Sweden.

Table 1: Estimated distance of action for HPM sabotage.

SOURCE (no shielding)	DISTANCE (meters)			SOURCE Shielding = 30 dB	DISTANCE (meters)		
	15	50	500		15	50	500
HPM Van	Permanent damage	Upset (note 1)	Upset (note 1)	HPM Van	Upset (note 1)	No effect	No effect
HPM Suitcase*	Upset (note 1)	Upset (note 1)	No effect	HPM Suitcase	No effect	No effect	No effect

* May cause permanent damage close to the victim
Note 1): May cause permanent function failure

Based on these investigations estimates can be made of possible distances of action for sabotage using HPM sources. The results in the table 1 are based essentially from test made on cars [6] and other unshielded or de-shielded equipment.

We consider two cases denoted *HPM van* (10 MW peak power) and *HPM suitcase* (100kW). Note that military HPM sources might have output powers of tens of GW, what we consider here is rather a very powerful (10 MW) radar transmitter. We assume the sources to roughly have the same pulse parameters as the MTF L- and S-band sources. For the HPM van we assume an antenna gain of 25 dB_i, e.g. a parabolic antenna with a diameter around one meter. In the table we also include estimates of distance of action if the equipment under attack has a shielding effectiveness (SE) of 30 dB. One reason for choosing 30 dB is that it approximately corresponds to the level of shielding that is necessary for the avionics in civil aircraft and helicopters in order to withstand the radar frequency HIRF (High Intensity Radiated Fields) environments. Another reason is that 30 dB is a level of shielding that can be implemented and maintained by certainly a careful, but not a too exotic and expensive, design.

In many cases unshielded equipment might have a certain degree of protection due to the way it is installed. It might e.g. be installed in a building with thick concrete walls or in a basement below a thick floor of concrete. In many cases it may be installed in such a way that a terrorist is prevented to come close enough. FMV has carried out a number of investigation on telecom stations by measuring the attenuation, i.e. the shielding effectiveness, from locations outside the station, from which a perpetrator might park a car or a truck, to the equipment inside the building [7]. As a guideline, it was found that glass, plasterboard and bricks give almost no attenuation while concrete walls and floors can give a rather good attenuation, especially if the material is thick. A comparison was made between three different types of typical telecom buildings, one built in wood, one using metal plates riveted together and one using metal plates welded together. The susceptibility was estimated by measuring the attenuation of each building, and assuming a truck equipped with a 2GHz 10 MW HPM source, antenna gain 30 dB_i, to be located 50 meters from the building. From the study it can be concluded that the wooden building gives almost no protection, only a few dB at 2 GHz. This means that internal equipment, if unshielded, can be disturbed but probably not permanently damaged. The building built by riveted metal plates gives an attenuation of about 10 dB (at 2 GHz), which means a risk for interference but not for permanent damage. The building built by welded plates has about 5 dB higher SE than the riveted one. This means still some risk for interference. In these studies it was obvious that an immunity assessment of a complex system requires a careful investigation of all sorts of points-of-entry, in the cases referred to here special attention had to be paid to leakage via cables and through door seams. It was also shown that sometimes certain improvements of the protection levels can be achieved by rather simple means such as conductive clothing or metallic shutters for the windows. Also a card reader for admittance control was tested. It was rather easy to disturb, from 80 V/m and above, but the disturbance did not result in an error permitting that one could enter the building.

The data above relates to back-door coupling, defined as coupling to electronics that could be shielded without leading to any degradation of its function, see Fig. 1. For front-door coupling, see Fig. 1, defined as coupling to e.g. antennas and sensors, i.e. to equipment intended to communicate with the exterior, it is known from studies of military equipment that the distance of action, for both upset and permanent damage, can be appreciably larger that for back-door coupling. This holds especially for the case when the equipment works at microwave frequencies, e.g. a radio-link system (which we denote first order front-door coupling). Also this aspect was covered by in the study of telecom stations carried out by FMV [8]. The coupling from the HPM source to the antenna port of the receiver was estimated and compared to experience-based results of the susceptibility of similar receivers. The result of this estimation was that the receiver can be permanently damaged by the 10 MW source (cf. above) from a distance of around 1 km.

PROPOSAL FOR FUTURE WORK

Further susceptibility investigations should be carried out on systems of importance for the civil infrastructure. This should include analyses of field penetration and coupling as well as immunity testing of sub-systems. Where possible, threat level testing of complete systems shall also be carried out.

In parallel, research has to be performed to further develop and evaluate methods for protection, hardness verification, and analysis of complex systems. In the case of back-door coupling one can probably use existing EMC protection methods while front-door protection will require, at least partly, new methods. Of special interest is to evaluate to what extent existing front-door protection, against e.g. radar pulses and NEMP, also work for HPM. Of course, the answer to this question is closely connected to the threat definition, i.e. what kind of HPM sources that may be considered to be used for sabotage. Especially the pulse length is of interest in evaluation of transient protectors. Methods and methodologies for system analysis and hardness verification have to be improved and adapted to civil systems. One challenge is the, in many cases, huge complexity of civil systems making a statistical treatment highly desirable. It is foreseen that computer-based expert systems and numerical field solvers will be of great use in system analysis.

CONCLUSIONS

Based on HPM susceptibility testing of typical civil electronics, such as cars, computers and telecom equipment, it is concluded that the distance for HPM sabotage can reach to about one kilometre. This distance requires a very powerful radar transmitter but not a military HPM weapon. For in-band front-door coupling this may cause permanent damage while for back-door coupling only upset will occur at this distance. Even the latter may however result in very serious problems if it leads to a permanent function failure, i.e. that a restart or a reset is needed to regain its function. Although most civil electronics per se lack protection against microwave radiation it may be fairly well protected due to the way it is installed in a building. It might e.g. be located in a cabinet behind a fairly protective wall and/or kept at a sufficiently long distance from a perpetrator. Future work should aim at investigations on the susceptibility of important systems and on development and evaluation on methods for protection and analysis of complex systems.

REFERENCES

[1] Proceedings of *13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, Supplement*, Zurich, Switzerland, February 16 – 18, 1999.
[2] Proceedings of *ICEAA01 International Conference on Electromagnetics in Advanced Applications*, Torino, Italy, 10 – 14 September 2001.
[3] "Microwave Test Facility", issued by Saab Avionics, Electromagnetic Technology Division, SE-581 88 Linköping, Sweden, www.avionics.saab.se.
[4] S. Silfverskiöld, M. Bäckström and J. Lorén, "Microwave Field-to-Wire Coupling Measurements in Anechoic and Reverberation Chambers, *IEEE Trans. on Electromagnetic Compatibility*, Vol EMC-44, No.1, February 2002.
[5] G. Göransson, "HPM Effects on Electronic Components and the Importance of This Knowledge in Evaluation of System Susceptibility", Proceedings of *1999 IEEE International Symposium on Electromagnetic Compatibility*, Seattle, USA, August 2 – 6, 1999.
[6] M. Bäckström, "HPM Testing of a Car: a Representative Example of the Susceptibility of Civil Systems", Proceedings of *13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, Supplement*, Zurich, Switzerland, February 16 – 18, 1999.
[7] M. Eriksson, "HPM – riskbedömning av tre telestationer", *FMV report: PROV 21 8480:49427/00,* 2000-12-22. Defence Material Administration (FMV), Box 13400, SE-580 13 Linköping, Sweden
[8] M Eriksson, "HPM-undersökning av inkoppling av HPM-pulser via antenner*", FMV report: PROV 21 8480:51306/00*, 2000-12-21. Defence Material Administration (FMV), Box 13400, SE-580 13 Linköping, Sweden.