

THE THREAT FROM INTENTIONAL EMI AGAINST THE CIVIL TECHNICAL INFRASTRUCTURE

Mats Bäckström

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

Keywords: Intentional EMI, HPM, HEMP

ABSTRACT

The widespread reliance of electronics in our society, also in mission- and safety-critical applications, brings the question of its robustness against electromagnetic interference (EMI) into focus. *Intentional EMI* (IEMI) refers to scenarios where the intent is to destroy or disturb the electronic function of a system. This kind of threat has been recognised for rather a long time by the military. Today, the threat against civilian systems, private as well as public, is getting an increased attention. For more than a decade the Swedish defence authorities have, in co-operation with Swedish industry and other countries, studied the effects of High Power Microwave (HPM) radiation on electronic systems. From these studies, it is concluded that the distance for HPM sabotage can reach about a kilometre. A protection level of about 30-40 dB should suffice for most civilian IEMI-HPM scenarios. The protection can in most cases be accomplished by use of standard EMC techniques. Apart from HPM there are also other IEMI threats that need to be addressed, such as the HEMP, the electromagnetic pulse from a nuclear explosion at high altitude.

INTRODUCTION

Our society is rapidly becoming more and more dependent on electrical and electronic systems for its function. This dependence comprise almost all aspect of modern life, from entertainment, sports and leisure activities to structures of critical importance for the basic functions of the society, such as transmission of electrical power, medical care, telecommunications, transportation, banking and finance, food and water supply, emergency services, radio/television and decision making. The widespread reliance of electronics, also in mission- and safety-critical applications of fundamental importance, brings the question of its robustness against electromagnetic interference (EMI) into immediate focus. Of special interest is the susceptibility of communication systems and of computer systems, used e.g. for information processing or control functions, see Figure 1. Of great interest is

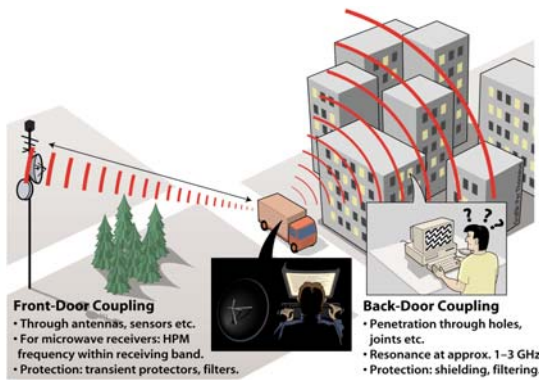


Figure 1. The coupling of the HPM radiation can occur either via antennas and sensors, denoted front-door coupling, or as back-door coupling, i.e. through imperfect shields or to cables.

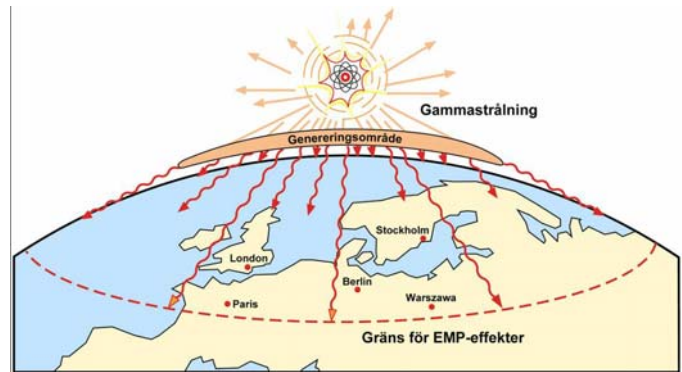


Figure 2. An electromagnetic pulse generated by a nuclear explosion at high altitude, around 30 km or more, over northern Europe.

also the rapidly spreading use of new types of wireless systems, such as Bluetooth, since these by their nature are open systems and thus easy to interfere with and difficult to protect. Wireless systems are today finding novel applications in many applications in e.g. processing industry, unmanned vehicles, traffic control systems, railways, cars etc. As an example, in the future it is planned that the European railways will have a common traffic management system, the *European Rail Traffic Management System* (ERTMS), see Figure 3. In 1996 the EU decided that ERTMS would become the standard for all high-speed lines. All instructions and line information to the engaged driver will be received by radio. No optical signals are required along the line. Several European countries, such as Switzerland, Italy, Holland, Spain and Sweden are now implementing ERTMS. In Sweden there is an ongoing project on Intentional EMI applied to railway systems [Thottappillil et al., 2005]

ERTMS/ETCS – LEVEL 2 ON THE BOTHNIA LINE

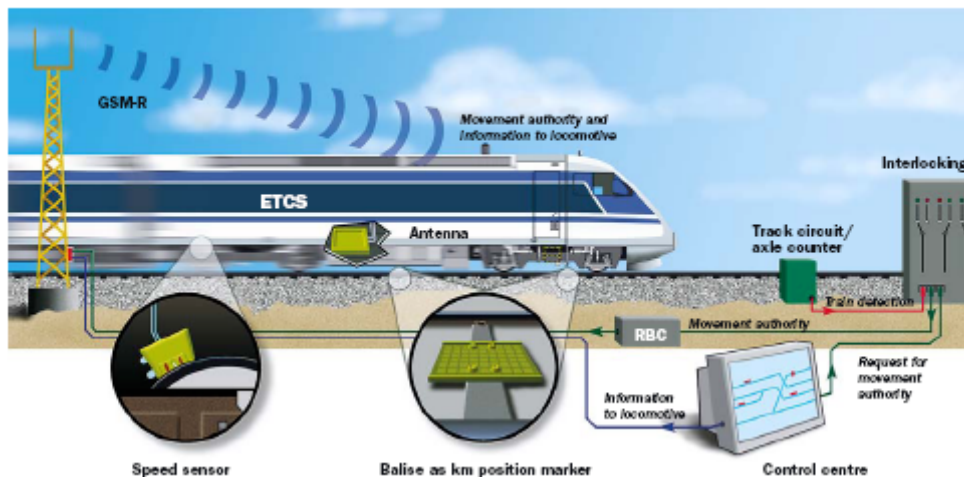


Figure 3. The *European Rail Traffic Management System* (ERTMS), level 2, for the Bothnia line in Sweden. From www.botniabanan.se.

Interference may be caused by natural sources such as lightning or electrostatic discharges, or by the immense number of man-made emitters of electromagnetic energy. In the latter case the interference may be unintentional due to lack of compatibility between the electromagnetic emission (conducted or radiated) from one electronic apparatus and the susceptibility of neighbouring equipment, or intentional, where the sole purpose is to disturb or destroy the function

of the system under attack. While the intentional electromagnetic threat has been recognised for rather a long time by the military, the threat against civilian systems, private as well as public, are now getting an increased attention. The increased awareness of the threat is reflected both in the scientific community and in the public debate. As a result of the former the subject has been addressed a several conferences, see e.g. [EMC Zurich'99, 1999] and [EMC Europe Workshop, 2005]. A special journal issue was recently published [*IEEE Trans. on EMC*, 2004].

There are several reasons why the threat against civil systems has to be taken with great seriousness. One is the above mentioned seemingly never-ending increase of electronics in all types of systems. Another reason is that in many cases, contrary to the typical military scenario, it is often possible for the perpetrator to come close to the system under attack. This means that the terrorist need not to have access to military 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. There is, to our knowledge, only one major exemption to this, namely civil aircraft and helicopters, which are designed to withstand the very harsh radar environments at airports.

So far, most reports and discussions on *Intentional EMI* (IEMI) have probably been focussed on the threat from HPM (High Power Microwaves) sources. The term HPM usually includes both narrow-band, i.e. radar-like, HPM (which this paper mostly deals with) as well as radiated powerful wideband pulses, often denoted UWB. UWB have the main part of the frequency content at or near microwave frequencies. However, Intentional EMI also includes other types of electromagnetic threats such as injection of low frequency pulses on power or telecom wires entering a building. Another alarming threat, which recently has gained a renewed interest is the electromagnetic pulse generated from a nuclear explosion at high altitude, the so called HEMP (High Altitude EMP), see Figure 2.

INVESTIGATIONS ON SYSTEM SUSCEPTIBILITY

Research on HPM effects has been carried out by the Swedish Defence Research Agency FOI, the Swedish Defence Material Administration (FMV) and Swedish defence industries during the last decades, often in co-operation with other countries. As a result, a comprehensive knowledge has been gained showing some very general trends for unshielded equipment concerning failure levels for upset and for permanent damage, frequency dependence, dependence of angle of incidence etc. By unshielded equipment we mean civil equipment and military equipment for which the protection, if available, has been removed. The testing has been carried out using low level coupling measurements as well as radiated susceptibility testing on complete systems at intermediate and high power density levels. For large systems, testing has usually been carried out using the MTF, the *Swedish Microwave Test Facility*, see below.

The effects of HPM on electronic systems 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. The latter may result in a catastrophic event. Permanent damage is caused by thermal effects or electrical breakdown in the electronic circuits. In this case the damaged component or equipment has to be repaired or replaced.

The Swedish Microwave Test Facility

The Microwave Test Facility, MTF, was designed by the US Company TITAN Beta and delivered in 1993 to Saab Communications AB, who operates the system for the Swedish Defence Material Administration, FMV. It was mainly specified and designed for aircraft HIRF (High Intensity Radiated Fields) testing. The overall requirement on the system was to generate a sub-set, at five spot frequencies, of the worst-case environment for Gripen, the Swedish fighter aircraft. The microwave test facility features were based on the knowledge of the microwave operational environment for civil and military systems. Also, research work indicated some desirable features of the MTF design such as need for a certain exposure area, pulse and burst length, pulse duration and repetition rate.



Figure 4. The Swedish Microwave Test Facility (MTF). Photo: Saab Communications AB, Linköping, Sweden.

General MTF System Data

The MTF is mobile and contained in a 12 m ISO container, see Figure 4. It is powered by a 230V, 540 kVA, AC, diesel generator. The capability of the system consists of five microwave sources at fixed frequencies in the L, S, C, X and Ku radar bands. Parameters, such as the pulse repetition frequency (PRF), the pulse and burst length, and the output power, can be varied. The generator data maximum characteristics are given in Table 1. The data are for normal outdoor operation. All maximum characteristics cannot be attained simultaneously, e.g. the maximum PRF cannot be attained at maximum pulse length.

Table 1. FMV Microwave Test Facility, maximum characteristics. PCS: Pulse compression System, CA: Cassegrain antenna. E_{peak} is given as the RMS peak value.

| Radar band | f (GHz) | Average Power (kW) | Maximum Power (MW) | Gain (dB) Outdoor antennas | PRF (pps) | Pulse duration (μs) | E _{peak} @ 15 meter (kV/m) |
|------------|---------|--------------------|--------------------|----------------------------|-----------|---------------------|-------------------------------------|
| L-band | 1.300 | 49 | 25 | ca 30 | 1000 | 5 | 30 |
| S-band | 2.857 | 20 | 20 (PCS: 140) | ca 30 (CA: 37) | 1000 | 5 (PCS: 0.4) | 30 (PCS: 80) |
| C-band | 5.710 | 5 | 5 | ca 30 (CA: 40) | 1000 | 5 | 17 |
| X-band | 9.300 | 1 | 1 | ca 30 | 1000 | 3.8 | 10 |
| Ku-band | 15.00 | 0.28 | 0.25 | ca 30 | 2100 | 0.53 | 6 |

System Data for Outdoor Testing

For outdoors HIRF testing the system is equipped with +/- 30 degrees horizontally and +/- 15 degrees vertically sweeping antennas. The diagonal horn antenna patterns were decided for a test object distance of 15-25 m. The radiation footprint at the test distance was specified to have a diameter of at least 10 wavelengths and should well cover any access door of an aircraft. At 15 meter distance the 3 dB beam width is 2.8 m at 1.3 GHz, 2.4 m at 2.857 GHz, 2.0m at 5.71 GHz, 1.6 m at 9.3 GHz and 1.1 m at 15.0 GHz. The near field limit of the antennas is 12 meters or less. The radiation polarity can be remotely shifted between vertical and horizontal mode.

FOI Facilities for HPM Susceptibility Testing

At FOI there are a number of test facilities, such as anechoic and reverberation chambers (mainly) for coupling measurements; lab for component testing by means of injection of microwave energy; a 3 GHz, 700 kW magnetron source for high level irradiation of small sized objects; and a RADAN 303B ultra-wide band source, see Figure 5.



Figure 5a. 3 GHz, 700 kW magnetron at FOI. Magnetron at right, transmitting antenna at left, test object on the carriage. Variation of field strength achieved by moving the carriage along the rail.



Figure 5b. Measurement set-up for testing of component susceptibility to HPM, and for characterisation of protection devices against HPM (limiters).



Figure 5c. Reverberation chamber at FOI. The chambers is connected to another reverberation chamber by the access door at the rear wall.



Figure 5d. RADAN 303B source equipped with a sub-ns slicer yielding an UWB pulse with ns-second pulse length and sub-ns rise time.

System Immunity Testing

Investigations on susceptibility to HPM carried out by FOI and FMV include the following:

- Missiles
- Tactical Radio Link
- Army radio
- Cars

- Computers
- Telecom stations
- GPS receivers, WLAN equipment, Wire-less Cameras, ...
- Low Noise Amplifiers, Limiters, ...

The HPM energy couples to the interior electronics of a system through two generic paths, *front-door coupling* and *back-door coupling*, see Fig. 1, here defined as follows:

1) *Front-Door Coupling*: The HPM radiation couples to equipment ports intended for wireless communication or interaction with the external environment. Hence, they cannot easily be fully shielded against microwave radiation without loosing or severely degrading their function. Examples are antennas and sensors. We subdivide it into the following.

a) *Front-Door Coupling, first order*: The frequency of the HPM radiation coincides, at least partly, with the working frequency of the equipment. An example is a telecom base-station irradiated in its pass band.

b) *Front-Door Coupling, second order*: The frequency of the HPM radiation does not coincide with the working frequency of the equipment. An example is a radio antenna.

2) *Back-Door Coupling*: The HPM radiation couples to electronic components through imperfections (apertures) in an electromagnetic shield, giving rise to a diffuse and complex field pattern within the shielded structure. The apertures can be unintentional or intentional. Examples of the latter are holes for drainage and ventilation. The radiation may also couple directly to an external wire connected to a component or a subsystem. The reason to define such a wire as back-door coupling and not as a second-order front-door coupling is due to the fact that the wire could be shielded without degrading its function.

The main results, regarding *back-door coupling* of the test of unshielded electronics can be summarized as follows, a more comprehensive account is given in [Bäckström, Lövstrand, 2004] and some more recent results in [Arnesen et al., 2005]:

- Interference effects are much more prominent at low frequencies (*L* and *S* band) compared to higher 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.

Some exceptions from the trends given above have been seen, such as:

- Upset levels as low as 15 V/m have been seen. This happened when the electronic control module in a public bus engine was irradiated at 1.3 GHz, at 200 Hz pulse repetition frequency and 50% duty cycle, causing the engine to stop.
- Damage levels as low as 100 V/m have been seen. This happened for a PC flat screen, at a frequency of 140 MHz and a pulse repetition frequency of 1 kHz. The duty cycle was 50%.

Some additional results for back-door coupling:

- The pulse length is of importance for both upset and permanent damage. For upset the susceptibility level, in terms of field strength, is usually lower for longer pulses. For permanent damage the same observation holds.
- At the pulse repetition frequencies (PRF) investigated, $PRF \leq 1$ kHz, permanent damage seems to be caused by the first pulse, i.e. neither thermal stacking nor any gradual erosion between subsequent pulses seem to occur.

- The PRF is crucial for some types of disturbances. It seems to be related to an operation cycle of a critical electronic function. A low PRF gives a low disturbance probability and requires high field intensities.

The rapid decrease of susceptibility versus frequency can be explained by:

- Field-to-wire coupling decreases, as a trend, by the square of the wavelength.
- Susceptibility of electronic components shows a similar dependence. For highly shielded objects this can, to some extent, be counteracted by the usual decrease of the shielding effectiveness towards higher frequencies.

For front-door coupling, it is well-known that the distance of action, for both upset and permanent damage, can be appreciably larger than for back-door coupling. This holds especially for the case when the interfering source operates at the same frequency as the victim (first order front-door coupling), e.g. a radio-link system. In first order front-door coupling it is important to differ between jamming, which can be accomplished by use of narrowband sources at low power levels (of the order of Watt), and HPM. Of course, jamming devices could be of great use for a perpetrator, see [Radasky, Bäckström, 2005], especially since jamming devices are easy and cheap to build. In the present context the concept of HPM in front-door scenarios refers to situations where the purpose is either to cause permanent damage or to perform wideband jamming, since the latter will require a source of high output (peak) power. The advantage of wideband jamming is that no information is needed beforehand about the operating frequency of the victims which also means that different types of equipment can be interfered with simultaneously. In addition one may of course also get back-door interference.

Permanent damage due to in-band front-door coupling has been studied by FOI and FMV in various ways. System studies include a radio link system, in which case HPM pulses were injected into the antenna port, and a telecom station. In the latter case 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 study was that the receiver can be permanently damaged by a 10 MW source from a distance of around 1 km. Injection of 1 μ s pulses at the antenna connector of a WLAN system showed a destruction level of 16 μ J [Nilsson et al, 2005]. A comprehensive study on the susceptibility of low noise amplifiers (LNA) is currently conducted at FOI. Results show destruction levels of around 0.5 μ J for pulses having a length of 100 ns, 2.5 μ J for 1 μ s pulse length and 25 μ J for 10 μ s pulse length. [Nilsson, Jonsson, 2005].

In Sweden, less data has been collected concerning the impact of UWB on systems. However, it seems that considerably higher field values are required to cause permanent damage, alternatively much higher pulse repetition frequencies than kHz. It seems reasonable to assume that the probability for destruction decreases since the pulses contain comparatively little energy (although other mechanisms than heating by the pulse energy itself for permanent failure may occur). Damage at high values of the PRF can be explained by thermal stacking in the victim component, i.e. the time between each pulse is so short that the heat from the preceding pulse has not enough time to dissipate. In the discussion of these questions, references should be given to the very extensive work done by the German companies Diehl and Rheinmetal on both development of wideband sources and on investigation on system susceptibility for these types of threats, see e.g. [Bohl, Stark, Wollman, 2004].

ESTIMATES OF DISTANCE OF ACTION FOR HPM IN A CIVIL SCENARIO

Based on the investigations referred to above, estimates can be made of possible distances of action for sabotage against unprotected equipment using HPM, see Table 2a. We consider two cases denoted *HPM van* (10 MW peak power, 10 J peak energy) and *HPM suitcase* (100 kW, 0.1 J). Note

Table 2a. Estimated Distance of Action for HPM. Back-door coupling and second order front-door coupling.

| HPM-SOURCE | DISTANCE | | | |
|--|----------------------------------|----------------------------------|---------------|------------------|
| | In close vicinity | 15 meter | 50 meter | 500 meter |
| HPM Van** (10 MW, 10J) | Irrelevant | Permanent Physical Damage | Upset* | Upset* |
| HPM Suitcase** (100 kW, 0.1 J) | Permanent Physical Damage | Upset* | Upset* | No Effect |

- *: 1. May cause permanent functional damage!
 2. Front-door coupling (in-band) might cause permanent damage at the same distance (interference at much larger).
 **: UWB/HPM sources of similar size may give similar distances, but permanent damage likely requires a very high PRF.

Table 2b. Estimated Distance of Action for HPM. 30 dB protection level.

| HPM-SOURCE | DISTANCE | | | |
|--|-------------------|------------------|------------------|------------------|
| | In close vicinity | 15 meter | 50 meter | 500 meter |
| HPM Van (10 MW, 10 J) | Irrelevant | Upset* | No Effect | No Effect |
| HPM Suitcase (100 kW, 0.1 J) | Upset* | No Effect | No Effect | No Effect |

certainly a careful, but not a too exotic and expensive, design. In first order front-door coupling, i.e. in-band coupling, a protection level of 30 dB is estimated to give protection against permanent damage (but not disturbance). In second-order front-door coupling 30 dB will give the same protection as for back-door coupling.

PROTECTION METHODS

1) *Back-Door Coupling*. If we assume a protection level of 30 dB to be sufficient, cf. Table 2b, conventional EMC protection techniques, such as shielding and filtering, should suffice. As already noted, a protection level of 30 dB is roughly what is needed for civil aircraft in order to comply with their external environment.

2) *Front-Door Coupling*. While in-band disturbances are difficult to neutralize, permanent damage effects can be mitigated by use of transient protectors. Out-of-band disturbances, i.e., second-order front-door coupling, can be handled by use of filtering, e.g., for radio equipment, or by use of metallic meshes or thin films for optical equipment. Often, protective measures will lead to a degradation of the intended function of the system.

It shall be pointed out that, especially in civil scenarios, protection may be achieved by simply locating the equipment at a sufficiently large “electrical” distance from a perpetrator.

OTHER IEMI THREATS

As noted in the introduction the IEMI threat to the society is not limited to microwave frequencies. Studies concerning damages caused by injection of low frequency pulses on wires entering a building has been reported, see [IEC 61000-1-5, 2004] and references therein. The HEMP, or NEMP, threat has gained a renewed interest. In July 2004 a U.S. Congressional Commission reported on the potential impact of HEMP on the civil infrastructure [Report., 2004]. In the report it is stated “Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication”, and “EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.” Finally, it shall be emphasized that a lot of harm can be caused by use of cheap and easy-to-build jamming devises.

INTERNATIONAL ACTIVITIES AND STANDARDIZATION

At its General Assembly 1999 the IEMI problem was recognized by the International Radio Scientific Union (URSI) and resulted in the “Resolution of Criminal Activities using Electromagnetic Tools”. Since then a number of sessions on IEMI have been arranged at various conferences.

A major IEMI standardization effort is currently underway. This effort has been organized under the International Electrotechnical Commission (IEC), an example of the outcome is [IEC 61000-1-5, 2004].

Concerning practical implementation of protection measures on civil systems, to our knowledge very little work has been done, at least in Europe.

CONCLUSIONS

- HPM testing at high-field levels has been carried out on military equipment as well as on civil equipment. It is concluded that the distance for HPM sabotage can reach about a kilometre. This distance requires e.g. 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.
- The threat can to a large degree be mitigated by existing standard EMC protection methods.
- In the future, the vulnerability of critical systems of the infrastructure should be investigated in a thorough and systematic way. Also, protection methods should be evaluated and applied, and further developed.
- In this process also other types of IEMI threats, such as HEMP, should be addressed.

ACKNOWLEDGEMENT

This work was financially supported by The Swedish Armed forces. The author acknowledges comments from and discussions with colleagues at FOI, FMV, and national and international co-operating organizations.

LITERATURE

- Arnesen, O.H., et al., 2005, High Power Microwave effects on Civilian equipment, Proceedings of XXVIIIth General Assembly of International Union Radio science (URSI), New Delhi, October 23-29, 2005
- Bohl, J., Stark, R.H., Wollman, 2004, G., RF Weapons for Non-Lethal Interference and Destruction of Communication, Information and Electronic Systems, proceedings of 2nd European Workshop on Survivability, Noordwijkerhout, The Netherlands, 23-25 March, 2004.
- Bäckström, M.G., Lövstrand, K.G., 2004, Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experiences, IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, August 2004, pp. 396 – 403.
- EMC Europe Workshop, 2005, Proceedings of EMC Europe Workshop. Electromagnetic Compatibility of Wireless Systems, Rome, Italy, 19-21 September 2005.
- EMC Zurich'99, 1999, Proceedings of 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, Supplement, Zurich, Switzerland, February 16 – 18 1999.
- IEC 61000-1-5, 2004, Electromagnetic compatibility (EMC) - Part 1-5: General – High power electromagnetic (HPEM) effects in civil systems, 2004-11.
- IEEE Transactions on Electromagnetic Compatibility, 2004, Vol. 46, No. 3, August 2004.
- Nilsson, T., Jonsson, R., 2005, Investigation of HPM Front-door Protection Devices and Component Susceptibility, FOI Technical Report, FOI-R--1771--SE, November 2005, Swedish Defence Research Agency FOI, Sensor Technology, P.O. Box 1165, SE-581 11 Linköping, Sweden.
- Nilsson, T., Lundén, O., Bäckström, M., 2005, HPM Susceptibility Measurements on GPS and WLAN Systems, Proceedings of EMC Europe Workshop, Electromagnetic Compatibility of Wireless Systems, Rome, Italy, 19-21 September 2005.
- Radasky, W.A., Bäckström, M., 2005, Overview of the Threat of Intentional EMI (IEMI) to Civil Wireless Systems, Proceedings of EMC Europe Workshop, Electromagnetic Compatibility of Wireless Systems, Rome, Italy, 19-21 September 2005.
- Report of the Commission to Assess the threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume I: Executive Report,” EMP Commission, April 2004.
- Thottappillil, R., et al., 2005, Response of Civilian Facilities to Intentional electromagnetic Interference (IEMI), with Emphasis on the Swedish Railway Network, Proceedings of EMC Europe Workshop. Electromagnetic Compatibility of Wireless Systems, Rome, Italy, 19-21 September 2005.