



EMCignal Solution to Stop High-Power Microwave

White Paper

EMCignal is offering a solution to stop and protect from High-Power Microwave (HPM) the new threat and electronic weapon possibility. What is HPM: A focused wave produces a very high voltage pulse that can damage and even destroy electronic hardware. Destructive weapons of this kind can easily be manufactured by terror groups, and may be used to damage crucial systems from a distance. The high-intensity pulse can be generated by relatively simple devices. The pulse is received by communication or power lines, which serve as antennas. These lines carry the signal to the electronic components to which they are connected, enabling the pulse to target and destroy essential hardware elements, even when protected in bunkers.

There is a real danger that E-weapon, when applied to essential systems (power plants, communication and computer centers, etc.), will serve hostile elements to create chaos.

EMCignal is currently developing a highly efficient protection technology, as well as products designed to counter such threats.

1 Abstract

An E-weapon is a high-power radio frequency microwave intended to cause damage to electronic systems.

The idea behind the E-weapon is that when a strong electromagnetic field, created by a high-power electromagnetic wave, hits a conductor, a very high voltage spike – up to tens of thousands of volts – develops.

None of the existing and future components, such as semiconductors, can withstand a voltage spike of this magnitude.

As a result, a destructive chain effect is initiated. First, a number of chips are damaged, followed by the immediate destruction of computers or controllers, possibly leading to complete system failure. When the E-weapon hits power stations, surface and air transportation, water control, communications, medical infrastructures or computer-based equipment, the outcome can cause chaos on a national scale.

Several armies are already equipped with E-weapons, as a modern threat against military and strategic targets. Unfortunately, it is relatively easy for terrorist groups to develop and use E-weapons, which could inflict major blows and cause severe damage to national utilities and infrastructure, as well as to business and commercial entities.

A simple device can cause traumatic damage on a national scale.

EMCignal Ltd. has developed high performance, yet cost-effective protective solutions. The EMCignal solution consists of state-of-the-art technology and efficient plug-and-play protective products.

EMCignal's breakthrough offers easily installed small sized add-on devices that provide a highly reliable full protection solution.

2 Background

IT infrastructure, electronic instruments and electrical systems are all highly sensitive and vulnerable to high-power electromagnetic fields. When a focused electromagnetic beam hits a copper conductor (e.g. communication wires, power lines, leads on printed circuit boards, IC terminals, etc.), an extremely high voltage spike (tens of thousands of volts) develops. This spike immediately destroys ICs and other semiconductors, as well as sensitive components.

As a result, the whole system (of whatever type) experiences malfunctions, degradation or severe damage. The chain effect could lead to damage on a massive scale.

Devices that produce a focused high-power electromagnetic beam have been added to the electronics warfare arsenal as "E-weapons". These are considered non-lethal warfare from the human point of view, but are extremely lethal to electronic systems.

Armies using these weapons will definitely cripple and neutralize their enemies, as almost every system is computerized to some extent. This includes combat systems (avionics, naval and ground), communications, intelligence, administration and even military logistic vehicles.

The means to create an electromagnetic pulse are available (and are not too complex) even to negative elements – terrorists and organized crime. A small, handheld electronic system the size of a briefcase could have a devastating effect within a radius of several dozen meters. A mobile system could incapacitate every computerized or electronic system within a radius of several miles.

An in-depth analysis of the information indicates:

- E-weapons are readily available
- Almost every aspect of everyday life is vulnerable
- The after-effect of a high-power microwave pulse is critical
- There is a clear and present danger that E-weapons could fall into the wrong hands
- Existing protection technologies are limited
- The vast majority of equipment is unprotected

The IEEE symposium held in Chicago in August 2003 published a draft standard which is to be redrafted as a recommended standard, and subsequently to a mandatory one.

These facts challenged EMCignal to develop a very high performance, yet highly cost-effective, protective solution.

3 What is an E-weapon?

E-weapons are high-power radio frequency waves that cause damage to electronic systems.

Throughout history, weapon systems have been developed by one side to take out the equipment and other facilities of the other side.

We are now in the electronics age, where almost every piece of equipment includes electronics. The developed (western hemisphere) world is totally dependant on computers, communications and other instruments, all of which are electronics based. This applies to military and defense equipment, as well as to commercial elements and commodities.

Consequently, the significant advantages that have been made available to mankind have now become an Achilles' heel.

It is therefore natural that nations, militaries and other organizations, including negative factors such as terrorists and organized crime, are seeking means to enable them to strike at the soft underbelly of their enemies – i.e. electronic systems.

In the mid-twentieth century, scientists began researching the possibility of developing an electromagnetic wave powerful enough to incapacitate electronic systems on impact. Today the technology is mature, and several kinds of radio frequency wave generators – “E-weapons” – are now in use.

The idea behind the E-weapon is that when a strong electromagnetic field, generated by a high-power electromagnetic wave in the microwave frequency range, hits conductors, a very high voltage spike – up to tens of thousands volts – occurs.

None of the existing components, such as semiconductors, can withstand a voltage spike of this magnitude.

The direct result is an electrical overstress that is well above the designed limit of the components. For example, almost all logic components are designed to operate at 1.5 to 5 volts. A high voltage spike as described above will immediately destroy or damage the components and circuitry.

The end effect is permanent system failure, instant or dormant.

In the case of a single PC the loss is affordable, but if a main infrastructure facility (TV station, electrical power station or military HQ) is hit, the chain effect is dramatic and acute.

One of the most effective ways of delivering sufficiently high energy to hit and destroy electronics is the high-power microwave (HPM). HPM generators are the bases of all E-weapon configurations.

4 How it works

The high-power microwave (HPM) is a pulse that is produced by a specific generator.

There are two kinds of HPM waves:

- Broadband wave

A broadband wave acts like a light bulb in a room. It affects the volume surrounding it.

- Narrowband wave

A narrowband wave acts like a spotlight or beam of light.

It is easier to produce a broadband wave and focus it on a target using a directional high gain antenna. The wave propagates at the speed of light. It is invisible and keeps moving straight ahead since it is not influenced by gravity. Continuity of broadband pulses creates a beam effect, which on a time axis produces high energy ($E = \int p dt$).

This energy penetrates electronics through any entrance, such as air-conditioners, non-metallic casings and exposed circuits. But the most critical and significant are the copper input/output (I/O) wires, including power, communication, video, sensors etc.

Such an electromagnetic wave produces high voltage and high current in the wires. These voltages and currents are developed between each line and its return, and the system ground (earth).

The modern electronics is based on low voltage (up to ± 15 volts), while in order to increase the consumption in fast communication circuitry voltages of 1.2V or 1.8V are fed into the ICs.

It is obvious that a higher voltage blast (hundreds of volts) will destroy semiconductors and damage the system.

To learn more about HPM, visit the following sites (there are more):

1. www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html
2. www.metatechcorp.com/URSI.htm
3. www.metatechcorp.com/Slide_Menu.htm
4. <http://www.globalsecurity.org/military/systems/munitions/hpm.htm>
5. www.wileyurope.com/WileyCDA/WileyTitle/productCd-0780360060.html
6. <http://66.102.11.104/search?q=cache:www.spectrum.ieee.org%2FWEBONLY%2Fpublicfeature%2Fnov03%2F1103ebom.html+%22Iraqi%20TV%20station%22>

5 Potential E-weapon targets

E-weapons can be used against:

- a) Military targets;
- b) National utilities and infrastructure;
- c) Commercial massive use computers, instruments and equipment;

Potential victims are:

Military targets:

- Command and control facilities:
 - Headquarters
 - Air traffic control stations
- Communications:
 - Transmitters and amplifiers
 - Communication stations relays
- Intelligence facilities:
 - Commint
- Aircraft:
 - Aircraft avionics
 - Communications
 - Navigation/ALS

- Armoured vehicles (tanks, APCs, artillery):
 - Communications
 - Fire control systems
- Logistic (tracked) vehicles:
 - Engine and gear electronic control systems

National utilities and infrastructure:

- Electrical power stations:
 - Production and safety control room
 - Distribution control systems
- Broadcasting and communications transmitters
- Banks and financial institutions:
 - Main and backup servers
 - Data transfer networks
- Airports and air traffic control:
 - Tower control and communications systems
 - Airfield infrastructure
- Commercial aircraft:
 - Communications and flight control systems
 - Vital onboard systems
- Railway control:
 - Signalling communications
 - Onboard systems
- Medical facilities:
 - Life-support systems:
 - Infrastructure

Massive damage or malfunction to:

- PCs
- ATMs
- E-election
- Advanced bar-coding systems

6 E-weapons

E-weapons can be realized in several configurations according to user needs.

6.1 Military E-weapon

Military E-weapons can be realized in:

- Air E-bomb: A high-power generator dropped by aircraft to affect a wider area.
- E-Cruise missile: A Cruise missile equipped with an HPM generator.
- E-Shell: An artillery device launched from a cannon in a close and restricted zone.
- Static E-ammunition generator (E-gun): A device carried by a ground vehicle for use at close range.
- Handheld E-ammunition: HPM for use by Special Forces.

6.2 Terrorism and organized crime

Many technologies developed due to military initiatives have subsequently gone into civilian and commercial use. Unfortunately, this reality includes also negative aspects. Since the resources (financial and technological) required, to build an E-weapon for limited usages are not extraordinary, there is a real danger that these will fall into the hands of terrorist organizations.

At the 13th International Symposium on Electromagnetic Compatibility in Zurich (February 1999), electromagnetic terrorism was defined as:

“Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electrical systems, thus disrupting, confusing or damaging these systems for terrorists or criminal purposes”.

Terrorists are most likely to use E-weapons against massive commercial applications targets, as described above.

A seemingly innocent car driving along a highway near a power plant can carry a device able to take out any electronic function within a one-mile range and initiate a chain reaction (domino effect) in the power plant with unpredictable consequences.

Another scenario could involve an individual carrying an attaché case, entering a transaction room in a bank or stock exchange and crippling the computers and network on the entire floor. The damage and chaos would be huge.

7 The principle of dealing with an E-Weapon

Total protection is based on two factors:

- General shielding of electronic systems

Metal shielding or the use of thick concrete walls can achieve system protection. Walls must be free even of air-conditioning system vents.

None of this requires any special technology.

- Filtering of input and output (I/O) wiring

Protecting inputs and outputs is the main issue. Since wires act as antennas, special consideration should be applied.

The existing filtering technologies are limited in performance (frequency range, linearity, attenuation, etc.).

A highly reliable and cost-effective solution that requires special expertise.

8 EMCSignal's answers to E-Weapon threats

The protection against E-weapons is based on a breakthrough filtering technology, "UG technology", developed, tested and applied by EMCSignal.

"UG technology" protects the ports of all input/output (I/O) copper wires in the system (such as: communication lines, video, sensor power lines and others).

"UG technology" works linearly in a wideband frequency range – above 20 GHz. It is a state-of-the-art new filtering technology, which maintains signal integrity while attenuating any undesired signals.

This filtering specifically protects the electronics against intentional aggressive signals produced by the E-weapon.

The response time of the UG filtering technology is extremely short and energy absorption and shunting capabilities are extremely high. During all of this time, the protection device continuously provides the rated voltage and current to the system.

This enables military and commercial/civilian systems to withstand high-power microwave weapons.

9 The value proposition of EMCSignal's approach

EMCSignal's breakthrough solution offers the following advantages:

- Full protection;
- Inexpensive;
- Extremely easy to install (plug-and-play);
- No degradation during life cycle;
- No maintenance required;
- Very small size;
- High reliability;

10 Protection methodology

EMCSignal's protection methodology is based on the assumption that it is relatively easy to shield sensitive electronic systems or even sub-systems by metal casing. This protects the electronic circuitry. However, the circuitry is still vulnerable through its input/output (I/O) wiring. Therefore, the main issue is to protect the wiring I/Os (communications, power lines, etc.) passing through the electronic system.

The protection consists of two main parts:

- Protection units that are deployed in all ports connected to copper wires, including communication wires, power wires, antenna wires, etc.
- Detectors that sense and provide an alert when a high magnitude electromagnetic field is developing in the area.

Electronic shielding is applied in addition to the above as required.

11 Protection products

□ Technology level

"UG" filtering is the base technology of the protection.

□ Basic protection core level

Based on this technology, two protection cores have been developed:

- Protection core for power lines.
This core is suitable for currents and voltages existing in power lines.
- Protection core for signal/data lines.
This core is suitable for a variety of signal lines, which should transfer low voltages and currents without any protocol degradation.

□ Product level

The products will be based on these two cores. The blend and extent of the use of each core will be decided according to interfaces, rigidity (for commercial or military applications), casing, space available, etc.

The protection products are divided into several family lines:

- Power line protectors
 - ◆ AC lines 1 phase
 - ◆ AC lines 3 phase (see fig. 2)
 - ◆ DC lines
- Low frequency signal line protectors
 - ◆ Up to 100KHz
 - ◆ Up to 1MHz (see fig. 1)
- High frequency signal line protectors
 - ◆ Up to 10 MHz
 - ◆ Up to 100 MHz
 - ◆ Up to 1 GHz

These frequencies cover audio, video, sensors, and data-com, RF etc.

□ System level

Protection system can include “black protection cabinet”, which consists of a different protector as per requirements (see fig. 4).

Fig. 1 illustrates single communication line plug-and-play protector, with RJ connectors.

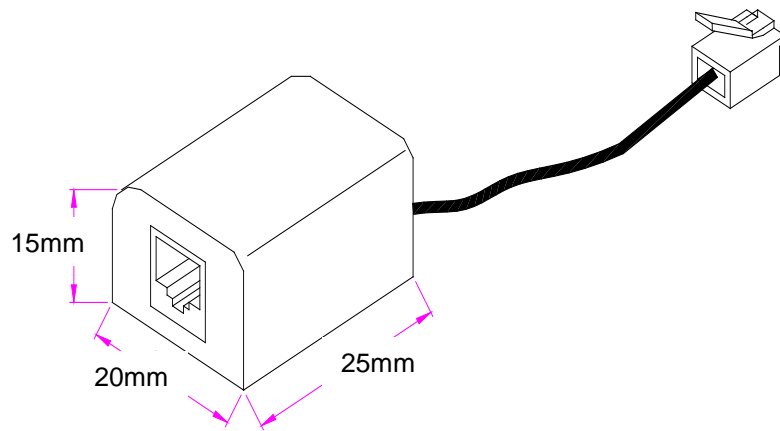


Fig. 1

Fig. 2 illustrates 3-phase power line plug-and-play protector, with screw terminals interface.

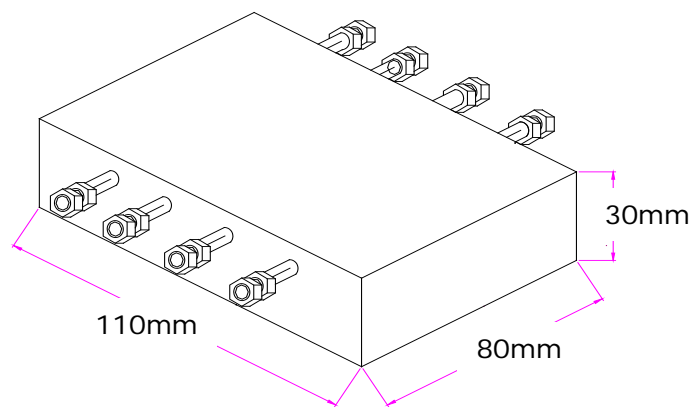


Fig. 2

Fig. 3 illustrates a distributed protection approach. Protection products are attached to each electronic device.

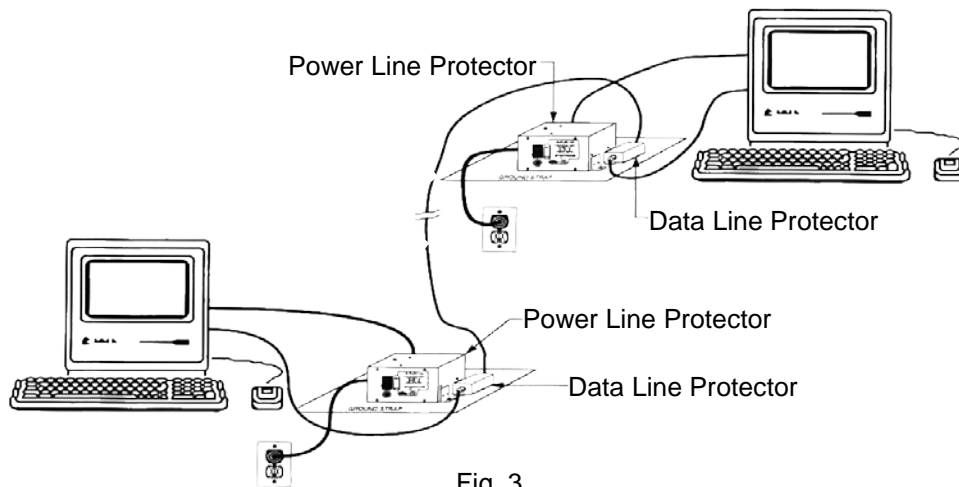


Fig. 3

Fig. 4 illustrates a concentrated (single point) protection approach, intended for use in protecting a system at a certain site. The central protection box consists of all the protection products combined in a single package, for all lines, in the form of a "protection black box unit".

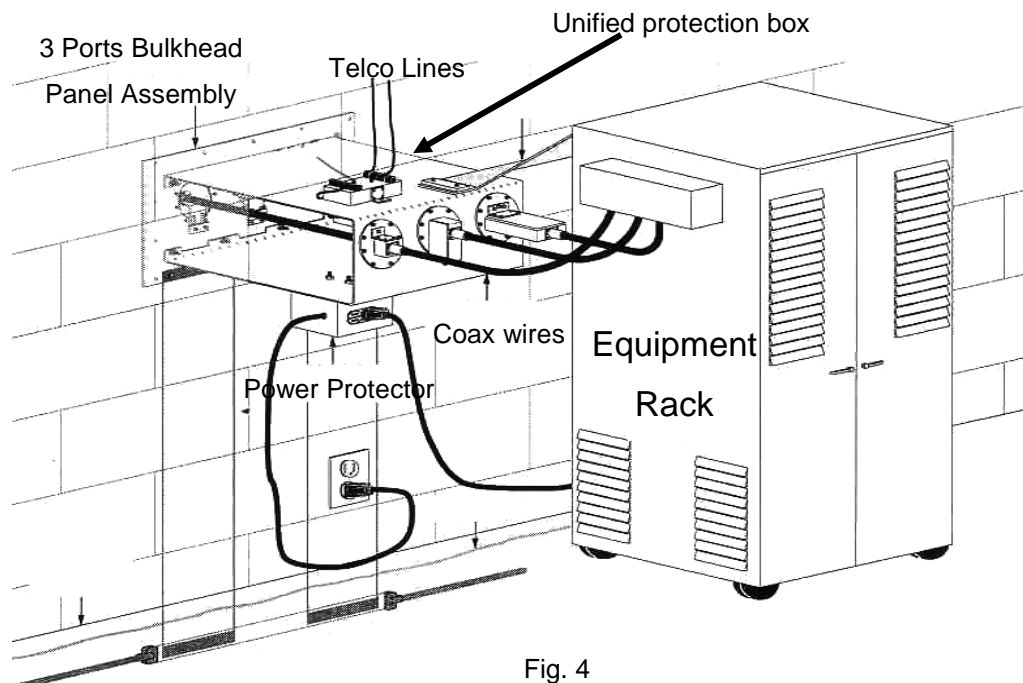


Fig. 4