AARMS
Vol. 3, No. 3 (2004) 443–457

SECURUTY

Defense against electromagnetic pulse weapons

SÁNDOR VASS

Zrínyi Miklós National Defense University, Electronic Warfare Department, Budapest, Hungary

Electromagnetic pulse weapons can be used by special forces teams who infiltrate the enemies and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a quite large area. Although electromagnetic pulse will disrupt and destroy essential communications systems; it is possible to establish a manageable and survivable communications system. This however may not always be possible, and therefore systems which can be expected to suffer exposure to the electro-magnetic weapons effects must be electro-magnetically hardened.

Introduction

The future of the battlefield will be closely tied in with the advance of electronics computers, robots and sensors will become more common on the future battlefield. Infantrymen are being equipped with digital radios and computers. Night vision devices have been around for some time. Tanks have highly sophisticated targeting computers, radar and imaging devices. All these devices are electronic in nature.

As these devices become more and more common they will be integrated into helmets, weapons, and battle suits. Vehicles will become highly automated and detection of the enemy will become easier. As weapons become more lethal it will become more important to have an advantage over the enemy and avoid being found by him.

It is unlikely that this trend will reverse itself. However, electronics are not invulnerable. There are presently two devices, which are similar, that can destroy the electronic advantage. These devices are not yet in widespread use but they are as dangerous to electronics as a non-nuclear electromagnetic pulse weapons. Countermeasures can protect electronics from these devices to some degree but no countermeasure is perfect.

Non-lethal weapons

Historically, militaries have sought to increase the lethality of weapons to better achieve military success and political objectives. Some non-lethal technologies may offer new

Received: April 22, 2004

Address for correspondence:
SÁNDOR VASS
Miklós Zrínyi National Defence University
Electronic Warfare Department
P.O. Box 15, H-1581 Budapest 146, Hungary
E-mail: vass@zmne.hu

options to our armed forces; others may prove to be more useful to our enemies because of our advanced society's many vulnerabilities. For example, a terrorist group with rudimentary knowledge of our information switches could shut down our stock market with several well-placed electromagnetic pulse generators.

Non-lethal weapons can be divided into two categories:

- counter-personnel and
- counter-material.[1]

Non-lethal counter-personnel capabilities allow the use of military force while reducing the risk of casualties among non-combatants or – in some cases – amongst enemy forces.

Non-lethal counter-materiel capabilities would enhance operations by reducing or eliminating the enemy's ability to use his equipment. It will be less destructive than conventional weapons and more productive. The risk of personnel casualties will be lowered. Consequently political risks will be minimized. The primary anti-machinery includes the non-nuclear electromagnetic pulse weapon.

Electromagnetic pulse weapons

Electromagnetic pulse weapons are one of the newest and most serious military developments in the world today.

Two types of non-nuclear electromagnetic pulse devices have been developed. One uses conventional explosives to induce the electromagnetic pulse, another uses a single-use, high-power microwave generation device.

Electromagnetic pulse was first detected at atomic-bomb tests, and induces power surges in conductors, destroying electronics connected to them.

Non-nuclear electromagnetic pulses produce a short, extremely high-energy pulse at relatively low frequencies. The most straightforward electromagnetic pulse weapons consist of a magnetron, attached to a vast capacitor bank to provide a current spike through it.

Electromagnetic pulse and High Powered Microwave weapons offer a significant capability against electronic equipment susceptible to damage by transient power surges. The conventional Electromagnetic pulse and High Powered Microwave weapons can disable non-shielded electronic devices including practically any modern electronic device within the effective range of the weapon.

The technology base, which may be applied to the design of electromagnetic bombs is both diverse, and in many areas quite mature. Key technologies, which are extant in the area are explosively pumped Flux Compression Generators, explosive or propellant driven Magneto-Hydrodynamic generators and a range of High Powered Microwave

devices, the foremost of which is the Virtual Cathode Oscillator.[2] Wide ranges of experimental designs have been tested in these technology areas, and a considerable volume of work has been published in unclassified literature.

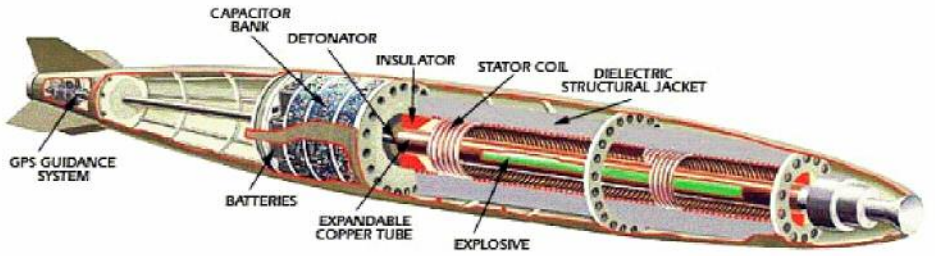

Figure 1. Electromagnetic bomb[3]

High Power Microwave devices generate much less focused beams of energy in the radio frequency range of the electromagnetic spectrum, which spans from around 1 megahertz to around 100 gigahertz. Additionally, the frequency content, or bandwidth, of microwave signals can vary significantly. Narrow band systems emit all their energy within a few tenths of one percent of a central frequency. Wideband and ultra-wideband systems can have their energy spread across a spectrum that is as much as twenty-five percent or more of the center frequency. Narrow band High Power Microwave spectra are typically in the few gigahertz to tens of gigahertz range and ultra-wideband spectra may contain energy in the frequency range from hundreds of megahertz to a few gigahertz.

While an electromagnetic pulse bomb is not easy to construct a High Energy Radio Frequency gun is much simpler. High Energy Radio Frequency guns are more directional and controllable than an Electromagnetic Pulse bomb.

High Energy Radio Frequency guns are able to shoot a high power radio signal at an electronic target and put it out of function. A variety of sources, including radio frequency oscillators, magnetrons, fast, high power electrical switches, and even non-nuclear weapon bursts generate microwave radiation.

Electromagnetic pulse effects

The effects of electromagnetic pulse warrant increased efforts to neutralize their potential to create chaos with communications systems. Electromagnetic pulse is a killer of unprotected electrical and electronic equipment. The electromagnetic bomb is typically used to damage an area instead of a single target.

This fact is especially significant when considering electromagnetic pulse power density of 1,000,000 watts per square meter versus the typical signal strength of 0.001

watt per square meter, which a radio receiver is designed to accept. Accordingly, since electromagnetic pulse is capable of delivering a signal a billion times stronger than the receiver is designed to accept, one can see the urgency to find solutions to this problem.[2]

There are two kinds of damage electromagnetic pulse can cause to electrical or electronic systems. First is the actual physical damage caused by electrical components shorting out or burning out such as capacitors, resistors, and transistors, thus causing the repair or replacement of the component.

The second is of lesser concern because it causes only temporary operational upsets such as instabilities, causing the system to shut itself down, upset computers so they must be started again. Both these effects increase in direct proportion to the amount of digital technology and the large scale integrated circuitry designed into our systems.

Some electrical equipment is innately electromagnetic pulse resistant. This includes large electric motors, vacuum tube equipment, electrical generators, transformers, relays, and the like. These might even survive a massive surge of electromagnetic pulse and would likely to survive if a few of the above precautions were taking in their design and deployment.

It is significant that modern military platforms are densely packed with electronic equipment, and unless these platforms are well hardened, an electromagnetic pulse device can substantially reduce their function or render them unusable.

Targets of electromagnetic pulse weapons

Electromagnetic pulse sources have been under investigation for several years as potential weapons for a variety of combat, sabotage, and terrorist applications.

Targets of electromagnetic pulse weapons:

- telecommunication systems;
- national power grid;
- finance and banking systems;
- national transporting systems;
- mass media;
- buildings housing government offices;
- production facilities;
- military bases and known radar sites and communications nodes, because these systems are based on electronic systems.

These targets are typically geographically fixed and thus may be attacked providing that the aircraft can penetrate to weapon release range.

Defense methods of electromagnetic pulse weapons

The major problem area in determining lethality is that of coupling efficiency, which is a measure of how much power is transferred from the field produced by the weapon into the target.

Front door coupling occurs typically when power from an electromagnetic pulse weapon is coupled into an antenna associated with radar or communications equipment. The antenna subsystem is designed to couple power in and out of the equipment.

Back door coupling occurs when the electromagnetic field from a weapon produces large transient currents or electrical standing waves on fixed electrical wiring and cables interconnecting equipment, or providing connections to mains power or the telephone network.

It is easy to say we can protect electronic equipment against electromagnetic pulse in principle but it is very difficult to implement and even more difficult to maintain. There are two basic methods of providing electromagnetic pulse protection. The first is to design and build the equipment so that the circuit can resist the electromagnetic pulse. The second is to provide a shield, which will not allow the electromagnetic pulse to enter.

Often the most cost effective way is to use a combination of both methods to defeat the electromagnetic pulse. We will look at a few ways to defeat the electromagnetic pulse, which are for the most part combinations of the two basic ways.

Features that need to be designed in are such things as pulse resistant fiber optics, improved power supply systems using batteries, solar power and thermonuclear power sources, and the use of nodule self-healing network architecture. In the case of computer memory we need to ensure that magnetic tape or some other semi permanent storage device are used to store data and programs for the computer.

A wide variety of active electromagnetic pulse countermeasures exist, with varying degrees of success. These countermeasures include:

- shielding;
- wave guide beyond cutoff;
- spark gap arrestor;
- filter network;
- metal oxide varistor;
- fiber optic circuitry and;
- high speed Zener diode.[4]

Shielding involves surrounding a circuit with metal or coating its enclosure with metallic paint and providing a low resistance path to ground. Although it provides some

degree of protection from electromagnetic pulse, shielding cannot be regarded as an effective countermeasure by itself, especially at high frequencies, since leakage can occur through even the smallest gaps.

Waveguides and spark gap arrestors represent relatively old protection technologies that generally are not suitable for suppressing electromagnetic pulse in digital, semiconductor based equipment.

A typical filter network for surge protection is a configuration of capacitor-inductor-capacitor called a pi filter because it's schematic resembles the Greek letter "pi". The pi filter has proven to be an effective countermeasure for threats such as electromagnetic interference and low-level electromagnetic pulse.

The metal oxide varistor is a recent generation semi-conducting device that conducts at high voltages. Metal oxide varistors are typically used in overload protection circuits. Drawbacks of using Metal oxide varistors for electromagnetic pulse suppression include relatively slow response time and a tendency for performance to degrade with each overload.

Using fiber optic circuitry might be considered an ideal solution to all types of frequency and voltage related threats. This would be an excellent alternative if a system could be built entirely from light sensitive logic devices. However, with the current off-the-shelf technology, interfaces with copper and silicon based electronic systems are still necessary. Thus, electromagnetic pulse suppression still must be provided at each point where optical signals are converted to electronic signals.

A high speed Zener diode provides electromagnetic pulse suppression. Since the pi filter protects against electromagnetic interference, the combination of these two countermeasures at circuit interfaces protects against both frequency and voltage related threats. Incorporating a dual filter design in each line that enters an electronic module or black box can provide effective and reliable protection against electromagnetic pulse and electromagnetic interference.

A passive electromagnetic pulse countermeasure consists of unplugging the equipment from the electrical power system and the antennae, plus providing some shielding.

Military equipment is designed to be resistant (not impervious) to electromagnetic pulse, but realistic tests are difficult to conduct and electromagnetic pulse protection rests on attention to detail. Minor changes in design, incorrect maintenance procedures, poorly fitting parts, loose debris, moisture, and ordinary dirt can cause elaborate electromagnetic pulse protections to be totally circumvented.

Shielding methods

In order to predict the effect of an electromagnetic pulse on electronic equipment, it is necessary to assess the environment. The structures housing the electronic equipment are made in various shapes and sizes and are connected to the outside world by conductors such as utility lines and pipes, communication lines, and access and ventilation structures.

For complex systems it is convenient to have several layers of shielding. A sealed metal box is an ideal structure for eliminating electromagnetic pulse penetration. However, power lines and signal cables require entry ports thus compromising the integrity of a shielded building. It is apparent that doors and windows would have a greater leakage effect.

More than one shield can be used to secure the environment of the machinery and electronic material contained within a building.

Shielding involves the use of a barrier or series of barriers to reduce the magnitude of the electromagnetic energy incident upon the electronic or electrical system to be protected. Shielding philosophy can be developed around different approaches as discussed in paragraphs through:

- global shielding (Faraday cage);
- tailored shielding;
- zonal or topological shielding;
- cable shielding;
- grounding;
- shield penetration protection concepts:
  - personnel entrances;
  - electrical penetrations;
  - transient suppression devices and filters;
  - electromagnetic isolation;
  - dielectric isolation;
  - isolation switching.[6]

Global shielding (or hardening) is a protection concept that uses an overall shield to encompass the entire facility. In this approach, all conducting penetrations and all apertures are protected at the shield. The intent is to keep all electromagnetic pulse fields and electromagnetic pulse induced transients outside the protected volume. The global shield could be placed on the entire outer walls, ceiling, and floor (surface) of the facility, or it could be reduced to a smaller volume that contains all sensitive equipment to be protected. The most common shield material for global shielding of ground based

facilities is sheet steel with welded seams, although other designs can provide adequate global electromagnetic pulse shielding.

Faraday cage

To solve this problem we can use Faraday cage or electrostatic shielding to simply exclude radio frequency signals from the environment occupied by the equipment. A good measure of protection may be applied to mains wiring by running it through metal enclosed cable trays, and threading it through flexible metal shielding armour from the tray to the wall socket where it is to be used. A wide range of off-the-shelf commercial products may be used to this end.

A computer room, office or even equipment cupboard may also be built or refitted as a Faraday cage, by covering the walls, floors and ceiling, windows and doors with conductive copper mesh.

One "survival system" for such sensitive equipment is the Faraday cage. A Faraday cage is simply a metal box designed to divert and soak up the electromagnetic pulse. If the object placed in the box is insulated from the inside surface of the box, it will not be effected by the electromagnetic pulse traveling around the outside metal surface of the box. The Faraday cage simple and cheap and often provides more protection to electrical components than "hardening" through circuit designs, which can't be (or haven't been) adequately tested. Many containers are suitable for make-shift Faraday cages: cake boxes, ammunition containers, metal filing cabinets, etc., etc., can all be used (Figure 2).

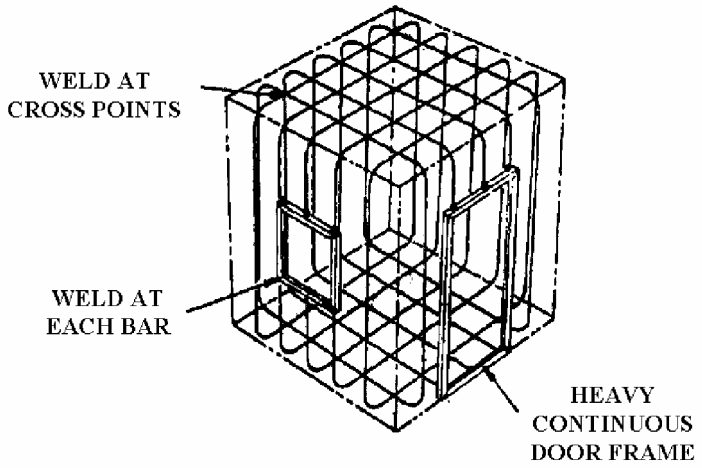

Figure 2. Faraday cage[6]

There are only two requirements for protection with a Faraday cage are:

- the equipment inside the box does not touch the metal container (plastic, wadded paper, or cardboard can all be used to insulate it from the metal);
- the metal shield is continuous without any gaps between pieces or extra-large holes in it.[5]

Thus, this elemental Faraday cage provides significant shielding for electromagnetic energy in the frequency range of lightning. For electromagnetic energy in the range of frequency modulation radio waves it provides limited shielding, for radar waves insignificant shielding.

Tailored shielding is a protection concept in which shielding is designed and constructed according to specific protection requirement for the equipment involved. Tailored shielding options may include global shielding, zonal shielding, shielding of cabinets or components, or combinations thereof. In a typical tailored protection design, discrete protection will be provided to eliminate specific, localized deficiencies.

Zonal or topological shielding is a concept in which a facility is divided into zones, with shielding barriers located topologically in a shield within a shield configuration. Figure 3 shows a generic topological shielding system. The outer zone is designated zone 0; zone 1 is inside shield 1 but outside shield 2. Zones and shields are assigned increasingly larger numbers as they progress toward the more deeply nested areas.[6]

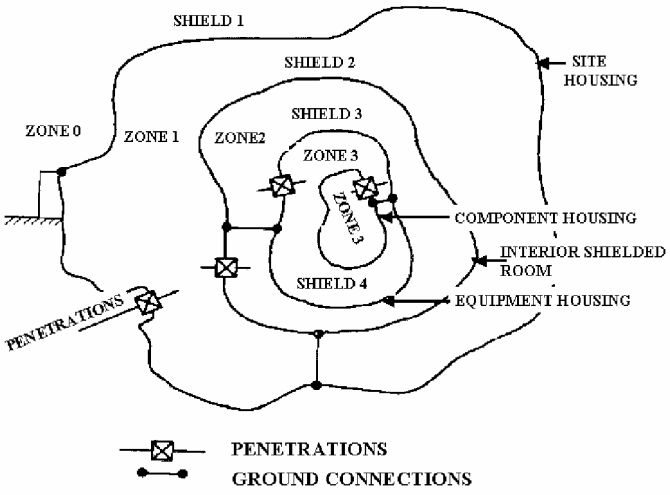

Figure 3. Zonal shielding[6]

Note that Figure 3 is a simple schematic to represent the zoning concept; although not depicted, each zone could contain more sets of sub zones. For example, shield 3 could contain 2 or more zones designated as zone 4. Further, Figure 3 shows possible shield types including a site housing shield and an interior shielded room, with equipment and component housings making up the shields of the next topological orders.

The zonal concept shown in Figure 4 is a specific example of an underground facility that uses topologically zoned protection.

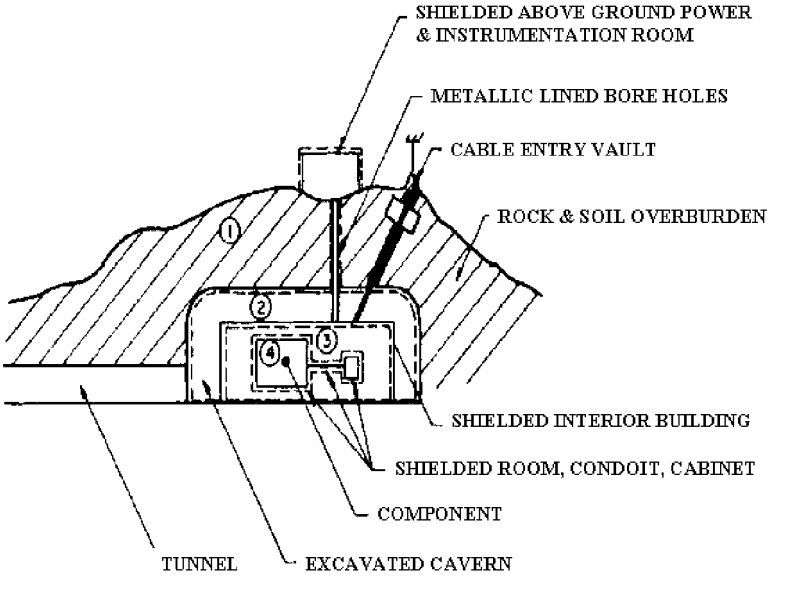

Figure 4. Zonal shielding concept[6]

The rock and soil overburden above the facility serves as shield 1. Zone 1 is the volume between the underground building and the excavated outline of overhead rock. In some cases, a shield of this type provides adequate protection for robust electrical or electronic equipment. Shield 2 is composed of a sheet metal building that may provide only a limited level of shielding. Inside this building (zone 2), some systems would be adequately protected. The above-ground building and connecting conduit represent an extension of zone 2.

Shield 3 is then the interior shielded room which provides further protection within zone 3 where sensitive, electronic equipment may be operated.[6]

Conductive or metallic cable shielding or conduit is used in the zonal/topological protection concept to extend the boundary formed by equipment enclosures and thus provide a way to interconnect elements while maintaining boundary continuity. Cable shielding is also used to protect a wire or wires as they travel from one boundary to another. This would be the case with a shielded radio frequency signal traveling from its entrance into a building to the radio frequency receiver. Of course the shield is somewhat reciprocal in that it also prevents signals from radiating out of the cable. The main feature of cable shielding stressed here is continuity of the boundary provided by the cable shield/connector combination, which may require special joints.

Some form of grounding is required in any electrical or electronic system for protecting personnel from electrical shock, controlling interference, proper shunting of transient currents around sensitive electronics, and other reasons. Ideally, grounding would keep all system components at a common potential. In practice, because of possible inductive loops, capacitive coupling, line and bonding impedances, antenna ringing effects, and other phenomena, large potentials may exist on grounding circuits.

Shield penetration protection concepts

All shielded zones will require penetrations to allow entry of equipment, personnel, electric power, communications, and control signals, ventilation, water, fuel, and various fluids. Without protection, these penetrations compromise the shield.

Two concepts are commonly used for personnel entrances: conventional electromagnetic pulse/radio frequency interference shielded doors and personnel tunnels that act as waveguides below cutoff. The shielded doors generally use metal fingerstock or electromagnetic pulse/radio frequency interference gaskets to provide an electromagnetic seal around the doorjamb periphery (Figure 5). Currently available gasket and fingerstock doors require regularly scheduled maintenance and/or replacement to maintain required shielding levels. The gaskets are relatively easily damaged and also require replacement. Air-expandable doors may also be used, although they typically have more maintenance problems. These doors generally use a movable subassembly of two shielding plates on a framework that is moved on rollers in and out of a steel-framed opening. When closed, air expansion tubes cause the two shielding plates to make uniform surface contact with the frame inner surfaces.

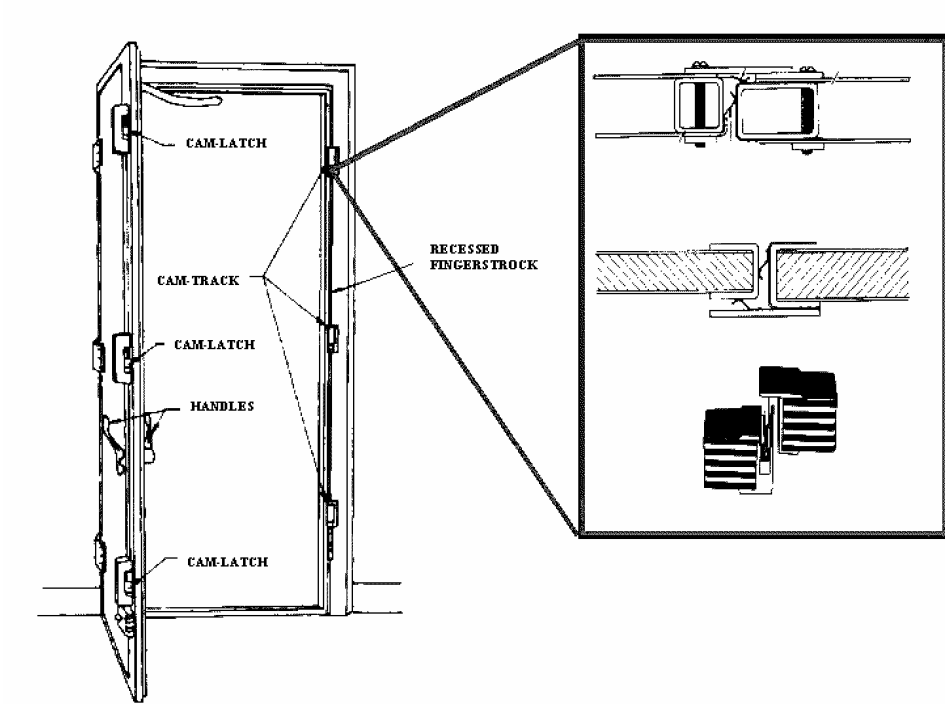

Figure 5. Shielded door

A common feature for electrical penetrations in a global protection approach is a cable entry vault to prevent large currents on external conductors from being conducted into the facility. Ideally, all penetrations should enter a single vault. In some cases, however, it may be necessary to separate the vault into two compartments or to use two vaults for penetrations by different types of lines: power, signal and control, and antenna. The vault must be connected directly to the external facility ground system. The cable entry vault serves three purposes: to insure that penetrating conductors do not cause conducted electromagnetic pulse energy to enter the protected topology; to contain and divert penetrator-conducted electromagnetic pulse energy to the boundary exterior; and to contain or divert radiant electromagnetic energy resulting from the activation of transient suppression devices subjected to a conducted pulse. Conductive penetrations, such as a conduit, waveguide, or shielded cable, must have a circumferential weld or other means of providing good electrical connection at the intersection with the entry vault.

Transient suppression devices fill a critical gap in the concept of topological protection. The necessity of supplying power to a facility and of communicating over cables or antennas are two major factors contributing to their use. Power lines entering a facility are typically connected to an unshielded power grid so that large, conducted currents must be bled off to prevent their entry into a facility. These currents are diverted to the exterior boundary of the topology. This boundary can be an overall external shield or an enclosed entrance vault. Antennas, such as for high-frequency communications, are designed to gather electromagnetic signals (at wavelengths in the electromagnetic pulse frequency spectrum) and to apply these signals to the center conductor of a shielded cable. The electromagnetic pulse transients associated with a high-frequency antenna can be, by far, the largest single signal entering a facility. Transient suppressors are often used in conjunction with filters. Filters are frequency-selective whereas surge suppressors are amplitude-selective. Filters are frequently used to attenuate transients associated with the nonlinear operation of surge arresters. They are also used for selectively passing (or stopping) frequency bands as in the case of antenna cable penetrations. Transient suppressors are an integral part of the electromagnetic topology, demanding specific installation techniques as will be seen later. A spark gap is a surge suppressor that provides a conducting path to ground when the voltage across the device exceeds the gap breakdown level.

Spark gaps with a high current capacity do not operate fast enough to block all electromagnetic pulse energy transients entering the vault. For this reason, it may be necessary to use other protection devices in conjunction with the spark gap.

The electromagnetic isolation concept involves the use of elements either immune to interaction with electromagnetic radiation or that provide a current path interruption. Optical fibers are examples of elements immune to electromagnetic radiation that can be used to reduce the number of conductive penetrations. For practical purposes, optical fibers can be used for long communications links without signal interference from electromagnetic pulse. Further, they can be used to enter shielded zones through waveguide below cutoff penetrations without compromising the electromagnetic shielding effectiveness. Where possible, optical fibers are recommended for:

- voice and data communications lines;
- energy monitoring and control systems;
- intrusion detection systems;
- other security systems;
- control systems;
- any other use where possible and practical.[6]

Dielectric isolators for shield penetration when external metallic electromagnetic energy collectors are involved. Examples are control rods or cables (normally metallic), piping systems for fluids, and metallic duct systems for air.

Dielectric sections are installed at or near the shield to prevent the energy induced on the external metallic part from being conducted through the shield. Dielectric control rods can enter through a shield in the same way as optical fibers, that is, through a waveguide-below-cutoff section.

Isolation switching has been provided at facilities so they can use commercial electric power during routine operation, but can switch to internal generators or power systems in the event of an emergency such as non-nuclear attack. Since the commercial power wiring is a source of significant electromagnetic pulse energy injection through a shield, switching to internally generated power is an obvious advantage when advance warning of impending nuclear attack is received and throughout the entire non nuclear attack cycle. This concept applies to communications lines and control lines as well as power lines. Switching used in past facility designs has been called “alert attack” switching. Such switching must provide adequate switch contact separation to prevent arcing, and must be designed to reduce coupling interactions between wiring and switch contacts to acceptable levels. It should be noted that advance notice of an electromagnetic pulse attack is not always provided.

Conclusions

Electromagnetic pulse devices are Weapons of Electronical Mass Destruction with applications across a broad spectrum of targets, spanning both the strategical and tactical. As such their use offers a very high payoff in attacking the fundamental information processing and communication facilities of a target system.

The non-lethal nature of electro-magnetic weapons makes their use far less politically damaging than that of conventional munitions, and therefore broadens the range of military options available. Electromagnetic bombs can be an affordable force multiplier for military forces, which are under post Cold War pressures to reduce force sizes, increasing both their combat potential and political utility in resolving disputes.

Given the potentially high payoff deriving from the use of these devices, it is incumbent upon such military forces to appreciate both the offensive and defensive implications of this technology. It is also incumbent upon governments and private industry to consider the implications of the proliferation of this technology, and take measures to safeguard their vital assets from possible future attack. Those who choose not to may become losers in any future wars.

References

1. Legal Issues Concerning Military Use of Non-Lethal Weapons. http://www.murdoch.edu.au/elaw/indices/title/sautenet72_abstract.html
2. *Electromagnetic Pulse Bomb – Weapon of Electronic Mass Destruction.* http://www.abovetopsecret.com/pages/ebomb.html
3. *Military & Weapons*. http://www.geocities.com/howananee/m-w.html
4. *Shielding Electronic Components from Nuclear Effects.* http://kyem.dma.state.ky.us/KY%20EOP/Ky%20EOP%20Word/B/APPENDIX%20B-6.doc
5. *Elemental Faraday Cage*. http://www.boltlightningprotection.com/Elemental_Faraday_Cage.htm
6. *Electromagnetic Pulse (EMP) and Tempest Protection for Facilities*, http://www.parallaxresearch.com/dataclips/pub/infosec/emsec_tempest/emp/emp.htm