August, 2011

High Power Electromagnetic Weapons: A Brief Tutorial

George H Baker, III, *James Madison University*

High Power Electromagnetic Weapons: A Brief Tutorial

George H. Baker

Background. High power electromagnetic weapons, also referred to as high power radiofrequency (HPRF) weapons, are a type of directed energy weapons. The system effects of high power electromagnetic environments are well recognized by world scientific and military communities. Former CIA Director John Deutch has said that, "the electron is the ultimate precision-guided weapon." In the course of the investigation ofnuclear EMP effects on electronics during the Cold War period, it became evident that garden variety, unprotected electronics would malfunction, in some cases burn out, in the presence of electromagnetic fields in the hundreds to thousands of volts per meter. The EMP experience has led to the development of non-nuclear high power electromagnetic sources to create fields that equal or exceed EMP levels, albeit over relatively small ranges. Achievable electronic effects could have serious consequences in terms of interruption or termination of critical system operation. The effects are of particular interest to the military in the context of information warfare and missile defense. Because most critical infrastructures are controlled by electronics, HPRF weapons are a concern for civilian systems as well. The weapons could be used to disrupt computer electronics controlling electric power grids, telecommunications networks, financial institution databases, security systems, and aircraft.

Military forces in many countries are pursuing the development of HPRF weapons. These programs are normally classified. HPRF weapons represent a revolutionary concept because they operate at the speed of light, can be used covertly, and harm equipment rather than humans (non-lethal). HPRF weapons may be enclosed in briefcases, packing containers, truck beds, or aircraft and maneuvered to expose critical military or infrastructure systems.

Electromagnetic Weapon Characteristics. There are three elements to be considered in discussing HPRF weapons systems: the weapon itself, the propagation of the weapon output to the target, and the target response (see Figure 1).

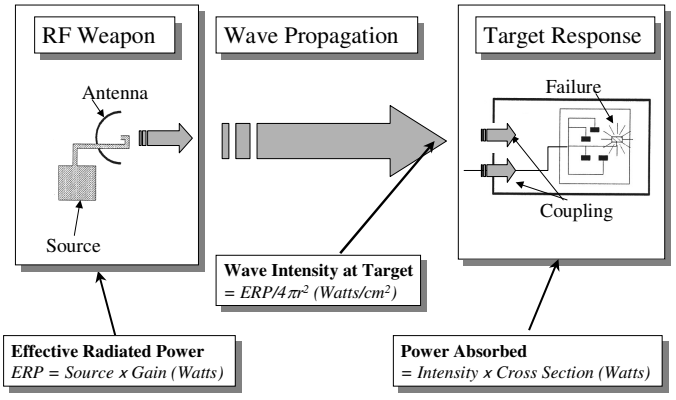

Figure 1. High Power RF Weapon Operation Elements

Weapon Design. An HPRF weapon consists of a power source, or driver and a radiating antenna. The source is normally pulsed. Outputs may be sine waves (providing a narrow frequency band signal) or pulses (providing a wide frequency band signal). High power electromagnetic source technology includes electron beam devices (magnetrons, vircators, gyrotrons, backward wave oscillators), solid-state devices (bulk avalanche, optical switches, silicon carbide circuits) and explosive generators (magnetic flux compression using high explosives). Output power levels in the gigawatts are feasible over a wide range of frequencies. Design details will determine output characteristics. Power, frequency, bandwidth, repetition rate, and duty cycle are the important HPRF weapon output parameters.

The HPRF weapon source must be connected to an antenna with sufficient gain to "beam" the RF energy to a useful range. Portability requirements impose major limits on antenna area which in turn largely governs the maximum intensity (power per area) that can be delivered to a target system at a given range. Compact sources that may be moved covertly in briefcases, packing containers, truck beds, or aircraft and maneuvered for close-up exposures of critical military or infrastructure systems are of most interest. Antenna size limits largely determine the maximum intensity (power/area) that can be delivered to a target system at a given range. A table of approximate relative portable platform sizes is provided below.

Table 1. Portable Platform Size Comparisons (Approximate)

Capacity: Platform:	Volume	RF system Weight	Basis
Briefcase	0.02 m^3	5 kg	Typical hard side
Footlocker	0.15	40 kg	1 person portable
Pickup truck	4 m^3	1000 kg	1 ton capacity
Econoline van	8 m^3	2000 kg	Bed volume
Tractor trailer	80 m^3	20,000 kg	20 ton capacity

High Power Electromagnetic Wave Propagation. Electromagnetic waves propagate at the speed of light through the atmosphere. Under most conditions, the atmosphere will not attenuate HPRF waves as they travel from source to target. However, if the electromagnetic wave's peak field level exceeds the air ionization threshold a cascade process will occur in which an atmospheric plasma is created that will absorb most or all of the energy in the wave. This phenomenon is referred to as air breakdown.

A typical threshold for breakdown at sea level is approximately 1 megawatt/cm^2 . As an example, a 1 Gigawatt source radiating through a 1-foot radius circular antenna will produce an average intensity over the antenna of 0.35 megawatts/cm^2, a factor of 3 below air breakdown. Once away from the antenna, EM intensity falls off as the beam spreads (typically as $1/4\pi r^2$ where r is the distance to the target).

The HPRF signal intensity on target depends on source transmission power (P_t), antenna gain, and range according to the following equation:

$$S_t = \frac{ERP}{4\pi r^2} = \frac{P_t \cdot G}{4\pi r^2} \frac{watts}{m^2}$$

The antenna gain may be approximated by $G \approx \frac{4\pi A_e}{\lambda^2}$ where A_e is the effective antenna area and λ is the wavelength of the radiated HPRF signal. This yields a simple formula for the intensity on target:

$$S_t = \frac{P_t A_e}{r^2 \lambda^2}$$

So, for example, a 1 Gigawatt source radiating at 1 GigaHz (λ = 0.3m) with a 1-m^2 antenna will produce a beam intensity of 11 kW/m^2 (or 1.1 watts/cm^2) on a target 1000 meters away. If the pulse duration were 1 microsecond, the energy fluence on target would be power x time or, 1.1 microjoules/cm^2.

Target Response. Once the electromagnetic wave signal reaches the target, its energy couples to the system in a very complex manner through various paths associated with the topology of the target system. The HPRF signal will induce currents on any external conductors (antennas, wires, etc) that penetrate to the system interior. The signal will also couple to any external metal shielding and then may reradiate to internal conductors. Signal waves will penetrate through any holes in external shielding to interior portions of the system. The main concern is the amount of energy that finds its way to critical electronic circuits, causing the system to malfunction.

To simplify coupling calculations, it is possible to determine an effective "coupling cross section" for critical internal circuits. In effect, this treats each internal circuit as a receiver. The power received by the circuit may be expressed as a simple function in incident wave power and an effective coupling cross section:

$$P_i = S_t \mathrm{A}_\sigma$$

P_i is the power induced in the internal circuit, S_t is the incident power at the system's exterior, and A_σ is the coupling cross section of the internal circuit. A_σ is a function of frequency and incorporates all the complexity of coupling including multiple paths, layers and mechanisms. There are two major coupling modes, front door and back door, as shown in figure 2.

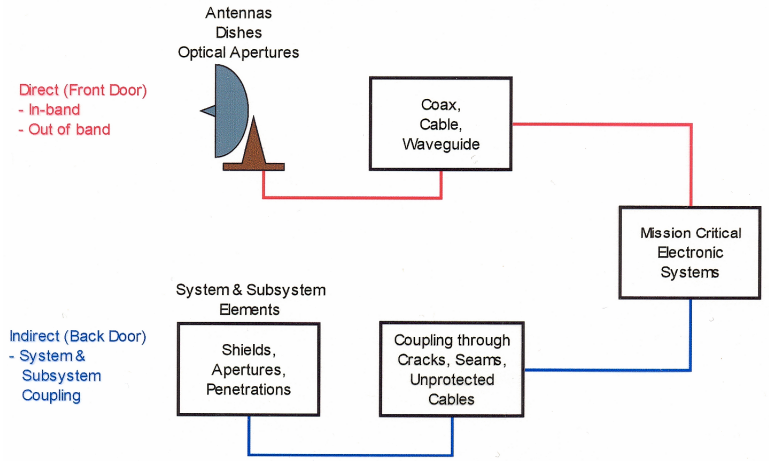

Figure 2. Front Door and Back Door Coupling Modes

The physics of front and back door coupling are the same. In each case, energy resident in the incident wave induces currents in the system that flow to a sensitive system circuit. Each can be characterized parametrically by equation $P_i = S_t A_\sigma$. The coupling cross-section, A_σ, is typically large for front door coupling and small for back door coupling. The coupling cross sections for front door coupling are of the order of the physical area of the antenna or aperture. Effective coupling cross section values for back door coupling of unhardened systems range from $10^{-4} – 10^{2}$ cm^2. Coupling cross-sections are hard to predict analytically and can be determined confidently only by direct measurement. This creates a problem for an attacker's confidence since HPRF effects are subject to much higher uncertainties than conventional weapon effects.

HPRF Weapon Effects on Systems. EMP and HPRF affect systems by disrupting the operation of electronic components either temporarily (upset or latchup) or permanently (component damage). Damage may be "direct" where energy inherent in the EMP/HPRF field is sufficient to cause malfunctions or "indirect" where EMP/HPRF energy triggers effects involving a system internal power supply. Even though the power delivered to a circuit by the HPRF field is small, the much larger energy available in the system's power supply (or fuel and ordnance) can be improperly diverted by an HPRF induced overvoltage arc or malfunction of system digital control circuit, causing major system damage.

Upset refers to an induced change of state in a digital circuit in which the system continues to operate, although possibly with erroneous data bit streams. Latchup refers to changes of state in digital circuits where the affected portion of the system ceases to operate until the system resets itself or (worse) a manual reset is required. In either case, system components are not directly damaged and recovery is often possible (depending on time criticality of affected function).

Exploitation of upset effects should not be discounted. In some cases they are tantamount to permanent damage. Upset may result in major system damage, e.g., a missile plunges into ocean due to a guidance system upset, or computer equipment is destroyed by an upset sprinkler system. Small, upset-level transient pulses can also act to

trigger the release of energy from a system's own power supply causing components to burn out at fluences much lower than would normally cause permanent damage.

To give an indication of HPRF wave energies required to cause system effects, ITT industries (formerly Kaman Sciences) openly exposed circuit cards to 2.9 GHz microwave pulses with duration 1 microsecond. Onset of upset occurred at 1 watt/ cm^2 (equivalent to 1 microjoule/cm^2 for this pulse duration). All components were upset at wave intensities of 1000W/cm^2. Onset of damage occurred at 100W/cm^2 (for a 1 microsecond pulse, this is equivalent to 100 microjoules/cm^2). All components were damaged at wave intensities of 1000 W/ cm^2 (equivalent to 1000 microjoules/cm^2).

System Protection. System hardening involves a combination of operational and hardware techniques. Operational techniques may include the provision of spares for soft critical subsystems or boxes, disconnecting susceptible circuits upon warning, and/ or establishment of a physical keep-out perimeter (with barriers and/or security force) or zones around critical equipment to prevent positioning of HPRF weapons at close ranges. Operational controls may also be built into software to provide circumvention and reset, error-correcting codes, voting logic, and status detection. For some non time-sensitive systems, provisions for rapid system repair may be an option.

Conceptually, hardware approaches involve placing a conducting material between the incident HPRF wave and susceptible internal circuits. Hardening techniques have been successfully demonstrated and codified for EMP (ref. article on nuclear EMP). The EMP community has placed a heavy reliance on exterior shielding while limiting the number of penetrations that have to be individually protected. Such protection applied at the system exterior allows interior boxes to go untreated. This approach works well when designed in from the start. For retrofit protection, however, it is often prohibitively expensive.

Hardware approaches for HPRF protection, while conceptually similar, have some differences in emphasis from EMP. Because EMP is extremely broadband, typically only a small fraction of the energy comes through the front door in band. HPRF weapons can be tuned to the front door center frequency such that all the beam energy flows into the system. Also since HPRF weapons operate at higher frequencies, attention to smaller apertures (including cracks and seams) is required and dimensions of waveguide-beyond-cutoff penetration treatments will require changes (longer and more narrow waveguides are needed).

Front door in-band protection is one of the more challenging (but not insurmountable) HPRF protection problems. The high gains associated with most front door paths make these potentially the most susceptible portion of the system. However these well-characterized front door receive paths have received much attention in terms of protection engineering. Radar systems are often protected from their own or neighboring transmitters by a receiver protector or RP. Similar protection can be applied to communication receivers against in band HPRF environments. Table 2 summarizes HPRF hardening techniques.

Table 2. HPRF Hardening Methods

Operational Techniques	Hardware Techniques	
	Front Door	**Back Door**
Disconnect on warning	Tuned metallic radomes	Shielding, topology control
Spares	Bandstop reflectors	Internal cable shields
Physical keep-out perimeters or zones	Antenna gain pattern control	Non corrosive mating surfaces
Software Techniques: Circumvention/reset Error correcting codes Voting logic Status detection/ alarm	Filters	Closely spaced fasteners
	TR devices/ limiters	RF gaskets and seals
	Terminal protection devices	Aperture screens and conductive films
		Selection of hard circuits and components
		Pin protection
		Fiber Optics
		Filtering, limiting at penetration points

Future Directions. HPRF generation techniques have matured to the point where practical devices have become technically feasible. Miniaturization of pulse-power source components, more efficient power supplies, and advances in electronic pulse forming, energy conversion, and antennas enable reduced size and increased efficiency of HPRF generation hardware. Simple weapons can also be built using inexpensive magnetrons from common microwave ovens.

Military trends to computerized battle management, weapons tracking, and landline/wireless network communications are a double-edged sword, introducing serious HPRF vulnerabilities. Military use of commercial off-the-shelf equipment and dependence on civilian infrastructure exacerbate the problem. Senior military officials have dropped hints about pursuing offense technology but there are no officially published details concerning weapon availability or capabilities.

Several other countries also have extensive background in the development of RF weaponry. The former Soviet Union pioneered the development of HPRF weapon technology and this technology is now being offered to other countries. According to a recent report from the Office of the US Secretary of Defense on the military power of China, "Captain Shen Zhongchang from the Chinese Navy Research Institute…envisions a weaker military defeating a superior one by attacking its space-based communications and surveillance systems…in future wars, Shen highlights radar, radio stations, communications facilities, and command ships as priority targets vulnerable to smart weapons, electronic attack, and electromagnetic pulse weapons." It is expected that in future conflicts the United States will encounter adversaries using HPRF weapons as part of asymmetric tactics to disrupt information systems.

See also: Nuclear Electromagnetic Pulse (EMP)

References and Further Reading

Abrams, M., "The Dawn of the E-bomb," IEEE Spectrum, October, 2003.

Backstrom, M. et al; *Preliminary Study Regarding the Resistance of Critical Societal Systems to High Intensity Electromagnetic Radiation*; Royal Swedish Defense Research Agency; Report FOA-R-97-00538-612-SE; August, 1997.

Barker, R., Schamiloglu, E., *High-Power Microwave Sources and Technologies,*Wiley-IEEE Press, 2001.

Benford, J., Segle, J., *High Power Microwaves*, 2nd Edition, Institute of Physics, 2004.

Guyatt, D. G., "Some Aspects of Antipersonnel Electromagnetic Weapons," ICRC Symposium on the Medical Profession and the Effects of Weapons, February, 1996.

Kopp, C., "The E-Bomb – A Weapon of Electrical Mass Destruction," INFOWAR Conference, Washington, D.C. September 1996.

Lucier, J. P., "Backyard Terrorism - E-Zapper Could Break the Bank," Insight Magazine, April 1, 2002.

McKenna, T., "Flash in the Plan," Journal of Electronic Defence, May 2003.

Price, D. et al, "Compact Pulse Power for Directed Energy Weapons," Journal of Directed Energy, Volume 1, Fall 2003.

Saxton, J., Chairman, *Congressional Hearing on Electromagnetic Weapons*, Joint Economic Committee, Intelligence and Security, Source: http://www.house.gov/jec/hearings/02-25-8h.htm, June 17, 1997.

National Research Council, Technology for the United States Navy and Marine Corps, 2000-2035, Volume 2: Technology, National Academy Press, Washington, DC, 1997.

About the author: George Baker is Professor of Integrated Science and Technology at James Madison University. He also serves as Technical Director of the University's Institute for Infrastructure and Information Assurance (IIIA). He is a consultant in the areas of critical infrastructure assurance, high power electromagnetics, nuclear and directed energy weapon effects, and risk assessment. He served as senior staff on the Congressional EMP Commission. Baker is former director of the Defense Threat Reduction Agency's Springfield Research Facility, a national center for critical system vulnerability assessment. Much of his career was spent at the Defense Nuclear Agency (DNA) as the Integrated Electromagnetics Team Leader directing the development of

electromagnetic protection, underground testing, and standards including MIL-STD-188-125, MIL-STD-2169B, and MIL-HDBK-423. He also headed the Agency's Innovative Concepts Division overseeing the joint US-Russian space nuclear power technology, electro-thermal chemical (ETC) gun development, radiofrequency directed energy source concept development and testing, and DNA's university grants programs. Baker received the Agency Legacy Award for his leadership and innovation. He is a member of the NDIA Homeland Security Executive Board, the Institute of Electrical and Electronic Engineers, the Directed Energy Professional Society (Charter Member), and the Association of Old Crows. He is a Summa Foundation EMP Fellow and holds a Ph.D. from the U.S. Air Force Institute of Technology.