The Hazards of Electro-Magnetic Terrorism

And why North American power plants should take note.

By V. Gurevich, Ph.D

Electromagnetic terrorism has huge implications for the international power industry. Manuel W. Wik, chief engineer and strategic specialist on future defense science and technology programs at the Defense Materiel Administration, Stockholm, writes:

> "Electromagnetic terrorism (EM terrorism) is the intentional, malicious generation of electromagnetic energy, introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes. EM terrorism can be regarded as one type of offensive information warfare. EM terrorism needs to be considered more carefully in the future because information and information technology are increasingly important in everyday life."[1]

Electronic components and circuits (such as microprocessors) are working at increasingly higher frequencies and lower voltages, and thus are increasingly more susceptible to electromagnetic interference (EMI). But the threat of intentional EMI is not limited to radio frequency (RF) energy. Yuri Parfenov and Vladimir Fortov of the Russian Academy of Sciences Institute for High Energy Densities recently experimented with injection of disturbances into power lines outside a building and found that the signals penetrate very easily and at a high enough voltage to cause damage to computers inside the building.[2] Additionally, radiated fields often become a conducted threat due to coupling of RF energy to exposed wires. Dr. A. Prishchipenko, member-correspondent of the Russian Academy of Military Sciences, today heads research and practical development in this field in Russia.

An astonishing number of research projects devoted to EM terrorism are concerned with the EMI impact on objects such as communication systems, telecommunications, airplanes, and computers, but practically no projects are devoted to investigating resistance of microprocessor-based protective relays to EMI. Microprocessor-based protective relays obviously are more prone to EMI impact than electromechanical and even analog electronic ones. Because microprocessor relays are the combined protection systems uniting many kinds of protection functions, deliberate damage to even one such relay can lead to much heavier failure in power systems than would damage of the electromechanical relay.

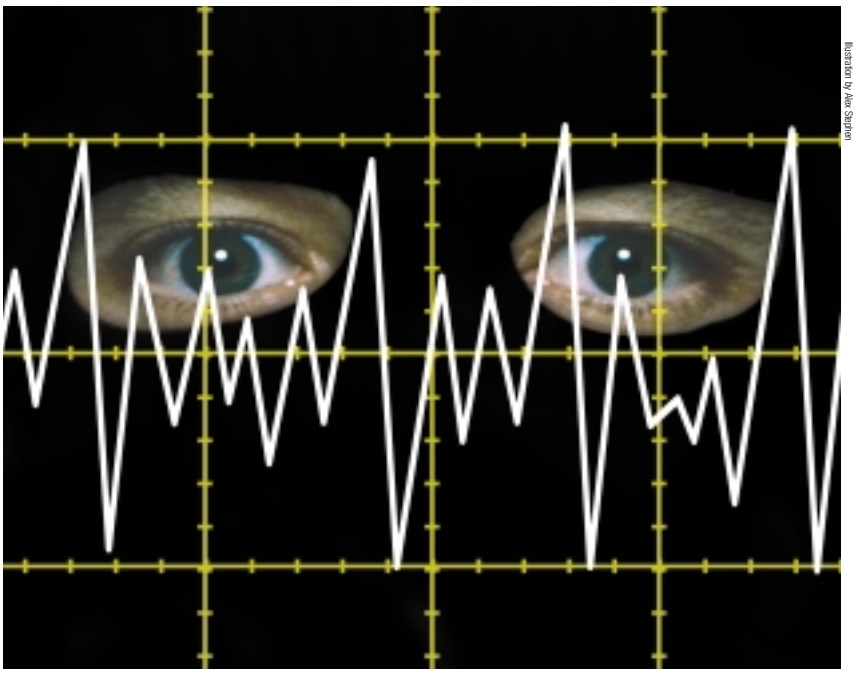

Illustration by Alex Stephen

Cyber Nightmare

In addition, microprocessor-based relays are prone to another form of modern remote terrorism besides electromagnetic terrorism: cyber-attacks.

Hackers' attacks are becoming terrorist weapons. Real cases of terrorist attacks of this kind usually are kept secret, but some already are known. For example, the special services of Iran for several months in 2003 attempted to damage the Israeli power system with the help of a hacker's attack.[3] Fortunately, the security service of the Israel Electric Corp. managed to »

NOTICE OF RFP BY NEW MEXICO ATTORNEY GENERAL'S OFFICE FOR UTILITY REGULATORY CONSULTING SERVICES – RELEASE DATE: June 1, 2005

The New Mexico Attorney General's Office represents ratepayers before the New Mexico Public Regulation Commission and also represents the state of New Mexico before courts and regulatory bodies. The AGO invites written proposals in response to RFP 06-305-P625-0001, from persons interested in providing consulting and expert witness services to the AGO in public utility regulatory proceedings.

For copies of the RFP with more information and instructions, fax a request to Lisa Ortiz at 505.827.6071 or write:

Office of the New Mexico Attorney General
Administrative Services Div.
PO Drawer 1508
Santa Fe, NM 87504-1508

Responses to this RFP must be received by the AGO by 4:00 p.m. on June 21, 2005.

Electromagnetic Weaponry

Physicist Arthur H. Compton proposed the theory behind the E-bomb in 1925. Compton demonstrated that firing a stream of highly energetic photons into atoms that have a low atomic number causes them to eject a stream of electrons. Physics students know this phenomenon as the Compton Effect. It became a key tool in unlocking the secrets of the atom.

Ironically, this nuclear research led to an unexpected demonstration of the power of the Compton Effect, and spawned a new type of weapon. In 1958, nuclear weapons designers ignited hydrogen bombs high over the Pacific Ocean. The detonations created bursts of gamma rays that, upon striking the oxygen and nitrogen in the atmosphere, released a tsunami of electrons that spread for hundreds of miles. Street lights were blown out in Hawaii and radio navigation was disrupted for 18 hours as far away as Australia. The United States set out to learn how to "harden" electronics against this electromagnetic pulse (EMP) and develop EMP weapons.

Now, intensive investigations in the electromagnetic weapons field are being carried out in Russia, the United States, England, Germany, and China. In the United States such research is carried out by the biggest companies of the military-industrial establishment, such as TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratories, the Air Force Research Laboratory at Kirtland Air Force Base, New Mexico, and many civil organizations and universities. But market compact electromagnetic pulse sources of directional radiation and with output power of 1 GW and more already are available for sale.—***VG***

block these attacks. Meanwhile, attacks of this kind to the main national computer systems of Israel have become more frequent, leading to a special subdivision within Israeli Counter-Intelligence and Internal Security Service (SHABAK) for countering such attacks.

But this problem is not only Israel's. The North American electric power network is vulnerable to electronic intrusions launched from anywhere in the world, according to studies by the White House, FBI, IEEE, North American Electric Reliability Council (NERC), and National Security Telecommunications Advisory Committee (NSTAC). At the heart of this vulnerability is the capability for remote access to control and protection equipment at generation facilities and transmission and distribution utilities.[4] Remote access to protective equipment historically has been limited to proprietary systems and dedicated network connections. Now, however, there is an increased use of public telephone services, protocols, and network facilities, concurrent with a growing, more sophisticated, worldwide population of computer users and computer hackers.

Is there a solution for this situation? Yes, but only if we:

- Completely replace all electric wires connected to microprocessor relays, including current and voltage circuits, with non-conductive fiber-optical wires;
- Use opto-electronic CT and VT, instead of traditional instrument transformers;
- Provide full galvanic separation from the power electric network by using a power supply of microprocessor relays to carry through the unit "motor-generator";
- Place microprocessor-based relays in a completely closed metal case made with a special technology used for ultrahigh frequencies in which there are no other kinds of the electric equipment.

This is the price we must pay for progress in the field of relay protection. F

V. Gurevich is an engineer at Israel Electric Corp. Contact him at gurevich2@bezeqint.net.

Endnotes:

1. "Electromagnetic Terrorism—What Are the Risks? What Can Be Done?" *Internationl Product Compliance Magazine*, 1997.
2. "The New Cold War: Defending Against Criminal EMI" *Compliance Magazine*, 2001, 5.
3. Internet News Portal "ISRAlandTM" (*http://www.isra.com/*), 2004.
4. "Electric Power Grid Vulnerability to Natural and Intentional Geomagnetic Distrubances." Processing of 16th International Zurich Symosium on Electromagnetic Compatibilities, February 4-18, 2005, Zurich.