Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)

William A. Radasky, *Senior Member, IEEE*, Carl E. Baum, *Fellow, IEEE*, and Manuem W. Wik, *Senior Member, IEEE*

***Abstract*—A new threat to civil society has recently emerged. It is known as intentional electromagnetic interference (IEMI) and covers the threat of intense electromagnetic disturbances that may be applied to the sophisticated electronic systems that are so important to our daily lives. This paper provides a brief background for the threat, defines important terms, describes the different types of electromagnetic threats, explores the importance of topological concepts, summarizes the current understanding of equipment susceptibility, provides an overview of protection concepts, and summarizes the ongoing work in international standardization. This paper also serves as the introduction to the IEMI papers in this special issue.**

***Index Terms*—High-power electromagnetics (HPEM), intentional electromagnetic interference (IEMI), standardization, system effects, transients.**

I. Introduction to the Special Issue

THE SPECIAL ISSUE begins with this introductory paper:

- Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI).

The next group of papers deals with the classification of IEMI waveforms and HPEM test capabilities to generate waveforms:

- Classification of Intentional Electromagnetic Environments (IEME), by D. V. Giri and F. M. Tesche.
- Overview of Four European High-Power Microwave Narrow-Band Test Facilities, by F. Sabath, M. Bäckström, B. Nordström, D. Sérafin, A. Kaiser, B. Kerr, and D. Nitsch.
- Survey of Worldwide High-Power Wideband Capabilities, by W. D. Prather, C. E. Baum, R. J.Torres, F. Sabath, and D. Nitsch.

The next three papers deal with the coupling process as applied to cables and systems:

- New Propagation Models for Electromagnetic Waves Along Uniform and Nonuniform Cables, by H. Haase, T. Steinmetz, and J. Nitsch.
- EMEC—An EM Simulator Based on Topology, by J. Carlsson, T. Karlsson, and G. Undén.
- Numerical Coupling Models for Complex Systems and Results, by J.-P. Parmantier.

The next six papers deal with the effects of IEMI on equipment, systems and communications:

- Predicting the Breakdown Behavior of Microcontrollers Under EMP/UWB Impact Using a Statistical Analysis, by M. Camp, H. Gerth, H. Garbe, and H. Haase.
- Susceptibility of Some Electronic Equipment to HPEM Threats, by D. Nitsch, M. Camp, F. Sabath, J. L. ter Haseborg, and H. Garbe.
- Trends in EM Susceptibility of IT Equipment, by R. Hoad, N. J. Carter, D. Herke, and S. P. Watkins.
- Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience, by M. G Bäckström and K. Lövstrand.
- Conducted IEMI Threats for Commercial Buildings, by Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky, and M. Ianoz.
- Hardware Invariant Protocol Disruptive Interference for 100BaseTx Ethernet Communications, by I. Jeffrey, C. Gilmore, G. Siemens, and J. LoVetri.

The last three papers deal with protection, measurements and standards:

- Linear and Nonlinear Filters Suppressing UWB Pulses, by T. Weber, R. Krzikalla, and J. L. ter Haseborg.
- Measurement Techniques for Conducted HPEM Signals, by T. Weber and J. L. ter Haseborg.
- Development of High-Power Electromagnetic (HPEM) Standards, by M. W. Wik and W. A. Radasky.

A. Background

The term, high-power electromagnetics (HPEM), has been used for many years and generally describes a set of transient electromagnetic (EM) environments where the peak electric and magnetic fields can be intense. The typical environments considered are the EM fields from nearby lightning strikes, the EM fields near an electrostatic discharge, the EM pulse (EMP) created by nuclear bursts, and the EM fields created by radar systems. It should be noted that the Electromagnetic Compatibility (EMC) Society of the IEEE has a technical committee TC-5 with the title of "High Power Electromagnetics" dealing with all of these subjects. In addition, the International Electrotechnical Commission (IEC) is developing standards for commercial

Manuscript received September 15, 2003; revised April 14, 2004. This work was supported in part by Metatech Corporation IR&D, Goleta, CA 93117.

W. A. Radasky is with Metatech Corporation, Goleta, CA 93117 USA (e-mail: wradasky@aol.com).

C. E. Baum is with the Air Force Research Laboratory, Directed Energy Directorate, Kirtland Air Force Base, NM 87118 USA (e-mail: Magdalena.Lopez@kirtland.af.mil).

M. W. Wik is with the Defence Materiel Administration (FMV) in Stockholm, SE-115 88 Sweden (e-mail: manuel.wik@fmv.se).

Digital Object Identifier 10.1109/TEMC.2004.831899

0018-9375/04$20.00 © 2004 IEEE

equipment and systems under subcommittee 77C which is entitled, "EMC: High power transient phenomena."

Most recently two new terms have arisen in the EMC field—EM terrorism [1] and IEMI [2]. In recent years the scientific community has decided to promote the more generic term IEMI, which includes EM terrorism. In February 1999, at a workshop held at the Zurich EMC Symposium, a widely accepted definition for IEMI was suggested: "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."

Note that hackers are not mentioned explicitly in this definition, although in most countries of the world, an attack on commercial interests for "entertainment" is against the law. While the motives of the attackers may vary, the results can be the same for civil society. The scientific community has been working to understand this threat and to protect against it in a more precise manner.

It is important to recognize that this IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY Special Issue is following two related important IEEE special issues covering the nuclear EMP in 1978 [3], and the Special Issue on High-Power Microwaves (HPM) in 1992 [4]. It is clear that many EM models and codes developed in the past to deal with the intense, high-frequency portion of the EMP and the high levels of fields associated with HPM are relevant to the new field of IEMI. This is due to the fact that the analysis of transient, time-domain EM fields, their coupling to electronic systems, and the protection of equipment and systems from these environments require an understanding of both time-dependent and nonlinear aspects, factors not always present in the routine treatment of EMC.

B. Past Experience With HPEM Effects on Systems

While concern is often directed at modern electronic devices with solid-state digital electronics that are common today, damage to electronic systems has occurred in the past. In particular, in 1967, the *USS Forrestal* was involved in one of the worst cases of electromagnetic interference (EMI) ever documented. During a carrier landing, a military aircraft was exposed to the ship's radar and accidentally fired its munitions hitting a fully armed and fueled aircraft on the deck. The explosions caused severe damage to the carrier and resulted in 134 deaths. A later investigation discovered that a degraded cable shield termination on the landing aircraft was the cause of the accident [5].

Such occurrences of EMI are not limited to the military. When antilock braking systems (ABS) were first introduced, problems arose in Germany on the autobahn when brakes were applied when the autos passed a nearby radio transmitter. This problem was mitigated by the placement of a mesh screen [5].

The medical care industry has also been affected by EMI. A 93-year-old heart attack victim died when the attached monitor and defibrillator shut down every time the radio transmitter was used in an ambulance. This was due to the metal fiberglass ambulance roof that allowed high levels of radiated radio fields inside the patient area of the ambulance [5].

These instances of HPEM fields impacting electrical systems were inadvertent consequences of a poor system design or implementation, abnormally large EM fields, or both. It is possible, however, to envision the use of HPEM sources to intentionally cause upset or damage in a system. Such a situation could occur in a military setting, where the HPEM environment could be directed toward an enemy system. More to the point for our concerns for civil society, an attack by hackers, criminals, or terrorists could produce IEMI.

IEMI concerns have been the subject of technical sessions in recent scientific symposia [6]–[9] and continue to be discussed in the popular press [10], [11]. Although there are several unconfirmed accounts of instances where such (EM) weapons have been used against civil and military systems [12], [13], obtaining clear, convincing and documented evidence of these cases remains elusive.

While there is a lack of clear proof linking the use of such HPEM sources to attack civil facilities, several governments have publicly indicated that they are assessing the possible effects of HPEM environments on their systems and infrastructure. Two examples include a research effort in Sweden [14] and recent testimony before the U.S. Congress about the possibility of the use of radio frequency (RF) weapons [15].

C. Impacts of IEMI on Society

The first question one might ask is whether there really is any reason for society to be concerned about this problem. In fact there are many as indicated below:

1) terrorist threats are increasing world-wide;
2) covert operation outside physical barriers are attractive;
3) technological advances have produced higher-energy RF sources and more efficient antennas;
4) proliferation of IEMI sources is increasing;
5) society's dependence on information and on automated mission-critical and safety-critical electronic systems is increasing;
6) EM susceptibility of new high-density IT systems working at higher frequencies and lower voltages is increasing.

In August of 1999, this problem was recognized by the International Radio Scientific Union (URSI) during a special session that resulted in an URSI resolution. The URSI "Resolution of Criminal Activities using Electromagnetic Tools" [9] was intended to make people aware of the following:

1) the existence of criminal activities using EM tools and associated phenomena;
2) the fact that criminal activities using EM tools can be undertaken covertly and anonymously and that physical boundaries such as fences and walls can be penetrated by EM fields;
3) the potentially serious nature of the effects of criminal activities using EM tools on the infrastructure and important functions in society such as transportation, communication, security, and medicine;
4) that the possible disruptions of the health and economic activities of nations could have major consequences.

The URSI Council recommended to the scientific community in general, and the EMC community in particular, to take account of this threat and to undertake the following actions.

1) Perform additional research pertaining to criminal activities using EM tools in order to establish appropriate levels of vulnerability.

2) Investigate techniques for appropriate protection against criminal activities using EM tools and to provide methods that can be used to protect the public from the damage that can be done to the infrastructure by terrorists.
3) Develop high-quality testing and assessment methods to evaluate system performance in these special EM environments.
4) Provide data regarding the formulation of standards of protection and support standardization work.

II. Sources/Antennas/Environments

In order to understand the threats to electronic equipment, it is necessary to understand the different types of EM environments that can be produced and that can create operational problems for exposed equipment. There are two major categories of EM environments of concern: narrowband and wideband. There are also two major ways for this energy to be delivered to a system: radiated and conducted.

A narrowband waveform is nearly a single frequency (typically a bandwidth of less than 1% of the center frequency) of power delivered over a fixed time frame (from 100 ns to microseconds). For experiments performed on equipment where vulnerabilities have been noted due to radiated fields, frequencies between 0.2 and 5 GHz seem to be of most concern. Of course higher and lower frequencies may also cause problems with system performance, especially if a system resonance is found. Also some environments in this category include modulation of the sine waves, shifting frequencies, and repetitive applications. This category of radiated threat is often referred to as high-power microwaves (HPM), although this term is used loosely to include frequencies outside of the microwave range.

A wideband waveform [sometimes referred to as ultrawideband (UWB) or short pulse (SP)] is usually one in which a time domain pulse is delivered, often in a repetitive fashion. The term "wideband" indicates that the energy in the waveform is produced over a substantial frequency range relative to the "center frequency." Of course many pulse waveforms do not have an explicit center frequency, and more precise definitions are being developed at this time to divide the wideband category into several subcategories. As described by Giri and Tesche [16], they have suggested four terms to describe the bandwidths of wideband waveforms: hypoband, mesoband, subhyperband, and hyperband. These terms have been defined based on the bandratio (ratio of high and low frequencies containing 90% of the energy) with values of $<1.01, 1.01–3, 3–10$, and >10, respectively.

In terms of system vulnerabilities, the narrowband threat is usually one of very high power, since the electrical energy is delivered in a narrow frequency band. It is fairly easy to deliver fields on the order of thousands of volts/meter at a single frequency. Of course each system under test may have a vulnerable frequency that is different from the next. Often the malfunctions observed in testing equipment with narrowband waveforms are those of permanent damage. Available test facilities using the narrowband or hypoband waveforms are found in the paper by Sabath *et al.* [17].

The wideband threat is somewhat different in this respect. Since a time domain pulse produces energy over many frequencies at the same time, the energy density at any single frequency is much less. This means that damage is not as likely as in the narrowband case; however, it is easier to find a system's vulnerability since many frequencies are applied at the same time. Sources that have been built in the past typically produce repetitive pulses that can continue for many seconds or minutes thereby increasing the probability of producing a system upset. Test facilities producing these types of waveforms are described in the paper by Prather, *et al.* [18].

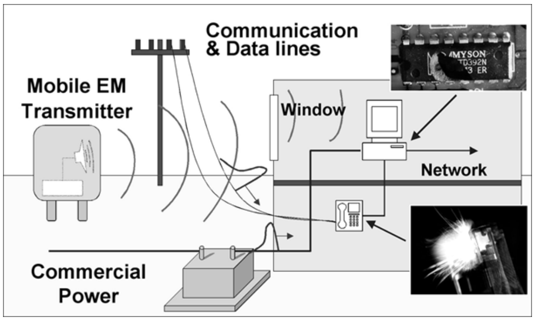

Fig. 1. Typical IEMI interactions of radiated fields.

While the waveform characteristics are defined above, there are two primary ways that they may be delivered to a system. One is through the application of radiated fields, and the other is through conduction along cables and wires. These two methods of delivery are consistent with the general treatment of EM disturbances in the field of EMC where nearly all environments and tests are defined in terms of radiated or conducted environments (e.g., IEC 61 000-2-5) [19].

For radiated fields, it seems clear that frequencies above 100 MHz are of primary concern in that they are able to penetrate unshielded or poorly protected buildings very well and yet couple efficiently to the equipment inside of the building. In addition, they have the advantage that antennas designed to radiate efficiently at these frequencies are small. Fig. 1 illustrates a qualitative view of how radiated fields may illuminate and couple to system electronics through apertures (e.g., windows) and through building wiring.

For conducted voltages and currents, there are some differences in terms of the frequency range of interest. It is well established that if conducted signals are injected into the power supply or telecom cables outside of a building, that frequencies below 10 MHz (and pulsewidths wider than 50 ns) propagate more efficiently than higher frequencies. Experiments by Parfenov *et al.* have shown that these "lower" frequencies can disrupt the operation of equipment inside a building [20]. Parfenov *et al.* [21] provides a complete overview of the problem posed by conducted threats.

III. The EM Interaction Process

A. Topology

The fundamental concept for understanding the interaction of EM fields with complex electronic systems (e.g., an aircraft) is EM topology. In this concept, the system is divided into a set of volumes with boundary surfaces connecting these surfaces [22]. Judicious choices of such surfaces include conducting sheets, which can be utilized for their shielding properties. Unavoid-

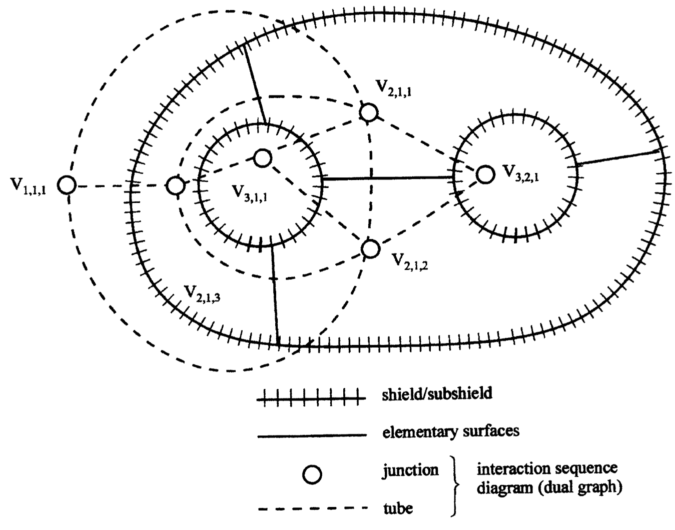

Fig. 2. Electromagnetic topology (hierarchical).

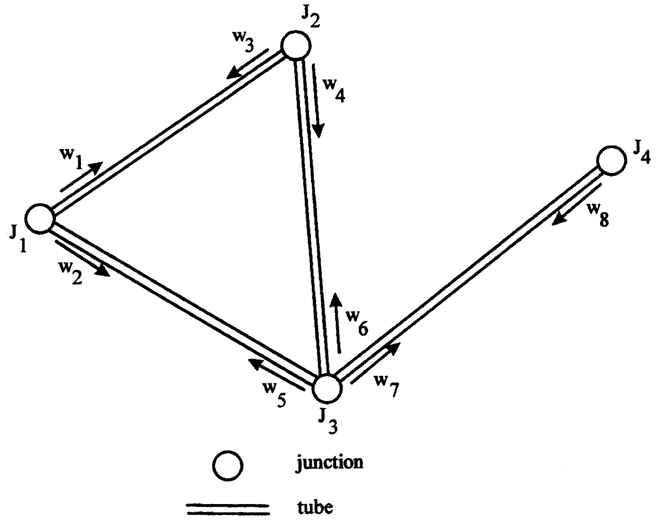

Fig. 3. MTL network.

ably, there will be penetrations (apertures, signal and power conductors, water pipes, etc.).

At this level of description, we have a qualitative EM topology in which the volumes and surfaces can be placed in a one-to-one correspondence with the vertices (nodes or junctions) and edges (branches, tubes), respectively, in a graph known as the interaction sequence diagram [23], as indicated in Fig. 2.

At this level of detail we have presented a fundamental concept for system protection (hardening): the control of all EM fields penetrating selected surfaces (shields, subshields) to control the interior fields via the EM uniqueness theorem. This includes all penetrations such as wires and apertures.

The subject of quantitative EM topology is tied to the Baum–Liu–Tesche (BLT) equation [24]. In its original form we have

$$\begin{aligned}&[((1_{n,m})_{u,v})((\tilde{S}_{n,m}(s))_{u,v})\\&\quad - \Theta((\tilde{\Gamma}_{n,m}(s))_{u,v})]\Theta((\tilde{V}_n(s))_u)\\&\qquad = ((\tilde{S}_{n,m}(s))_{u,v})\Theta((\tilde{V}_n^s(s))_u)\end{aligned} \tag{1}$$

which applies to a uniform multiconductor-transmission-line (MTL) network such as in Fig. 3.

Here the outer indices (u, v) on the supermatrices are topological parameters labeling the various waves $(\tilde{V}_n(s))_u$ (linear combinations of voltage and current vectors leaving the junctions) propagating on the tubes. We also have defined

$$\begin{aligned}\left((\tilde{S}_{n,m}(s))_{u,v}\right) &= \text{scattering supermatrix}\\ \left((\tilde{\Gamma}_{n,m}(s))_{u,v}\right) &= \text{propagation supermatrix}\\ \left((\tilde{V}_n^s(s))_u\right) &= \text{combined voltage source vector including}\\ &\quad\ \text{integrals over the distributed sources.}\end{aligned} \tag{2}$$

There is a large set of literature covering the BLT equation, and the reader is referred to the references, such as those included in a summary paper [25]. This form of the BLT equation (BLT1) has been implemented with great success in computer codes such as CRIPTE [26]. In both aircraft and automobiles it has given good results (a few decibel accuracy) for frequencies from zero to about 500 MHz. Special forms of the BLT equation have also been developed to include nonuniform MTLs, direct connection between junctions, and special forms for early and late times [27], [28].

One advantage of the topological description concerns the definition of closed surfaces (shields, subshields) that results in a hierarchical topology, as in Fig. 2. In this case, if one can control the signals penetrating these closed surfaces to be small compared to those outside the surfaces, one can use the good shielding approximation which separates the interaction supermatrix [left part of (1)] into three parts corresponding to the surface itself [29], thereby greatly simplifying the computation.

B. Norms

At this point one can further simplify the interaction problem, especially for design purposes by looking for bounds on the internal signals instead of detailed calculations. The mathematically rigorous way to do this is by the use of norms [25], [30]. In the frequency domain, norms reduce complex matrices and vectors to real nonnegative scalars. The time domain norms also reduce waveform vectors and convolution matrices to such scalars. The most commonly used norms are the ∞-norm for the peak signal and the 2-norm (square root of the integral of the square) related to power or energy. In conjunction with the good-shielding approximation, the resulting products of matrices and vectors reduce to products of scalars.

Further developments are needed to extend the utility of such norm computations to higher frequencies for application to the IEMI problem. This requires formulating aperture and cavity problems in terms of scattering matrices suitable for inclusion in the BLT formalism [31], in the form of equivalent voltages and currents and in linear combinations to give wave variables.

C. Optimal Illuminating-Environmental Waveforms

Modern electronic equipment is very dependant on computers, which operate at logic levels of a few volts. So an intentional interference needs but to produce a few volts at critical circuits to cause logic upset. Of course, there are details of some significance in the waveform, but the above is the zeroth-order view of the problem. If one raises the interfering signal to some tens of volts, then one may expect permanent damage to occur to the circuit elements by some kind of breakdown, which in turn provides a path for the power supply to insert much more energy. The question then, is how to illuminate the system with some waveform, which optimally couples into critical circuits of interest.

The externally incident fields are characterized by the direction of incidence, polarization, amplitude (volt per meter), and waveform $f(t)$. Concentrating on the waveform, what should this be? There are many possibilities and various sources/antennas to produce them. An important fact to note is that the waveform reaching a critical circuit is in general different from that incident on the system. This is due to the transfer function from the external environment to the internal circuit, with this transfer function typically exhibiting resonant behavior [32]. Using norms one can maximize the ratio of the circuit waveform to the environmental waveform, this having been done for both ∞-norm (peak voltage over peak field) and 2-norm (proportional to the square root of the ratio of square integrals) [33], [34].

This approach shows clearly the great advantage of hypoband (narrowband) waveforms tuned to a resonance in the transfer function. While a hyperband waveform covers a broad spectrum of frequencies, the content matched to a transfer-function resonance is small. Typically a mistuned hypoband waveform produces no less a circuit signal than does a hyperband waveform. The pulse width of the exciting hypoband waveform needs to be somewhat larger than the decay time of the transfer-function resonance (related to Q), so as to ring up the response to near maximum. Typically 100 cycles or so of the exciting waveform are adequate for this purpose of coupling into representative electronic systems. A recent paper gives an experimental demonstration of the above results [35].

Now consider the frequencies of general interest for IEMI. Radiating antenna systems have a gain, which increases with frequency, allowing higher fields on target at higher frequencies. Practical antenna sizes of a few meter aperture dimensions also limit the gain, especially at the lower frequencies. However, practical high-power sources can typically be built with greater power at lower frequencies, implying a tradeoff. Next we must consider the frequencies for maximum transfer functions into the system. It turns out that frequencies around 1 GHz are important for IEMI because typical dimensions of things people build are resonant in this region (the rule of the hand, or Baum's Law [32], [34]). Published data supports the view that the range of roughly 200 MHz to 5 GHz is quite important [36], [37], even demonstrating for unprotected (basically open) systems, functional upset from radiated fields of about 30 V/m.

IV. Susceptibility Levels of Electronic Equipment and Systems

Over the past five years there have been significant experiments that have tested the response of commercial equipment to narrowband and wideband threats similar to those expected from IEMI. In general this testing has emphasized personal computer equipment since it is in wide usage in many different industries.

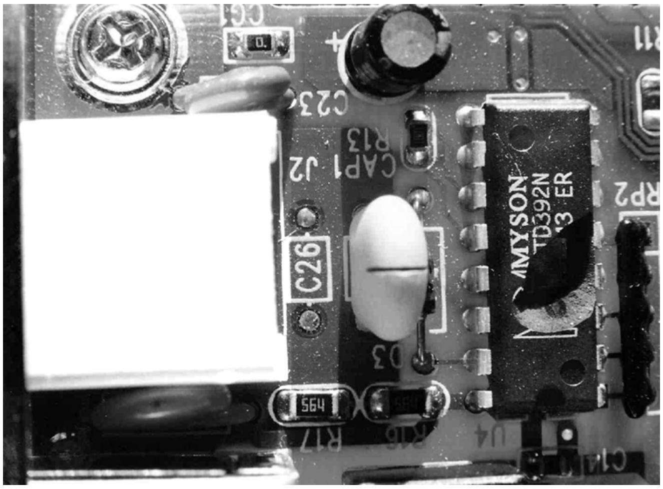

Fig. 4. Damage produced on an Ethernet 10 Base2 computer interface board due to the cable injection of a 500-V telecom pulse as defined in IEC 61 000-4-5.

Modern computers and other types of equipment using microprocessors appear to be vulnerable to malfunction from radiated narrowband fields above 30 V/m [37]. There appear to be large variations in the responses of equipment due to the specific experiment setups and the quality of the equipment enclosures that are used. In addition, tests performed over the range of 1–10 GHz seem to indicate that malfunctions occur at lower field levels at lower frequencies [38]. Unfortunately there have not been many experimental results published that have covered frequencies below 1 GHz, so it is not clear if this trend continues to lower frequencies. There is less experience with the use of wideband radiated field testing, however, there are some indications that peak incident pulse field levels of 1 kV/m will produce malfunctions for a 0.1/1 ns pulse, when it is repetitively pulsed.

One should note that these experiments are usually performed by directly exposing the equipment under test within line of sight of a radiating antenna. Of course if the equipment is inside a building or in a room without a window, there will be a reduction of the incident field from outside to inside. Also, most experiments have not carefully examined the polarization and angle of incidence aspect thoroughly, and therefore most of the effects noted during testing will actually occur at lower field levels when an optimum coupling geometry is applied.

For the conducted threats, it seems clear that if access to external telecom or power cables is not prevented, it is fairly easy to inject harmful signals into a building. Experiments have shown that narrowband voltages injected into the grounding system of a building can cause significant equipment malfunctions inside. Frequencies below 100 Hz and levels below 100 V have been known to cause problems [21]. For slow pulsed waveforms, it appears that pulsewidths on the order of 100 μs can create damage to equipment power supplies and to interface circuit boards (see Fig. 4) at levels as low as 500 V, but more typically at levels of 2–4 kV [20].

While these failure values may seem to be low, they should not be a surprise. When one examines the EMC test requirements for immunity in the IEC, it is unusual to see a narrowband radiated field level requirement above 10 V/m (for frequencies above 80 MHz). This is the recommended immunity level for medical devices that are needed to support life [39]. Higher levels are not recommended because of the expense of providing the increased protection. For narrowband voltages induced on cables connected to equipment, 10 V is the upper level required in most cases [40]. The frequencies of application are below 80 MHz.

For wideband-conducted transients, most of the lightning and electric fast transient tests for EMC are performed for levels up to 2 kV. Only in special cases, such as for equipment in a power generating facility or a substation, will the immunity test levels be higher. The typical EMC wideband test waveforms have rise-times as fast as 5 ns and pulsewidths as long as 700 μs.

There is one area in which a wideband threat has higher levels to consider—the high–altitude EM pulse. HEMP is generated from a high-altitude nuclear detonation. HEMP standards developed by the IEC suggest radiated field tests for fully exposed equipment to a peak electric field level of 50 kV/m with a $2.5/25$ ns wideband pulse [41]. There are corresponding wideband-conducted waveforms that are created during the coupling process. These induced voltages may reach levels of hundreds of kilovolts on external (to the building) power lines [42]. Of course we cannot expect that commercial equipment connected to these lines are immune to HEMP threats, and therefore, it is clear that the IEMI threats exceed the levels that equipment are protected to using "normal" EMC standards. Some protection is therefore required if one wishes to survive this new threat.

V. Protection Concepts

When it comes to protecting a system and its internal equipment from the threat of IEMI, there are several aspects of protection to keep in mind. In particular, solutions can be envisaged in terms of a basic security approach and the well-established EM shielding and penetration protection approach. After a brief summary of each approach, a more detailed discussion of EM hardening measures is provided.

A. Security Approach

From a security point of view, many "normal" security measures can reduce the threat of IEMI:

- develop a "keep out" or buffer zone around your system;
- prevent unauthorized access to all power and communications entering a building;
- keep important internal equipment away from the outer walls of the system;
- use redundancy and diverse routing for important wiring inside the system;
- make backup power available for critical operations.

B. Electromagnetic Approach

From an EM point of view, a list of specific IEMI protection measures is provide as follows:

- provide EM shielding for critical equipment;
- provide surge protection and filters for cables used in critical operations;
- use nonmetallic fiber optic cables when possible;
- monitor the system and its wiring for unusual transients—provide alarms to security personnel;
- develop a verification program to periodically test the immunity of the system.

For fixed systems (e.g., buildings) where nearly all equipment and functions inside are considered critical, it is likely that an approach similar to that taken to protect from HEMP should be considered. This involves a well-shielded (from EM fields) building with all penetrating conductors (including those from external antennas) to be protected with high-level filters and surge protectors. Unfortunately this approach can be very expensive especially if it is not used when the building is constructed. It is also clear that enhancements of the HEMP protection approach to cover frequencies above 100 MHz should also be considered for IEMI.

C. Electromagnetic Protection (Hardening)

After understanding how high-level external EM environments interfere with the functioning of electronic systems, one is then in a position to design protection into the system. This can be accomplished in several ways.

1) Distance (Separation From the Interfering Source): By forcing the interfering source to be farther away from the electronic system, the interfering environment incident at the system is reduced. Generally one is in the far field zone where the fields fall off as $1/r$. This separation can be enforced by building physical barriers (fences, walls) around the site (e.g., an airport).

2) Shielding: Referring back to Section III-A on qualitative topology, one can utilize conductors (e.g., metal sheets, braids) as shields. The thickness of highly conductive metal is generally unimportant; the continuity is very important especially at high-IEMI frequencies. Where possible, existing conductors placed for mechanical reasons can be incorporated into the shielding design. For protection of commercial systems from IEMI, it may be sufficient to consolidate critical equipment inside the building and to shield that equipment in a small room or in racks.

3) Penetration Control: If there are to be electrical connections (antennas, communication lines, power lines) to the outside world, then these penetrate the shields and can allow in the interfering environment with little attenuation. Such penetrations must be controlled. Surge arresters and filters will be needed to reduce the high-level and generally fast IEMI disturbances. Inside a building the use of fiber optic cables (without metallic conductors) can also be advantageous as long as they are properly inserted through equipment shields using appropriate waveguides.

4) Resonance Reduction: Since resonance in transfer functions to the interior can be exploited in IEMI, it is useful to reduce its effect. This requires damping (lowering the Q) of the resonances. This can be accomplished by combinations of inductance and resistance to load conductors in cavities and by judicious placement of resistors electrically connected between conductors inside cavities [43]. Viewed another way, such resonance loading provides some place(s) for the interfering energy to be absorbed, instead of in critical circuits.

5) Fault-Tolerant Computation: Since digital equipment is subject to upset [change in logic state(s)], one should design redundancy in the form of error detection and correction. This makes the system less susceptible. One should also account for the possibility that the IEMI environment may be repetitive at rates up to the megahertz range.

6) Circumvention: One can also include special detectors that sense the presence of an IEMI environment. In turn, the electronic system is commanded to take appropriate action, such as repeating certain computations that may have been made in error by the interference.

There are many details to be added with respect to the guidelines provided here. It is expected that over the next few years, additional information will emerge from the technical community especially due to the active standardization work ongoing in this area in the IEC.

VI. Standardization

Two major IEMI standardization efforts are currently underway. The first is an effort that has been organized under the IEC. The IEC is headquartered in Geneva, Switzerland, and it is responsible for preparing voluntary standards for electrical and electronic equipment worldwide. It is the worldwide leader in the development of EMC standards.

In the late 1980s, the IEC began the development of environment, protection, and test standards for commercial equipment that might be exposed to the EM fields produced from a high-altitude nuclear burst. These fields are generally known as HEMP (high altitude EMP), although in actuality the term represents a series of pulses with different frequency content that needs to be considered. These range from nanosecond pulses to pulses with rise and fall times of seconds. This work was assigned to Subcommittee 77C, and in 1999 this work was expanded to include all high-power EM transient threats, including those from IEMI.

As of March 2004, SC 77C has 17 documents in its program of work, including 14 that have been published. The publications of SC77C are part of the IEC EMC 61 000 series of documents. There are three documents that deal with HPEM and IEMI being prepared at this time. See the paper by Wik and Radasky in this special issue for more details on the work of IEC SC 77C [44].

A second standardization activity has begun in the IEEE EMC Society to develop standard practices to protect public accessible computers including electronic voting machines from IEMI [45], [46]. It is envisaged that protection guidelines and tests will be defined as part of this effort.

References

[1] R. L. Gardner, "Electromagnetic terrorism. A real danger," in *Proc. 11th Symp. Electromagnetic Compatibility*, Wroctaw, Poland, June 1998.

[2] W. A. Radasky, M. A. Messier, and M. W. Wik, "Intentional electromagnetic interference (EMI)—Test and data implications," in *Proc. Zurich EMC Symp* , Zurich, Switzerland, Feb. 2001.

[3] *IEEE Trans. Electromagn. Compat. (Joint Special Issue on the Nuclear Electromagnetic Pulse)*, vol. 20, Feb. 1978.

[4] *IEEE Trans. Electromagn. Compat. (Joint Special Issue on High-Power Microwaves)*, vol. 34, Aug. 1992.

[5] P. O. Leach and M. B. Alexander, "Electronic Systems Failures and Anomalies Attributed to Electromagnetic Interference," National Aeronautics and Space Administration, Washington, DC, NASA Report 1374, July 1995. CC 20 546-0001.

[6] "Workshop on electromagnetic terrorism and adverse effects of high power electromagnetic (HPE) environments," in *Proc. 13th Int. Zurich Symp. Technical Exhibition on Electromagnetic Compatibility*, Feb. 16–18, 1999.

[7] *Proc. AMEREM'96*, Albuquerque, NM, May 27–31, 1996.

[8] *Proc. EUROEM'98*, Tel. Aviv., Israel, June 14–19, 1998. EUROEM 2000 Edinburgh, Scotland, 30 May—2 June 2000.

[9] *Int. Radio Scientific Union (URSI) General Assembly*, 1999.

[10] E. Rosenberg, "New face of terrorism: radio-frequency weapons," *The New York Times*, June 23, 1997.

[11] "City surrenders £400 million to gangs," in *The Sunday Times*, London, U.K., June 2, 1996.

[12] V. M. Loborev, "The modern research problems," presented at the Plenary Lecture, AMEREM'96, Albuquerque, NM, May 1996.

[13] D. Sawyer, 20/20 *Segment on Non-Lethal Weapons*. New York: American Broadcasting Company (ABC), Feb. 1999.

[14] M. Bäckström, C. Frost, and P. Ånäs, *Förstudie rörande vitala samhällssystems motståndsförmåga mot elektromagnetisk strålning med hög intensitet (HPM)*, Aug. 1997, Användarrapport FOA-R-97-00 538-612-SE, ISSN 1104-9154. Abstract in English, English title: "Preliminary Study on the Resistance of Critical Societal Functions Against Intense Electromagnetic Radiation".

[15] I. W. Merritt, *Proliferation and Significance of Radio Frequency Weapons Technology*: United States Congress, U. S. Army Space and Missile Defense Command, Feb. 25, 1998. Testimony before the Joint Economic Committee.

[16] D. V. Giri and F. Tesche, "Classification of Intentional Electromagnetic Environments (IEME)," *IEEE Trans. Electromagn. Compat*, vol. 46, pp. 322–328, Aug. 2004.

[17] F. Sabath, M. Backstrom, B. Nordstrom, D. Serafin, A. Kaiser, B. Kerr, and D. Nitsch, "Overview of four European high-power microwave narrow-band test facilities," *IEEE Trans. Electromagn. Compat*, vol. 46, pp. 329–334, Aug. 2004.

[18] W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath, and D. Nitsch, "Survey of worldwide high-power wideband capabilities," *IEEE Trans. Electromagn. Compat*, vol. 46, pp. 335–344, Aug. 2004.

[19] *Electromagnetic compatibility (EMC)—Part 2: Environment—Section 5: Classification of Electromagnetic Environments.*

[20] V. Fortov, Yu. Parfenov, L. Zdoukhov, R. Borisov, S. Petrov, and L. Siniy, "A computer code for estimating pulsed electromagnetic disturbances penetrating into building power and earthing connections," in *Proc. 14th Int. Zurich Symp. Technical Exhibition EMC*, Zurich, Switzerland, Feb. 2001.

[21] Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky, and M. Ianoz, "Conducted IEMI threats for commercial buildings," *IEEE Trans. Electromagn. Compat.*, vol. 46, pp. 404–411, Aug. 2004.

[22] J.-P. Parmantier, "Numerical coupling models for complex systems and results," *IEEE Trans. Electromagn. Compat.*, vol. 46, pp. 359–367, Aug. 2004.

[23] C. E. Baum, "How to think about EMP interaction," in *Spring FULMEN Mtg. (FULMEN 2)*, Albuquerque, NM, 1974, pp. 12–23.

[24] C. E. Baum, T. K. Liu, and F. M. Tesche, "On the analysis of general multiconductor transmission-line networks," *Interaction Note 350*, Nov. 1978.

[25] C. E. Baum, "The theory of electromagnetic interference control," in *Modern Radio Science 1990*, J. B. Andersen, Ed. London, U.K.: Oxford Univ. Press, 1989, Interaction Note 478, pp. 87–101.

[26] J. P. Parmantier and P. Degauque, "Topology based modeling of very large systems," in *Modern Radio Science 1996*, J. Hamelin, Ed. London, U.K.: Oxford Univ. Press, pp. 151–177.

[27] C. E. Baum, "Generalization of the BLT equation," in *Proc. 13th Int. Zurich Symp. EMC*, Interaction Note 511, 1995, 1999, pp. 131–136.

[28] ——, "Extension of the BLT equation into time domain," in *Proc. 14th Int. Zurich Symp. EMC*, Interaction Note 553, 1999, 2001, pp. 211–216.

[29] ——, "On the use of electromagnetic topology for the decomposition of scattering matrices for complex physical structures," *Interaction Note 454*, 1985.

[30] ——, "Norms of time-domain functions and convolution operators," in *Recent Advances in Electromagnetic Theory*, H. N. Kritikos and D. L. Jaggard, Eds. New York: Springer-Verlog, 1990, Mathematics Note 86, 1985, ch. 2, pp. 31–55.

[31] ——, "Including aperture and cavities in the BLT formalism," *Interaction Note 581*, 2003.

[32] ——, "Maximization of electromagnetic response at a distance," in *IEEE Trans. Electromagn. Compat. 1992*, vol. 34, Aug. 1992, pp. 148–153.

[33] ——, "Comparative system response to resonant and unipolar waveforms," in *Proc. 13th Int. Zurich Symp, EMC*, Interaction Note 509, 1994, 1999, pp. 15–20.

[34] ——, "A time-domain view of choice of transient excitation waveforms for enhanced response of electronic systems," in *Proc. ICEAA 01*, Interaction Note 560, 2000, Turin, Italy, 2001, pp. 181–184.

[35] D. Nitsch, F. Sabath, H.-U. Schmidt, and C. Braun, "Comparison of the HPM and UWB susceptibility of modern microprocessor boards," in *Proc. 15th Int. Zurich Symp. EMC*, System Design and Assessment Note 36, 2002, 2003, pp. 121–126.

[36] J. Bohl, "High power microwave hazard facing smart ammunitions,", System Design and Assessment Note 35, 1995.

[37] J. LoVetri, A. T. M. Wilburs, and A. P. M. Zwamborn, "Microwave interaction with a personal computer: Experiment and modeling," in *Proc. 13th Int. Zurich Symp. EMC*, 1999, pp. 203–206.

[38] M. Bäckström, "HPM testing of a car: A representative example of the susceptibility of civil systems," in *13th Int. Zurich Symp. Supplement*, Feb. 1999, pp. 189–190.

[39] *Medical Electrical Equipment—Part 1–2: General Requirements for Safety—Collateral Standard: Electromagnetic Compatibility—Requirements and Tests*.

[40] *Electromagnetic Compatibility (EMC)—Part 4–6: Testing and Measurement Techniques—Immunity to Conducted Disturbances, Induced by Radio-Frequency Fields*.

[41] *Electromagnetic Compatibility (EMC)—Part 2: Environment—Section 9: Description of HEMP Environment—Radiated Disturbance*.

[42] *Electromagnetic Compatibility (EMC)—Part 2–10: Environment—Description of HEMP Environment—Conducted Disturbance*.

[43] C. E. Baum and D. P. McLemore, "Damping transmission-line and cavity resonance," in *Proc. 12th Int. Zurich Symp. EMC, 1999*, Interaction note 503, 1994, pp. 239–244.

[44] M. W. Wik and W. A. Radasky, "Development of high power electromagnetic (HPEM) standards," *IEEE Trans. Electromagn. Compat.*, pp. 439–445, Aug. 2004.

[45] *Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI*, IEEE Recommended Practice Project 1642 under development.

[46] *Recommended Practice for Protecting Voting Equipment and Systems from Intentional EMI*, IEEE Recommended Practice Project 1643 under development.

William A. Radasky (S'67–M'68–SM'92) was born in Johnstown, PA, in 1946. He received the B.S. degree with a double major in electrical engineering and engineering science from the U.S. Air Force Academy, Colorado Springs, CO, in 1968, and the M.S. and Ph.D. degrees in electrical engineering from the University of New Mexico, Albuquerque, in 1971 and the University of California, Santa Barbara, in 1981, respectively.

In 1968, he started his career as a Research Engineer at the Air Force Weapons Laboratory in Albuquerque, NM, working on the theory of the electromagnetic pulse (EMP). In 1984, he founded Metatech Corporation in Goleta, CA, where he is currently President and Managing Engineer. During his 36-year career, he has published over 260 technical papers and reports dealing with electromagnetic interference (EMI) and protection. His current research interests include studies to understand the threat of intentional electromagnetic interference (IEMI) and to develop mitigation and monitoring methods to protect facilities from this new threat.

Dr. Radasky is Chairman of IEC Subcommittee 77C, which is developing high-power electromagnetic protection and test standards for civil systems. He is also the Chairman of TC-5 (High Power EM) for the IEEE Electromagnetic Compatibility Society. In addition, he is the Chairman of the IEC Advisory Committee on EMC (ACEC), which is tasked to coordinate all EMC standardization work for the IEC. He was selected as an EMP Fellow in 1988. He is a Member of Eta Kappa Nu and Tau Beta Pi.

Carl E. Baum (S'62–M'63–SM'78–F'84) was born in Binghamton, NY, on February 6, 1940. He received the B.S. (hons), M.S., and Ph.D. degrees in electrical engineering from the California Institute of Technology, Pasadena, in 1962, 1963, and 1969, respectively.

He was stationed at the Air Force Research Laboratory, Directed Energy Directorate (formerly Phillips Laboratory, formerly Air Force Weapons Laboratory), Kirtland AFB, Albuquerque, NM, from 1963 to 1967, and again from 1968 to 1971. Since 1971, has served as a civil servant and Senior Scientist at the Air Force Research Laboratory. He has published four books: *Transient Lens Synthesis: Differential Geometry in Electromagnetic Theory* (New York: Taylor & Francis, 1991), *Electromagnetic Symmetry* (New York: Taylor & Francis, 1995), *Ultra-Wideband, Short-Pulse Electromagnetics 3* (New York: Plenum Press, 1997), *Detection and Identification of Visually Obscured Targets* (New York: Taylor & Francis, 1998). He has led an EMP short course and HPE workshops at numerous locations around the globe.

Dr. Baum was awarded the Air Force Research and Development Award in 1990 and the Air Force Research Laboratory Fellow Award in 1996. He is editor of several interagency note series on electromagnetic pulse (EMP) and related subjects, and received the 1984 Richard R. Stoddart Award from the IEEE Electromagnetic Compatibility Society. He is the recipient of the 1987 Harry Diamond Memorial Award, one of the IEEE Field Awards which carries the citation "for outstanding contributions to the knowledge of transient phenomena in electromagnetics." He is a member of Commissions A, B, and E of the U.S. National Committee of the International Union of Radio Science (URSI). He is Founder and President of the SUMMA Foundation, which sponsors various electromagnetics related activities including scientific conferences, publications, short courses, fellowships, and awards.

Manuel W. Wik (SM'76) was born in Stockholm, Sweden, in 1936. He received the M.S. degree in electrical engineering from The Royal Institute of Technology, Stockholm, Sweden, in 1962.

In 1990, he became a Chief Engineer and the first person to receive the title Strategic Specialist at the Defence Materiel Administration (FMV) in Stockholm. Although retired in 2001, he is still active with the FMV. Formerly, he was head of procurement at the Swedish Armed Forces Telecommunication Transmission Network Section at FMV, and prior to that he worked as a Research Engineer at The Research Institute of National Defence (FOA) responsible for protection against electromagnetic effects from low- and high-altitude nuclear explosions. He contributed to the International Council of Scientific Union, Scientific Committee on Problems of the Environment Project on Environmental Consequences of Nuclear War (ICSU SCOPE ENUWAR) resulting in a series of books. He has written numerous articles, contributed to books, government reports and conference proceedings, and given presentations in the fields of nuclear electromagnetic pulse effects (EMP), electromagnetic compatibility, intentional electromagnetic interference, electronic warfare, threats to telecommunications and national strategy for enhanced IT-security and protection against information operations. His present research interests as a Strategic Specialist include emerging technologies such as high-power electromagnetics (HPEM), and systems and methods for Network Centric Warfare (NCW) (in Sweden named Network Based Defence).

Mr. Wik is Fellow of the Royal Swedish Academy of War Sciences and Secretary of its Division of military technology, Member of the Swedish National Committee of the International Union of Radio Science (URSI), Secretary of the International Electrotechnical Committee (IEC) standardization Subcommittee SC 77C and recognized as an EMP Fellow by the US Summa Foundation. He has been awarded the Carolus XIV medal Ingenio et Fortitudine from the King of Sweden.