Metatech

Meta-R-323

Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid

William Radasky
Edward Savage

Metatech Corporation
358 S. Fairview Ave., Suite E
Goleta, CA 93117

January 2010

Prepared for

Oak Ridge National Laboratory
Attn: Dr. Ben McConnell
1 Bethel Valley Road
P.O. Box 2008
Oak Ridge, Tennessee 37831
Subcontract 6400009137

FOREWORD

This report has been written to provide an overview of Intentional Electromagnetic Interference (IEMI) threats to the electric power infrastructure. It is based on the past 10 years of research by the authors and their colleagues who have been active in the field. Some of the information provided here is adapted from the IEEE Special Issue on HPEM and IEMI published in the IEEE EMC Transactions in August 2004. Additional information is presented from recent published papers and conference proceedings.

This report begins in Section 1 by explaining the background and terminology involved with IEMI. Section 2 summarizes the types of EM weapons that have been built and the IEMI environments that they produce. Section 3 provides insight concerning the basic EM coupling process for IEMI and why certain threat waveforms and frequencies are important to commercial systems. Section 4 provides a selection of commercial equipment susceptibility data covering important categories of equipment that may be affected by IEMI. Section 5 discusses more specific aspects of the IEMI threat for the power system, and Section 6 indicates the IEC standardization efforts that can be useful to understanding the threat of IEMI and the means to protect equipment from the threat.

Table of Contents

List of Figures

List of Tables

**Section 1
Introduction**

1.1 Background

The term, "electromagnetic pulse" (EMP) has unfortunately been used in recent years (mainly by the media) to describe many different types of electromagnetic threats to electronic systems. In this report we will differentiate this general type of electromagnetic threat from the high-altitude electromagnetic pulse (HEMP). The HEMP is generated from a nuclear detonation in space, but the intense electromagnetic fields created there reach the Earth's surface. In the case of non-nuclear EMP, there are many subcategories of terms that describe this electromagnetic threat, which we will clarify and discuss in this report. In general we are speaking of the intense electromagnetic fields generated by a repeatable (non-explosive) high-power generator, which are directed to a target by an antenna. Our concern is how to protect our commercial infrastructure from these new mobile threats. We will refer specifically to this threat as IEMI (intentional electromagnetic interference).

In order to fully describe the terminology we will first describe the term "High Power Electromagnetics (HPEM)"; it has been used for many years and generally describes a set of transient EM environments where the peak electric and magnetic fields can be very high. The typical environments considered are the electromagnetic fields from nearby lightning strikes, the electromagnetic fields near an electrostatic discharge, the electromagnetic fields created in substations due to switching and arcing events, and the electromagnetic fields created by radar systems. In addition to these natural and accidental EM threats, we add, the electromagnetic pulse (HEMP) created by high altitude nuclear bursts and the intentional electromagnetic interference (IEMI).

Figure 1-1 shows qualitatively several of these electromagnetic environments, along with the narrowband and wideband IEMI threats that are the subject of this report. It should be noted that the 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 IEC is developing standards to protect commercial equipment and systems under Subcommittee 77C, which is entitled "EMC: High power transient phenomena".
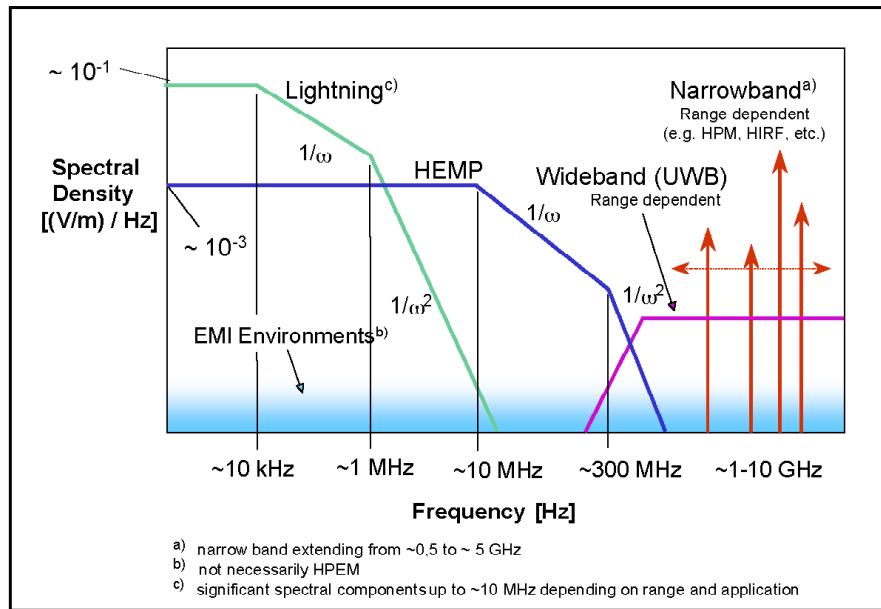
Figure 1-1. Comparison of HPEM environments.

Most recently two new terms have arisen in the EMC field – EM Terrorism [1] and Intentional Electromagnetic Interference (IEMI) [2]. Over the past 10 years the scientific community has decided to accept 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 also 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.

While this report aims to inform the reader about the threat of IEMI against commercial electronic equipment and systems in general, it is clear that the biggest threat is against the civil infrastructure, as shutting down the control electronics associated with the power grid, the telecom network or other parts of the critical infrastructure could have widespread impacts.

1.2   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 EMI ever documented. While sitting on the deck, a military aircraft was exposed to the ship's radar and accidentally fired its munitions, hitting another fully armed and fueled aircraft

on the deck. The explosions and resulting fire caused severe damage to the carrier and resulted in 134 deaths. A later investigation discovered that a degraded cable shield termination on the first aircraft was the cause of the accident [5].

Such occurrences of accidental 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 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 high-power electromagnetic (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 towards 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].

1.3   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:
- Terrorist threats are increasing world-wide
- Covert operation outside physical barriers are attractive
- Technological advances have produced higher-energy RF sources and more efficient antennas
- Proliferation of IEMI sources is increasing
- Society's dependence on information and on automated mission-critical and safety-critical electronic systems is increasing

- EM susceptibility of new high density IT systems working at higher frequencies and lower voltages is increasing

In August 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 existence of criminal activities using electromagnetic tools and associated phenomena
- The fact that criminal activities using electromagnetic tools can be undertaken covertly and anonymously and that physical boundaries such as fences and walls can be penetrated by electromagnetic fields
- The potentially serious nature of the effects of criminal activities using electromagnetic tools on the infrastructure and important functions in society such as transportation, communication, security, and medicine
- 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:
    - Perform additional research pertaining to criminal activities using electromagnetic tools in order to establish appropriate levels of vulnerability
    - Investigate techniques for appropriate protection against criminal activities using electromagnetic 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
    - Develop high-quality testing and assessment methods to evaluate system performance in these special electromagnetic environments
    - Provide data regarding the formulation of standards of protection and support standardization work

It is noted that the International Electrotechnical Commission (IEC) added the IEMI threat to its previous standardization work dealing with HEMP in 1999.

1.4   Definitions of Terms

Every effort is made in this report to define terms as they are used, but this list of terms should be of use to the reader to understand some of the new terminology used in dealing with IEMI. Many of these terms are found in IEC 61000-2-13 [34].

attenuation
reduction in magnitude (as a result of absorption and scattering) of an electric or magnetic field or a current or voltage; usually expressed in decibels

bandratio
br
ratio of the high and low frequencies between which there is 90% of the energy; if the spectrum has a large dc content, the lower limit is nominally defined as 1 Hz

bandratio decades
brd
bandratio expressed in decades as: $brd = \log10(br)$

burst
typically a time frame in which a series of pulses occurs with a given repetition rate. When multiple bursts occur, the time between bursts is usually defined

conducted HPEM environment
high power electromagnetic currents and voltages that are either coupled or directly injected to cables and wires with voltage levels that typically exceed 1 kV

continuous wave
CW
time waveform that has a fixed frequency and is continuous

electromagnetic compatibility
EMC
ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment

electromagnetic disturbance
any electromagnetic phenomenon which may degrade the performance of a device, equipment or system

electromagnetic interference
EMI
degradation of the performance of a device, transmission channel or system caused by an electromagnetic disturbance
NOTE   Disturbance and interference are respectively cause and effect.

(electromagnetic) shield
electrically continuous housing for a facility, area, or component used to attenuate incident electric and magnetic fields by both absorption and reflection

(electromagnetic) susceptibility
inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance
NOTE   Susceptibility is a lack of immunity.

high-altitude electromagnetic pulse
HEMP
electromagnetic pulse produced by a nuclear explosion outside the earth's atmosphere
NOTE   Typically above an altitude of 30 km.

high-power microwaves
HPM
narrowband signals, nominally with peak power in a pulse, in excess of 100 MW at the source
NOTE This is a historical definition that depended on the strength of the source. The interest in this document is mainly on the EM field incident on an electronic system.

hyperband signal
signal or waveform with a pbw value between 163.4% and 200% or a bandratio >10

hypoband signal
narrowband signal
signal or waveform with a pbw of <1% or a bandratio <1.01

intentional electromagnetic interference
IEMI
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

L band
radar frequency band between 1 and 2 GHz

mesoband signal
signal or waveform with a pbw value between 1% and 100% or a bandratio between 1.01 and 3

percentage bandwidth
pbw
bandwidth of a waveform expressed as a percentage of the center frequency of that waveform
NOTE The pbw has a maximum value of 200% when the center frequency is the mean of the high and low frequencies. The pbw does not apply to signals with a large dc content (e.g., HEMP) for which the bandratio decades is used.

point-of-entry
PoE
port-of-entry
PoE
physical location (point) on an electromagnetic barrier, where EM energy may enter or exit a topological volume, unless an adequate PoE protective device is provided
NOTE 1 A PoE is not limited to a geometrical point.
NOTE 2 PoEs are classified as aperture PoEs or conductive PoEs according to the type of penetration. They are also classified as architectural, mechanical, structural or electrical PoEs according to the functions they serve.

pulse
a transient waveform that usually rises to a peak value and then decays, or a similar waveform that is an envelope of an oscillating waveform

radiated HPEM environment
high power electromagnetic fields with peak electric field levels that typically exceed 100 V/m

sub-hyperband signal
a signal or a waveform with a pbw value between 100% and 163.4% or a bandratio between 3 and 10

transient
pertaining to or designating a phenomenon or a quantity which varies between two consecutive steady states during a time interval which is short compared with the time-scale of interest
NOTE   A transient can be a unidirectional impulse of either polarity or a damped oscillatory wave with the first peak occurring in either polarity.

ultrawideband
UWB
a signal that has a percent bandwidth greater than 25%

Section 2
IEMI Environments and Sources

2.1   IEMI Environment Terminology

In order to understand the threats to electronic equipment, it is necessary to understand the different types of electromagnetic 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 as shown in Figure 2-1 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 nanoseconds to microseconds). For experiments performed on equipment where vulnerabilities have been noted due to radiated fields, frequencies between 0.3 and 3 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 (very small handheld equipment may have resonances at frequencies higher than 3 GHz). 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. We prefer to use the term narrowband as it is technically accurate and does not depend on the strength of the source.

20 cycles of f = 1 GHz
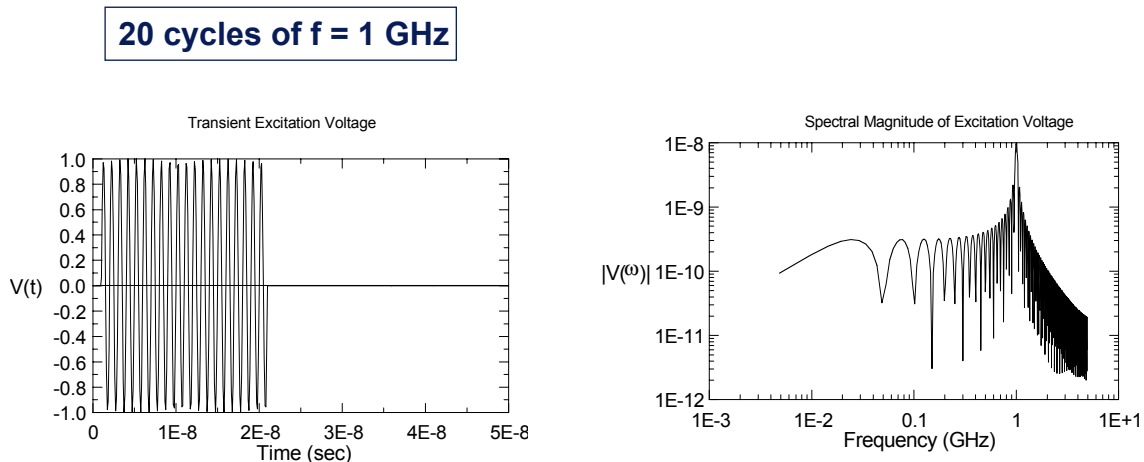
Source: IEC Standard 61000-2-13

Figure 2-1. Example of narrowband waveform and spectrum

A wideband waveform (sometimes referred to as ultrawideband – UWB) 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 have been developed by the IEC to divide the wideband category into several subcategories. Figure 2-2 illustrates a simple example of a wideband pulse.

One cycle at f = 1 GHz

Peaks at 840 MHz
¥BW= 900 MHz
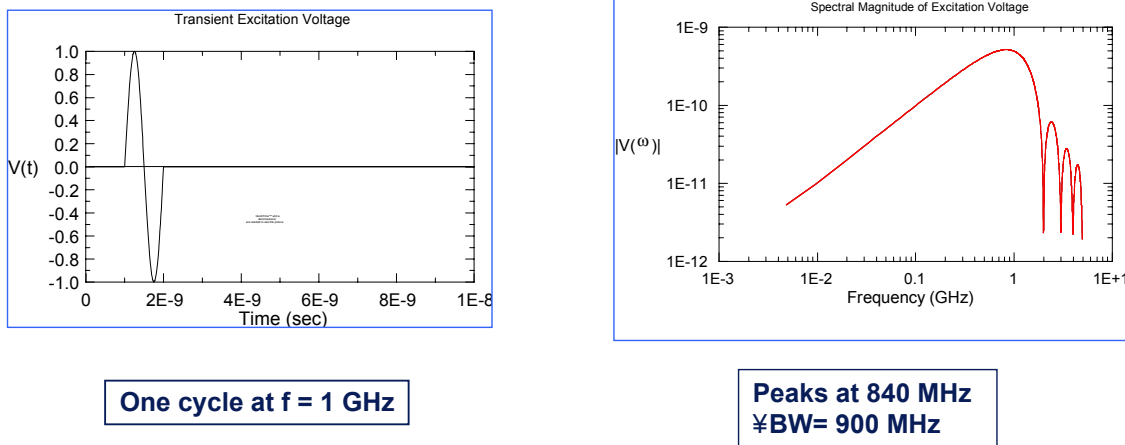
Source: IEC Standard 61000-2-13

Figure 2-2. Example of wideband waveform and spectrum

As described in a paper by Giri and Tesche [16] and published in IEC 61000-2-13, it has been suggested that four terms be used to describe the bandwidths of wideband waveforms – hypoband, mesoband, sub-hyperband 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. Figure 2-3 illustrates these four categories and their relationship to bandwidth formulas. Figure 2-4 illustrates how these bandratios are evaluated.

	Percentage Bandwidth	Bandratio
hypoband or narrowband	$< 1\%$	< 1.01
mesoband	$1\% < \text{pbw} \leq 100\%$	$1.01 < \text{br} \leq 3$
sub-hyperband	$100\% < \text{pbw} < 163.4\%$	$3 < \text{br} \leq 10$
hyperband	$163.4\% < \text{pbw} < 200\%$	$\text{br} \geq 10$

$$\text{band ratio} = \text{br} = \frac{f_h}{f_l}$$

$$\text{band ratio decades} = \text{brd} = \log_{10}(\text{br})$$

$$\text{pbw} = 200\frac{(br-1)}{(br+1)}$$

$$\text{br} = \frac{[1 + \dfrac{pbw}{200}]}{[1 - \dfrac{pbw}{200}]}$$

Figure 2-3. IEMI bandwidth definitions for wideband pulses

Evaluate integral to obtain minimum bandwidth

$$\frac{\displaystyle\int_{f_\ell}^{f_h} \left| \tilde{V}(j\omega) \right|^2 d\omega}{\displaystyle\int_0^\infty \left| \tilde{V}(j\omega) \right|^2 d\omega} = 0.9$$
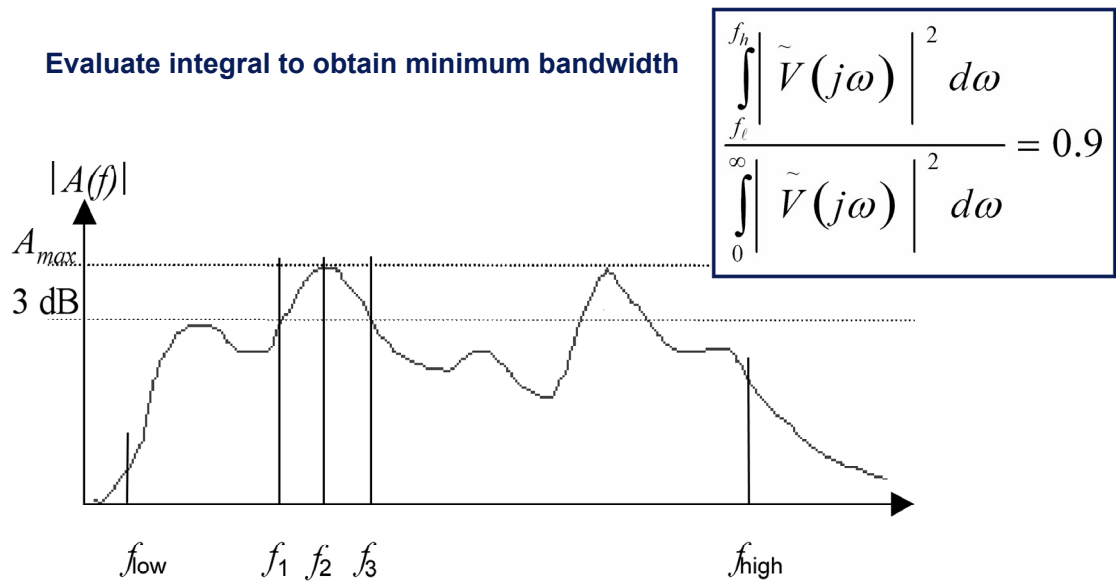
Source: IEC Standard 61000-2-13

Figure 2-4. Method to evaluate the bandratio for wideband pulses

In terms of system vulnerabilities, the narrowband threat is usually one of very high power and high energy, 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 can be found in a paper by Sabath et al. [17] and have recently been published in IEC 61000-4-35.

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 a paper by Prather, et al. [18] and were also published in IEC 61000-4-35.

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 electromagnetic disturbances in the field of electromagnetic compatibility (EMC) where nearly all environments and tests are defined in terms of radiated or conducted environments (e.g., IEC 61000-2-5) [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. Figure 2-5 illustrates a qualitative view of how radiated fields may illuminate and couple to system electronics through apertures (e.g., windows) and through building wiring.
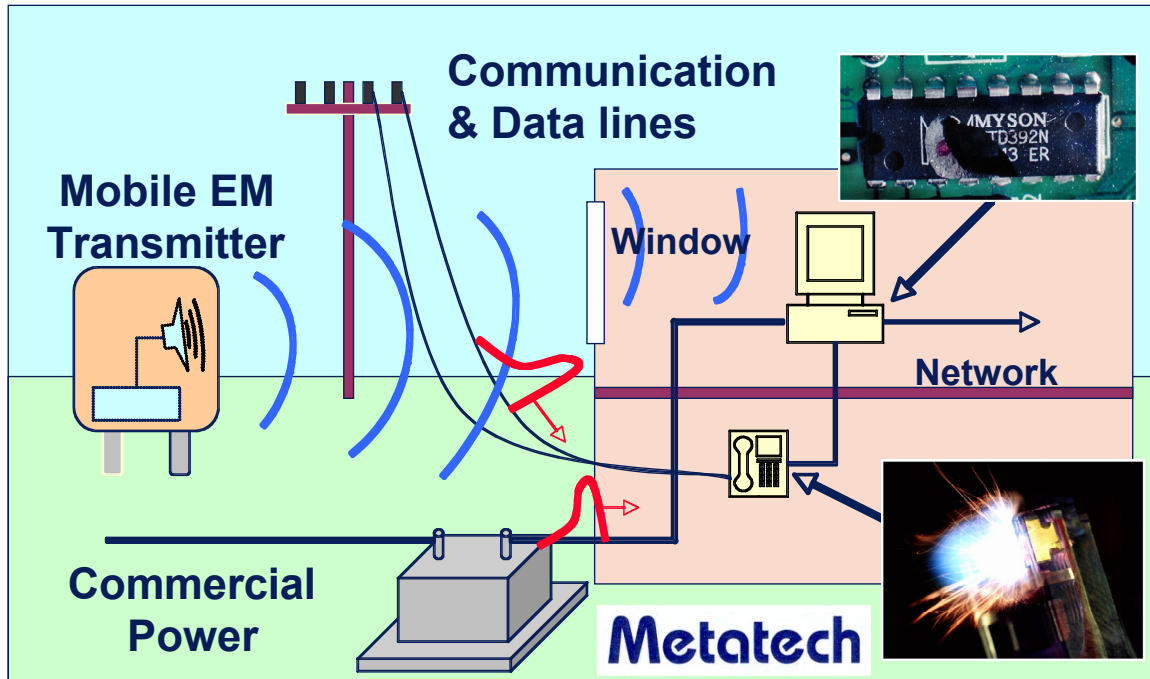
Figure 2-5. Typical IEMI interactions of radiated fields.

For conducted voltages and currents, there are some differences in terms of the frequency range of interest. It is well established that if common-mode conducted signals are injected into the power supply or telecom cables outside of a building, that frequencies below 10 MHz (and pulse widths 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]. A recent IEEE paper provides a complete overview of the problem posed by conducted IEMI threats [21].

2.2   IEMI Radiated Threat Weapons

With regard to actual threat "weapons", the following four figures describes some published examples of devices that could be used as weapons. Figure 2-6 illustrates a briefcase weapon (mesoband) developed by a German company for anti-terrorist actions. Figures 2-7 and 2-8 illustrate hyperband laboratory test generators, which are designed to test equipment near to the source. Note that the actual source of the EM fields is the small high voltage generator. Figure 2-9 illustrates a hyperband source that produces an extremely high level of field at a distance. Narrowband sources can be produced by small radar or microwave systems that can be purchased as military surplus.

- Diehl Munitions Systeme is marketing a small interference source (including antenna)
  - 350 MHz damped sine field
  - 120 kV/m at 1 meter (omni-directional antenna)
  - 30 minute continuous operation (5 pulses per second) or 3 hours in bursts
  - 20 x 16 x 8 inches and 62 pounds

- Demonstration in Summer 2004

Figure 2-6. DIEHL Munitions damped sine IEMI generator.
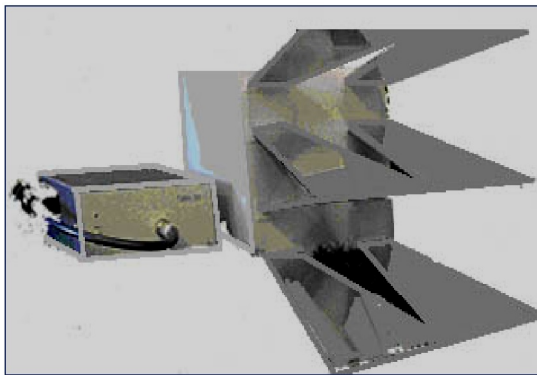
Parameters	Values
Amplitude at 20 m distance	2 kV/m
Pulse duration	0.2 ns
Pulse repetition rate	Up to 1000 Hz
Antenna aperture	0.35 m x 0.35 m

Source: Dr. Yuri Parfenov, Russia

Figure 2-7. Laboratory hyperband pulse generator used in Russia.

In collaboration with D. Månsson at Uppsala University, Sweden.

Radan Waveform
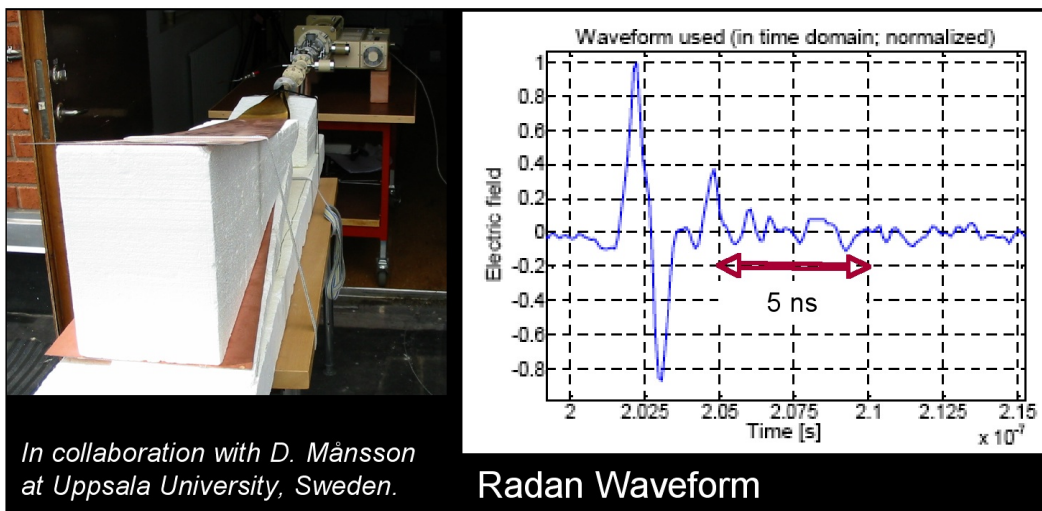
Figure 2-8. RADAN 303B hyperband generator used in Sweden.

AFRL has developed an extremely powerful IRA system that produces UWB pulses
  –E*R = 5.3 MV
  –pulse width ~100 ps

Figure 2-9. High intensity JOLT hyperband generator used in the United States.

Figure 2-10 illustrates a narrowband test facility in Sweden. This facility is designed to test military aircraft to intense EM fields, however, it is designed to operate only at spot frequencies.

Radar band	f (GHz)	Average Power(kW)	Max Power (MW)	Gain (dB)	PRF (pps)	Pulselength (µs)	E_{peak}@15m (kV/m)
L-band	1.300	49	25	ca 30	1000	5	30
S-band	2.857	20	20 (PCS: 140)	ca 30 (CA: 37)	1000	5 (PCS: 0.4)	30 (PCS: 80)
C-band	5.710	5	5	ca 30 (CA: 40)	1000	5	17
X-band	9.300	1	1	ca 30	1000	3.8	10
Ku-band	15.00	0.28	0.25	ca 30	2100	0.53	6
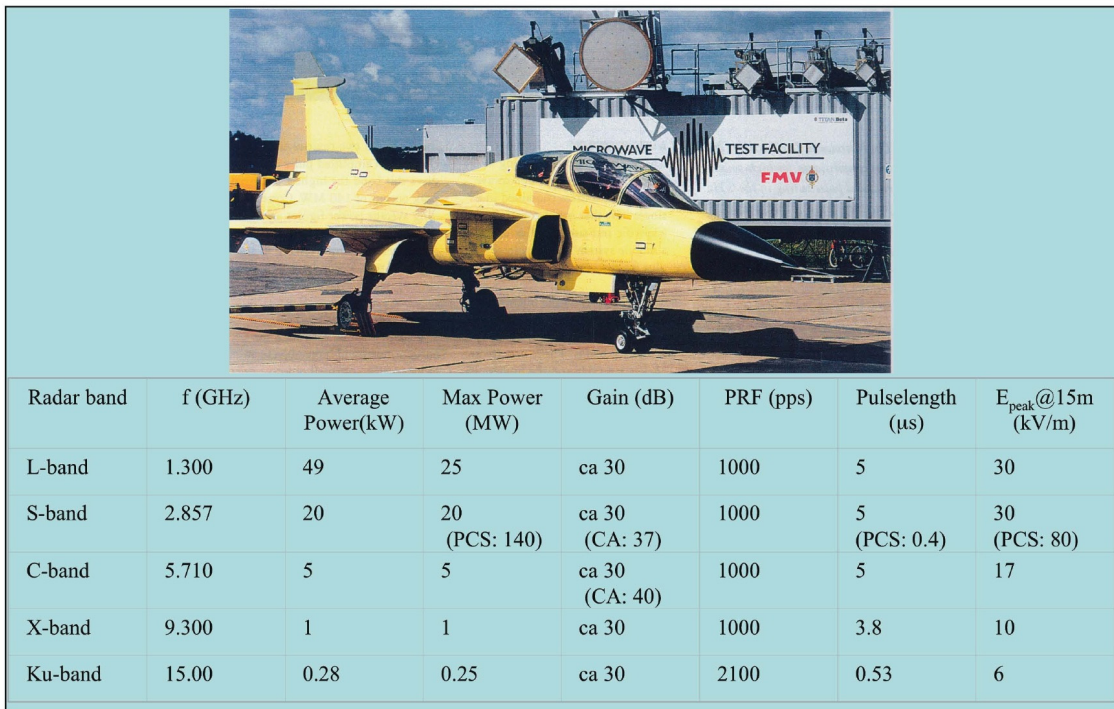
Figure 2-10. Microwave Test Facility (MTF) in Sweden

2.3 IEMI Conducted Threat Weapons

Unlike the situation for the radiated IEMI environments, there is no major advancement of the state of the art required to produce high levels of injected conducted environments. This is because all of the threat waveforms can be easily produced using available generators that are typically used in EMC testing or field investigations. Since there does not appear to be any advantage in moving to common-mode pulses with frequency content above 100 MHz, due to high-frequency propagation losses in existing telecom and power wiring networks, the main issues for the future involve the reduction of generator size and improvements in methods of injection. It is possible that higher frequency injection systems could be effective if they were injected in a differential mode. Some new work is examining this aspect.

2.3.1 Injected CW Environments

The main importance of CW environments as an intentional interference threat comes from the injection of low frequency currents into the grounding system of a facility. For this purpose, existing briefcase test generators are sufficient to create operational problems, if the facility and its internal equipment are not properly grounded. As an example, Figure 2-11 (left side) illustrates a briefcase generator which operates up to 12 V and 10 A for frequencies of 50, 200 and 400 Hz.

In order to establish low-frequency CW threats for the grounding system of a facility, frequencies between 1 Hz and 1 000 Hz should be considered. Voltage and current levels up to 100 volts and 100 amperes should also be considered.

Figure 2-11. Examples of briefcase generators for producing conducted environments: CW generator (left) and impulse generator (right) [15]

2.3.2 Injected Pulse Environments

In terms of pulse generators, many of the laboratory generators used to test compliance to EMC and to insulation safety standards generate sufficiently high peak pulse levels to provide a conducted threat to electronic equipment. In particular the "ITU" pulse defined in IEC 61000-4-5 provides a significant threat to computer equipment connected to

Ethernet cables at levels above those typically specified for normal EMC purposes. There are similar, but smaller pulsers designed for fieldwork as shown in Figure 2-11 (right side).

Based on the information available to date, it appears that existing IEC EMC test generators produce waveforms that when injected on external power or communications lines to a facility can create interference inside of the facility. For this reason pulse waveforms as defined in IEC 61000-4-4, IEC 61000-4-5 and IEC 61000-4-12 shall be considered as appropriate pulse threats. Peak voltage levels up to 10 kV should be considered as direct injected conducted IEMI threats.

2.3.3 Conducted Waveforms Produced by Radiated Fields

As described earlier, there are many types of radiated field threat environments that may illuminate equipment and systems directly. Of course nearly all equipment and systems are connected to data lines and to the power supply, so there are cables entering the equipment. As has been recognized in dealing with EMC aspects of electronic equipment, it is important to consider both the radiated fields that are incident on a system and the conducted environment that is coupled to the equipment cables locally. This is the purpose of the companion IEC 61000-4-3 (radiated tests) and IEC 61000-4-6 (conducted tests for the coupled radiated fields) for EMC applications.

For this report we make several assumptions that are appropriate given the nature of the threat and the location of equipment relative to the electromagnetic generators that may be used. In particular, the generators are expected to be outside of an installation or are located in an adjacent room in a large building. For the external generator case, it is clear that high-frequency radiated fields will induce currents and voltages on external power lines and communication lines. However, given that the frequencies of interest are greater than 100 MHz, it is unlikely that these induced voltages will be able to propagate well over the large distances necessary to reach individual equipment inside of the building. It has been established that for common-mode situations, frequencies below 1 MHz propagate well on low voltage power wiring in buildings; however, these disturbances are more easily created through direct injection into cables.

For the case of a generator in a nearby room with a dielectric wall, or for the case of the radiated fields entering a building through windows, the cables attached directly to equipment or systems are of the greatest interest. In this case, the cables are fairly short, and will allow higher levels of conducted environments to reach the equipment.

Studies have been performed for both CW and pulsed EM fields for the coupling to metallic cables. These studies have considered coupling to finite length lines at all possible angles of incidence. For the case of a 1 m straight cable, the maximum induced voltage is computed. From the calculations, the voltage into an assumed load of 100 Ω is plotted in Figure 2-12. Note that these results should not be applied outside of the frequency range shown.

Ordinarily one would expect the induced voltage per incident electric field (an effective coupling length) to be bounded by the physical length at low frequencies and the wavelength at high frequencies [20]. It is possible, however, to exceed these "limits" due to the consideration of coupling geometries that include grazing incidence angles.
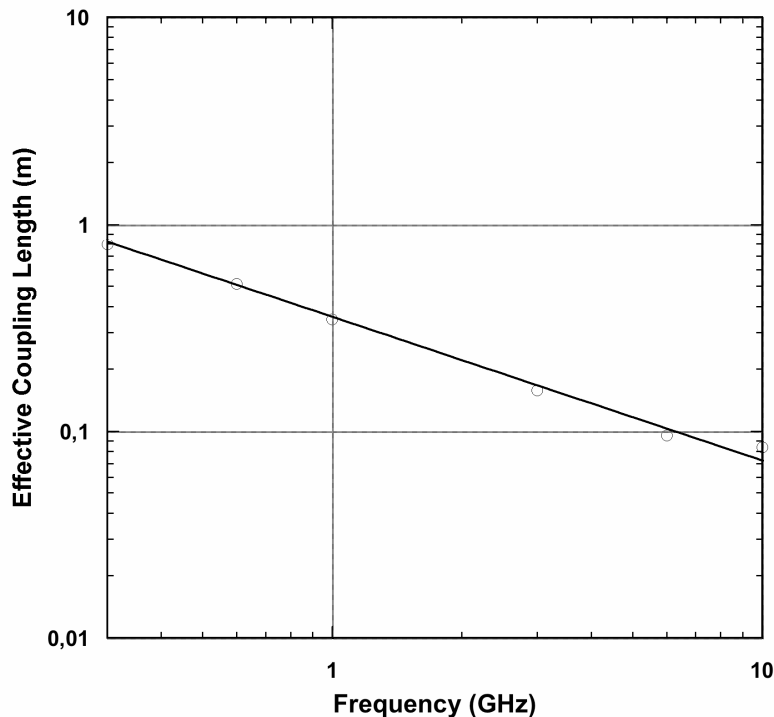
Figure 2-12. Effective coupling length for a 1 m metallic cable [34]

As indicated in Figure 2-12, an analytic approximation to the calculations is found to be:

$$\text{Effective coupling length (m)} \sim 0.36\, f^{-0.69} \text{ for } f \text{ in GHz}$$

For CW frequencies between 300 MHz and 10 GHz, this equation shall be applied to determine the maximum induced current / voltage on a cable entering a system or equipment. The applicable time waveform shall be the same as the incident electric field waveform for the radiated field. For monopolar pulsed time waveforms, one can still use the equation above by computing an approximate frequency from the pulsewidth: $f_a = 1/(3*pw)$, where pw is in units of nanoseconds and f_a is in units of GHz.

2.4   Summary of IEMI Threat Levels

For wideband radiated threat waveforms, buildings can be exposed externally to hyperband waveforms with peak field levels on the order of 10 kV/m. For briefcase devices, the same level of peak field in the hyperband to the mesoband range can be delivered and should be considered. The frequency range of these devices is from 100 MHz to 10 GHz.

For narrowband radiated threat waveforms, buildings can be exposed externally to radar type waveforms again in the range of 10 kV/m. Small internal narrowband generators have not been observed beyond the level of cellular phones or walkie-talkies at very close ranges (~100 V/m) or weapons made from microwave ovens (~1 kV/m).

For conducted IEMI threats, the induced conducted voltage from a 10-kV/m peak field (narrowband or wideband) is on the order of 10 kV. The typical injected capability is also on the order of 10 kV, although there are newer pulsers that may exceed this level.

Section 3
The EM Interaction Process

The modern civil infrastructure is very dependent on computers, which operate at logic levels of a few volts. So an intentional interference can occur at a few volts in critical circuits, causing logic upset. Of course the shape of the time waveform is also important, but the peak-coupled voltage provides the zeroeth-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 type of breakdown, which in turn provides a path for the power supply to insert much more energy than provided initially by the incident waveform. 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 (V/m), and waveform (rise time and pulse width). Concerning the waveform, 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 frequency-dependent transfer function from the external environment to the internal circuit, caused by aperture penetration and resonance, for example. Using time domain norms one can maximize the ratio of the circuit waveform to the environmental waveform, this having been done for both the infinity norm (peak voltage over peak field) and 2-norm (proportional to the square root of the ratio of squared integrals) [22], [23].

This approach shows the advantage of hypoband (narrowband) waveforms when 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 for the same levels of incident environment. 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 the purpose of coupling into representative electronic systems. A recent paper gives an experimental demonstration of the above results [24]. It is important to note, however, that resonances are not always easily found, and for this reason the hyperband waveforms are likely to be more consistent in producing an upset effect in commercial equipment, which for modern electronics may not be automatically recoverable (without human intervention).

Next we consider the frequencies of general interest for Intentional EMI. Radiating antenna systems have a gain, which increases with frequency, allowing higher fields on a 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 Intentional EMI

because typical dimensions of things people build are resonant in this region (the rule of the hand, or Baum's Law [23]). Published data supports the view that the range of roughly 200 MHz to 5 GHz is quite important [25], [26], even demonstrating, for unprotected (basically open, unshielded) systems, functional upset from radiated fields as low as 30 V/m.

Section 4
Susceptibility Levels of Electronic Equipment and Systems

4.1   Susceptibility Testing

Over the past ten 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 (including networks) since they are in wide usage in many different industries. In addition, recent testing has included cash machines, industrial control equipment, power supplies, Ethernet components, WIFI networks, automobiles, GPS electronics, cellular phones, PDAs and different types of sensors. We will only summarize here a small representative portion of the data acquired and published.

Modern computers and other types of equipment using microprocessors appear to be vulnerable to malfunction from radiated narrowband fields above 30 V/m [26], although newer high-speed PCs have higher susceptibility levels (~300 V/m). 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 [27] as indicated in Figure 4-1.

> Fixed frequencies between 1.3 - 15 GHz were tested
>
> Most prominent effects at the lower test frequencies, also when the car was not operating. Types of damage observed included: engine control units, relays, speedometer, revolution counter, burglar alarm, and a video camera.
>
> Upset (engine stop):   500 V/m
>
> Permanent damage: 15 kV/m at 1.3 GHz
> 24 kV/m at 2.86 GHz
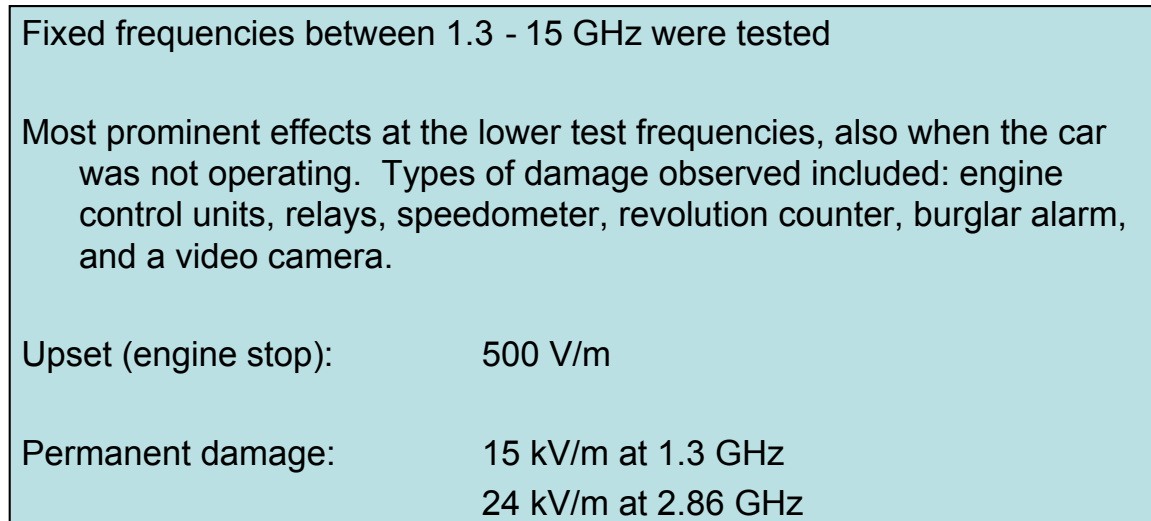
Figure 4-1. Susceptibility of automobiles to narrowband radiated fields, by Bäckström.

Until recently there have not been many experimental results published that have covered radiated frequencies below 1 GHz, so it was not clear if this trend continues to much lower frequencies. Figure 4-2 indicates some recent test data for personal computers in a reverberation chamber from Hoad in the UK. The newer PCs have failures as low as 300 V/m at 400 MHz, although the shape of the frequency curve is flattening out. Clearly field levels below 1 GHz are still creating severe upsets at lower frequencies for PCs.
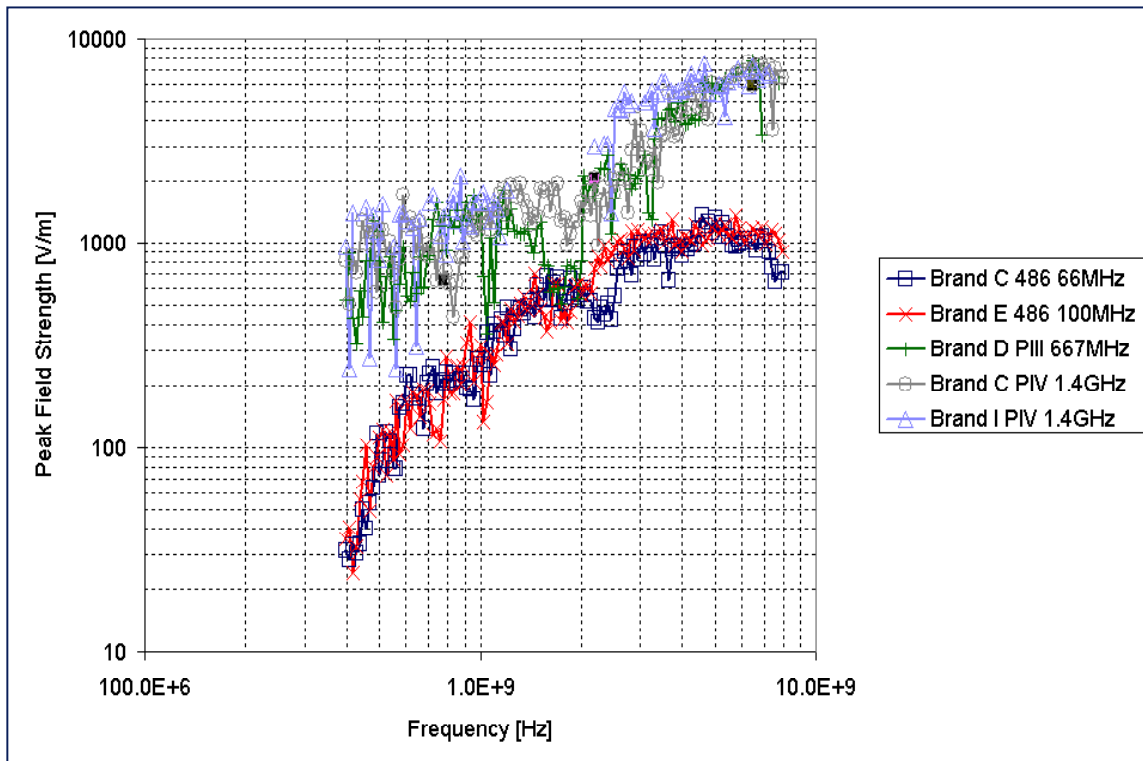
Figure 4-2. PC susceptibility trends for exposure to narrowband fields as measured by Hoad.

There is less experience with wideband, radiated-field testing; however, some recent data have been collected in Russia and Germany (Figures 4-3 and 4-4). Note that susceptibility levels for standalone cash machines of ~2 kV/m occur for pulses with pulse widths on the order of 200 ps (hyperband waveform).

Upset levels

ECM type	SAMSUNG ER-4615RF	SAMSUNG ER-250RF
Critical level of UWB field, kV/m	2.3–2.5	2.2–2.4

Level of damage

Level of UWB field, kV/m	2.5	3.1	3.9	4.4	4.8	5.1
Result	Upset	Upset	Upset	Upset	Upset	Damage

Source: Dr. Yuri Parfenov, IHED, Russia, Presented at EUROEM 2004

Figure 4-3. Upset and damage levels for a hyperband, radiated field with a pulse width of less than 200 ps.

In Figure 4-4 Nitsch and his colleagues used five different pulse shapes to illuminate a computer motherboard, with a clear trend of effects occurring at a lower peak field level for faster pulses (more high frequency content). The data also shows generally a low correlation with repetition rate, implying that the effects noted do not require a large number of pulses to be effective.
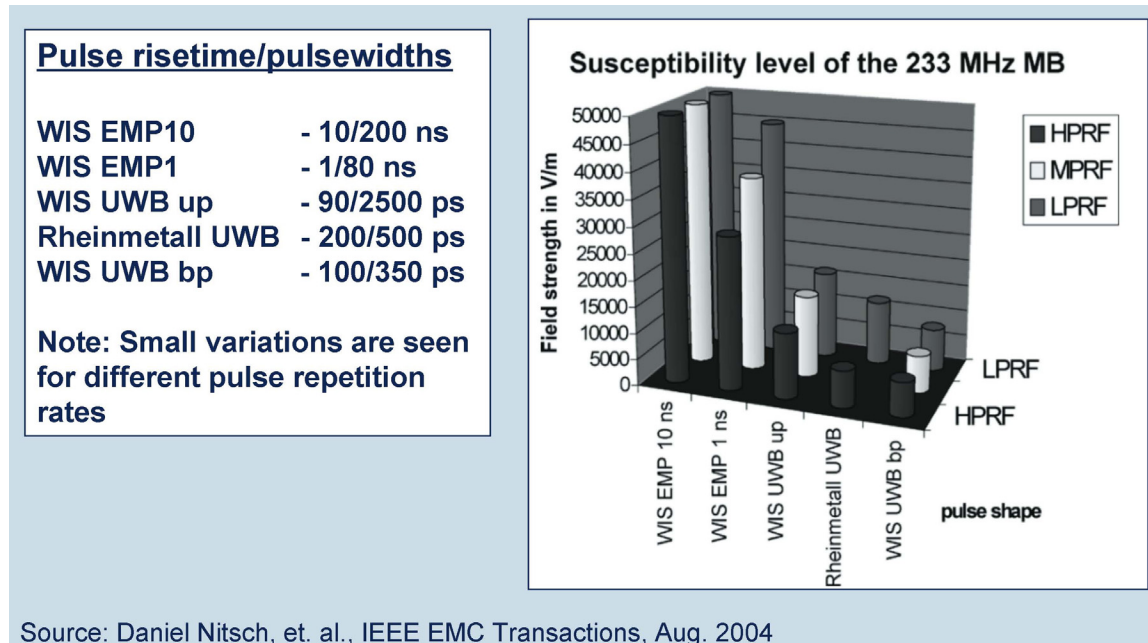
Figure 4-4. Susceptibility levels for a computer motherboard for EM pulse variations.

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 (due to time and expense aspects), and therefore most of the effects noted during testing will actually occur at lower field levels when an optimum coupling geometry is considered. It is well known that above 1 GHz the orientation of the incident field to the test object is very important.

For conducted IEMI 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 volts have been known to cause problems [21]. For slow pulsed waveforms, it appears that pulse widths on the order of 100 microseconds can create damage to equipment power supplies and to interface circuit boards (see Figure 4-5) at levels as low as 500 volts, but more typically at levels of 2 – 4 kV [20].
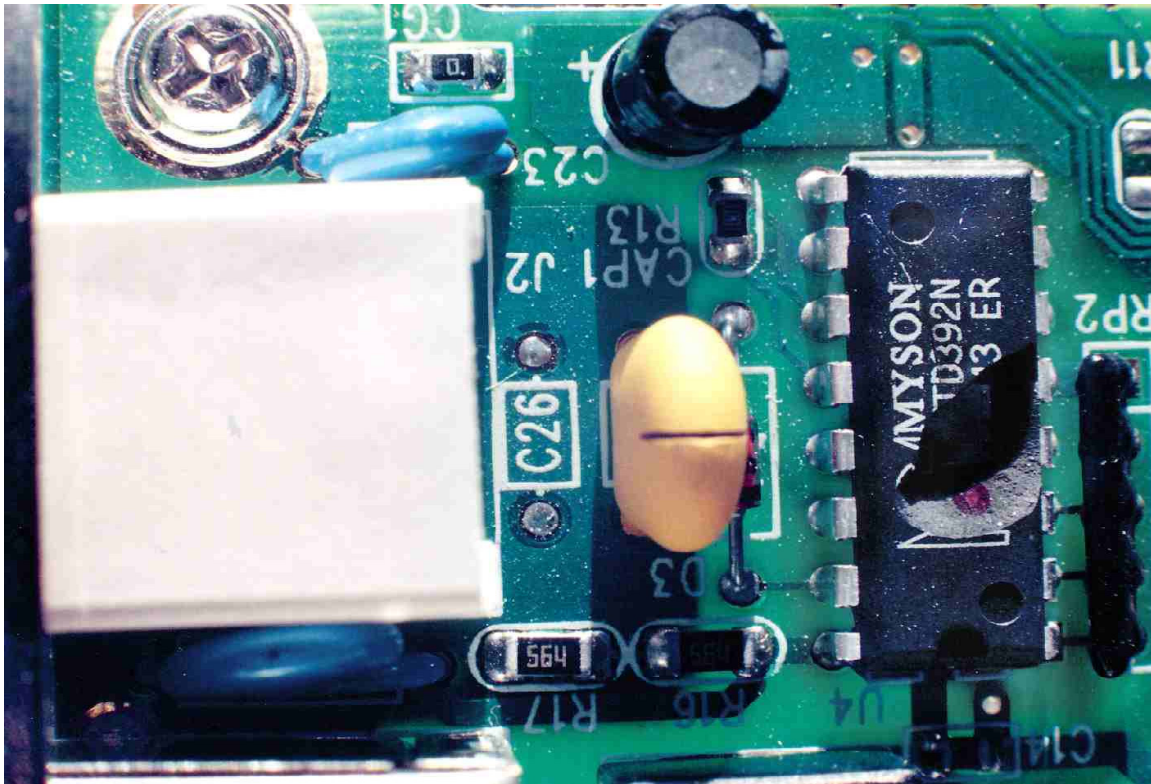
Figure 4-5. Damage produced on an Ethernet 10 Base2 computer interface board due to the cable injection of a 500-volt telecom pulse as defined in IEC 61000-4-5.

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 immunity requirement above 10 V/m (for frequencies above 80 MHz). This is also the current recommended immunity level for medical devices that are needed to support life [28], although there are discussions to raise this level to 30 V/m due to problems with some medical equipment. Higher levels are not recommended for home or factory applications because of the expense of providing the increased protection. For narrowband voltages induced on cables connected to equipment, 10 V is the upper IEC EMC test level required in most cases [29]. The frequencies of application are below 80 MHz for this test.

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 pulse widths as long as 700 microseconds.

There is one area in which a wideband threat requires higher levels to be considered – the high altitude electromagnetic 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 [30]. There are corresponding wideband-conducted waveforms that are created during the HEMP coupling process. These induced voltages may reach levels of hundreds of kilovolts on external (to the building) power lines [31]. Of course, we cannot expect that commercial equipment connected to these lines are immune to HEMP threats, and therefore it is clear that the Intentional EMI 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.

4.2   Summary of IEMI Susceptibility Levels

For narrowband, radiated fields, it appears that modern electronic equipment will have serious upsets at 0.5 kV/m for a frequency of 1 GHz. At 400 MHz upsets occur at levels as low as 0.3 kV/m. Above 1 GHz, higher levels are required.

For wideband, radiated fields, the onset of upsets occurs at ~2 kV/m. Damage occurs at levels of only a factor of 2-3 higher (~5 kV/m).

For conducted, wideband voltages, fast pulses with 5/50 ns pulse characteristics (rise time/pulse width), show serious malfunctions at peak levels of ~2 kV and damage at ~4 kV. There is not much data for faster pulse injection waveforms at this time, so it is possible that the susceptibility levels could be even lower for faster pulses. Slower pulses (10/700 microseconds) have shown damage as low as 0.5 kV with rare upsets.

For conducted narrowband voltages, only limited testing has been performed, but severe upsets have occurred when the grounding system of buildings were injected at levels of 100 V for frequencies below 100 Hz.

Section 5
Electric Power System IEMI Impacts

5.1 Introduction

In this section we consider the likely impacts of IEMI on various parts of the electric power system. It is clear that there are many similarities between the peak field levels that can be produced by EM weapons at close ranges and by E1 HEMP. The IEMI waveforms tend to have higher frequency content that E1 HEMP, so they are likely to create equipment and system failures at lower peak levels that E1 HEMP.

The big difference between the IEMI threat and E1 HEMP is the fact that IEMI is a local threat that can illuminate a small building or part of a large building to intense EM fields, while E1 HEMP can illuminate a continent with nearly constant fields. Because of the variation of the fields with distance (typically 1/r for the electric field) and the non-planar aspect of the IEMI wavefront, the IEMI fields can only couple efficiently to less than 10 meters of cables, which reduces its threat to very long power lines (100s of meters or more).

It should be noted that IEMI has some advantages over the E1 HEMP in that the EM weapons may be carried inside of facilities (briefcase weapons) and therefore any external shielding of a building will be ineffective. In addition, there are conducted IEMI threats that will allow the direct injection of high-level voltages into power or communications circuits, which cannot happen with E1 HEMP. E1 HEMP must couple to external lines to generate high levels of conducted voltages.

In terms of susceptibilities, most of the equipment tested to E1 HEMP transients through direct injection will be vulnerable to IEMI at even lower peak levels. Studies have shown that a faster rise time is more effective in creating equipment malfunctions.

Metatech has performed a large number of test and analysis studies dealing with portions of the U.S. power grid and their vulnerability to high-level EM fields and voltages:
1. High voltage substation controls and communications
2. Power generation facilities
3. Power control centers
4. Distribution transformers
5. Distribution line insulators

Of these 5 portions of the power system, items 1-3 are of biggest concern due to IEMI, although we will briefly discuss item 4 in this report. The ability to induce 100-300 kV of voltage to an elevated power line using an EM weapon is highly unlikely due to the inefficient coupling process for IEMI and long lines and the difficulty of generating over 100 kV/m at the height of a power line.

It has been determined that there are two main ways for IEMI to reach the electronic equipment that control the operation of the grid. One is through the direct illumination of the equipment and the other is through the coupling of the IEMI fields to cables and wiring (over the last 10 meters), producing conducted transients that can exceed the withstand capability of the connected electronics. Direct injection of an IEMI waveform is also a threat to power control centers in buildings if access to the entry areas for power and communications cables is not limited.

5.2   IEMI Coupling to Lines

As described in Section 2 of this report, at frequencies near 300 MHz, the maximum coupling efficiency from electric field to induced voltage is approximately 1.0 (meter). This means that an incident narrowband field of 10 kV/m at 300 MHz will induce 10 kV on a cable. A hyperband waveform with a pulse width of 1 ns would also have the same effectiveness in coupling (1.0) and again a 10 kV/m electric field would induce a peak voltage of 10 kV.

Since the coupling process is only effective over up to 10 meters of cable length, it is likely that the conducted threat is most important for the coupling to cables inside of a substation or power generator control building. It is also a threat to the sensors mounted in the high voltage yard. It is unlikely that the IEMI coupling to the control cables outside will lead to an important vulnerability to the electronics inside the control building.

The same situation is true for power control, centers as the external cables leading to the building are unlikely to propagate very high frequency IEMI transients in a common-mode geometry.

For distribution transformer winding insulation or power line insulators, the BIL ratings are typically 100 kV or higher, and the induced IEMI voltage levels of 10 kV at frequencies on the order of 1 GHz are unlikely to cause any problems.

5.3   Susceptibility of Power System Equipment

As noted above, calculations indicate that control/sensor/communication wires can have coupled common-mode IEMI peak voltages of up to 10 kV. Normally such lines transmit signals of a few volts, and so IEMI pulses could certainly be disruptive. There are many electronic devices that are located in a power substation, central control facility, or generator station that would also have attached cables. These include:
1. Computers, of various kinds.
2. PLCs – programmable logic controllers – basically computers, but specialized with I/O ports, such as A/D and D/A converters (A=analog, D=digital) so that they can be process controllers.
3. Communication devices – modems, routers, switches, etc.
4. Solid-state safety relays (increasingly used as replacements for the older electromechanical power relays).

5. SCADA systems (Supervisory Control And Data Acquisition) – this involves communication of data and controls between unmanned substations and manned control centers.

Such devices can be vulnerable to either upset or damage from IEMI pulses coming in on the connected wiring. (There is always the possibility that some functional upsets might actually lead to damage, in which the system's own energy is turned against itself, such as for devices controlling moving structures or burning of fuels, for example.)

There has recently been some susceptibility testing of samples of such devices, especially using pulse injection testing. There have been many tests of common systems, such as PC computers, and their associated devices. General pulse width variation is as expected, with the wider pulses more easily producing damage. Often there is much variation in results, depending on the device model and manufacturer. Typically damage has been found at levels of several thousand volts. Some damage has been at levels less than 1000 volts, and sometimes no damage is found up to the highest typical pulse levels (about 5 kV is typical for most test equipment). Typical upset levels are generally lower than typical damage levels, but often there is not a huge difference for a given electronic device. Susceptibility is usually found by slowly increasing the pulse level on successive pulses, until an effect is found (upset or damage), and sometimes damage occurs without any upset being noted at lower pulse levels. The following information summarizes an extensive set of testing performed by Metatech Corporation, mainly for E1 HEMP, but the results are also applicable to IEMI conducted transients.

Pulse testing of representative substation equipment was done for the EMP Commission in a relatively rapid test program. NERC (North American Electric Reliability Council) provided the EMP Commission with a priority list of power system equipment that should be tested. In these tests, the DUT (device under test) was pulsed with an E1 HEMP (and IEMI) relatable waveform into a single port for each shot, with the device running during the test. After each shot there was a quick check for upset or damage. The pulser drive level was gradually increased in steps, to try to resolve the level of failure, if any occurred. A full set of tests was done using a standard fast pulse waveform (5 ns rise, 50 ns wide), and there were also some tests using wider pulses – 50 microseconds wide. Here we will show a few results. Pulsing was also done for both polarities of pulses. Also, when there were multiple ports of the same type, each individual port was tested. We should never assume that polarity does not matter, or that all ports of the same type will behave in the same manner.

In the past substation power control used big electromechanical relays, and there are many such devices still in use. Figure 5-1 shows an overcurrent relay, and Figure 5-2 shows a distance relay. Pulse testing was done on both devices, up to the 8 kV level, and no failures were noted (although there was some minor arcing).

Newer relays are now electronic (solid state), such as shown in Figure 5-3, with an inside view in Figure 5-4. This device is well built, with protection on most of the ports. This shows up in the system not suffering any damage up to the highest pulse level available,

as indicated in the chart of Table 5-1. The table also includes the results for SCADA units (Figure 5-5) that are made by the same company, and also appear to have good protection against fast pulses. The SEL 311L relay did have upset, however, and it was repeatable and affected several aspects of the unit besides just the port that was pulsed. This was at a pulse level of 3.2 kV going into a serial port. The relay had to be turned off and then back on to get it to work properly again.

Table 5-2 shows results for wider pulses for some of the ports. The protection worked reasonably well for this wide pulse too, but in this case we did get damage, on three ports. The IRIG ports for both the SEL 331L and SEL 2032 were broken at a level of a few hundred volts (600 volts open circuit). The Ethernet connection on the SCADA unit was also damaged at a low level (1.2 kV open circuit). In this case we heard a "bang" associated with the damage, and further testing showed that a resistor on the circuit board was blown up.

In Figure 5-6 we show a sample oscilloscope recording from a shot on the SEL 311L relay. During pulse testing there may be thousands of shots, and the current and voltage signals are recorded for each. This helps look for unusual behavior (often the occurrence of arcing can be seen in the waveforms), but we it also is useful if there happens to be damage – it helps characterize the parameters of damage (and once damaged, the sample unit cannot be tested again, at least not on the same port, so we cannot go back and try to make measurements afterwards). In this case the pulse was negative. Vulnerability should be checked with both positive and negative pulse drive – sometimes effects will occur at a lower level for one polarity than for the other. These results for a protected port show common results. The width of the current waveform is similar to that of the incident pulse; the voltage is much shorter. This is because the protection devices (MOVs – metal oxide varistors) suddenly become very conductive when the voltage gets too high, and shorts out the pulse. This MOV turn-on is indicated by the voltage suddenly dropping to a low value (as shown by the violet arrow).

The next results are for two types of PLCs (programmable logic controllers). They are used as the "brains" of automated controls of processes. These devices do simple computing, using many I/O (input/output) ports of various types. There are analog-to-digital and digital-to-analog converters. These are for sensors and controls that work on continuous range of voltages or currents. There are also binary I/O ports – with just two states, either on or off. These PLCs generally might need to occasionally send status information and receive instructions from elsewhere (and they need to be programmed), so they also have communications ports, either serial or Ethernet (or both).

These devices are much cheaper than the SEL equipment just discussed, and it shows in the hardiness of the units. The ports are not well protected (the cases are plastic, so there is no Faraday cage around the devices).

Figure 5-7 shows the Fisher ROC809 unit (showing how it is configurable – one of the optional cards is pulled out). It also has a separate power supply, not shown. Table 5-3 gives the fast pulse results. Two types of ports did not have effects, but the rest had

either upset or damage (or both). The effects ranged from some that were localized to the port that was pulsed, up to effects occurring on other parts of the device. Damage was as low as 1 kV for the analog out port. The analog out card damage was subtle at first – its output was more and more inaccurate as the pulse level was increased, until finally (at 1 kV) the level was too high, and it no longer would work.

The serial port results were interesting. The ROC809 has a plastic case, and no "ground". This can be challenging when trying to do common-mode pulse tests. For the serial port tests the power supply ground was used as the ground. For the higher level pulses a clicking noise was heard in the power supply. Furthermore, a completely separate card ended up being damaged – the analog input (ADC) card. It was suspected that this was due to there not being a clean return path of the current pulse sent into the serial port – finding a path back to the ground in the power supply might have involved some of the current going through the ADC card.

The Ethernet port was upset at 3 kV, and damaged at 4.5 kV. In this case negative pulses had these effects, but positive pulses did not. Note that Ethernet cables can be fairly long, and so will have large IEMI pickup inside a building.

The Allen-Bradley MicroLogix 1000 PLC, shown in Figure 5-8, is a similar unit. It is not configurable, as the ROC809 is, but it does have similar ports: analog input and output, binary input and output, and a serial port for programming and communications. For Ethernet communications there is a separate unit (shown on the left) that connects to the serial port.

The MicroLogix 1000 fast pulse results, shown in Table 5-4, also have a similar range of results, with ports that show: no effects, upsets, and damage. For breadth-of-effect there is the full range of only affecting only the pulsed port, to having effects on other parts of the device. As for many cases in these tests, upset generally required re-booting the device (power off/on cycle). For some upsets the program had to be re-inserted into the PLC to get it to work again. For damage to the analog input, it was noticed that some bits of the ADC were permanently stuck, so that accuracy was compromised. For this unit we also damaged the Ethernet port – at the 7 kV level.

Some slow pulse testing was also done, with the results shown in Table 5-5. The analog out (DAC) was damaged at a low pulse level, 600 volts. This killed all of the analog out ports – as they all share the same converter circuit.

A computer was also tested. This was a standard PC, matched with a simple Ethernet switch. Table 5-6 gives the results for the fast pulse. The Ethernet switch was upset (stopped working) at the 2.0 – 2.5 kV level. The full 8-port unit stopped communicating, although the pulse was sent into only one port. A power reset restored the device. On the computer two different network circuits were tried – one on the motherboard and the other an expansion card. These upset at the 4-5 – 5.0 kV level, and worked again after a re-boot. The serial port on the computer died at a very low level – 750 volts. This occurred for both the built-in serial port and an expansion card serial port. The phone

modem had no failure up to the 8 kV maximum, and the AC power plugs also had no problems.
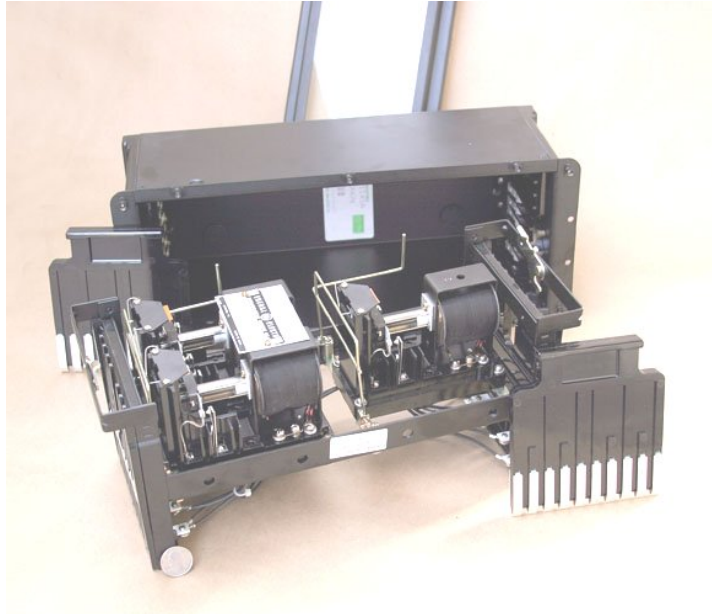

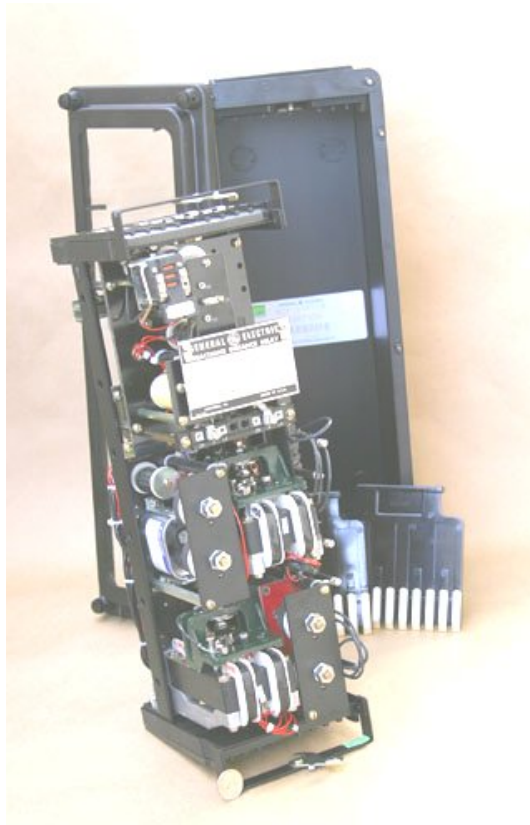Figure 5-1. GE-PJC electromechanical overcurrent relay.

Figure 5-2. GE-GCX electromechanical distance relay.

Figure 5-3. Modern relay unit, the SEL-311L (front view on top, back view on the bottom).
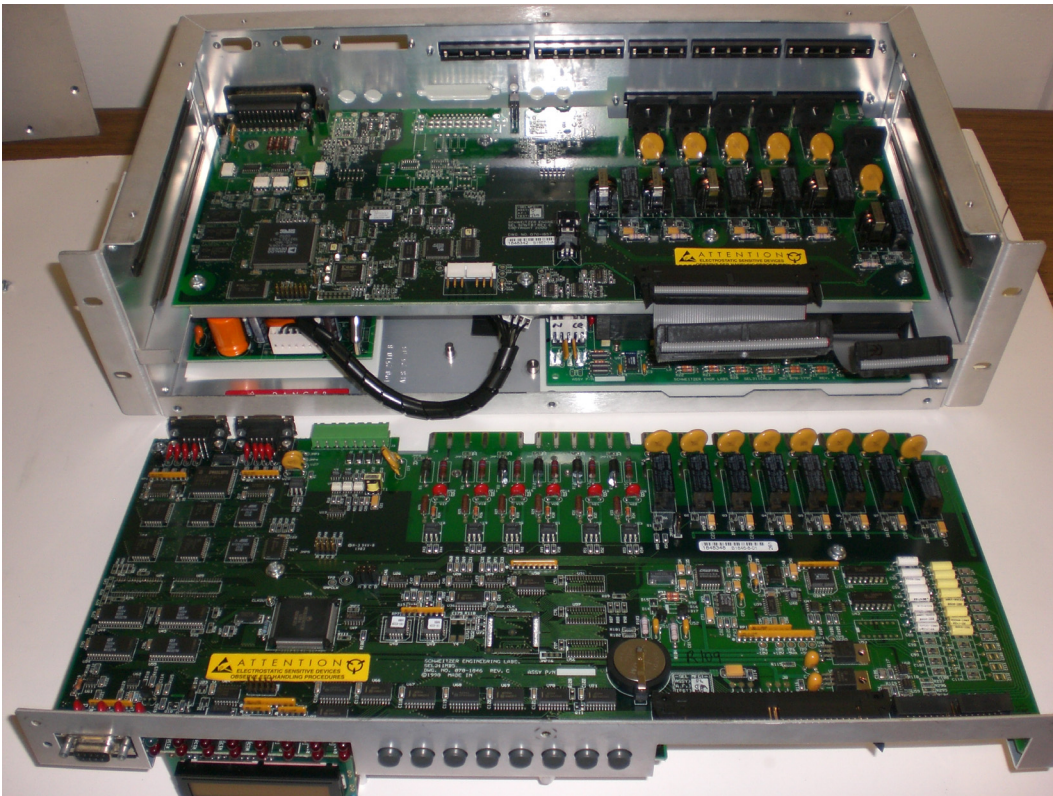

Figure 5-4. Inside the SEL-311L electronic relay unit.

Figure 5-5. Modern SCADA unit, the SEL-2032 (front view on top, back view on the bottom).

Table 5-1. Fast pulse results for the Schweitzer Engineering Laboratories relay (SEL-311L) and SCADA (SEL-2032) units. The entries show the test level – for example, 5.5/3.2 means the pulser open-circuit level was 5.5 kV, but the peak voltage was 3.2 kV for the shot (due to loading). The columns show: "No Effect" means no failures up to the level shown (the pulser limit), "Upset" means an upset was found, and "Damage" indicates permanent physical damage and failure of the system. The cell color is used to indicate the breadth of the effect – just the pulsed port (yellow), other ports of the same type also affected (orange), or also effects on other system functions (red).

Schweitzer Electronic Relays					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
SEL 311L Relay	Discrete In	Differential	8.0/7.9	-	-
	Discrete Out	Differential	8.0/4.0	-	-
	Analog In, V	Differential	8.0/5.8	-	-
	Analog In, I	Differential	8.0/5.5	-	-
	Serial Port	Differential	-	5.5/3.2	-
	IRIG In	Differential	8.0/4.3	-	-
	Power In	Differential	8.0/4.7	-	-
SEL 2032 Comm. Unit	Discrete In	Differential	8.0/8.0	-	-
	Discrete Out	Differential	8.0/4.8	-	-
	Serial Port	Differential	8.0/4.1	-	-
	IRIG Out	Differential	8.0/5.0	-	-
	Ethernet	Common	8.0/4.5	-	-
		Differential	8.0/4.1	-	-
	Power In	Differential	8.0/4.9	-	-
SEL 9310 Power Supply	Power Out	Differential	8.0/4.0	-	-
	AC In	Differential	8.0/4.8	-	-
SEL 9502 Arc Supp.	Contact	Differential	8.0/4.2	-	-
	I Sensor	Differential	8.0/5.0	-	-
Breadth of Effect:	Pulsed Port		Associated Ports		System Wide

Table 5-2. Slow pulse test results for the SEL units.

| Schweitzer Electronic Relays, CWG Pulse					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
SEL 311L Relay	Discrete In	Differential	4.3/4.4	-	-
	Discrete Out	Differential	4.3/4.1	-	-
	Analog In, V	Differential	4.3/4.7	-	-
	Analog In, I	Differential	4.3/0.2	-	-
	Serial Port	Differential	4.3/0.1	-	-
	IRIG In	Differential	-	-	0.6/0.14
	Power In	Differential	4.3/1.0	-	-
SEL 2032 Comm. Unit	Discrete In	Differential	4.3/4.4	-	-
	Discrete Out	Differential	4.3/0.7	-	-
	Serial Port	Differential	4.3/0.1	-	-
	IRIG Out	Common	4.3/0.01	-	-
		Differential	-	-	0.6/0.2
	Ethernet	Common	-	-	1.2/0.1
SEL 9310 Power Supply	Power Out	Differential	4.3/0.4	-	-
Breadth of Effect:	Pulsed Port		Associated Ports		System Wide
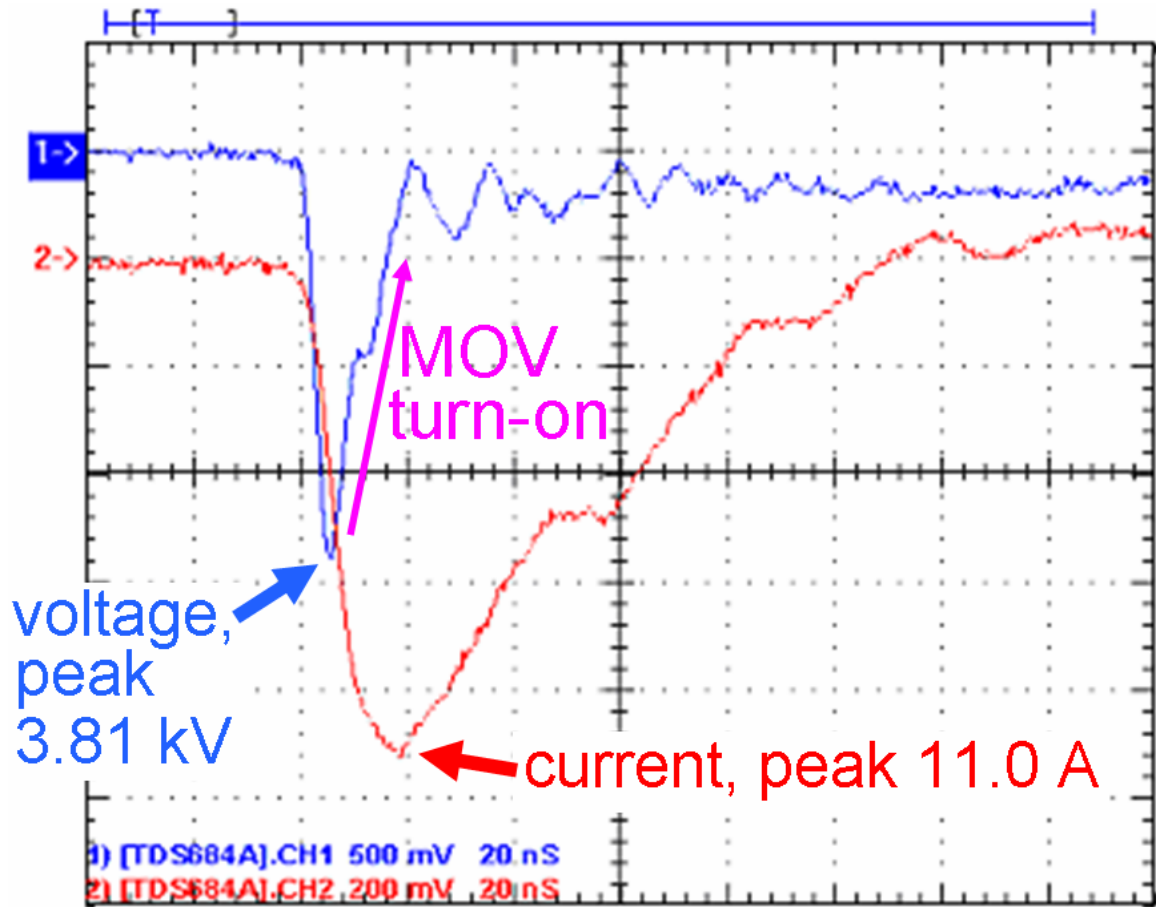
Figure 5-6. Sample recording of the voltage (blue) and current (red) at protected port of the SEL 311L. (The horizontal axis is 20 ns per major division.)
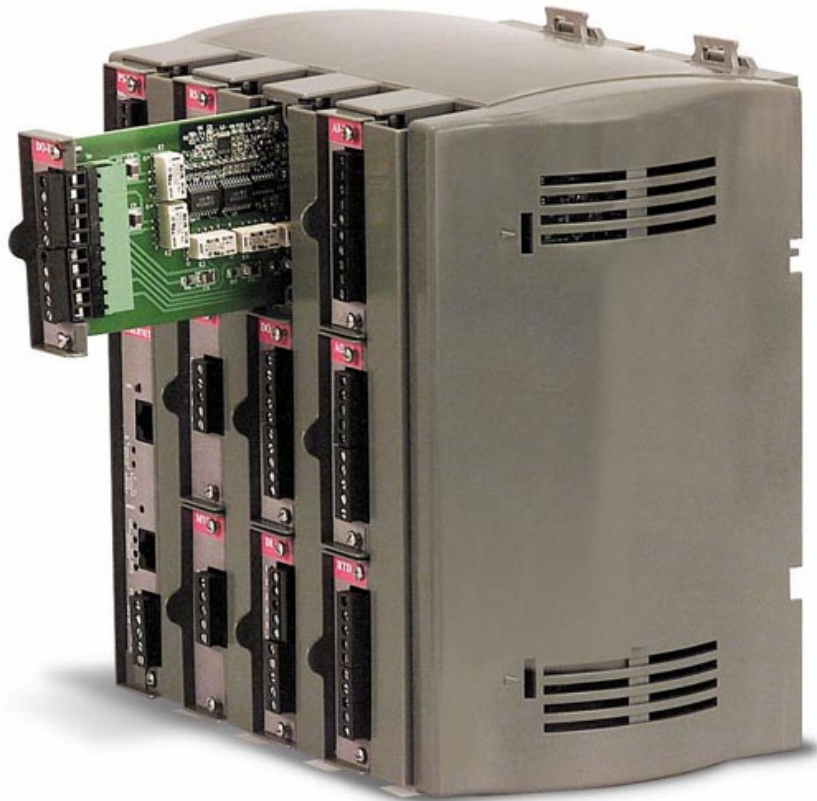
Figure 5-7. The Fisher ROC809 Remote Operations Controller. This is a PLC, such as might be used for remote controlling of a pipeline. It has a computer, and then may be configured with various I/O units: analog, binary, and communications.

Table 5-3. Fast pulse results for the Fisher ROC809 unit.

Fisher ROC809 Remote Operations Controller					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
ROC809	Discrete In	Differential	-	3.0/3.4	-
	Discrete Out	Differential	-	8.0/5.2	
	Analog In	Differential	8.0/4.5	-	-
	Analog Out	Differential	-	-	1.0/0.6
	Serial Port	Common	-	-	2.5/2.1
	Ethernet	Common	-	3.0/3.0	4.5/4.7
Power Supply	AC In	Differential	8.0/5.1	-	-
Breadth of Effect:		Pulsed Port		Associated Ports	System Wide

Figure 5-8. The Allen-Bradley MicroLogix 1000 PLC (on the right). This has analog and binary I/O ports. Its communications are handled by the 1761-NET-ENI unit shown on the left.

Table 5-4. Fast pulse results for the Allen-Bradley MicroLogix 1000 PLC.

Allen-Bradley MicroLogix 1000 PLC					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
MicroLogix 1000 PLC	Discrete In AC	Differential	8.0/7.1	-	-
	Discrete In DC	Differential	-	8.0/6.2	-
		Common	-	4.5/1.6	-
	Discrete Out	Differential	8.0/6.1	-	-
	Analog In, V	Differential	-	-	3.5/3.3
	Analog In, I	Differential	-	2.5/1.7	-
	Analog Out, V	Differential	4.5/2.0	-	-
	Serial Port	Common	-	7.0/5.9	-
	AC power	Differential	8.0/5.0	-	-
ENI	Ethernet	Common	-	4.5/3.9	2*3.5/4.0
Breadth of Effect:	Pulsed Port		Associated Ports		System Wide

Table 5-5. Slow pulse results for a few ports of the Allen-Bradley MicroLogix 1000 PLC.

Allen-Bradley MicroLogix 1000 PLC, CWG Pulse					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
MicroLogix 1000 PLC	Discrete In AC	Differential	-	-	4.0/4.0
	Analog Out, V	Differential	-	-	0.6/0.6
Breadth of Effect:		Pulsed Port		Associated Ports	System Wide

Table 5-6. Fast pulse results for a typical PC and network switch.

Compaq PC					
DUT		Drive	Voltage Level: Charge/Load, kV		
Unit	Port		No Effect	Upset	Damage
Network Switch	Downlinks	Common	-	2.5/2.3	-
	Uplink	Common	-	2.0/2.0	-
	AC Power	Differential	8.0/6.8	-	-
PC	LAN PC Card	Common	-	4.5/3.8	-
	Onboard LAN	Common	-	5.0/2.4	-
	Modem	Common	8.0/4.3	-	-
	Serial Port	Common	-	-	0.75/0.5
	AC power	Differential	8.0/5.1	-	-
Breadth of Effect:		Pulsed Port		Associated Ports	System Wide

Given the vulnerability levels for such equipment, and the levels of coupled signal that IEMI can produce, it can be seen that the "brains" and communication systems of any modern power facility could be vulnerable to IEMI. This applies to power substations, control centers, and power generation facilities. However, there can be a large range of variation, which depends significantly on the particular layout of each facility (which determines the level of IEMI field that penetrates to the location of the equipment and its cables).

5.4   High Voltage Substation Controls and Communications

It is important to evaluate the IEMI threat to high voltage power networks throughout the world, and to develop protection methods to deal with the threat. High voltage power substations are especially at risk as they are usually operating without on-site personnel.

The biggest IEMI concern within a high voltage substation is not the high voltage transmission lines and transformers, but rather the low voltage sensor and control lines that extend from the transformer yard to the relays and other control electronics in the control building. While these cables are in conduits aboveground (shown in Figure 5-9)

these conduits are not effective electromagnetic shields at high frequencies. Currents and voltages coupled to an external conduit are likely to leak into the internal cables at the joints and at connection points to sensors and the controls. For IEMI we are more concerned with the cables inside of the control building, although the last few meters of trenway could be a factor.
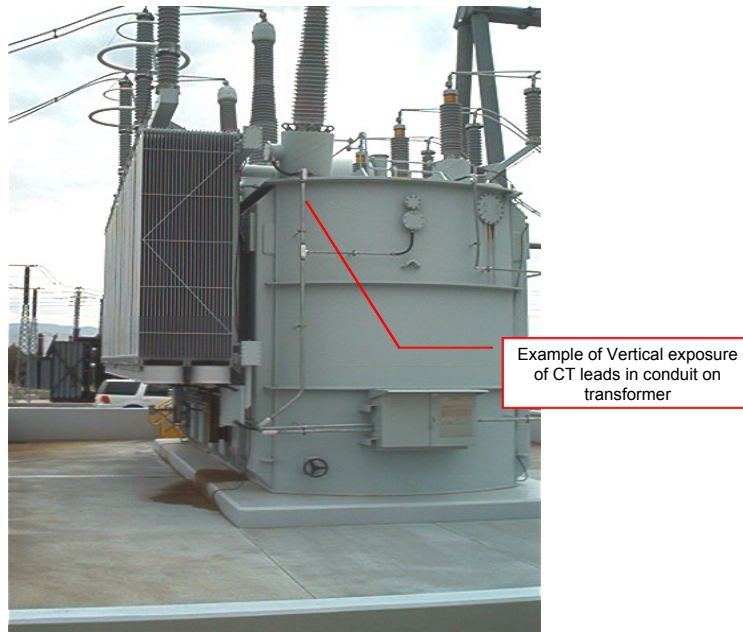

Figure 5-9. Exposure of cable conduits on transformers

In Figures 5-10 and 5-11 the sensor and control cables are seen to run slightly below ground in trenways that are "buried" in the gravel in the transformer yard. The length of these cables and the poor electromagnetic shielding of the trenway and the gravel at high frequencies will allow the penetration and coupling of high frequency fields to the cables and the subsequent propagation of these currents and voltages to the control building.
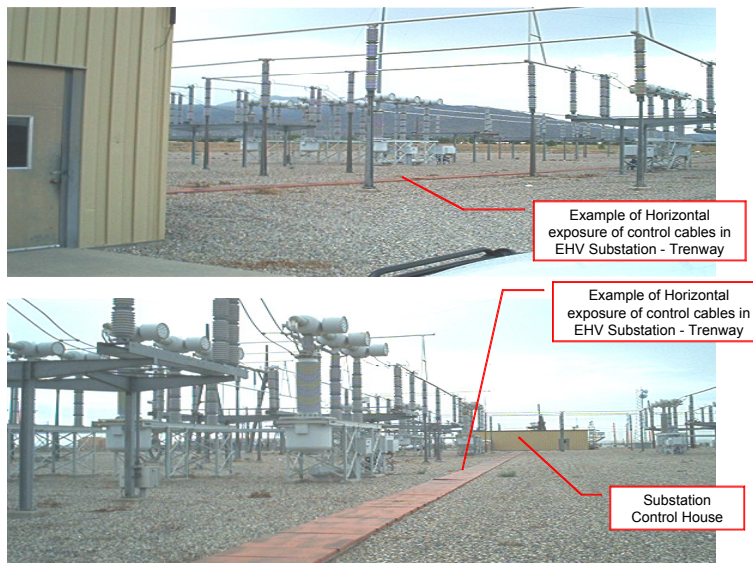

Figure 5-10. Long runs of "buried" cables in low conductivity gravel.

Example of Horizontal exposure of control cables in EHV Substation - Trenway
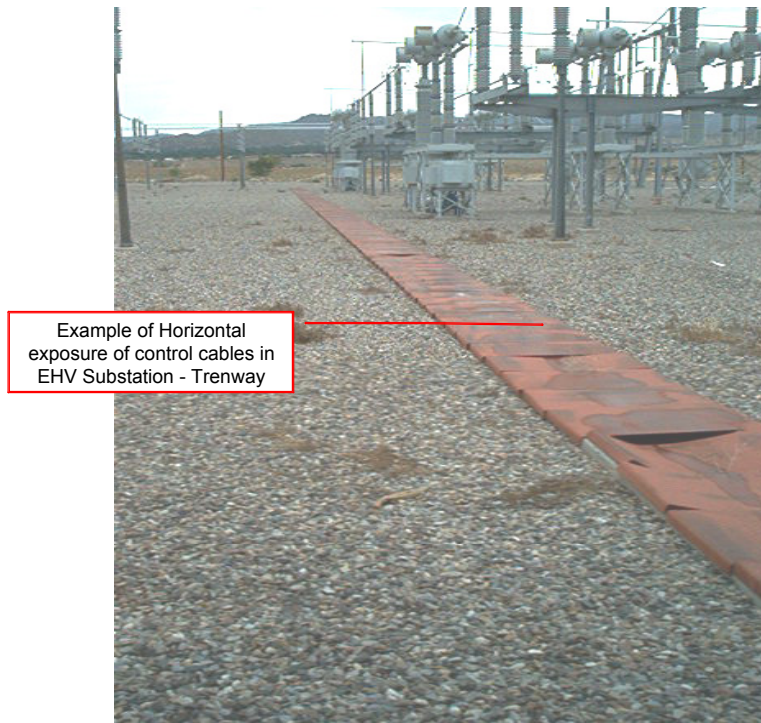
Figure 5-11. Second view of cable trenway

In Figure 5-12 the cables are buried at a shallow depth. Under the cable insulation there is a metal external "shield", however the optical coverage of most of these braided shields is not usually very high, and generally does not provide significant shielding of the inner conductor at frequencies above 10 MHz.

Close-up of trenway with cover removed - Multiple Control Cables

Close-up of trenway with cover removed - Multiple Control Cables

Figure 5-12. Control cables in trenway.

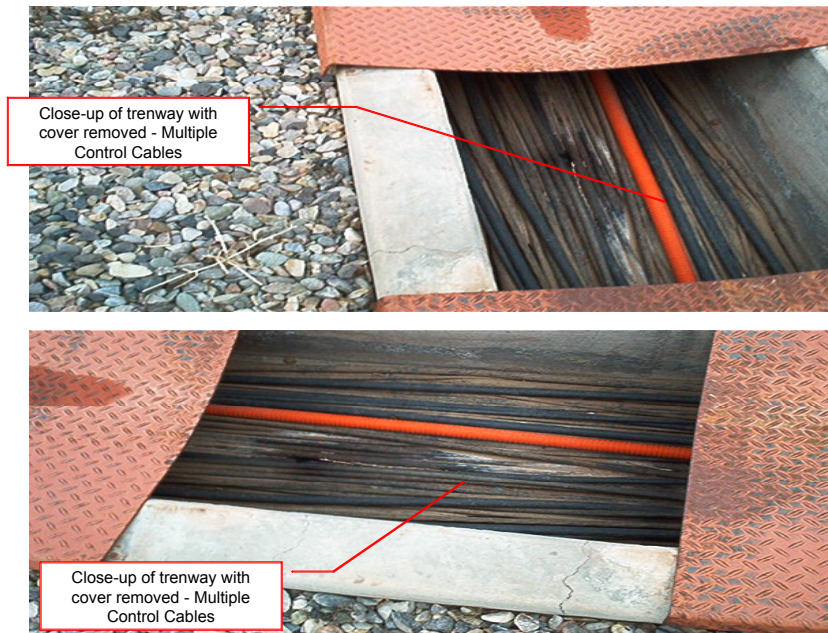In Figure 5-13 the control cables have their insulation stripped back and the shields are connected to ground cables. It is noted that the ground cables are on the order of 30 cm long (or longer), which provides significant impedance at high frequencies. While this length is acceptable for lightning frequencies (typically below 1 MHz), this will enable a significant portion of the high-frequency IEMI transients to continue to propagate on the signal wires inside the control facility instead of being directed to ground.
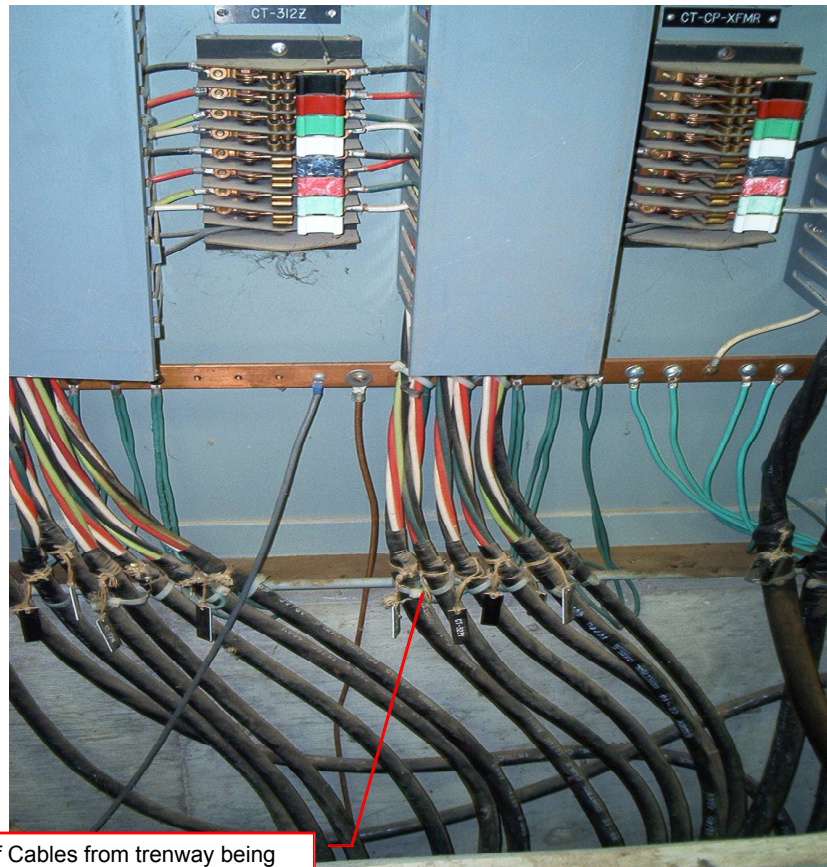
Close-up of Cables from trenway being brought into Control House Junction Box with ground termination details

Figure 5-13. Grounding of control cable shields and j-boxes in control building

In Figure 5-14 cables extend from the j-boxes to the individual racks of equipment. These cables will carry any remaining high-frequency transients that were coupled to the cables outside, and they will also be coupled to by the electromagnetic fields that propagate through the walls of the building (more important for IEMI). It is important to note that the direct coupling of fields inside the building is strongly influenced by the construction type of the building. There are strong variations for the penetrating electric fields at frequencies above 10 MHz due to whether the building is made of concrete (with or without reinforced bars), bolted metal, or wood.
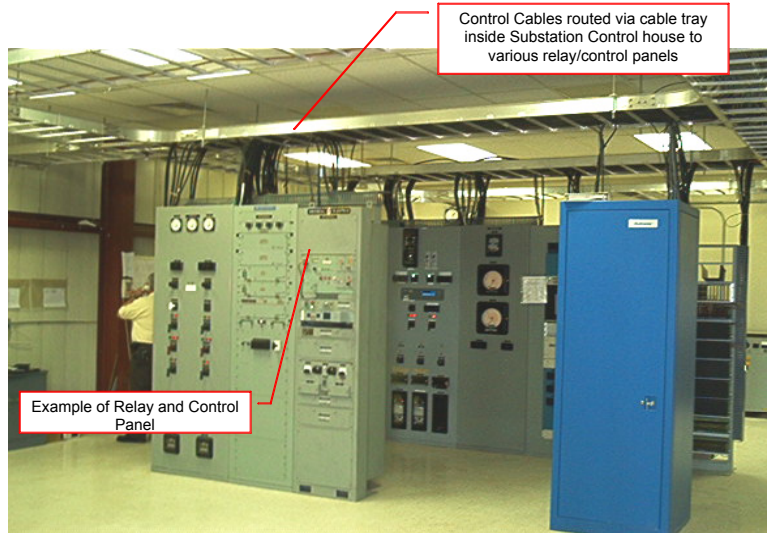
Figure 5-14. Distribution of control cables within building to cabinets

While these figures are provided to give an indication of the scope of the problem, it will be necessary to evaluate many factors that are common or different in various power substations in order to determine the seriousness of the IEMI threat and to recommend protection techniques that are cost effective.

From material presented in Section 2.3.3, it appears that maximum levels of approximately 10 kV may be coupled to horizontal buried lines in a substation yard just before entering the substation building. While the amount of these voltages that could propagate to the relays and other electronic control equipment is extremely variable, the fact that upsets on relays begin at 3.2 kV and damage to PLCs and PCs begin at approximately 0.5 kV, indicates a serious concern for the continued operation of a portion of the substations.

The more important problem for IEMI is that even if the cable penetrations into the control building are protected, there is still the problem of the penetration of the IEMI fields inside and coupling to the cables just above the electronic cabinets (see Figure 5-14). The level of the field penetrating the building is completely dependent on the type of wall and ceiling construction; given that field levels inside a poorly shielded control building could be as high as 10 kV/m, this means that up to 10 kV could be induced on cables leading to the electronics. Depending on the way that the cables enter the cabinets (whether the shields are bonded or not) will determine if these voltages reach the electronic equipment ports inside.

5.5   Power Generation Facilities

Power generator facilities are similar to industrial processing plants in that they use PLCs to control the flow of fuel and other aspects of the power generation process. As indicated in Tables 5-3 and 5-4, damage may occur for IEMI-like pulses at levels as low as 0.6 kV, although only one manufacturer's equipment failed at that level. The other failed at 3.3 kV. Since power generators are manned, the impact of upset may not be as

important as damage; however the damage levels indicated are quite low. In addition, it is not expected that the cabling within the generator facility will be better protected than in a substation, so again levels of induced voltages as high as 10 kV are possible at the locations of control electronics.

5.6   Power Control Centers

Power control centers can be described as distributed computer facilities with many communications lines entering and leaving the facility. Since these facilities do not deal directly with high voltage transformers nearby, most of the computer equipment is not afforded the same basic level of immunity as those found in substations, or in power generation facilities for that matter. Equipment like the PC (see Table 5-6) will fail its communications port due to a fast pulse at 0.5 kV, and other test data indicates that Ethernet ports are generally vulnerable at low levels. Given that ordinary building protection levels will allow up to 10 kV to be coupled to internal cables, this indicates a potential problem.

An important factor to consider is the location and type of wall construction of control centers. A control center built below the surface of the Earth has much better natural shielding than one built above grade in a high-rise building.

5.7   Distribution Transformers

During the ORNL power system studies in the 1980s, tests were performed to examine the possibility of E1 HEMP damage to distribution step-down transformers that can be found in the U.S. power grid. This testing included 19 samples of 7.2 kV/25 kVA power distribution transformers, using E1 HEMP like pulses. Damage that occurred was usually from dielectric breakdown within the windings – pinhole damage. The results of the testing are summarized in Table 5-7.

It is noted in the test results that failures occurred when the peak fast pulse voltage was between 264 and 304 kV. No damage occurred for peak pulses of 290 and 296 kV, so there appears to be some variability within the group of 19 transformers, although the variation is not that great. When lightning surge arresters were added to the transformers, no damage was noted up to the capability of the pulser (which was 1000 kV). For IEMI the likely maximum induced voltage level is about 10 kV, which is much smaller than the levels required to damage this type of distribution transformer.

Table 5-7. 7.2 kV/25 kVA transformer failure testing for fast pulses

XFMR	Shots #@kV	Peak Voltage (kV)	Time to Peak (ns)	Surge Arrester	Notes	Result
ZS1						Pulser calibration
ZS2	1@400	264	618	No	(1)	T-T failure
ZS3	2@400	288	668	No	(2)	HV-LV failure
ZS4	2@400	280	600	No	(1)	L-L failure
ZS5	1@400	272	550	No	(2)	HV-LV failure
ZS6	2@400	290	643	No	(1)	No damage
ZV1	1@400	296	601	No	(1)	No damage
ZV2	1@400	304	592	No	(2)	HV-LV failure
ZV3	2@400	110	100	Yes	(3)	No damage
ZV4	2@500	110	100	Yes	(3)	No damage
ZV4	2@780	116	110	Yes	(3)	No damage
XV1	1@400	272	500	No	(2)	HV-LV failure
XV2	2@400	115	110	Yes	(3)	No damage
ZW1	2@400	292	552	No	(1)	No damage
ZW2	2@400	16	Oscillatory	No	(4)	No damage
ZW3	2@780	100	110	Yes	(3)	No damage
ZW4	2@1000	112	105	Yes	(3)	No damage
ZD1	2@400	120	550	No	(5)	No damage
ZD2	2@400	20	Oscillatory	No	(4)	No damage
ZE1	2@1000	95	100	Yes	(6)	No damage
ZE2	6@780	95	100	Yes	(6)	No damage

(1) External flashover on HV bushing; T-T failure denotes turn-to-turn failure; L-L failure denotes line-to-line failure
(2) No external flashover; HV-LV failure denotes a high-voltage winding flashover to the low-voltage winding
(3) Surge arrester operation and no external flashover
(4) Surge applied to the low-voltage bushings with no external flashover
(5) Surge applied common mode to both HV bushings with external flashover
(6) Surge applied common mode to both bushings, and both arresters operated

Section 6
IEC Standardization for IEMI

One major IEMI standardization effort is currently underway at the International Electrotechnical Commission (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 electromagnetic compatibility (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 electromagnetic fields produced from a high altitude nuclear burst. These fields are generally known as HEMP (high altitude electromagnetic pulse), 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 Intentional EMI.

As of December 2009, SC 77C has 20 published documents in its program of work. The publications of SC 77C are part of the IEC EMC 61000 series of documents. There are five published documents that deal with high power electromagnetics (HPEM/IEMI). Figure 6-1 summarizes the documents completed. See the paper in the IEEE Special Issue for more details on the work of IEC SC 77C [33].
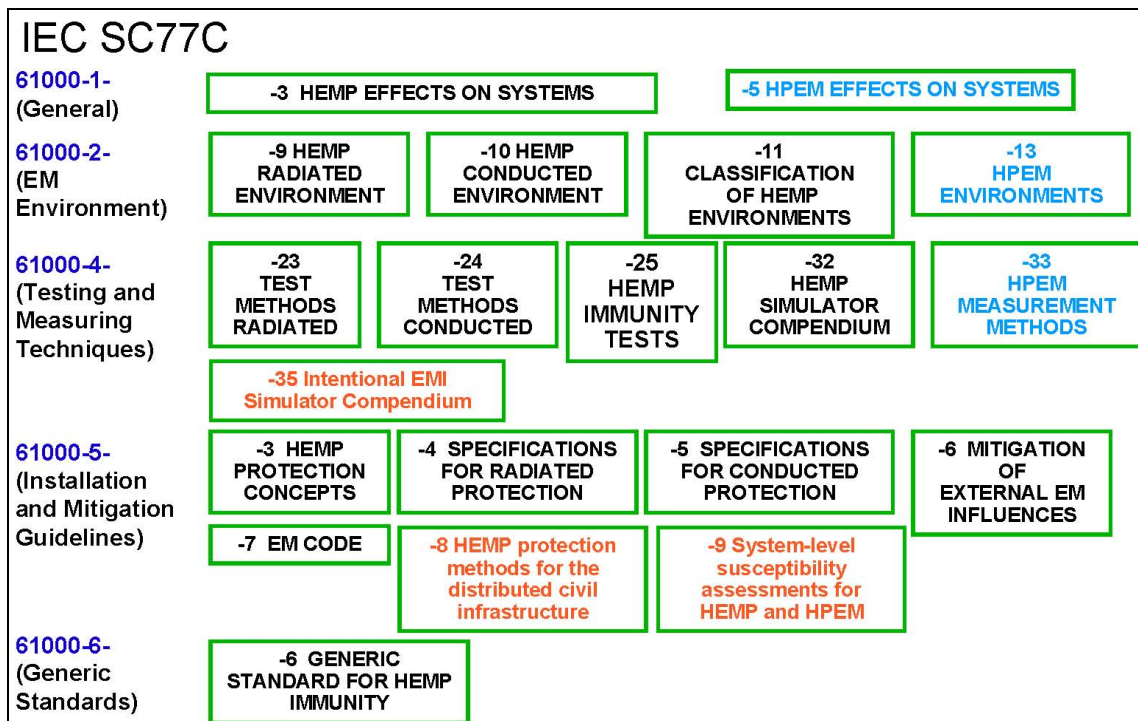

Figure 6-1. IEC SC 77C publications dealing mainly with HEMP (black) and HPEM/IEMI (blue) completed before 2009. Three additional documents were published in 2009 (orange).

References

[1] R. L. Gardner, "Electromagnetic Terrorism. A Real Danger, "Proceedings of the XIth Symposium on Electromagnetic Compatibility", Wroclaw, Poland, June 1998.

[2] W. A. Radasky, M. A. Messier and M. W. Wik, "Intentional Electromagnetic Interference (EMI) – Test and Data Implications", Zurich EMC Symposium, February 2001.

[3] "Joint Special Issue on the Nuclear Electromagnetic Pulse", IEEE Transactions on EMC, Vol. 20, No. 1, February 1978.

[4] "Joint Special Issue on High Power Microwaves", IEEE Transactions on EMC, 1992.

[5] P. O. Leach and M. B. Alexander, "Electronic Systems Failures and Anomalies Attributed to Electromagnetic Interference", NASA Report 1374, National Aeronautics and Space Administration. Washington, CC 20546-0001, July 1995.

[6] Workshop on "Electromagnetic Terrorism and Adverse Effects of High Power Electromagnetic (HPE) Environments", Proceedings of the 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, February 16 - 18, 1999.

[7] AMEREM'96, Albuquerque, New Mexico, May 27-31, 1996.

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

[9] International Radio Scientific Union (URSI) General Assembly, Toronto, 1999.

[10] E. Rosenberg, "New Face of Terrorism: Radio-Frequency Weapons", New York Times, 23 June 97.

[11] "City surrenders to £400m gangs", The Sunday Times, London, 2 June 1996.

[12] V. M. Loborev, "The Modern Research Problems", Plenary Lecture, AMEREM'96, Albuquerque, New Mexico, USA, May 1996.

[13] D. Sawyer, "20/20 Segment on Non-lethal Weapons", American Broadcasting Company (ABC), aired in February 1999.

[14] M. Bäckström, C. Frost and P. Ånäs, "Förstudie rörande vitala samhällssystems motståndsförmåga mot elektromagnetisk strålning med hög intensitet (HPM)", Användarrapport FOA-R--97-00538-612-SE, August 1997, 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, U. S. Army Space and Missile Defense Command, "Proliferation and Significance of Radio Frequency Weapons Technology", testimony before the Joint Economic Committee, United States Congress, February 25, 1998.

[16] D. V. Giri and F. M. Tesche, "Classification of Intentional Electromagnetic Environments (IEME)", IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[17] F. Sabath, M. Bäckström, B. Nordstrom, D. Serafin, A. Kaiser, B. Kerr and D. Nitsch, "Survey of Four European High-Power Microwave Narrow-Band Test Facilities", IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[18] W. P. Prather, C. E. Baum, R. J. Torres, F. Sabath and D. Nitsch, "Survey of Worldwide High-Power Wideband Capabilities", IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[19] IEC 61000-2-5, "Electromagnetic compatibility (EMC) – Part 2: Environment – Section 5: Classification of electromagnetic environments", Geneva, Switzerland.

[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" 14th International Zurich Symposium and Technical Exhibition on EMC, February 2001.

[21] Y. Parfenov, L. Zdoukhov, W. Radasky and M. Ianoz, "Conducted IEMI Threats for Commercial Buildings", IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[22] C. E. Baum, "Comparative System Response to Resonant and Unipolar Waveforms", AFWL Interaction Note 509, 1994; Proc. 13th International Zurich Symposium on EMC, 1999, pp. 15-20.

[23] C. E. Baum, "A Time-Domain View of Choice of Transient Excitation Waveforms for Enhanced Response of Electronic Systems", AFWL Interaction Note 560, 2000; Proc. ICEAA 01, Turin, Italy, 2001, pp. 181-184.

[24] D. Nitsch, F. Sabath, H.-U. Schmidt and C. Braun, "Comparison of the HPM and UWB Susceptibility of Modern Microprocessor Boards", AFWL System Design and Assessment Note 36, 2002; Proc. 15th Int. Zurich Symposium on EMC, 2003, pp. 121-126.

[25] J. Bohl, "High Power Microwave Hazard Facing Smart Ammunitions", AFWL System Design and Assessment Note 35, 1995.

[26] J. LoVetri, A. T. M. Wilburs and A. P. M. Zwamborn, "Microwave Interaction with a Personal Computer: Experiment and Modeling", Proc. 13th International Zurich Symposium on EMC, 1999, pp. 203-206.

[27] M. Bäckström, "HPM testing of a Car: A Representative Example of the Susceptibility of Civil Systems", 13th International Zurich Symposium Supplement, February 1999, pp. 189-190.

[28] IEC 60601-1-2, "Medical electrical equipment – Part 1-2: General requirements for safety – Collateral standard: Electromagnetic compatibility – Requirements and tests", Geneva, Switzerland.

[29] IEC 61000-4-6, "Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields", Geneva, Switzerland.

[30] IEC 61000-2-9, "Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance", Geneva, Switzerland.

[31] IEC 61000-2-10, "Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance", Geneva, Switzerland.

[32] C. E. Baum, "Damping Transmission-Line and Cavity Resonance", AFWL Interaction note 503, 1994; coauthor D.P. McLemore, Proc. 12th Int. Zurich Symposium on EMC, 1999, pp. 239-244.

[33] M. W. Wik and W. A. Radasky, "Development of High-Power Electromagnetic (HPEM) Standards", IEEE Transactions on EMC, Vol. 46, No. 3, August 2004.

[34] IEC 61000-2-13, "Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic environments – Radiated and conducted", Geneva, Switzerland.