

IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI)

IEEE Electromagnetic Compatibility Society

Sponsored by the

Standards Development Committee

IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI)

Sponsor

**Standards Development Committee
of the
IEEE Electromagnetic Compatibility Society**

Approved 26 January 2015

IEEE-SA Standards Board

Acknowledgments

Grateful acknowledgment to the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standard IEC 61000-2-13 ed.1.0 (2005) [B10]). All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and content.

Grateful acknowledgment to Eindhoven University of Technology for permission to reproduce information from Conference Proceedings EMC Europe 2004, Eindhoven, The Netherlands© [B8].

Grateful acknowledgment to ETH Zurich, Laboratory for Magnetic Fields and Microwave Electronics for permission to reproduce information from [B4], [B24], and [B35].

Grateful acknowledgment to Proc. 1st Asia-Pacific Symposium on EMC, 2008 for permission to reproduce information from [B25].

Abstract: Appropriate electromagnetic threat levels, protection methods, monitoring techniques, and test techniques for specific classes of computer equipment are established. This equipment is expected to be accessible to the public at ranges less than 100 m, and the loss of operation of the equipment due to intentional electromagnetic interference is expected to cause losses (both financial and of confidence) to businesses operating computer equipment, which are providing services to the public or to private companies. The principle class of equipment to be considered in this recommended practice includes fixed (non-mobile) computer equipment. Examples include automated teller machines; electronic cash registers at stores; computer equipment in banks and at airports; computer equipment controlling traffic flow; computer equipment controlling communications or allowing Internet access; computer equipment providing police, fire, and security services; computer equipment controlling the operation of the power grid (including smart meters); computer equipment operating in hospitals; etc.

Keywords: electromagnetic protection, IEEE 1624™, intentional electromagnetic interference; IEMI, high-power electromagnetics; HPEM

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2015 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 3 February 2015. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-9490-5 STD20083
Print: ISBN 978-0-7381-9491-2 STDPD20083

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/xpl/standards.jsp> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE recommended practice was completed, the Intentional Electromagnetic Interference Committee Working Group had the following membership:

William Radasky, *Chair*

Mats Bäckström
William Croisant
Sven Fisahn
Heyno Garbe
Richard Hoad

Daniel Månsson
Michael McInerney
Yury Parfenov
Frank Sabath
Edward Savage

Kwok Soohoo
Rajeev Thottappillil
Holger Thye
Anthony Wraight
Perry Wilson

The following members of the individual balloting committee voted on this recommended practice. Balloters may have voted for approval, disapproval, or abstention.

Jacob Ben Ary
William Bush
Brian Cramer
William Croisant
Alistair Duffy
Randall Groves
Donald Heirman
Werner Hoelzl
Daniel Hoolihan

Lars Juhlin
Piotr Karocki
Yuri Khersonsky
Arthur H. Light
William Lumpkins
Greg Luri
Edward McCall
Michael McInerney
Michael Newman
Charles Ngethe

Bansi Patel
Ghery Pettit
William Radasky
Bartien Sayogo
Walter Struppler
Thomas Tullia
John Vergis
Barry Wallen
Daidi Zhong

When the IEEE-SA Standards Board approved this recommended practice on 26 January 2015, it had the following membership:

John Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Peter Balma
Farooq Bari
Ted Burse
Clint Chaplain
Stephen Dukes
Jean-Phillippe Faure
Gary Hoffman

Michael Janezic
Jeffrey Katz
Joseph L. Koepfinger*
David J. Law
Hung Ling
Oleg Logvinov
T. W. Olsen
Glenn Parsons

Ron Peterson
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Don Wright
Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Michelle Turner
IEEE-SA Content Production and Management

Patricia Gerdon
IEEE-SA Technical Program Operations

Introduction

This introduction is not part of IEEE Std 1642™-2015, IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI).

The purpose of this recommended practice is to provide information for manufacturers and users to specify the electromagnetic compatibility (EMC) requirements for computer equipment and systems that can be used by the public or businesses, which require a high level of security to prevent intentional electromagnetic fields from interfering with the operation of these computers.

Contents

| | |
|---|----|
| 1. Overview | 1 |
| 1.1 Scope | 1 |
| 1.2 Purpose | 2 |
| 1.3 Background..... | 2 |
| 2. Normative references..... | 3 |
| 3. Definitions, acronyms, and abbreviations | 3 |
| 3.1 Definitions | 3 |
| 3.2 Acronyms and abbreviations | 5 |
| 4. Description of the IEMI threat..... | 5 |
| 4.1 Introduction to the threat | 5 |
| 4.2 Threat levels | 7 |
| 4.3 Examples of equipment susceptibilities to radiated threats | 9 |
| 4.4 Examples of equipment susceptibilities to conduct threats..... | 11 |
| 4.5 Summary of IEMI threat level and equipment susceptibilities | 15 |
| 5. Types of equipment and systems to be protected | 16 |
| 6. Protection methods | 17 |
| 6.1 Protection approaches | 17 |
| 6.2 Security approach | 17 |
| 6.3 Electromagnetic approach | 17 |
| 7. Monitors and alarms | 19 |
| 8. Recommended protection approach | 21 |
| 9. Test methods..... | 21 |
| 9.1 Equipment-level test methods..... | 21 |
| 9.2 Rack-level test methods..... | 22 |
| 9.3 Building-level test methods | 22 |
| Annex A (informative) Bibliography | 23 |

IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI)

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This recommended practice establishes appropriate electromagnetic (EM) threat levels, protection methods, monitoring techniques, and test techniques for specific classes of computer equipment. This equipment is expected to be accessible to the public at ranges less than 100 m, and the loss of operation of the equipment due to intentional electromagnetic interference (IEMI) is expected to cause losses (both financial and of confidence) to businesses operating computer equipment, which are providing services to the public or to private companies.

The principle class of equipment to be considered in this recommended practice includes fixed (non-mobile) computer equipment. Examples include automated teller machines (ATMs); electronic cash registers at stores; computer equipment in banks and at airports; computer equipment controlling traffic flow; computer equipment controlling communications or allowing Internet access; computer equipment providing police, fire, and security services; computer equipment controlling the operation of the power grid (including smart meters); computer equipment operating in hospitals; etc.

1.2 Purpose

The purpose of this recommended practice is to provide information for manufacturers and users to specify the electromagnetic compatibility (EMC) requirements for computer equipment and systems that can be used by the public or businesses, which require a high level of security to prevent intentional EM fields from interfering with the operation of these computers.

1.3 Background

The term high-power electromagnetics (HPEM) 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 in the past as part of HPEM are the EM fields from nearby lightning strikes, the EM fields near an electrostatic discharge (ESD), the high-altitude electromagnetic pulse (HEMP) created by nuclear bursts, and the EM fields created by radar systems. The EMC Society of the IEEE's Technical Committee 5 (TC-5), "High Power Electromagnetics," deals with all of these subjects. In addition, the International Electrotechnical Commission (IEC) is active in developing standards for commercial equipment and systems under Subcommittee 77C, "High power transient phenomena."

In the past 15 years, two new terms have arisen in the EMC field: EM terrorism [B5]¹ and intentional electromagnetic interference (IEMI) [B30]. In recent years, the scientific community has agreed to utilize the more generic term, IEMI, which includes EM terrorism. In February 1999 at a workshop held at the Zurich EMC symposium, the currently 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" [B41].

It is noted that hackers are not mentioned explicitly in this definition, although in most countries of the world, an attack on commercial interests for entertainment purposes 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 for many years to understand this threat and to provide useful guidance on protection.

While there has not been much publicity concerning this threat, five reported criminal usages of EM weapons have been found in the following literature:

- a) In The Netherlands, an individual disrupted a local bank's computer network because he was refused a loan. Type of crime: blackmail/criminal damage [B9].
- b) In Japan, two Yakuza criminals were caught using an EM disruptor on a Pachinko (gaming) machine to trigger a false win. Type of crime: robbery [B9].
- c) In St. Petersburg, Russia, a criminal used an EM disruptor to disable a security system on a jewelry store, so that he could commit a robbery. Type of crime: robbery [B37].
- d) In London, a city bank was the target of blackmail attempt whereby the use of EM disruptors was threatened to be used against the bank's systems. Type of crime: blackmail [B39].
- e) In Moscow, Russia, a telecommunications center was targeted and was put out of commission for 24 hours, denying service to 200 000 customers. Type of crime: blackmail/criminal damage [B37].

IEMI threats and protection methods have been evaluated in technical conferences throughout the world, and occasional articles have been published in the popular press, in the U. S. Congressional Record, and also by the IEC dealing with the threat of IEMI to civil society (see [B16], [B23], [B32], [B35], [B36] [B39], and [B40]). While well-documented cases of criminal attacks using IEMI have been difficult to obtain due to the sensitivity of security threats, it is clear from laboratory experiments performed by

¹ The numbers in brackets correspond to those of the bibliography in Annex A.

scientists that it is not difficult to create malfunctions in electronic equipment that is not protected from this threat.

It is important to recognize that a special issue of *IEEE Transactions on Electromagnetic Compatibility* devoted to HPEM and IEMI [B38] was produced in 2004 (hereafter referred to as “the 2004 Special Issue”), summarizing many years of work. This was preceded by two related special issues of these transactions covering the nuclear electromagnetic pulse in 1978 [B20] and high-power microwaves (HPM) in 1992 [B21]. It is clear that many EM models and codes developed in the past to deal with the intense, high-frequency portion of the electromagnetic pulse and the high levels of fields associated with HPM are relevant to the new field of IEMI. This is because the analysis of transient, high-frequency, 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 non-linear aspects, factors not always present in the routine treatment of EMC.

In addition, the development of miniaturized pulsers and antenna systems in recent years has produced a situation where different types of intense EM fields (narrowband to very wideband) can be produced at close ranges. With the development of more sophisticated computer equipment and the proximity of this equipment to the public, it is likely that criminals will use EM threat devices to interfere with these computers, disrupting the ability of companies to provide important services to the public. It is the purpose of this standard practice to recommend methods to protect computers from this new threat through a combination of equipment design and monitoring of the threat.

This standard practice first describes the IEMI threat in detail (Clause 4), which includes the capabilities of EM weapons, and follows with a discussion of the susceptibilities of typical electronic equipment (4.3 and 4.4). Clause 5 discusses the types of equipment to be protected. Protection methods (Clause 6) and monitoring concepts (Clause 7) are then described, followed by a methodology to determine the protection levels required (Clause 8). Finally, Clause 9 describes the basic test methods. A bibliography is also provided for those looking for further information on the subject of IEMI (Annex A).

2. Normative references

There are no normative references in this recommended practice. The bibliography in Annex A lists all of the documents cited in the text.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.²

bandratio (br): The 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.

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

²*IEEE Standards Dictionary Online* subscription is available at:
http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

continuous wave (CW): A time waveform that has a fixed frequency and is continuous.

electromagnetic compatibility (EMC): The 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 that 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.³

electromagnetic susceptibility: The 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): An electromagnetic pulse produced by a nuclear explosion outside the earth's atmosphere.

NOTE—The explosion typically occurs 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 an historical definition that depended on the strength of the source. This recommended practice is mainly interested in the EM field incident on an electronic system.

hyperband signal: A signal or waveform with a percentage bandwidth (pbw) value between 163.4% and 200% or a bandratio >10.

hypoband signal (narrowband signal): A signal or waveform with a pbw <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.

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

percentage bandwidth (pbw): The 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 approach is used.

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.

³ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

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 that varies between two consecutive steady states during a time interval that 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%.

3.2 Acronyms and abbreviations

| | |
|------|--|
| br | bandratio |
| CW | continuous wave |
| EFT | electric fast transient |
| EM | electromagnetic |
| EMC | electromagnetic compatibility |
| EMI | electromagnetic interference |
| ESD | electrostatic discharge |
| HEMP | high-altitude electromagnetic pulse |
| HPEM | high-power electromagnetics |
| HPM | high-power microwaves |
| IEMI | intentional electromagnetic interference |
| IRAs | impulse-radiating antennas |
| pbw | percentage bandwidth |
| UWB | ultrawideband |

4. Description of the IEMI threat

4.1 Introduction to the threat

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 0.1 GHz and 5 GHz seem to be of most concern. 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 HPM, although this term is used loosely to also include frequencies outside of the microwave range.

A wideband waveform (sometimes referred to as 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 are being developed at this time to divide the wideband category into several subcategories. As described in IEC 61000-2-13 [B10] and by Giri and Tesche in the 2004 Special Issue on HPEM and IEMI [B6], four terms are used to describe the bandwidths of narrowband and wideband waveforms: hypoband, mesoband, sub-hyperband, and hyperband. These terms have been defined based on the bandratio (i.e., the ratio of high and low frequencies containing 90% of the energy) with values <1.01 , 1.01 to 3 , 3 to 10 , and >10 , respectively.

In terms of system vulnerabilities, the narrowband threat usually requires very high power and, therefore, high peak electric fields (usually greater than 100 V/m), as the electrical energy is delivered in a narrow-frequency band; this requires a high-power generator. It is fairly easy to deliver fields on the order of thousands of volts per meter at a single frequency. Of course, each system under test may have a vulnerable frequency that is different from the next. Sometimes the malfunctions observed in testing equipment with narrowband waveforms are those of permanent damage, especially when considering thermal-heating type failures. Available test facilities using the narrowband or hypoband waveforms are described by Sabath et al. [B33].

The wideband threat is somewhat different with respect to the type of impact on electronics. Because 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, mainly due to a lower probability of thermal heating effects even though arcing and peak voltage breakdown may still occur. However, it is easier to find a system's vulnerability because 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 by Prather et al. in the 2004 Special Issue on HPEM and IEMI [B28].

There are two primary ways that a narrowband or wideband waveform may be delivered to a computer equipment or 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/TR 61000-2-5 [B17]).

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 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.

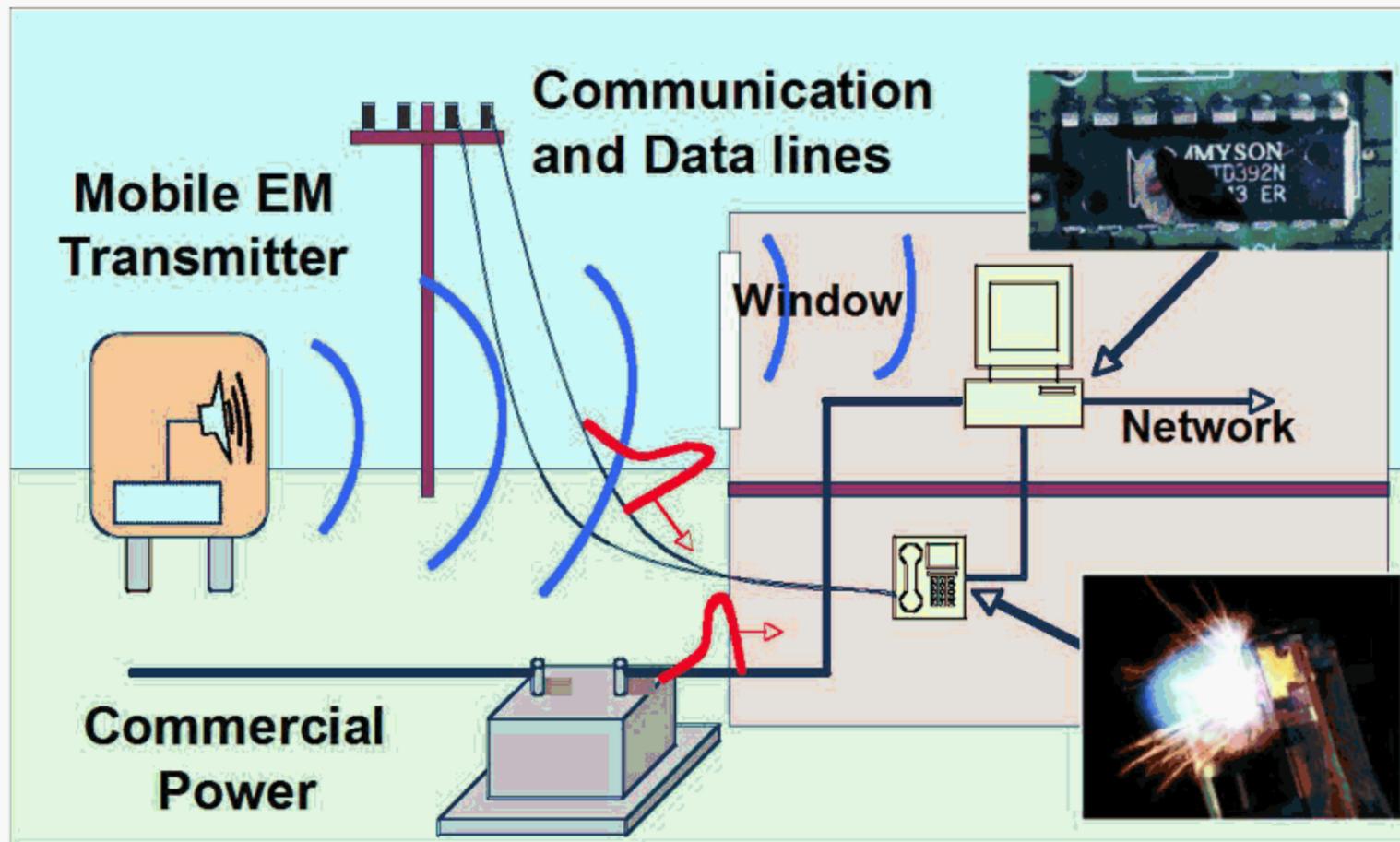


Figure 1—Typical radiated field interactions that would produce IEMI [B29]

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, frequencies below 10 MHz (and pulse widths wider than 50 ns) propagate more efficiently than higher frequencies on cable shields and bundles (common mode). Experiments by Fortov et al. have shown that these lower frequencies can disrupt the operation of equipment inside a building [B3]. More recent publications indicate that once IEMI creates a differential mode coupling between wires, these signals can propagate well even for frequencies above 1 GHz. In the 2004 Special Issue on HPEM and IEMI, Parfenov et al. provide an overview of the problem posed by conducted threats [B27].

4.2 Threat levels

The IEMI problem has two parts. One is the level of susceptibility of electronic systems and the second is the level of EM field that can be produced by an attacker. This subclause will discuss the approximate levels of the threat that can be produced, while 4.3 and 4.4 will provide some insight into susceptibility levels of modern electronics to the same types of EM waveforms.

In IEC 61000-2-13, the IEC examined three different types of technology levels to produce EM weapons [B10]. The first was described as low-tech and examined what fields could be produced with the magnetron from a microwave oven. Table 1 indicates the levels of narrowband fields that could be produced with different types of antennas for the 2.45 GHz signal. The most important parameter is rE_{peak} , which is defined as the product of the peak electric field and the range where it is measured. It provides an estimate of the strength of the EM field produced at a distance. One needs to divide rE_{peak} (in volts) by the range in meters to obtain the peak electric field level in volts per meter. For example, at a range of 30 m, the peak electric field level in the third row of Table 1 would be 156 V/m.

Table 1—Levels of narrowband rE_{peak} and peak electric fields at three ranges using the magnetron of a microwave oven with different types of antennas (considered to be low-tech [B10])

| Antenna type | Power rms | Peak E-field in WR 340 | rE _{peak} | E _{peak} r = 30 m | E _{peak} r = 100 m | E _{peak} r = 300 m |
|------------------------------------|-----------|------------------------|--------------------|----------------------------|-----------------------------|-----------------------------|
| Open-ended WR 340 | 1100 W | 25 kV/m | 540 V | 18 V/m | 5.4 V/m | 1.8 V/m |
| Pyramidal horn | 1100 W | 25 kV/m | 2200 V | 73 V/m | 22 V/m | 7.3 V/m |
| Reflector antenna (1.8 m diameter) | 1100 W | 25 kV/m | 4680 V | 156 V/m | 47 V/m | 15.6 V/m |

Reprinted with permission from IEC 61000-2-13 ed. 1.0 Copyright © 2005 IEC Geneva, Switzerland. www.iec.ch.

The IEC also examined the use of a commercial off-the-shelf radar system as a mid-tech IEMI source. Many older types of radars can be purchased in surplus sales. Table 2 shows the narrowband field levels for two antennas, one large and the other more modest. For the larger antenna, the rE_{peak} level is 1.9 MV. For the smaller antenna, the rE_{peak} level is 0.6 MV.

Table 2—Peak levels of narrowband electric fields at four ranges for two sizes of antennas produced by off-the-shelf radars and considered to be mid-tech. The average power of the magnetron is 2.5 MW and the frequency is 1.285 GHz [B10].

| Range <i>r</i> | Peak E-field antenna size 9.35 m ² | Peak E-field antenna size 0.935 m ² |
|----------------|---|--|
| 30 m | 63 kV/m | 20 kV/m |
| 100 m | 19 kV/m | 6 kV/m |
| 300 m | 6.3 kV/m | 2 kV/m |
| 1000 m | 1.9 kV/m | 600 V/m |

Reprinted with permission from IEC 61000-2-13 ed. 1.0 Copyright © 2005 IEC Geneva, Switzerland. www.iec.ch.

In the third example, the IEC examined wideband pulsers and antennas that could be considered high-tech. This survey was done at a time that many impulse-radiating antennas (IRAs) with matched pulsers were being built by national laboratories in several countries. At this time, many pulsers are available commercially, and the technology of designing IRAs is not as difficult as it was 5 years ago. In addition, the highest rE_{peak} level (not shown) today is 5 MV, as represented by the JOLT pulser. While these pulsers are labeled as high-tech in Table 3, it is reasonable to expect that an rE_{peak} level of 0.5 MV for a 0.1/1 ns (rise time/pulse width) pulse could be considered mid-tech for a wideband threat at this time.

Table 3—High-tech wideband pulsers and IRAs circa 2003 [B10]

| # | Name | Pulsar | Antenna | Near field | Far field | r E | Band ratio br | Band |
|---|--|--|--------------------------|-------------------------------|-----------------------------|---------|---------------|-------|
| 1 | Prototype IRA AFRL, KAFB, NM USA | ±60 kV 100 ps/20 ns 200 Hz burst | 3.66 m dia (F/D)=0.33 | 23 kV/m at r = 2 m | 4.2 kV/m at r = 304 m | 1280 kV | 100 | Hyper |
| 2 | Upgraded prototype IRA AFRL, KAFB, NM USA | ± ~ 75 kV 85 ps/20 ns ~ 400 Hz | 1.83 m dia (F/D)=0.33 | 41.6 kV/m at r = 16.6 m | 27.6 kV/m at r = 25 m | 690 kV | 50 | Hyper |
| 3 | Swiss IRA NEMP Laboratory Spiez, Switzerland | 2.8 kV 100 ps/4 ns 800 Hz | 1.8 m dia (F/D)=0.28 | 1.4 kV/m at r = 5 m | 220 V/m at r = 41 m | 10 kV | 50 | Hyper |
| 4 | TNO IRA The Hague Netherlands | 9 kV 100 ps/4 ns 800 Hz | 0.9 m dia (F/D)=0.37 | 7 kV/m at r = 1 m | Not available | 34 kV | 25 | Hyper |
| 5 | Univ. of Magdeburg Magdeburg, Germany | 9 kV 100 ps/4 ns 800 Hz | 0.9 m dia (F/D)=0.37 | 7 kV/m at r = 1 m | Not available | 34 kV | 25 | Hyper |

NOTE—rE in the table is the same parameter identified as rE_{peak} in this recommended practice.

Reprinted with permission from IEC 61000-2-13 ed. 1.0 Copyright © 2005 IEC Geneva, Switzerland. www.iec.ch.

4.3 Examples of equipment susceptibilities to radiated threats

In recent 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 (PC) equipment because it is in wide usage in many different industries.

Modern computers (with clock speeds of ~1 GHz) and other types of equipment using microprocessors appear to be vulnerable to malfunction from radiated narrowband fields above 200 V/m (depending on frequency). 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 on automobiles over the range of 1 GHz to 15 GHz seem to indicate that malfunctions occur at lower field levels at lower frequencies; the stopping of automobiles was reported by Bäckström at 500 V/m at 1.3 GHz for testing performed in the mid-1990s [B1]. There have not been as many experimental results published that have covered frequencies below 1 GHz, although tests performed on standalone PCs by Hoad et al. indicate that this trend of lower level failures at lower frequencies continues down to 400 MHz, as shown in Figure 2. Other data indicate that with network cables included, the susceptibility levels continue to decrease with frequency to 100 MHz or possibly lower, as shown in Figure 3.

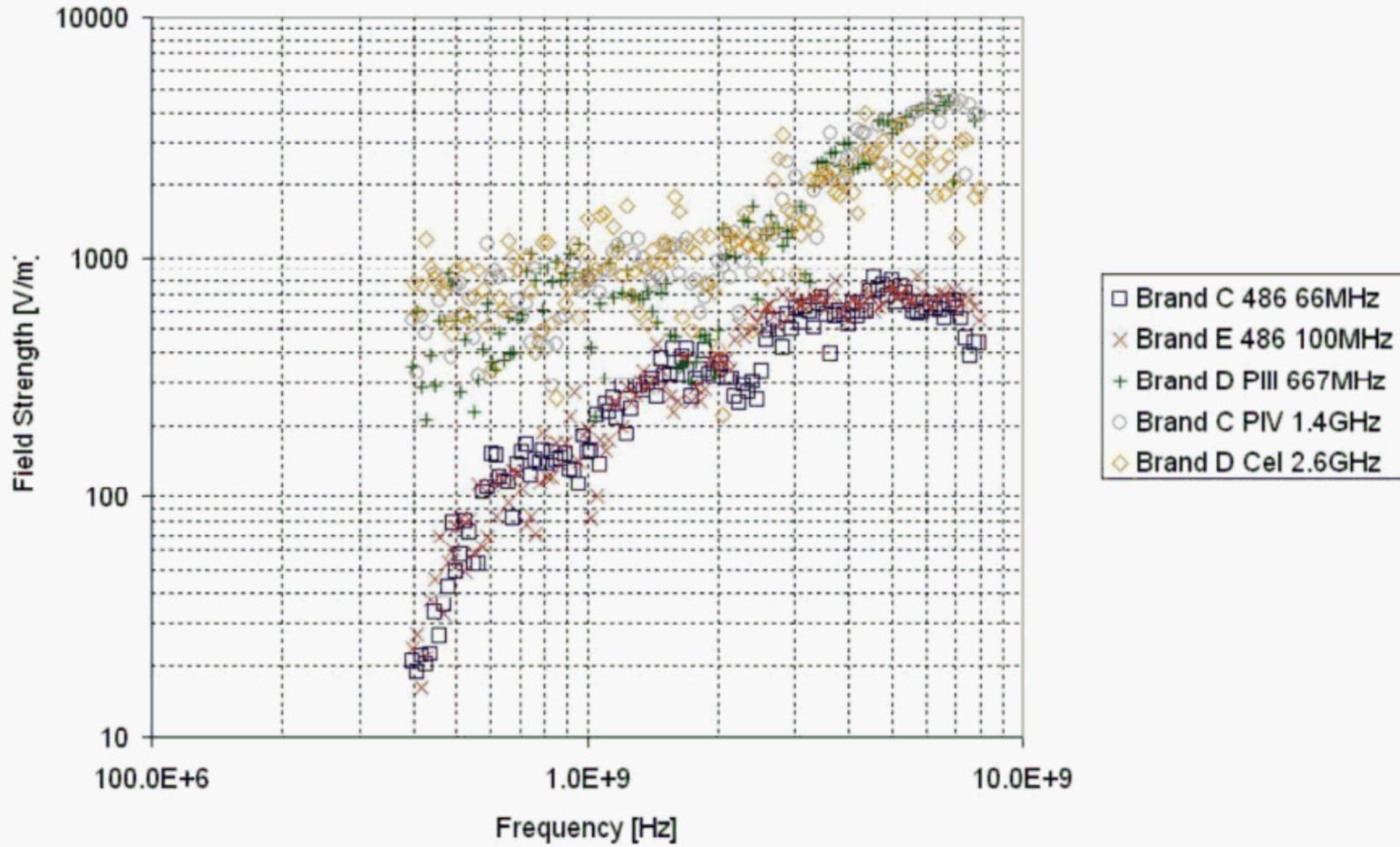
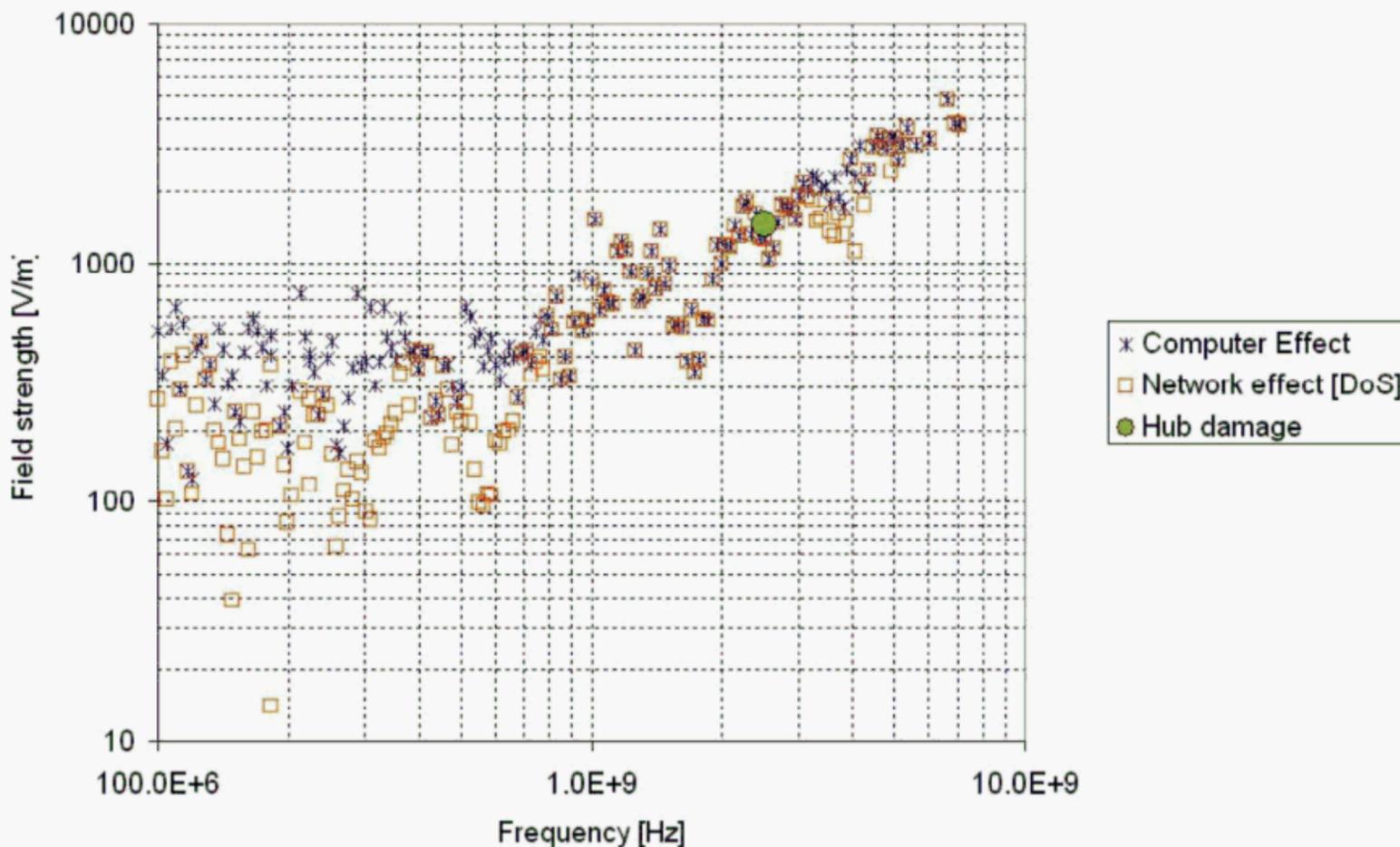


Figure 2—Susceptibility levels of modern PCs to narrowband electromagnetic fields in a mode-stirred chamber [B7]



Reprinted with permission from Eindhoven University of Technology from *Conference Proceedings EMC Europe 2004*, Eindhoven, The Netherlands © 2004.

Figure 3—Susceptibility levels of a modern networked PC to narrowband electromagnetic fields in a mode-stirred chamber [B8]

As far as wideband electric field testing of commercial electronics is concerned, Parfenov et al. tested electronic cash registers to determine their susceptibility to hyperband waveforms with a 0.1/1 ns pulse (rise time/pulse width). As seen in Figure 4, serious malfunctions occurred at peak values of ~2 kV/m and damage at ~5 kV/m [B26].

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 catastrophic refusal

| | | | | | | |
|---------------------------------|-------|-------|-------|-------|-------|----------------------|
| Level of UWB field, kV/m | 2.5 | 3.1 | 3.9 | 4.4 | 4.8 | 5.1 |
| Result | Upset | Upset | Upset | Upset | Upset | Catastrophic refusal |

Figure 4—Failure levels of electronic cash machines (cash registers) when exposed to a 0.1/1 ns hyperband electric field [B26]

Note that 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, then 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 (except in mode-stirred chambers), and, therefore, many of the serious effects noted during testing will actually occur at lower field levels when an optimum coupling geometry is applied, especially at frequencies above 1 GHz.

While these failure values may seem to be low, they should not be a surprise. When the EMC test requirements are examined for immunity in the IEC (see IEC 61000-4-3 [B11]), it is unusual to see a narrowband radiated field level requirement above 10 V/m (for frequencies above 80 MHz). Higher levels are not recommended because of the expense of providing the increased protection, and most of the natural commercial threats to electronics are below 10 V/m. Also it should be recognized that there is no radiated transient testing performed in the normal EMC series of tests, other than the fields produced during ESD testing. For narrowband voltages induced on cables connected to equipment, 10 V is the upper level required in most cases for EMC immunity testing. The frequencies of application for conducted tests are usually below 80 MHz.

It is important to recognize that these radiated and conducted EMC immunity levels do not protect equipment from all EM environments; rather, these levels are intended to cover most of the expected cases on a statistical basis. They do not cover intentional EM threats such as IEMI.

4.4 Examples of equipment susceptibilities to conduct threats

For 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 on power or communications cables. A comprehensive study performed by Parfenov indicated that both narrowband and wideband signals could be injected on the secondary of a building power supply and these signals would propagate easily within the wiring of a building with limited attenuation as shown in Figure 5. A related experimental study performed by

Fortov et.al, found that injected wideband pulsed voltages on the order of 5 kV to 6 kV could damage computer power supplies [B4].

Experiments have also shown that narrowband voltages injected into the grounding system of a building can cause significant equipment malfunctions inside [B4]. Frequencies below 100 Hz and levels below 100 V have been shown to cause problems.

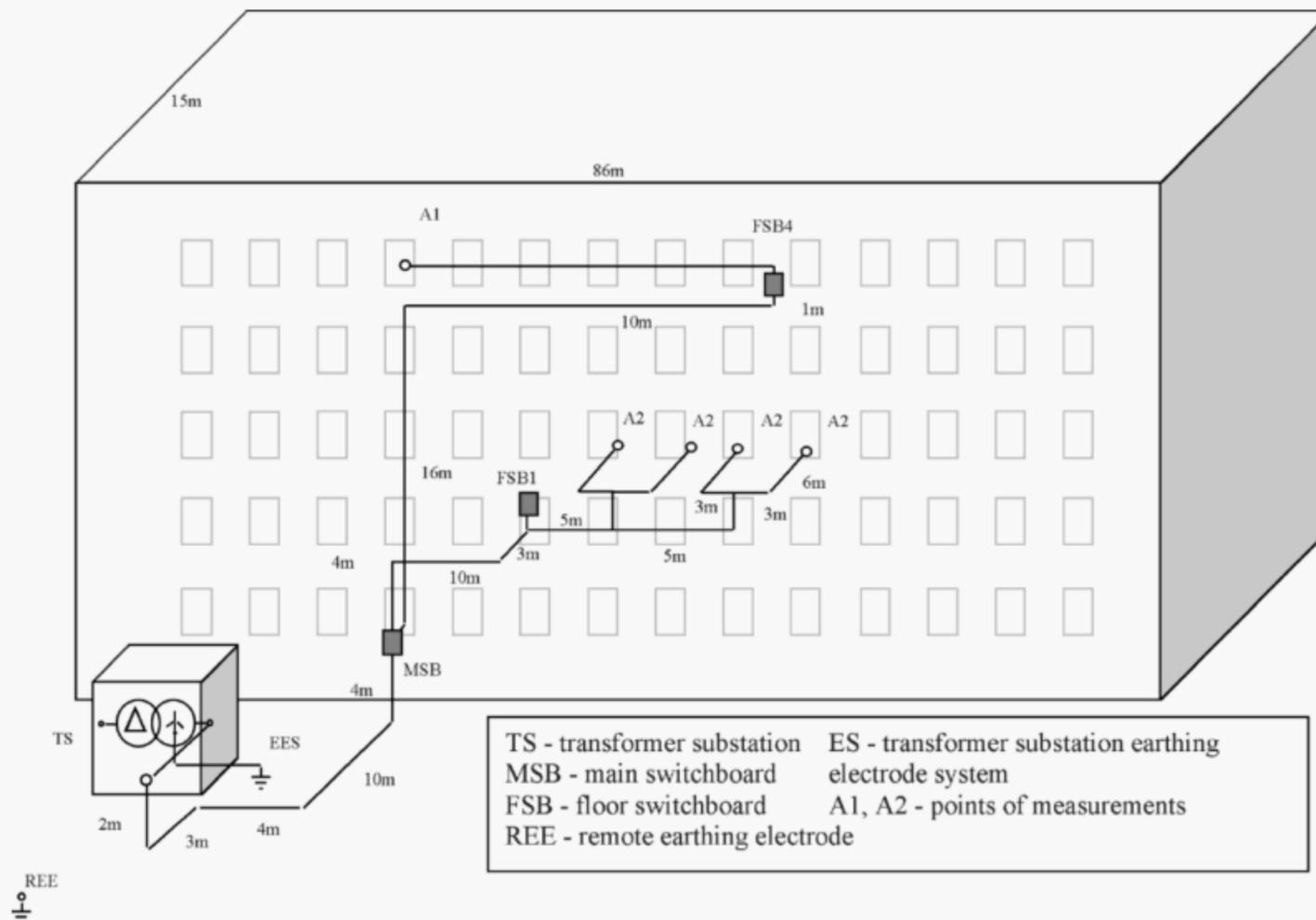


Figure 5—Building geometry and measurement points for injection of high-frequency transients into the power distribution system [B4]

Using the experimental data acquired, it was possible to develop a numerical estimation of the currents and voltages at different points of the power network of a building considering various ways of injection: in the phase-neutral circuit, in a break of the neutral wire, and between the transformer earthing point and a remote earthing electrode. A computer code known as the Conducted Threats Code was developed to model the propagation of conducted waveforms in other buildings [B4].

For wideband-conducted transients, most of the lightning and electric fast transient (EFT) tests for EMC immunity 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. Typical EMC wideband test waveforms have rise-times as fast as 5 ns and pulse widths as long as 700 μ s. Many of the possible IEMI conducted threats have rise times faster than 1 ns with pulse widths on the order of a few ns, and these have been found to propagate well in building power conductors in a differential mode, as demonstrated by Månsson [B22].

For longer waveforms, it appears that pulse widths on the order of 100 μ s can create damage to equipment power supplies and to interface circuit boards (see Figure 6) at levels as low as 500 V, but more typically at levels of 2 kV to 4 kV [B24]. Even the EFT pulse (5/50 ns) used in EMC testing will produce serious equipment malfunction and damage at levels of 4 kV/m to 5 kV/m.

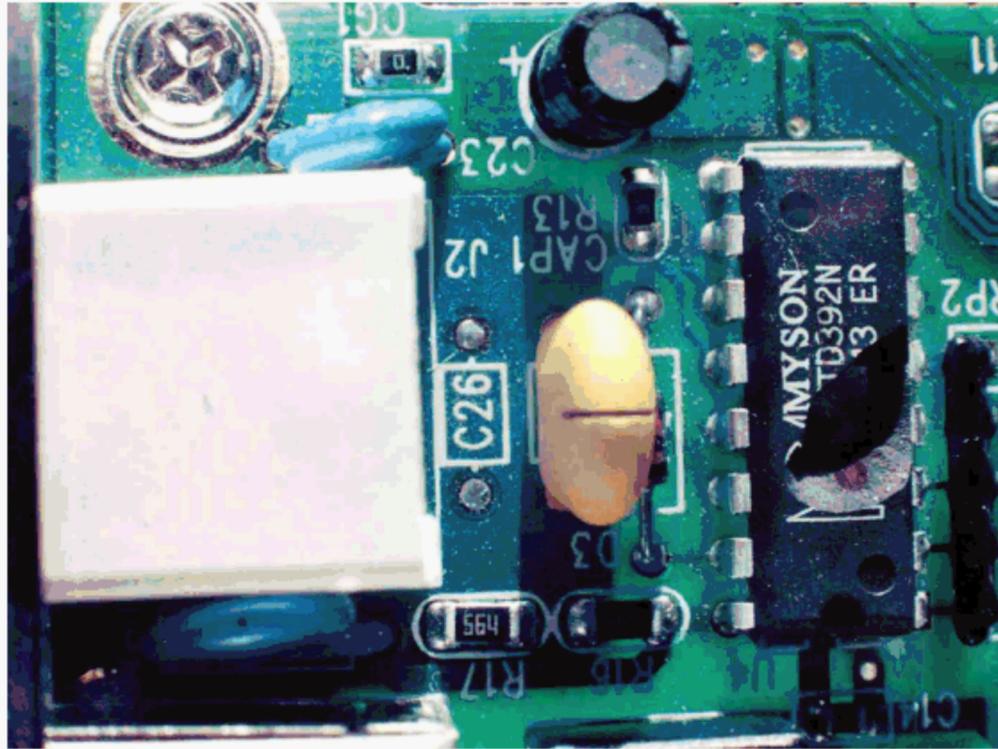


Figure 6—Damage produced on an Ethernet 10 Base2 computer interface board due to the cable injection of a 500-V telecom pulse as defined in IEC 61000-4-5 [B12]

Recent injection testing performed by Savage et al. [B35] on programmable logic controllers (PLCs) indicates that this class of simple industrial computer is extremely vulnerable to fast transients at levels only slightly higher than the levels of normal IEC EMC immunity testing. Sample susceptibility results are shown in Figure 7.

| Fisher ROC809 Remote Operations Controller – Fast Pulse | | | | | |
|---|--------------|--------------|--------------------------------|-------------|---------|
| DUT | | Drive | Voltage Level: Charge/Load, kV | | |
| Unit | Port | | No Effect | Upset | Damage |
| ROC 809 | 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 7—Upset and damage produced during the injection of the Fisher PLC using a 5/50 ns pulse [B35]

Another aspect of system vulnerability is the denial of service problem. In various civil electronic systems, data transmission subsystems are widely used. It is known that the basic characteristics of data links are the data rate (R) and the data packet length (N) [B25]. Characteristics of a fast pulse disturbance include the pulse repetition rate (f) and the parameter $Z0$, which is equal to signal/noise ratio in the data transmission network if $f = R$. It is important to note that the parameter $Z0$ [B25] is proportional to the square root of the average power of the pulse disturbance.

Figure 8 illustrates the results of calculations of the dependence of the probability P of incorrect transfer of data packets for variations in the pulse repetition rate f at $N = 1000$ bits and $R = 2 \times 10^6$ bps and for various

values of parameter Z_0 (i.e., at various values of average power of pulse disturbance). One can see that this dependence has a maximum. Therefore, it is necessary to choose characteristics of test pulses correctly for immunity testing of data transmission systems to periodically repeating voltage pulses.

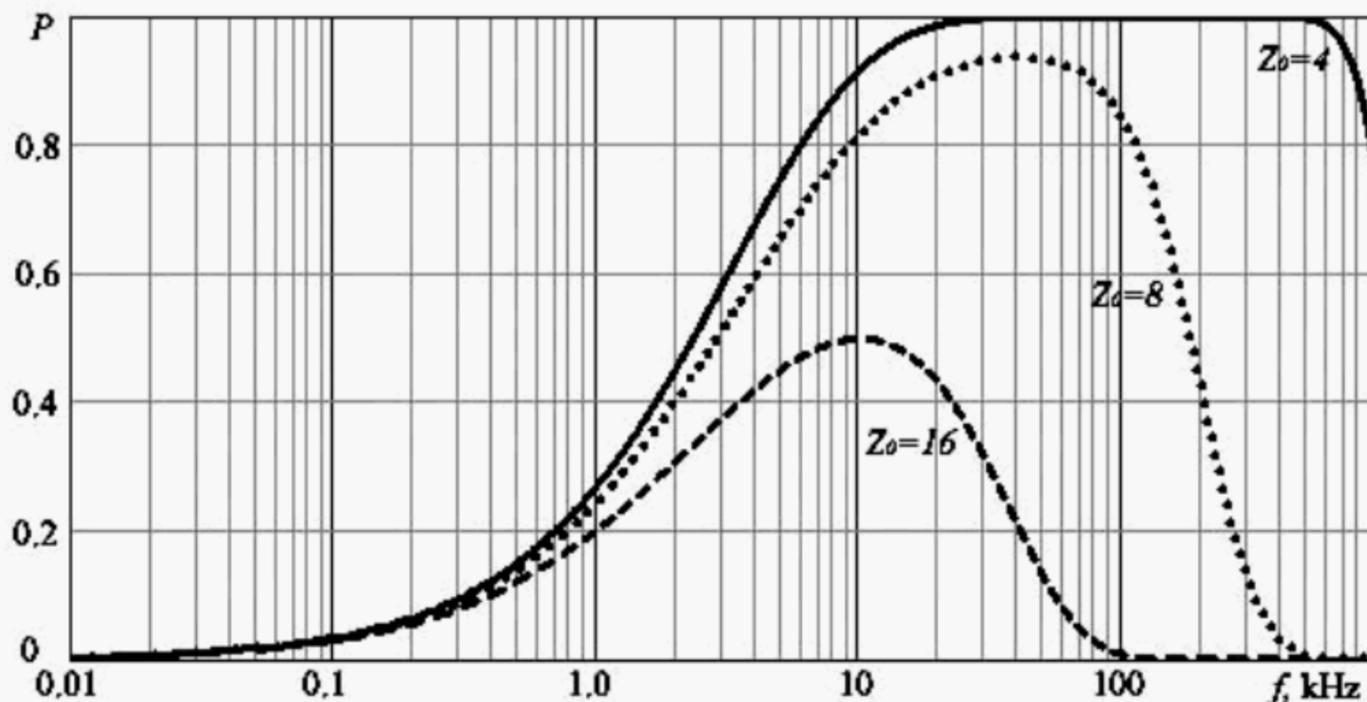


Figure 8—Calculated dependence of the probability of incorrect transfer of data packets from pulse repetition rates of $N = 1000$ bits and $R = 2 \times 10^6$ bps [B25]

It is important to note that the voltage disturbance will result in the degradation of the parameters of a computer network if the pulse peak is higher than working signal level by only a factor of 2 when the pulse repetition rate is about 1 kHz. At the same time, hundreds of volts may be induced between a wire and the equipment case using inductive injection in a power cable (or data cable) with a nanosecond generator with a voltage of several tens of kilovolts.

Experimental results justify the results presented above. Figure 9 illustrates the degradation of a data link when periodically repeating voltage pulses are injected in the power cable using an inductive method for a generator with the following parameters: 5/50 (rise time/pulse width) nanosecond waveform and a 50-kV peak voltage. Duration of influence was equal to 1 min. Figure 9 shows that the actual data rate of the data link decreases sharply for pulse repetition rates greater than 50 Hz. When the pulse repetition rate is equal to 500 Hz, the full degradation (denial of service) of the channel was observed.

It should be noted that a similar trend will take place when radiated disturbances are coupled to a network cable.

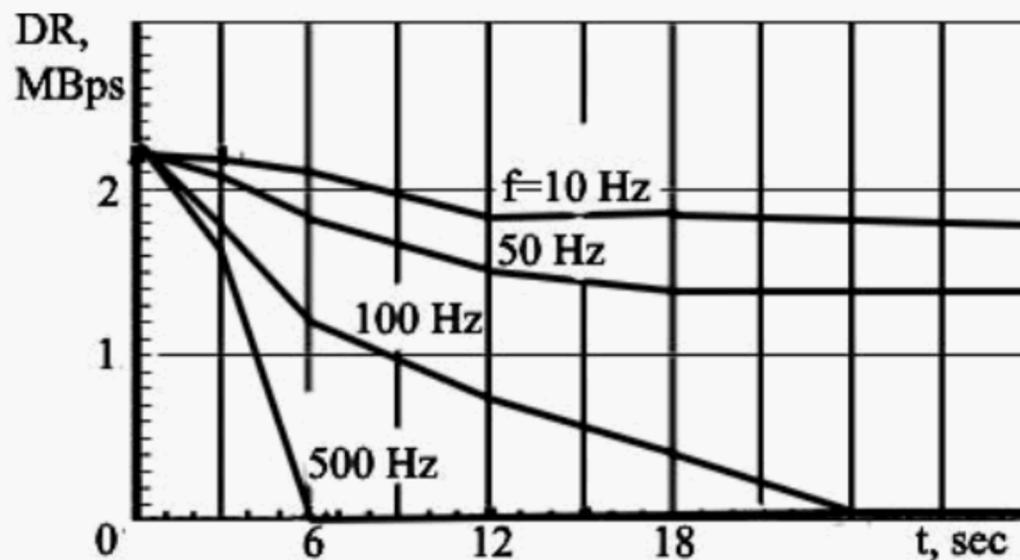


Figure 9— Degradation of the data link ($R = 2 \times 10^6$ bps) at different pulse repetition rates f in hertz, the data rate DR in megabits per second, and time t in seconds [B25]

4.5 Summary of IEMI threat level and equipment susceptibilities

4.5.1 Summary of IEMI threat levels

While the technology of developing threat pulsers varies, other factors, such as pulser/antenna size, enter into the likelihood of attack. Size is a factor in that it determines how close the pulser/antenna may be relative to a building, (where computers may be accessible to the public) without detection. In particular, it is clear that most narrowband pulsers generally require a large energy reserve and are therefore larger in size than wideband pulsers, which produce high peak power levels but require relatively low energy for each pulse. Therefore, this recommended practice considers the mid-tech narrowband pulsers described earlier to produce a severe threat for commercial equipment and systems. Further, this recommended practice estimates the peak electric field times range product to be 5.0 MV for narrowband threats.

For the wideband threat, the high-tech simulator JOLT can produce the peak wideband electric field times range product of 5.0 MV, which this recommended practice consider a severe threat for commercial equipment and systems.

For both cases (narrowband and wideband), this recommended practice estimates that a moderate EM threat will have a peak electric field times range product of 0.5 MV (10 times smaller in level). This information is needed to determine the level of field that can be produced at the location of the equipment of interest once a range is determined.

Once an electric field arrives at the location of the equipment, for frequencies in the range of 1 GHz and typical lengths of cables inside a building, it is expected that the common mode voltages coupled to cable shields or bundles vary depending on the angle of incidence of the electric field and its polarization. The ratio of the peak induced voltage and the peak incident electric field varies between 0.5 V/m and 1.5 V/m [B31]. For this reason, the selection of a ratio of 1.0 provides a reasonable factor for converting the incident volts per meter to volts induced.

In terms of directly injected voltage pulses, pulsers have been built that can inject several hundred kilovolt pulses, although typically with rise times of roughly 1 μ s (for lightning testing). Pulsers have been developed up to 100 kV with rise times of 10 ns, which could be used to inject high levels of IEMI conducted threats into a building on the power or communications lines. This recommended practice considers a 100-kV peak voltage with a 10 ns rise time to be a severe threat and 20 kV to be a moderate threat.

4.5.2 Summary of equipment susceptibility levels

For radiated field threats to electronic equipment, given a large but incomplete set of test data, it appears that for narrowband EM fields, the onset of upsets of electronics begins around 500 V/m. The database for permanent damage is sparse, but it appears to begin around 1 kV/m for some types of electronic systems. These levels do not include in-band jamming impacts, which occur at much lower levels.

For wideband radiated EM fields with pulse widths less than 10 ns, the onset of upset is around 2 kV/m with damage beginning at about 4 kV/m. Note that the damage levels are about four times higher for wideband than narrowband fields, due primarily to the fact that the number of peaks produced by narrowband fields is significantly higher in a short time frame than for wideband fields. On the other hand, the upset susceptibility levels for wideband fields with repetitive pulses are nearly the same as narrowband radiated fields.

For wideband common mode conducted susceptibility of equipment, a significant amount of data indicate upsets beginning in the 2 kV range, and damage in the 4 kV range for pulses with a rise time of 5 ns. There are much less data for narrowband common mode conducted susceptibility, although there are indications that networked electronics (e.g., Internet switches) have failed due to the cable voltages coupled by the incident EM fields. Analyses can extract an estimated level of 500 V at frequencies near 1 GHz creating the onset of upset. A factor of two higher level (1 kV) could create damage.

5. Types of equipment and systems to be protected

The scope of this recommended practice is to include all electronic equipment and systems containing a microprocessor that are placed in fixed locations. The reason for this scope is evidence that the microprocessor is extremely sensitive to malfunction from both narrowband and wideband transients at its input/output ports. In addition, mobile equipment is more difficult to protect due to the fact that only EM protection techniques can be applied at the equipment level, while in the case of fixed locations, protection and security measures at both the equipment and installation levels can be applied to reduce the possibility of malfunctions.

There are two general categories of equipment. The first general category involves remote locations where the public is usually present, but where there may not be anyone available to monitor the presence and actions of the public. The second general category includes dedicated computer facilities that usually limit access, but that allow visitors or tours nearby. This can provide an opportunity for a criminal to radiate the facility during a tour (e.g., with a briefcase pulser) or to apply a conducted IEMI threat to the building without detection by plugging in a pulser that may look like an ordinary piece of electronics. In general, if someone can access a position within 100 m of sensitive equipment, there is a significant threat to electronics.

Examples of types of equipment to be protected include:

- ATMs and other kiosks
- Point-of-sale terminals in shopping areas
- Computers used in business and factory applications
- Medical equipment that monitors the health of patients
- Electronic voting equipment
- Electronic control equipment for transportation applications (streetlight controls, railway traffic controls, aircraft control towers, etc.)
- Power system control electronics

- Bank and other financial computer systems
- Stock market computer systems
- Internet hub computer systems
- Telephone central office computer systems
- Water distribution computer systems

6. Protection methods

6.1 Protection approaches

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, this recommended practice provides a more detailed discussion of EM protection measures.

6.2 Security approach

From a security point of view, many normal security measures can reduce the threat of IEMI, especially for dedicated computer rooms:

- Develop a keep out or buffer zone around critical systems.
- Prevent unauthorized access to all power and communications cables entering a building.
- Keep important internal equipment away from the outer walls of the installation.
- Use redundancy and diverse routing for important wiring inside the installation.
- Make IEMI-protected backup power available for all critical operations.

The purpose of most of these actions is to increase the distance between a concealed portable EM weapon and the most critical computer systems and to provide redundancy in case of limited malfunctions. In addition, attention must be paid to the external penetrations into an installation to ensure that conducted IEMI threat waveforms cannot be injected easily into the power and telecom penetrations.

6.3 Electromagnetic approach

The following generic IEMI protection measures can be part of an EM shielding and penetration protection approach:

- Provide EM shielding around critical equipment.
- Provide surge protection and filters for metallic cables used in critical operations.
- Use non-metallic fiber optic cables when possible.
- Employ methods to decrease the resonance characteristics of critical equipment enclosures.
- Use fault-tolerant software in critical operations.

- Develop a verification program to periodically test the immunity of the system and its installation.

Subclauses 6.3.1 through 6.3.5 provide additional details concerning these generic measures.

6.3.1 Shielding

It is well established that topological techniques can be applied to provide complete EM shielding [B29]. Relying on qualitative topology, one can utilize conductors (e.g., metal sheets, braids) as shields for an equipment enclosure and for cable 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 a building and to shield that equipment in a small room or in shielded racks.

6.3.2 Penetration control for metallic cables and the use of fiber optics

If there are to be electrical connections (e.g., antennas, communication lines, power lines) to the outside world, then these penetrate the EM shields and allow the external environment to penetrate inside with little attenuation. Such penetrations shall be controlled. This is especially true in the case of ubiquitous metallic Ethernet cables. Ferrites, surge arresters, and/or filters will likely be needed to reduce the high-level and generally fast IEMI disturbances, and the high-frequency grounding of these protective elements is crucial. Inside a building, the use of fiber optic cables (without metallic cladding or internal conductors) can also be advantageous as long as they are properly inserted through room and/or rack shields using appropriate waveguides below cutoff.

6.3.3 Resonance reduction

Because resonances in transfer functions to the interior of equipment enclosures can be exploited in IEMI (especially for narrowband waveforms), it is useful to reduce their effects. 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 [B2]. Viewed another way, such resonance loading provides some places for the interfering energy to be absorbed, instead of in critical circuits.

6.3.4 Fault-tolerant computation

Because digital equipment is subject to upset (i.e., change in logic states), redundancy in the form of error detection and correction should be designed. This makes the system less susceptible. The design should also account for the possibility that the IEMI environment may be repetitive at rates up to the megahertz range.

6.3.5 Qualification of protective measures and periodic verification

It is well established that the best designs for EM protection for equipment, systems, and installations may not be properly installed or may be incomplete. Usually, the only way to determine this is to perform a realistic qualification test that covers the main aspects of the threat environment. For the case of applying EM protection to a single piece of equipment, the IEEE and the IEC provide well-defined test methods. For the case of IEMI threats, the levels of narrowband and wideband threats will need to be increased beyond the levels normally applied for EMC. These recommendations are provided in Clause 8.

For cases in which equipment may be placed inside of a shielded rack, tests should be performed on the rack to ensure that the shielding effectiveness of the enclosure meets the desired specifications and that the penetration control for cables is acceptable. This type of testing can be performed at lower levels, with external and internal measurements being performed to ensure that the proper attenuation is achieved (e.g., IEEE Std 299™-2006 [B18] and IEEE 299.1™-2013 [B19]). This testing should be performed with the final operational configuration. In addition, any time there is a change in the equipment inside of the rack, the tests should be performed again. Finally, if no changes are made, there is still a need to perform periodic verification tests over time to ensure that the shielding and the penetration control has not degraded over time. It is noted that the minimum frequency range for these tests is from 100 MHz to 3 GHz, although frequencies as high as 10 GHz may be of interest in special radiated cases. For conducted transients, tests should be performed for frequencies between 100 kHz and 1 GHz.

If a protection approach is applied to shield an entire building or a portion of a building through the construction of a shielded room, then a test program should be developed and performed to ensure that the shielded room meets the design requirements. Low-level tests should be performed after the room construction is complete (including the penetration of wiring) to ensure that the desired shielding effectiveness is present (e.g., IEEE Std 299-2006 [B18] and IEC 61000-4-23 [B13]). As in the case of shielded racks, periodic verification of the shielding effectiveness should be performed using low-level EM tests. The same frequency range as recommended for shielded racks should be applied at the building level.

7. Monitors and alarms

The inclusion of special EM detectors that sense the presence of an IEMI environment should be considered. This can be useful to counteract the impact of repetitive IEMI threat waveforms that create malfunctions. With these detectors, the reason for the problems can be quickly ascertained and security personnel can use hand-held detectors to find the location of the threat. In addition, it is possible to use detectors with a critical system in order to command the system to take appropriate action, such as repeating certain computations that may have been made in error by the interference or to power down and restart.

The requirements for radiated detectors should include the ability to detect CW signals above 100 V/m in the frequency range of 100 MHz to 3 GHz. For pulsed radiated waveforms, peak fields of 1000 V/m and higher should be detected with the ability to capture wideband waveforms with pulse widths greater than 200 ps. Both installed and mobile detectors are of value for radiated waveforms, as the fixed detectors could be placed in the vicinity of critical equipment while mobile detectors could be used by security personnel to determine the locations of interference sources. Figure 10 shows an example of a mobile detector.

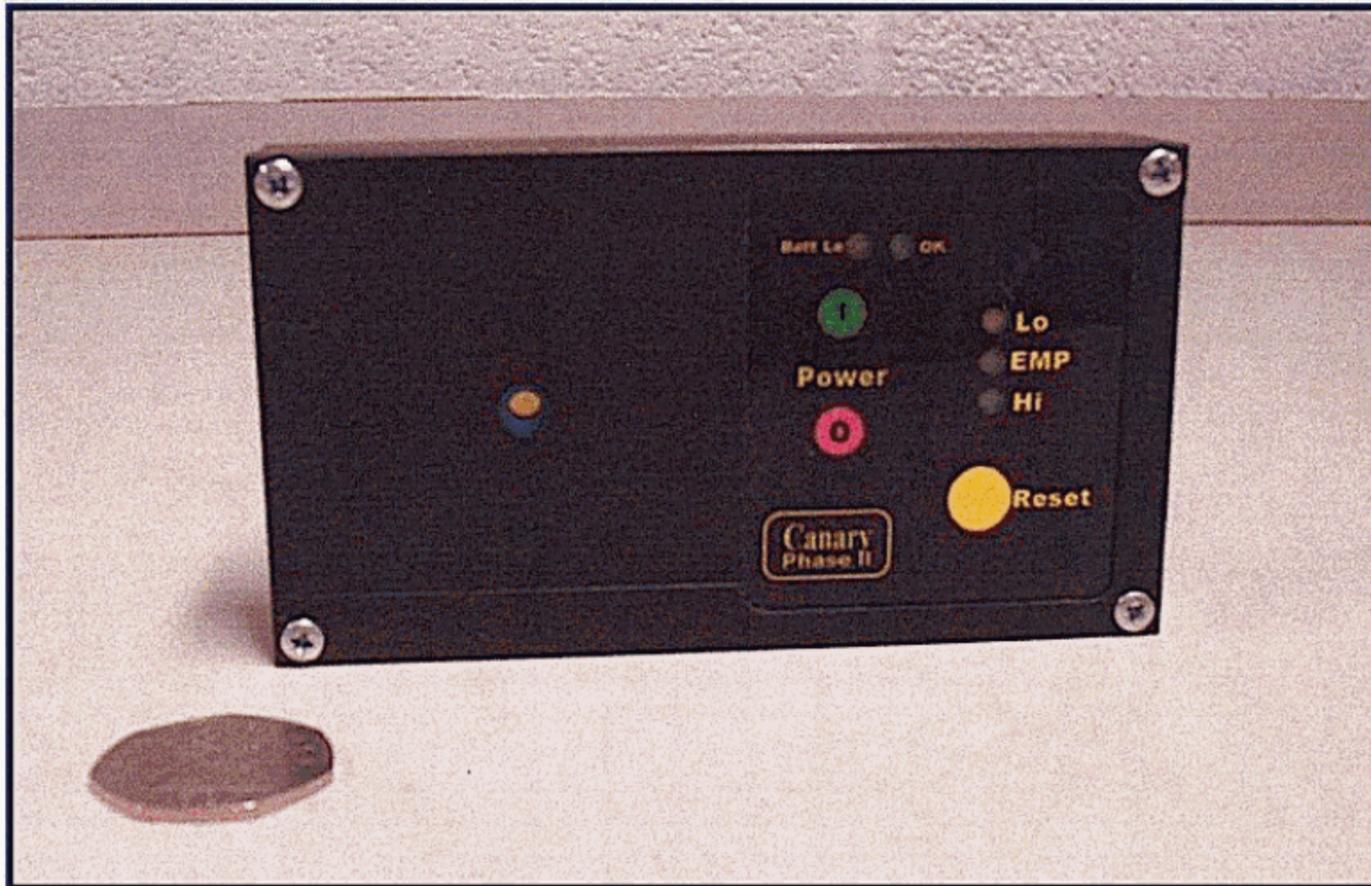


Figure 10—Example of IEMI hand-held mobile detector

It is necessary to note that the main characteristics of radiated disturbances are pulse average power and pulse frequency rate. Therefore, the detectors of radiated disturbances should also be capable of registering these characteristics.

Conducted detectors would require a frequency range between 100 kHz and 1 GHz for continuous waveforms and would be installed on the wiring leading into a critical system or equipment. For pulsed waveforms, pulse widths of 1 ns and longer should be detectable, with a peak detectable level of 4 kV and higher.

When there is a necessity to protect data links, then the detectors of conducted disturbances should register periodically repeating voltage pulses in power cables (or information lines) with a level of tens of volts and higher. Detectors should measure the pulse average power and pulse frequency rate. With reference to power cables, the detector should register disturbances between a phase wire and the case of the equipment in the data transmission system.

As in the case of detectors of radiated disturbances, the detectors of conducted disturbances should have an adjustable threshold level. When disturbances are higher than the threshold level, then the corresponding signals should move to emergency protection devices that provide time interruption of the system work or the changing of an operating mode, or other protection methods.

In addition to the abovementioned applications, conducted detectors may also be used to determine the conducted EM environment in critical systems by examining the injection of pulse disturbances in the power network of a building, both outside and inside of the building. The received data may be used in order to strengthen the protection (if necessary) by using security methods or EM attenuation methods.

8. Recommended protection approach

As indicated in this recommended practice, radiated threats are produced from EM weapons whose fields decrease as $1/r$ with range. In 4.5, the threat levels of severe and moderate have been defined for both narrowband and wideband radiated EM threats. The process to be followed for these EM radiated field threats is:

- a) Determine the class of the weapon (severe or moderate or both) (4.5.1).
- b) Determine the type of EM threat (narrowband or wideband or both) (4.2).
- c) Determine the closest location for a weapon to be placed without arousing suspicion (by inspection).
- d) Determine the location of the critical electronics inside the building and the range from the closest location of the EM weapon [by inspection and by calculation using the result from step c)],
- e) Determine the total shielding effectiveness of the building and/or rooms containing the critical electronics (from the location of the weapon to the location of the critical electronics) (9.3).
- f) Compute the EM field in the room of interest (at the location of the critical electronics) for each threat case [using the rE_{peak} value from step a) and step b) and the range from step d)].
- g) Estimate the common mode coupling of the radiated fields to cables in the room (where the critical electronics are located) connecting the electronics (4.5.1).
- h) Collect susceptibility data for critical equipment from published papers (4.3 and 4.4) or perform equipment testing by injection to determine upset and damage levels (9.1).
- i) Compare the estimated radiated fields and the coupled voltages to the radiated and conducted common mode susceptibility levels for the same type of waveform (narrowband or wideband) [step g) and step h)].
- j) Determine the amount of additional EM shielding (in the walls or around the cables) or cable point of entry surge protection and/or filtering required to reduce the estimated threat below the susceptibility level of the equipment (6.3), and/or consider IEMI monitors or alarms to determine when attacks are underway (Clause 7).

For injected conducted EM threats, the process is different in that efforts should be made to eliminate external access points where a criminal or terrorist could connect a pulser to wiring that enters the building. This is because the injected voltages and/or currents will not attenuate very much with distance, and trying to protect at the equipment level would be extremely difficult and expensive due to the high levels of induced voltages and the amount of equipment exposed. Normal security measures, including preventing physical access to the cable entries (through burial or fencing with security measures) and video monitoring of those points, should be sufficient. If access cannot be limited, it would be important to provide filtering or surge protection immediately inside the building for these outside cable entry points. A final possibility would be to connect monitoring equipment to these lines to determine if IEMI disturbances are being injected into an external cable.

9. Test methods

9.1 Equipment-level test methods

While typical levels of IEMI susceptibility have been determined for modern computer systems, it may be important in some cases to test critical equipment to determine its specific susceptibility to fast EM waveforms (testing is performed by slowly raising the peak level until malfunctions occur). Tests similar to those used by the IEEE and the IEC for EMC purposes can be performed to ensure that equipment will

perform when exposed to IEMI threats without additional rack- or building-level protection. CW radiated and conducted threats should be applied as well as ESD, EFT, and HEMP-like pulsed waveforms for radiated and conducted threats. The recommended levels are expected to be considerably higher than those required for EMC immunity. Two of the most comprehensive immunity equipment test standards for high-level pulsed transients are IEC 61000-4-25 [B14] and IEC 61000-6-6 [B15]. While these standards deal strictly with HEMP, they provide a complete strategy for developing and applying test waveforms to equipment for external EM pulses with rise times on the order of a few ns and with pulse widths on the order of 20 ns.

9.2 Rack-level test methods

Radiated and conducted shielding effectiveness tests are recommended to evaluate the reduction of the external threats to manageable levels for the computer equipment inside a rack. Several test methods have been defined by the IEEE and the IEC for these cases (e.g., IEEE Std 299-2006 [B18] and IEC 61000-4-23 [B13]). The test levels are not at threat level but are instead set at a CW field level consistent with the ability to measure small signals inside the rack to develop a transfer function versus frequency.

9.3 Building-level test methods

Radiated and conducted shielding effectiveness tests are recommended to evaluate the reduction of the external building threats to manageable levels for the computer equipment inside the building. Several test methods have been defined by the IEEE and the IEC for these cases (e.g., IEEE Std 299-2006 [B18] and IEC 61000-4-23 [B13]). Also, Savage et al. have described a new approach to reduce the time and cost of making low-level CW measurements that involves the use of radio transmitters in bands between 1 MHz and 2 GHz [B34]. This method involves taking measurements using plane wave commercial radio signals outside and inside of a building and using these data to evaluate the effectiveness of the building wall in reducing any type of IEMI signal.

Annex A

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Bäckström, M., “HPM testing of a car: A representative example of the susceptibility of civil systems,” Workshop W4, *Proceedings of the 13th International Zurich Symposium and Technical Exhibition on EMC*, pp. 189–190, Feb. 1999.

[B2] Baum, C. E., and D. P. McLemore, “Damping transmission-line and cavity resonance,” *Proceedings of the 12th International Zurich Symposium on EMC*, pp. 239–244, 1999.

[B3] Fortov, V., V. Loborev, Y. V. Parfenov, W. Radasky, V. Sisranov, and B. Yankovskii, “Estimation of pulse electromagnetic disturbances penetrating into computers through building power and earthing circuits,” *Proc. Int. Symp. High-Power Electromagnetics, (EUROEM)*, Edinburgh, UK, 2000.

[B4] Fortov, V., Y. V. 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*, Feb. 2001.

[B5] Gardner, R. L., “Electromagnetic terrorism. A real danger,” *Proceedings of the XIth Symposium on Electromagnetic Compatibility*, Wroclaw, Poland, June 1998.

[B6] Giri, D. V., and F. Tesche, “Classification of intentional electromagnetic environments (IEME),” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 322–328, Aug. 2004.

[B7] Hoad, R., N. J. Carter, D. Herke, and S. P. Watkins, “Trends in EM susceptibility of IT equipment,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 390–395, Aug. 2004.

[B8] Hoad, R., N. J. Carter, D. Herke, S. P. Watkins, and A. Wraight, “An investigation into radiated susceptibility of IT networks,” *Conference Proceedings of EMC Europe*, Eindhoven, The Netherlands, Sept. 2004.

[B9] Hoad, R., and I. Sutherland, “The forensic utility of detecting disruptive electromagnetic interference,” *ECIW 2007: The 6th European Conference on Information Warfare and Security*, Defence College of Management and Technology, Shrivenham, UK, July 2–3, 2007.

[B10] IEC 61000-2-13 ed1.0 (2005), Electromagnetic compatibility (EMC) - Part 2-13: High-power electromagnetic (HPEM) environments - Radiated and conducted.⁴

[B11] IEC 61000-4-3 ed3.2 (2010), Electromagnetic compatibility (EMC) – Part 4.3: Testing and measurement techniques- Radiated, radio-frequency, electromagnetic field immunity test.

[B12] IEC 61000-4-5 ed3.0 (2014), Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques- Surge immunity test.

[B13] IEC 61000-4-23 ed1.0 (2000), Electromagnetic compatibility (EMC) - Part 4-23: Testing and measurement techniques - Test methods for protective devices for HEMP and other radiated disturbances.

[B14] IEC 61000-4-25 ed1.0 (2001), Electromagnetic compatibility (EMC) - Part 4-25: Testing and measurement techniques - HEMP immunity test methods for equipment and systems.

⁴ IEC publications are available from the International Electrotechnical Commission (<http://www.iec.ch/>). IEC publications are also available in the United States from the American National Standards Institute (<http://www.ansi.org/>).

- [B15] IEC 61000-6-6 ed1.0 (2003), Electromagnetic compatibility (EMC) - Part 6-6: Generic standards - HEMP immunity for indoor equipment.
- [B16] IEC/TR 61000-1-5 ed1.0 (2004), Electromagnetic compatibility (EMC) - Part 1-5: General = High power electromagnetic (HPEM) effects on civil systems.
- [B17] IEC/TR 61000-2-5 ed2.0 (2011), Electromagnetic compatibility (EMC) - Part 2-5: Environment - Description and classification of electromagnetic environments.
- [B18] IEEE Std 299-2006, IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures.^{5,6}
- [B19] IEEE Std 299.1™-2013, IEEE Standard Method for Measuring the Shielding Effectiveness of Enclosures and Boxes Having all Dimensions between 0.1 m and 2 m.
- [B20] “Joint Special Issue on the Nuclear Electromagnetic Pulse,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 20, no. 1, Feb. 1978.
- [B21] “Joint Special Issue on High Power Microwaves,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 34, no. 3, Aug. 1992.
- [B22] Månsson, D., “Response of Civilian Facilities and Systems to High Power Electromagnetic (HPEM) Pulses and the Threat of Intentional Electromagnetic Interference (IEMI).” Ph.D. diss., Uppsala University, 2006.
- [B23] Merritt, I. W., 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, Feb. 25, 1998.
- [B24] Messier, M. A., K. S. Smith, W. A. Radasky, and M. J. Madrid, “Response of telecom protection to three IEC waveforms,” *Zurich EMC Conference*, pp. 127–132, Feb. 2003.
- [B25] Parfenov, Y. V., I. Kohlberg, W. A. Radasky, B. A. Titov, and L. N. Zdoukhov, “The probabilistic analysis of immunity of a data transmission channel to the influence of periodically repeating voltage pulses,” *Proc. 1st Asia-Pacific Symposium on EMC*, 2008.
- [B26] Parfenov, Y. V., L. Zdoukhov, and W. Radasky, “Research concerning the influence of ultrawideband (UWB) electromagnetic fields on electronic cash machines,” 2002.
- [B27] Parfenov, Y. V., L. Zdoukhov, W. Radasky, and M. Ianoz, “Conducted IEMI threats for commercial buildings,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 404–411, Aug. 2004.
- [B28] Prather, D. P., C. E. Baum, R. J. Torres, F. Sabath, and D. Nitsch, “Survey of worldwide high power wideband capabilities,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 335–344, Aug. 2004.
- [B29] Radasky, W. A., C. E. Baum, and M. W. Wik, “Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI),” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 31–321, Aug. 2004.
- [B30] Radasky, W. A., M. A. Messier, and M. W. Wik, “Intentional electromagnetic interference (EMI) – Test and data implications,” *Zurich EMC Symposium*, Feb. 2001.
- [B31] Radasky, W., K. Smith, and J. Gilbert, “The sensitivity of coupling of IEMI waveforms to cables,” *AMEREM Conference*, Ottawa, Canada, July 7, 2010.
- [B32] Rosenberg, E., “New Face of Terrorism: Radio-Frequency Weapons,” *New York Times*, June 23, 1997.
- [B33] Sabath, F., M. Bäckström, B. Nordström, D. Sérafin, A. Kaiser, B. A. Kerr, and D. Nitsch, “Overview of four European high-power microwave narrow-band test facilities,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 329–334, Aug. 2004.

⁵ The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

⁶ IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

- [B34] Savage, E. B., J. L. Gilbert, W. A. Radasky, and M. J. Madrid, "An alternative EM shielding effectiveness measurement method for buildings," *2010 Asia-Pacific International Symposium on Electromagnetic Compatibility*, Beijing, China, April 12–16, 2010.
- [B35] Savage, E. B., K. S. Smith, M. J. Madrid, J. L. Gilbert, and W. A. Radasky, "Fast pulse testing of power system control equipment to determine their susceptibility to HEMP conducted transients," *Proceedings of the 16th International Zurich Symposium on EMC*, Zurich, Switzerland, pp. 377–380, Feb. 2005.
- [B36] Sawyer, D., "Non-lethal Weapons," *20/20*, American Broadcasting Company (ABC), February 10, 1999.
- [B37] Siniy, L., V. E. Fortov, and Y. V. Parfenov, "Russian research of intentional EMI disturbances over the past 10 years," *AMEREM 2006*, Albuquerque, New Mexico, USA, July 2006.
- [B38] "Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, Aug. 2004.
- [B39] *The Sunday Times*, "City surrenders to £400m gangs," London, June 2, 1996.
- [B40] United States Department of Homeland Security, "The Threat of Radio Frequency Weapons to Critical Infrastructure Facilities," TSWG and DTEO Publications, August 2003.
- [B41] Wik, M. W., R. L. Gardner, W. A. Radasky, "Electromagnetic Terrorism and Adverse Effects of High Power Electromagnetic Environments," Workshop W4, 13th International Zurich Symposium and Technical Exhibition on EMC, February 1999, pp. 181-185.

Consensus

WE BUILD IT.

Connect with us on:



Facebook: <https://www.facebook.com/ieeesa>



Twitter: @ieeesa



LinkedIn: <http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118>



IEEE-SA Standards Insight blog: <http://standardsinsight.com>



YouTube: IEEE-SA Channel