IEEE STANDARDS ASSOCIATION

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
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1642™-2015

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

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

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

Photocopies

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

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

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.