International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

K.81

(08/2014)

SERIES K: PROTECTION AGAINST INTERFERENCE

High-power electromagnetic immunity guide for telecommunication systems

Recommendation ITU-T K.81

Recommendation ITU-T K.81

High-power electromagnetic immunity guide for telecommunication systems

Summary

In an information security management system (ISMS) based on Recommendation ITU-T X.1051 and ISO/IEC Standards 27001 and 27002, physical security is a key issue. The electromagnetic interference caused by a high-power electromagnetic (HPEM) attack and the ability to intercept information due to unintentional electromagnetic emissions of equipment are significantly determined by the applied physical security measures.

When information security is managed, it is necessary to evaluate and mitigate the threat to either the equipment or the site. This threat is related to "vulnerability" and "confidentiality" in ISMS.

Recommendation ITU-T K.81 presents guidance on establishing the threat level presented by an intentional HPEM attack and the physical security measures that may be used to minimize this threat. The HPEM sources considered are those presented in IEC 61000-2-13, as well as some additional sources that have emerged more recently.

Recommendation ITU-T K.81 also provides information on the vulnerability of equipment. The equipment is assumed to meet the immunity requirements presented in Recommendation ITU-T K.48 and relevant resistibility requirements, such as those described in Recommendations ITU-T K.20, ITU-T K.21 and ITU-T K.45.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T K.81	2009-11-29	5	11.1002/1000/10018
2.0	ITU-T K.81	2014-08-29	5	11.1002/1000/12287

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T K.81

High-power electromagnetic immunity guide for telecommunication systems

1 Scope

This Recommendation presents guidance on:

- establishing the threat level presented by an intentional high-power electromagnetic (HPEM) attack on an electronic device or system;
- the physical security measures that may be employed to reduce this threat level;
- establishing the vulnerability of the equipment (or system) to be protected from a HPEM attack.

When establishing detailed countermeasures to HPEM attacks, it is extremely important that the threat level (strength) of the attack be adequately estimated. Underestimation means that the applied countermeasures will be insufficient and hence increases the risk that equipment may malfunction; whereas overestimation means that the applied countermeasures may add significant (and unnecessary) cost to the equipment or system.

Estimation of the threat level (strength) is calculated using sources such as the IEC Standards, as well as the independent market studies performed during the preparation of this Recommendation.

The vulnerability of the electronic device (or system) to be protected is based on either an assessment of the standards that the electronic device (or system) satisfy, or the results of independent evaluation (i.e., testing) of a sample device.

The threat and vulnerability levels considered within this Recommendation reflect the technology levels current as of 2012. Hence, it is expected that this Recommendation will require periodic review in the light of ongoing technological change in order to remain current.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T K.20] Recommendation ITU-T K.20 (2011), *Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents*.

[ITU-T K.21] Recommendation ITU-T K.21 (2011), *Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents*.

[ITU-T K.42] Recommendation ITU-T K.42 (1998), *Preparation of emission and immunity requirements for telecommunication equipment – General principles*.

[ITU-T K.43] Recommendation ITU-T K.43 (2009), *Immunity requirements for telecommunication network equipment*.

[ITU-T K.44] Recommendation ITU-T K.44 (2012), *Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation*.

[ITU-T K.45] Recommendation ITU-T K.45 (2011), *Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents*.

[ITU-T K.48] Recommendation ITU-T K.48 (2006), *EMC requirements for telecommunication equipment – Product family Recommendation*.

[ITU-T K.66] Recommendation ITU-T K.66 (2011), *Protection of customer premises from overvoltages*.

[IEC 61000-2-13] IEC 61000-2-13 (2005), *Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted*.

[IEC CISPR 24] CISPR 24 (2010), *Information technology equipment – Immunity characteristics – Limits and methods of measurement*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 availability [b-ISO/IEC 27002]: Ensuring that authorized users have access to information and associated assets when required.

3.1.2 emanation [b-IETF RFC 2828]: A signal (electromagnetic, acoustic, or other medium) that is emitted by a system (through radiation or conductance) as a consequence (i.e., by-product) of its operation, and that may contain information. (See: TEMPEST.)

3.1.3 integrity [b-ISO/IEC 27002]: Safeguarding the accuracy and completeness of information and processing methods.

3.1.4 TEMPEST [b-IETF RFC 2828]: A nickname for specifications and standards for limiting the strength of electromagnetic emanations from electrical and electronic equipment and thus reducing vulnerability to eavesdropping.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 confidentiality: Ensuring that information is accessible only to those authorized to have access. Information leakage due to insufficient electromagnetic emanations security (EMSEC) is a risk to this confidentiality. In this Recommendation, if the equipment cannot be EM mitigated itself, the emission values of existing electromagnetic compatibility (EMC) requirements indicate the level of this confidentiality.

3.2.2 EM mitigation: The preparations made to avoid either:

- a malfunction due to a vulnerability caused by high-altitude electromagnetic pulses (HEMP) or high-power electromagnetic (HPEM) emissions, or
- a lack of confidentiality due to an insufficient electromagnetic emanations security (EMSEC).

The level of the EM mitigation of the equipment can be calculated from the threat level and the vulnerability level.

3.2.3 electromagnetic emanations security (EMSEC): Physical constraints to prevent information compromise through signals emanated by a system, particularly the application of TEMPEST technology to block electromagnetic radiation.

In this Recommendation, EMSEC means only information leakage due to unintentional electromagnetic emission.

3.2.4 threat: A potential security violation that arises from taking advantage of a vulnerability caused by high-altitude electromagnetic pulses (HEMP) or high-power electromagnetic (HPEM) emissions, and which could lead to a lack of confidentiality due to insufficient electromagnetic emanations security (EMSEC). The level of a HPEM threat is defined by the intrusion area, the portability and the availability but also by the strength of the electromagnetic field.

3.2.5 vulnerability: The possibility that the equipment does not function correctly when exposed to HEMP or HPEM.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AM Amplitude Modulation

ASP Application Service Provider

CB Citizen Band

CSP Contents Service Provider

CW Continuous Wave

DB Database

DC Direct Current

EM Electromagnetic

EMC Electromagnetic Compatibility

EMSEC EM emanations Security

ERP Enterprise Resource Planning

FET Field Effect Transistor

FM Frequency Modulation

FTP File Transfer Protocol

GTEM Gigahertz Transverse Electromagnetic

HEMP High-altitude EM Pulse

HF High Frequency

HPEM High Power EM

IGBT Insulated Gate Bipolar Transistor

IP Internet Protocol

IRA Impulse Radiating Antenna

ISMS Information Security Management System

ISP Internet Service Provider

IT Information Technology

LAN Local Area Network

MSP Management Service Provider

NEBS Network Equipment Building Systems

PC Personal Computer

SE Shield Effect

TCP Transfer Control Protocol

VSWR Voltage Standing Wave Ratio

5 Threat evaluation

In order to evaluate a threat, it is necessary to consider its:

- portability level;
- intrusion areas, and
- availability level.

5.1 Definitions of threat portability levels

This Recommendation defines the four levels of threat portability presented in Table 1.

Table 1 – Definitions of threat portability levels

Threat portability level	Definition
PI	Pocket-sized or body-worn (Note 1)
PII	Briefcase or backpack sized (Note 2)
PIII	Motor-vehicle sized (Note 3)
PIV	Trailer-sized (Note 4)
NOTE 1 – This portability level applies to threat devices that can be hidden in the human body and/or in clothing. NOTE 2 – This portability level applies to threat devices that are too large to be hidden in the human body and/or in clothing, but that are still small enough to be carried by a person (such as in a briefcase or a back-pack). NOTE 3 – This portability level applies to threat devices that are too large to be easily carried by a person, but small enough to be hidden in a typical consumer motor vehicle. NOTE 4 – This portability level applies to threat devices that are too large to be either easily carried by a person or hidden in a typical consumer motor vehicle. Such threat devices require transportation using a commercial/industrial transportation vehicle.	

5.2 Definition of the intrusion area

This Recommendation recognizes the concept of intrusion area. This concept indicates both:

- the portability levels of threat device(s) that may be present;
- the typical minimum separation distance that may be achieved between the threat device and the electronic equipment to be protected.

The concept of intrusion area is depicted in Figure 1 and summarized in Table 2.

Intrusion area Zone 0 applies to the public spaces surrounding the site or building that houses the equipment to be protected. Within this area, people and vehicles are free to move in accordance with local legal requirements (i.e., the owner of the equipment to be protected has no ability to control the movement of people and/or vehicles). Hence, Zone 0 can contain threat devices of all the portability levels defined in Table 1. The typical minimum separation between the threat devices located in this zone and the equipment to be protected is between ~ 100 m and ~10 m. The higher figure is associated with situations in which the equipment to be protected is situated inside a building that is surrounded by a site where access is controlled. The lower figure is associated with situations in which the

equipment to be protected is situated inside a building that is surrounded by a public space. This applies to buildings located in urban centres, where the building may be surrounded by publicly accessible streets.

Intrusion area Zone 1 applies to locations within the same site that houses the equipment to be protected. It is recommended that physical security be applied at the site entrance, such that vehicular access to the site is controlled. Hence it is presumed that Zone 1 will not contain threat devices of portability levels PIII and PIV, i.e., that anything trailer-sized will not be admitted and smaller vehicles will be left at a visitor car park. It is recommended that the location of the visitor car park be considered as part of the site physical security plan. A visitor car park located outside the site perimeter, near to the entrance will maximize the separation of any threat of portability levels PIII and PIV and the equipment to be protected. If the visitor car park is to be located within the site boundary, it should be situated as far as possible from the equipment to be protected. The typical separation between the threat devices located in this zone and the equipment to be protected is between 10 m and 100 m.

Intrusion area Zone 2 applies to locations within the same building that house the equipment to be protected. It is recommended that physical security be applied at the site entrance, such that vehicular access to the site is controlled. This means that Zone 2 will not contain threat devices of portability levels PIII and PIV, i.e., that anything trailer-sized will not be admitted and smaller vehicles will be left at a visitor car park. It is further recommended that physical security be applied to prevent access to the room containing the equipment under protection. Hence, the typical minimum separation between the threat devices located in this zone and the equipment to be protected is between 1 m and 10 m.

Intrusion area Zone 3 applies to locations within the same room that houses the equipment to be protected (i.e., the equipment room). It is recommended that physical security be applied at the site entrance, such that vehicular access to the site is controlled. This means that Zone 3 will not contain threat devices of portability levels PIII and PIV, i.e., that anything trailer-sized will not be admitted and smaller vehicles will be left at a visitor car park. It is further recommended that physical security be applied to control access to the room containing the equipment to be protected. This physical security means that all types of briefcases and backpacks should be surrendered to a security guard before access to the room is granted. Additional physical security measures are also recommended: visitors to the equipment room shall be asked to empty the content of their pockets and/or undergo some additional screening (such as via a metal detector) before access is granted. Hence, the typical minimum separation between the threat devices located in this zone and the equipment to be protected is between 0 m and 1 m.

Hence, it is necessary for the owner of the equipment to be protected to review the intended (or actual) location of the equipment and develop a physical security protocol that controls the ability of threat devices to be taken near to the equipment to be protected.

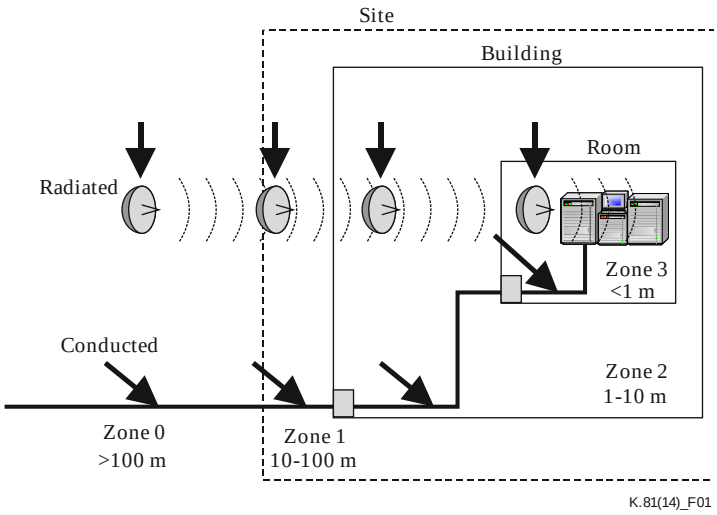


Figure 1 – Classification of intrusion areas

Table 2 – Intrusion area and portability levels

Intrusion area	Threat device location	Threat device portability levels (Note)	Typical minimum separation distance (m)
Zone 0	Public space	PI, PII, PIII, PIV	> 100
Zone 1	Same site	PI, PII	100 – 10
Zone 2	Same building	PI, PII	10 – 1
Zone 3	Same room	PI, PII	< 1
NOTE – The portability level of the threat devices that may be located in each intrusion zone is determined by the physical security measures applied.			

5.3 Definition of threat availability levels

This Recommendation recognizes the four threat availability levels (AI to AIV) presented in Table 3. The threat availability level shall be thought of as a measure of both the cost and the technological sophistication of the threat device:

Table 3 – Definitions of threat availability levels

Availability level	Definition	Examples
AI	'Consumer'	Wireless local area network (LAN) device, stun-gun, illegal citizen band (CB) radio
AII	'Hobbyist'	CW generator, amateur wireless device
AIII	'Professional'	Navigation radar
AIV	'Bespoke'	Impulse radiating antenna (IRA), JOLT, commercial radar

5.4 Examples of threat devices

Examples of threat devices for which the assessment is described in clauses 5.1, 5.2 and 5.3 are summarized in Table 4. The basis of the data presented is given in Appendix I.

Table 4 – Example of threats related to high-power electromagnetic waves

Threat type	Example of attack device	Intrusion range on attack side	Strength	Frequency range	Porta-bility	Availa-bility	Threat number
Electroma-gnetic wave attack – Radiated	JOLT	Zone 0	72 kV/m@100 m	50 MHz-2 GHz	PIV	AIV	K1-0
	IRA (Hi-tech)	Zone 0	12.8 kV/m@100 m	300 MHz-10 GHz	PIV	AIV	K1-1
	Commercial radar (Mid-tech)	Zone 0	60 kV/m@100 m	1 GHz-10 GHz (1.285 GHz)	PIV	AIV	K1-2
	Navigation radar	Zone 0	385 V/m@100 m	1 GHz-10 GHz (9.41 GHz)	PIII	AIII	K1-3
	Magnetron generator	Zone 1	475 V/m@10 m	1 GHz-3 GHz	PIII	AII	K1-4
	Amateur wireless device	Zone 2	286 V/m@1 m	100 MHz-3 GHz	PII	AII	K1-5
	Amateur wireless device	Zone 3	169 V/m@10 cm	100 MHz-3 GHz	PI	AI	K1-6
	Illegal CB radio	Zone2	573 V/m@10 m	27 MHz	PII	AI	K1-7
Electrostatic discharge attack	Stun gun	Zone 3	500 kV	100 MHz-3 GHz	PI	AI	K2-1
Electroma-gnetic wave attack – Conducted	Lightning-surge generator	Zone 0	50 kV (charging voltage)	1.2/50 µs 10/700	PIV	AIV	K3-1
	Compact lightning-surge generator	Zones 0-3	10 kV (charging voltage)	1.2/50 µs 10/700	PII	AII	K3-2
	CW generator	Zones 0-3	100 V~240 V/4 kV	1 Hz-10 MHz	PII	AII	K3-3
	Commercial power supply	Zones 0-3	100 V~240 V	50/60 Hz	PI	AI	K3-4

6 Vulnerability of devices to be protected

6.1 Definition of vulnerability classifications

The immunity standards and the overvoltage standards shown in Table 5 and Table 6 have several differences with regard to the vulnerability levels of devices to be protected. Specific vulnerability levels are set for each of the standards. ZI1 to ZI3 indicates the vulnerability level with respect to immunity standards while ZK1 to ZK5 indicates the vulnerability level with respect to overvoltage standards. The differences are described in Appendix I.

In addition, the typical immunity level for routers servers obtained by testing is described in Table 7. This immunity level is comparable to results given in [ITU-T K.48].

Table 5 – Immunity standards and vulnerability levels

Vulnerability level	Standard	Target device	Remarks
ZI1	[IEC CISPR 24]	IT equipment	International Standard
ZI2	[ITU-T K.48]	Network equipment	Recommendation
ZI1	[ITU-T K.43]	Network equipment	Recommendation
ZI1	[b-NTT-TR 549001]	Network equipment	NTT
ZI1	[b-NEBS GR-1089]	Network equipment	US Standard
ZI3	NEBS LEVEL 3	Network equipment	US Standard

Table 6 – Overvoltage standards and vulnerability levels

Vulnerability level	Standard	Target device	Remarks
ZK1	[ITU-T K.20]	Network equipment	Recommendation
ZK2	[ITU-T K.21]	Terminal equipment	Recommendation
ZK3	[ITU-T K.66]	Communication device, network equipment	Recommendation
ZK4	[b-NEBS GR-1089]	Network equipment	US Standard
ZK5	NEBS LEVEL 3	Network equipment	US Standard

Table 7 – Immunity levels of typical IT devices

Type of EM emanation	Immunity level
Radiated electromagnetic field	3 V/m (actual field value) (Note)
Conducted voltage	3 V (actual voltage value) (Note)
Static discharge	8 kV (direct discharge)
Lightning surge	4 kV (power port – line to ground) 2 kV (communications port – line to ground)
NOTE – This immunity level corresponds to a carrier that is subjected to 80% amplitude modulation (AM) with a 1 kHz tone.	

6.2 Examples of vulnerability of various equipment types to be protected

An example of vulnerability of equipment to be protected will be described according to the classification definitions above. Many of the immunity standards were established several years ago and in the case of equipment with a long life expectancy such as telephone equipment, prognosis is difficult. Telephone line immunity and overvoltage vulnerability levels are shown in Table 9.

For IP equipment, various levels of vulnerability are identified in Table 10 that reflect the service level agreements (SLAs) that are offered commercially. Table 8 provides a description of the types of service provider. For a management service provider (MSP), it is assumed that the equipment is of network equipment building systems (NEBS) Level 3 ('carrier grade').

For PCs or the servers that are typically used, a general immunity level of ZI2, as shown in Table 11, is assumed. In the case of electromagnetic security, it is necessary to assume equipment having an immunity level of ZI1.

Examples of the vulnerability levels of various types of equipment to be protected are shown in Table 9, Table 10 and Table 11.

Table 8 – Type of service provider

Service provider	Description
Application service provider (ASP)	A provider that provides business application software to a customer via a network such as the Internet.
Contents service provider (CSP)	A provider that stores and distributes digital contents.
Internet service provider (ISP)	A provider that performs a service for connecting to the Internet.
Management service provider (MSP)	A provider that takes responsibility for operation, monitoring and maintenance of servers or networks belonging to a business.

Table 9 – Vulnerability level of telephone lines

Type	Immunity	Overvoltage
General public line	ZI1	ZK1
Dedicated line (general)	ZI1	ZK1
Dedicated line (fire department, police, etc.)	ZI1	ZK1

Table 10 – Vulnerability level of IP equipment (network service)

Type	General level (ISP, etc.)		Carrier grade (MSP, etc.)	
	Immunity	Overvoltage	Immunity	Overvoltage
Data centre (E-Commerce site)	ZI1	ZI1	ZI3	ZK5
Data centre (storage)	ZI1	ZI1	ZI3	ZK5
Router, switching	ZI1	ZI1	ZI3	ZK5

Table 11 – Vulnerability level of IP equipment (company network)

Type	Immunity	Overvoltage
PC	ZI2	ZI1
Mail server	ZI2	ZI1
Enterprise resource planning (ERP) server	ZI2	ZI1
Storage	ZI2	ZI1
Customer database (DB) server	ZI2	ZI1
Router, switch	ZI2	ZI1

7 Determination of EM mitigation levels

This clause presents general guidance for the determination of equipment EM mitigation levels and presents some examples.

7.1 General

The threat levels generated by a high power EM (HPEM) attack (described in clause 5) all exceed the vulnerability levels of protected devices (described in clause 6) and hence a HPEM attack will affect the device or system.

Given that the purpose of EM mitigation is to reduce the threat to a level equal to or below the vulnerability level of the device (or system), the required EM mitigation level is the margin between the threat level and the equipment's vulnerability level, given by:

$$\text{(EM mitigation level)} = \text{(Threat level)} - \text{(Vulnerability level)} \quad (1)$$

The shield effect (SE) is calculated in dB by:

$$SE = 20\log_{10}\{\text{(Threat level)}/\text{(Vulnerability level)}\} \quad (2)$$

Assuming:

- that the applied physical security protocol can restrict the threat devices to an availability level of no higher than AIII, and
- that the vulnerability level of general IT equipment is ZI2,

then the EM mitigation level that is required to be achieved via either shielding and/or filtering is as shown in Table 12 and the overvoltage mitigation level is as shown in Table 13.

Table 12 – Examples of the calculation of the required EM mitigation level of general IT equipment for a threat of AIII or less

Threat number	Threat strength (V)	Vulnerability (V)	EM mitigation level (dB)	Frequency/ waveform	Counter-measure location	EM mitigation achieved via
K1-3	385	3	43	1 GHz-10 GHz	Zones 0-3	Shielding
K1-4	475	3	44	1 GHz-3 GHz	Zones 1-3	Shielding
K1-5	286	3	40	100 MHz-3 GHz	Zones 2-3	Shielding
K1-6	169	3	35	100 MHz-3 GHz	Zone 3	Shielding
K1-7	573	3	46	27 MHz	Zones 2-3	Shielding
K2-1	5×10^5	8×10^4	16	100 MHz-3 GHz	Zone 3	Shielding or static electricity countermeasures
K3-3	240	3	38	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	3	38	50/60 Hz	Zones 2-3	Filter

Table 13 – Examples of the calculation of the required EM mitigation level of general IT equipment for a threat of AIII or less (overvoltage)

	Waveform	Restriction voltage	Peak current	Recommended element	Recommended operating voltage
Communication port	Combination	500 V	5 kA	Arrester	1.6 × or more of the voltage used by the equipment. 270 V or more when the equipment used is a commercial power supply.
	10/700		500 A		
Power-supply port	Combination	4 kV	5 kA	Varistor	
	10/700		500 A		

When there is a possibility of an EM emanations security (EMSEC) device coming within 20 m of the equipment to be protected, the EM mitigation level is 15 dB at 30 MHz to 1 GHz. The relationship between the required EM mitigation level and the frequency is as shown in Figure 2.

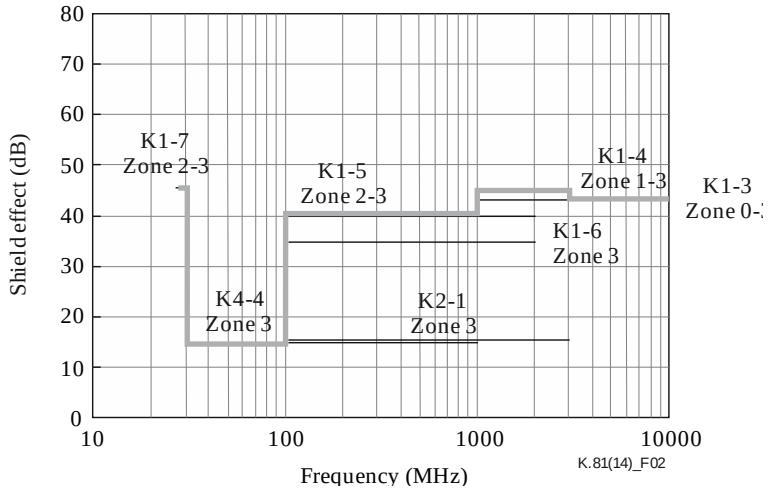


Figure 2 – Example of the calculation of the relationship between the EM mitigation level and frequency

Appendix I

HPEM threat and vulnerability

(This appendix does not form an integral part of this Recommendation.)

I.1 Calculating HPEM threat

I.1.1 Impulse radiating antenna (IRA) and JOLT

IRA is one example of a method, described in Annex B of [IEC 61000-2-13], of electromagnetic wave radiation with a high-tech level that causes a high-voltage pulse to be generated in a device at the focus of a parabolic reflector.

An image of a parabolic reflector is shown in Figure I.1. Annex B of [IEC 61000-2-13] also provides detailed examples of IRA, and examples of the electromagnetic field strengths that are generated. Of the examples provided, the one with the strongest electric field strength is "prototype USA" and Figure I.2 shows the relationship between the peak electric field strength and the associated protection distance. In the case of "prototype USA", the parabolic reflector diameter is 3.66 m, so the portability level is evaluated as being PIV (see Table I.1). Therefore, the intrusion area on the attack side becomes Zone 0. In the case of Zone 0, the minimum protection distance is taken to be 100 m, so the maximum peak electric field strength is found to be approximately 12.8 kV/m.

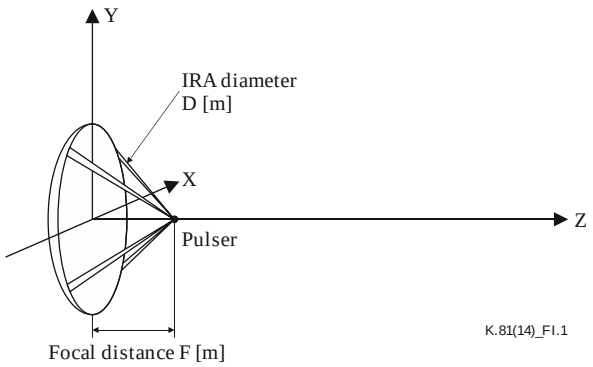


Figure I.1 – Image of an IRA

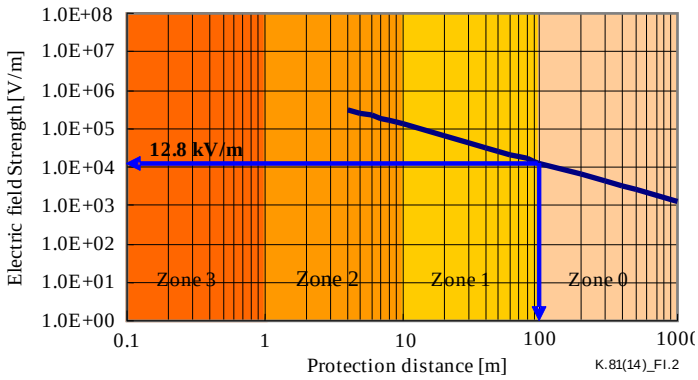
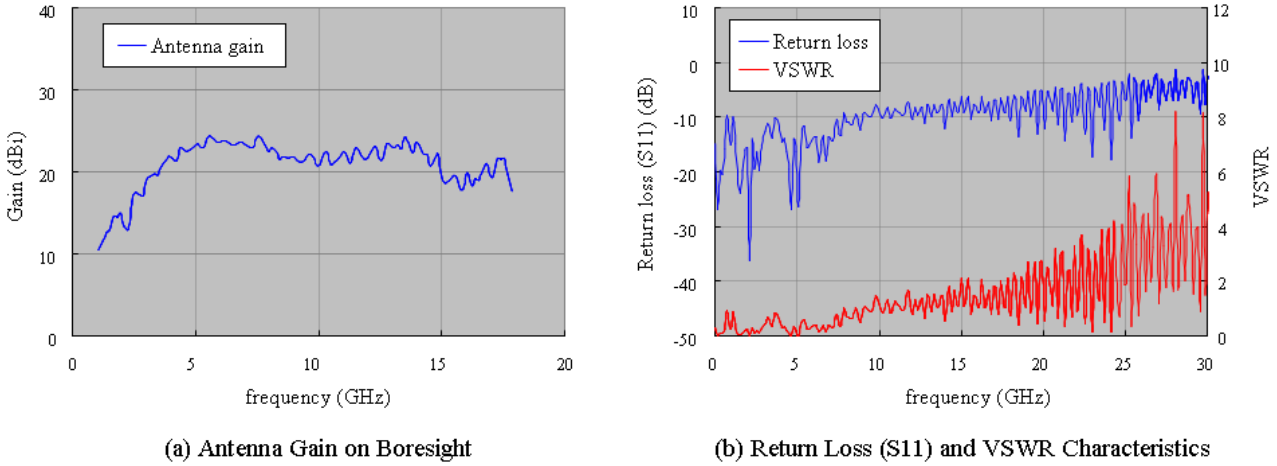


Figure I.2 – Relationship between the IRA peak electric field strength and the protection distance (Pulse voltage: 60 kV, parabolic reflector diameter: 3.66 m)

Figure I.3 shows the example of measured basic characteristics of IRA. The IRA-3M (Farr Research, Inc.) is used for the measurement. The IRA-3M parabolic reflector is 46 cm in diameter and has a focal length of 23 cm.

Figure I.3(a) shows the frequency dependence of the antenna gain. The antenna gain has an almost flat level, at about 22 dBi, from 4 GHz to 15 GHz. Figure I.3(b) shows the return loss (S_{11} parameter) and the voltage standing wave ratio (VSWR) characteristics of the same IRA.



(a) Antenna Gain on Boresight

(b) Return Loss (S11) and VSWR Characteristics

Figure I.3 – Basic characteristics of the IRA (Farr Research, Inc.; IRA-3M)

Figure I.4 shows an example of performance of the HPEM pulse propagation of the same IRA.

The waveform and frequency spectrum (FFT of the waveform) of the HPEM pulse used in this measurement are shown in Figures I.4(a) and I.4(c), respectively. The HYPS pulse source (Grant Applied Physics) was used to generate this pulse. The time dependence of electric field strength of the radiated pulse, measured at 3 m away from the IRA on boresight, is shown in Figure I.4(b), and its frequency spectrum is shown in Figure I.4(d).

The main frequency spectrum of the HPEM pulse expands to above 2 GHz and the IRA has the potential to radiate almost the whole spectrum range of this pulse (except for the direct current (DC) component). The peak electric field strength was about 270 V/m in this case.

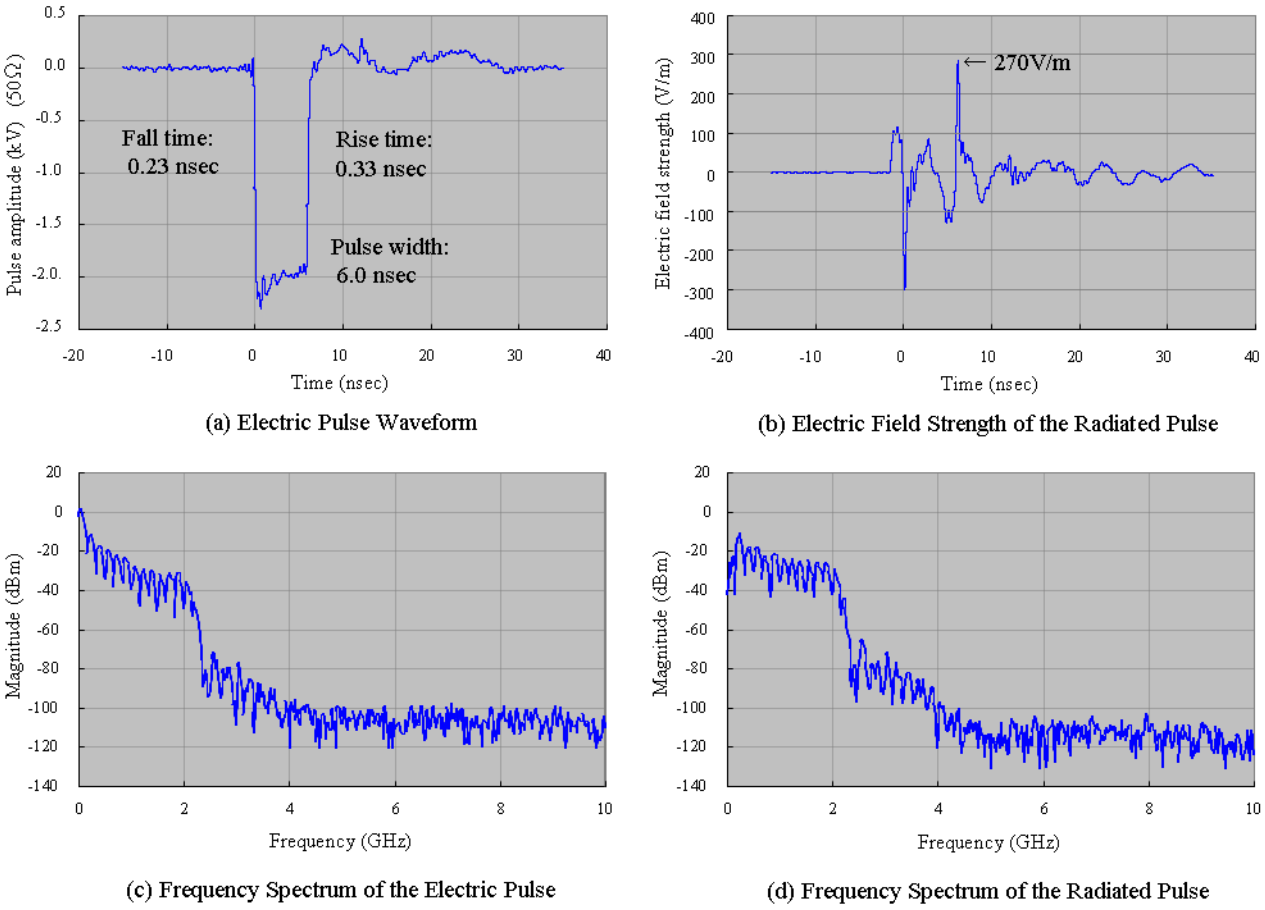


Figure I.4 – Performance of the high-power electromagnetic pulse propagation of the IRA

The JOLT system is composed of an IRA antenna with a repetitive high impulse generator. Figure I.5 shows an overview of the JOLT system. The radiated field has a fairly flat spectrum from about 50 MHz to about 2 GHz. The pulsed power system is centred on a very compact resonant transformer capable of generating over 1 MV at a pulse-repetition frequency of ~ 600 Hz. This is switched, via an integrated transfer capacitor and an oil peaking switch onto an 85-ohm half-impulse radiating antenna. This unique system will deliver a far radiated field with a full-width at half-maximum on the order of 100 ps, and a field-range product (rE_{far}) of ~ 5.3 MV, exceeding all previously reported results.

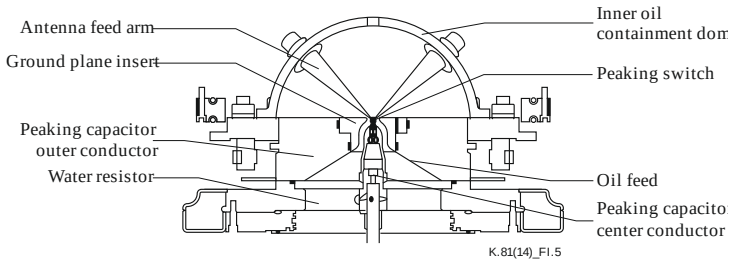


Figure I.5 – Overview of the JOLT system

The dependence between far-field electric field strength and the distance r is derived from Equation I.1. The far-field distance r is derived from Equation I.2.

$$rE_{far}(r,t) = \left(\frac{D}{4\sqrt{2}}\right)\frac{1}{2\pi c f_g}\frac{dV(t)}{dt} \quad \text{(I.1)}$$

$$range \quad r \geq \left(\frac{D^2}{2ct_{mr}}\right) \quad \text{(I.2)}$$

where:

– geometric impedance factor f_g is the ratio of the antenna input impedance Z_c to the characteristic impedance of free space Z_0, or $f_g = (Z_c/Z_0)$;

– D is the diameter of IRA;

– $\frac{dV(t)}{dt}$ is the assumed maximum rate of rise. The values are shown in Table I.1;

– the symbol c is the speed of light in the vacuum; and

– t_{mr} is the maximum rate of the rise of the voltage the same as dV/dt.

Table I.1 – Achievable peak values of (rE_{far}) for assumed maximum rate of rise

Case #	Assumptions about the maximum rate of rise of the voltage wave-form launched on to the reflector	Peak value of (rE_{far}) from Equation (I.1) = 1.08×10^{-9} (dV/dt)max	"Gain" (rE_{far})/V_p
1	V_p = 800 kV; t_{mr} = 200 ps (dV/dt) max ~ 4×10^{15} V/s	4.32 MV	5.4
2	V_p = 800 kV; t_{mr} = 160 ps (dV/dt) max ~ 5×10^{15} V/s	5.40 MV	6.75
3	V_p = 1 MV; t_{mr} = 200 ps (dV/dt) max ~ 5×10^{15} V/s	5.40 MV	5.4
4	V_p = 1 MV; t_{mr} = 180 ps (dV/dt) max ~ 5.556×10^{15} V/s	6.0 MV	6.0
5	V_p = 1 MV; t_{mr} = 150 ps (dV/dt) max ~ 6.667×10^{15} V/s	7.2 MV	7.2

When D = 3.048 m, the peak far-field electric field strength is calculated by Equation I.1 and the experimental results, respectively, 65 kV/m @ 85 m 5.4 MV and 62 kV/m @ 85 m 5.3 MV. Figure I.6 shows the relationship between the JOLT peak electric field strength and the protection distance.

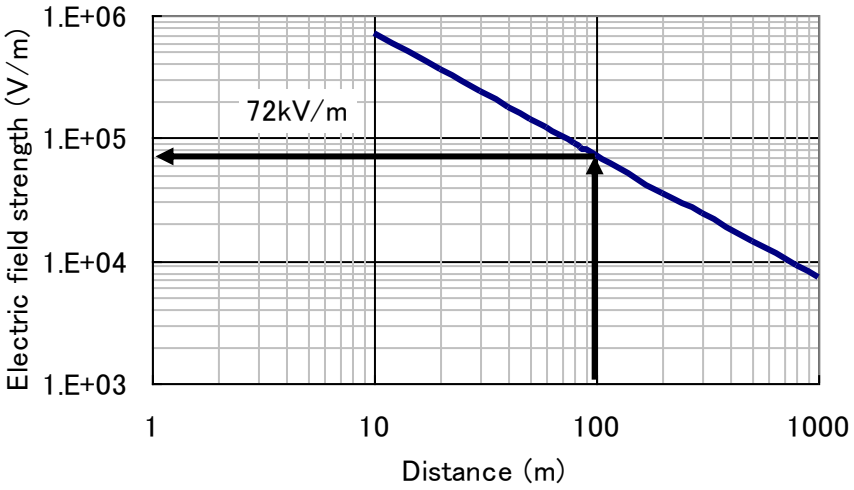


Figure I.6 – Relationship between the JOLT peak electric field strength and the protection distance (Case #5 in Table I.1; reflector diameter: 3.048 m)

I.1.2 Commercial radar

In Annex B of [IEC 61000-2-13], an example of commercial radar is given as an electromagnetic wave reflector with an intermediate technical level. The peak electromagnetic field strength (E_f) of the commercial radar in a remote field can be found by Equations I.3 and I.4.

$$E_f = E_a(A/\lambda)/r \tag{I.3}$$

$$E_a = 630[kV/m]\cdot(ab/F\lambda) \tag{I.4}$$

where:

E_a is the electric field strength at the opening;

A is the area of the antenna opening;

λ is the wavelength;

r is the distance;

a is the length of one side of the opening of the wave guide tube (long side);

b is the length of one side of the opening of the wave guide tube (short side);

F is the antenna's focal distance.

When the peak transmission power is 5 MW, the antenna diameter is approximately 5 m, a = 16.51 cm and b = 8.26 cm, Equations I.3 and I.4 are used to find the relationship between the electric field strength and the distance and the result is as shown in Figure I.7.

In Japan, the output of a radar that can be legitimately obtained is less than 5 kW; however, since larger radars can be imported, they are presented here as an example of a threat. Also, since the antenna diameter is approximately 5 m, the portability is evaluated as being PIV. Therefore, the intrusion range of the attack side becomes Zone 0. In the case of Zone 0, the minimum protection distance is taken to be 100 m, so the maximum peak electric field strength is found to be approximately 60 kV/m.

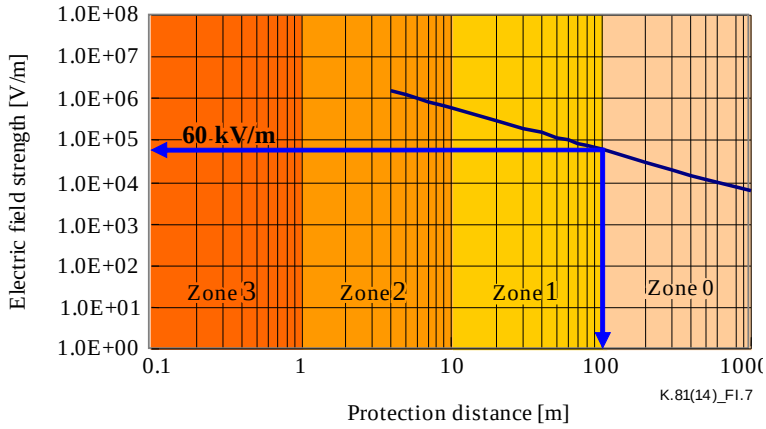


Figure I.7 – Relationship between the peak electric field strength of a commercial radar and protection distance (peak transmission output: 5 MW; transmission duty: 50%; transmission efficiency: 100%)

I.1.3 Navigation radar

In Japan, for example, navigation radar is a type of radar system that can be obtained legitimately. As stated in the previous clause, currently, if the transmission output is less than 5 kW, it is possible for an individual to purchase a commercial navigation radar. However, as a result of market research, it was found that even radars with a transmission output of 12 kW are being sold. Consequently a risk evaluation was performed for the case of a radar system in which a circular parabolic antenna with a diameter of 51 cm was connected. Examples of navigation radar systems, available on the market, are shown in Table I.2. There are cases of open antennas that are used as the antenna for navigation radars, however risk evaluation was performed here for the case of a high-gain parabolic antenna.

Table I.2 – Examples of navigation radars

Antenna type	Output power[kW]	Range [nm] (Note)
6-feet open antenna	12	72
2-feet open antenna	4.9	72
51-cm Radome antenna	4.9	24
NOTE – Nautical mile =1.852 km		

The gain of a circular parabolic antenna can be found from Equation I.5 [b-NEBS GR-1089]. Also, the relationship between the electric field strength and distance in remote field conditions is found from Equation I.6 [b-NEBS SR-3580]. With an antenna diameter of 51 cm, opening efficiency η=1 and frequency of 9.41 GHz, the relationship between the peak electric field strength of the navigation radar and protection distance is found from Equations I.5 and I.6, and is as shown in Figure I.8.

$$G = \frac{4\pi s}{\lambda^2}\eta\,[\mathrm{dBi}] \tag{I.5}$$

where:

S: Opening area [m^2];

η: Opening efficiency;

λ: Wavelength [m].

$$E = \frac{7\sqrt{PG}}{d}[\mathrm{V/m}] \tag{I.6}$$

where:

P: Antenna supply power [W];

G: Antenna gain [dBr];

d: Distance from antenna [m].

The size of the navigation radar system on one side is about 30 cm, and the diameter of the connected antenna is also 51 cm, so the portability level PIII, and the intrusion area of the attack side becomes Zone 0. In the case of Zone 0, the minimum protection distance is taken to be 100 m, so the maximum peak electric field strength is calculated to be approximately 385 V/m.

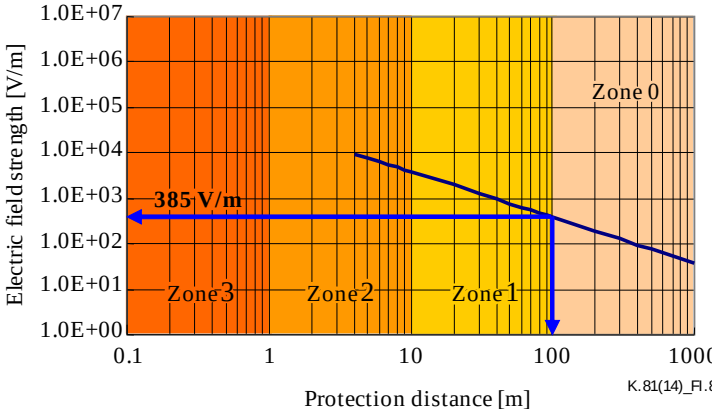


Figure I.8 – Relationship between the peak electric field of a navigation radar and protection distance (peak transmission output: 12 kW; 51 cm parabolic antenna (34 dBi); transmission efficiency: 100%)

I.1.4 Magnetron generator

In this attack, an antenna is connected to a magnetron output and generates a strong electric field. Commonly used magnetron-based devices are the microwave oven or microwave medical devices. There are two kinds of microwave oven: the general domestic kind found in people's homes and the industrial kind that is often located at convenience stores or fast food stores. Examples of microwave ovens are shown in Table I.3. Currently, the maximum rated output of an industrial microwave oven is 1.8 kW and the availability level can be evaluated as AII.

Table I.3 – Examples of industrial microwave ovens

Model	High-frequency output [W]	Rated power consumption [W]
Model A	1’800	2’800 (200 V)
Model B	1’800	2’800 (200 V)
Model C	1’700	2’990 (200 V)
Model D	1’500	2’650 (200 V)

However, the situation is changing with regard to microwave medical devices that, up until now, have generally been located in hospitals, such as osteopathic hospitals. As home care increases, microwave medical devices have also started to appear in people's homes as well. Typical microwave medical devices are shown in Table I.4 and Figure I.9. The transmission output of commercially sold microwave medical devices is about 100 to 400 W, so the risk evaluation can be the same as the magnetron of a microwave oven.

Table I.4 – Typical microwave medical devices

Model	High-frequency output [W]	Magnetron drive method
Model A	200	Inverter
Model B	200 × 2	Transformer
Model C	150	Transformer

(1) Model A

(2) Model B

Figure I.9 – Examples of microwave medical equipment

With regard to the antenna, the oscillation frequency of a microwave oven magnetron is 2.46 GHz, so a Yagi antenna for amateur radio that has a large gain at this frequency, or a grid-type parabolic antenna for a wireless LAN bridge, can be used. Examples of these products are shown in Table I.5 and Figure I.10. The antenna gain of the Yagi antenna is 19 dBi and the antenna gain of the grid-type parabolic antenna is 24 dBi. Neither antenna is expensive.

Table I.5 – Examples of antennas that can be used at 2.4 GHz

Model	Model	Gain [dBi]	Remarks
Yagi antenna	Model A	15	14 elements
	Model B	15	27 elements
	Model C	19	27 elements
Grid-type parabolic antenna	Model D	24	

(1) Grid-type parabolic antenna

(2) Yagi antenna (27 elements)

Figure I.10 – Examples of antennas

Concerning a Yagi antenna, there is a quad type that is capable of supplying signals to four antennas simultaneously. When using this antenna, the electromagnetic waves generated by each antenna are combined and theoretically, the electromagnetic field strength is 4 times that obtained when using only one antenna. A device or system to be protected must exist at an ideal location where the phase of each of the electromagnetic waves generated by the antennas coincide. However, when there is only one set of high-frequency signal source and power amplifier connected to the antenna, the power supplied to each of the four antennas is 1/4 that of only one antenna. (The set power is divided into four.) Therefore, in conditions other than the ideal conditions, the electromagnetic field strength that is generated by using a quad type antenna is less than that of one antenna.

However, when a high-frequency signal source and power amplifier are connected to each antenna, the power consumed by these devices becomes large and a separate electric generator is necessary. Therefore, there are drawbacks when including the antennas; the system on the attack side becomes large, the noise from the generator is significant and operation is easily detectable. In other words, when a quad type antenna is used as a receiving antenna, it is possible to combine the receiving power of the four antennas, so it is possible to improve the sensitivity when compared with just one antenna; however, when used as a transmission antenna, there are few advantages.

Based on the above, when the relationship between the peak electric field strength estimated for this attack method and the protection distance is calculated using Equation I.6, the results are as shown in Figure I.11. Here, the assumed condition is that a grid-type parabolic antenna (gain 24 dBi) is connected to a magnetron generator with a rated output of 1.8 kW.

Equation I.6 can be applied for remote field conditions; however, when considering that the oscillation frequency of a microwave oven magnetron is 2.46 GHz, the wavelength is approximately 12 cm, so a distance of 10 m sufficiently satisfies the condition for a remote field.

In the case of Zone 1, the protection distance is 10 m or more, so the maximum peak electric field strength becomes about 475 V/m. This value is given in Table B.1.1-1 of Annex B of [IEC 61000-2-13] and is nearly the same value as the electric field strength (468 V/m at 10 m) when attaching an antenna to a microwave oven.

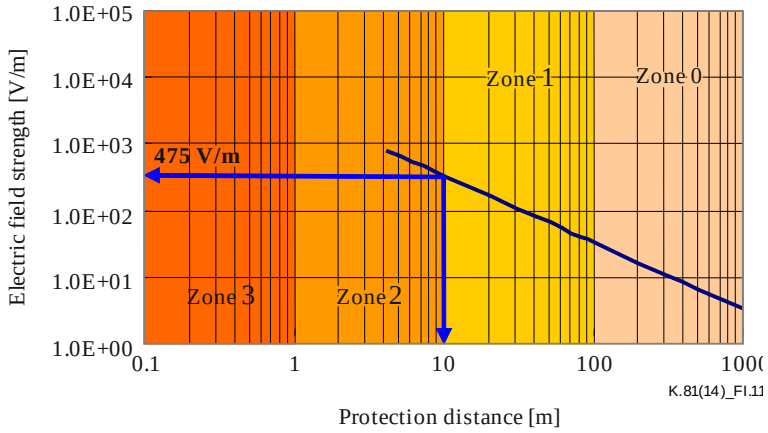


Figure I.11 – Relationship between the peak electric field strength of a magnetron generator and protection distance (frequency: 2.46 GHz; peak transmission output: 1.8 kW; antenna gain: 24 dBi; transmission efficiency: 100%)

I.1.5 Illegal CB radio

CB radio is a radio transmitter that uses the 27 MHz band (26.968 MHz to 27.144 MHz) and does not require a license. More specifically, CB radios are commonly attached to the trucks of long-distance transportation companies. The transmission output set by the radio law is 0.5 W or less; however, in order to make communication at longer distances possible, illegal radios with increased output are being sold and used quite openly. It is very difficult to know the exact transmission output of illegal radios since there are no reports on the subject. However, specifications for commercially sold antennas correspond to a maximum of 4 kW, so here, risk evaluation is performed assuming that the transmission output of an illegal CB radio is 4 kW.

On the other hand, when considering the antenna, in order to maximize the radiation efficiency in the 27 MHz band, an antenna with a 5 m long element is necessary. However, at this length, it is difficult to mount to the truck and operate so, a loading coil type antenna with a length that is shortened by mounting a coil in the element is often used. In this case, the element length becomes about 1.5 m. The directional pattern of a loading coil antenna is the same as a normal monopole antenna, so the antenna gain can be considered to be 2.15 dBi.

By substituting a transmission output of 4 kW and antenna gain of 2.15 dBi into Equation I.6, it is possible to find the relationship between the electric field strength of the illegal CB radio and the protection distance. The results are shown in Figure I.12. In the case of an illegal CB radio, since the element length is about 1.5 m, the portability level is considered to be PII, and the intrusion zone becomes Zone 2. In the case of Zone 2, since the minimum protection distance is 1 m, the maximum peak electric field strength is found to be about 573 V/m.

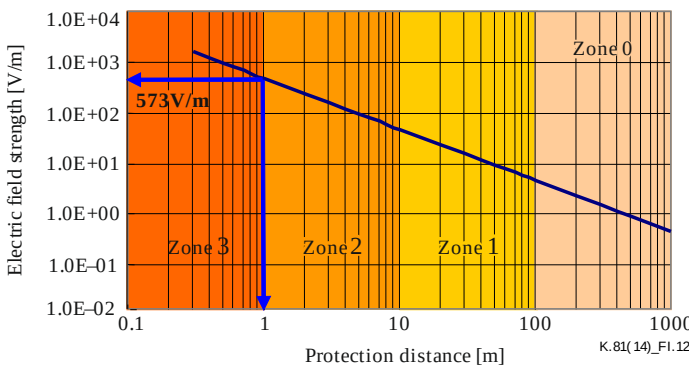


Figure I.12 – Relationship between the peak electric field strength of an illegal CB radio and the protection distance (peak transmission output: 4 kW; antenna gain: 2.15 dBi; transmission efficiency: 100%)

I.1.6 Amateur radio

In order to start and operate an amateur radio station, it is necessary to have government-recognized qualifications as an amateur radio operator. The qualifications are divided into four ranks, 1 to 4, depending on the maximum output and mode (AM, frequency modulation (FM), continuous wave (CW), etc.) of the radio station that can be operated. The frequency bands that are allotted to amateur radio consist of a large range from 1.9 MHz to 248 GHz, however, of the currently operated frequency bands, the frequency band of 2.4 GHz is said to be the highest.

Amateur radio transmitting/receiving equipment comprises two types: stationary equipment and hand-held transceivers. The transmission output of stationary equipment is large and the maximum transmission output of the hand-held type is between 5 W (when used with a car battery) and 3.5 W (when using normal batteries). Examples of amateur radios available on the market are given in Table I.6.

In the case of stationary equipment, by connecting a linear amplifier to the transmitting/receiving equipment, it is possible to operate at a maximum of 1 kW (however, first class amateur radio operator qualifications are required). Examples of linear amplifiers are also shown in Table I.6. The type of antenna varies depending on the frequency band. Yagi antennas are partially used, however, for a frequency band (high frequency (HF)) in which a 1 kW output linear amplifier can be used, an antenna having characteristics corresponding to a dipole antenna should be used.

On the other hand, for hand-held type equipment an antenna such as a monopole antenna or helical antenna is used, but all have characteristics corresponding to a dipole antenna.

Table I.6 – Examples of amateur radios

Type	Model	Major characteristics
Stationary type amateur radios	Model A	Transmission output 200 W
	Model B	Transmission output 200 W
	Model C	Transmission output 50 W
	Model D	Transmission output 50 W
Hand-held type amateur radios	Model E	Transmission output 5 W (When car batteries are used.)
Linear amplifiers	Model F	Transmission output 1’000/500 W
	Model G	Transmission output 200 W
	Model H	Transmission output 50 W
Antennas	Model I	430 MHz, 15-element Yagi antenna (15 dBi)
	Model J	2.45 GHz, 14-element Yagi antenna (15 dBi)

In the case of use of a stationary-type amateur radio, the relationship between the electric field strength and the protection distance is calculated and is as shown in Figure I.13. This relationship is evaluated by substituting the conditions of a transmission output of 1 kW and an antenna gain of 2.15 dBi into Equation I.6. In this case, from the size of the transmitter/receiver itself, the linear amplifier and the battery, the portability level is evaluated as PII. Therefore, the intrusion range on the attack side becomes Zone 2. In the case of Zone 2, since the minimum protection distance is 1 m, the maximum peak electric field strength is found to be about 286 V/m.

However, in the case of a hand-held type amateur radio, the relationship between the electric field strength and protection distance is calculated and is as shown in Figure I.14. This relationship is calculated by substituting the conditions of a transmission output of 3.5 W and antenna gain of 2.15 dBi into Equation I.6. The size of a hand-held type amateur radio corresponds to a portable telephone, so the portability level is evaluated as being PI. Therefore, the intrusion range on the attack

side becomes Zone 3. In the case of Zone 3, the minimum protection distance can be considered to be 0 m. However, when considering the risk of how easy it would be to discover the intent by carrying the device, the minimum protection distance is taken to be 10 cm here. In this case, the maximum peak electric field strength is found to be about 169 V/m.

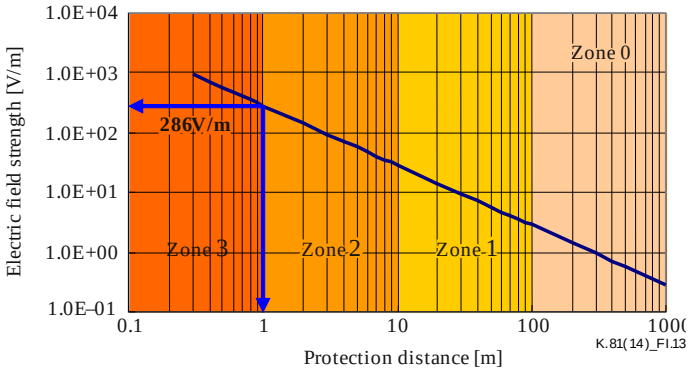


Figure I.13 – Relationship between the peak electric field strength of a stationary-type amateur radio and protection distance (peak transmission output: 3.5 W; antenna gain: 2.15 dBi; transmission efficiency: 100%)

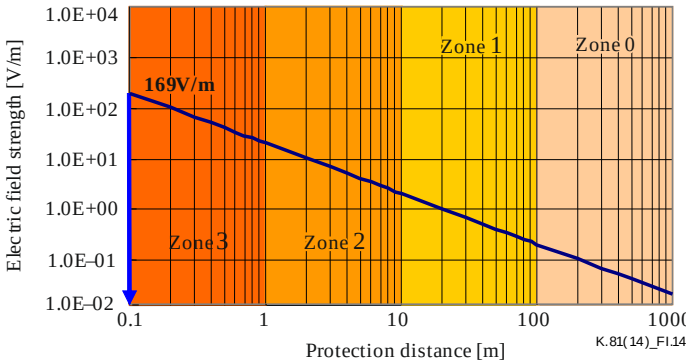


Figure I.14 – Relationship between the peak electric field strength of a hand-held type amateur radio and protection distance (peak transmission output: 3.5 W; antenna gain: 2.15 dBi; transmission efficiency: 100%)

I.1.7 Stun gun

Stun guns are commercially sold as a static-electricity generating device for personal protection and as shown in Figure I.15, they use a capacitor charge/discharge circuit to generate a high-voltage impulse. The voltage generated from the circuit shown in Figure I.15 is proportional to the terminal voltage of the capacitor and the waveform is such that it has a peak every 2τ [s]. Here, τ is the charge/discharge constant of the circuit shown in Figure I.15; using the capacitance of the capacitor C [F] and resistance R [Ω], $\tau = CR$.

For example, in the case of a commercially sold static-electricity discharge tester, $C = 1.5 \times 10^{-10}$ F and R = 330 Ω.

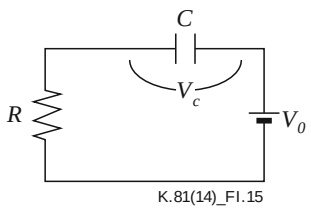
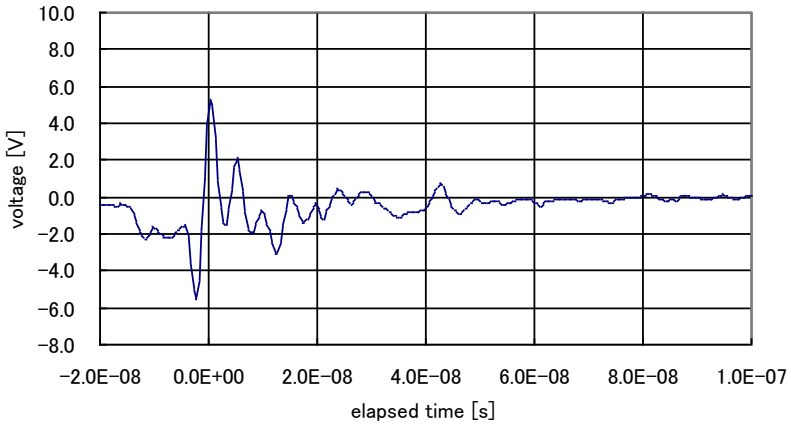


Figure I.15 – Charge/discharge circuit that uses a capacitor

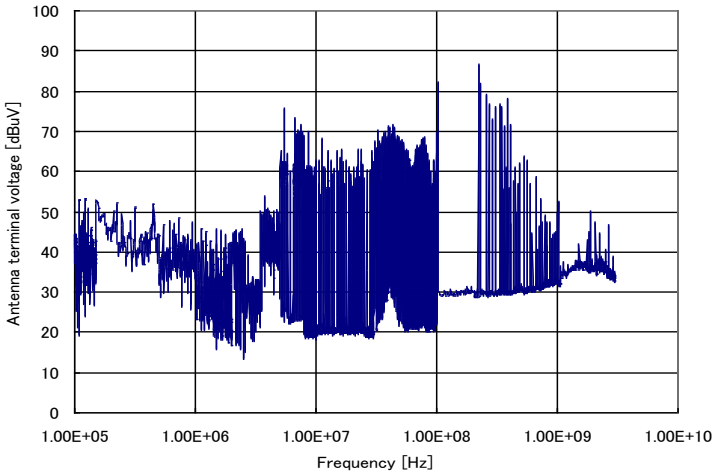
Figure I.16(a) is an example measurement of the discharge waveform from a commercially sold stun gun. The catalogue value for the discharge voltage is 500 kV. In the time waveform, a damped oscillation waveform with a rise time of about 2 ns is observed and in the frequency domain a 3 GHz spectrum is observed. Measurement of the discharge waveform is performed using a gigahertz transverse electromagnetic (GTEM) cell. The relationship between the input/output terminal voltage, V, of the GTEM and the electric field strength, E, of the cell is given by Equation I.7.

$$E = \frac{\sqrt{50V^2 / R}}{d} \tag{I.7}$$

Here, R is the characteristic impedance [Ω] of the GTEM cell and d is the distance between the internal conductor and external conductor [m]. From the measurement results shown in Figure I.16(b), the maximum input/output terminal voltage is about 90 dBμV and the electric field strength is about 0.032 V/m (when d = 1.5 m).



(a) Example of time domain measurement



(b) Example of frequency domain measurement

Figure I.16 – Examples of electric field measurement of the radiation from a stun gun (discharge voltage: 500 kV)

In the case of a discharge in air by the circuit shown in Figure I.15, R≈∞, and even though the discharge voltage is high, the current flowing in the circuit is very small. In addition, since the power

supply used for charging the stun gun is a 9 V DC battery, the current for the large charge/discharge voltage is found to be very small. Therefore, the electric field strength during discharge is a small value. This is the same for a commercially sold static-electricity-discharge tester. Therefore, with regard to a stun gun, the effect of the electromagnetic field during discharge at a great distance does not need to be considered.

However, by directly connecting an antenna to the electrodes of a stun gun, it is possible to generate an electric field with a peak at a specified frequency. Here, a slot antenna adjusted to a frequency of about 291 MHz, at which the resistance to electromagnetic waves was the lowest, was made for a PC and evaluation was performed with a stun gun connected to the power supply points of the antenna from which electromagnetic waves were radiated. As a result, at a distance of 10 cm or less, the PC did not malfunction.

In this respect, in the case of a stun gun, risk evaluation should be performed to define the effects of a direct discharge to the device or system to be protected and when there is discharge to nearby metal.

A stun gun is small enough to fit in a pocket, so the portability level is PI, and the intrusion area of the attack side becomes Zone 3. In the case of Zone 3, there is a possibility of direct discharge to a device or system, so the threat level is the maximum discharge voltage is 500 kV.

I.1.8 Lightning-surge generator

Lightning-surge generators are sold as lightning-surge testers that conform to various standards. When the charge voltage is several kV, the mechanism is not very complicated. However, a capacitor with a high voltage resistance is necessary. By charging in parallel and discharging in series, it is also possible to create a surge generator using a relatively easily available capacitor with a low voltage resistance. Examples of lightning-surge testers that can typically be purchased are shown in Table I.7 and Figure I.17. Compact models that are used for maintenance in the field have a sufficiently large output compared with the vulnerability of the device, so if it is assumed that it is used in Zone 0 to Zone 3, then at PII and AII, a charge voltage (open end voltage) of 10 kV becomes a threat. Also, if outside a building is assumed to be Zone 0, then 50 kV in PIV and AIV becomes a threat.

In [IEC 61000-2-13], the threat is indicated as being large. However, when considering the threat from a lightning-surge generator, inside and outside a building, it is necessary to obtain a power supply and to connect directly to a conductor on a communication line or power line. For example, if it is impossible or difficult to make physical contact, as is the case when countermeasures using a protector or routine inspection patrols are thorough, it is not considered to be a threat. The risk of being able to make such physical contact is considered to be small in Zone 1 to Zone 3 and even when the portability level is PII, it can be assumed that there could only be an attack from Zone 0.

Table I.7 – Examples of lightning-surge generators

Portability level	Availability level	Model	Waveform	Maximum charge voltage	Maximum output current
PII	AII	Model A	Combination	4.4 kV	2.2 kA
PII	AII	Model B	Combination · 10/700	6 kV · 6 kV	3 kA · 150 A
PII	AII	Model C	Combination	10 kV	5 kA
PIII	AIII	Model D	Combination · 10/700	15 kV · 15 kV	3 kA · 375 A
PIII	AIII	Model E	Combination · 10/700	25 kV · 25 kV	12.5 kV · 1 kA
PIV	AIV	Model F	Combination · 10/700	50 kV · 50 kV	25 kV · 10 kA

Figure I.17 – Examples of lightning-surge generators

I.1.9 CW generator

As indicated in [IEC 61000-2-13], in order to pass through the power supply from the outside and reach an internal device, 10 MHz or less is a required condition when taking into consideration the attenuation of the power-supply line. A continuous wave (CW) generator of up to 10 MHz can be easily made by switching a commercial power supply using a semiconductor, such as a field effect transistor (FET), or an insulated gate bipolar transistor (IGBT). In recent years, FETs that are capable of handling large currents and elements that are driven at that frequency can be obtained through mail order. In addition, since the size is such that it can fit inside a trunk, the portability level and availability level are assumed to be PII and AII, respectively. Also, instead of a CW generator, burst testers or fast transient testers that are regulated by [b-IEC 61000-4-4] and have the same frequency band can be obtained relatively easily. Examples of these are shown in Table I.8 and Figure I.18.

In [IEC 61000-2-13], the threat is indicated as large. However, when considering the threat from these generators, inside and outside a building, a power supply is required and it is necessary to connect directly to a conductor on a communication line or power line. For example, if it is impossible or difficult to make a physical contact, as in the case when countermeasures using a protector or routine inspection patrols are thorough, they are not considered to be a threat. In [IEC 61000-2-13], it is indicated that for a communication line, a frequency of up to about 1 GHz must be considered. However, even in this case, the risk of being able to connect directly with the communication line, or the risk when the frequency characteristics are those of the normal mode and physical contact is made, is considered to be small in Zone 1 to Zone 3.

Therefore, even when the portability level is PII, it assumed that there is only a threat of attack in Zone 0.

Table I.8 – Examples of CW generators and burst testers

Portability	Availability	Model	Waveform, frequency, etc.	Maximum output voltage
PII	AII	Model A	1 Hz – 10 MHz	240 V
PII	AII	Model B	50 – 400 ns burst	4 kV
PII	AII	Model C	0.11 kHz – 1 MHz ±2%	4.8 kV

Figure I.18 – Examples of CW and burst generators

I.1.10 Commercial power supply

Up until now, attacks were assumed to use a tester or some similar device, however, in the case of a communication line, connecting a commercial power supply directly to a communication line would also be a large threat. If there is a fuse in the communication line, the fuse will blow. Recently however, many devices have become available on the market that do not have fuses and in such a case there is a possibility of fire occurring. There are also many reports of damage due to mixed contacts and since it is possible to bring about a sufficiently large amount of damage from Zone 0 with light equipment such as a wiring or nippers, the risk is considered to be high.

I.2 Vulnerability of IT equipment

I.2.1 Vulnerability to an electromagnetic wave attack

The resistance of IT equipment to an electromagnetic wave attack can be estimated from applied immunity standard values. Examples of immunity standards that have been applied to IT equipment since January 2004 up until the current time are shown in Table I.9. Of these, the only enforced standards are those for equipment exported to the EU, Australia and New Zealand. The others are voluntary standards for manufacturers or for procurement businesses. Emission standards are compared in this way, so there are many variations of voluntary correspondence by manufacturers and often discerning which immunity standards have been applied is not clear. Normally in such cases compliance to [IEC CISPR 24], which is an International Standard, is assumed, and equipment is considered to have the resistance shown in Table I.10.

Table I.9 – Examples of IE equipment immunity standards

Standard	Type	Target equipment
[IEC CISPR 24]	International Standard	IT equipment
[b-EN 55024]	European Standard (CISPR 24 compliance)	IT equipment
[ITU-T K.43]	Recommendation	Communications equipment
[ITU-T K.48]	Recommendation	Network equipment
[b-NEBS GR-1089]	Voluntary standard	Network equipment
[b-NTT TR 549001]	Voluntary standard (compliance to various standards)	Communications equipment

Table I.10 – Immunity levels of IT equipment

Item	Immunity level
Radiated electromagnetic waves	3 V/m (effective electric field value)
Conducted voltage	3 V (effective voltage value)
Static electricity discharge	8 kV (direct discharge)
Lightning surge	4 kV (1 line – ground)

In addition, as in the case of emission standards, coordination of immunity standards is also being implemented since the movement by the World Trade Organization (WTO) to do away with non-tariff barriers. However, since the installation environment of the target equipment differs, some standard values also differ. A comparison of various immunity standards is shown in Table I.11 (2004 to the present). Particularly, in the case of NEBS standards, the required value for a radiated electromagnetic field for Level 3 products is 8.5 V/m and by revising [ITU-T K.48], the immunity level for a radiated electromagnetic field has been raised to 10 V/m. Due to differences in applied standards such as this and a movement to revise the standards, it is necessary to periodically review the standards for resistance of equipment to electromagnetic wave attacks and to reflect these changes in decisions of whether or not countermeasures are necessary.

Table I.11 – Comparison of various immunity standards

Item	CISPR 24 EN 55024	ITU-T K.43	ITU-T K.48	NEBS GR-1089-CORE NEBS SR-3580
Static electricity discharge	4 kV (contact) 8 kV (in air)	4 kV (contact) 8 kV (in air)	4 kV (contact) 4 kV (in air)	8 kV (contact) 4 and 15 kV (in air)
Radiated electric field	3 V/m ≤ 80 ~ 1’000 MHz 1 kHz 80% AM	1 V/m ≤ 80 ~ 1’000 MHz 1 kHz 80% AM	3 V/m ≤ 80 ~ 1’000 MHz 1 kHz 80% AM	8.5 V/m (0.01 ~ 0.024 MHz) 8.5 ~ 1.7 V/m*1 (0.024 ~ 0.12 MHz) *1: 106.2-20log (f [MHz]) f is the frequency. 1.7 V/m (0.12 MHz ~ 10 GHz) When there is a high-output transmission location within 3 km, 8.5 V/m (0.01 MHz ~ 10 GHz). For SR-3580, 10 V/m (0.01 MHz ~ 10 GHz).
Fast transient	0.5 kV (communication port) 0.5 kV (DC power-supply port)	0.25 kV (outdoor, indoor communication port) 0.25 kV (DC power-supply port)	[In the Centre] 0.5 kV (communication port) 0.5 kV (DC power-supply port) [Outdoors]	There are no standards for the communication port and power-supply port.

Table I.11 – Comparison of various immunity standards

Item	CISPR 24 EN 55024	ITU-T K.43	ITU-T K.48	NEBS GR-1089-CORE NEBS SR-3580
	1.0 kV (AC power-supply port)	0.5 kV (AC power-supply port)	0.5 kV (communication port) 0.5 kV (DC power-supply port) 1.0 kV (AC power-supply port)	
Lightning-surge immunity	1.5 kV (No primary protection, communication port, 10/700 μs) 4.0 kV (Primary protection, communication port, 10/700 μs) 0.5 kV (DC power-supply port, common mode, combination *2) 1.0 kV (AC power-supply port, normal mode, combination) 2.0 kV (AC power-supply port, common mode, combination) *2: 1.2/50(8/20) μs	0.5 kV (Outdoor communication port, normal mode, 10/700 μs) 1.0 kV (Outdoor communication port, common mode, 10/700 μs) 0.5 kV (Indoor communication port, normal mode, combination*3) 0.5 kV (AC power-supply port, normal mode, combination) 1.0 kV (AC power-supply port, common mode, combination) *3: 1.2/50(8/20) μs	[In the Centre] 0.5 kV (Outdoor communication port, normal mode, 10/700 μs) 1.0 kV (Outdoor communication port, common mode, 10/700 μs) 0.5 kV (Indoor communication port, normal mode, combination*4) [Outdoors] 0.5 kV (Outdoor communication port, normal mode, 10/700 μs) 1.0 kV (Outdoor communication port, common mode, 10/700 μs) 0.5 kV (AC power-supply port, normal mode, combination) 1.0 kV (AC power-supply port, common mode, combination) *4: 1.2/50 (8/20) μs	There are no standards for lightning-surge immunity. Standards for power-supply trouble and lightning-surge testing. Also, standards for ground testing.

Table I.11 – Comparison of various immunity standards

Item	CISPR 24 EN 55024	ITU-T K.43	ITU-T K.48	NEBS GR-1089-CORE NEBS SR-3580
Wireless frequency conduction	3 V_{emf} *5 (Communication port, AC power-supply port, DC power-supply port) 0.15 ~ 80 MHz 1 kHz 80% AM *5: Effective emf	1 V_{emf} *6 (Communication port, AC power-supply port, DC power-supply port) 0.15 ~ 80 MHz 1 kHz 80% AM *6: Effective emf	[In the Centre] 3 V_{emf} *7 (Outdoor, indoor communication port, DC power-supply port) [Outdoors] 3 V_{emf} *7 (Communication port, AC power-supply port, DC power-supply port) *7: Effective emf	28 mA (0.01 ~ 0.27 MHz) 7.6 ~ 9.4 mA (0.27 ~ 0.8 MHz) 9.4 mA (0.8 ~ 30 MHz) These values correspond to the conduction emission reference value +10 dB.
Power-supply frequency electromagnetic field	1 A/m (50, 60 Hz)	No standards	No standards	No standards
Voltage dip, temporary blackout	– Voltage dip > 95% decrease, 0.5 cycle 30% decrease, 25 cycles – Temporary blackout > 95% decrease, 250 cycles	– Voltage dip > 95% decrease, 0.5 cycle 30% decrease, 25 cycles – Temporary blackout > 95% decrease, 250 cycles	[In the Centre] No standards [Outdoors] – Voltage dip > 95% decrease, 0.5 cycle 30% decrease, 25 cycles – Temporary blackout > 95% decrease, 250 cycles	No standards

I.2.2 Vulnerability evaluation of a sample device

As described above, it is possible to estimate the resistance of equipment or a system to be protected against electromagnetic wave attacks from the applied immunity standards. However, since most standards are not enforced standards, the case in which the actual resistance is less than the standard value is assumed. In order to estimate the size of this kind of risk, resistance evaluation was performed for samples of typical IT equipment (two PCs and one small router).

I.2.2.1 Vulnerability to a radiated electromagnetic field

As a method for evaluating the resistance to a radiated electromagnetic field, there is the radiation immunity test that complies with [b-IEC 61000-4-3]. However, this test is an inefficient test in that it is necessary to change the antenna and power amplifier depending on the frequency of the radiated electromagnetic waves. Consequently this evaluation was performed using a GTEM cell that complies with [b-IEC 61000-4-20].

The evaluation system is shown in Figure I.19. In the case of a PC, the test was executed with communication performed using the PC that was installed outside the GTEM cell (Aux equipment) and resistance to electric fields that can cause significant drops in communication speed, blocked communication and a downed system due to malfunctions was evaluated. Communication was via file transfer protocol (FTP) communication using TCP/IP.

With regard to the router, two PCs were connected and communication was performed using TCP/IP and then routing was performed.

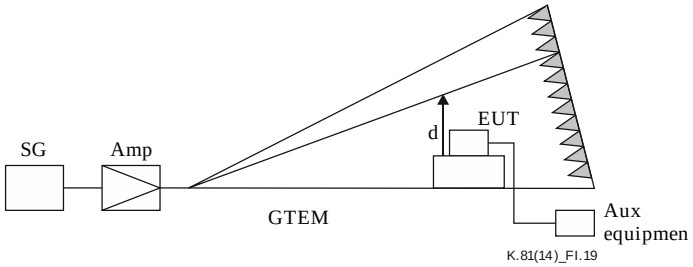
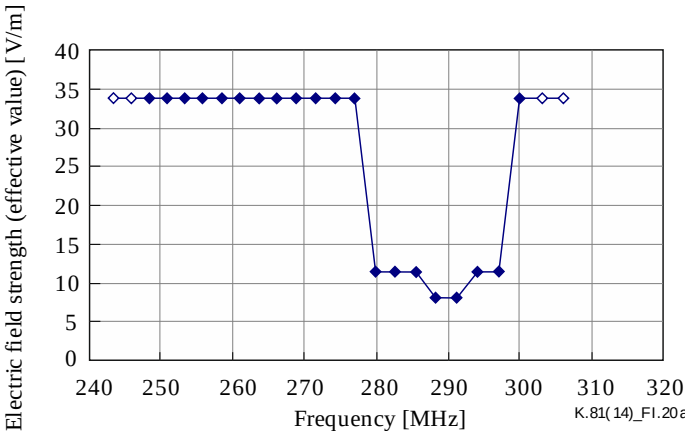
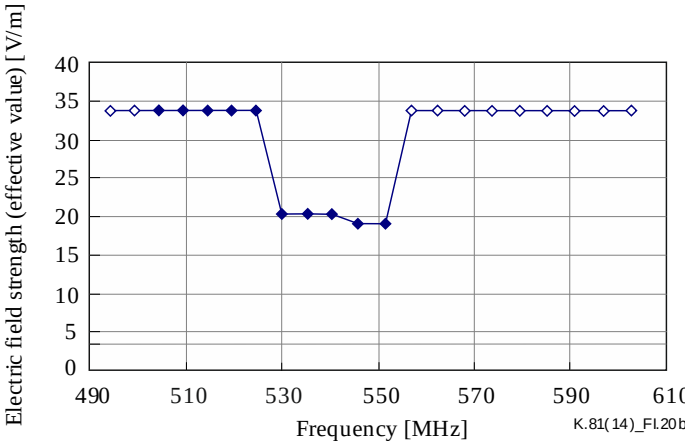


Figure I.19 – Vulnerability evaluation system for a radiated electromagnetic field

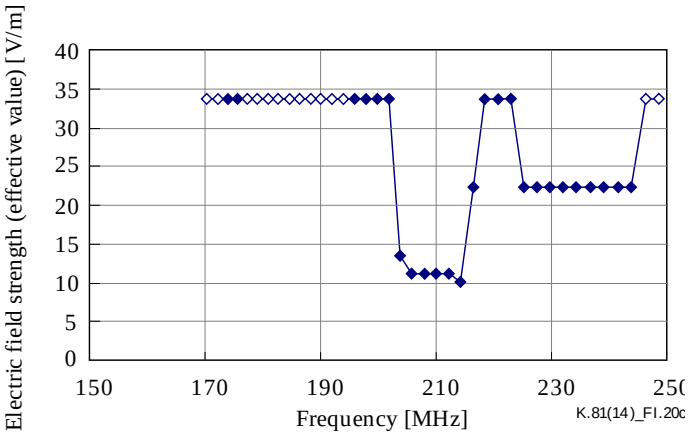
The evaluation results are shown in Figure I.20 and Table I.12. Figure I.20 shows the frequency along the horizontal axis. The electric field that was applied during testing is shown along the vertical axis. The white dots show that malfunctions did not occur at that electric field strength (in other words, malfunctions did not occur in this test even when the maximum electric field strength was applied). Shaded dots show that malfunctions did occur at that electric field strength. Both the PC and router had low resistance to certain frequencies that corresponded to integral multiples of the clock frequency as shown in Table I.12. In the case of PC1 that had the lowest resistance, the electric field strength at which malfunctions occurred was 7.8 V/m, which is about 2.6 times (about +8 dB) the general resistance (at 3 V/m) shown in Table I.10 in clause I.2.1. Normally, 6 to 10 dB is taken to be the safety factor, so resistance based on the actual evaluation results can be said to be good at 3 V/m.



(a) Evaluation results for PC1



(b) Evaluation results for PC2



(c) Evaluation results for the router

Figure I.20 – Evaluation results for vulnerability to radiated electromagnetic waves

Table I.12 – Lowest resistances and frequencies

Device	Lowest resistance value	Frequency	Remarks
PC1	7.8 V/m	291.2 MHz	About 3 × the system clock (99.75 MHz)
PC2	20.2 V/m	535.1 MHz	About 8 × the system clock (66.0 MHz)
Router	11.2 V/m	214.24 MHz	–

I.2.3 Vulnerability to electrostatic discharge

Resistance evaluation was performed using a stun gun with a 500 kV discharge voltage. When the stun gun made contact with metal parts of the PC, such as expansion board fittings on the back of the PC and was discharged the result was the system going down. In the static electricity discharge test, 8 kV was cleared, so in these guidelines, the resistance to static electricity discharge is taken to be 8 kV.

Appendix II

Examples of EM mitigation levels

(This appendix does not form an integral part of this Recommendation.)

II.1 Example of EM mitigation levels for an IP network service

II.1.1 Data centre (European Community site)

Countermeasures must be considered for a server that circulates information with an information value level greater than the threat level. At the same time, when complete remote duplication is performed at a location sufficiently far away so that the threat from electromagnetic attack does not occur, it is only necessary to consider EMSEC countermeasures. Examples of the calculation of the EM mitigation levels when the threat that satisfies the availability and integrity limits regulated by SLA is assumed to be able to intrude up to AII or the Zone 2 level, the vulnerability level is ZI1, and information leakage intrusion is at 10 m are shown in Table II.1a and Table II.1b.

Table II.1a – Examples of the calculation of EM mitigation levels (European Community data centre)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K1-4	475	1	54	1 GHz-3 GHz	Zones 1-3	Shield
K1-5	286	1	50	100 MHz-3 GHz	Zones 2-3	Shield
K1-7	573	1	56	27 MHz	Zones 2-3	Shield
K3-3	240	1	48	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	1	48	50/60 Hz	Zones 2-3	Filter
K4-5	300 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Filter

Table II.1b – Examples of the calculation of EM mitigation levels (European Community data centre)

<table>
<tr><th></th><th>Waveform</th><th>Restriction voltage</th><th>Peak current</th><th>Recommended element</th><th>Recommended operating voltage</th></tr>
<tr><td rowspan="2">Communication port</td><td>Combination</td><td>500 V</td><td>5 kA</td><td rowspan="2">Arrester</td><td rowspan="4">270 V or more in the case of a device that uses a commercial power supply.
1.6 × or more of the voltage used by the device.</td></tr>
<tr><td>10/700</td><td></td><td>500 A</td></tr>
<tr><td rowspan="2">Power-supply port</td><td>Combination</td><td rowspan="2">4 kV</td><td>5 kA</td><td rowspan="2">Varistor</td></tr>
<tr><td>10/700</td><td>500 A</td></tr>
</table>

II.1.2 Data centre (storage)

Countermeasures must be considered for a server that stores information with an information value level greater than the threat level. At the same time, when complete remote duplication is performed at a location sufficiently far away so that the threat from electromagnetic attack does not occur, it is only necessary to consider EMSEC countermeasures. Examples of calculation of the EM mitigation levels when the threat that satisfies the availability and integrity limits regulated by SLA is assumed

to be able to intrude up to AIII or the Zone 2 level, the vulnerability level is ZI2, and information leakage intrusion is at 10 m are shown in Table II.2a and Table II.2b.

Table II.2a – Examples of the calculation of EM mitigation levels (Storage)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K1-4	475	3	44	1 GHz-3 GHz	Zones 1-3	Shield
K1-5	286	3	40	100 MHz-3 GHz	Zones 2-3	Shield
K1-7	573	3	46	27 MHz	Zones 2-3	Shield
K3-3	240	3	38	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	3	38	50/60 Hz	Zones 2-3	Filter
K4-5	263 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Filter

Table II.2b – Examples of the calculation of EM mitigation levels (Storage)

<table>
<tr><th></th><th>Waveform</th><th>Restriction voltage</th><th>Peak current</th><th>Recommended element</th><th>Recommended operating voltage</th></tr>
<tr><td rowspan="2">Communication port</td><td>Combination</td><td rowspan="2">500 V</td><td>5 kA</td><td rowspan="2">Arrester</td><td rowspan="3">270 V or more in the case of a device that uses a commercial power supply.
1.6 × or more of the voltage used by the device.</td></tr>
<tr><td>10/700</td><td>500 A</td></tr>
<tr><td rowspan="2">Power-supply port</td><td>Combination</td><td rowspan="2">4 kV</td><td>5 kA</td><td rowspan="2">Varistor</td></tr>
<tr><td>10/700</td><td>500 A</td></tr>
</table>

II.1.3 Routers and switches (MSP)

Examples of the calculation of EM mitigation levels for a management service provider when operating carrier grade equipment has vulnerability levels of ZI3 and ZK5 and when the threat that satisfies the availability and integrity limits regulated by SLA is assumed to be able to intrude up to AIV or the Zone 2 level, are shown in Table II.3.

Table II.3 – Examples of the calculation of EM mitigation levels (Routers and switches)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K1-3	385	8.5	34	1 GHz-10 GHz	Zones 0-3	Shield
K1-4	475	8.5	35	1 GHz-3 GHz	Zones 1-3	Shield
K1-5	286	8.5	31	100 MHz-3 GHz	Zones 2-3	Shield
K1-7	573	8.5	37	27 MHz	Zones 2-3	Shield
K3-3	240	3	38	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	3	38	50/60 Hz	Zones 2-3	Filter
K4-5	263 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Filter

II.1.4 Data centre of a local government unit or government organization

Countermeasures must be considered for a server that stores information with an information value level greater than the threat level. At the same time, when complete remote duplication is performed at a location sufficiently far away so that the threat from electromagnetic attack does not occur, it is only necessary to consider EMSEC countermeasures. Examples of the calculation of the EM mitigation levels when the level of the threat to the required availability and integrity is assumed to be able to intrude up to AIII or the Zone 2 level, the vulnerability level is ZI2 and information leakage intrusion is 10 m, are shown in Table II.4a and Table II.4b.

Table II.4a – Examples of the calculation of EM mitigation levels (government organization)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K1-4	475	3	44	1 GHz-3 GHz	Zones 1-3	Shield
K1-5	286	3	40	100 MHz-3 GHz	Zones 2-3	Shield
K1-7	573	3	46	27 MHz	Zones 2-3	Shield
K3-3	240	3	38	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	3	38	50/60 Hz	Zones 2-3	Filter
K4-5	263 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Filter

Table II.4b – Examples of the calculation of EM mitigation levels (government organization)

	Waveform	Restriction voltage	Peak current	Recommended element	Recommended operating voltage
Communication port	Combination	500 V	5 kA	Arrester	270 V or more in the case of a device that uses a commercial power supply. 1.6 × or more of the voltage used by the device.
	10/700		500 A		
Communication port	Combination	4 kV	5 kA	Arrester	
	10/700		500 A		

II.1.5 Examples of EM mitigation levels of an IP company network

II.1.5.1 Work station

Normally, only an EMSEC threat is assumed. An example of calculating the EM mitigation level when the vulnerability level is Class B, the threat intrudes up to Zone 1 and the availability level is AII, is shown in Table II.5.

Table II.5 – Examples of the calculation of EM mitigation levels (Work station)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remark
K4-5	47 m	Class B	15	30 MHz-1 GHz	Zones 2-3	Shield

II.1.5.2 Mail server

Normally, only an EMSEC threat is assumed. An example of the calculation of the EM mitigation level when the vulnerability level is Class A, the threat intrudes up to Zone 1 and the availability level is AI, is shown in Table II.6.

Table II.6 – Examples of the calculation of EM mitigation levels (Mail server)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K4-5	263 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Shield

II.1.5.3 ERP server, storage, customer DB server

Examples of the calculation of EM mitigation levels for a corporation DB, a highly valued information storage, a customer DB, etc., when the threat is assumed to intrude up to level AII and Zone 2 are shown in Table II.7a and Table II.7b.

Table II.7a – Examples of the calculation of EM mitigation levels (Database)

Threat number	Strength	Vulnerability level	EM mitigation level (dB)	Frequency/ Waveform	Counter-measure location	Remarks
K1-4	475	1	54	1 GHz-3 GHz	Zones 1-3	Shield
K1-5	286	1	50	100 MHz-3 GHz	Zones 2-3	Shield
K1-7	573	1	56	27 MHz	Zones 2-3	Shield
K3-3	240	1	48	1 Hz-10 MHz	Zones 2-3	Filter
K3-4	240	1	48	50/60 Hz	Zones 2-3	Filter
K4-5	263 m	Class A	25	30 MHz-1 GHz	Zones 2-3	Shield

Table II.7b – Examples of the calculation of EM mitigation levels (Database)

<table>
<tr><th></th><th>Waveform</th><th>Restriction voltage</th><th>Peak current</th><th>Recommended element</th><th>Recommended operating voltage</th></tr>
<tr><td rowspan="2">Communication port</td><td>Combination</td><td rowspan="2">500 V</td><td>5 kA</td><td rowspan="2">Arrester</td><td rowspan="4">270 V or more in the case of a device that uses a commercial power supply.
1.6 × or more of the voltage used by the device.</td></tr>
<tr><td>10/700</td><td>500 A</td></tr>
<tr><td rowspan="2">Communication port</td><td>Combination</td><td rowspan="2">4 kV</td><td>5 kA</td><td rowspan="2">Barrister</td></tr>
<tr><td>10/700</td><td>500 A</td></tr>
</table>

Appendix III

IEC Standards related to HPEM

(This appendix does not form an integral part of this Recommendation.)

III.1 Overview of the IEC HPEM Series

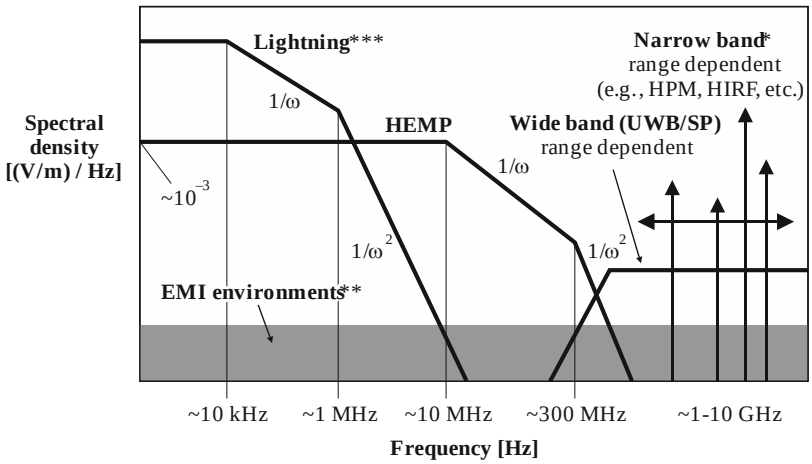
From February 2004 to the present day, three standards have been proposed for HPEM as shown in Table III.1. The documents that will be referenced here are the documents with the document numbers shown in Table III.1.

Table III.1 – Standards and summaries related to HPEM of the IEC 61000 series

Standard number	Standard name	Description and summary
[b-IEC 61000-1-5]	High power electromagnetic (HPEM) effects on civil systems	Example of the effects (HPEM) of high-power electromagnetic waves on civil systems and a summary of test results
[IEC 61000-2-13]	High-power electromagnetic (HPEM) environments – Radiated and conducted	Description of HPEM environments, summary of generating devices, definition of waveforms, etc.
[b-IEC 61000-4-33]	Measurement methods for high power transient parameters	Measurement methods for the high-power transient phenomenon

In [b-IEC 61000-1-5], an example of HPEM and background for research of HPEM as well as an introduction to HPEM generators and summaries of test results on devices such as a PC are described. In conduction, a lightning-surge generation is included as a HPEM generator. In addition, chapter 7 of [b-IEC 61000-1-5] touches on countermeasure concepts and describes countermeasure methods such as shielding and surge-voltage protection, as well as the existence of alternative countermeasure methods such as active protection or system degeneration, error detection and error collection software.

The differences in the frequencies and levels considered among the various IEC 61000 series electromagnetic compatibility (EMC) standards are shown in Figure III.1.



* Narrow band extending from ~0.5 to ~5 GHz
** Not necessarily HPEM
*** Significant spectral components up to ~10 MHz depending on range and application

K.81(14)_FIII.

Figure III.1 – Differences between HPEM and HEMP

The following text, based on the scope clause of [IEC 61000-2-13], clearly defines HPEM. Moreover, the importance of a review process is also explained.

A threat environment is provided by an artificially caused high-power electromagnetic wave (HPEM). That kind of threat environment can give large damage to consumer electrical equipment and electronic devices as described in [b-IEC 61000-1-5]. In order to establish protection methods, it is necessary to define radiation and conduction environments. The objective of these standards is a high-power condition in which a free-space plane wave having a peak electric field intensity that exceeds 100 V/m and corresponds to a power density of 26.5 W/m^2 is output. Based on the normal EMC criteria covered by the standards made by the IEC SC 77B, these standards intentionally define very high electromagnetic radiation and conduction criteria.

HPEM Environment:

– radiation, or conduction combination;
– a single-envelope having a several repetitions of a single cycle (an ultra-narrow-band signal possibly having a variable frequency);
– burst having many single-cycle pulses;
– ultra-wide-band transient pulse (MHz to several GHz, having a spectrum of up to 10 GHz);
– a burst having many ultra-wide-band transient pulses.

An HPEM signal can be a signal from a signal source such as a nearby-located radar or other transmission device, or can be a signal that is output from an intentional generator for the purpose of targeting civil equipment. A radiated signal becomes conducted voltage and current through combination and is applied. In addition, a conduction-combined HPEM environment can also be directly applied to an installed wire.

High-altitude EM pulse (HEMP) and HPEM are clearly classified from the aspect of distance and range from the signal source to the affected electrical component. In the case of HEMP, the range is not important. That is because HEMP propagates by being showered down to the earth from space and is a phenomenon that occurs comparatively uniformly for 1'000 km or more. On the other hand, in the case of HPEM, the effect greatly decreases due to distance. Therefore, the process of standardizing a HPEM environment is more difficult. The recommended approach is to investigate the various types of HPEM that could possibly be used now or in the near future, and then make an appropriate HPEM reference waveform from that investigation. That kind of reference HPEM waveform must be corrected for technology that emerges that is capable of making those kinds of waveforms.

In chapter 5 of [IEC 61000-2-13], various kinds of radiation HPEM generators are described, and examples of waveforms are given. When seen from the generator side, the frequency is 300 MHz to 5 GHz and when considered from the aspect of the size of the device or screw spacing, the frequency to pay attention to is from 1 to 2 GHz. Chapter 6 of [IEC 61000-2-13] describes the threat due to conduction. The frequency range to take notice of for a power-supply line is from 50 Hz to 1 MHz, since at 10 MHz or greater and also 40 dB or greater the frequency is damped. The frequency range to take notice of for a communication line is from 1 kHz to 1 GHz. The size of the generator is introduced as a trunk-size CW generator and an ITU-T (10/700) lightning-surge generator.

Annex A of [IEC 61000-2-13] gives an example of four types of class divisions during a landing at a commercial airport. Annex B of [IEC 61000-2-13] describes a HPEM generator that is hierarchized in technical levels and for the low-tech level, an example of converting a microwave oven is given. For the medium-tech level, an example of converting a commercial radar system is given and for the high-tech level, an example of an IRA is given. Examples of the electric field intensity of each are also given.

In [b-IEC 61000-4-33], general items related mainly to the measurement methods for measuring impulses are described.

Bibliography

ITU-Security

[b-ITU-T SECMAN] ITU-T Handbook (2003), *Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications*.x <http://www.itu.int/ITU-T/edh/files/security-manual.pdf>.

IEC-HEMP

[b-IEC 61000-1-3] IEC/TR 61000-1-3 (2002), *Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems*.

[b-IEC 61000-2-9] IEC 61000-2-9 (1996), *Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance. Basic EMC publication*.

[b-IEC 61000-2-10] IEC 61000-2-10 (1998), *Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance*.

[b-IEC 61000-2-11] IEC 61000-2-11 (1999), *Electromagnetic compatibility (EMC) – Part 2-11: Environment – Classification of HEMP environments*.

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

[b-IEC 61000-4-4] IEC 61000-4-4 (2012), *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*.

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

[b-IEC 61000-4-24] IEC 61000-4-24 (1997), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 24: Test methods for protective devices for HEMP conducted disturbance – Basic EMC publication*.

[b-IEC 61000-4-25] IEC 61000-4-25 (2012), *Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems*.

[b-IEC 61000-4-32] IEC 61000-4-32 (2002), *Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques High-altitude electromagnetic pulse (HEMP) simulator compendium*.

[b-IEC 61000-5-3] IEC 61000-5-3 (1999), *Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts*.

[b-IEC 61000-5-4] IEC/TS 61000-5-4 (1996), *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 4: Immunity to HEMP – Specifications for protective devices against HEMP radiated disturbance. Basic EMC publication*.

[b-IEC 61000-5-5] IEC 61000-5-5 (1996), *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 5: Specification of protective devices for HEMP conducted disturbance. Basic EMC publication*.

[b-IEC 61000-5-7] IEC 61000-5-7 (2001), *Electromagnetic compatibility (EMC) – Part 5-7: Installation and mitigation guidelines – Degrees of protection provided by enclosures against electromagnetic disturbances (EM code)*.

[b-IEC 61000-6-6] IEC 61000-6-6 (2003), *Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment*.

IEC-HPEM

[b-IEC 61000-1-5] IEC/TR 61000-1-5 (2004), *Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems*.

[b-IEC 61000-4-20] IEC 61000-4-20 (2010), *Electromagnetic compatibility (EMC) – Part 4-20: Testing and measurement techniques – Emission and immunity testing in transverse electromagnetic (TEM) waveguides.*

[b-IEC 61000-4-33] IEC 61000-4-33 (2005), *Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters*.

IST in Japan

[b-IST SG] IST (Information Security Technology study group).
<http://www.ist-sg.jp/index.html>

Architectural Institute of Japan – Measurement methods (in Japanese)

[b-AIJ cond] Architectural Institute of Japan, Environmental Engineering Committee, Electromagnetic Environment Committee, *Method of Measuring Conductive Noise in Power Lines and Communication Lines*.
<http://news-sv.aij.or.jp/kankyo/s4/wg/keisoku/denji/sensok.pdf>.

[b-AIJ build] Architectural Institute of Japan, Environmental Engineering Committee, Electromagnetic Environment Committee, *Method of Measuring Electromagnetic Shield Room Performance at a Building Site*.
<http://news-sv.aij.or.jp/kankyo/s4/wg/keisoku/denji/roomkai.pdf>.

[b-AIJ mat] Architectural Institute of Japan, Environmental Engineering Committee, Electromagnetic Environment Committee, *Method of Measuring Electromagnetic Shield Material Performance*.
<http://news-sv.aij.or.jp/kankyo/s4/wg/keisoku/denji/zaisok.pdf>.

[b-AIJ perf] Architectural Institute of Japan, Environmental Engineering Committee, Electromagnetic Environment Committee, *Method of Testing Electromagnetic Shield Performance of Materials.*
<http://news-sv.aij.or.jp/kankyo/s4/wg/keisoku/denji/zaikai.pdf>.

[b-AIJ shield] Architectural Institute of Japan, Environmental Engineering Committee, Electromagnetic Environment Committee, *Method of Measuring Electromagnetic Shield Room Performance.*
<http://news-sv.aij.or.jp/kankyo/s4/wg/keisoku/denji/roomsok.pdf>.

Standards related to IT security

[b-ISAC 210-1.0] JIP ISAC 210-1.0 (2002), *Japan Information Processing Development Corporation ISMS guide*.

[b-ISO/IEC 15408-1] ISO/IEC 15408-1 (2009), *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/IEC 15408-2] ISO/IEC 15408-2 (2008), *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*.

[b-ISO/IEC 15408-3] ISO/IEC 15408-3 (2008), *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002 (2013), *Information technology – Security techniques – Code of practice for information security management*.

Other standards related to shield measurement methods

[b-CISPR 17] CISPR 17 (1981), *Methods of measurement of the suppression characteristics of passive EMC filtering devices*.

[b-IEC TS 61587-3] IEC/TS 61587-3 (1999), *Mechanical structures for electronic equipment – Tests for IEC 60917 and IEC 60297 – Part 3: Electromagnetic shielding performance tests for cabinets, racks and subracks*.

[b-IEEE 299] IEEE 299 (2006), *IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures*.

Other documents

[b-EN 55024] EN 55024 (2010), *Information technology equipment. Immunity characteristics. Limits and methods of measurement*.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-JOLT] Baum, C.E. *et al.* (2004), *JOLT: A highly directive, very intensive, impulse-like radiator*, Proceedings of the IEEE, Vol. 92, No. 7.

[b-NEBS GR-1089] NEBS GR-1089 (2011), *Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunications Equipment*.

[b-NEBS SR-3580] NEBS SR-3580 (2012), *NEBS Criteria Levels*.

[b-NTT TR 549001] NTT TR 549001 (2005), *Technical Requirements for Immunity of Telecommunications Equipment*.

HEMP documents

[b-Agrawal] Agrawal, A., Price, J., Gurbaxani, S. (May 1980), *Transient Response of a Terminated Two-wire Transmission Line Excited by a Non-uniform Electromagnetic Field*, IEEE Transactions on EMC, Vol. 22, No. 2, pp. 119-129.

[b-Barnes] Barnes, P. (February 1974), *The Effects of Electromagnetic Pulse (EMP) on State and Local Radio Communications*, Oak Ridge National Laboratory, ORNL-4873.

[b-blast] *U.S. Fires Atomic Blast 200 miles Over Pacific*, Front page headline and article in the New York Tribune, European Edition, 10 July 1962.

[b-Eichler] Eichler, C., Legro, J., Barnes, P.R. (April 1989), *Experimental determination of the effects of steep front-short duration surges on 25 kVA pole mounted distribution transformers*, Power Delivery, IEEE Transactions, Vol. 4, No. 2, pp. 1103-1110.

[b-Ellis] Ellis, V.J. (June 1989), *Consumer Electronics Testing to Fast-Rise EMP (VEMPS II Development)*, Harry Diamond Laboratories, HDL-TR-2149.

[b-EMP] *EMP Engineering and Design Principles*, Bell Laboratories, 1975.

[b-Glasstone] Glasstone, S., Dolan P. (1977), *The Effects of Nuclear Weapons*, U.S. Department of Defense and Energy Research and Development Administration.

[b-Greetsai] Greetsai *et al*. (November 1998), *Response of long lines to nuclear high-altitude electromagnetic pulse (HEMP), Electromagnetic Compatibility, IEEE Transaction on* Vol. 40, No. 4, pp. 348-354.

[b-Hansen] Hansen, D., Schaer, H., Koenigsten, D., Hoitink, H., Garbe, H., Giri, D. (February 1990), *Response of an overhead wire near a NEMP simulator*, Electromagnetic Compatibility, IEEE Transactions, Vol. 32, No. 1, pp. 18-27.

[b-Ianoz] Ianoz, M., Rachidi, R., Mazzetti, C., Nucci, C.A. (October 1993), *Response of multiconductor power lines to close indirect lightning strokes*, Proc. CIGRE Symposium, Power System EMC, Lausanne, paper 200-07.

[b-Imposimato] Imposimato, C., Pandini, L., Bottari, E., Inzoli, L. (February 1999), *Evaluation of the Radiated Lightning Coupling on Real Medium Voltage Power Lines by an EMP Simulator*, 13th International Zurich Symposium on EMC, paper 62J6.

[b-Loborev] Loborev, V. (June 1994), *Up to Date State of the NEMP Problems and Topical Research Directions*, Proceedings of the European Electromagnetics International Symposium – EUROEM 94, pp. 15-21.

[b-Parfenov] Parfenov, Yu. (October 1998), *Reality of EMP Effect*, Memorandum.

[b-Tesche] Tesche, F. (1987), *Discussion of EMP,* Paper by M. Rabinowitz, IEEE Transactions on Power Delivery, PWRD-2, p. 1213.

[b-Vittitoe] Vittitoe, C. (April 1989), *Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?* Sandia National Laboratories, SAND88-3341.

HPEM documents

[b-Agee] Agee, F. J., Baum, C. E., *et al*. (June 1992), *Ultra-Wideband Transmitter Research*, IEEE Transactions on plasma science, Vol. 26, No. 3.

[b-Baum EMP] Baum, C.E. (June 1992), *From the Electromagnetic Pulse to High-Power Electromagnetics*, Proceedings of the IEEE, Vol. 80, No. 6.

[b-Baum High] Baum, C. E., Lehr, J. M. (October 2002), *Tapered Transmission-Line Transformers for Fast High-Voltage Transients*, IEEE Transactions on plasma science, Vol. 30, No. 5.

[b-Baum Resp] Baum, C.E. (August 1992), *Maximization of Electromagnetic Response at a Distance*, IEEE Transactions on EMC, Vol. 34, No. 3.

[b-Giri] Giri, D. V., Baum, C. E., *et al.* (October 2000), *Intermediate and Far Fields of a Reflector Antenna Energized by a Hydrogen Spark-Gap Switched Pulser*, IEEE Transactions on plasma science, Vol. 28, No. 5.

[b-Mianoz] Ianoz, M., Radasky, W. A., (1996), *Modeling of an EMP Conducted Environment*, IEEE Transactions on EMC, Vol. 38, No. 3.

[b-Mikheev] Mikheev, O. V., *et al*. (February 1997), *New Method for Calculating Pulse Radiation from an Antenna With a Reflector*, IEEE Transactions on electromagnetic compatibility, Vol. 39, No. 1.

[b-Prather] Prather, W.D., Baum, C. E., *et al*. (October 2000), *Ultra-Wideband Source and Antenna Research*, IEEE Transactions on plasma science, Vol. 28, No. 5.

[b-Silfverskiold 1] Silfverskiold, S., *et al*. (August 1999), *Induced Voltages in a Low-Voltage Power Installation Network Due to Lightning Electromagnetic Fields: An Experimental Study*, IEEE Transactions on electromagnetic compatibility, Vol. 41, No. 3.

[b-Silfverskiold 2] Silfverskiold, S., *et al*. (February 2002), *Microwave Field-to-Wire Coupling Measurements in Anechoic and Reverberation Chambers*, IEEE Transactions on electromagnetic compatibility, Vol. 44, No. 1.

EMSEC documents

[b-DOD eval] DOD 5200.28-STD (1985), *Department Of Defense Trusted Computer System Evaluation Criteria*, United States Department of Defense.

[b-DOD rev] MIL-HDBK-232A (1987), *Red/Black Engineering-Installation Guidelines*, United States Department of Defense.

[b-Kuhn EMan] Kuhn, Markus G. (1998), *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, Information Hiding 1998, LNCS 1525, pp. 124-142.

[b-Kuhn home] Dr Markus Kuhn's home page, <http://www.cl.cam.ac.uk/~mgk25/>.

[b-Loughry] Loughry Joe, (August 2002), *Information Leakage from Optical Emanations*, ACM Transactions on Information and System Security, Vol. 5, No. 3.

[b-NSA 2-95] National Security Agency, *TEMPEST/2-95, Red/Black Installation Guidance*, Fort George G. Meade, Md, 1995, <http://cryptome.org/tempest-2-95.htm>.

[b-NSA 94-106] Specification NSA No. 94-106 (1994), *Specification for Shielded Enclosures*, National Security Agency, Fort George G. Meade, Md. <http://cryptome.org/nsa-94-106.htm>.

[b-NSA 5000] National Security Agency, *NACSIM 5000 TEMPEST Fundamentals*, National Security Agency, Fort George G. Meade, 1992, Md. <http://cryptome.org/jya/nacsim-5000/nacsim-5000.htm>.

[b-Smulders] Smulders, P. (1990), *The threat of information theft by reception of electromagnetic radiation from RS-232 cables*, Computer &. Security, No. 9, pp. 53-58.

[b-Temp End] *TEMPEST: A Signal Problem*, <http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf>.

[b-Temp Maint] NSTISSAM/TEMPEST 1-00 (December 2000), *Maintenance and Disposition of TEMPEST Equipment*, National Security Telecommunications and Information Systems Security Committee.

[b-TEMPEST] The Complete, Unofficial TEMPEST Information Page, <http://cryptome.org/> and others.

[b-Van Eck] Van Eck, W. (1985), *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, Computer & Security No. 4, pp. 269-286.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	**Protection against interference**
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015