International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series K

Supplement 5

(04/2016)

SERIES K: PROTECTION AGAINST INTERFERENCE

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

ITU-T K-series Recommendations – Supplement 5

Supplement 5 to ITU-T K-series Recommendations

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

Summary

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 information security management system (ISMS).

Supplement 5 to ITU-T K-series Recommendations presents evaluation and calculation examples for the threat of an intentional high-altitude electromagnetic pulse (HPEM) attack. The HPEM sources considered are those presented in IEC 61000-2-13, as well as some additional sources that have emerged more recently.

This Supplement also provides information on the vulnerability of telecom equipment, and presents the example of vulnerability. It is desirable that the equipment meets 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 Suppl. 5	2016-04-27	5	11.1002/1000/12965

Keywords

Electromagnetic security, electrostatic discharge, high-altitude electromagnetic pulse, HPEM, IEMI, immunity, resistibility.

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Introduction

In order to establish the sufficient mitigation to HPEM attacks, it is extremely important that the threat level (electric field strength) and the vulnerability of telecom equipment are adequately estimated. This Supplement provides the calculation examples of threat level from various sources presented in IEC 61000-2-13. The vulnerability examples of telecom equipment are also provided.

Supplement 5 to ITU-T K-series Recommendations

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

1 Scope

This document is a supplement to ITU-T K.81. This Supplement presents evaluation and calculation examples for the threat of an intentional HPEM attack.

2 References

[ITU-T K.20] Recommendation ITU-T K.20 (2016), *Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents*.

[ITU-T K.21] Recommendation ITU-T K.21 (2016), *Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents*.

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

[ITU-T K.45] Recommendation ITU-T K.45 (2016), *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.81] Recommendation ITU-T K.81 (2016), *High-power electromagnetic immunity guide for telecommunication systems*.

[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 Supplement 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 confidentiality [ITU-T K.81]: 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.

3.1.3 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.).

3.1.4 EM mitigation [ITU-T K.81]: 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.

3.1.5 electromagnetic emanations security [ITU-T K.81]: Physical constraints to prevent information compromise through signals emanated by a system, particularly the application of TEMPEST technology to block electromagnetic radiation.

3.1.6 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.

3.1.7 vulnerability [ITU-T K.81]: The possibility that the equipment does not function correctly when exposed to HEMP or HPEM.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AM	Amplitude Modulation
CB	Citizen Band
CW	Continuous Wave
DC	Direct Current
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMSEC	EM emanations Security
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

NEBS Network Equipment Building Systems

PC Personal Computer

SE Shield Effect

TCP Transfer Control Protocol

VSWR Voltage Standing Wave Ratio

5 Conventions

None.

6 Calculating HPEM threat

6.1 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 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 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 1 in [ITU-T K.81]). 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.

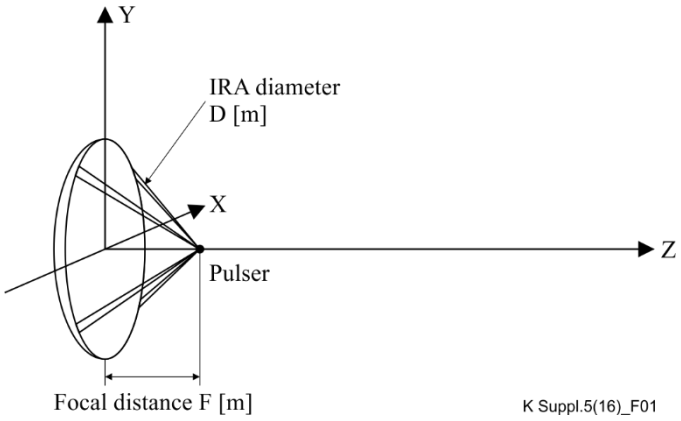


Figure 1 – Image of an IRA

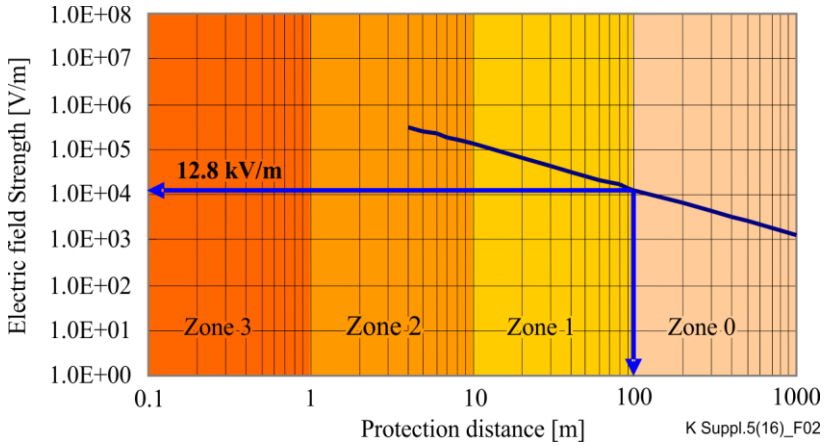


Figure 2 – Relationship between the IRA peak electric field strength and the protection distance (Pulse voltage: 60 kV, parabolic reflector diameter: 3.66 m)

Figure 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 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 3(b) shows the return loss (S_{11} parameter) and the voltage standing wave ratio (VSWR) characteristics of the same IRA.

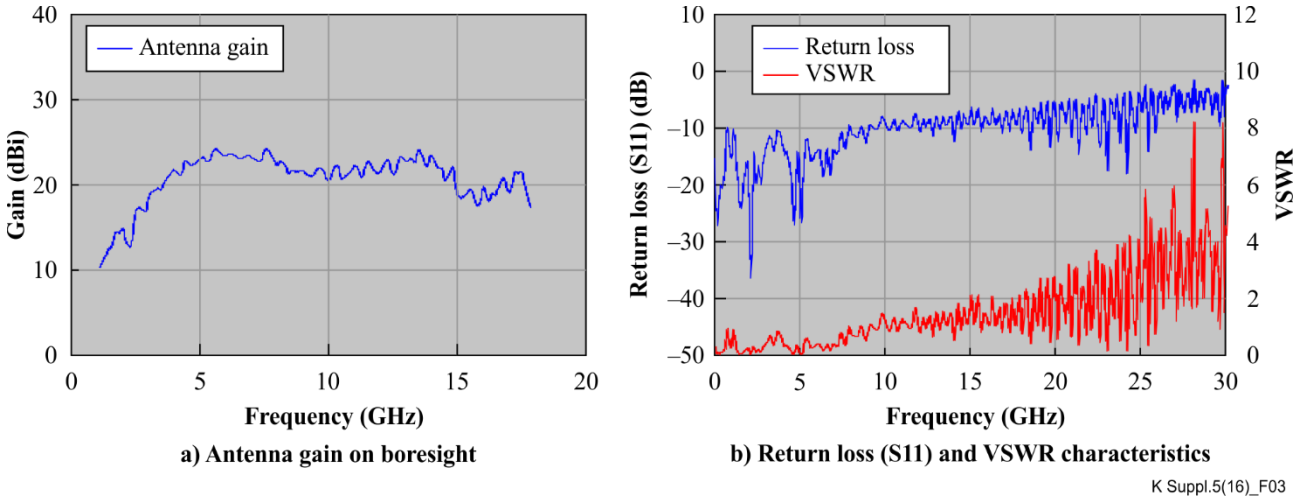


Figure 3 – Basic characteristics of the IRA (Farr Research, Inc.; IRA-3M)

Figure 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 4(a) and 4(c), respectively. The HPEM 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 4(b), and its frequency spectrum is shown in Figure 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.

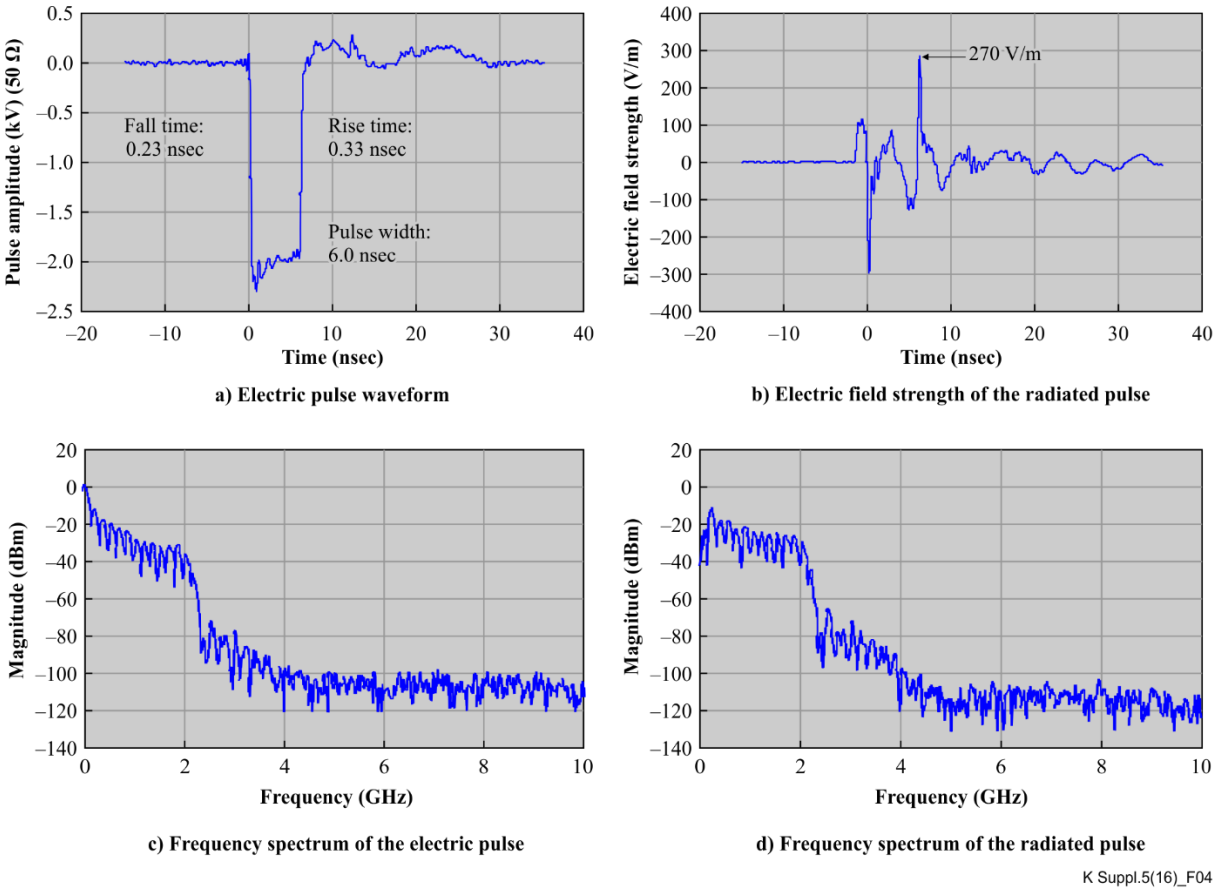


Figure 4 – Performance of the high-power electromagnetic pulse propagation of the IRA

The JOLT system is composed of an IRA antenna with a repetitive high impulse generator. Figure 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.

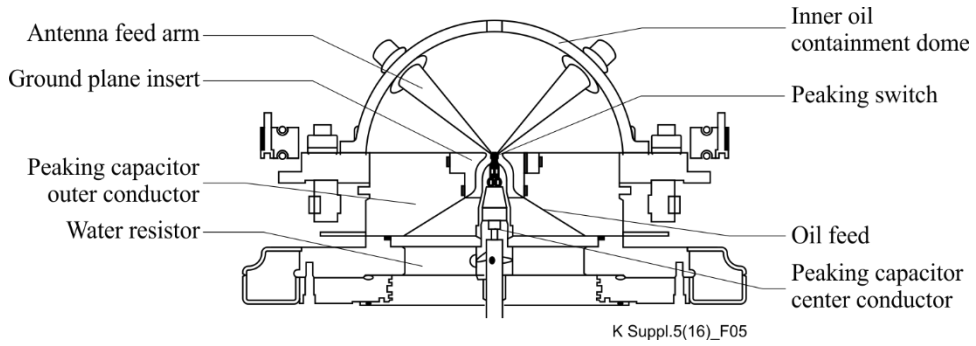


Figure 5 – Overview of the JOLT system

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

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

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

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 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 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 (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 (1) and the experimental results, respectively, 65 kV/m @ 85 m 5.4 MV and 62 kV/m @ 85 m 5.3 MV. Figure 6 shows the relationship between the JOLT peak electric field strength and the protection distance.

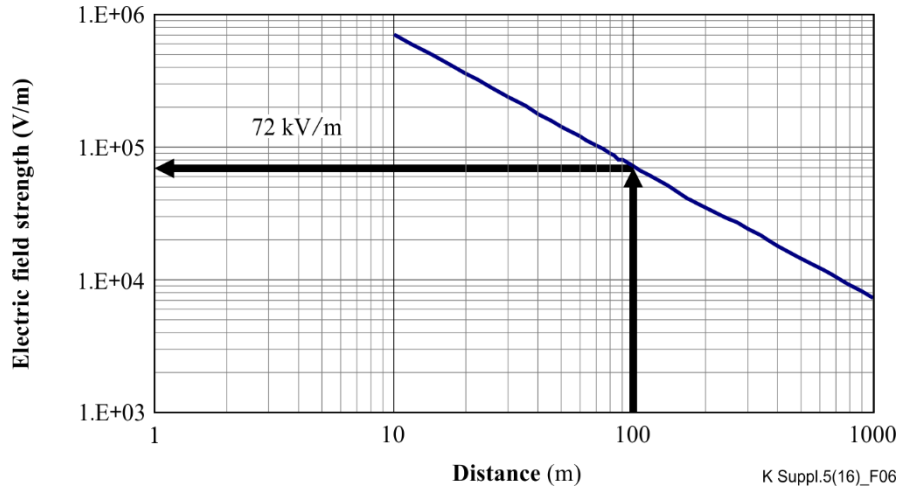


Figure 6 – Relationship between the JOLT peak electric field strength and the protection distance (Case #5 in Table 1; reflector diameter: 3.048 m)

6.2 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 (3) and (4).

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

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

where:

E_a: the electric field strength at the opening

A: the area of the antenna opening

λ: the wavelength

r: the distance

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

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

F: 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 (3) and (4) are used to find the relationship between the electric field strength and the distance and the result is as shown in Figure 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.

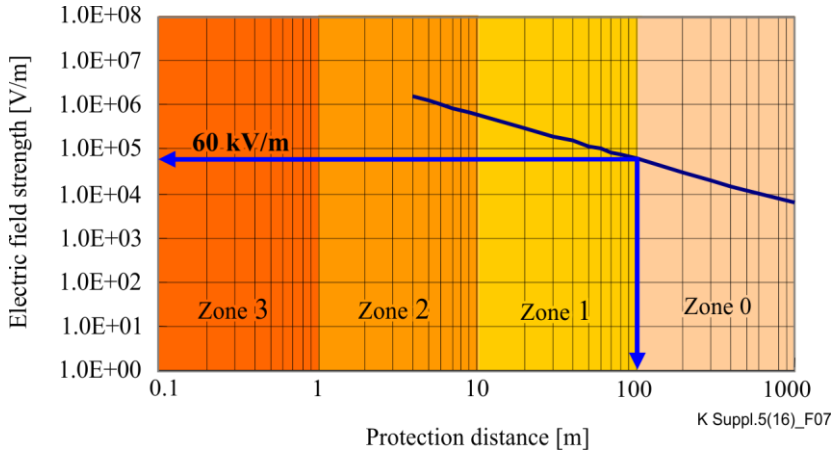


Figure 7 – Relationship between the peak electric field strength of a commercial radar and protection distance (peak transmission output: 5 MW; transmission duty: 50%; transmission efficiency: 100%)

6.3 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 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 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 (5) [b-NEBS GR-1089]. Also, the relationship between the electric field strength and distance in remote field conditions is found from Equation (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 (5) and (6), and is as shown in Figure 8.

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

where:

S: Opening area [m^2]

η: Opening efficiency

λ: Wavelength [m]

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

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.

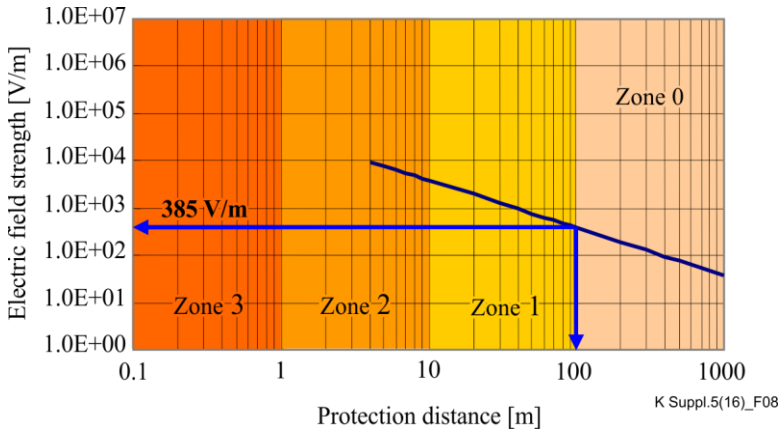


Figure 8 – Relationship between the peak electric field of a navigation radar and protection distance (peak transmission output: 12 kW; 51 cm parabolic antenna (34 dBi); transmission efficiency: 100%)

6.4 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 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 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 4 and Figure 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 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 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 5 and Figure 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 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 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 (6), the results are as shown in Figure 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 (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.

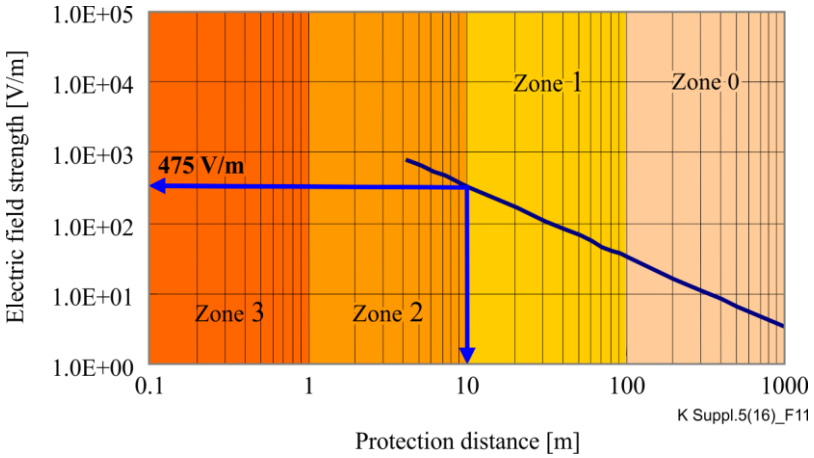


Figure 11 – Relationship between the peak electric field strength of a magnetron generator and protection distance (frequency: 2.46 GHz; peak transmission output: 1.8 kW; antenna gain: 24 dBi; transmission efficiency: 100%)

6.5 Illegal citizen band radio

Citizen band (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 (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 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.

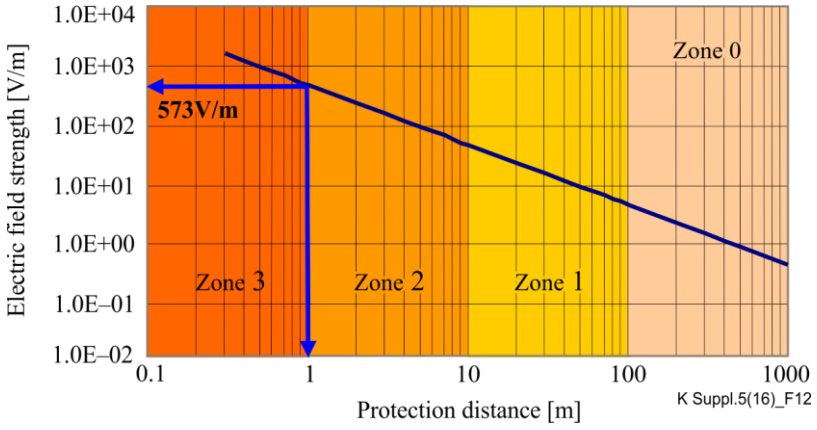


Figure 12 – Relationship between the peak electric field strength of an illegal CB radio and the protection distance (peak transmission output: 4 kW; antenna gain: 2.15 dBi; transmission efficiency: 100%)

6.6 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 (amplitude modulation (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 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 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 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 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 (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 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 (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.

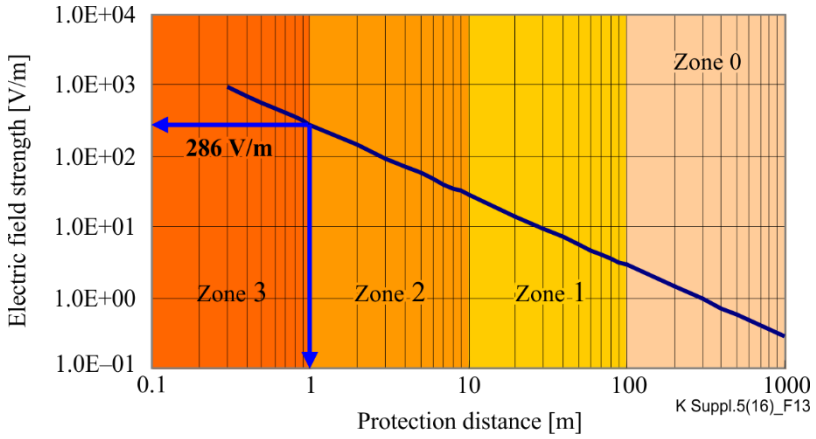


Figure 13 – Relationship between the peak electric field strength of a stationary-type amateur radio and protection distance (peak transmission output: 3.5 W; antenna gain: 2.15 dBi; transmission efficiency: 100%)

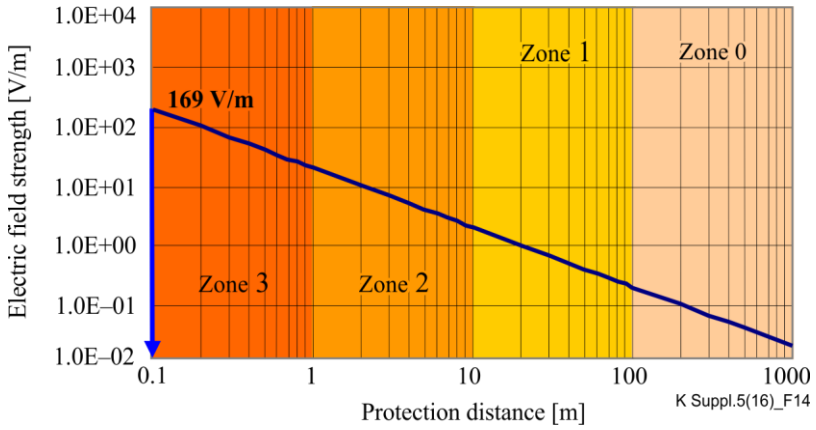


Figure 14 – Relationship between the peak electric field strength of a hand-held type amateur radio and protection distance (peak transmission output: 3.5 W; antenna gain: 2.15 dBi; transmission efficiency: 100%)

6.7 Stun gun

Stun guns are commercially sold as a static-electricity generating device for personal protection and as shown in Figure 15, they use a capacitor charge/discharge circuit to generate a high-voltage impulse. The voltage generated from the circuit shown in Figure 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 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.

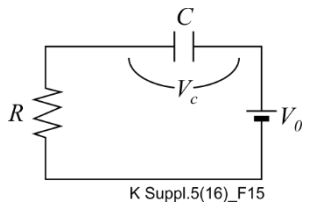


Figure 15 – Charge/discharge circuit that uses a capacitor

Figure 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 (7).

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

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 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).

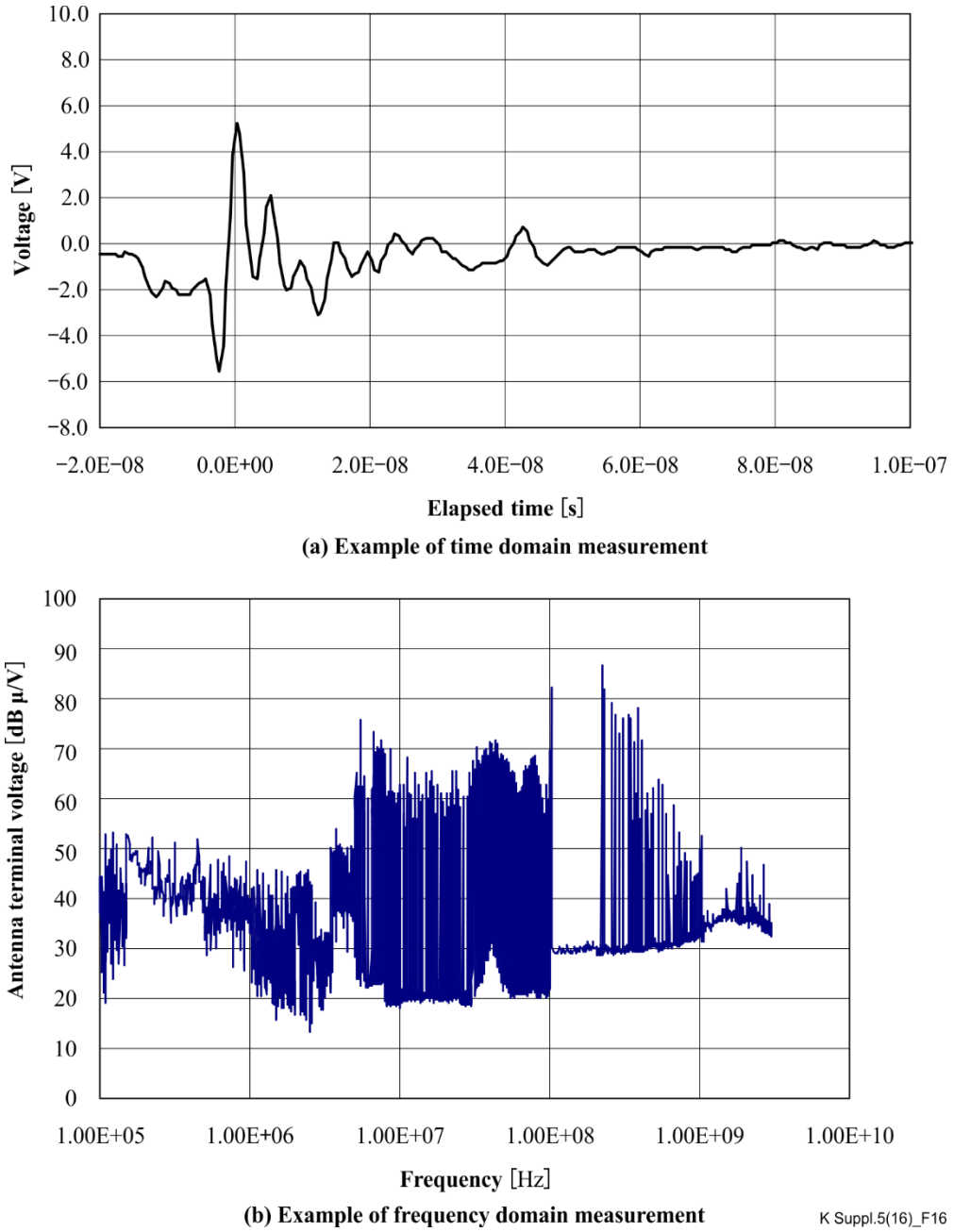


Figure 16 – Examples of electric field measurement of the radiation from a stun gun (discharge voltage: 500 kV)

In the case of a discharge in air by the circuit shown in Figure 15, $R \approx \infty$, 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.

6.8 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 7 and Figure 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 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 17 – Examples of lightning-surge generators

6.9 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 8 and Figure 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 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 18 – Examples of CW and burst generators

6.10 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 does 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.

7 Vulnerability of IT equipment

7.1 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 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 10.

Table 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 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 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 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).

Table 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
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.
	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 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

7.2 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).

7.2.1 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 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.

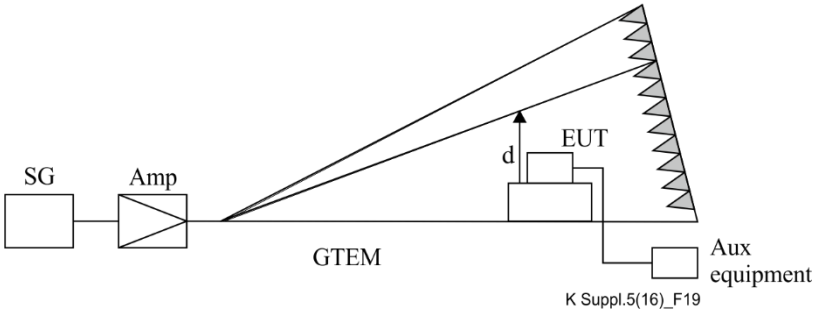
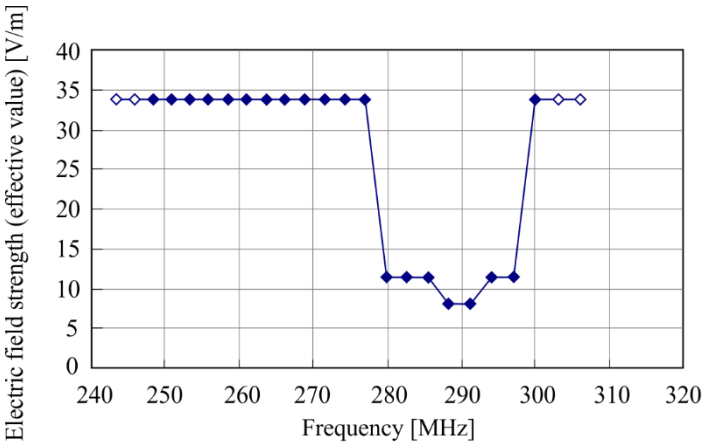
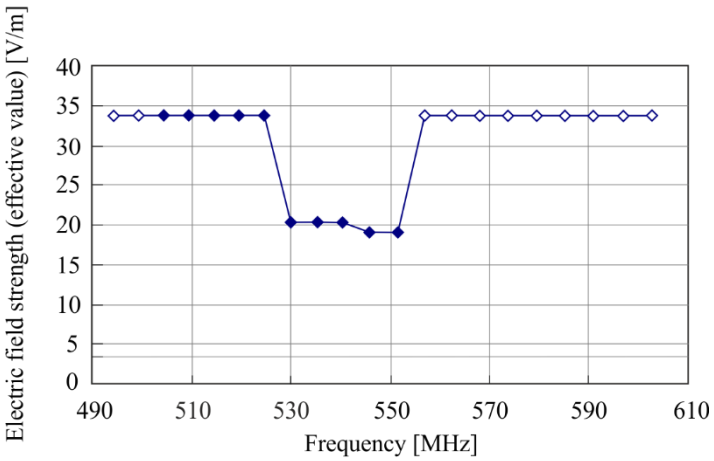


Figure 19 – Vulnerability evaluation system for a radiated electromagnetic field

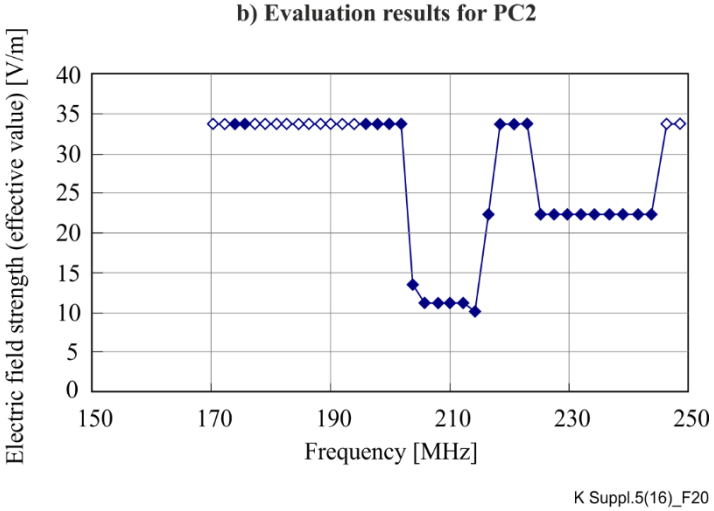
The evaluation results are shown in Figure 20 and Table 12. Figure 20 shows the frequency along the horizontal axis. The electric field that was applied during testing is shown along the vertical axis. The white dots show that malfunctions did not occur at that electric field strength (in other words, 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 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 10 in clause 7.1. 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 20 – Evaluation results for vulnerability to radiated electromagnetic waves

Table 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	–

7.3 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.

Bibliography

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

[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*.

[b-TEMPEST] National Security Agency (NSA), *The TEMPEST: A Signal Problem* <https://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf>

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016