International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

K.81

(06/2016)

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. ITU-T K-Supplement 5 provides the calculation results of the intentional HPEM threats. 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 example of vulnerability is provided in ITU-T K-Supplement 5. 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.

The 2016 version of this Recommendation deletes Appendices I, II and III. Appendix I was republished as Supplement 5 to the K-series Recommendations, and the relevant parts of Appendix II were transferred to ITU-T K.115.

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
3.0	ITU-T K.81	2016-06-29	5	11.1002/1000/12877

* 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.

Keywords

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

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 2016. 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 (2015), *Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents*.

[ITU-T K.21] Recommendation ITU-T K.21 (2015), *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 (2015), *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.

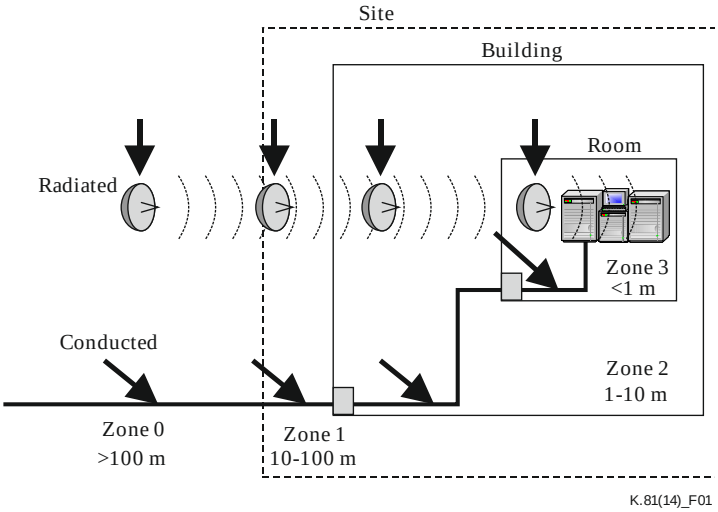

Figure 1 – Classification of intrusion areas

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 [b-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 [b-ITU-T K-Sup.5].

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 [b-ITU-T K-Sup.5].

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.

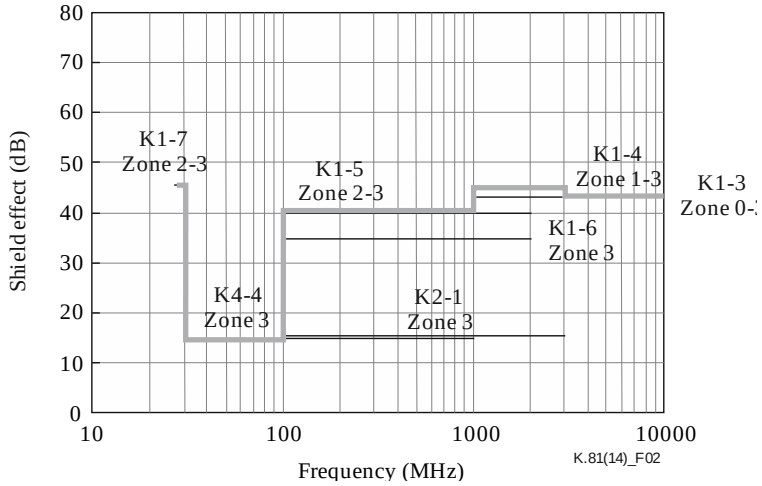

Figure 2 – Example of the calculation of the relationship between the EM mitigation level and frequency

Bibliography

[b-ITU-T K-Sup.5] ITU-T K-series Recommendations – Supplement 5 (2016), *ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems*.

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

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

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