

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

K.84

(01/2011)

SERIES K: PROTECTION AGAINST INTERFERENCE

Test methods and guide against information leaks through unintentional electromagnetic emissions

Recommendation ITU-T K.84



International
Telecommunication
Union

Documents
Document Sharing Hub

Copyright International Telecommunication Union/ITU Telecommunication Sector

Recommendation ITU-T K.84

Test methods and guide against information leaks through unintentional electromagnetic emissions

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.

When security is managed taking the above references into consideration, we should evaluate the threats and mitigate their impact against equipment or sites. Threats are related to confidentiality in the ISMS.

Recommendation ITU-T K.84 describes threats from information leakage due to unintentional electromagnetic emanations, and the two approaches of mitigation, i.e., reduction of emission from equipment and the level of site shielding are described. Information leakage test methods for conducted and radiated emission are presented.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T K.84	2011-01-13	5

Keywords

Emission, EMC, emission, ISMS, security, shield.

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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations.....	3
5 Test method and guide for EMSEC.....	3
5.1 Threats against EMSEC	3
5.2 Security management approach.....	4
5.3 EMSEC requirements for radiation	5
5.4 EMSEC requirements for conducted emission.....	7
Annex A – Methods of testing for radiation in EMSEC.....	9
A.1 Overview	9
A.2 General requirements for measurement.....	9
A.3 Method of testing for radiation leakage (Wideband method)	10
A.4 Method of testing for radiation leakage (Narrow-band method).....	11
Annex B – Methods of testing for conductive coupling in EMSEC.....	14
B.1 Overview	14
B.2 General requirements for measurement.....	14
B.3 Method of testing for conducted leakage	14
Appendix I – Threat of EMSEC	16
I.1 Electromagnetic wave leakage	16
I.2 Method of estimating possible distance for information leakage.....	17
Appendix II – Confidentiality of IT equipment.....	20
Appendix III – Example of wideband measurement	22
Appendix IV – Example of narrow-band measurement	24
Bibliography.....	26

Introduction

Radio waves are unintentionally emitted from information technology equipment, and there have been cases where information has been reproduced by electromagnetic waves being received. Information leakage due to unintentional electromagnetic radiation from equipment is related to physical security in adopting the information security management system (ISMS) based on [ITU-T X.1051], [ISO/IEC 27001], [ISO/IEC 27002] and [b-IEC 17799]. This phenomenon is referred to as EMSEC (emanation security or Electromagnetic emanation security) in this Recommendation. It is important to prevent a lack of confidentiality due to unintentional electromagnetic radiation, particularly in equipment that is handling important information. This Recommendation describes threats and confidentiality related to EMSEC, and two approaches to mitigation methods. The first approach involves emission requirements for equipment and the second involves shielding requirements for sites, when equipment that is examined with existing EMC emission standards such as [ITU-T K.48] and [CISPR 22] is installed at a site.

Recommendation ITU-T K.84

Test methods and guide against information leaks through unintentional electromagnetic emissions

1 Scope

It is the purpose of this Recommendation to prevent information leakage due to unintentional electromagnetic radiation from telecommunication equipment handling important information, when the telecommunication equipment or sites are managed by ISMS.

This Recommendation gives guidance to reduce the threats from information leakage due to unintentional electromagnetic emanation from information equipment at telecommunication centres.

Information is transmitted through electromagnetic waves unintentionally radiated from many kinds of equipment such as personal computers, data servers, laser printers, keyboards, and cryptographic modules. Amongst them, this Recommendation treats only information leakage from equipment including raster scan video signal. Further study is needed on issues involving other kinds of leaked signals.

Two approaches to protect against threats are given in this Recommendation.

The first approach is:

Emission requirements and methods of examining equipment are applied when the equipment cannot be installed in the shielding site, which should reduce the emission of the equipment.

The second approach is:

Shielding requirements for sites such as buildings are applied when the equipment can be installed at secure sites.

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.42] Recommendation ITU-T K.42 (1998), *Preparation of emission and immunity requirements for telecommunication equipment – General principles*.
- [ITU-T K.48] Recommendation ITU-T K.48 (2006), *EMC requirements for telecommunication equipment – Product family Recommendations*.
- [ITU-T K.78] Recommendation ITU-T K.78 (2009), *High altitude electromagnetic pulse immunity guide for telecommunication centres*.
- [ITU-T K.81] Recommendation ITU-T K.81 (2009), *High-power electromagnetic immunity guide for telecommunication systems*.
- [ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

- [CISPR 16-1] CISPR 16-1 (All parts), *Specification for radio disturbance and immunity measuring apparatus*.
- [CISPR 16-2] CISPR 16-2 (All parts), *Specification for radio disturbance and immunity measuring apparatus and methods*.
- [CISPR 22] CISPR 22 ed 5.2 (2006), *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*.
- [ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.
- [ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 availability [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 [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. EMSEC is a threat to this confidentiality. In this Recommendation, if the equipment cannot be mitigated itself, the emission values of existing electromagnetic compatibility (EMC) requirement show the level of this confidentiality. The details are described in Appendix II.

3.2.2 electromagnetic emanations security (EMSEC): Physical constraints to prevent information compromised through signals emanated by a system, particularly by the application of TEMPEST technology to block electromagnetic radiation. In this Recommendation, the term EMSEC is used only for information leakage due to unintentional electromagnetic emission.

3.2.3 threat: A potential security violation which could lead to a lack of confidentiality due to an insufficient electromagnetic emanation security (EMSEC). Examples of threats are described in clause 5.

3.2.4 time varying stripe: A vertical stripe pattern whose vertical lines vary. The number of stripes on the VSP increases from 1 to half the number of horizontal pixels over time.

3.2.5 vertical stripe pattern: White vertical lines on a black screen on VDU of the equipment under test (EUT). The width of the white and black lines are the same.

3.2.6 vulnerability: The possibility that equipment will function falsely with EMSEC.

4 Abbreviations

This Recommendation uses the following abbreviations:

AMN	Artificial Mains Network
BPF	Band Pass Filter
EMC	Electromagnetic Compatibility
EMSEC	Emanation security or Electromagnetic emanation security
EUT	Equipment Under Test
ISMS	Information Security Management System
LM	Level Meter
NEBS	Network Equipment Building Systems
NF	Noise Figure
RBW	Resolution Bandwidth
SN	Signal to Noise ratio
TVS	Time Varying Stripe (pattern)
VBW	Video Bandwidth
VDU	Video Display Unit/Visual Display Unit
VESA	Video Electronics Standards Association
VSP	Vertical Stripe Pattern

5 Test method and guide for EMSEC

5.1 Threats against EMSEC

EMSEC threats are determined according to comparisons of the confidentiality and threat levels as given in clause 5 of [ITU-T K.81]. The threat level is determined by intrusion range, portability and availability of the threat devices. The threat of EMSEC is described in Appendix I. The confidentiality level of the equipment, which is evaluated with existing EMC standards, is presented in Appendix II. Examples of threats against EMSEC are summarized in Table 5.1-1. Definitions of threat related to portability levels and threat availability levels are presented in Tables 5.1-2 and 5.1-3. The availability level shall be thought of as a measure of both the cost and the technological sophistication of the threat devices such as receivers, antennas and so on.

Table 5.1-1 – Examples of threats related to information leakage

Types of threats	Examples of receiver	Possible distance for EMSEC		Threat level			Threat number
		Confidentiality level class A	Confidentiality level class B	Intrusion range on attack side	Portability	Availability	
EMSEC	Special receiver	330 m ^{a)}	105 m ^{a)}	Zone 0	PIII	AIV	K4-1
	Special receiver	330 m ^{a)}	105 m ^{a)}	Zone 1	PIII	AIV	K4-2
	General-purpose EMC receiver	59 m ^{a)} 263 m	19 m ^{a)} 83 m	Zone 1	PII	AIII	K4-3
	General-purpose EMC receiver	59 m ^{a)} 263 m	19 m ^{a)} 83 m	Zone 2	PII	AIII	K4-4
	Amateur receiver	33 m ^{a)} 148 m	11 m ^{a)} 47 m	Zone 1	PII	AII	K4-5
	Amateur receiver	33 m ^{a)} 148 m	11 m ^{a)} 47 m	Zone 2	PII	AII	K4-6
	Amateur receiver	33 m ^{a)} 148 m	11 m ^{a)} 47 m	Zone 3	PII	AII	K4-7
a) Assumed to have reinforced concrete walls as 13 dB attenuation.							

Table 5.1-2 – 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 or in clothing. NOTE 2 – This portability level applies to threat devices that are too large to be hidden in the human body or in clothing, but is still small enough to be carried by a person (such as in a briefcase or a backpack). NOTE 3 – This portability level applies to threat devices that are too large to be easily carried by a person, but large 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.	

Table 5.1-3 – Definitions of threat availability levels

Availability level	Definition	Examples
AI	'Consumer'	
AII	'Hobbyist'	Amateur receiver
AIII	'Professional'	General-purpose EMC receiver
AIV	'Bespoke'	Special receiver

5.2 Security management approach

From Table 5.1-1, when the threat level is assumed to be AII (amateur receiver level) and the confidentiality level is assumed to be Class B, for example, and the threat device never gets closer than 47 m, security is well managed. Therefore, no additional mitigation is necessary.

Where the possibility that the threat device will get closer is high, e.g., when the customer must operate the equipment near a window or it is installed near a window, the presence of information leakage due to unintentional electromagnetic radiation should be assessed. The requirement level of equipment is described in clause 5.3, and the test method is explained in Annex A.

Where the possibility that the threat device will get closer is low, e.g., the equipment is installed at a secure site and is surrounded by walls, the walls separate the distance between the equipment and the threat device. Confidentiality can be maintained with a shield and the use of equipment that is explained in the existing EMC emission standards. The level of requirement for shielding is described in clause 5.4.

5.3 EMSEC requirements for radiation

Electromagnetic emanations containing information signals from electrical and electronic equipment should be attenuated to less than the E_{th} (minimum EM level whose information can be detected). The E_{th} is defined by the sensitivity of receiver and gain of antenna. An example is shown in Appendix I.

Electromagnetic emanation from equipment in buildings is generally attenuated by the distance between the equipment and receiver and the walls of buildings. It is also attenuated by measures in the equipment itself and building shields. Therefore, the electromagnetic field strength at the receiver should be evaluated by taking into account the condition of site where the equipment is installed. The requirements of emission from the equipment and site shielding are determined according to this concept.

Figure 5.3-1 shows the EM level at the receiver evaluated from that at the distance of 1 m. Figure 5.3-2 shows the EM level variation, and the level at the receiver should be compared to the E_{th} and determine the threat.