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

# 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

Emanation, 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/.

## Table of Contents

## 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)]<br>263 m | 19 m[a)]<br>83 m | Zone 1 | PII | AIII | K4-3 |
| | General-purpose EMC receiver | 59 m[a)]<br>263 m | 19 m[a)]<br>83 m | Zone 2 | PII | AIII | K4-4 |
| | Amateur receiver | 33 m[a)]<br>148 m | 11 m[a)]<br>47 m | Zone 1 | PII | AII | K4-5 |
| | Amateur receiver | 33 m[a)]<br>148 m | 11 m[a)]<br>47 m | Zone 2 | PII | AII | K4-6 |
| | Amateur receiver | 33 m[a)]<br>148 m | 11 m[a)]<br>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 Eth (minimum EM level whose information can be detected). The Eth 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 Eth and determine the thread.

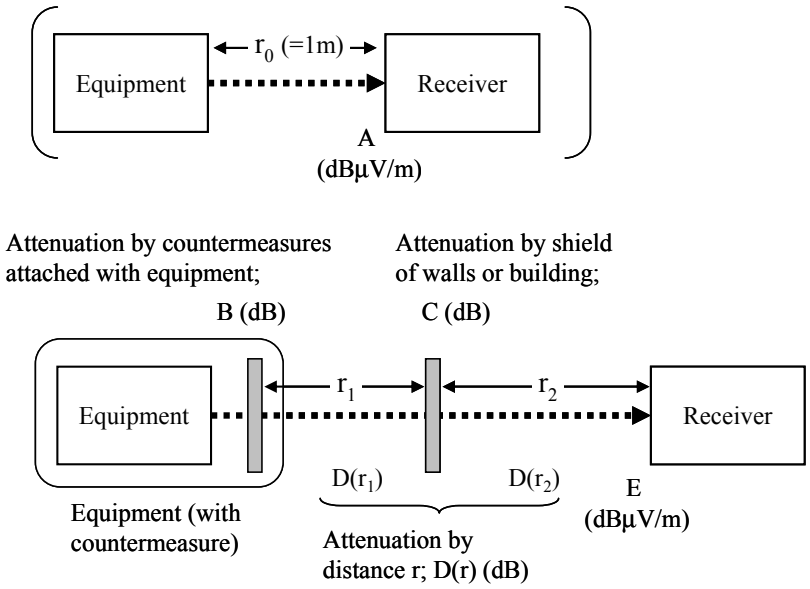



**Figure 5.3-1 – Attenuation of emission from equipment**

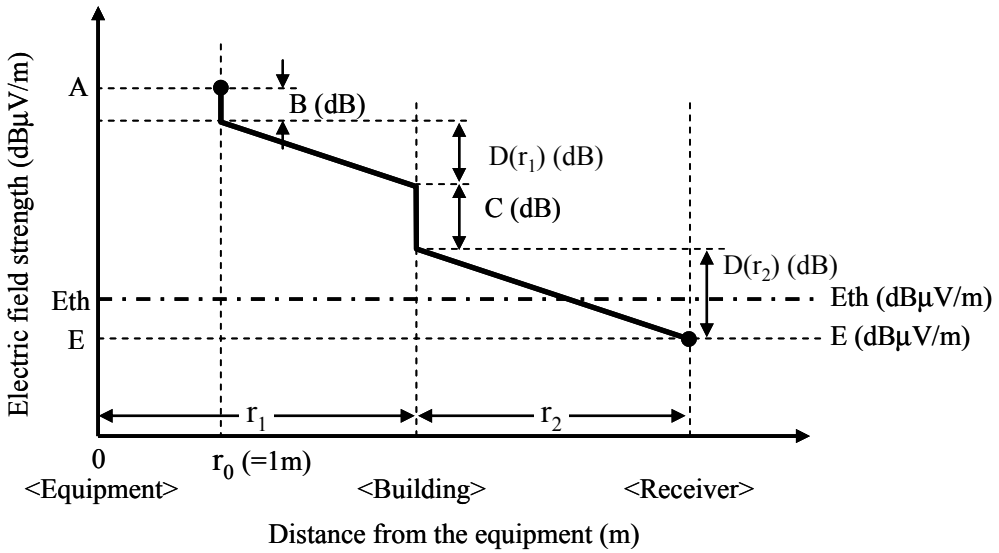



**Figure 5.3-2 – Attenuation emission from the equipment**

Attenuation calculated by the distance between the equipment and receiver is:

$$D(r_1 + r_2) = 20\log((r_1 + r_2))/r_0 \text{ [dB]} \qquad (5.3\text{-}1)$$

Consequently, the level of electric field strength at receiver E is derived from Equation 5.3-2.

$$E = A - B - C - D(r_1 + r_2) \qquad [\text{dB}\mu\text{V/m}] \qquad (5.3\text{-}2)$$

Where:

*A* is the electric field strength of the electromagnetic emanation containing the information signal measured at distance $r_0$(m) from the electrical and electronic equipment, *A* (dBμV/m).

*B* is the attenuation achieved by countermeasures attached to the equipment, *B* (dB).

*C* is the attenuation achieved by the building shield, *C* (dB).

*D*(*r*) is the attenuation achieved by the distance *r*(*m*), *D*(*r*) (dB).

$E$ is the electric field strength of electromagnetic emanation at a receiver, $E$ (dBμV/m).

$r_0$ is the standard distance for measuring the electric field strength, $r_0(m)$. The calculations of field strength are simplified if $r_0$ = 1 m.

$r_1$ is the distance between the equipment and building shield, $r_1(m)$.

$r_2$ is the distance between the building shield and receiver, $r_2(m)$.

If E is less than Eth, the information cannot be discriminated by the radiated emission, so the security of information is maintained.

$$E \le Eth \qquad [\mathrm{dB\mu V/m}] \tag{5.3-3}$$

### 5.3.1 For equipment

The level of requirements for equipment or equipment being measured is defined as in Equation 5.3.1-1.

$$A - B \le Eth + C + D(r_1 + r_2) \quad [\mathrm{dB\mu V/m}] \tag{5.3.1-1}$$

### 5.3.2 For building shield

The level of requirements for a building shield is defined as in Equation 5.3.2-1.

$$C \ge A - B - D(r_1 + r_2) - Eth \quad [\mathrm{dB}] \tag{5.3.2-1}$$

## 5.4 EMSEC requirements for conducted emission

Electromagnetic conducted emission containing information signals from electrical and electronic equipment should be attenuated to less than the Vth (minimum voltage level whose information can be detected). The test method is defined in Annex B.

Electromagnetic conducted emission from equipment in buildings is generally attenuated by filters installed in lines. The level of requirements is defined according to the following concept.

Figure 5.4-1 shows the level of conducted emission taking into account the reduction by filters at the equipment and the building. Requirements for the emission level of equipment and filters can be obtained by the comparison between V and Vth.

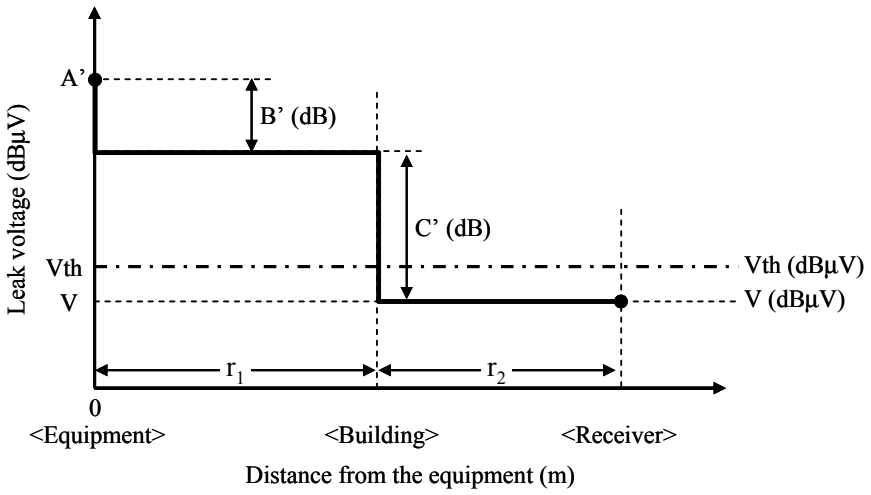



**Figure 5.4-1 – Levels for conducted emission from the equipment**

Here, the attenuation of conducted signals transmitting on the lines is negligible. Therefore, the signal level at the receiver V is derived from Equation 5.4-1.

$$V = A' - B' - C' \quad [\text{dB}\mu\text{V}] \tag{5.4-1}$$

Where:

$A'$ is the leaked voltage at the electrical and electronic equipment, $A'$ (dBμV).

$B'$ is the attenuation achieved by countermeasures in the conductive line connected to the equipment, $B'$(dB).

$C'$ is the attenuation achieved by countermeasures at the building shielded, $C'$ (dB).

$V$ is the leaked voltage at the receiver, $V$ (dBμV).

$r_1$ is the distance between the equipment and building shield, $r_1(m)$.

$r_2$ is the distance between the building shield and receiver, $r_2(m)$.

If $V$ is less than $Vth$, the information cannot be discriminated by the conducted emission, so the security of information is maintained.

$$V \leq Vth \quad [\text{dB}\mu\text{V}] \tag{5.4-2}$$

### 5.4.1 For equipment

The level of requirements for equipment or equipment being measured is defined as in Equation 5.4.1-1.

$$A' - B' \leq Vth + C' \quad [\text{dB}\mu\text{V}] \tag{5.4.1-1}$$

### 5.4.2 For building shields

The level of requirements for filters or shields on buildings is defined as in Equation 5.4.2-1.

$$C' \geq A' - B' - Vth \quad [\text{dB}] \tag{5.4.2-1}$$

# Annex A

# Methods of testing for radiation in EMSEC

(This annex forms an integral part of this Recommendation.)

## A.1 Overview

Two methods of measurement can be used, i.e., wideband and narrow-band receivers can be used, depending on the measurement bandwidth of the measuring receiver. The wideband method needs a special receiver that has a wide RBW (resolution bandwidth) of more than tens of megahertz and obtains results that are well correlated to the threat of information leakage, i.e., the resolution of the reconstructed image. However, a conventional spectrum analyser (RBW = 100 kHz) can be used in the narrow-band method, which has better sensitivity and can be used to analyse the frequency component of the leakage signal.

The readers of this Recommendation can select a method of measurement depending on their specific limitations and purposes.

## A.2 General requirements for measurement

### A.2.1 Measurement conditions

The general measurement conditions are based on [CISPR 22] and include the electromagnetic emanation level, including the information signal in the image displayed from the equipment with a monitor.

### A.2.2 EUT conditions

#### 1) Equipment under test

Equipment under test is used for telecommunications, and it uses a video or a visual display unit (VDU) as a monitor. It includes, for example, data processing equipment, office machines, electric business equipment, and telecommunication equipment.

#### 2) EUT configuration

The general EUT configuration is based on sections 8.1 and 10.4 of [CISPR 22].

#### 3) Operation of EUT

The general operation of EUT is based on sections 8.1, 8.2, and 10.4 of [CISPR 22]. Four operation rules shall be used.

a) The EUT is measured under conditions where an actual configuration is used and an actual operation is carried out as much as possible. An EUT that consists of a number of separate units shall be configured to form a minimum representative configuration. The number and mix of units included in the test configuration shall normally be representative of that used in a typical installation.

b) The operation of the VDU shall use white lines on a black screen to represent all colours. The white lines are vertical for a horizontal raster scan display. The white lines are horizontal for a vertical raster scan display.

c) As a rule, the selection of the operation mode of the VDU in measurement executes all the combinations when there are no regulations in the standards or specifications of the equipment. Most of the operation modes are described in the monitor timing specifications of the Video Electronics Standards Association (VESA).

d) The maximum emanation configuration is determined based on section 8.1.1 of [CISPR 22].

### A.2.3 Measurement site

The measurement site is based on sections 9.3 and 10.3 of [CISPR 22].

## A.3 Method of testing for radiation leakage (Wideband method)

### A.3.1 Measuring equipment and settings

The measuring receivers shall comply with [CISPR 16-1]. Note that the settings for the receivers are to conform to Table A.3-1 to measure video output.

**Table A.3-1 – Settings for receivers**

| Measurement mode | Zero span |
|---|---|
| RBW: Resolution bandwidth | More than 6 MHz; preferably more than 20 MHz |
| VBW: Video bandwidth | = RBW |
| Detection mode | Peak |
| Scale | Linear |

### A.3.2 Method of measurement

The method of measurement is based on [CISPR 16-2] and shall conform to the items 1) and 2) below.

#### 1) Measurement set-up

The configuration for the system of measurement is outlined in Figure A.3-1.

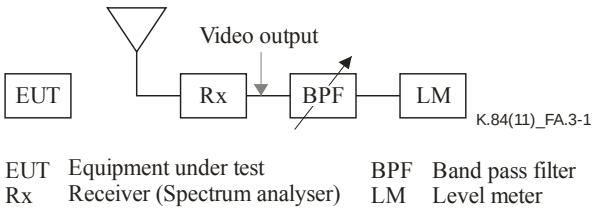



**Figure A.3-1 – Test configuration for receivers**

Where:

a) EUT: Equipment under test

The operation of the VDU on the EUT shall use white lines on a black screen. The line cycle is calculated from the operation mode of the horizontal raster scan display (screen resolution).

For example:

If the operation mode of the horizontal raster scan display is 800×600@60 Hz, 40 vertical white lines are displayed on a black screen, the line cycle is then about 2 MHz (see the specification of VDU or VESA standards).

b) Antenna

The receiving antenna shall comply with the requirements in [CISPR 16-1-4].

c) Rx: Receiver

The operation mode is based on Table A.3-1. The reference level is properly adjusted.

d) BPF: Band pass filter

The centre frequency is set to the line cycle. The bandwidth of the band pass filter should be less than the periodic frequency of the horizontal scan of the display.

For example, if the operation mode of the horizontal raster scan display is 800×600@60 Hz, the period of a horizontal scan is about 20 µs. Consequently, the periodic frequency is 50 kHz. The bandwidth of the band pass filter should be less than 50 kHz to detect only the component produced by VSP by eliminating the component of horizontal scan frequency.

e) LM: Level meter

The level meter measures the component emitted from VSP in the video output signal of the receiver. Noises can be reduced by averaging and time-gating signal processing.

The intervals for the time-gating process should be the same as the interval of horizontal scan period 20 µs. The larger the number of averaging, the better the reduction of noise, but the effect saturates at about 50 because of the fluctuation of the clock of the VDU.

NOTE – The functions of BPF and LM can be accomplished with a conventional spectrum analyser.

**2) Measurement procedure**

a) Electromagnetic emanation from the EUT is measured using the measurement set-up outlined in Figure A.3-1.

The general method of measurement is based on section 10.2 of [CISPR 22].

The distance between the antenna and EUT is 3 m for this method of measurement.

The maximum emanation configuration is determined based on section 8.1.1 of [CISPR 22].

The settings for the receiver then change to conform to those in Table A.3-1.

b) The receiving frequency changes from 30 MHz to 1000 MHz.

c) The video output of the receiver is measured with a level meter through the band pass filter.

Here, the centre frequency and the bandwidth of the band pass filter depend on the VSP and setting of the VDU such as resolution and refresh rate on the EUT. Typical settings of the VDU are executed.

### A.3.3 Evaluation of emanation threat

The measured level of the VSP at 3 m distance should be applied to evaluate the level at intrusion range described in clause 5.3. This level is compared with threat level, Eth.

## A.4 Method of testing for radiation leakage (Narrow-band method)

### A.4.1 Measuring equipment and settings

The measuring receiver shall comply with [CISPR 16-1-1]. Note that the settings for the receiver are to conform to those in Table A.4-1. The operation mode is based on Table A.4-1. The $N_{pts}$ is the number of measurement frequencies during the frequency scan for the receiver, and $f_h$ is the horizontal synchronization frequency of the VDU.

**Table A.4-1 – Parameters of receiver (spectrum analyser)**

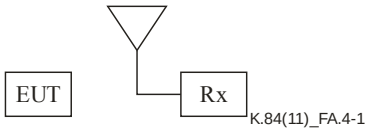
| | |
|---|---|
| RBW: Resolution bandwidth | 100 kHz |
| VBW: Video bandwidth | ≥ RBW |
| Sweep time ($T_{swp}$) | Longer than 2 * ($N_{pts}$ – 1)/$f_h$ |
| Detector | Peak (max. hold mode) |

### A.4.2 Method of measurement

A time varying stripe (TVS) pattern should be used to determine the frequency component of the emission from the displayed image in narrow-band measurement. The frequency component can be determined by comparing the measured emissions when the white screen and TVS are displayed on the VDU.

#### 1) Measurement set-up

The set-up for measurement is outlined in Figure A.4-1. The receiving antenna shall comply with the requirements in [CISPR 16-1-4]. The distance between the antenna and the EUT is typically 3 m.




EUT Equipment under test
Rx Receiver (Spectrum analyser)

**Figure A.4-1 – Measurement set-up**

#### 2) Displayed pattern on EUT

The measurement is executed while the white screen is displayed on the VDU. Then the TVS is displayed and the measurement is executed. The number of stripes on the TVS is increased from 1 to $X_d/2$ (half number of the horizontal pixels $X_d$) at a defined time step (twice the sweep time of the receiver is recommended). The selected parameters are listed in Table A.4-2.

**Table A.4-2 – Parameters of TVS**

| | |
|---|---|
| Minimum number of stripes | 1 |
| Maximum number of stripes | $X_d/2$ |
| Time steps for adding one stripe | 2 * $T_{swp}$ |

**3) Measurement procedure**

a) Electromagnetic emanation from the EUT is measured using the measurement set-up outlined in Figure A.4-1.

The general method of measurement is based on section 10.2 of [CISPR 22].

The maximum emanation is determined based on section 8.1.1 of [CISPR 22].

b) The receiving frequency changes from 30 MHz to 1000 MHz.

c) Electromagnetic emanation from the EUT is measured when white screen is displayed.

d) Electromagnetic emanation from the EUT is measured when the TVS is displayed.

e) Spectrum measured on c) and d) are compared. The emanation frequency can be determined as the frequency where the difference of the level is considerably large.

### A.4.3 Evaluation of emanation threat

The measured level of the emanation frequency of TVS at 3 m distance should be applied to evaluate the level at intrusion range described in clause 5.3. This level is compared with threat level, Eth.

# Annex B

# Methods of testing for conductive coupling in EMSEC

(This annex forms an integral part of this Recommendation.)

## B.1 Overview

Procedures are given for measuring the level of electromagnetic conductive leaks including the information signal of the displayed image from equipment with a monitor. The levels are specified for a frequency range from 30 MHz to 1000 MHz. The difference from Annex A "Methods of testing radiation in EMSEC" is as follows.

## B.2 General requirements for measurement

### B.2.1 Measurement conditions

The general conditions are based on [CISPR 22] for measuring the level of electromagnetic conductive leaks, including the information signal on the displayed image from equipment with a monitor.

### B.2.2 Conditions for EUT

#### 1) EUT configuration

The general configuration for the EUT is based on sections 8.1, 9.3, and 9.4 of [CISPR 22].

#### 2) Set-up of EUT

The general set-up of the EUT is based on sections 9.2 and 9.5 and Annexes C and D of [CISPR 22]. Three set-up rules shall be used:

a) The EUT is to be measured as much as possible under conditions where an actual configuration is used and an actual operation is carried out. An EUT that consists of a number of separate units shall be configured to form a minimum representative configuration. The number and mix of units included in the test configuration shall normally be representative of that used in a typical installation.

b) The operation of the VDU shall use white lines on a black screen to represent all colours. The white lines are vertical for a horizontal raster scan display. The white lines are horizontal for a vertical raster scan display.

c) As a rule, the selection of the operation mode of the VDU in measurement executes all combinations when there are no regulations in the standards or specifications of the equipment. Most of the operation modes are described in the monitor timing specifications of the Video Electronics Standards Association (VESA).

### B.2.3 Measurement equipment and settings

The measuring receiver shall comply with [CISPR 16-1]. The settings for the receiver are to conform to Table A.3-1 to measure video output.

### B.2.4 Measurement site

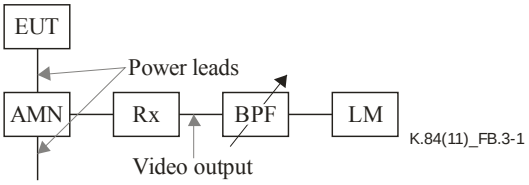
The measurement site is based on sections 9.3 and 9.4 of [CISPR 22].

## B.3 Method of testing for conducted leakage

### B.3.1 Method of measurement specific for conducted leakage

The method of measurement is based on sections 9.2 and 9.5 and Annexes C and D of [CISPR 22] and the details are as follows.

**1) The configuration for the system of measurement is outlined in Figure B.3-1**




| | | | |
|---|---|---|---|
| EUT | Equipment under test | BPF | Band pass filter |
| AMN | Artificial mains network | LM | Level meter |
| Rx | Receiver (Spectrum analyser) | | |

**Figure B.3-1 – Test configuration for receivers**

Here, AMN is artificial mains network. The AMN is used for the frequency range from 30 MHz to 1000 MHz.

### B.3.2 Method of measurement common for conducted and radiation leakage

The methods described in clauses A.3 and A.4 apply.

# Appendix I

# Threat of EMSEC

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

## I.1 Electromagnetic wave leakage

Typical means of obtaining information from leaking electromagnetic waves, (TEMPEST) includes a method of using antennas to detect electromagnetic waves leaking into space, a method of installing probes into metal portions of a buildings (window frames, or plumbing, etc.), or a method of installing probes into the power-supply lines.

Of these, the method of installing probes into power lines to detect leaking electromagnetic waves is considered to pose the least danger. The reason for this is that the power supply is currently controlled by inverters in many devices, and inverter noise in the power supply lines overlaps a wide range of frequencies. Serial signal components such as display signals or keyboard input are then concealed in that noise, making them difficult to detect.

Also, as the signal level induced in window frames or plumbing is low, highly sensitive receivers would be necessary in methods where probes were installed into metal portions of buildings. Furthermore, as it is necessary to enter buildings or areas around buildings to install these probes, the risk of intent being discovered is high (security measures to protect against intruders are sufficient as countermeasures to protect information).

The method of detecting leaking electromagnetic waves in space using antennas that can achieve its intent from remote distances can therefore be considered to be the most effective for attacks as a means of EMSEC.

There is an example of an EMSEC system configuration that uses an antenna in Figure I.1. In addition to leaking electromagnetic waves that contain information, electromagnetic noise that accompanies transmission waves, radio communication, and the operation of devices is also simultaneously detected when using an antenna to receive surrounding electromagnetic waves. Leaking electromagnetic waves that contain information generally have a lower level than these surrounding electromagnetic waves. It is therefore necessary to increase the sensitivity of the receiver. However, when doing this, the receiving amplifier becomes saturated and it becomes impossible to receive leaking electromagnetic waves when there are strong electromagnetic waves near the received bandwidth. A band pass filter is used in front of the amplifier to avoid this situation.

The amplifier has its own unique thermal noise, and it is possible to establish its value from the noise figure (NF) characteristics. When the NF value is large, background noise is amplified at the same time that the required signal is amplified, so it may not be possible to maintain a sufficient SN ratio for the required signal and background noise. Therefore, a low-noise amplifier is used. Normally, a low-noise amplifier that has high gain has a large NF value, and an amplifier that has a certain amount of gain but a small NF value is comparatively expensive.

The signal that is enlarged by the amplifier is received by the receiver, and then it passes through an analogue or digital converter. By undergoing signal processing such as sampling and averaging, the signal is converted to the required signal (display signal or keyboard input signal). This series of processes can currently be executed in real time, also making video EMSEC possible.

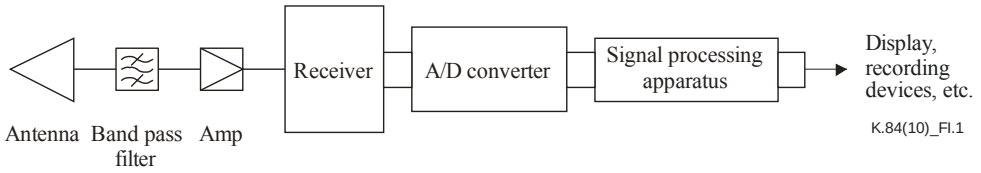



**Figure I.1 – Example of system configuration for detecting leaking electromagnetic waves**

## I.2 Method of estimating possible distance for information leakage

There is a relationship given by Equation I-1 between the strength of electromagnetic waves in the air (electric field strength $E$ [dBμV/m]) and the input terminal voltage of the receiver ($V$ [dBμV]).

$$E = V + A_f \tag{I-1}$$

Here, $A_f$ is a coefficient called the antenna factor (dB), and when the input impedance of the antenna is 50 Ω, it is expressed using the antenna gain (G [dB]) below.

$$A_f = 20\log_{10}(f[MHz]) - G - 29.79 \tag{I-2}$$

Here, $f$ is the frequency.

However, when the minimum receiving voltage of the receiver is taken to be $V_{min}$ [dBμV], it is possible to express the leaking electromagnetic wave level ($E_{min}$ [dBμV/m]) for which a signal can actually be reproduced with the equation below.

$$E_{min} = V_{min} + SN + A_f \tag{I-3}$$

Here, SN is the strength ratio (SN ratio [dB]) between the signal required for signal reproduction and noise.

From the above, the maximum value for the distance for which EMSEC is possible can be found from the distance at which the strength of the leaking electromagnetic waves that are radiated from a device or system equals $E_{min}$ that was found from Equation I-3. The attenuation of leaking electromagnetic wave strength at this time is a combination of distance attenuation and the attenuation resulting from the shielding effect of buildings.

### I.2.1 Performance of system equipment

As shown in Equation I-3, the antenna factor (gain) of the EMSEC system antenna, the minimum receiving voltage of the receiver and the required SN ratio for reproduction become the parameters for the maximum distance at which EMSEC is possible. Performance is evaluated for all devices in the system to determine the values of each of the parameters.

#### I.2.1.1 Antenna factor

Antennas that are compact and have high gain are suitable for use in EMSEC. As current Yagi or beam antennas that are used for amateur radio, or 2.4 GHz non-LAN bridge antennas (Yagi antenna, r patch antennas) satisfy these requirements, they are considered to be suitable. Details on Yagi and beam antennas that are used for amateur radio are listed in Table I.1. The results obtained by using Equation I-2 to calculate the antenna factor for these are also summarized in Table I.1.

**Table I.1 – Examples of VHF band Yagi antennas for amateur radio**

| Model | Frequency band | Number of elements | Gain [dBi] | Antenna factor [dB] |
|---|---|---|---|---|
| Model A | 144 MHz zone | 5 | 9.1 | 4.3 |
| Model B | 144 MHz zone | 5 | 11.2 | 2.2 |
| Model C | 430 MHz zone | 10 | 13.1 | 9.8 |
| Model D | 430 MHz zone | 9 | 14.8 | 8.1 |
| Model E | 1.2 GHz zone | 23 | 19.5 | 12.3 |
| Model F | 2.4 GHz zone | 27 | 19 | 19.0 |

As can be seen from Equation I-1, an antenna with a small antenna factor is highly sensitive, which means that it is suitable for EMSEC. Therefore, out of the examples given in Table I.1, the antenna with an antenna factor of 2.2 dB is the most suitable.

### I.2.1.2 Receiver performance

Receivers that can be used for EMSEC can be divided into three groups, multi-band kinds for amateur radio (receiver I), EMC measurement kinds (receiver II), and highly sensitive kinds for EMSEC (receiver III).

The minimum receiving voltage level for each of these receivers differs, depending on the model and frequency; however, the minimum receiving voltage level in the VHF and UHF bands is $-13\,\mathrm{dB}\mu\mathrm{V}(=-120\,\mathrm{dBm}@50\ \Omega)$ at the receiving bandwidth of 120 kHz. From the studies that have been carried out up to now, it has been found that a receiving bandwidth of about 3 MHz is necessary to reproduce signals with EMSEC. The minimum receiving voltage level of the receiver depends on the receiving bandwidth. Consequently, when the receiving bandwidth of 120 kHz is converted to 3 MHz, from the equation below the minimum receiving voltage level is found to be approximately 0.98 dBµV.

$$-13+10\log_{10}\left(3\times10^{6}/1.2\times10^{5}\right)=0.98\ \ [\mathrm{dB\mu V}]$$

However, based on studies carried out previously, the SN ratios needed for signal regeneration are understood to be 20 dB for receiver I, 15 dB for receiver II, and 0 dB for receiver III.

### I.2.2 Possible distance for EMSEC

The results obtained after the possible distance is calculated using the performance of the EMSEC systems described in the previous clause are presented in Figure I.2. It has been assumed that the strength of the leaking electromagnetic waves that are radiated from the device or system to be protected is equal to the emission levels, for example, class A, class B in [ITU-T K.48]. It has also been assumed that the electric field strength is inversely proportional to the distance and is attenuated over distance. Refer to Appendix II for an overview of the confidentiality of IT equipment.

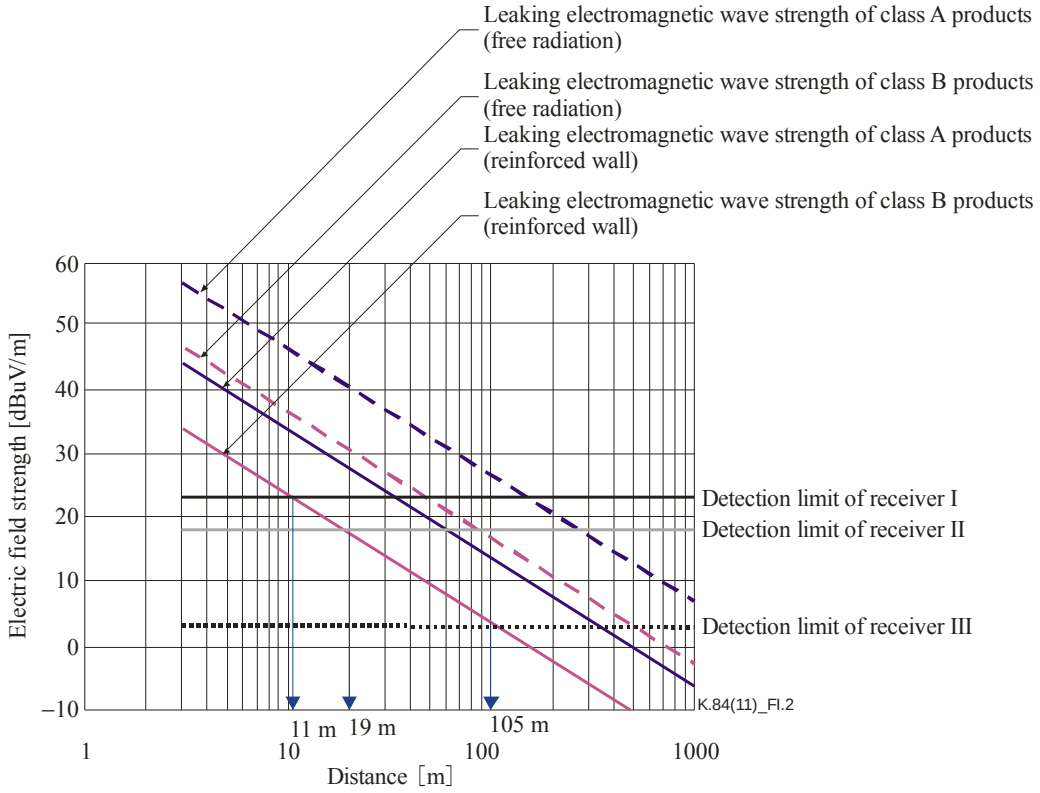



**Figure I.2 – Relationship between possible electric field strength (strength of leaking information) and distance for EMSEC**

# Appendix II

# Confidentiality of IT equipment

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

## II.1 Confidentiality of IT equipment

### II.1.1 Confidentiality against information leakage

Confidentiality against information leakage due to electromagnetic waves that are radiated into space can be evaluated by using the leaking electromagnetic wave strength radiated by the equipment or system to be protected. The leaking electromagnetic wave strength (emissions) of IT equipment is regulated by national standards or the standards of individual countries (emission standards) to protect transmission work and wireless work. There are examples of emission standards listed in Table II.1.

**Table II.1 – Examples of emission requirements**

| Standard name | Type | Target equipment | Reference value/class (Note 2) |
|---|---|---|---|
| [CISPR 22] | International standards | IT equipment (Note 1) | Class A/Class B |
| [b-EN 55022] | European standards (Note 3) ([CISPR 22] compliance) | IT equipment | Class A/Class B |
| [ITU-T K.42] | Recommendations ([CISPR 22] compliance) | Communications equipment | Class A/Class B |
| FCC Part 15 | US standards | IT equipment, etc. | Class A/Class B |
| [b-NEBS GR 1089] | Independent standards (FCC compliance) | Network equipment | Class A/Class B |
| VCCI | Independent standards ([CISPR 22] compliance) | IT equipment | Class A/Class B |
| NOTE 1 – Includes communications equipment, business equipment, AV equipment, and PC equipment.<br>NOTE 2 – Class B has a 10 dB stricter value than Class A in all standards.<br>NOTE 3 – Australia and New Zealand are in compliance according to European standards. | | | |

Of the standards summarized in Table II.1, [b-NEBS GR 1089] are standards related to electrical or electromagnetic items (including EMC), which are a collection of the installation conditions for communications equipment established by AT&T and US regional communications companies (RBOC). There are products that comply with NEBS Level 3 as servers or routers for IP equipment.

As many countries are implementing emission standards in this way, the maximum values for emission levels of IT equipment can be considered to be reference values for the applicable standards. In doing so, the reference values for two classes, Classes A and B, have been established according to the environment to set up the equipment for each standard. All of the emission standards are continually being coordinated Except for FCC Part 15 and the NEBS standards that quote them, all of the standards correspond to the contents of [CISPR 22]. Figure II.1 compares the reference emission values for [CISPR 22] and NEBS. At 30 to 1000 MHz, there is little difference between the two, and they can be considered to have the same emission levels.

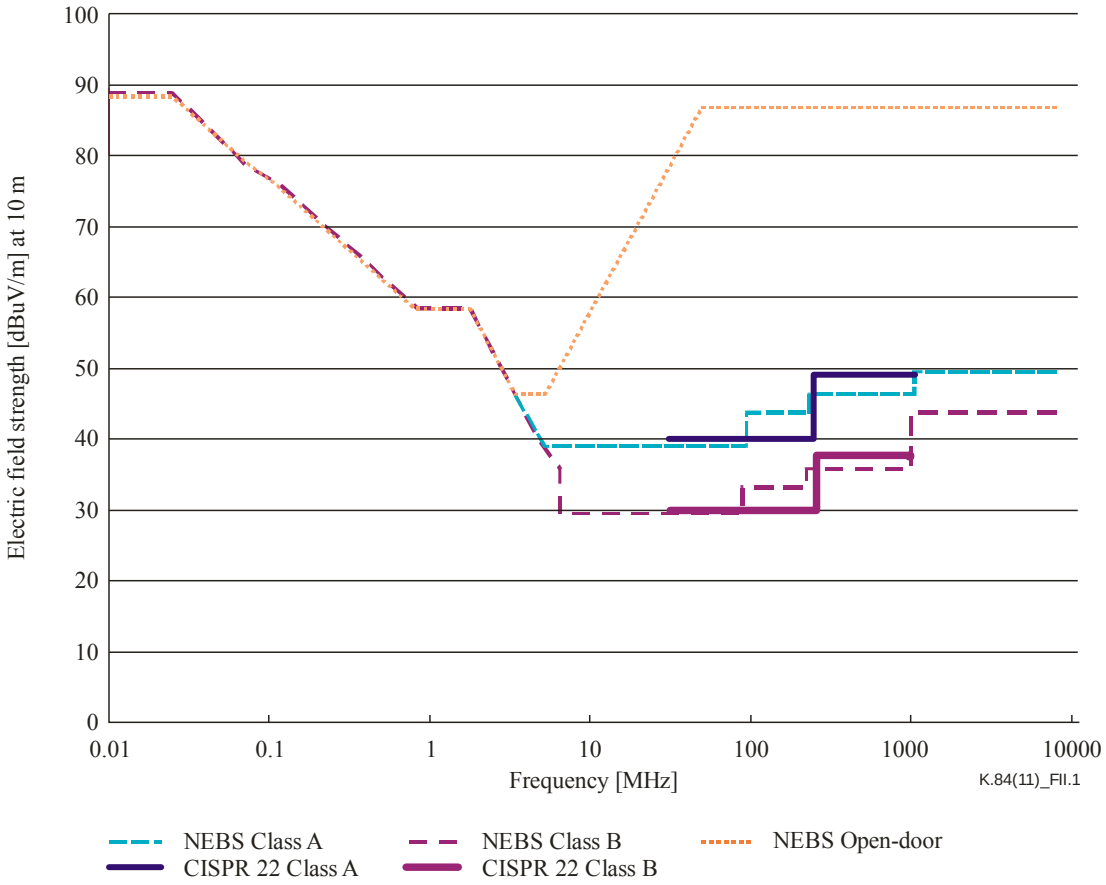



**Figure II.1 – Comparison of reference emission values ([CISPR 22] and [b-NEBS GR 1089])**

# Appendix III

## Example of wideband measurement

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

The display setting parameters are set to a display resolution of 800 × 600 pixels and a vertical refresh rate of 60 Hz as an example of measurement. An image with periodic 8-pixel wide vertical stripes is then displayed in the test display monitor, as shown in Figure III.1. Therefore, the frequency switching of the RGB signals could be calculated from the stripe width of 8 pixels and the total number of pixels and the exact refresh rate for the computer display monitor. The specific frequency is about 5 MHz. This frequency denotes the information signal expressing the switching of RGB signals on the test display monitor.

Figures III.2 (a) and (b) are outlines of a system block configuration. The antenna is a log-periodic antenna that is usable in a frequency range of 80 to 1000 MHz and is located 1 m from the front of the EUT in a compact anechoic chamber. The first receiver is set to the zero-span mode, with an bandwitdth RBW and video bandwidth (VBW) of 100 MHz. The second receiver is set up with start and stop frequencies corresponding to 5.00 and 5.01 MHz, an RBW and VBW of 10 Hz, an attenuator (ATT) of 10 dB, and a sweep time of 20 s with 1001 measurement points.

Test measurements are carried out to detect information signal S and noise signal N, which have a frequency of about 5 MHz, when the test image and a black image are displayed on the computer display. Figure III.3 shows the results obtained from measuring the signal to noise ratio (SN) at each receiving frequency band in the radiated emissions. The level of SN depends on the receiving frequency band. As a result, information signal S was contained at high volume in the frequency region between 300 and 600 MHz in the radiated emission. This tendency depends on the EUT. This method and system of measurement can become a valid approach to quantitatively evaluate the information leakage from displayed images caused by the electromagnetic emissions of PCs.

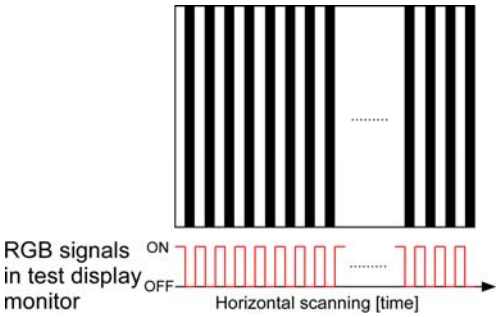



**Figure III.1 – Test image with periodic 8-pixel wide vertical stripes**

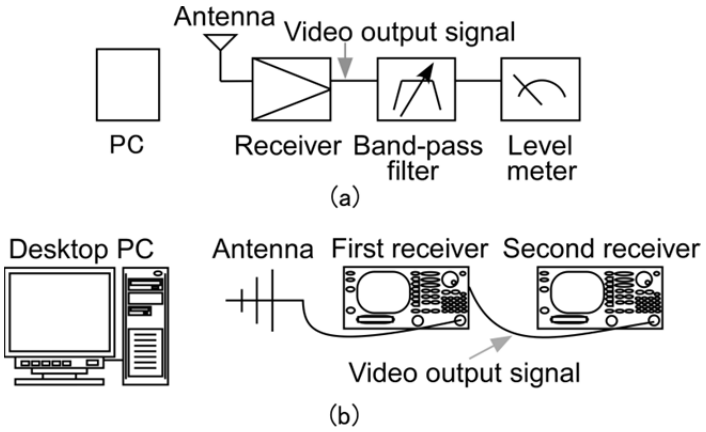



**Figure III.2 – (a) System block configuration and (b) measurement system to detect information signal in radiated electromagnetic emissions of PC**

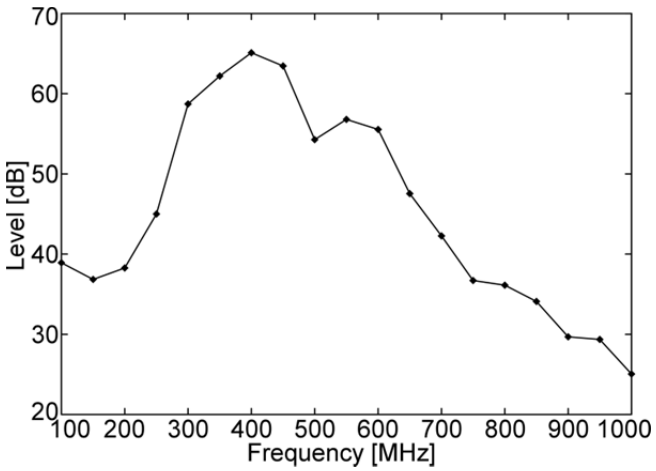



**Figure III.3 – Measurement results for SN at each receiving frequency band in radiated electromagnetic interference**

# Appendix IV

## Example of narrow-band measurement

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

The parameters of the TVS pattern are set as listed in Table IV.1, and the image is changed as shown in Figure IV.1 to provide an example of measurement. The parameters of the receiver are set as listed in Table IV.2. The measurements are done in an anechoic chamber. The distance from the EUT to the receiving antenna is 1 m, because the measured electric field is low and it is difficult to determine the difference in levels when TVS and white patterns were displayed. A log-periodic antenna is used to measure the electric field strength. An XGA display (1024 × 768), which is commercially available, is used in this example.

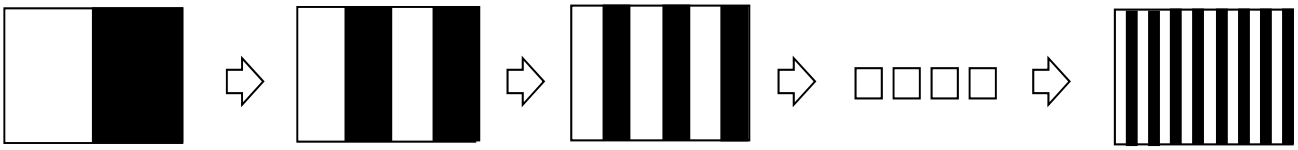


**Figure IV.1 – Time step to add one stripe to TVS pattern**

**Table IV.1 – Parameters of TVS pattern**

| Items | Parameters |
|---|---|
| Minimum number of stripes | 1 |
| Maximum number of stripes | 512 |
| Time step to add one stripe: $t_{add}$ | 84 ms ($m$ = 2) |

**Table IV.2 – Parameters of receiver**

| Item | Parameters |
|---|---|
| RBW/VBW | 100 kHz/100 kHz |
| Measurement span | 100 MHz |
| Measurement points: $N_{pts}$ | 1001 |
| Sweep time: $t_{swp}$ | 42 ms |
| Detector | Peak (max. hold) |

The electric field strength when patterns are displayed is presented in Figure IV.2. The measurement frequency range is 300 to 1000 MHz. The difference in levels is observed as shown in Figure IV.3. The large difference in levels contains the frequency component of the displayed pattern. Thus, the level of the frequency component should be reduced more than the threat level, Eth.

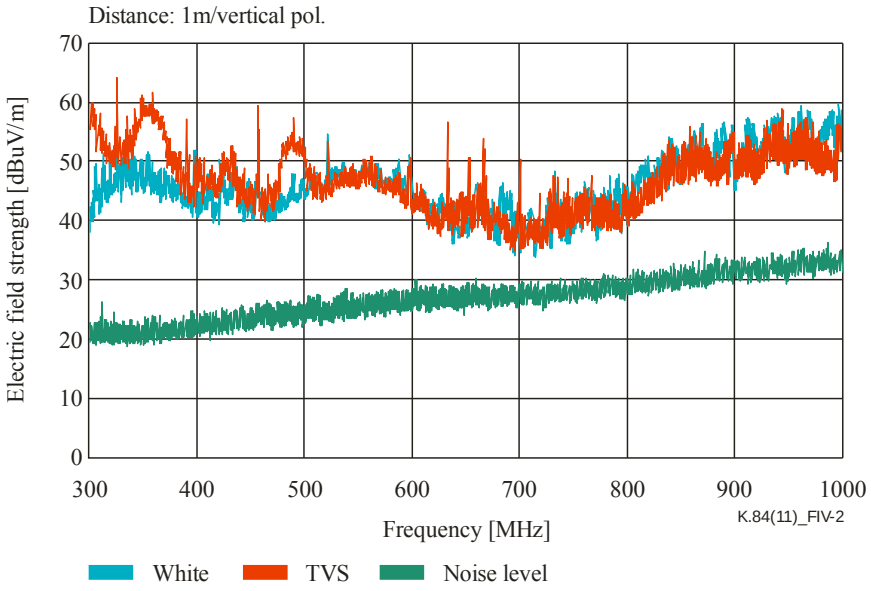



**Figure IV.2 – Received level when white and TVS images are displayed from 300 to 1000 MHz**

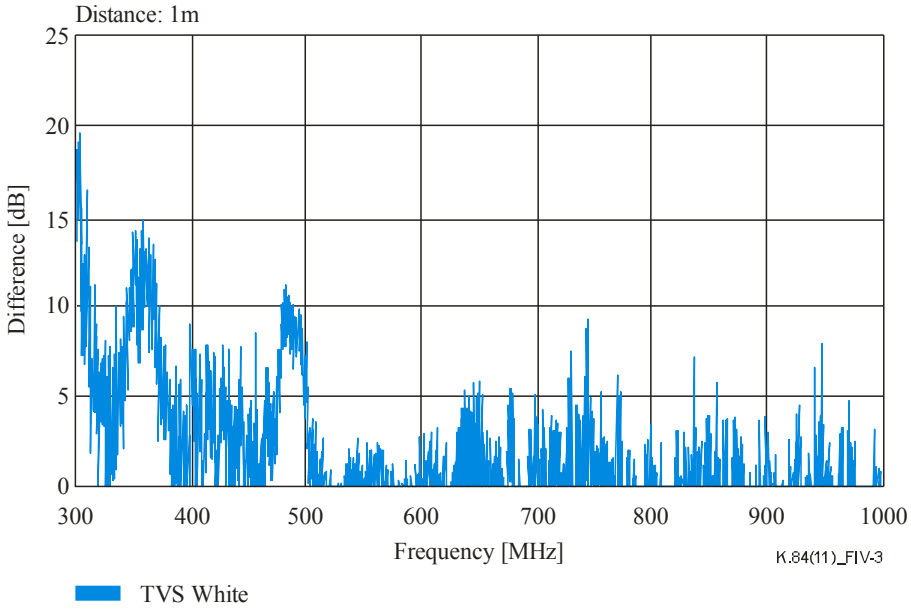



**Figure IV.3 – Difference in levels of spectrum when white and TVS images are displayed from 300 to 1000 MHz**

# Bibliography

The following ITU-T Recommendations and other references provide additional information.

**ITU-Security**


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


**Standards for VDU**


[b-VESA1] VESA Standard DMT 1 (2007), *Industry Standards and Guidelines for Computer Display Monitor Timing (DMT) Standard, Version 1.0, Revision 12*.

[b-VESA2] VESA GTF 1 (1999), *Generalized Timing Formula (GTF), Version 1.1*.


**Standards related to IT security**


[b-CISPR 17] CISPR 17 (1981), *Methods of measurement of the suppression characteristics of passive radio interference filters and suppression components*.

[b-EN 55022] EN 55022 (1998), *Information technology equipment. Radio disturbance characteristics. Limits & methods of measurement*.

[b-EN 55024] EN 55024 (1998), *Information technology equipment. Immunity characteristics. Limits and methods of measurement*.

[b-FIPS PUB 140-2] NIST FIPS PUB 140-2 (2001), *Security Requirements for Cryptographic Modules*. < http://csrc.nist.gov/cryptval/140-2.htm>.

[b-GIAJ 98] Safety Engineering Report 98-1 (1998), *Network Risk Diagnosis Check List Report, General Insurance Association of Japan, Safety Engineering Section, Safety and Disaster Prevention Section*, March.

[b-GIAJ REP 97] Safety Engineering Report 97-1 (1998), *Risk and Countermeasures in the Network Society, General Insurance Association of Japan, Safety Engineering Section*, March.

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

[b-IEC 15408-1] IEC 15408-1 (1999), *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-IEC 15408-2] IEC 15408-2 (1999), *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*.

[b-IEC 15408-3] IEC 15408-3 (1999), *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*.

[b-IEC 17799] IEC 17799 (2000), *Information technology – Code of practice for information security management*.

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

[b-NEBS GR-089] NEBS GR-089-CORE (2006), *EMC and Electrical Safety for Network Telecommunications Equipment*.

[b-NEBS GR 1089] NEBS GR 1089 (2002), *Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunications Equipment*.

[b-NEBS GR 1089] Telcordia GR-1089, v6 (2011), *Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunications Equipment*.

[b-NEBS SR-3580] NEBS SR-3580 (2007), *Criteria Levels*.

[b-NEBS SR-3580] Telcordia SR-3580, v4 (2011), *NEBS Criteria Levels*.

**IST in Japan**

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

**EMSEC documents**

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

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

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

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

[b-Sekiguchi rad] Sekiguchi, H., and Seto, S. (2009), *Measurement of Radiated Computer RGB Signals*, Progress In Electromagnetics Research C, Vol. 7, pp. 1-12.

[b-Sekiguchi cond] Sekiguchi, H., and Seto, S. (2009), *Measurement of Computer RGB Signals in Conducted Emission on Power Leads,* Progress In Electromagnetics Research C, Vol. 7, pp. 51-64.

[b-Smulders] Smulders, P. (1990), *The threat of information theft by reception of electromagnetic radiation from RS-232 cables*, Computers of Security 9, 1, 53-58.

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

[b-Tosaka] Tosaka, T., Yamanaka, Y., and Fukunaga, K. (2010), *Evaluation method of information in electromagnetic disturbance radiated from PC display using time varying stripe image*, Proceedings of the 4th Pan-Pacific EMC Joint Meeting, pp. 67–70.

[b-Van Eck] Van Eck, W. (1985), *Electromagnetic radiation from video display units: An eavesdropping risk?* Computers of Security 4, 269-286.

## SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2012