International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# K.115

(11/2015)

SERIES K: PROTECTION AGAINST INTERFERENCE

## Mitigation methods against electromagnetic security threats

Recommendation ITU-T K.115

# Recommendation ITU-T K.115

## Mitigation methods against electromagnetic security threats


### Summary

Recommendation ITU-T K.115 specifies mitigation methods against electromagnetic (EM) security threats such as high-altitude electromagnetic pulse (HEMP), high-power electromagnetic (HPEM), information leakage and lightning for telecommunication equipment and facilities. This Recommendation applies to all types of telecommunication equipment and facilities such as switching equipment, modems and buildings where equipment is installed.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T K.115 | 2015-11-29 | 5 | 11.1002/1000/12664 |

### Keywords

Electromagnetic security, EM security, high-altitude electromagnetic pulse, HEMP, high-power electromagnetic, HPEM, information leakage, lightning.


---

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

## FOREWORD

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

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

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

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

## NOTE

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

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

## INTELLECTUAL PROPERTY RIGHTS

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

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

## Table of Contents

# Recommendation ITU-T K.115

## Mitigation methods against electromagnetic security threats

### 1 Scope

This Recommendation specifies mitigation methods against electromagnetic (EM) security threats for telecommunication equipment and facilities. This Recommendation applies to all types of telecommunication equipment and facilities such as switching equipment, modems and buildings where equipment is installed.

### 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.11] Recommendation ITU-T K.11 (2009), *Principles of protection against overvoltages and overcurrents*.

[ITU-T K.12] Recommendation ITU-T K.12 (2010), *Characteristics of gas discharge tubes for the protection of telecommunications installations*.

[ITU-T K.20] Recommendation ITU-T K.20 (2015), *Resistibility of telecommunication equipment installed in a telecommunication 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.27] Recommendation ITU-T K.27 (2015), *Bonding configurations and earthing inside a telecommunication building*.

[ITU-T K.28] Recommendation ITU-T K.28 (2012), *Parameters of thyristor-based surge protective devices for the protection of telecommunication installations*.

[ITU-T K.36] Recommendation ITU-T K.36 (1996), *Selection of protective devices*.

[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.46] Recommendation ITU-T K.46 (2012), *Protection of telecommunication lines using metallic symmetric conductors against lightning-induced surges*.

[ITU-T K.47] Recommendation ITU-T K.47 (2012), *Protection of telecommunication lines against direct lightning flashes*.

[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*.

[ITU-T K.77] Recommendation ITU-T K.77 (2009), *Characteristics of metal oxide varistors for the protection of telecommunication installations*.

[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 (2014), *High-power electromagnetic immunity guide for telecommunication systems*.

[ITU-T K.82] Recommendation ITU-T K.82 (2010), *Characteristics and ratings of solid-state, self-restoring overcurrent protectors for the protection of telecommunications installations*.

[ITU-T K.84] Recommendation ITU-T K.84 (2011), *Test methods and guide against information leaks through unintentional electromagnetic emissions*.

[ITU-T K.85] Recommendation ITU-T K.85 (2011), *Requirements for the mitigation of lightning effects on home networks installed in customer premises*.

[ITU-T K.87] Recommendation ITU-T K.87 (2011), *Guide for the application of electromagnetic security requirements – Overview*.

[ITU-T K.95] Recommendation ITU-T K.95 (2014), *Surge parameters of isolating transformers used in telecommunication devices and equipment*.

[ITU-T K.96] Recommendation ITU-T K.96 (2014), *Surge protective components: Overview of surge mitigation functions and technologies*.

[ITU-T K.98] Recommendation ITU-T K.98 (2014), *Overvoltage protection guide for telecommunication equipment installed in customer premises*.

[ITU-T K.99] Recommendation ITU-T K.99 (2014), *Surge protective component application guide – Gas discharge tubes*.

[ITU-T K.101] Recommendation ITU-T K.101 (2014), *Shielding factors for lightning protection*.

[ITU-T K.102] Recommendation ITU-T K.102 (2014), *Parameters of fixed-voltage thyristor overvoltage protector components used for the protection of telecommunication installations*.

[ITU-T K.103] Recommendation ITU-T K.103 (2015), *Surge protective component application guide – Silicon PN junction components*.

[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*.

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

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

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

[IEC 61000-4-5] IEC 61000-4-5 (2014), *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques –Surge immunity test*.

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

[IEC 61000-4-24] IEC 61000-4-24 (2015), *Electromagnetic compatibility (EMC) – Part 4-24: Testing and measurement techniques – Test methods for protective devices for HEMP conducted disturbance*.

[IEC 61000-4-25] IEC 61000-4-25 (2001), *Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques - HEMP immunity test methods for equipment and systems*.

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

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

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

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

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

[IEC TR 61000-5-6] IEC TR 61000-5-6 (2002), *Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences*.

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

[ISO/IEC 27001] ISO/IEC 27001 (2013), *Information technology – Security techniques – Information security management systems – Requirements*.

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

## 3 Definitions

### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 antenna port** [IEC 61000-6-6]: A port that is connected to an antenna, either directly or by a cable. The antenna may be external or internal to the building.

NOTE – Antenna ports connected to antennas internal to the building are covered by signal ports.

**3.1.2 availability** [ISO/IEC 27001], [ISO/IEC 27002]: Ensuring that authorized users have access to information and associated assets when required.

**3.1.3 cable port** [IEC 61000-6-6]: A port at which a conductor or cable is connected to the apparatus.

**3.1.4 confidentiality** [ISO/IEC 27001]: Ensuring that information is accessible only to those authorized to have access.

**3.1.5 electrical fast transient/burst (EFT/B)** [IEC 61000-4-4]: The 5/50 ns pulse defined in [IEC 61000-4-4].

**3.1.6 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., byproduct) of its operation, and that may contain information. (See: TEMPEST.)

**3.1.7 emanations security (EMSEC)** [b-IETF RFC 2828]: Physical constraints to prevent information compromise 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.

**3.1.8 enclosure port** [IEC 61000-6-6]: A physical boundary of the apparatus which electromagnetic fields may radiate through or impinge upon. The equipment case is normally considered the enclosure port.

**3.1.9 functional earth port** [IEC 61000-6-6]: A cable port other than a signal, control or power port, intended for connection to earth for purposes other than safety.

**3.1.10 HEMP immunity test** [IEC 61000-4-25]: The HEMP immunity test is made up of four types of tests. The radiated test is defined in section 5 of [IEC 61000-4-25], and is used with a large HEMP simulator and a small radiated test facility. The other three types are the conducted tests along the HEMP waveforms; early-, intermediate- and late-HEMP. These are also defined in section 5 of [IEC 61000 4-25].

**3.1.11 high voltage (HV) transmission line** [IEC 61000-4-25]: Power line with a nominal a.c. system voltage equal to or greater than 100 kV.

**3.1.12 immunity (to a disturbance)** [b-IEC 60050-161]: The ability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance.

**3.1.13 integrity** [ISO/IEC 27001], [ISO/IEC 27002]: Safeguarding the accuracy and completeness of information and processing methods.

**3.1.14 large HEMP simulator** [IEC 61000-6-6] [IEC 61000-4-25]: Transient electromagnetic pulse test facility with a test volume sufficiently large to test objects with cubical dimensions equal to or greater than 1 m × 1 m × 1 m.

**3.1.15 low voltage (LV) power circuit** [IEC 61000-6-6]: Power circuit with a nominal a.c voltage equal to or less than 1.

**3.1.16 medium voltage (MV)** [b-IEC 60050-601]: Power circuit with a nominal a.c voltage equal to or less than 1.

NOTE – The boundaries between medium and high voltage levels overlap and depend on local circumstances and history or common usage. Nevertheless, the band 30 kV to 100 kV frequently contains the accepted boundary.

**3.1.17 power port** [IEC 61000-6-6]: Point at which a conductor or cable carrying the electrical power needed for operation of the equipment is connected to the apparatus.

**3.1.18 small radiated test facility** [IEC 61000-6-6] [IEC 61000-4-25]: Laboratory transient electromagnetic pulse test facility such as a transverse electromagnetic (TEM) cell with a test volume sufficiently large to test objects with cubical dimensions of less than 1 m × 1 m × 1 m.

**3.1.19 surge protection device (SPD)** [b-IEC 61643-21]: A device to suppress line conducted overvoltages and currents, such as surge suppressors defined in [b-IEC 61643-21].

**3.1.20 telecommunication port** [ITU-T K.88]: Point of connection for voice, data and signalling transfers intended to interconnect widely-dispersed systems via such means as direct connection to multi-user telecommunication and similar networks.

**3.1.21 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.

**3.1.22 threat** [ITU-T K.81]: 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 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 vulnerability**: The possibility that equipment does not function correctly when exposed to HEMP or HPEM and will function falsely with EMSEC.

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

Vulnerability as defined in [ITU-T K.84]: The possibility that equipment will function falsely with EMSEC.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| DB | Database |
| EM | Electromagnetic |
| EMI | Electromagnetic Interference |
| EMSEC | Emanation Security |
| HEMP | High-altitude Electromagnetic Pulse |
| HPEM | High-Power Electromagnetic |
| ISMS | Information Security Management System |
| PoE | Point of Entry |
| RF | Radio Frequency |
| SPD | Surge Protection Device |

## 5 Conventions

None.

## 6 Mitigation methods against electromagnetic security threats

Electromagnetic (EM) security threats are classified into EM interference (EMI) and information leakage. Moreover, EMI is separated into intentional EMI, e.g., high-altitude electromagnetic pulse (HEMP), high-power electromagnetic (HPEM), and natural EMI, e.g., lightning. See [ITU-T K.87].

### 6.1 High-altitude electromagnetic pulse

#### 6.1.1 Introduction

A HEMP environment is defined as the consequences of a high-altitude nuclear explosion [IEC 61000-2-9], [IEC 61000-2-10].

For civil systems, high-altitude nuclear explosions are more important than those at low altitude. In a HEMP environment, the other effects of a nuclear explosion: blast, ground shock, thermal, and nuclear ionizing radiation are not present at ground level. However, the electromagnetic pulse associated with an explosion can cause disruption of, and damage to, communication, electronic and electric power systems, thereby impairing the infrastructure of a modern society.

A guide to the protection of telecommunication centre equipment, such as that for switching, transmission, radio, and power, from damage and disruption due to a HEMP is given in [ITU-T K.78]. The overall radiated and conducted immunity against HEMP is a combination of the inherent immunity of equipment, surge protection device (SPD) surge mitigation, and the electromagnetic screening of building and equipment enclosures. [ITU-T K.78] discusses the contribution of each item to immunity and defines an approach to immunity testing and testing levels for HEMP.

#### 6.1.2 Reference documents

HEMP environments for radiated disturbance are defined in [IEC 61000-2-9] and those for conducted disturbance are defined in [IEC 61000-2-10].

Test methods for protective devices against HEMP and other disturbances are described in [IEC 61000-4-23] and [IEC 61000-4-24].

Protection concepts against HEMP are given in [IEC TR 61000-5-3], which aims to provide elements for the design of an adequate protection for civil facilities against HEMP and the evaluation of already existing protections with respect to stresses imposed by HEMP. It also gives a comparison of the requirements of HEMP and lightning protection in order to show whether they can be combined at low cost.

HEMP immunity requirements for electrical and electronic equipment intended for use indoors are given in [IEC 61000-6-6], which also contains information on how an indoor HEMP environment depends on the electromagnetic shielding quality of a facility and the level of protection against the conducted environment.

#### 6.1.3 Protection approaches

There are two approaches for applying protection measures:

- case 1: When protection measures are applied to a telecommunication centre building, in which a system has already been installed, the only options are additional shielding and surge protection. In this case, the system equipment must conform to the minimum requirement against HEMP.
- case 2: When the system has not yet been installed, an equipment requirement is applied, which works in the given shielding and surge protection measures of the building. In this case, the requirement depends on the protection concept of the building.

### 6.1.4 Protection concepts

A protection concept describes the fundamental ideas that guide the operator to obtain HEMP-resistant equipment, systems and/or buildings. As this Recommendation aims at telecommunication centre applications, the HEMP-hardened system consists of telecommunication equipment that is sometimes housed in special enclosures.

The protection concepts deal mainly with housing and interconnections in a building. The required immunity level of equipment is set by the concept level of the building and/or enclosure where the equipment is installed. Figure 1 shows the protection concepts and immunity test levels.

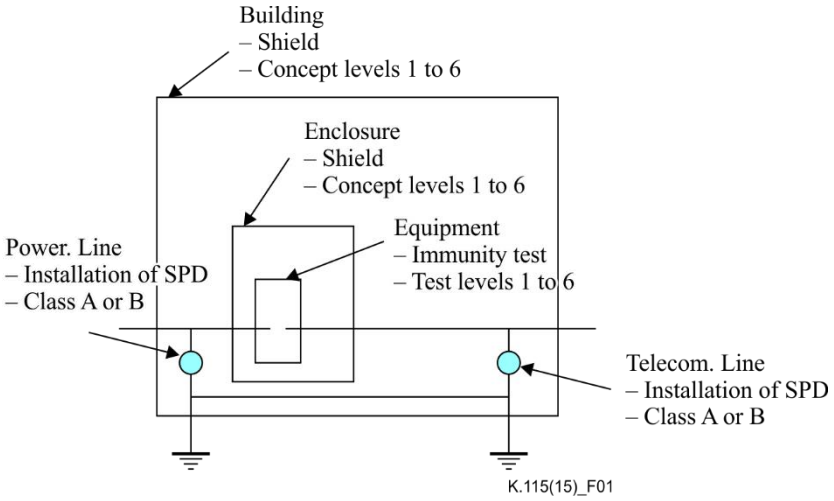



**Figure 1 – Concept and immunity test levels**

For the purposes of this HEMP environment classification, six major protection concepts are defined below (see [IEC 61000-5-3] for additional details). The external environments and protection concepts result in internal environment levels, which are appropriate for equipment or subsystems that are placed within these protection zones. The concepts, shown in Table 1, are described as:

– **concept 1**: Above-ground wooden, brick or concrete building or structure with large windows and doors without rebar or other explicit shielding. Lack or presence of conducted lightning protection (overvoltage protection without filtering) defines subconcepts 1A and 1B, respectively.

– **concept 2**: Above-ground concrete building or structure with rebar or buried brick or concrete. Lack or presence of conducted lightning protection (overvoltage protection without filtering) defines subconcepts 2A and 2B, respectively.

– **concept 3**: Shielded enclosure with minimal radio frequency (RF) shielding effectiveness such as a typical equipment box with small apertures and nominal lightning overvoltage and EMI conducted penetration protection (filtering).

– **concept 4**: Shielded enclosure with modest RF shielding effectiveness, good bonding at all points of entry (PoEs) and nominal lightning overvoltage and EMI conducted penetration protection (filtering).

– **concept 5**: Shielded enclosure with good RF shielding effectiveness and PoE protection (overvoltage and filtering).

– **concept 6**: Shielded enclosure with high-quality RF shielding and PoE protection (overvoltage and filtering).

The EM field attenuation levels described below in Table 1 are to be evaluated at frequencies between 100 kHz and 30 MHz for concepts 1 and 2, and at frequencies between 1 MHz and 200 MHz for concepts 3 to 6, using the methods described in [IEC 61000-4-23].

**Table 1 – Minimum required attenuation of peak time domain external environments for six principal protection concepts**

| Concept level | Minimum attenuation dB | | |
|---|---|---|---|
| | Electric field | Magnetic field | Conducted current |
| 1A | 0 | 0 | 0 |
| 1B | 0 | 0 | 20 |
| 2A | 20 | 20 | 0 |
| 2B | 20 | 20 | 20 |
| 3 | 20 | 20 | 40 |
| 4 | 40 | 40 | 40 |
| 5 | 60 | 60 | 60 |
| 6 | 80 | 80 | 80 |
| NOTE – Frequency evaluation ranges for E and H fields are 100 kHz to 30 MHz for concepts 1 and 2, and 1 MHz to 200 MHz for concepts 3 to 6. | | | |

When the telecommunication centre is protected from HEMP phenomena, the surge protectors should be installed on all lines such as a.c. mains, telecommunication lines and antenna feeds.

### 6.1.5 Topological considerations

From a topological point of view, two possible approaches can be considered: global protection and distributed protection.

If global protection is chosen, the entire installation, which consists of several interconnected pieces of equipment, will be in a protected environment.

If distributed protection is chosen:

– each piece of equipment should be, at times, hardened with a shielding cabinet;

– the connection cables between the equipment should be hardened.

To select the concept and immunity test levels, the following flows should be used.

### 6.1.6 Design procedure

#### 6.1.6.1 General considerations

When an operator or a manufacturer chooses a protection concept, the first question to answer should be whether or not to provide installation or equipment protection against HEMP.

The answer to this question will depend on:

– the importance for the installation or equipment to survive HEMP. It should be noted that, in some cases, only a portion of the installation need survive;

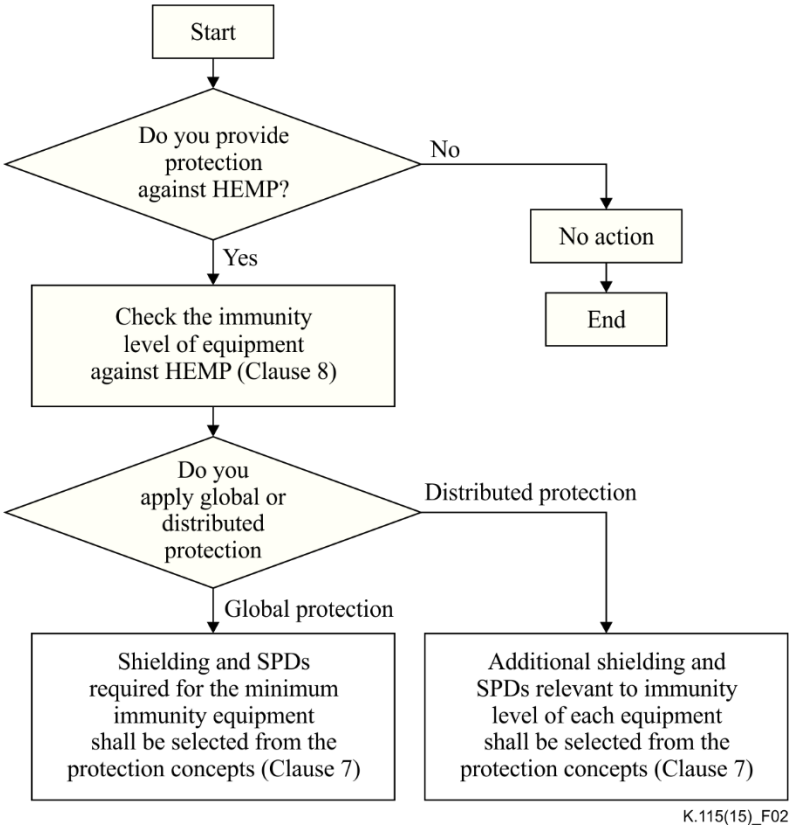
– considerations on whether interruptions of a certain time duration are permitted.

Once the protection concept has been decided upon, the immunity test level is determined by the degree of the protection concept applied to the portion where the equipment is installed. The performance criteria are set by the acceptable degree of degradation determined by the operator.

#### 6.1.6.2 Design flow chart for case 1

When a protection concept is applied to a telecommunication centre building in which a system has already been installed, only additional shielding and surge protection measures can be applied. The design flow chart is shown in Figure 2. In this case, the system equipment must conform to the immunity requirement against HEMP. If the equipment is HEMP immune (see clause 8 of

[ITU-T K.78]), an additional shielding level can be selected as a building concept level (see clause 7 of [ITU-T K.78]). If the equipment has the minimum HEMP immunity level (see Appendix I of [ITU-T K.78]), the additional shielding level is concept level 5 or 6 with additional SPDs and filters on telecommunication and power lines. The required mitigation level for the overvoltage of telecommunication port and power port by SPDs is shown in Table 2.




NOTE – Clause numbers refer to [ITU-T K.78]

**Figure 2 – Design flow chart for case 1**

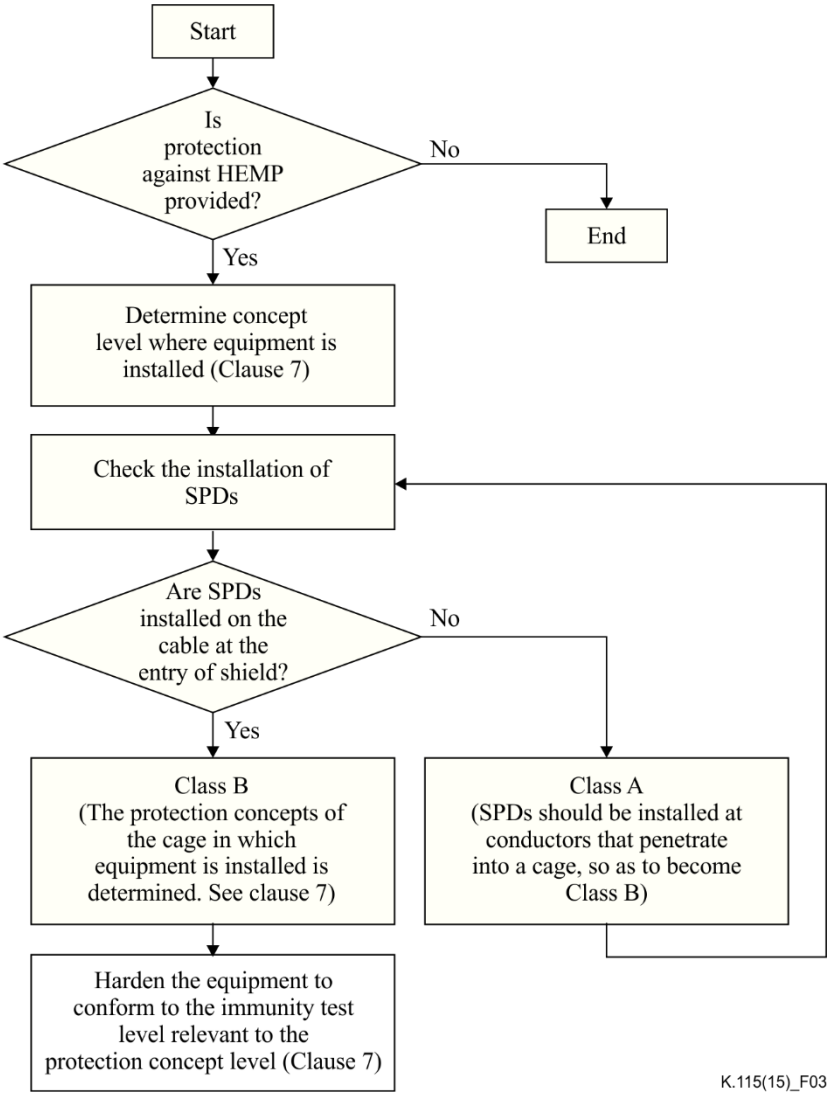
**Table 2 – Required mitigation level for telecommunication port and power port**

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

### 6.1.6.3 Design flow chart for case 2

When the building has yet to have a system installed, it can be required that the equipment will work in the given shielding and surge protection measures of the building. In this case, the requirement depends on the protection concept of the building. The design flow chart is shown in Figure 3. For example, when the building concept level is determined as level 4 (shield 40 dB, see clause 7 of [ITU-T K.78]), the installation of SPDs on the cable should first be confirmed, and the equipment,

which should have a HEMP immunity level of 4 (see clause 8 of [ITU-T K.78]), should be installed in the telecommunication centre. To protect telecommunication port and power port by SPDs, the required mitigation level is shown in Table 2.




NOTE – Clause numbers refer to [ITU-T K.78]

**Figure 3 – Design flow chart for case 2**

## 6.2 High-power electromagnetic

### 6.2.1 Introduction

HPEM is defined in [IEC 61000-2-13].

Electromagnetic environments with operating frequency spectra extending well beyond several gigahertz, including the ultra-wideband (UWB) and short pulse (SP) environments and the narrowband, high-power microwave (HPM), have been developed or postulated. Such signals, together with conducted high-power currents and voltages, are collectively denoted as HPEM environments. High-power conditions are achieved when the peak electric field exceeds 100 V/m, corresponding to a plane-wave free-space power density of 26.5 $W/m^2$.

In the light of newly emerging transient antenna technology and the increasing use of digital electronics, the possibility of equipment being upset or damaged by these environments is of concern.

The HPEM signal can originate from sources such as radar or other transmitters in the vicinity of an installation or from an intentional generator system targeting a civilian facility. Radiated signals can also induce conducted voltages and currents through the coupling process. In addition, conducted HPEM environments may also be directly injected into the wiring of an installation.

To estimate the mitigation level against HPEM for telecommunication centre equipment, such as that for switching, transmission, radio, and power equipment, both the estimation of the threat level (strength) and the vulnerability of the electronic device (or system) to be protected are needed. The estimation measures of mitigation level are presented in [ITU-T K.81].

### 6.2.2 Reference documents

The background material describing the motivation for developing IEC standards on the effects of HPEM fields, currents and voltages on civil systems is provided in [IEC TR 61000-1-5], which describes a general introduction, the HPEM environments that are of concern, and a discussion of the various effects that these environments can induce in civil systems. Finally, a summary of techniques used to protect systems against these environments is given.

It is necessary to define the radiated and conducted environments, in order to develop protection methods. A set of typical radiated and conducted HPEM environment waveforms that may be encountered in civil facilities are defined in [IEC 61000-2-13].

[ITU-T K.81] gives guidance on establishing the threat level presented by an intentional HPEM attack and the physical security measures that may be used to minimize it. [ITU-T K.81] also gives details of the vulnerability of equipment. The equipment is assumed to meet the immunity requirements presented in [ITU-T K.48] and relevant resistibility requirements, such as [ITU-T K.20], [ITU-T K.21], and [ITU-T K.45].

### 6.2.3 Example of EM mitigation levels for an IP network service

To apply the countermeasures, the determination of mitigation level is important. Mitigation level is determined from clause 7 of [ITU-T K.81]. This clause shows some examples of EM mitigation levels by classification of an IP network service.

#### 6.2.3.1 Data centre (electronic commerce)

Countermeasures must be considered for a server that circulates information with an information value level greater than the threat level. At the same time, when complete remote duplication is performed at a location sufficiently far away so that the threat from electromagnetic attack does not occur, it is only necessary to consider emanation security (EMSEC) countermeasures. Examples of the calculation of the EM mitigation levels when the threat that satisfies the availability and integrity limits regulated by the service level agreements (SLAs) is assumed to be able to intrude up to AII or the Zone 2 level, the vulnerability level is ZI1, and information leakage intrusion is at 10 m, are shown in Table 3a and Table 3b.

**Table 3a – Examples of the calculation of EM mitigation levels (electronic commerce data centre)**

| Threat number | Strength | Vulnerability level | EM mitigation level (dB) | Frequency | Counter-measure location | Remarks |
|---|---|---|---|---|---|---|
| K1-0 | 72 kV/m@100 m | 1 | 98 | 300 MHz - 10 GHz | Zones 1-3 | Shield |
| K1-4 | 475 V/m@10 m | 1 | 54 | 1 GHz - 3 GHz | Zones 1-3 | Shield |
| K1-5 | 286 V/m@1 m | 1 | 50 | 100 MHz - 3 GHz | Zones 2-3 | Shield |
| K1-7 | 573 V/m@10 m | 1 | 56 | 27 MHz | Zones 2-3 | Shield |
| K3-3 | 100 V~ 240 V/4 kV | 1 | 48 | 1 Hz - 10 MHz | Zones 2-3 | Filter |
| K3-4 | 100 V~ 240 V | 1 | 48 | 50/60 Hz | Zones 2-3 | Filter |
| K4-5 | 300 m | Class A | 25 | 30 MHz - 1 GHz | Zones 2-3 | Filter |

**Table 3b – Examples of the calculation of EM mitigation levels (electronic commerce data centre)**

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

### 6.2.3.2 Data centre (storage)

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

**Table 4a – Examples of the calculation of EM mitigation levels (storage)**

| Threat number | Strength | Vulnerability level | EM mitigation level (dB) | Frequency | Counter-measure location | Remarks |
|---|---|---|---|---|---|---|
| K1-0 | 72 kV/m@100 m | 3 | 88 | 300 MHz - 10 GHz | Zones 1-3 | Shield |
| K1-4 | 475 V/m@10 m | 3 | 44 | 1 GHz - 3 GHz | Zones 1-3 | Shield |
| K1-5 | 286 V/m@1 m | 3 | 40 | 100 MHz - 3 GHz | Zones 2-3 | Shield |
| K1-7 | 573 V/m@10 m | 3 | 46 | 27 MHz | Zones 2-3 | Shield |
| K3-3 | 100 V~ 240 V/4 kV | 3 | 38 | 1 Hz - 10 MHz | Zones 2-3 | Filter |
| K3-4 | 100 V~ 240 V | 3 | 38 | 50/60 Hz | Zones 2-3 | Filter |
| K4-5 | 263 m | Class A | 25 | 30 MHz - 1 GHz | Zones 2-3 | Filter |

**Table 4b – Examples of the calculation of EM mitigation levels (storage)**

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

### 6.2.3.3 Routers and switches (MSP)

Examples of the calculation of EM mitigation levels for a management service provider (MSP) when operating carrier grade equipment has vulnerability levels of ZI3 and ZK5 and when the threat that satisfies the availability and integrity limits regulated by SLAs is assumed to be able to intrude up to AIV or the Zone 2 level, are shown in Table 5.

**Table 5 – Examples of the calculation of EM mitigation levels (routers and switches)**

| Threat number | Strength | Vulnerability level | EM mitigation level (dB) | Frequency | Counter-measure location | Remarks |
|---|---|---|---|---|---|---|
| K1-3 | 72 kV/m@100 m | 8.5 | 34 | 1 GHz - 10 GHz | Zones 0-3 | Shield |
| K1-4 | 475 V/m@10 m | 8.5 | 35 | 1 GHz - 3 GHz | Zones 1-3 | Shield |
| K1-5 | 286 V/m@1 m | 8.5 | 31 | 100 MHz - 3 GHz | Zones 2-3 | Shield |
| K1-7 | 573 V/m@10 m | 8.5 | 37 | 27 MHz | Zones 2-3 | Shield |
| K3-3 | 100 V~ 240 V/4 kV | 3 | 38 | 1 Hz - 10 MHz | Zones 2-3 | Filter |
| K3-4 | 100 V~ 240 V | 3 | 38 | 50/60 Hz | Zones 2-3 | Filter |
| K4-5 | 263 m | Class A | 25 | 30 MHz - 1 GHz | Zones 2-3 | Filter |

### 6.2.3.4 Data centre of a local government unit or government organization

Countermeasures must be considered for a server that stores information with an information value level greater than the threat level. At the same time, when complete remote duplication is performed at a location sufficiently far away so that the threat from electromagnetic attack does not occur, it is only necessary to consider EMSEC countermeasures. Examples of the calculation of the EM mitigation levels when the level of the threat to the required availability and integrity is assumed to be able to intrude up to AIII or the Zone 2 level, the vulnerability level is ZI2 and information leakage intrusion is 10 m, are shown in Table 6a and Table 6b.

**Table 6a – Examples of the calculation of EM mitigation levels (government organization)**

| Threat number | Strength | Vulnerability level | EM mitigation level (dB) | Frequency | Counter-measure location | Remarks |
|---|---|---|---|---|---|---|
| K1-0 | 72 kV/m@100 m | 3 | 88 | 300 MHz - 10 GHz | Zones 1-3 | Shield |
| K1-4 | 475 V/m@10 m | 3 | 44 | 1 GHz - 3 GHz | Zones 1-3 | Shield |
| K1-5 | 286 V/m@1 m | 3 | 40 | 100 MHz - 3 GHz | Zones 2-3 | Shield |
| K1-7 | 573 V/m@10 m | 3 | 46 | 27 MHz | Zones 2-3 | Shield |
| K3-3 | 100 V~ 240 V/ 4 kV | 3 | 38 | 1 Hz - 10 MHz | Zones 2-3 | Filter |
| K3-4 | 100 V~ 240 V | 3 | 38 | 50/60 Hz | Zones 2-3 | Filter |
| K4-5 | 263 m | Class A | 25 | 30 MHz - 1 GHz | Zones 2-3 | Filter |

**Table 6b – Examples of the calculation of EM mitigation levels (government organization)**

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

### 6.2.3.5 Examples of EM mitigation levels of an IP company network

#### 6.2.3.5.1 Work station

Normally, only an EMSEC threat is assumed. An example of calculating the EM mitigation level when the vulnerability level is Class B, the threat intrudes up to Zone 1 and the availability level is AII, is shown in Table 7.

**Table 7 – Examples of the calculation of EM mitigation levels (work station)**

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

#### 6.2.3.5.2 Mail server

Normally, only an EMSEC threat is assumed. An example of the calculation of the EM mitigation level when the vulnerability level is Class A, the threat intrudes up to Zone 1 and the availability level is AI, is shown in Table 8.

**Table 8 – Examples of the calculation of EM mitigation levels (mail server)**

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

#### 6.2.3.5.3 ERP server, storage, customer DB server

Examples of the calculation of EM mitigation levels for a corporation database (DB), a highly valued information storage, a customer DB, etc., when the threat is assumed to intrude up to level AII and Zone 2 are shown in Table 9a and Table 9b.

**Table 9a – Examples of the calculation of EM mitigation levels (database)**

| Threat number | Strength | Vulnerability level | EM mitigation level (dB) | Frequency | Counter-measure location | Remarks |
|---|---|---|---|---|---|---|
| K1-0 | 72 kV/m@100 m | 1 | 98 | 300 MHz - 10 GHz | Zones 1-3 | Shield |
| K1-4 | 475 V/m@10 m | 1 | 54 | 1 GHz - 3 GHz | Zones 1-3 | Shield |
| K1-5 | 286 V/m@1 m | 1 | 50 | 100 MHz - 3 GHz | Zones 2-3 | Shield |
| K1-7 | 573 V/m@10 m | 1 | 56 | 27 MHz | Zones 2-3 | Shield |
| K3-3 | 100 V~ 240 V/4 kV | 1 | 48 | 1 Hz - 10 MHz | Zones 2-3 | Filter |
| K3-4 | 100 V~ 240 V | 1 | 48 | 50/60 Hz | Zones 2-3 | Filter |
| K4-5 | 263 m | Class A | 25 | 30 MHz - 1 GHz | Zones 2-3 | Shield |

**Table 9b – Examples of the calculation of EM mitigation levels (database)**

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

## 6.3 Information leakage

### 6.3.1 Introduction

Radio waves are unintentionally emitted from information technology equipment and there have been cases where information has been reproduced by such 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], and [ISO/IEC 27002]. This phenomenon is referred to as EMSEC (emanation security or electromagnetic emanation security). It is important to prevent a lack of confidentiality due to

unintentional electromagnetic radiation, particularly in equipment that is handling important information.

Threats from information leakage due to unintentional electromagnetic emanations, test methods to evaluate information leakage for conducted and radiated emission, and approaches to mitigation, are presented in [ITU-T K.84].

### 6.3.2 Reference documents

[ITU-T K.84] gives guidance on reduction of threats from information leakage due to unintentional electromagnetic emanation from information equipment handling important information at telecommunication centres.

### 6.3.3 Mitigation methods against information leakage

In order to prevent information leakage due to compromising emanations, countermeasures are categorized into:

– reduction of leaked electromagnetic radiation reaching receivers (eavesdroppers);

– enhancement of difficulty of reconstructing the original video signal, even if leaked radiations are intercepted.

The former is regarded as signal reduction and the latter as noise generation; both are measures to decrease signal-to-noise ratio (SNR) of the leaked signal at the receiver.

There are some countermeasures against information leakage. Shielding structures or equipment, inserting filters in the video signal line, decoupling at power source, and keeping a certain distance from possible eavesdroppers (zoning) are countermeasures aimed at signal reduction. Signal masking and overlying additional noise are countermeasures aimed at noise generation.

In the case of information leakage on computer systems, specific countermeasures are shown in Figure 4.

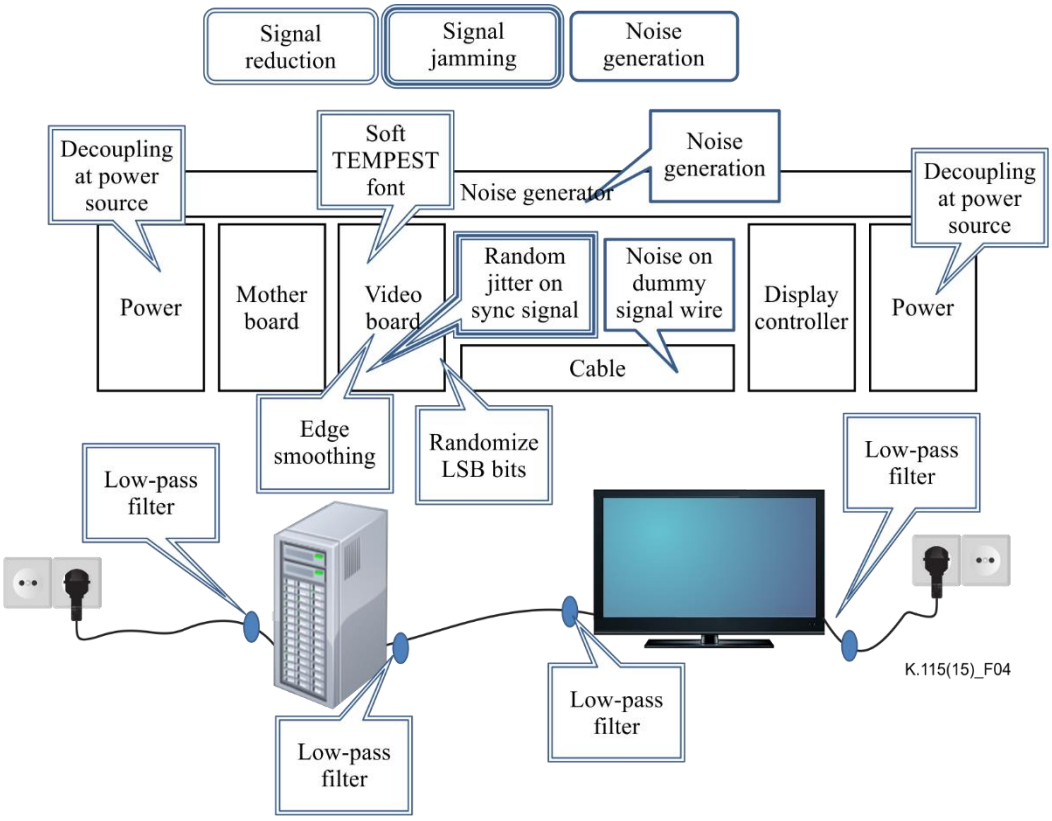



**Figure 4 – Countermeasures against information leakage from a PC system**

#### 6.3.3.1 Shielding facilities

Shielding facilities, such as specified areas, rooms or occasionally buildings, with metallic materials is the most reliable way to prevent radio waves from penetrating. However, this scheme is usually very expensive, especially when shielding rooms or buildings.

There are shielding solutions that provide modular shielding systems installed in a given facility. These solutions can be adapted to existing facilities to meet the dimension and operational needs of a particular entity, and are less expensive than the construction of shielded rooms. In these cases, the equipment or systems under protection must be used within the shielded facilities, so they cannot be mobile.

The key to obtaining good performance and reliability of a shielding system is understanding that seams, doors, and other penetrations are critical elements that must function as a whole to create an effective shielding system. Continuous maintenance of the shielding system is also important for its integrity.

Performance of the shielding system at a facility needs to be determined as follows. Electromagnetic emission from the equipment or systems to be protected should first be surveyed; then the emission level should be compared with the susceptibilities of the eavesdropping equipment, assuming the worst case. Shielding is also an effective measure for HPEM/HEMP protection. Therefore, if the equipment or systems require protection from these threats (e.g., they are mission critical or need the highest level security), shielding performance should be determined considering not only requirements for information leakage prevention, but also requirements for HPEM/HEMP (see clause 6.1 and clause 6.2).

The final decision will be based on a trade-off between the estimated shielding level and the cost of providing this shielding.

#### 6.3.3.2 Shielding equipment

Shielding equipment or components which emit compromising emanations is also a reliable way of preventing leakage. However, it should be noted that the compromising emanations are generated from various points, such as circuit boards in PCs, displays, printers, and peripherals, individual components on the circuit board, cables and connectors. Shielding is effective only if all equipment that has a possibility of leaking information is suitably protected.

Shielding is usually performed by enclosing and sealing equipment with metallic material, therefore it is difficult to shield parts where there is a human interface, such as a display screen, touch panel, keyboard, and mouse. Currently, there is some pre-measured commercially available equipment that is sometimes labelled "Tempest PC2" or similar (e.g., in the case of a laptop). Shielded equipment can be mobile, but it is usually more expensive and heavier than its static equivalent. The degree of mitigation of such mobile equipment is determined only by shield performance.

#### 6.3.3.3 Filtering, decoupling

Inserting filters into interface cables, especially video cables, is also effective for suppressing emissions. However, this is effective only if emissions radiate mainly from the interface cables, because the video signal is radiated not only from the interface cables, but also from printed circuit boards or internal connection wires in the main body of the PC or other equipment. Decoupling of the power source or power line of the equipment is also effective. Such decoupling prevents the video signal leaking from the equipment along the power lines due to electromagnetic coupling, but is effective only if the main part of the emissions is leaked conductively from the power cables. A power line filter interposed between the power network and the electronic device power socket is also an effective countermeasure against such conductive emission propagation across a power cable network [b-Kasmi].

#### 6.3.3.4 Zoning

Zoning is a policy for maintaining a certain distance from possible eavesdroppers. This enables appropriate countermeasures to be chosen according to the protection level defined in each zone, which is classified into several ranks by the distance between the equipment and a possible eavesdropping area.

Protected areas can be divided into the following typical zones (Figure 5):

- zone 0: Outside (>100 m distant from the system);
- zone 1: Same site (100-10 m distant from the system);
- zone 2: Same building (10-1 m distant from the system);
- zone 3: Same room (<1 m distant from the system).

Zoning can be used for facility or equipment shielding and serves as an excellent tool for deciding what is critical and how it should be protected [b-Bindar].

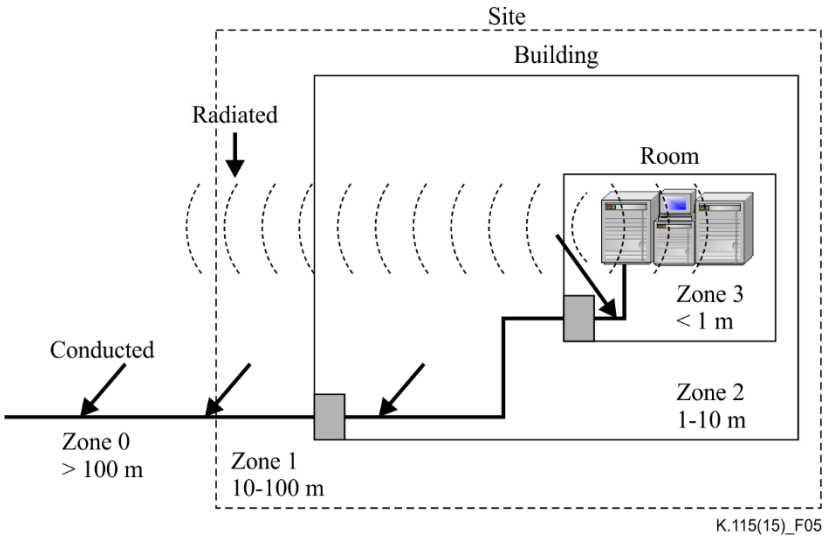



**Figure 5 – Classification of intrusion areas (zoning)**

#### 6.3.3.5 Soft Tempest

Soft Tempest is a type of countermeasure software. It has been reported that the strength of emissions can be reduced when smoothing functions, such as a low-pass or Gaussian filter, are applied to screen fonts and entire images [b-Kuhn],[b-Tanaka].

#### 6.3.3.6 Masking, noise addition

Masking or noise addition is another countermeasure technique that intentionally overlays masking signals or noise, such as random noise or meaningless signals, on the original emanation. In addition, masking signals are more effective if they are synchronized with a pixel clock to cover the frequency range of information leakage [b-Suzuki] and [b-SuzukiY] (Figure 6).

Masking is an effective and low-cost countermeasure, but masking signal and additional noise must be carefully chosen because there is some possibility that these signal can interfere with the normal function of other equipment or systems nearby.

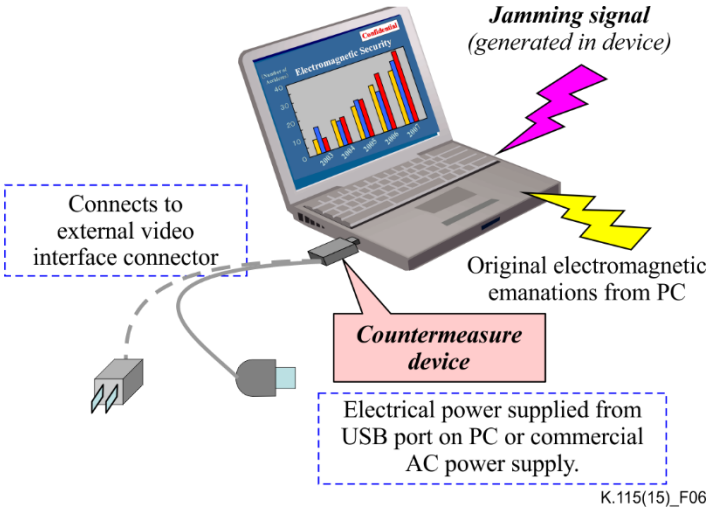



**Figure 6 – Example of countermeasure device adapted to PC**

Another countermeasure method is to apply phase noise to the oscillators used to generate clock timing (video clock or another significant clock used in the equipment) [b-Kinugawa]. Information via electromagnetic fields usually leaks through the clock frequency and higher harmonic waves. This countermeasure technique increases the amplitude fluctuation of these leaked signals at the clock frequency and its harmonics, in order to prevent satisfactory reception of the original signal.

#### 6.3.3.7 Protocol level measure

A protocol level measure, a technique that modulates the standard screen timing, is defined in [b-VESA], and is reported in [b-Watanabe] and [b-WatanabeT]. Techniques for randomizing lower significant bits of images to reduce signal and increase noise concurrently are also proposed [b-KuhnMG].

Conventional countermeasures have been developed to protect information from eavesdroppers. The features of these countermeasure schemes are listed in Table 10.

**Table 10 – Countermeasures and their features**

| Countermeasure | Protection performance | Initial cost | Availability for mobile use | Additional appliance for pre-installed equipment |
|---|---|---|---|---|
| Shielding structures | High | Very high | Impossible | Hard to apply |
| Shielding equipment | High | High | Available but not suitable (heavy weight) | Hard to apply |
| Filtering | Medium | Low | Available | Applicable |
| Zoning | (Adaptable for each case) | Low | Difficult to apply | Applicable |
| Soft Tempest | Medium | Low to medium | Available | Applicable |
| Masking | High | Low to medium | Available | Applicable |

Each countermeasure technique does not necessarily cover everything, and a combination of methods can be important to strengthen system security. An example of overall countermeasure policy is shown in Figure 7.

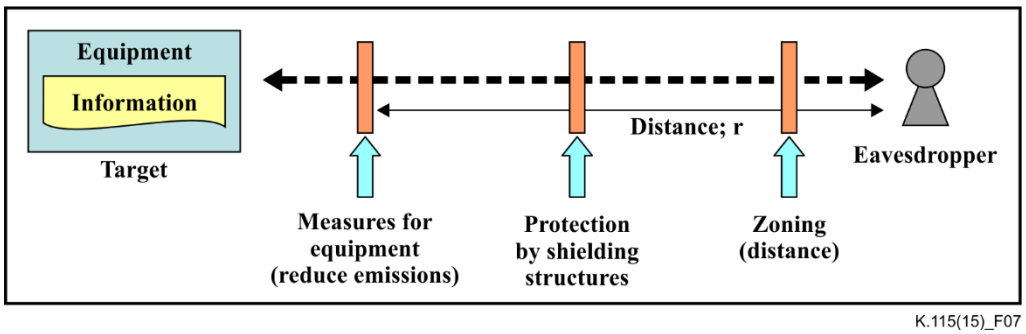



**Figure 7 – Overall countermeasure policy (example)**

## 6.4 Lightning

### 6.4.1 Introduction

Lightning is an overvoltage phenomenon and can occur in the public network or in the installation of the electricity user. Lightning that is caused by events that are external to an installation is generally a very short term overvoltage travelling in waves that attenuate with distance and whose wave front becomes less steep. The major mechanisms by which lightning produces surge voltages are the following:

a) direct lightning strike to an external (outdoor) circuit injecting high currents producing voltages by either flowing through earth resistance or flowing through the impedance of the external circuit;

b) an indirect lightning strike (i.e., a strike between or within clouds or to nearby objects, which produces electromagnetic fields) that induces voltages or currents on the conductors outside or inside a building;

c) lightning earth current flow resulting from nearby direct-to-earth discharges coupling into the common ground paths of the earthing system of the installation. The rapid change of voltage and flow of current that can occur as a result of the operation of a lightning protection device can induce electromagnetic disturbances in adjacent equipment.

Damage to equipment can occur as a result of:

– surges entering on metallic service cables, with respect to the local earth;

– lightning strikes to antennas;

– lightning current entering the ground at or near the building with respect to a remote earth;

– induction in indoor cabling due to lightning nearby.

### 6.4.2 Reference documents

A basic test for lightning is defined in [IEC 61000-4-5], which provides the immunity requirements, test methods, and range of recommended test levels for equipment to unidirectional surges caused by overvoltages from switching and lightning transients.

A test method for telecommunication equipment affected by lightning is provided in [ITU-T K.44] as a basic standard. Recommendations on a resistibility test method for telecommunication equipment installed in a telecommunication centre are provided in [ITU-T K.20] and installed in customer premises are provided in [ITU-T K.21]. Also, bonding configurations for telecommunication building is given in [ITU-T K.27] and for customer premises is in [ITU-T K.66].

A protection method for telecommunication equipment by lightning is provided in [ITU-T K.11] as a basic standard, and specific protection methods are provided in [ITU-T K.46], [ITU-T K.47], [ITU-T K.66], [ITU-T K.85], and [ITU-T K.98]. Shielding factors for lightning protection are provided in [ITU-T K.101].

An overview of protection components is provided in [ITU-T K.96], and a guide for their selection is presented in [ITU-T K.36]. Details of the functions and applications of protective devices are provided in [ITU-T K.12], and [ITU-T K.99] for gas discharge tubes, [ITU-T K.28] and [ITU-T K.102] for thyristor-based devices, [ITU-T K.77] for metal oxide varistors, [ITU-T K.82] for solid-state, self-restoring overcurrent protectors, [ITU-T K.82] for solid-state overcurrent protectors, [ITU-T K.103] for silicon PN junction components and [ITU-T K.95] for isolating transformers.

### 6.4.3 Mitigation methods against lightning

The telecommunication network can be endangered by atmospheric discharge, power influence and voltage across its components. Protective measures must be coordinated with the system to be protected. The fundamental protection methods for a telecommunication network are described in [ITU-T K.11], and they are as follows:

a) earthing: Reliable electrical connection of the system with a conductor that provides a low impedance path to the earth (ground) to prevent hazardous voltages from appearing on equipment. Normally, an earthing conductor does not carry current.

b) equipotential bonding: Electrical connection putting various exposed conductive parts and extraneous conductive parts at a substantially equal potential. It is orientated to reduce the earth potential difference between different metallic conductors, equipment, and circuits in the case of faults or external interference (such as lightning strike).

c) shielding: The process of limiting the flow of electromagnetic fields between two locations, by separating them with a barrier made of conductive material. Typically, it is applied to enclosures, separating the system from the electrical environment. Shielding used to block radio frequency electromagnetic radiation is also known as RF shielding.

d) improving insulation strength: Improvement of the insulation level of the equipment and lines to prevent overvoltage from damaging insulation so as to ensure equipment and personal safety.

e) disconnection: Allocation of the line with a fuse, resettable overcurrent protector (OCP), or switch facility to prevent excessive energy from entering sensitive circuits.

f) current distribution: Installation of an SPD between the lines or between lines and earth. SPDs restrict the voltage of a designated port or ports, caused by a surge, when it exceeds a predetermined level. The decision to use SPDs is most properly based on an analysis of the risks that are seen by the network or system under consideration.

g) countervoltages: Countervoltages are used to compensate for induced voltages.

These mitigation methods must be coordinated with the system to be protected. Appropriate protective measure for a given system can be selected according to the reference documents shown in clause 6.4.2.

#### 6.4.3.1 Protection concepts

The need for protective measures should be based on a risk assessment taking into consideration the cost and importance of the system, the electromagnetic environment at the particular site, and the probability of damages overvoltage and overcurrent caused by lightning discharge.

The protection levels and the type of protective methods should also be chosen regarding the costs of installation and maintenance of protective devices.

An assessment of the probability of overvoltage occurrences and the sensitivity of the existing telecommunication installation shall allow a well-balanced protection of the whole system to be attained.

This assessment takes into account the consequences of the loss of service for the customer and the network operator, the importance of the system (e.g., hospitals, traffic control), the electromagnetic environment at the particular site (probability of damages), and costs related to repair.

The performance of a telecommunications system with respect to overvoltages depends on:

– the environment, i.e., the magnitude and probability of overvoltages occurring in the line network associated with the system;
– the construction of the line network;
– the resistibility of equipment in the system;
– the provision of protective devices;
– the quality of the earth system provided for the operation of the protective devices.

The above aspects have to be taken into account to assess the risk.

#### 6.4.3.2 Protection device

Protection devices are usually divided into overvoltage and overcurrent elements. They may consist of single components or more complex devices, where several functions are integrated.

There are basically two types of overvoltage components: voltage switching and voltage-limiting devices.

A switching component has a discontinuous current–voltage characteristic (e.g., a gas discharge tube). A voltage-limiting device limits the voltage to a specified level and has a continuous current-voltage characteristic (e.g., a Zener diode).

The aim of such components is to protect equipment against surges of short duration by limiting the voltage and diverting the current. They are shunt connected with the equipment to be protected.

Overcurrent protective devices are divided into resettable and non-resettable components. The aim of such components is to protect the equipment against overcurrents of long duration. They will open the circuit or attenuate the current by going to high resistance. They are put in series with the equipment or elements to be protected.

Hybrid protective elements comprise different components that are integrated into assemblies that fulfil more complex protection functions. Depending on their design they may be shunt, series or a combination of the two.

Isolating devices are divided into optical insulators and electrical insulators. The aim is to create a total galvanic separation between two parts of a circuit to provide a full electrical immunity for highly exposed equipment.

Details of the functions and applications of these devices are reviewed in documents referred in clause 6.4.2.

# Bibliography


[b-IEC 60050-161] IEC 60050-161 (1990), *International Electrotechnical Vocabulary. Chapter 161: Electromagnetic compatibility*.

[b-IEC 60050-601] IEC 60050-601 (1985), *International Electrotechnical Vocabulary. Chapter 601: Generation, transmission and distribution of electricity – General*.

[b-IEC 61643-21] IEC 61643-21 (2012), *Low voltage surge protective devices – Part 21: Surge protective devices connected to telecommunications and signalling networks – Performance requirements and testing methods*.

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

[b-Bindar] Bindar, V., Popescu, M., Vulpe, A. (2014), *Considerations regarding shielding effectiveness and testing of electromagnetic protected enclosures used in communications security*, IEEE 10th International Conference on Communications (COMM), pp. 1-6.

[b-Kasmi] Kasmi, C., Coiffard, D., Helier, M., Darces, M. (2014), *Performance analysis of a power network Counter-TEMPEST filter in realistic cabling scenarios*, IEEE International Symposium on Electromagnetic Compatibility (EMC Europe), pp. 1166-1169.

[b-Kinugawa] Kinugawa, M., Hayashi, Y., Mizuki, T., Sone, H. (2011), *Information leakage from the unintentional emissions of an integrated RC oscillator*, IEEE 8th Workshop on Electromagnetic Compatibility of Integrated Circuits (EMC Compo), pp. 24-28.

[b-Kuhn] Kuhn, M.G., Anderson, R.J. (1998), *Soft Tempest: Hidden data transmission using electromagnetic emanations*, Information hiding – Lecture Notes in Computer Science, Vol. 1525, pp. 124-142. Heidelberg: Springer.

[b-KuhnMG] Kuhn, M.G. (2005), *Electromagnetic eavesdropping risks of flat panel displays*, *Privacy enhancing technologies* – Lecture Notes in Computer Science, Vol. 3424, pp. 88-107. Heidelberg: Springer.

[b-Suzuki] Suzuki, Y., Kobayashi, R., Masugi, M., Yamane, H. (2008), *Development of countermeasure device to prevent leakage of information caused by unintentional PC display emanations*, EUROEM 2008 European Electromagnetics, e177.

[b-SuzukiY] Suzuki, Y., Akiyama, Y. (2010), *Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals*, IEEE International Symposium Electromagnetic Compatibility, pp. 132-137.

[b-Tanaka] Tanaka, H., Takizawa, O. Yamamura, A. (2005), *Evaluation and improvement of TEMPEST fonts*, Information Security Applications (WISA2004) – Lecture Notes in Computer Science, Vol. 3325, pp. 457-469. Heidelberg: Springer.

[b-VESA] Video Electronics Standards Association (1998), *Monitor Timing Specifications*, Version 1.0, Revision 0.8.

[b-Watanabe] Watanabe, T., Nagayoshi, H., Sako, H., Uemura, T. (2009), *Synchronization clock frequency modulation technique for compromising emanations security (21P1-4),* International Symposium on Electromagnetic Compatibility, pp. 13-16, Kyoto.

[b-WatanabeT] Watanabe, T., Franke, K., Sako, H. (2011), *Towards large-scale EM-leakage evaluation by means of automated TOE synchronization,* IEEE International Symposium Electromagnetic Compatibility (EMC).

## 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