International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

K.87
(08/2022)

SERIES K: PROTECTION AGAINST INTERFERENCE

Guide for the application of electromagnetic security requirements – Overview

Recommendation ITU-T K.87

Recommendation ITU-T K.87

Guide for the application of electromagnetic security requirements – Overview

Summary

Recommendation ITU-T K.87 provides general guidelines of information security management for telecommunications organizations are presented in Recommendation ITU-T X.1051, which is based on ISO/IEC 27002. In an information security management system (ISMS) based on Recommendation ITU-T X.1051, physical security is one of key issues, as shown for example in the following text presented in Recommendation ITU-T X.1051:

"a site whose environment is least susceptible to damage from the environment should be selected for communication centres – where a site is chosen that is vulnerable to environmental damage, appropriate measures should be taken against known hazards including: natural disasters [see e)] and temperature extremes;"

"a site whose environment is least susceptible to damage from strong electromagnetic field shall be selected for communication centres - where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect telecommunications equipment rooms with electromagnetic shields;"

When security is managed, the threat to equipment or site should be evaluated and mitigated. The threat is related to "vulnerability" and "confidentiality" in ISMS.

This Recommendation, ITU-T K.87, outlines electromagnetic security risks of telecommunication equipment and illustrates how to assess and prevent those risks in order to manage ISMS in accordance with Recommendation ITU-T X.1051. Major electromagnetic security risks addressed in this Recommendation are as follows:

- natural electromagnetic (EM) threats (e.g., lightning);
- unintentional interference (i.e., electromagnetic interference, EMI);
- intentional interference (i.e., intentional electromagnetic interference, IEMI);
- deliberate EM attacks via high-altitude electromagnetic pulse (HEMP);
- deliberate high-power electromagnetic (HPEM) attacks;
- information leakage from EM emanation (i.e., electromagnetic security, EMSEC).

Mitigation methods against electromagnetic security threats are also described in this Recommendation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T K.87	2011-11-13	5	11.1002/1000/11426
2.0	ITU-T K.87	2016-06-29	5	11.1002/1000/12878
3.0	ITU-T K.87	2022-08-13	5	11.1002/1000/15038

Keywords

Electromagnetic emanation security, EMSEC, HEMP, high-altitude electromagnetic pulse, high-power electromagnetic, HPEM, IEMI, information leakage.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T K.87

Guide for the application of electromagnetic security requirements – Overview

1 Scope

This basic Recommendation presents guidance on the management of physical security caused by electromagnetic interference and/or emanation, for telecommunications centre managers to implement the information security management system (ISMS) requirements of Recommendation [ITU-T X.1051].

This Recommendation is a guide for the application of [ITU-T K.78] (HEMP), [ITU-T K.81] (HPEM), [ITU-T K.84] (information leakage) [ITU-T K.115] (mitigation method) and K series Recommendations on lightning protection.

This Recommendation represents an overview of electromagnetic security; it classifies the environments where devices and equipment in need of protection are installed and classifies predicted threats and vulnerabilities as well as countermeasures.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T K.20] Recommendation ITU-T K.20 (2021), *Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents*.

[ITU-T K.21] Recommendation ITU-T K.21 (2019), *Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents*.

[ITU-T K.40] Recommendation ITU-T K.40 (2019), *Protection against LEMP in telecommunications centres*.

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

[ITU-T K.44] Recommendation ITU-T K.44 (2019), *Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents – Basic Recommendation*.

[ITU-T K.45] Recommendation ITU-T K.45 (2019), *Resistibility of telecommunication equipment installed in the access and trunk networks to overvoltages and overcurrents*.

[ITU-T K.48] Recommendation ITU-T K.48 (2006), *EMC requirements for telecommunication equipment – Product family Recommendation*.

[ITU-T K.78] Recommendation ITU-T K.78 (2020), *High altitude electromagnetic pulse immunity guide for telecommunication centres*.

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

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

[ITU-T K.115] Recommendation ITU-T K.115 (2015), *Mitigation methods against electromagnetic security threats*.

[ITU-T X.1051] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[CISPR 32] IEC CISPR 32:2019, *Electromagnetic compatibility of multimedia equipment – Emission requirements*.

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

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

[IEC 61000-2-10] IEC 61000-2-10:2021, *Electromagnetic Compatibility (EMC) – Part 2-10: Description of HEMP environment – Conducted disturbance*.

[IEC 61000-2-11] IEC 61000-2-11:1999, *Electromagnetic Compatibility (EMC) – Part 2-11: Classification of HEMP environments*.

[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 61000-4-20] IEC 61000-4-20 (2022), *Electromagnetic compatibility (EMC) – Part 4-20: Testing and measurement techniques – Emission and immunity testing in transverse electromagnetic (TEM) waveguides*.

[IEC 61000-4-23] IEC 61000-4-23 (2016), *Electromagnetic Compatibility (EMC) – Part 4-23: 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: Testing and Measurement Techniques – Section 24: Test methods for protective devices for HEMP conducted disturbance – Basic EMC publication*.

[IEC 61000-4-25] IEC 61000-4-25:2019, *Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems*.

[IEC 61000-4-32] IEC 61000-4-32 (2002), *Electromagnetic Compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium-First Edition*.

[IEC 61000-4-33] IEC 61000-4-33 (2005), *Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high power transient parameters*.

[IEC 61000-4-36]	IEC 61000-4-36:2020 Ed. 2.0, *Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems. Basic EMC publication*.
[IEC 61000-5-3]	IEC TR 61000-5-3:1999, *Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts*.
[IEC 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*.
[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 61000-5-9]	IEC 61000-5-9:2009, *Electromagnetic compatibility (EMC) - Part 5-9: Installation and mitigation guidelines - System-level susceptibility assessments for HEMP and HPEM*.
[IEC 61000-6-6]	IEC 61000-6-6:2003, *Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment*.
[IEC TR 61000-4-35]	IEC TR 61000-4-35:2009, *Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – HPEM simulator compendium.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

3.1.3 emanation [b-IETF RFC 2828]: A signal (electromagnetic, acoustic, or other medium) that is emitted by a system (through radiation or conductance) as a consequence (i.e., by product) of its operation, and that may contain information. (See TEMPEST)

3.1.4 HEMP immunity test [ITU-T K.78] [IEC 61000-4-25]: The HEMP immunity test is made up of four types of tests. The radiated test is defined in clause 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 clause 5 of [IEC 61000 4-25].

3.1.5 high-altitude electromagnetic pulse (HEMP) [b-IEC glossary], [b-IEC 61000-1-3]: Electromagnetic pulse produced by a nuclear explosion outside the earth's atmosphere.

Note to entry – Typically above an altitude of 30 km.

3.1.6 high-power electromagnetic (HPEM) [b-IEC glossary], [IEC 61000-4-35]: General area or technology involved in producing intense electromagnetic radiated fields or conducted voltages and currents with a peak power which has the capability to damage or upset electronic systems.

3.1.7 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.

3.1.8 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.

3.1.9 integrity [b-ISO/IEC 27001] [ISO/IEC 27002]: Safeguarding the accuracy and completeness of information and processing methods.

3.1.10 intentional electromagnetic interference (IEMI) [b-IEC glossary]: Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purpose.

3.1.11 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.

3.1.12 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.

3.1.13 signal port [IEC 61000-6-6]: A cable port at which there is a cable carrying information for transferring data to or from the apparatus. Examples are input/output (I/O) data ports and telecom ports, etc.

3.1.14 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.

3.1.15 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.

3.1.16 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.17 vulnerability [ITU-T K.115]: The possibility that equipment does not function correctly when exposed to HEMP or HPEM and will function falsely with EMSEC.

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 deals with the risk of losing this confidentiality.

NOTE – In this Recommendation, if this risk cannot be mitigated at the equipment itself, the level of confidentiality is indicated based on the emission values of existing electromagnetic compatibility (EMC) requirements. Appendix II of Recommendation ITU-T K.84 provides further details.

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.

NOTE – In this Recommendation, the term EMSEC is used only for information leakage due to unintentional electromagnetic emission.

3.2.3 EM mitigation: The preparations made to avoid either a malfunction due to a vulnerability caused by high-altitude electromagnetic pulses (HEMPs), high-power electromagnetic (HPEM) emissions or the lack of confidentiality due to insufficient emanation security (EMSEC). The level of the EM mitigation of the equipment can be calculated from the threat level and the vulnerability level.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CB	Citizen Band
CW	Continuous Wave
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMSEC	Electromagnetic emanation Security
HEMP	High-altitude Electromagnetic Pulse
HOB	Height of Burst
HPEM	High-Power Electromagnetic
HV	High Voltage
I/O	Input/Output
IEMI	Intentional Electromagnetic Interference
IRA	Impulse Radiating Antenna
ISMS	Information Security Management System
LEMP	Lightning Electromagnetic Pulse
PC	Personal Computer
TEM	Transverse Electromagnetic

5 Conventions

This Recommendation uses the following conventions:

E1	Early time high-altitude electromagnetic pulse electric field
E2	Intermediate time high-altitude electromagnetic pulse electric field
E3	Late time high-altitude electromagnetic pulse electric field

6 Threads and protection measures relating to electromagnetic phenomena

6.1 Kinds of threats and relating Recommendations

There are two primary categories on threat relating to the electromagnetic security.

One is high-power electromagnetic interference, either natural (such as lightning) or deliberate (malicious EM attack) that causes damage and disruption for telecommunication centre equipment such as switching, transmission, radio and power.

Another is information leakage caused by unintentional electromagnetic emanations from telecommunication equipment such as servers, computers and transmission equipment, which process or carry information. There is the possibility that a malicious and skilled eavesdropper could reconstruct significant information from intercepted emanations.

Table 1 shows some EM security problems, categorized by EM phenomena, discussed in this Recommendation. Also shown are the relevant Recommendations for each security problem and their mitigation techniques.

The relationship between [ITU-T X.1051] and this Recommendation is shown as Figure 1.

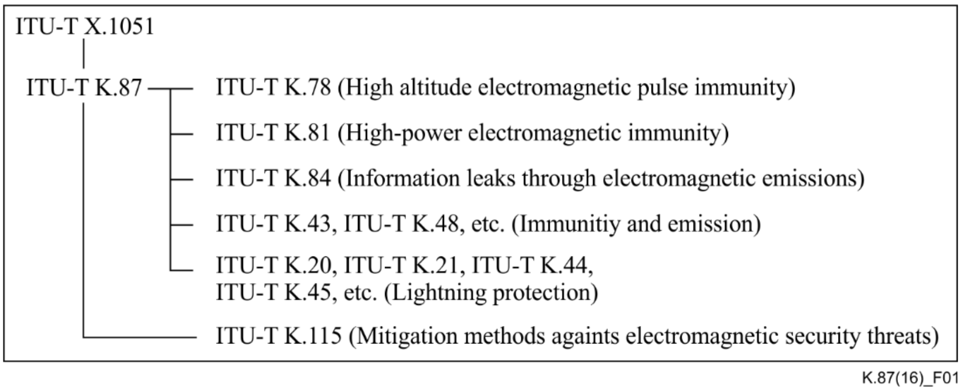


Figure 1 – The relationship between security Recommendations

Table 1 – EM security problems considered in this Recommendation

Phenomena		Category of security problem	Relevant ITU-T Recommendation	
			Requirements	Mitigation
EMI	Intentional EMI (IEMI)	HEMP	[ITU-T K.78]	[ITU-T K.115]
		HPEM	[ITU-T K.81]	
	Natural EMI	Immunity and emission	[ITU-T K.43], [ITU-T K.48], etc.	
		Lightning protection	[ITU-T K.20], [ITU-T K.21], [ITU-T K.44], [ITU-T K.45], etc.	
Information leakage		EMSEC	[ITU-T K.84]	
EMI: Electromagnetic interference HEMP: High-altitude electromagnetic pulse HPEM: High-power electromagnetic EMSEC: Electromagnetic emanation security				

6.2 Lightning

6.2.1 Introduction

Cloud to ground lightning strikes can produce high voltage surges into power and telecommunication lines by electromagnetic induction. Lightning strikes to buildings or to ground near buildings or cables can produce surges by conductive coupling into power and telecommunication circuits. These surges may cause damages in telecommunication equipment. To ensure a reliable telecommunication service, it is necessary to ensure that the equipment has an adequate level of resistibility to protect it from the majority of inductively coupled high voltage surges and protect it against the majority of higher energy surges by the installation of lightning protection measures external to the equipment. The equipment shall comply with the appropriate resistibility Recommendations listed in clause 6.1.2 below to achieve this.

6.2.2 Relation to the reference documents

The three product resistibility Recommendations, [ITU-T K.20], [ITU-T K.21] and [ITU-T K.45], provide the requirements for lightning, power induction and power contact tests. Two levels of requirements are provided: "basic level" and "enhanced level". Guidance on the application of the basic and enhanced levels is given in [ITU-T K.44]. [ITU-T K.44] contains common information relevant to the three product recommendations including test methods and test configurations with schematics.

[ITU-T K.40] presents the guidelines for the design of an effective protective system structure against lightning electromagnetic pulse (LEMP) applicable to structures for telecommunication centre. The concept of lightning protection zones is introduced as a framework where the specific protective measures, such as earthing, bonding, cable routing and shielding are merged. Information about simulation of the LEMP effects and the options of the protective measures applicable to existing and newly planned buildings are also given.

6.3 Intentional electromagnetic interference

As the value of information has increased in recent years, so too has the value and importance of information security. Information is increasingly being integrated into data strongholds, which require ever more formidable methods to resist attacks such as cyber terror.

When strong electromagnetic fields are applied intentionally from a distance to target electronic devices or systems, such as ICT equipment or transmission systems, malfunctions or more serious damages of the elements or circuits could result.

Intentional electromagnetic interference (IEMI) is the term applied to the intentional generation of strong electromagnetic energy aiming to introduce interferences to IT equipment. Lightning is not classified to IEMI, because it occurs unintentionally. The IEMI threat is classified to two types: high-power electromagnetic (HPEM) and high-altitude electromagnetic pulse (HEMP) threats. HEMP is the term applied to the electromagnetic pulse produced by a nuclear explosion at high-altitude atmosphere, typically above an altitude of 30 km. HPEM is the term applied to an intentionally produced strong electromagnetic radiated field or conducted voltages and currents with a peak power which has the capability to damage or upset electronic systems. There are many kinds of devices that generate such strong electromagnetic waves, including illegal devices, appearing on the market. For example, devices that can radiate high power electromagnetic waves including citizen band (CB) radio equipment, amateur radio equipment, navigation radars, microwave ovens, and devices that create high voltage static electricity include stun guns. Also, compact lightning-surge-generators and continuous wave (CW) generators with amplifier used generally in test labs can generate electromagnetic waves or can be used to generate conducted interferences by way of metal wires. These threats are classified as radiated and conducted threats according to the propagation paths from HPEM sources to ICT equipment. Examples are shown in Table 2.

Table 2 – Examples of propagation paths and threat

Electromagnetic wave attack – radiated	Attack by applying strong electromagnetic waves using a high-power wireless device, microwave generator, radar, etc.
Electromagnetic wave attack – conducted	Attack by applying high voltage/current waves directly to communication lines or power lines using a compact lightning-surge generator, high-power CW generator, etc.

The threat of IEMI is evaluated by several factors, i.e., portability of an EMI generation device, an intrusion area and availability in terms of required cost and technical level. It is necessary to perform risk evaluation and classify the level of threat in order to determine adequate countermeasures against IEMI in each case.

6.4 High-altitude electromagnetic pulse (HEMP)

6.4.1 Introduction

HEMP is the term applied to the electromagnetic pulse produced by a nuclear explosion at high-altitude. In this context, "high altitude" is typically above 30 km, such that other physical effects associated with a nuclear detonation are not present at ground level.

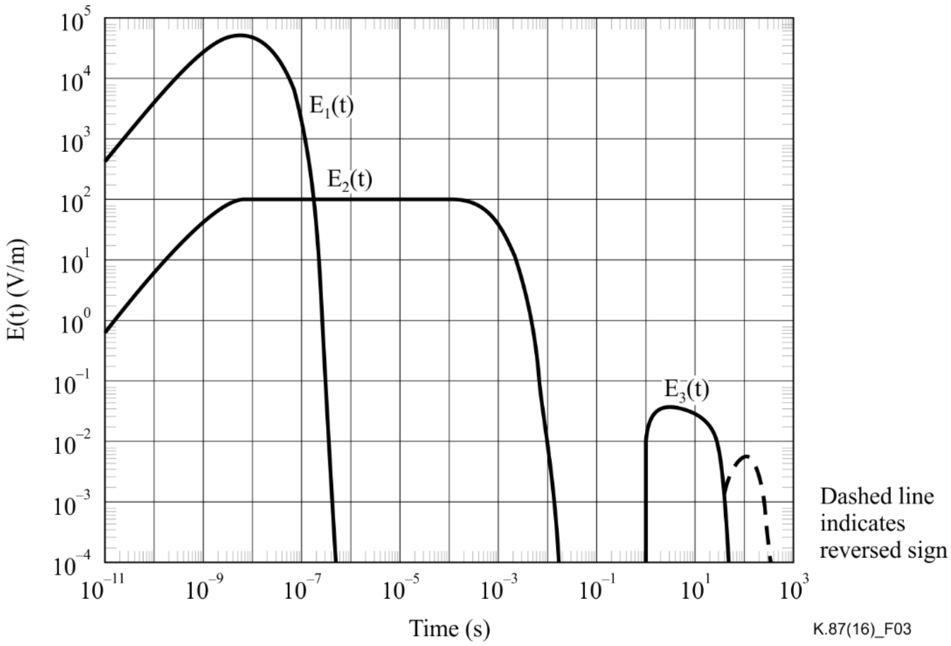
HEMP generates an electromagnetic pulse that contains both a radiated component (due to the detonation itself) and a conducted component (due to the coupling of the radiated environment with exposed, overhead cables and subsequent propagation along the cable).

A high-altitude nuclear detonation acts as a point source from which a spherical wave-front propagates, at the speed of light, from the point of detonation towards the surface of Earth. This wave-front is, depending upon altitude, able to illuminate a large section of the Earth's surface. An example of this phenomenon is illustrated in Figure 2, which shows the electromagnetic field at the ground level produced by the detonation of a 200 kt nuclear explosive at an altitude of 300 km.

Figure 2 – Example of a HEMP event

Precise figure of the typical variations in peak incident E1 HEMP electric fields is shown in Figure 6 of [IEC 61000-2-9]. For a 300 km burst height, the range to the outer circle should be ~1900 km. The location of the 0.75 Emax contour to the South of the burst is at a range of 4.2 times of the height of burst (HOB) or 1260 km. The outer circle should be at a range of 1900 km or nearly 6.3 times of HOB given the scale.

HEMP consists of three separate and distinct pulses that are produced by different mechanisms (see Figure 3, originally from Figure 10 in [IEC 61000-2-9]).



NOTE – New information regarding E3(t), [b-Edward], has raised the IEC peak field recommendation to ~0.1 V/m)

Figure 3 – Pulse characteristics

The first pulse, referred to as the "early-time HEMP (E1)" pulse (E_1 in Figure 3), is generated by the high-energy gamma-rays produced during the detonation as they undergo Compton scattering by atmospheric atoms. This interaction ionizes the atmospheric atoms, producing a very large number of high-energy electrons that experience the Lorentz force due to the earth's magnetic field. This force causes the high energy electrons to turn coherently and in phase creating a line of transverse currents in the upper atmosphere and hence radiate electromagnetic energy. The electromagnetic energy of early time HEMP arrives at ground-level. This pulse has the following characteristics:

- a very rapid rise time (of the order of a few nanoseconds, i.e., $\sim 10^{-9}$ s);
- a ground-level electric field amplitude up to 50 kV/m beneath the detonation;
- a very short duration (of the order of hundreds of nanoseconds, i.e., $\sim 100 \times 10^{-9}$ s).

The second pulse, referred to as the "intermediate time HEMP (E2)" pulse (E_2 in Figure 3), is also generated by the Compton scattering of gamma-rays by atmospheric atoms, but involves comparatively lower-energy interactions that take place after the initial, hugely energetic phase associated with the nuclear detonation. This pulse has the following characteristics:

- a much slower rise time (of the order of a few hundreds of nanoseconds, i.e., $\sim 100 \times 10^{-9}$ s);
- a ground-level electric field amplitude up to 100 V/m directly beneath the detonation;
- a much longer duration (of the order of tens of milliseconds, i.e., $\sim 10 \times 10^{-3}$ s).

The third pulse, referred to as the "late time HEMP (E3)" (E_3 in Figure 3), is essentially similar to the phenomena that has been observed in the higher northern latitudes in response to geomagnetic storms in the upper atmosphere due to solar storm. The high-altitude nuclear detonation induces the flow of currents in the upper atmosphere to behave in a manner similar to the phenomena observed during a geomagnetic storm. This pulse has the following characteristics:

- a much slower rise time (of the order of a few seconds, i.e., ~1 s);
- a ground-level electric field amplitude up to 10 mV/m directly beneath the detonation (see Note)
- a much longer duration (of the order of hundreds of seconds, i.e., ~100 s).

NOTE – New information regarding $E_3(t)$ [b-Edward] shows a ground-level electric field amplitude up to 100 mV/m directly beneath the detonation.

Table 3 shows examples of evaluated HEMP threat.

Detailed environment description is in [IEC 61000-2-9]. [61000-2-10] and [61000-2-11].

Table 3 – Example of evaluated threat related to HEMP

Threat type	Example of attack device	Strength	Wave form/frequency range
HEMP attack	Radiation (early-time HEMP)	50 kV/m peak	2.5/23 ns/1 MHz-200 MHz
	Conduction (intermediate-time HEMP)	20 kV peak	125/1500 μs, 1 kHz-1 MHz

6.4.2 Relation to the reference documents

[ITU-T K.78] provides the radiated and conducted immunity requirements for telecommunication equipment such as switching, transmission, radio, and power installed in telecommunication centres against a high-altitude electromagnetic pulse (HEMP).

[ITU-T K.78] contains immunity test methods and levels for telecommunication equipment in each installation condition.

6.5 High-power electromagnetic (HPEM)

6.5.1 Introduction

HPEM is the term applied to the intentionally produced electromagnetic phenomena created by high-power electromagnetic (HPEM) sources. These sources are discussed in the IEC 61000 series standards listed in clause 2. IEC standard, technical report and technical standard are published for HPEM threats as shown in Table 4; and also related deliverables are published under the responsibility of IEC SC 77C.

Table 4 – Standards and summaries related to HPEM of the IEC 61000 series

Standard number	Standard name	Description and summary
[IEC TR 61000-1-5]	High-power electromagnetic (HPEM) effects on civil systems	Example of the effects (HPEM) of high-power electromagnetic waves on civil systems, and a summary of test results.
[IEC 61000-2-13]	High-power electromagnetic (HPEM) environments – radiated and conducted	Description of HPEM environments, summary of generating devices, definition of waveforms, etc.
[IEC TR 61000-4-35]	HPEM simulator compendium	Information about extant system-level High-Power Electromagnetic (HPEM) simulators and their applicability as test facilities, etc.
[IEC 61000-4-36]	IEMI immunity test methods for equipment and systems. Basic EMC publication	This standard provides methods to determine test levels for the assessment of the immunity of equipment and systems to intentional electromagnetic interference (IEMI) sources. It introduces the general IEMI problem, IEMI source parameters, derivation of test limits and summarizes practical test methods.
[IEC 61000-5-9]	Installation and mitigation guidelines - System-level susceptibility assessments for HEMP and HPEM	It provides information on available methods for the assessment of system-level susceptibility as a result of HEMP and HPEM environments.

[IEC TR 61000-1-5] provides an example of HPEM and describes the background for research of HPEM, introduces HPEM generators and provides summaries of test results on devices such as personal computers (PCs). In conduction, a lightning-surge generation is included as an HPEM generator. Further, Chapter 7 of [IEC TR 61000-1-5] touches on countermeasure concepts and describes countermeasure methods such as shielding and surge-voltage protection, as well as the existence of alternative countermeasure methods such as active protection or system degeneration, error detection and error collection software.

In [IEC 61000-2-13] the importance of reviewing the HPEM process is clearly explained as follows:

"A threat environment is provided by an artificially caused high-power electromagnetic wave (HPEM). That kind of threat environment can give large damage to consumer electrical equipment and electronic devices as described in [IEC TR 61000-1-5]. In order to establish protection methods, it is necessary to define radiation and conduction environments."

Various kinds of radiation HPEM generators and examples of waveforms are also described in Chapter 5 of [IEC 61000-2-13], and the threat due to conduction is explained in Chapter 6 of [IEC 61000-2-13]. Examples of the electric field intensity of some types of HPEM generators are given in Annex B of [IEC 61000-2-13].

The IEC 61000 series documents listed in clause 2 and [ITU-T K.81] guide immunity requirements for telecommunication systems.

In [ITU-T K.81] HPEM threats are classified by particular factors, i.e., threat portability level, the intrusion area and availability levels; they are also defined in [ITU-T K.81]. Classifications of threat and associated examples are described in clause 5 of [ITU-T K.81]. Table 5 (originally from Table 5.4-1 in [ITU-T K.81]) shows calculation examples of HPEM threat.

Table 5 – Evaluated threat of examples of HPEM devices

Threat type	HPEM device	Strength	Frequency range
Radiated electromagnetic wave	IJOLT	172 kV/m@100 m	350 MHz-2 GHz
	IRA (hi-technology)	12.8 kV/m@100 m	300 MHz-10 GHz
	Commercial radar (mid-technology)	60 kV/m@100 m	1 GHz-10 GHz (1.285 GHz)
	Navigation radar	385 V/m@100 m	1 GHz-10 GHz (9.41 GHz)
	Magnetron generator	475 V/m@10 m	1 GHz-3 GHz
	Amateur wireless device	286 V/m@1 m	100 MHz-3 GHz
	Amateur wireless device	169 V/m@10 cm	100 MHz-3 GHz
	Illegal CB radio	573 V/m@10m	27 MHz
Electrostatic discharge	Stun gun	500 kV	100 MHz-3 GHz
Conducted disturbance	Lightning-surge generator	50 kV (charging voltage)	1.2/50 µs 10/700 µs
	Compact lightning-surge generator	10 kV (charging voltage)	1.2/50 µs 10/700 µs
	CW generator	100 V~240 V/4 kV	1 Hz-10 MHz
	Commercial power supply	100 V~240 V	50/60 Hz

EM mitigation levels against HPEM attack are defined in clause 6 of [ITU-T K.81], considering both HPEM threat and vulnerability levels. Examples of mitigation levels for some HPEM devices are also presented.

Examples of HPEM threat and vulnerability that use impulse radiating antenna (IRA) with the repetitive high impulse generator discussed in [b-Baum 2004], are described in detail in Appendix I of [ITU-T K.81].

6.5.2 Relation to the reference documents

[ITU-T K.81] provides the radiated and conducted immunity requirements for telecommunication equipment such as switching, transmission, radio, and power installed in telecommunication centres against a high-power electromagnetic (HPEM).

[ITU-T K.81] contains immunity test methods and levels for telecommunication equipment in each installation condition. [ITU-T K.115] also provides mitigation methods for the threats of an HPEM. [b-CIGRE C4.206] provides the mitigation methods for power stations and so on.

6.6 Information leakage

6.6.1 Introduction

Electronic equipment usually emit unintentional electromagnetic waves, and some of these emissions may carry important information processed inside the equipment. This emitted information can often be stolen by intercepting such emissions from a distance.

This Recommendation gives guidance to reduce the threats from such information leakage due to unintentional electromagnetic emanation from information equipment at telecommunication centres managed by an information security management system (ISMS).

EMSEC is the term applied to the information leakage due to unintentional electromagnetic emission in this Recommendation. Threat of EMSEC is considerable for many kinds of equipment such as personal computers, data servers, laser printers, keyboards, and cryptographic modules. This Recommendation only treats information leakage from equipment that includes raster scan video signal. Further study is required of equipment involving other kinds of leaked signals.

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

1 emission requirements and methods of examining equipment are applied when the equipment cannot be installed in the shielding site (the shielding site should reduce the emissions of the equipment);

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

EMSEC threats are determined according to comparisons of the confidentiality and threat levels as given in clause 5 of [ITU-T K.84]. The threat level is determined by intrusion range, portability, and availability of the threat devices. The threat of EMSEC is described in Appendix I of [ITU-T K.84]. The confidentiality level of the equipment, which is evaluated with existing EMC standards, is presented in Appendix II of [ITU-T K.84]. Examples of threats against EMSEC are summarized in Table 6 (originally Table 5.1-1 of [ITU-T K.84]). Definitions of threats related to portability levels and threat availability levels are presented in Tables 7 and 8 (originally, Tables 5.1-2 and 5.1-3 of [ITU-T K.84]). 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, antenna, etc.

Table 6 – Examples of threats related to information leakage

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

Table 7 – Definitions of threat portability levels

Threat portability level	Definition
PI	Pocket-sized or body-worn (Note 1)
PII	Briefcase or back-pack sized (Note 2)
PIII	Motor-vehicle sized (Note 3)
PIV	Trailer-sized (Note 4)
NOTE 1 – This portability level applies to threat devices that can be hidden in the human body and/or in the clothing. NOTE 2 – This portability level applies to threat devices that are too large to be hidden in the human body and/or in the clothing, but still small enough to be carried by a person (such as in a briefcase or a back-pack). NOTE 3 – This portability level applies to threat devices that are too large to be easily carried by a person, but small enough to be hidden in a typical consumer motor vehicle. NOTE 4 – This portability level applies to threat devices that are too large to be either easily carried by a person or hidden in a typical consumer motor vehicle. Such threat devices require transportation using a commercial/industrial transportation vehicle.	

Table 8 – 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

As shown in Table 6, 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 is high that the threat device will get closer, 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 security requirement level of equipment is described in clause 5.3 of [ITU-T K.84], and the test method is explained in Annex A of [ITU-T K.84].

Where the possibility is low that the threat device will get closer, e.g., the equipment is installed at a secure site and it 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, which is explained in existing EMC emission standards. The level of security requirements for shielding is described in clause 5.4 of [ITU-T K.84].

6.6.2 Relation to the reference documents

[ITU-T K.84] provides guidance to reduce the threats from information leakage due to EMSEC of information equipment at telecommunication centres. [ITU-T K.115] also provides mitigation methods for information leakage from information equipment.

[ITU-T K.84] 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 32] is installed at a site.

[ITU-T K.84] also provides a method of testing EMSEC for radiation in its Annex A and for conductive coupling in its Annex B. Examples of measurement methods, wideband measurement, and narrowband measurement, are presented in Appendix III and Appendix IV of [ITU-T K.84].

Bibliography

ITU security

[b-ITU-T Handbook] ITU-T Handbook (2006), *Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications*.

IEC EMC

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

Standards related to ICT security

[b-CISPR 17] CISPR 17:2011, *Methods of measurement of the suppression characteristics of passive EMC filtering devices*.

[b-CISPR 24] CISPR 24:2010, *Information technology equipment – Immunity characteristics – Limits and methods of measurement*.

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

[b-ISO/IEC 15408-1] ISO/IEC 15408-1 (2009), *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/IEC 15408-2] ISO/IEC 15408-2 (2008), *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements*.

[b-ISO/IEC 15408-3] ISO/IEC 15408-3:2008, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*.

[b-ISO/IEC 19790] ISO/IEC 19790 (2012), *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27002] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection – Information security controls*.

Other standards related to shield measurement methods

[b-IEC 61587-3] IEC TS 61587-3 (2013), *Mechanical structures for electronic equipment – Tests for IEC 60917 and IEC 60297 – Part 3: Electromagnetic shielding performance tests for cabinets, racks and subracks*.

[b-IEEE 299] IEEE Std 299-2006, *IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures*.

Other documents

[b-IEC Glossary] https://std.iec.ch/glossary

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

[b-NEBS SR-3580] Telcordia Technologies NEBS SR-3580 (2012), *Criteria Levels*.

[b-NTT TR 549001] Nippon Telegraph and Telephone Corporation TR 549001 (2005), *Technical requirements for immunity of telecommunications equipment*.

HEMP documents

[b-Agrawal] Agrawal, A., Price, J., Gurbaxani, S. (1980), *Transient Response of multiconductor Transmission Lines Excited by a Nonuniform Electromagnetic Field*, IEEE Transactions on EMC, Vol. 22, No. 2, May; pp. 119-129.

[b-Barnes] Barnes, P., *et al.* (1973), *The Effects of Electromagnetic Pulse (EMP) on State and Local Radio Communications*, Oak Ridge, TN, Defense Technical Information Center.

[b-Bell] Bell Laboratories (1975), *EMP Engineering and Design Principles*, Whippany, NJ, Bell Laboratories.

[b-Edward] Edward Savage, William Radasky (2017), *Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures*, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume II, July, http://www.firstempcommission.org

[b-Eichler] Eichler, C., Legro, J., Barnes, P.R. (1989), *Experimental Determination of the Effects of Steep Front-Short Duration Surges on 25 kVA Pole Mounted Distribution Transformers*, IEEE Transactions on Power Delivery, Vol. 4, No. 2, April; pp. 1103-1110.

[b-Ellis] Ellis, V., HDL-TR-2149 (1989), *Consumer Electronics Testing to Fast-Rise EMP (VEMPS II Development)*, Adelphi, MD, Harry Diamond Laboratories.

[b-Glasstone] Glasstone, S., Dolan P. (1977), *The Effects of Nuclear Weapons*, Washington, DC, U.S. Department of Defense and Department of Energy.

[b-Greetsai] Greetsai, V.N., *et al*. (1998), *Response of Long Lines to Nuclear High-Altitude Electromagnetic Pulse (HEMP*), IEEE Transactions on EMC, Vol. 40, No. 4, November; pp. 348-354.

[b-Hansen] Hansen, D., *et al.* (1990), *Response of an Overhead Wire Near a NEMP Simulator*, IEEE Transactions on EMC, Vol. 32, No. 1, February; pp. 18-27.

[b-Ianoz] Ianoz, M., *et al.* (1993), *Response of Multiconductor Power Lines to Close Indirect Lightning Strokes*, Proceedings of the CIGRE Symposium, Power System Electromagnetic Compatibility, Lausanne.

[b-IEC 61000-1-3] IEC TR 61000-1-3 (2002), *Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems*.

[b-Imposimato] Imposimato, C., *et al.* (1999), *Evaluation of the radiated lightning coupling on real MV power lines by an EMP Simulator*, 13th International Zurich Symposium on EMC.

[b-Loborev] Loborev, V. (1994), *Up to Date State of the NEMP Problems and Topical Research Directions*, Proceedings of the European Electromagnetics International Symposium – EUROEM 94, pp. 15-21.

[b-Vittitoe] Vittitoe, C. (1989), SAND 88-3341, *Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?* Sandia National Laboratories.

HPEM documents

[b-CIGRE C4.206] CIGRE WG C4.206 (2014), *Protection of the High Voltage Power Network Control Electronics Against Intentional Electromagnetic Interference (IEMI)*.

[b-Agee] Agee, F.J., *et al*. (1998), *Ultra-Wideband Transmitter Research*, IEEE Transactions on Plasma Science, Vol. 26, No. 3, June; pp. 860-873.

[b-Baum 1992a] Baum, C.E. (1992), *From the Electromagnetic Pulse to High-Power Electromagnetics*, Proceedings of the IEEE, Vol. 80, No. 6, June; pp. 789-817.

[b-Baum 1992b] Baum, C.E. (1992), *Maximization of Electromagnetic Response at a Distance*, IEEE Transactions on EMC, Vol. 34, No. 3, August; pp. 148-153.

[b-Baum 2002] Baum, C.E., Lehr, J.M. (2002), *Tapered Transmission-Line Transformers for Fast High-Voltage Transients*, IEEE Transactions on Plasma Science, Vol. 30, No. 5, October; pp. 1712-1721.

[b-Baum 2004] Baum, C.E., *et al.* (2004), *JOLT: A Highly Directive, Very Intensive, Impulse-Like Radiator*, Proceedings of the IEEE, Vol. 92, No. 7, July; pp. 1096-1109.

[b-Giri] Giri, D.V., *et al.* (2000), *Intermediate and Far Fields of a Reflector Antenna Energized by a Hydrogen Spark-Gap Switched Pulser*, IEEE Transactions on Plasma Science, Vol. 28, No. 5, October; pp. 1631-1636.

[b-Ianoz] Ianoz, M., Nicoara, B.I.C, Radasky, W.A. (1996), *Modeling of an EMP Conducted Environment*, IEEE Transactions on EMC, Vol. 38, No. 3, August; pp. 400-413.

[b-Mikheev] Mikheev, O.V., *et al*. (1997), *New Method for Calculating Pulse Radiation from an Antenna With a Reflector*, IEEE Transactions on Electromagnetic Compatibility, Vol. 39, No. 1, pp. 48-54.

[b-Prather] Prather, W.D., *et al*. (2000), *Ultra-Wideband Source and Antenna Research*, IEEE Transactions on Plasma Science, Vol. 28, No. 5, October; pp. 1624 1630.

[b-Silfverskiold 1999] Silfverskiold, S., *et al*. (1999), *Induced Voltages in a Low-Voltage Power Installation Network Due to Lightning Electromagnetic Fields: An Experimental Study*, IEEE Transactions on Electromagnetic Compatibility, Vol. 41, No. 3, August; pp. 265-271.

[b-Silfverskiold 2002] Silfverskiold, S., *et al*. (2002), *Microwave Field-to-Wire Coupling Measurements in Anechoic and Reverberation Chambers*, IEEE Transactions on Electromagnetic Compatibility, Vol. 44, No. 1, February; pp. 222-232.

EMSEC documents

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

[b-Kuhn 2011] Kuhn, M.G. (2011), *Compromising Emanations of LCD TV Sets*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 931-936.

[b-Kuhn 1998] Kuhn, M.G., Anderson, R.J. (1998), *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, Proceedings of the Second International Workshop on Information Hiding, Portland, Oregon, 14-17 April; pp. 124-142.

[b-Loughry] Loughry J., Umphress, D.A. (2002), *Information Leakage from Optical Emanations*, ACM Transactions on Information and System Security, Vol. 5, No. 3, August; pp. 262-289.

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

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

[b-Sekiguchi 2009b] Sekiguchi, H., 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-Sekiguchi 2011] Sekiguchi, H., Seto, S. (2011), *Estimation of Receivable Distance for Radiated Disturbance Containing Information Signal from Information Technology Equipment*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 942-945.

[b-Smulders] Smulders, P. (1990), *The threat of information theft by reception of electromagnetic radiation from RS-232 cables*, Computers and Security, Vol. 9, No.1, January; pp. 53-58.

[b-Tosaka] Tosaka, T., Yamanaka, Y., 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, May; pp. 67–70.

[b-Van Eck] Van Eck, W. (1985), *Electromagnetic radiation from video display units: An eavesdropping risk?* Computers and Security, Vol 4, No. 4, December; pp. 269-286.

[b-Watanabe] Watanabe, T., Franke, K., Sako, H. (2011), *Towards Large-scale EM-leakage Evaluation by means of Automated TOE Synchronization*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 937-941.

EMSEC documents (side-channel attacks)

[b-Hayashi] Hayashi, Y., *et al.* (2011), *Non-Invasive EMI-Based Fault Injection Attack against Cryptographic Modules*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 763-767.

[b-Ikematsu] Ikematsu, T., *et al.* (2011), *Suppression of Information Leakage from Electronic Devices Based on SNR*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 920-924.

[b-Iokibe] Iokibe, K., *et al.* (2011), *On-Board Decoupling of Cryptographic FPGA to Improve Tolerance to Side-Channel Attacks*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 925-930.

[b-Meynard] Meynard, O., *et al.* (2011), *Identification of Information Leakage Spots on a Cryptographic Device with an RSA Processor*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 773-778.

[b-Sauvage] Sauvage, L., *et al.* (2011), *Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation*, Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, 14-19 August; pp. 768-772.

Standards for video display units

[b-VESA 1999] VESA (1999), *Generalized Timing Formula (GTF)*, Version 1.1, Milpitas, CA, Video Electronics Standards Association.

[b-VESA 2007] VESA (2007) *VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT)*, Version 1.0, Milpitas, CA, Video Electronics Standards Association.

IST in Japan

[b-IST SG] Information Security Technology Study Group website.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022