

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series K

Supplement 5

(04/2016)

SERIES K: PROTECTION AGAINST INTERFERENCE

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

ITU-T K-series Recommendations – Supplement 5

ITU-T

Supplement 5 to ITU-T K-series Recommendations

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

Summary

When information security is managed, it is necessary to evaluate and mitigate the threat to either the equipment or the site. This threat is related to "vulnerability" and "confidentiality" in information security management system (ISMS).

Supplement 5 to ITU-T K-series Recommendations presents evaluation and calculation examples for the threat of an intentional high-altitude electromagnetic pulse (HPEM) attack. The HPEM sources considered are those presented in IEC 61000-2-13, as well as some additional sources that have emerged more recently.

This Supplement also provides information on the vulnerability of telecom equipment, and presents the example of vulnerability. It is desirable that the equipment meets the immunity requirements presented in Recommendation ITU-T K.48 and relevant resistibility requirements, such as those described in Recommendations ITU-T K.20, ITU-T K.21 and ITU-T K.45.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T K Suppl. 5	2016-04-27	5	11.1002/1000/12965

Keywords

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

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

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

© ITU 2016

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

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Supplement	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Calculating HPEM threat.....	3
	6.1 Impulse radiating antenna (IRA) and JOLT	3
	6.2 Commercial radar	7
	6.3 Navigation radar	8
	6.4 Magnetron generator	9
	6.5 Illegal citizen band radio	11
	6.6 Amateur radio	12
	6.7 Stun gun.....	14
	6.8 Lightning-surge generator	16
	6.9 CW generator.....	17
	6.10 Commercial power supply.....	18
7	Vulnerability of IT equipment	18
	7.1 Vulnerability to an electromagnetic wave attack	18
	7.2 Vulnerability evaluation of a sample device	21
	7.3 Vulnerability to electrostatic discharge	24
	Bibliography.....	25

Introduction

In order to establish the sufficient mitigation to HPEM attacks, it is extremely important that the threat level (electric field strength) and the vulnerability of telecom equipment are adequately estimated. This Supplement provides the calculation examples of threat level from various sources presented in IEC 61000-2-13. The vulnerability examples of telecom equipment are also provided.

Supplement 5 to ITU-T K-series Recommendations

ITU-T K.81 – Estimation examples of the high-power electromagnetic threat and vulnerability for telecommunication systems

1 Scope

This document is a supplement to ITU-T K.81. This Supplement presents evaluation and calculation examples for the threat of an intentional HPEM attack.

2 References

- [ITU-T K.20] Recommendation ITU-T K.20 (2016), *Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents*.
- [ITU-T K.21] Recommendation ITU-T K.21 (2016), *Resistibility of telecommunication equipment installed in customer premises to overvoltages and overcurrents*.
- [ITU-T K.43] Recommendation ITU-T K.43 (2009), *Immunity requirements for telecommunication network equipment*.
- [ITU-T K.45] Recommendation ITU-T K.45 (2016), *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.81] Recommendation ITU-T K.81 (2016), *High-power electromagnetic immunity guide for telecommunication systems*.
- [IEC 61000-2-13] IEC 61000-2-13 (2005), *Electromagnetic compatibility (EMC) – Part 2-13: Environment – High-power electromagnetic (HPEM) environments – Radiated and conducted*.
- [IEC CISPR 24] CISPR 24 (2010), *Information technology equipment – Immunity characteristics – Limits and methods of measurement*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

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

3.1.2 confidentiality [ITU-T K.81]: Ensuring that information is accessible only to those authorized to have access. Information leakage due to insufficient electromagnetic emanations security (EMSEC) is a risk to this confidentiality. In this Recommendation, if the equipment cannot be EM mitigated itself, the emission values of existing electromagnetic compatibility (EMC) requirements indicate the level of this confidentiality.

3.1.3 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 EM mitigation [ITU-T K.81]: The preparations made to avoid either:

- a malfunction due to a vulnerability caused by high-altitude electromagnetic pulses (HEMP) or high-power electromagnetic (HPEM) emissions, or
- a lack of confidentiality due to an insufficient electromagnetic emanations security (EMSEC).

The level of the EM mitigation of the equipment can be calculated from the threat level and the vulnerability level.

3.1.5 electromagnetic emanations security [ITU-T K.81]: Physical constraints to prevent information compromise through signals emanated by a system, particularly the application of TEMPEST technology to block electromagnetic radiation.

3.1.6 threat: A potential security violation that arises from taking advantage of a vulnerability caused by high-altitude electromagnetic pulses (HEMP) or high-power electromagnetic (HPEM) emissions, and which could lead to a lack of confidentiality due to insufficient electromagnetic emanations security (EMSEC). The level of a HPEM threat is defined by the intrusion area, the portability and the availability but also by the strength of the electromagnetic field.

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

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AM	Amplitude Modulation
CB	Citizen Band
CW	Continuous Wave
DC	Direct Current
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMSEC	EM emanations Security
FET	Field Effect Transistor
FM	Frequency Modulation
FTP	File Transfer Protocol
GTEM	Gigahertz Transverse Electromagnetic
HEMP	High-altitude EM Pulse
HF	High Frequency
HPEM	High Power EM
IGBT	Insulated Gate Bipolar Transistor
IP	Internet Protocol
IRA	Impulse Radiating Antenna
ISMS	Information Security Management System

ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
NEBS	Network Equipment Building Systems
PC	Personal Computer
SE	Shield Effect
TCP	Transfer Control Protocol
VSWR	Voltage Standing Wave Ratio

5 Conventions

None.

6 Calculating HPEM threat

6.1 Impulse radiating antenna (IRA) and JOLT

IRA is one example of a method, described in Annex B of [IEC 61000-2-13], of electromagnetic wave radiation with a high-tech level that causes a high-voltage pulse to be generated in a device at the focus of a parabolic reflector.

An image of a parabolic reflector is shown in Figure 1. Annex B of [IEC 61000-2-13] also provides detailed examples of IRA, and examples of the electromagnetic field strengths that are generated. Of the examples provided, the one with the strongest electric field strength is "prototype USA" and Figure 2 shows the relationship between the peak electric field strength and the associated protection distance. In the case of "prototype USA", the parabolic reflector diameter is 3.66 m, so the portability level is evaluated as being PIV (see Table 1 in [ITU-T K.81]). Therefore, the intrusion area on the attack side becomes Zone 0. In the case of Zone 0, the minimum protection distance is taken to be 100 m, so the maximum peak electric field strength is found to be approximately 12.8 kV/m.

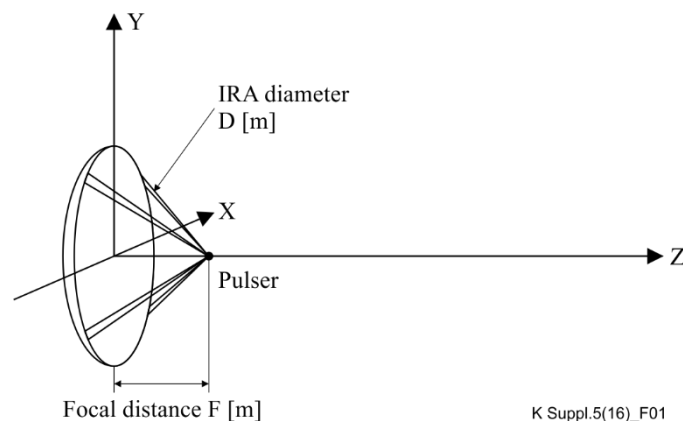


Figure 1 – Image of an IRA

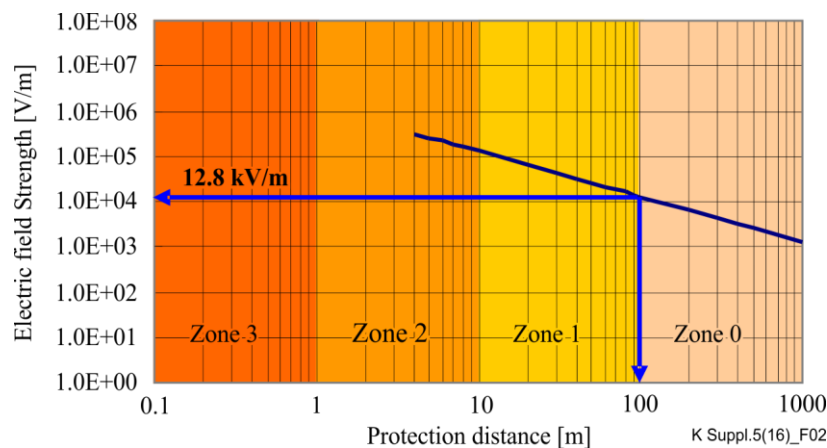


Figure 2 – Relationship between the IRA peak electric field strength and the protection distance (Pulse voltage: 60 kV, parabolic reflector diameter: 3.66 m)

Figure 3 shows the example of measured basic characteristics of IRA. The IRA-3M (Farr Research, Inc.) is used for the measurement. The IRA-3M parabolic reflector is 46 cm in diameter and has a focal length of 23 cm.

Figure 3(a) shows the frequency dependence of the antenna gain. The antenna gain has an almost flat level, at about 22 dBi, from 4 GHz to 15 GHz. Figure 3(b) shows the return loss (S_{11} parameter) and the voltage standing wave ratio (VSWR) characteristics of the same IRA.

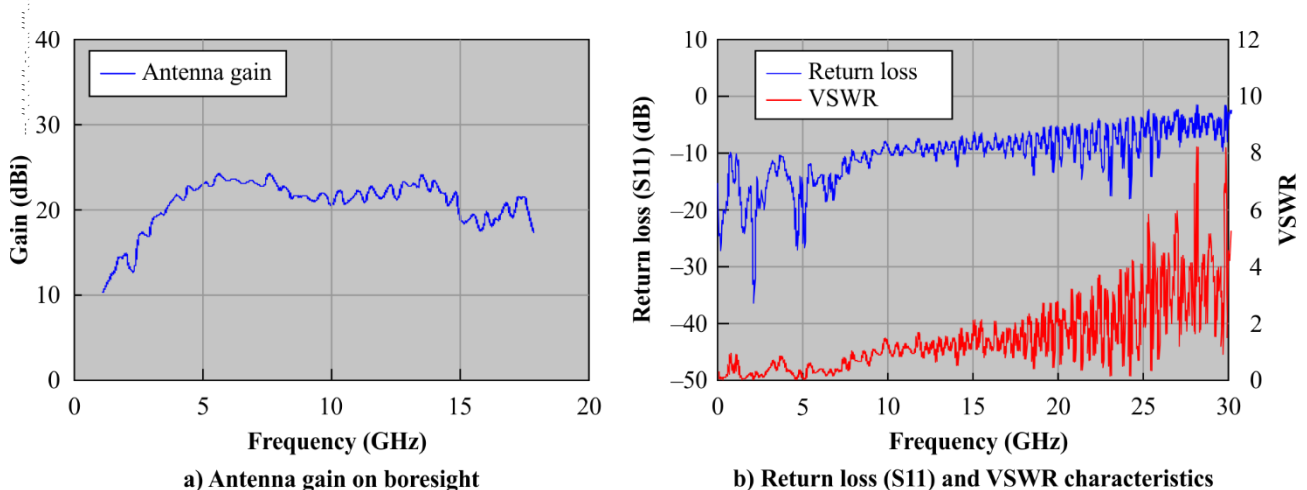
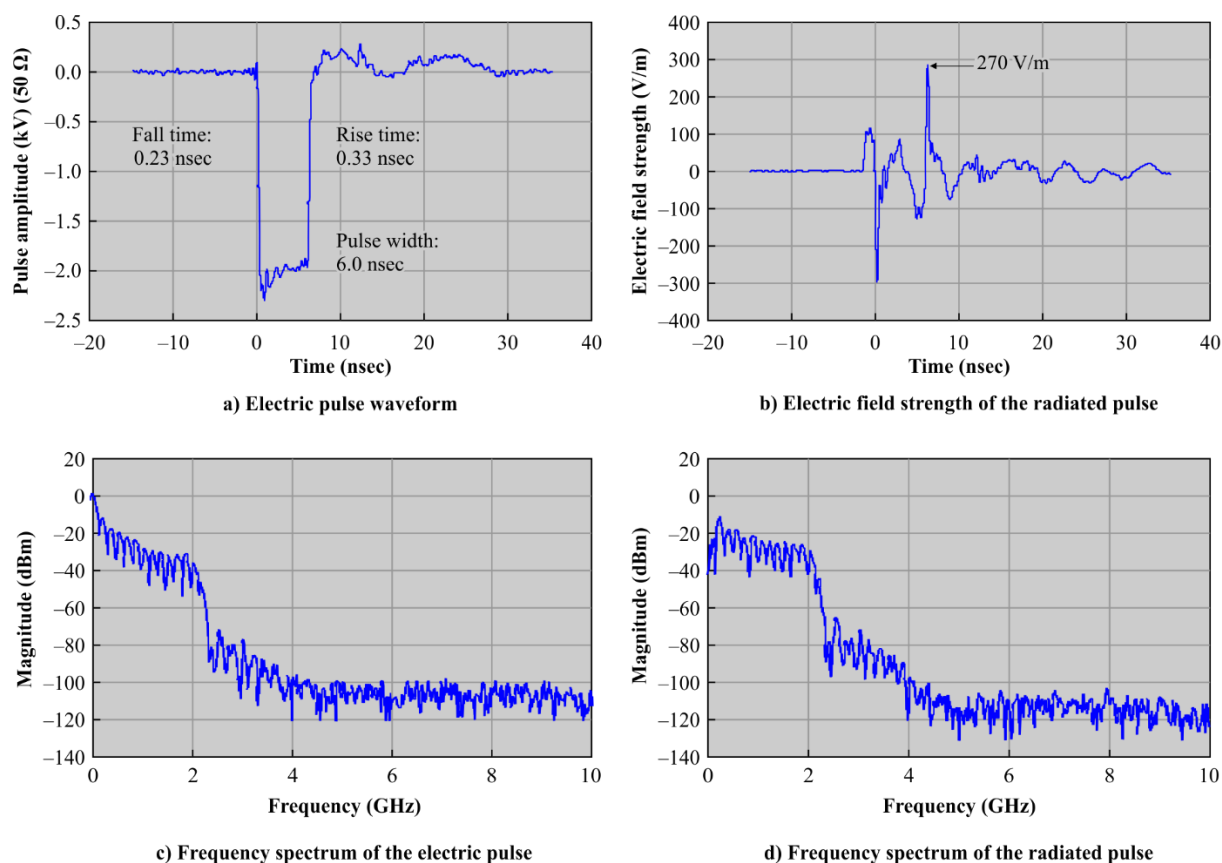


Figure 3 – Basic characteristics of the IRA (Farr Research, Inc.; IRA-3M)

Figure 4 shows an example of performance of the HPEM pulse propagation of the same IRA.

The waveform and frequency spectrum (FFT of the waveform) of the HPEM pulse used in this measurement are shown in Figures 4(a) and 4(c), respectively. The HPEM pulse source (Grant Applied Physics) was used to generate this pulse. The time dependence of electric field strength of the radiated pulse, measured at 3 m away from the IRA on boresight, is shown in Figure 4(b), and its frequency spectrum is shown in Figure 4(d).

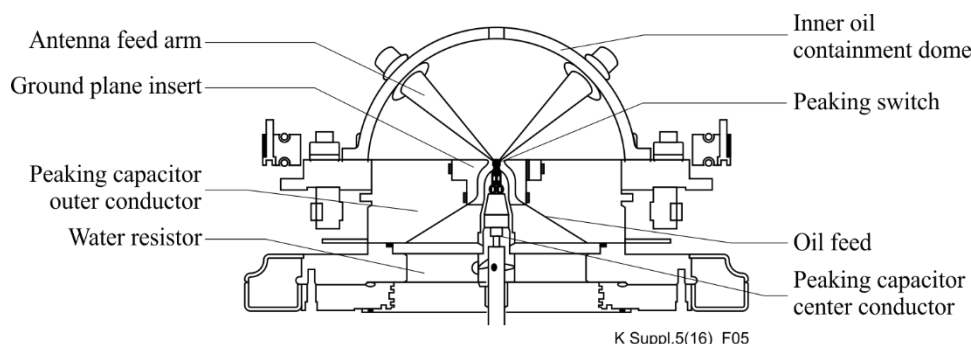
The main frequency spectrum of the HPEM pulse expands to above 2 GHz and the IRA has the potential to radiate almost the whole spectrum range of this pulse (except for the direct current (DC) component). The peak electric field strength was about 270 V/m in this case.



K Suppl.5(16)_F04

Figure 4 – Performance of the high-power electromagnetic pulse propagation of the IRA

The JOLT system is composed of an IRA antenna with a repetitive high impulse generator. Figure 5 shows an overview of the JOLT system. The radiated field has a fairly flat spectrum from about 50 MHz to about 2 GHz. The pulsed power system is centred on a very compact resonant transformer capable of generating over 1 MV at a pulse-repetition frequency of ~ 600 Hz. This is switched, via an integrated transfer capacitor and an oil peaking switch onto an 85-ohm half-impulse radiating antenna. This unique system will deliver a far radiated field with a full-width at half-maximum on the order of 100 ps, and a field-range product (rE_{far}) of ~ 5.3 MV, exceeding all previously reported results.



K Suppl.5(16)_F05

Figure 5 – Overview of the JOLT system

The dependence between far-field electric field strength and the distance r is derived from Equation (1). The far-field distance r is derived from Equation (2).