Protecting Telecommunication Devices against High Power Electromagnetic Effects: The Work of ITU-T SG5 Q15

T. Tominaga[#1], D. J. Carpenter[%2], H. Sekiguchi[*3], S. Seto[*4], Y, Suzuki[#5], M. Hattori[+6]

[#]*NTT Corporation*
Musashino-shi, 180–8585 Tokyo, Japan
[1]tominaga.tetsuya@lab.ntt.co.jp
[5]suzuki.yasunao@lab.ntt.co.jp

[%]*BT Design*
Martlesham Heath, IP5 3RE, United Kingdom
[2] darren.carpenter@bt.com

[*]*National Institute of Information and Communications Technology*
Koganei-shi, 184–8795 Tokyo, Japan
[3]hide@nict.go.jp
[4]setos@nict.go.jp

[+]*NTT Advanced Technology Corporation*
Musashino-shi, 180–8585 Tokyo, Japan
[6] mitsuo.hattori@ntt-at.co.jp

Abstract— **This paper introduces the draft Recommendation of the ITU-T SG5 related to the protection of existing electronic devices in telecommunications and data centre against HPEM attack. The paper explain the security threat due to the HPEM effects, the vulnerability of the electronic device and the mitigation calculation method, using some examples.**

Key words: Information Security, Intentional Electromagnetic Interference (IEMI), High Power Electromagnetic (HPEM), Telecommunications and Data Centre.

I. Introduction

The rapid adoption of services based upon the Internet Protocol (IP) has transformed many aspects of everyday life: we are all now used to using the internet to search for and purchase flights, hotels and rental cars; to shop for almost everything from DVDs to groceries; to organise our personal finances and investments; and to do many other things. Access to these services has become an essential tool to our lives. The disruption of these services would therefore have a serious impact on all aspects of our society.

The information security community is concerned about the possibility of disruption to telecommunications caused by an Intentional Electro-Magnetic Interference (IEMI), because it is well known that electronic devices malfunction and breakdown in the High Power Electro-Magnetic (HPEM) environment. General information security specifications exist as the well-known ISO/IEC 2700 [1] and ISO/IEC 27002 [2] published by the International Electrotechnical Commission (IEC) as the Information Security Management System (ISMS). The ISMS is a systematic approach for organizations to manage their sensitive information, and requires the assessment of the security risk and the selection of appropriate controls and protections. The ISO/IEC 27002 also mentions the protection of equipment from strong electromagnetic fields.

The IEC Technical Committee (TC) 77 Sub-committee (SC) 77C has gone furthest in standardization related to the security for electronic devices due to HPEM [3, 4]. Currently, several documents on HPEM have been published; including an overview, specification of the HPEM environment and measurement methodology [5 - 7].

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) has also published the X.1051 as the ISMS in the field of telecommunication [8]. The ITU-T Study Group (SG) 5 has also started work during the 2005 – 2008 Study Period on the preparation of Recommendation designed to protect the telecommunications and data centre from disruption due to HPEM effects [9, 10]. In this paper, we present an overview of this Recommendation and present a lot of examples of the security threats, the vulnerability of the electronic devices and the mitigation calculation method (as described for the non-technical/non-expert reader).

II. Classifications of Threat Due to the HPEM

We have first needed assessing the security threat due to the HPEM for the electronic devices in the telecommunications and data centre. The threat level (strength) should be adequately estimated. In the Recommendation of ITU-T SG5, the threat level has been estimated from consideration of three concepts: the Portability Level, the Intrusion Area and the Availability of the HPEM device.

A. Portability of the HPEM device

HPEM devices exist in many sizes. As examples, a stun-gun is one of the smallest HPEM devices, whereas a weather radar system is one of the largest. Since the device size is relevant to the accessible distance to the target, the concept of portability is a very important factor to estimate the threat. The portability levels are classified into four categories as shown in Table I.

TABLE I
Examples of Portability Levels

Portability Level	Size
PI	Pocket–in or body-worn size
PII	Briefcase size
PIII	Vehicle-size
PIV	Trailer-size

Thus, the threat can be estimated according to portability as follows. As an example, if everyone is shaken down whenever entering the target room, the PI level is then outside the range of the estimation of the threat. As another example, if everyone is checked the hand baggage whenever entering the building, the PI and PII levels are then outside the range of the estimation of the threat.

B. Intrusion Area of the HPEM device

The minimum separation distance between the target and the HPEM device is generally determined by the Portability Level. Fig. 1 shows the concept of the Intrusion Area of the HPEM device getting close to the target. The Intrusion Area is classified into four categories. The Zone 0, 1, 2 are the outside of the target site, building, and room respectively, in where the inside are controlled by monitoring and patrolling. The Zone 3 is the inside of the target room. The distances noted in Fig. 1 for each Zone are presented as examples. The separation distance is used in the calculation of the electromagnetic field strength of the threat. Table II shows the close relation between the Portability Level and the Zone.

C. Availability Levels of the HPEM

The Availability Level of the HPEM device is divided into four categories as shown in Table III. A HPEM device produced by the individual is assumed as the level of the AI or the AII. A HPEM device by an organization is assumed as the level from the AI to AIV. As an example, the AI level applies to the stun gun or illegal Citizens' Band (CB) radio that are generally available in the marketplace. The AII level applies to deliberately modified amateur radio devices. The AIII level applies to combination devices assembled expertly from commercially available generators, antennas, amplifiers etc.. The AIV level applies to devices developed for military purposes and are significantly more potent than the AIII level. In addition, the Availability Level is also thought to depend on the technical capability and the cost of the HPEM device itself. In the Annex A of IEC 61000-2-13, the technical capability has been classified into 'High-tech', 'Mid-tech' and the like.

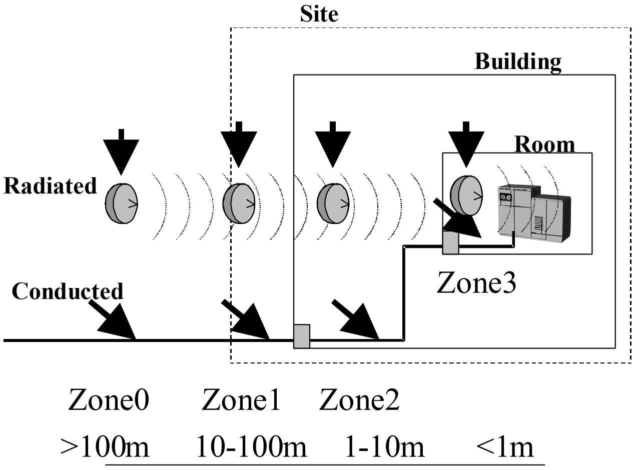

Fig. 1 Concept of the intrusion area

TABLE II
Examples for the Availability Levels

Intrusion area	Portability level	
Zone 0	Public space	The threat is located within the Public Space located outside the Site of the equipment to be protected, where people are free to move without restriction. So, threats of portability levels PI, PII, PIII & PIV can be located here.
Zone 1	Site	The threat is located within the same Site as the equipment to be protected and hence has passed through the physical Site Security. So, threats of portability levels PIII & PIV can be located here. The existence of PI & PII depends upon physical security protocols applied to visitors to the site (e.g. the surrender of portable electronic devices at the Site entrance)..
Zone 2	Building	The threat is located within the same building as the equipment to be protected and hence has passed through both the Site and any Building Physical Security. So, threats of Portability Levels PIII & PIV cannot be located here; only threats of Portability Level I and II can be taken into the building.
Zone 3	Room	The threat is located within the same room as the telecoms equipment to be protected. So, threats of Portability Levels PIII & PIV cannot be located here; only threats of Portability Level I and II can be taken into the building.

TABLE III
EXAMPLES FOR THE AVAILABILITY LEVELS

Availability level	Definition
AI	Low class device (Consumer)
AII	Middle-class device (Hobbyist)
AIII	High class device (Professionals)
AIV	Very high class device (Other custom build)

D. *Examples of the threat due to the HPEM*

Some estimation examples of the security threat due to the HPEM devices are shown in Table IV. The electromagnetic field strength is found to be considerably larger than general immunity levels.

TABLE IV
ESTIMATION EXAMPLES OF THE THREAT DUE TO HPEM DEVICES

Example of the HPEM device	Intrusion area	Field strength	Frequency Range	Portability
Commercial radar	Zone 0	20 kV/m @300m	1GHz-10GHz (1.285GHz)	PIV
Magnetron generator	Zone 1	475 V/m @10 m	1GHz-3GHz	PIII
Illegal CB radio	Zone2	573 V/m @10 m	27MHz	PII
Amateur wireless device	Zone 3	169 V/m @10 cm	100MHz-3GHz	PI

III. VULNERABILITY OF TELECOMMUNICATION DEVICES

The vulnerability of electronic devices in telecommunications and data centre (telecommunication devices) needs to consider the immunity and over-voltage levels. At the present moment, the immunity and the over-voltage level is specified by the standards shown in Tables V and VI. Thus, the vulnerability levels are different for each of the standards.

As an example, the typical immunity level for router servers shows in Table VII and is the same as that of the 2004 version of ITU-T K.48.

TABLE V
EXAMPLE FOR IMMUNITY STANDARDSAND VULNERABILITY LEVEL

Vulnerability Level	Standard Name	Target Device	Remarks
ZI1	CISPR24	IT equipment	International standards
ZI1	EN55024	IT equipment	European standards
ZI2	ITU-T K.48	Network equipment	Recommendations
ZI1	ITU-T K.43	Network equipment	Recommendations
ZI1	NTT-TR 549001	Network equipment	NTT
ZI1	NEBS GR 1089	Network equipment	US standards
ZI3	NEBS LEVEL 3	Network equipment	US standards

TABLE VI
EXAMPLE FOR OVER-VOLTAGE STANDARDS AND VULNERABILITY LIEVELS

Vulnerability Level	Standard Name	Target Device	Remarks
ZK1	ITU-T K.20	Network equipment	Recommendations
ZK2	ITU-T K.21	Terminal	Recommendations
ZK3	ITU-T K.66 Appendix IV	Communication device, network equipment	Recommendations
ZK4	NEBS GR 1089	Network equipment	US standards
ZK5	NEBS LEBEL 3	Network equipment	US standards

TABLE VII
IMMUNITY AND OVER-VOLTAGE LEVEL OF THE 2004 VERSION OF ITU-T K.48

Item	Immunity Level
Radiated electromagnetic field	3 V/m(actual field value) *)
Conducted voltage	3 V(actual voltage value) *)
Static discharge	8 kV(direct discharge)
Lightning surge	4 kV(power port - line to ground) 2kV(communications port - line to ground)

IV. MITIGATION CALCULATION METHOD

The mitigation level that can protect telecommunication devices from the HPEM threat is calculated from the following equation:

EM mitigation Level = Threat level – Vulnerability level

The Shield Effect (SE) is calculated in dB by the following equation:

SE = 20 x Log10 (Threat level / Vulnerability level)

As examples, the mitigation levels of general IT devices against the HPEM devices in Table III are shown in Table VIII. Note that the vulnerability of the IT device is assumed as the immunity level of 3 V/m.

TABLE VIII
CALCULATION EXAMPLES OF THE REQUIRED MITIGATION LEVEL OF GENERAL IT DEVICES AGAINST THE HPEM DEVICES

Example of the HPEM device	Threat level (V/m)	Vulnerability level (V/m)	Required Shield Effect (dB)
Commercial radar	20,000 @300 m	3	76
Magnetron generator	475 @10 m	3	44
Illegal CB radio	573 @10 m	3	46
Amateur wireless device	169 @0.1 m	3	35

V. Conclusion

In this paper, the draft ITU-T SG5 Recommendation related to security issues for electronic devices in the telecommunications and data centre arising from the HPEM has been introduced. The draft Recommendation estimates the security threat (strength) from consideration of the three concepts of the Portability Level, the Intrusion Area, and the Availability Level of the HPEM device. The security threat is considered from a lot of HPEM devices. The protection needs to consider the vulnerabilities of the immunity and over-voltage levels of these electronic devices. The mitigation level can be calculated from the security threat level due to the HPEM devices and the vulnerability level of the electronic devices. Although this paper presented a few examples of the security issues regarding HPEM, the draft Recommendation will describe many examples to the non-technical/non-expert reader. Note that the security threat level and the vulnerability level in this paper are estimated from technical levels investigated during March 2004. It is necessary to perform such investigation periodically based on the newest trends of the surrounding technology and the state of the society, because the threat and vulnerability turn up generation after generation.

Acknowledgments

This research was partially supported by a Strategic Information and Communications R&D Promotion Programme (SCOPE) (073103006, 2007) from the Ministry of Internal Affairs and Communications, Japan.

References

[1] "ISO/IEC 27001: Information Security Management Systems - Requirements," International Organization for Standardization and INTERNATIONAL ELECTROTECHNICAL COMMISSION (ISO/IEC), Geneva, Switzerland, 2005.

[2] "ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management," International Organization for Standardization and INTERNATIONAL ELECTROTECHNICAL COMMISSION (ISO/IEC), Geneva, Switzerland, 2005.

[3] W. A. Radasky and C. E. Baum and M. W. Wik, "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)," IEEE_J_EMC, vol. 46, 2004, pp. 314--321.

[4] W. A. Radasky, "New Developments in the Protection Against Intentional Electromagnetic Interference (IEMI) Sice AMEREM 2006," in Proc. of EUROEM 2008 European Electromagnetics, Lausanne, Switzerland, July 2008, p. 27.

[5] "IEC/TR 61000-1-5: Electromagnetic compatibility (EMC) - Part 1-5: High power electromagnetic (HPEM) effects on civil systems," INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), Geneva, Switzerland, 2004.

[6] "IEC 61000-2-13: Electromagnetic compatibility (EMC) - Part 2-13: High-power electromagnetic (HPEM) environments - radiated and conducted," INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), Geneva, Switzerland, 2005.

[7] "IEC 61000-4-33: Electromagnetic compatibility (EMC) - Part 4-33: Testing and measurement techniques - Measurement methods for high power transient parameters," INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC), Geneva, Switzerland, 2005.

[8] "X.1051: Information Security Management System - Requirements for Telecommunications (ISMS-T)," International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), Geneva, Switzerland, 2004.

[9] D.J. Carpenter, H. Sekiguchi, T. Tominaga, "Protecting Telecommunications and Data Centres from Electromagnetic Attack: The Work of ITU-T SG5 Q15," in Proc. of EUROEM 2008 European Electromagnetics, Lausanne, Switzerland, July 2008, p. 88.

[10] "Draft text of Recommendation K.hpem: Application of requirements against HPEM to telecommunication systems," International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), Geneva, Switzerland, 2008.

[11] "EMR Security Guidelines," Information Security Technology Study Group, Oct. 2004, http: //www.j-netcom.co.jp/ist/ist-glv3.pdf (in Japanese).