



**Workshop on Cryptographic Hardware and Embedded Systems 2011**  
**Nara, Japan**  
**Wednesday September 28<sup>th</sup> - Saturday October 1<sup>st</sup>**

# **Standardization Works for Security regarding the Electromagnetic Environment**

**Tetsuya Tominaga**

**NTT Energy and Environment Systems labs.**

- Why Electromagnetic Security have to be considered?
  - My experience and motivation (Electromagnetic Compatibility troubles)
- What is TEMPEST ? (EMSEC: Electromagnetic emanation security)
  - Mechanism, Example of Mitigation, and ITU-T Recommendation K.84
- Why the Electromagnetic Security standards needs?
  - Security management, Related standards, ITU-T Recommendation K.78, K.81, K.87
- Future work
- Conclusion

- Increasing to use of ICT for controlling such as Smart Grid, Smart community and so on.
- We have to keep safety and secure communication.
- The exact knowledge is required for adequate countermeasure or mitigation
- The exact knowledge; Definition of Threat, Mechanism, Evaluation Method, Mitigation Methods.
- We are welcome to your contributions.

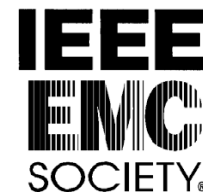
***Study Group 5  
Question 15***



***Technical Committee 77  
Sub Committee 77C***



***Technical Committee 5  
Sub Committee 2***



# **Why Electromagnetic Security have to be considered?**

My experience and motivation  
(Electromagnetic Compatibility troubles)

# My experience <Case Study 1>

- When I was field engineer in NTT (East) Technical Assistance and Support Center EMC group
- I met many Electromagnetic Compatibility troubles.
- And I have to solve the troubles

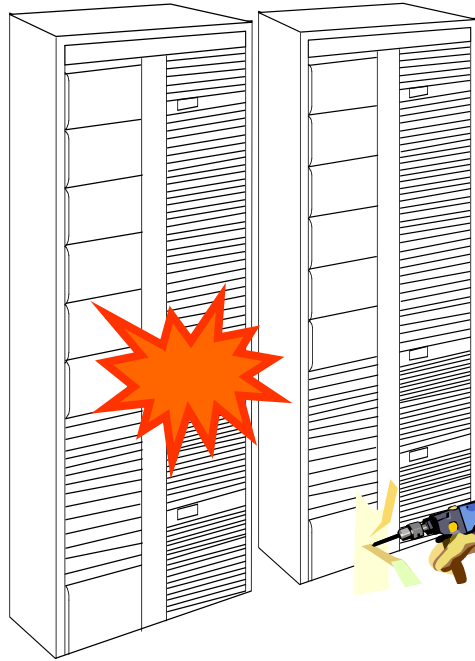
Over 10 years ago, One worker called by mobile phone

10 V/m @ 10 cm

Transmitting system had an EMC trouble

Prohibit the use of mobile phone in telecom equipment room





Over 10 years ago, One worker drilled the floor in order to install a telecom equipment,



Electro Static Discharge due to dust explosion  
20 kV

The telecom equipment had an EMC trouble

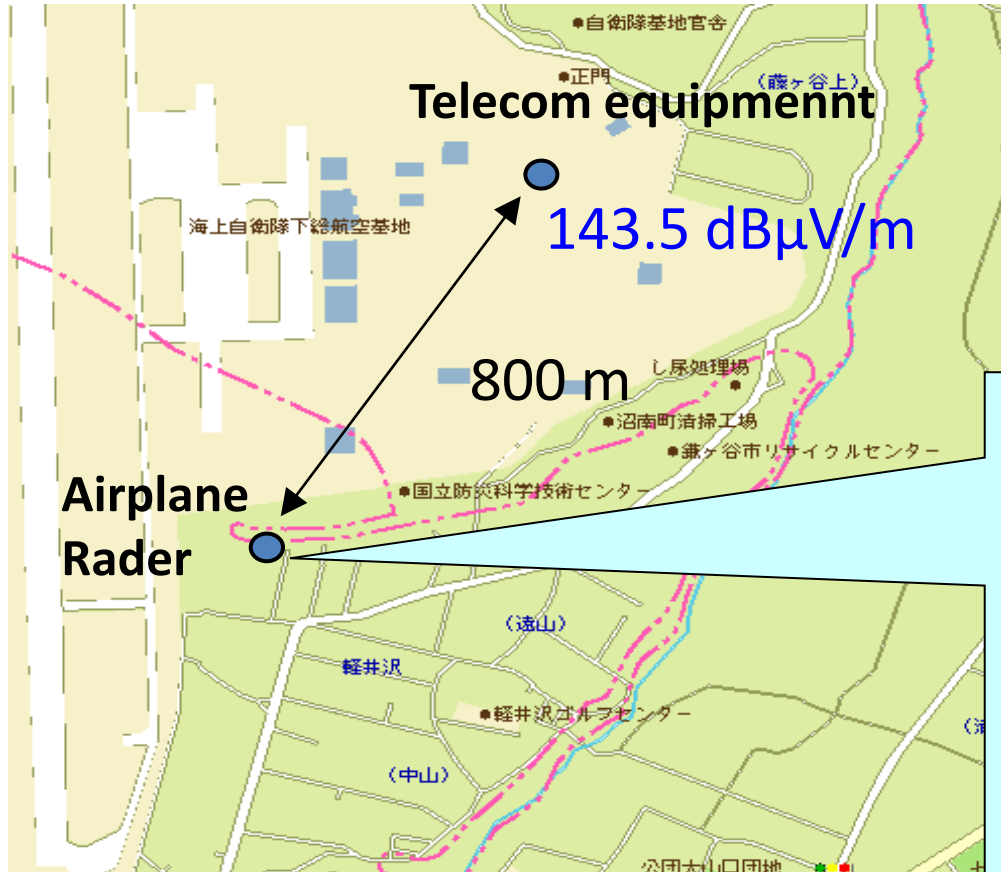
and he cleaned the drilled powder by vacuum cleaner.

# My experience <Case Study 3>

Over 10 years ago, The telecom equipment was installed near by Airplane Searching Rader.

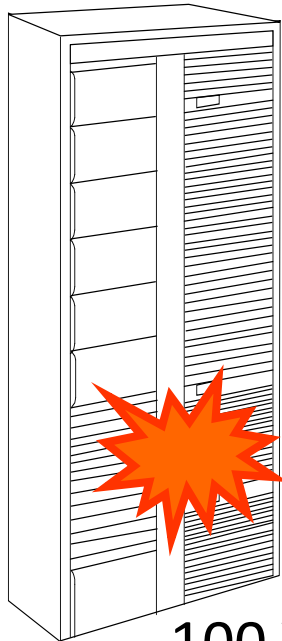
The Rader affected the telecom equipment

Shield Enclosure is required  
The level:  
20dB@1GHz~3GHz

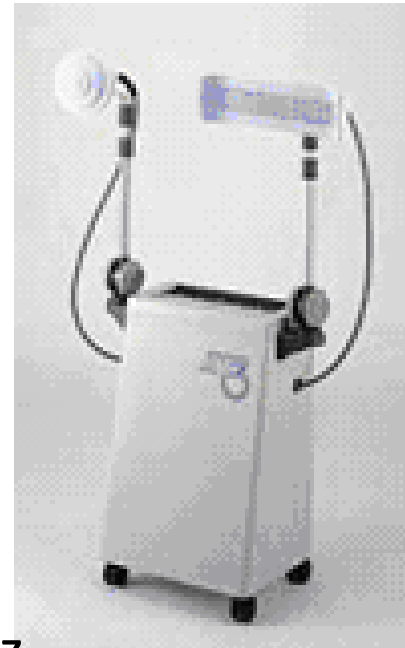
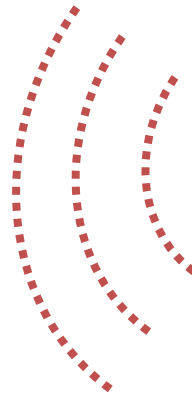


Over 10 years ago, The telecom equipment was occurred trouble  
The equipment was installed in Pain Clinic

Telecom equipment



Microwave therapeutic apparatus



100 V/m @ 2.45 GHz

IC which has caused the error was shielded with thin aluminum film.



- If someone does these kind of EMC intentionally,
- I am afraid..
- When the customer request the high security,
- We have to asses these kind of EMC

IEMI: Intentional Electromagnetic Interference

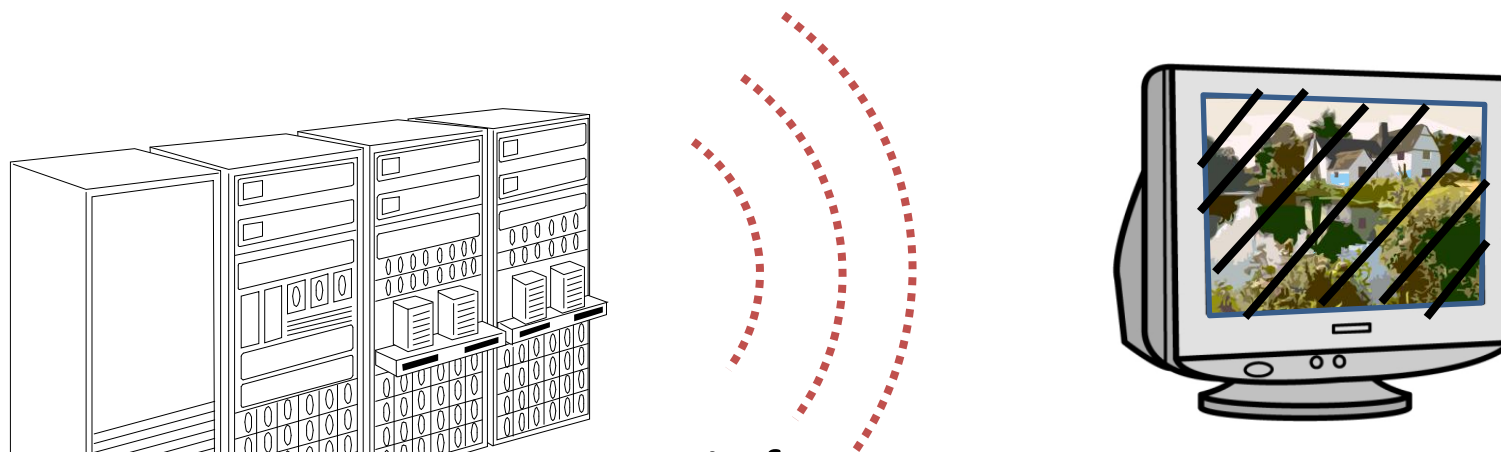
HPEM: High Power Electromagnetic

## How to do the assessment?

Immunity levels of telecom equipment is required 1 V/m in existing telecom standard  
Shielding Level (Mitigation Level, Methods), Evaluation methods

# My experience <Case Study 5>

Over 10 years ago, One new telecom equipment was installed,  
The complaint came from neighboring residents that it became impossible to watch television.



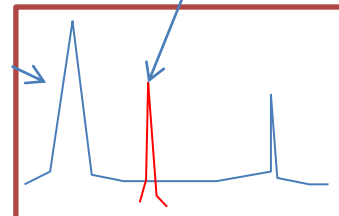
Harmonic frequency

$$32 \times 6 = 192$$

Clock Freq. :32 MHz



TV signal  
50 dBuV/m



192 MHz  
30 dBuV/m

Shield Enclosure  
was required

The level:  
20dB @ TV band

Band width 6 MHz

# My experience <Case Study 6>

One day, our customer asked the question.

“Our server room is secure about TEMPEST ?”

Another customer asked,

“Our machine is secure about TEMPEST?”

The other customer asked,

“Our meeting room is secure about TEMPEST?”



K.84: Test methods and guide against information leaks through unintentional EM emissions

- I know every emissions are due to electric signal which is used in electric circuit boards and cables.
- I had to answer the questions.
- What is TEMPEST ?

# What is TEMPEST

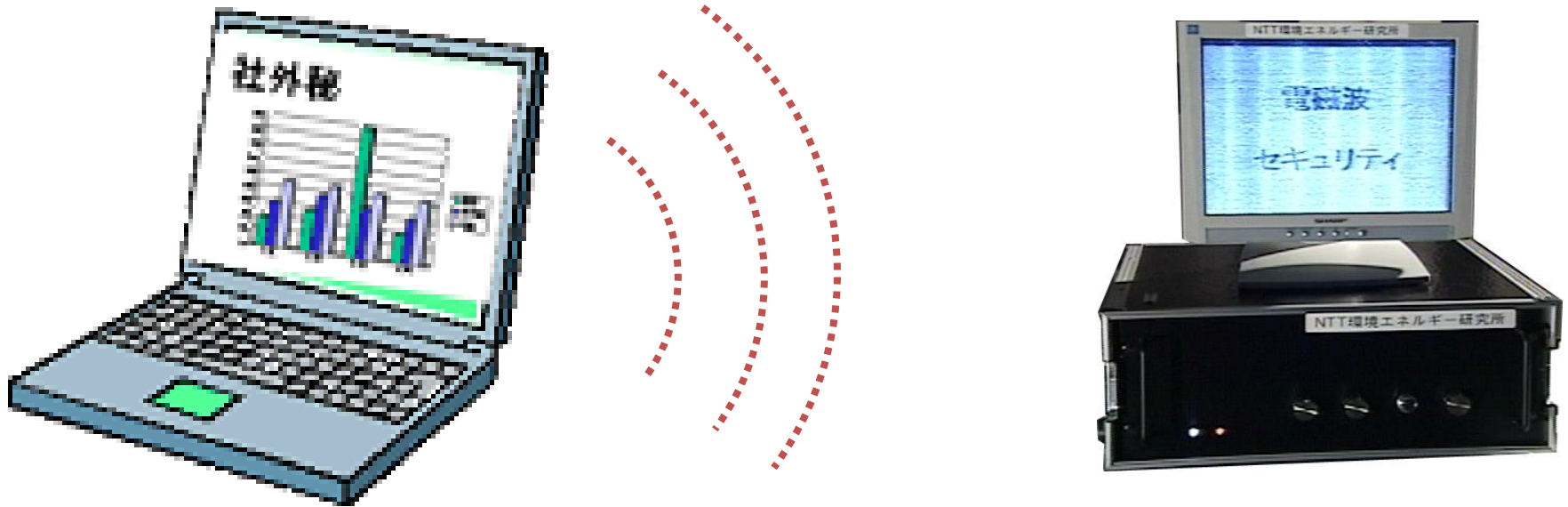
Mechanism, Example of Mitigation, and  
ITU-T Recommendation K.84

**TEMPEST** [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.

## Definition in K.84

**electromagnetic emanations security (EMSEC):** Physical constraints to prevent information compromised through signals emanated by a system, particularly by the application of TEMPEST technology to block electromagnetic radiation. In this Recommendation, term of EMSEC is used only for information leakage due to unintentional electromagnetic emission.

- The display image leaks from the unexpected emission.



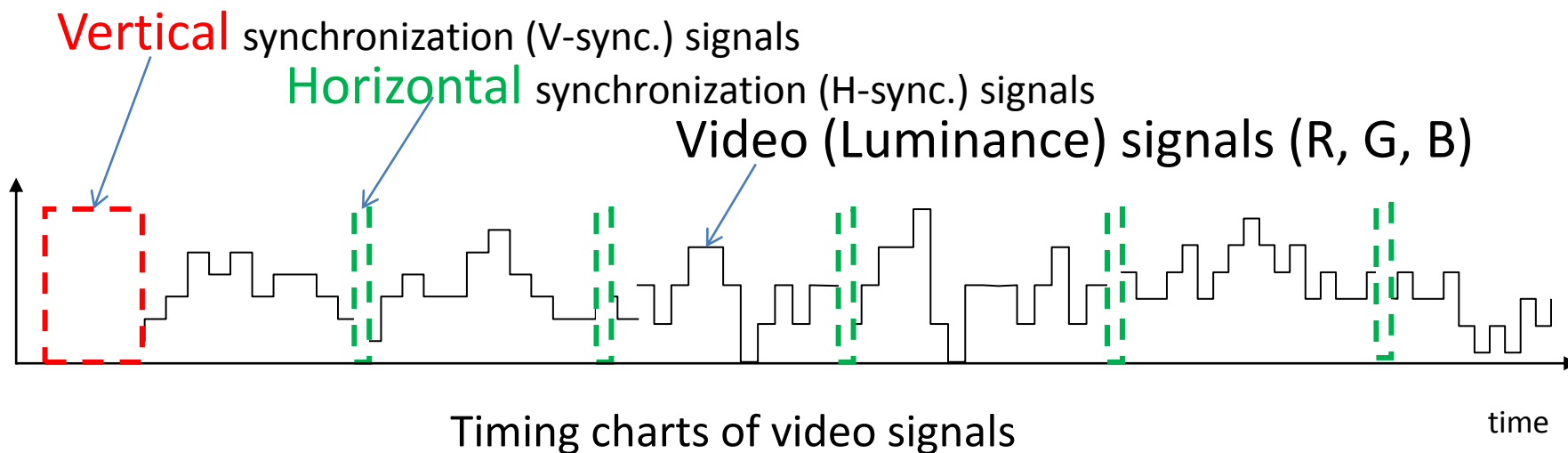
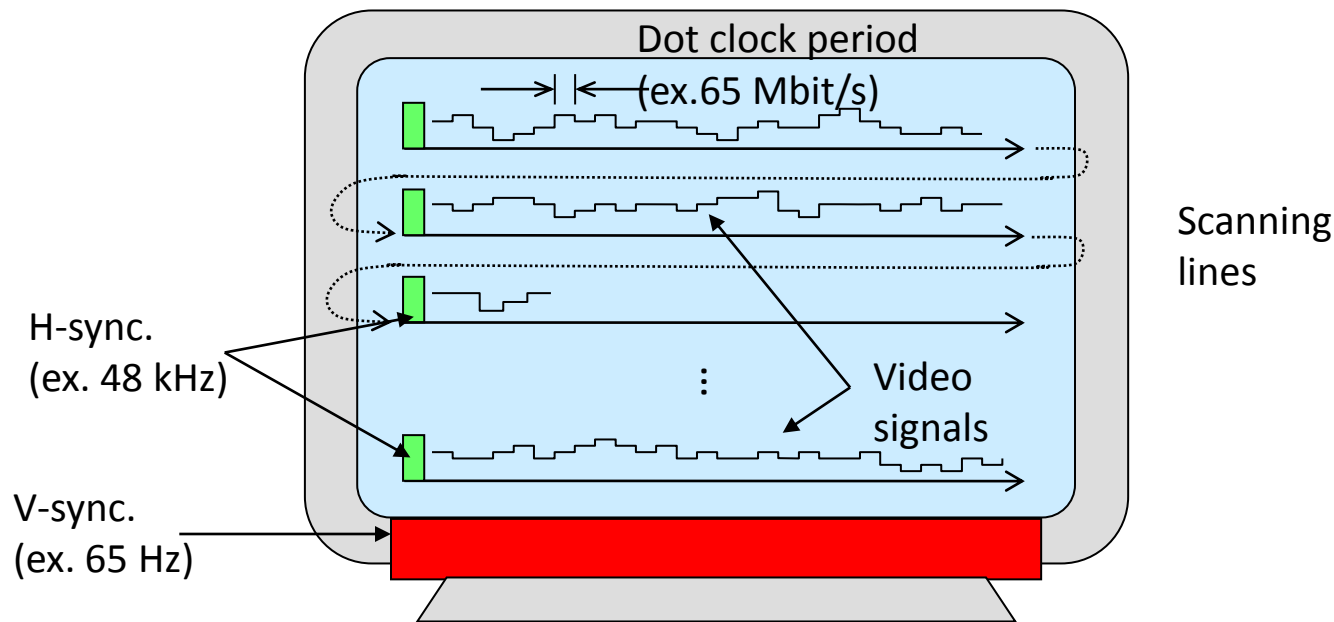
I have to investigate ...

- The mechanism of EMSEC
- The threat of EMSEC
- Possible distance of EMSEC and so on..

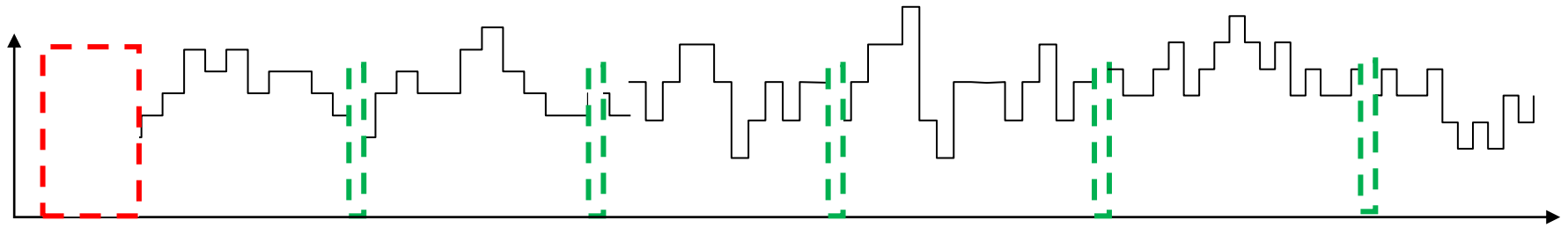
➤ Movie



# Raster scan video signal (Mechanism)

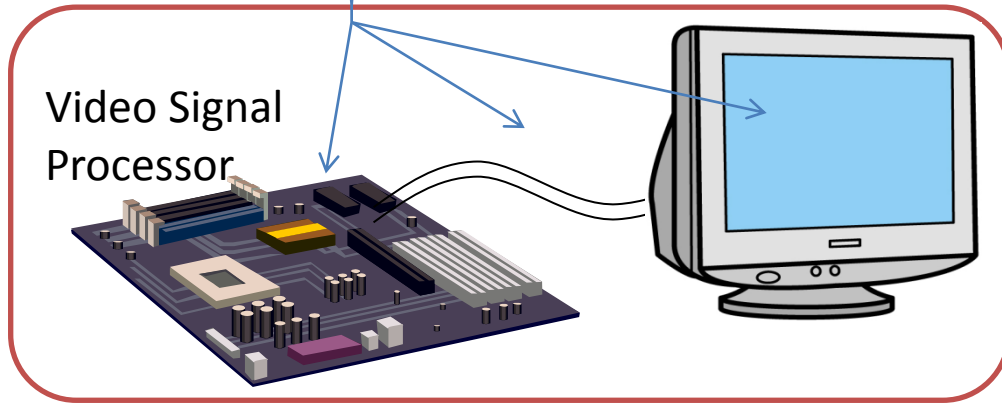


# Raster scan video signal and Emission

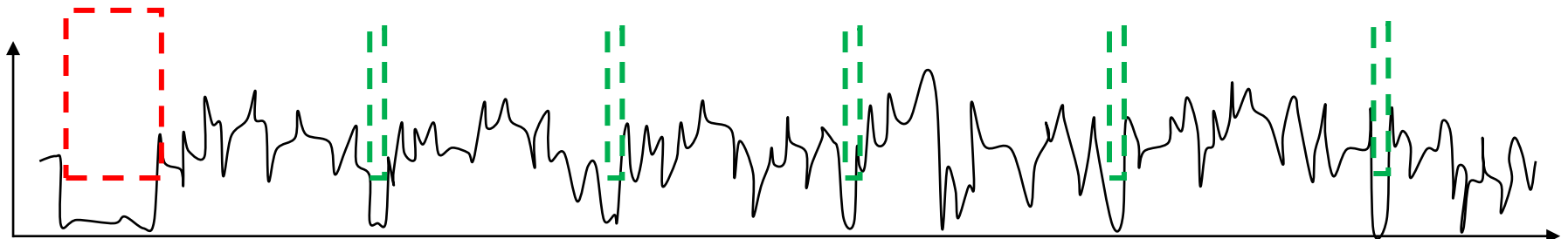
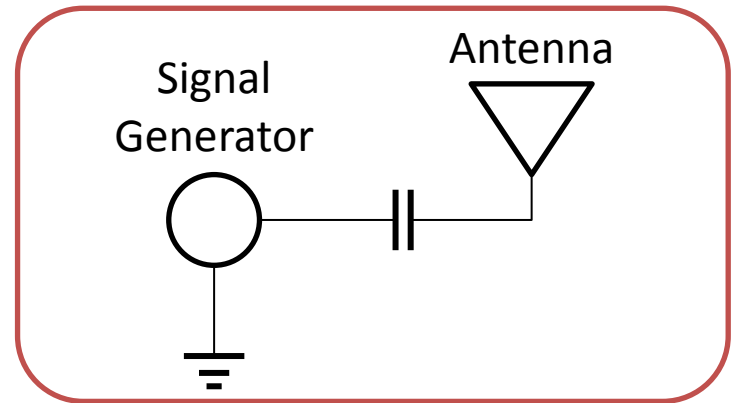


Timing charts of video signals

time

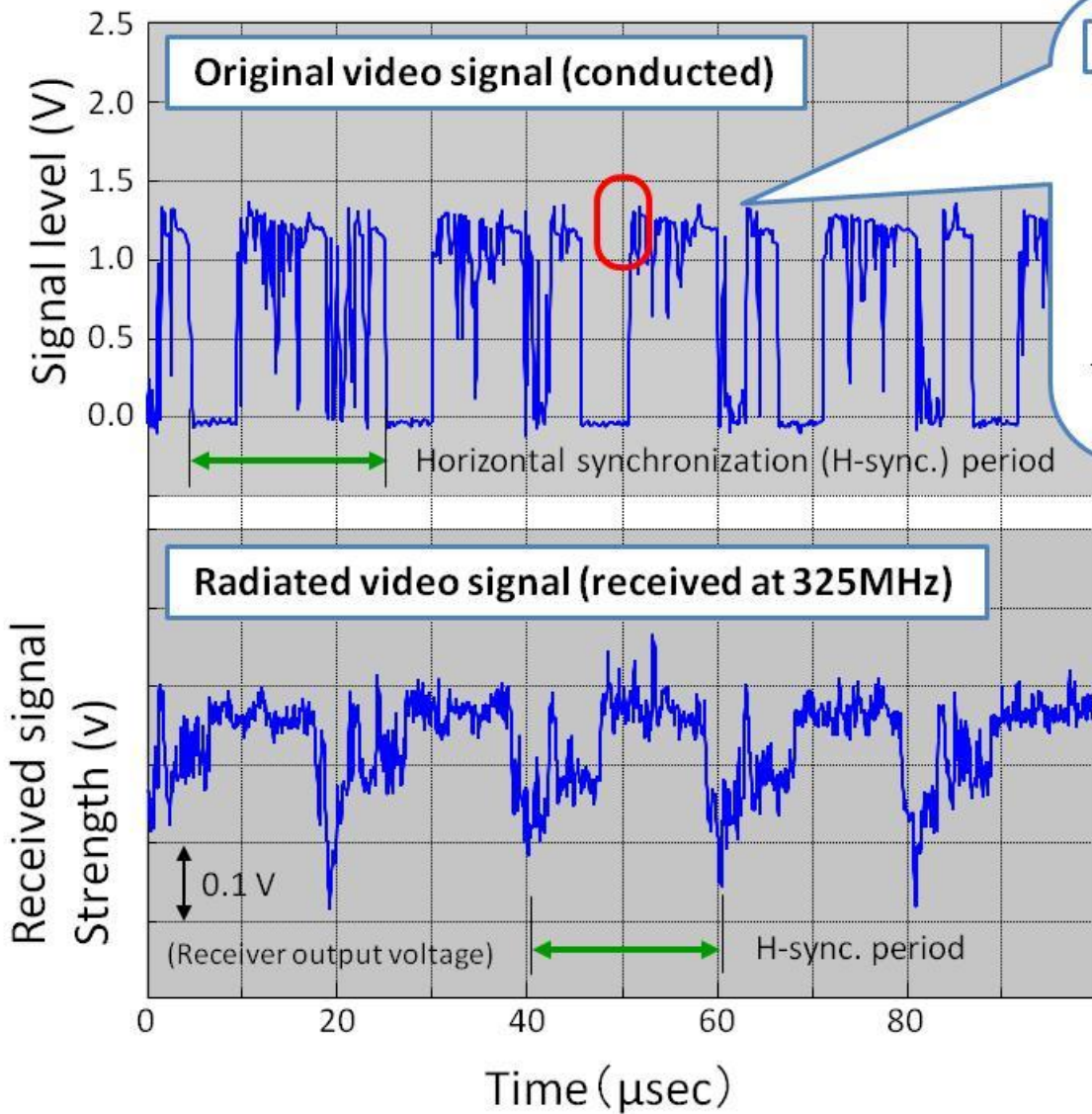


=

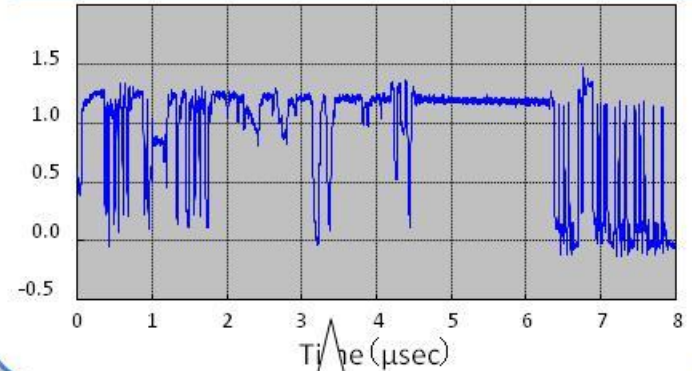



Emitted radio wave

# Video signals and Leaked Radio Waves

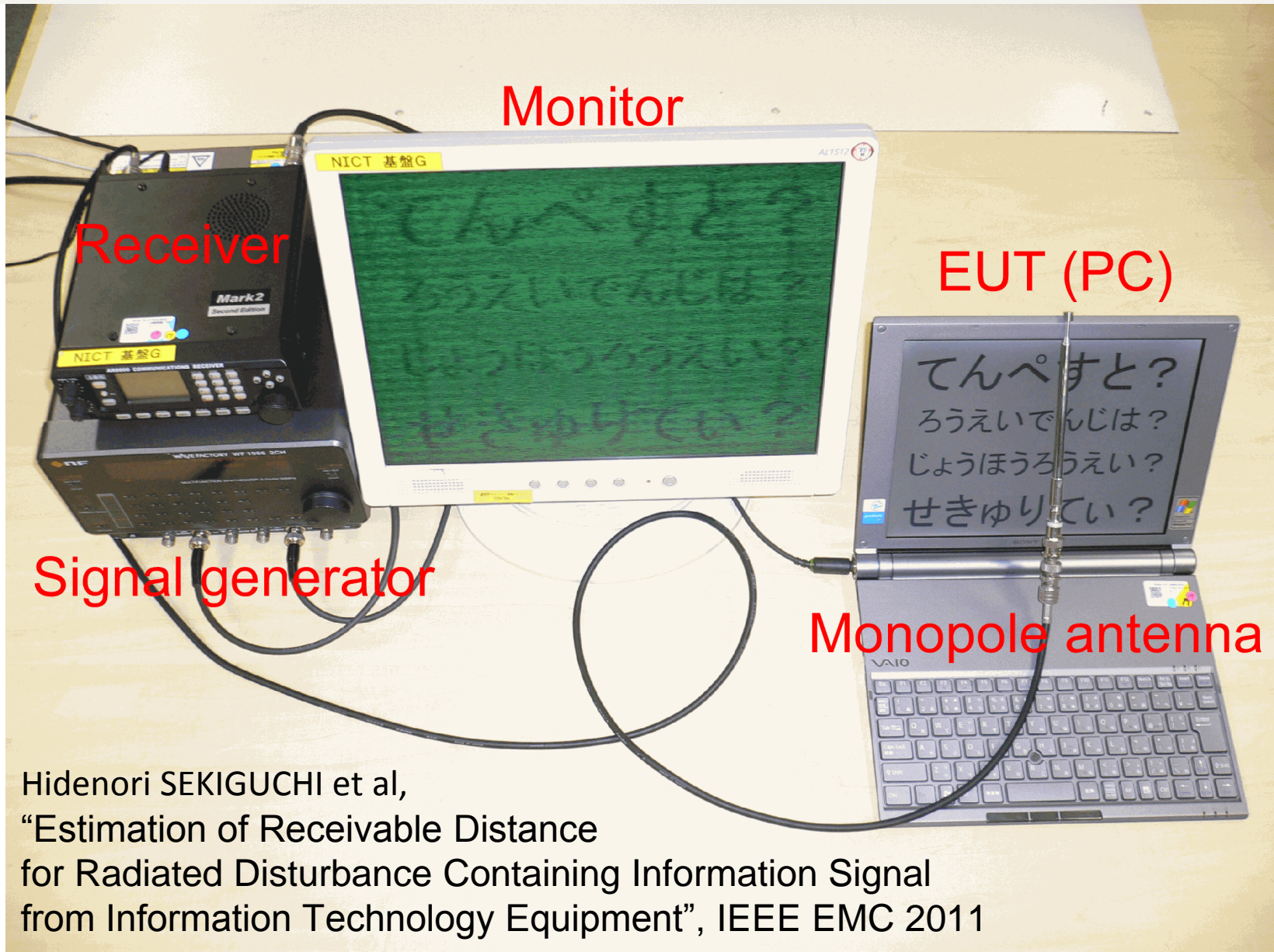


Video signal that draws a scanning line



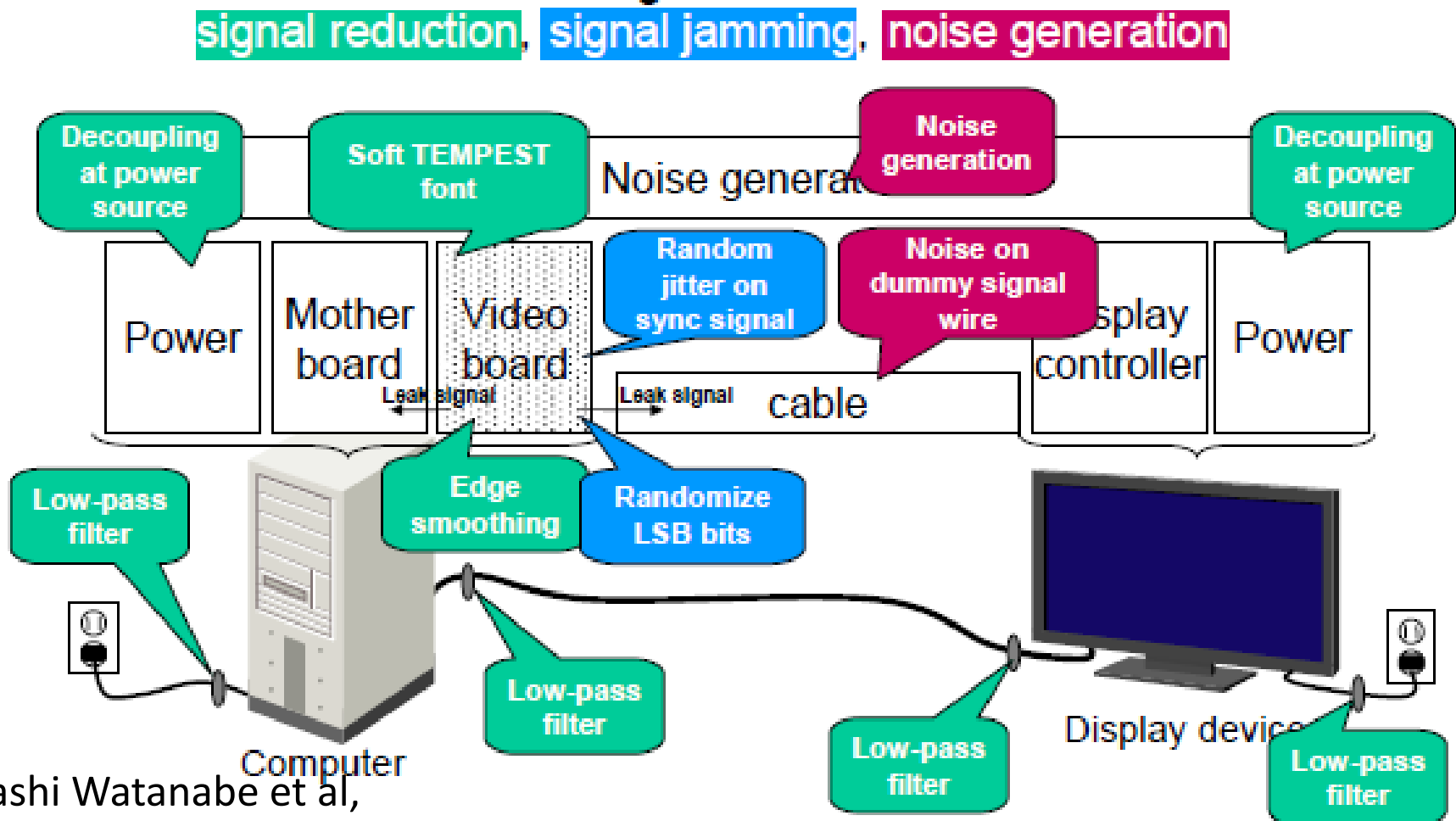
 **Dot (pixel) clock pulse**  
(65 Mbit/s in this case)

# Can you buy in Akihabara? Yes you can.



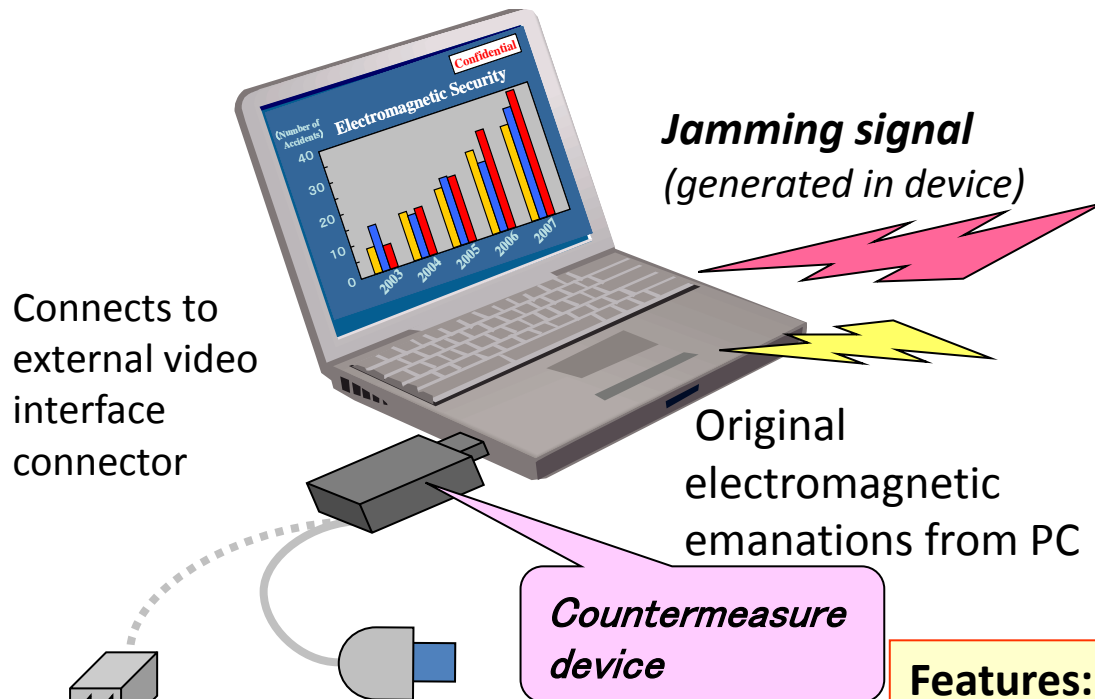
# Mitigation methods for EMSEC

For preventing information leakage, countermeasures are categorized into :

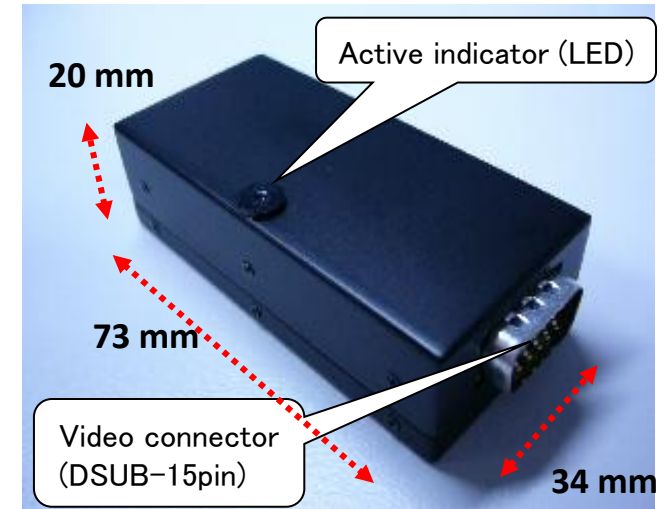


Takashi Watanabe et al,  
“Towards large-scale EM information  
leakage evaluation by means of automated TOE\* synchronization”, IEEE EMC 2011

# Example of countermeasure device



How to use the device

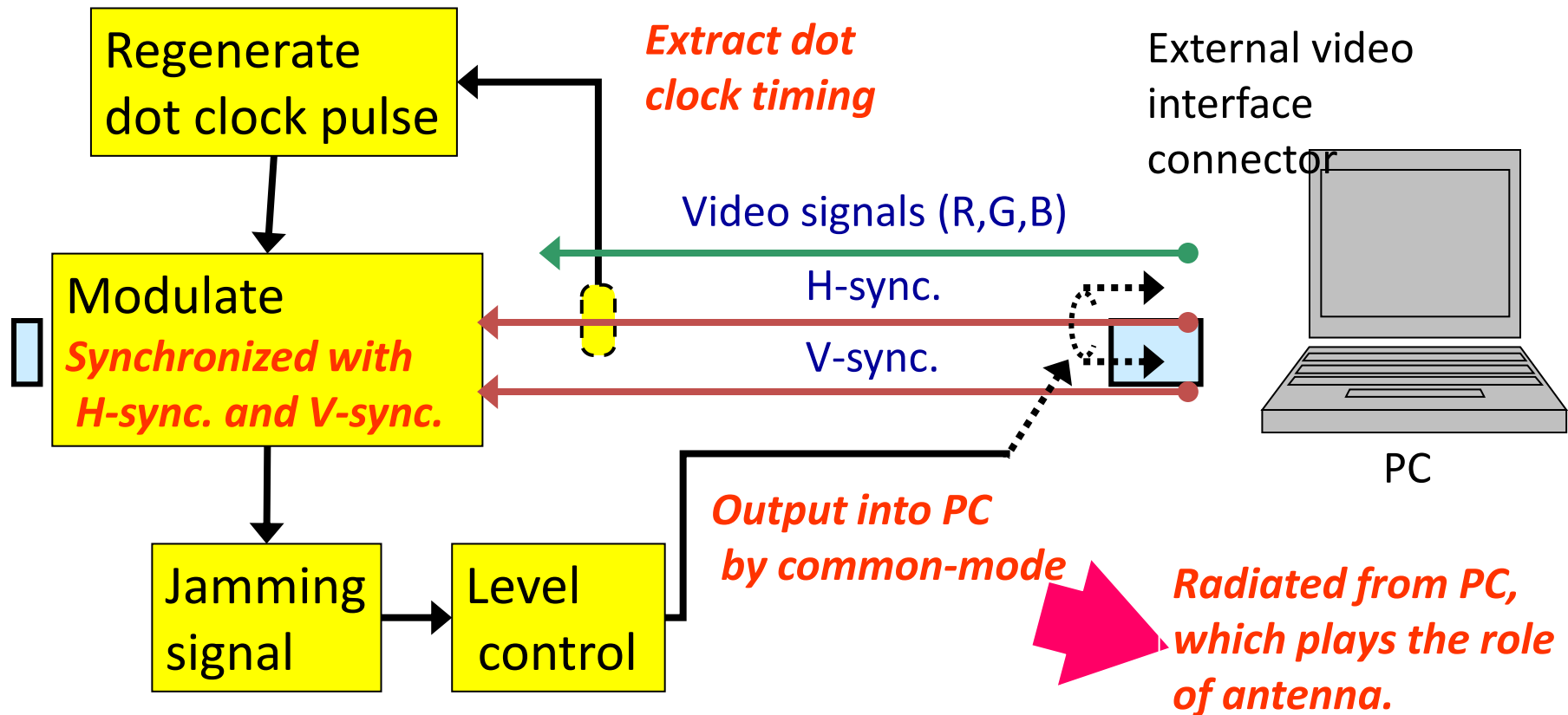


Appearance of prototype device

## Features:

- **Compact and light.**
- **Applicable to both desktop and mobile PCs.**  
(Available for mobile use.)
- **Easy to setup and activate.**
- **Automatically adapts to any video signal standard.**

# A device for generating jamming signals



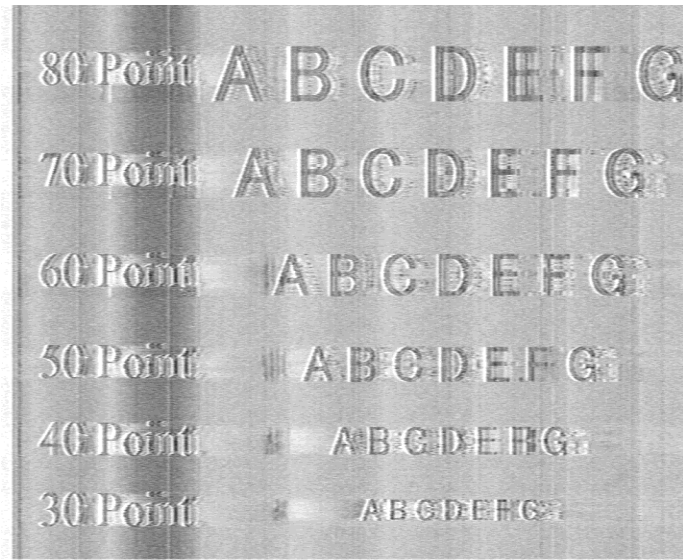
A function diagram of the developed countermeasure device

# Performance of mitigation device

Original display  
image on PC monitor

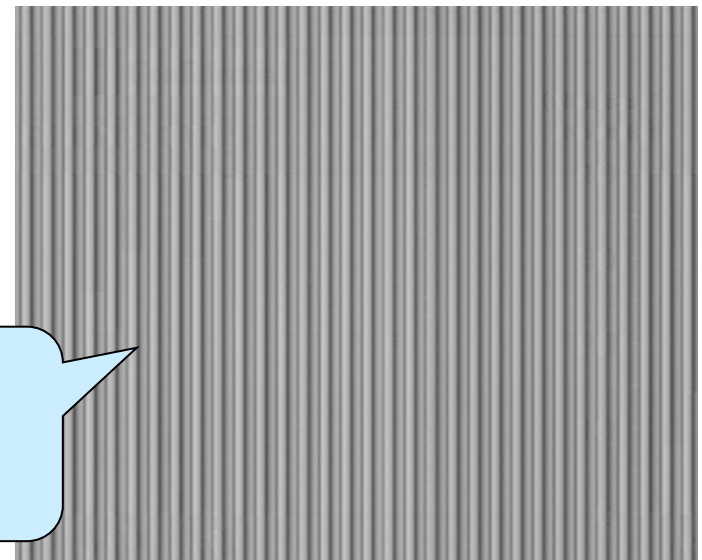
80 Point	A B C D E F G
70 Point	A B C D E F G
60 Point	A B C D E F G
50 Point	A B C D E F G
40 Point	A B C D E F G
30 Point	A B C D E F G

**Jamming**



(Averaged 32 frames)

Reconstructed image from  
emanation (without mitigation  
device)



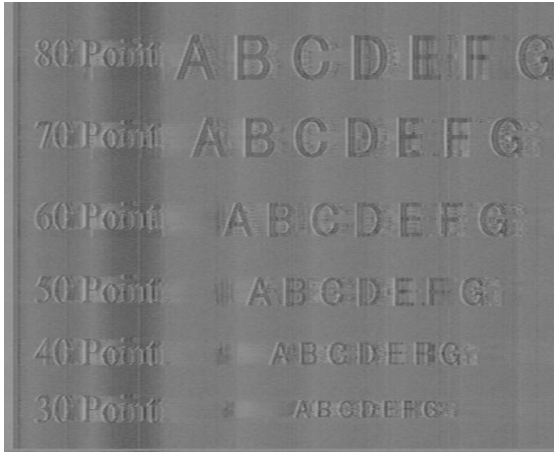
(Averaged 32 frames)

Reconstructed image with jamming  
signal from countermeasure device

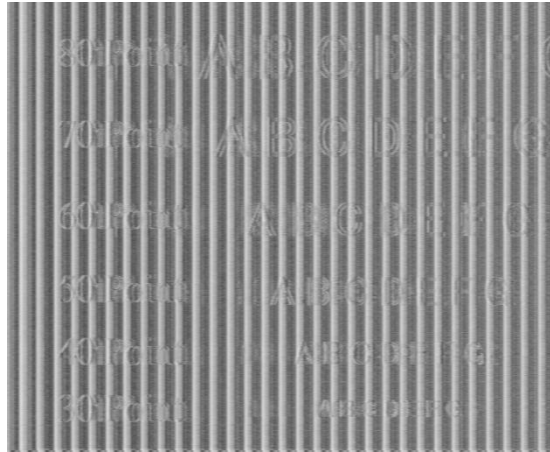
Original  
images are  
disappeared



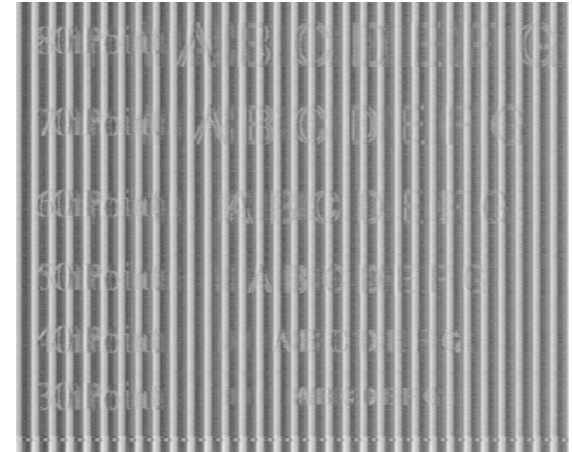
# Reconstructed image with jamming signal (averaged 32 frames)



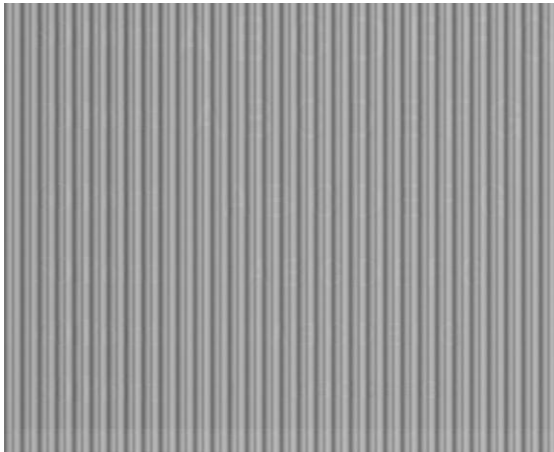
Only PC



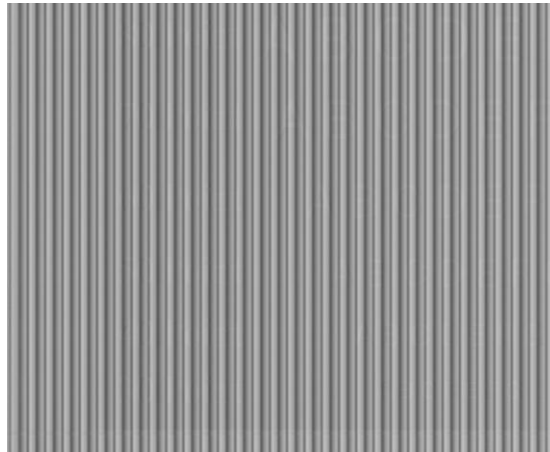
Jamming Signal (dB $\mu$ V/m)  
Original Signal (dB $\mu$ V/m) = 1.8 dB



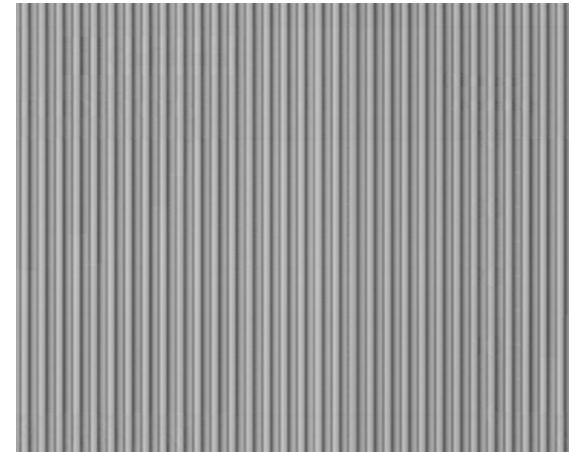
Jam./Org. = 2.9dB



Jam./Org. = 5.6dB

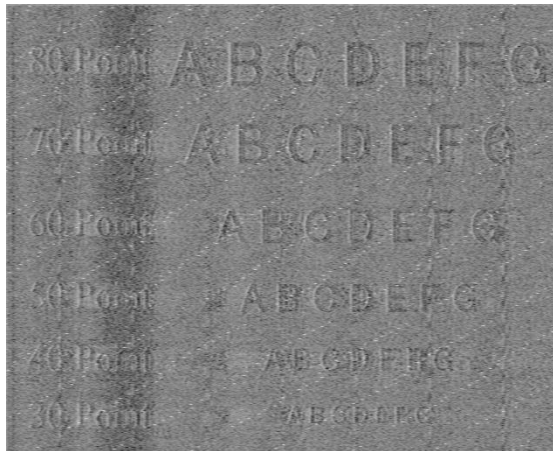


Jam./Org. = 9.4dB

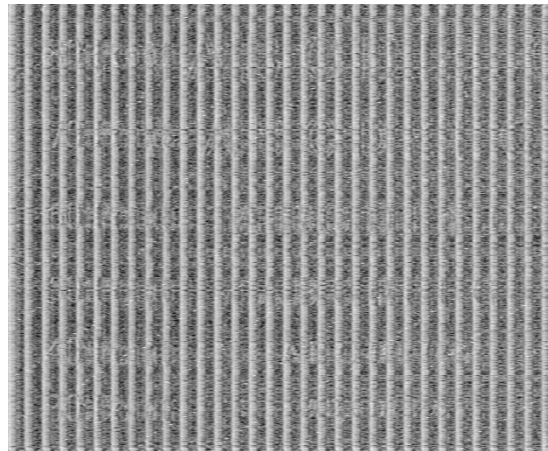


Jam./Org. = 12.7dB

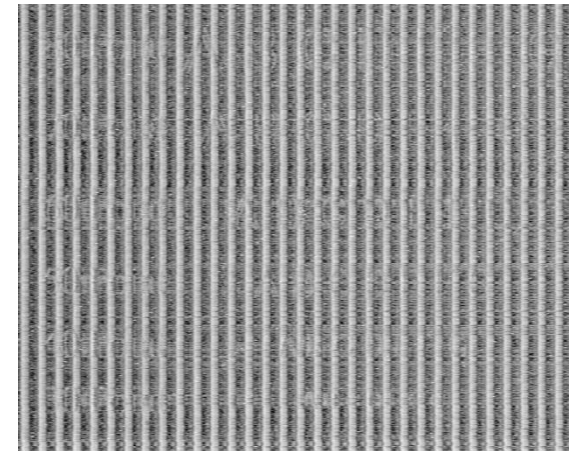
# Reconstructed image with jamming signal (single frame)



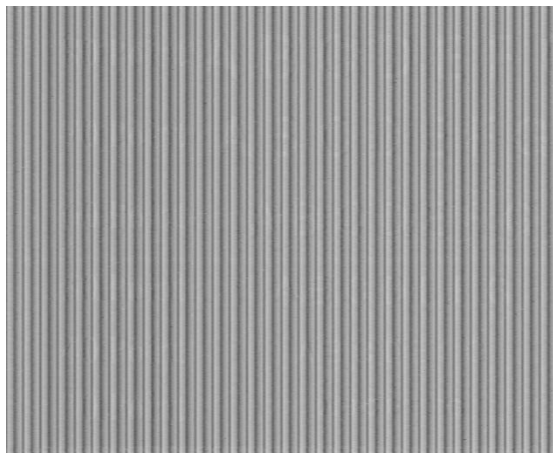
Only PC



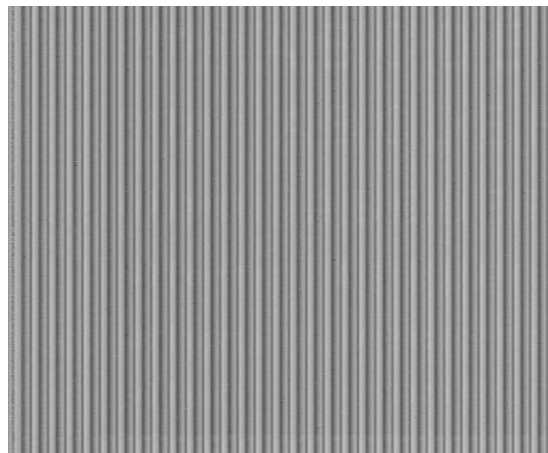
Jamming Signal (dB $\mu$ V/m)  
Original Signal (dB $\mu$ V/m) = 1.8 dB



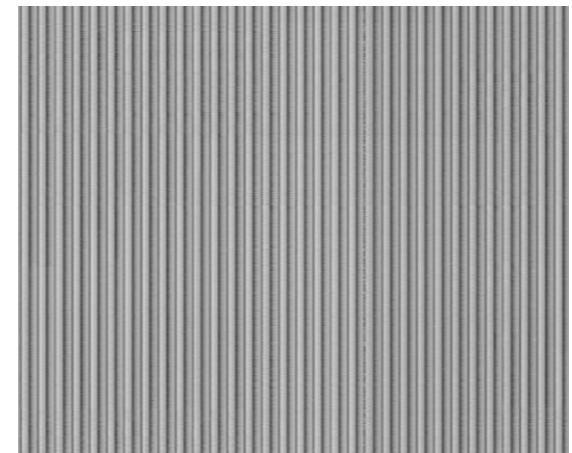
Jam./Org. = 2.9dB



Jam./Org. = 5.6dB

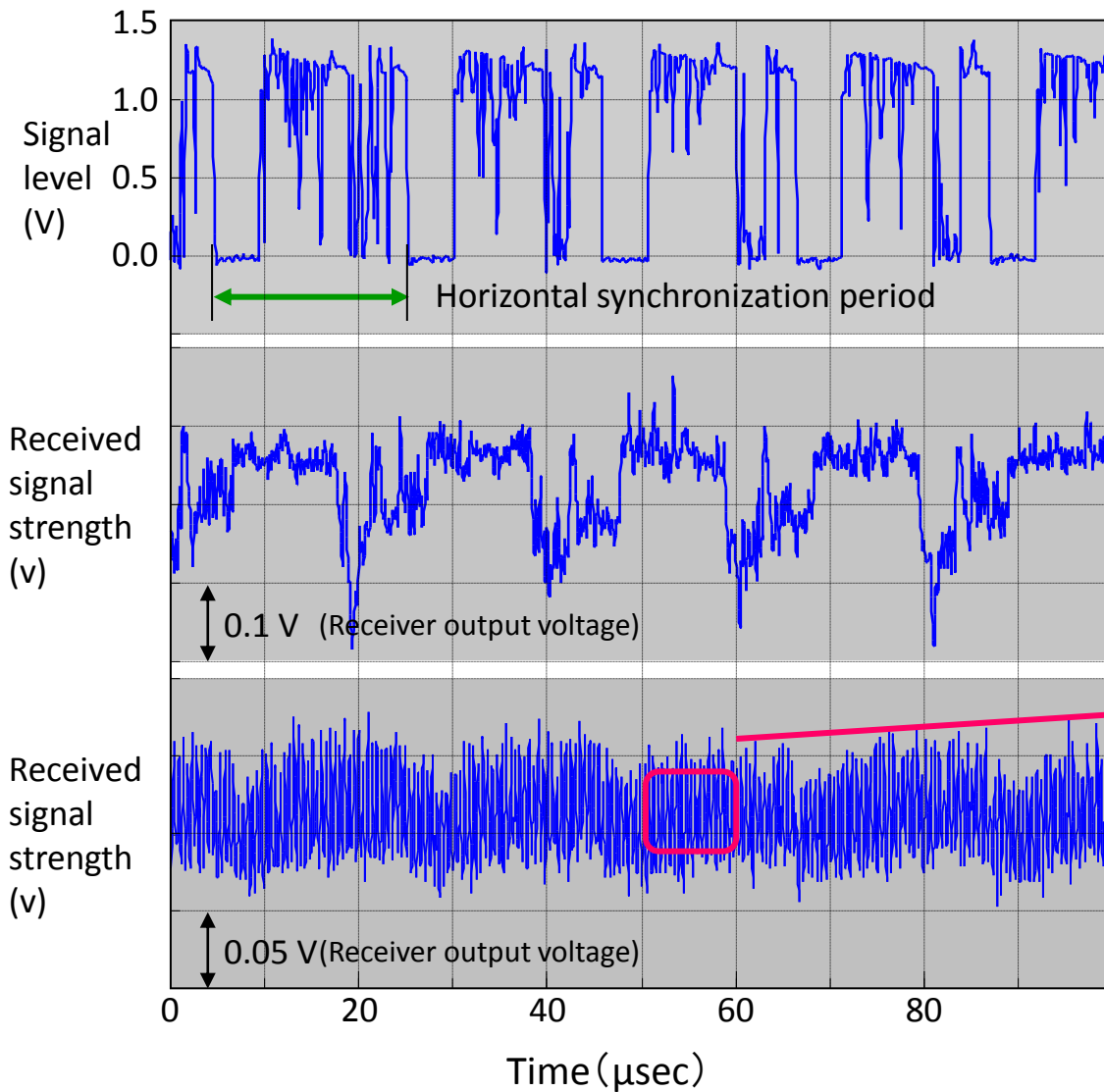


Jam./Org. = 9.4dB



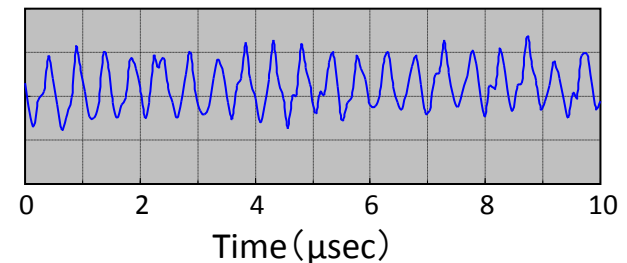
Jam./Org. = 12.7dB

# Waveform of jamming signal



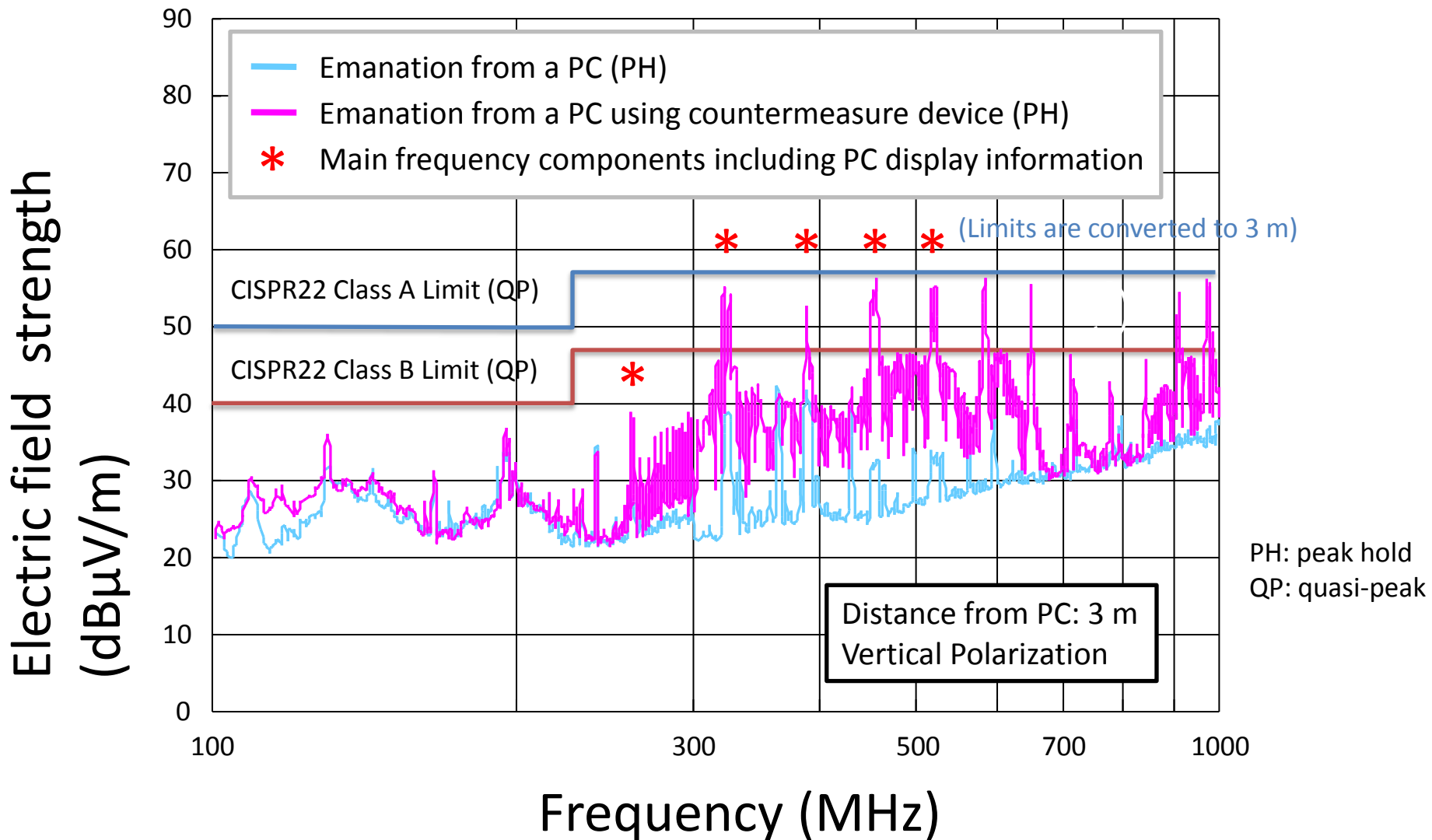
**(a) Original video signal (conducted)**

**(b) Radiated video signal (without countermeasure device)**

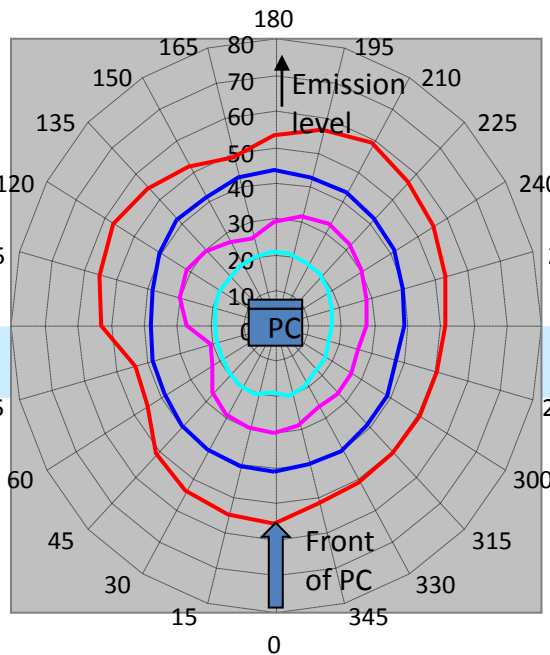


**(c) Radiated video signal with jamming signal of countermeasure device**

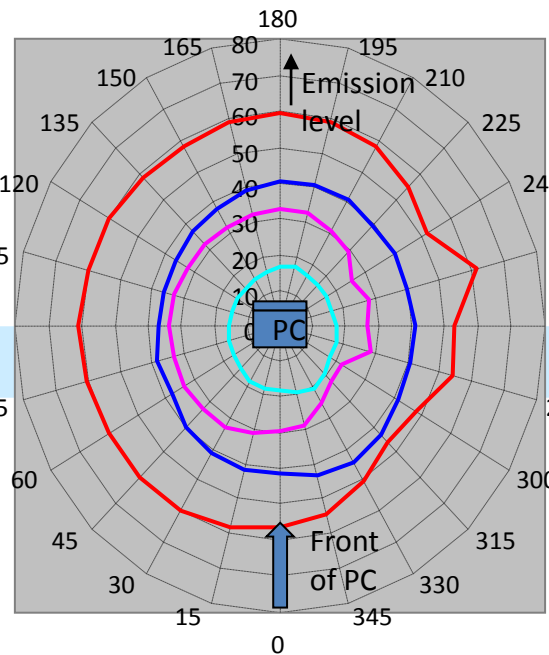
# Frequency spectrum of mitigation device



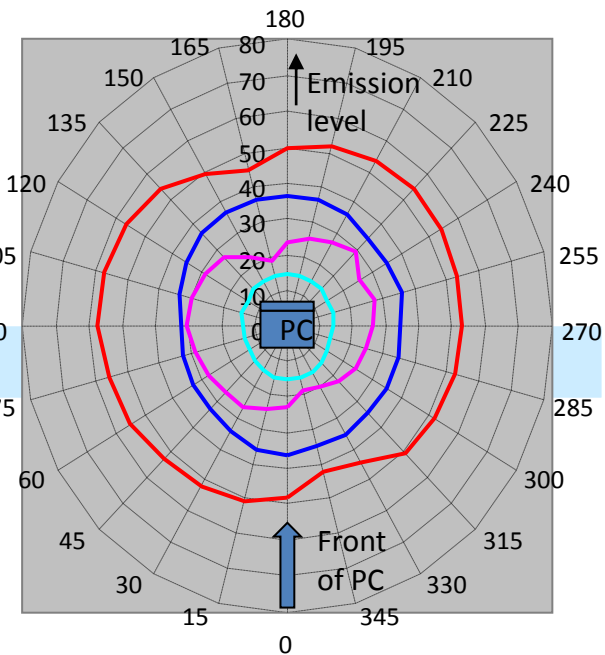
# Radiation pattern of mitigation device



Height of antenna :  $\pm 0$  m



Height of antenna : +1.5 m



Height of antenna : +3 m

*The field strength of the jamming signal of the countermeasure device is almost isotropic and much higher than that of the emission from a single PC, at any direction from the PC position.*

	Averaged	} Only PC
	Peak hold	
	Averaged	} PC with counter-measure device
	Peak hold	

※ Number of averaged or peak held data: 128.

Directional dependence of electromagnetic field strength at 390 MHz peak.

# K.84: Test methods and guide against information leaks through unintentional EM emissions

## Scope

It is the purpose of this recommendation to prevent information leakage due to unintentional electromagnetic radiation from telecommunication equipment handling important information, when the telecommunication equipment or sites are managed by ISMS.

This recommendation gives guidance to reduce the threats from information leakage due to unintentional electromagnetic emanation from information equipment at telecommunication centres.

Information is transmitted through electromagnetic waves unintentionally radiated from many kinds of equipment such as personal computers, data servers, laser printers, keyboards, and cryptographic modules. Among of them, **this recommendation treats only information leakage from equipment including raster scan video signal.** *We need study further on issues involving other kinds of leaked signals.*

Two approaches to protect against threats are given in this recommendation.

The first approach is :

Emission requirements and methods of examining equipment are applied when the equipment cannot be installed in the shielding site, it should be reduced the emission of the equipment.

The second approach is:

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

1. Scope
2. References
3. Definitions
4. Abbreviations
5. Test method and guide for EMSEC
  - 5.1. Threats against EMSEC
  - 5.2. Security management approach
  - 5.3. EMSEC requirements for radiation
  - 5.4. EMSEC requirements for conducted emission

## Annex A. Method of testing for radiation in EMSEC

1. Overview
2. General requirements for measurement
3. Method of testing for radiation leakage (Wideband method)
4. Method of testing for radiation leakage (Narrowband method)

## Annex B. Method of testing for conductive coupling in EMSEC

1. Overview
2. General requirements for measurement
  - 2.3. Measurement equipment and settings
3. Method of testing for conducted leakage

## APPENDIX I. Threat of EMSEC

1. Electromagnetic Wave Leakage
2. Method of Estimating Possible Distance for information leakage
  - 2.1. Performance of System Equipment
    - 2.1.1. Antenna Factor
    - 2.1.2. Receiver Performance
  - 2.2. Possible Distance for EMSEC

## APPENDIX II. Confidentiality of IT Equipment

1. Confidentiality of IT Equipment
  - 1.1. Confidentiality against Information Leakage

## APPENDIX III Example of wideband measurement

## APPENDIX IV Example of narrowband measurement

## Bibliography

EMSEC threats are determined according to comparisons of the **confidentiality** and **threat levels**

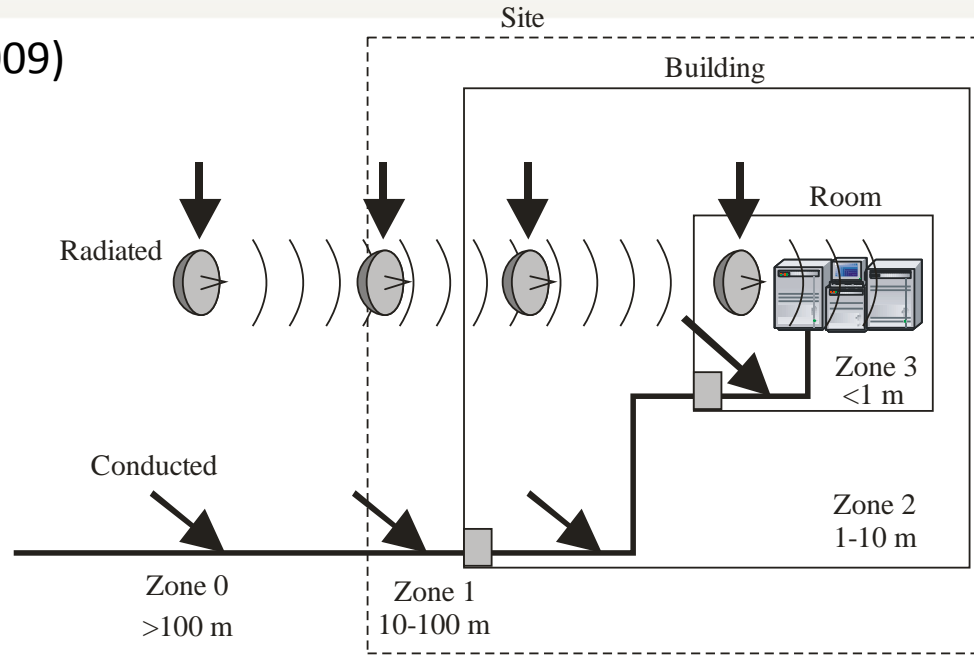
The threat level is determined by

- ◆ intrusion range
- ◆ portability
- ◆ availability

of the threat devices.



Rec. ITU-T K.81 (11/2009)



**Figure 5.2-1 – Classification of intrusion areas**

**Table 5.2-1 – Intrusion area and portability levels**

Intrusion area	Threat device location	Threat device portability levels (Note)	Typical minimum separation distance (m)
Zone 0	Public space	PI, PII, PIII, PIV	> 100
Zone 1	Same site	PI, PII	100 – 10
Zone 2	Same building	PI, PII	10 – 1
Zone 3	Same room	PI, PII	< 1

NOTE – The portability level of the threat devices that may be located in each intrusion zone is determined by the physical security measures applied.

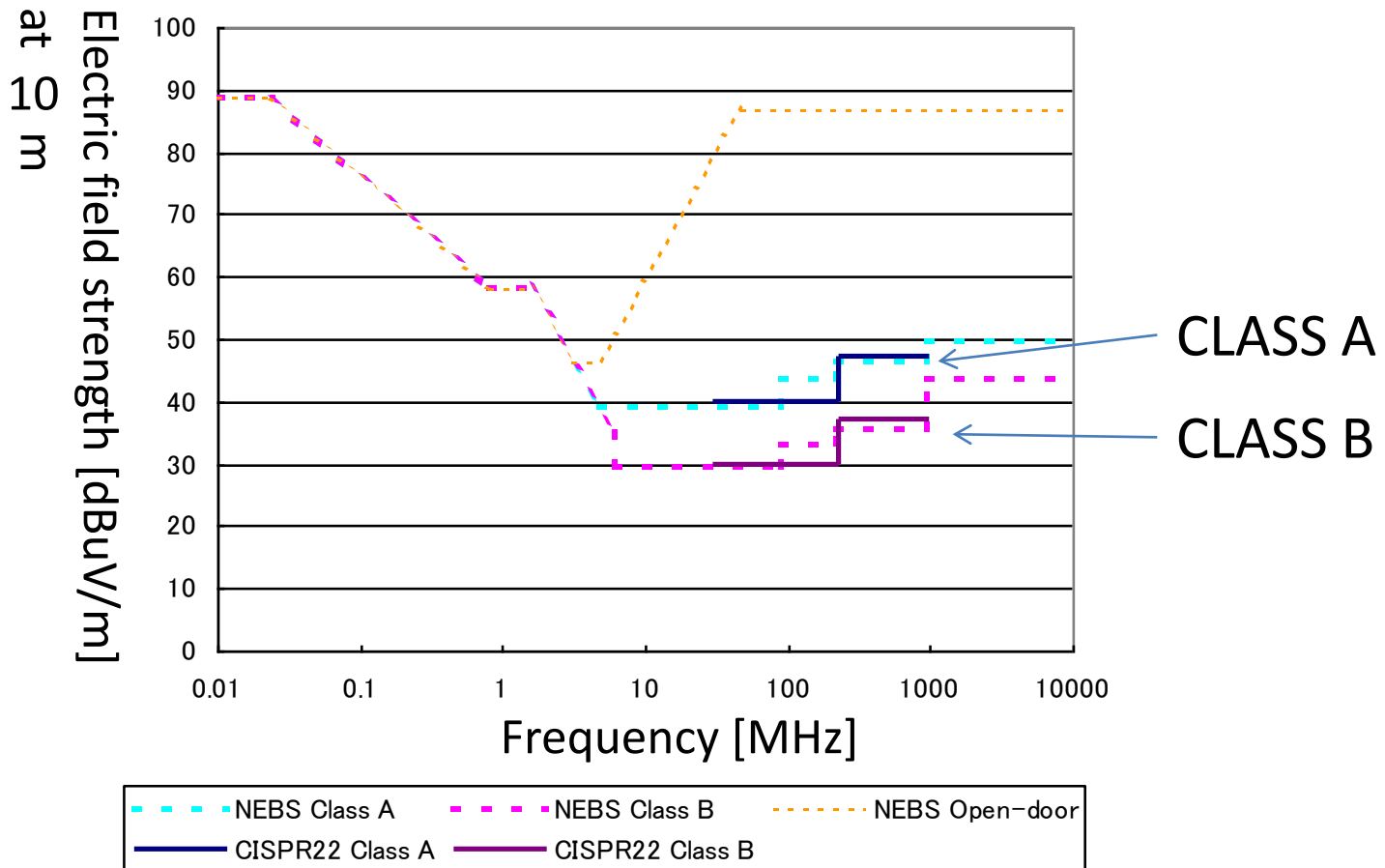
## Table 5.1-2 - Definitions of threat portability levels

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

## Table 5.1-3 - Definitions of threat availability levels

<b>Availability level</b>	<b>Definition</b>	<b>Examples</b>
AI	'Consumer'	
AII	'Hobbyist'	Amateur receiver
AIII	'Professional'	General-purpose EMC receiver
AIV	'Bespoke'	Special receiver

The leaking electromagnetic field strength (emissions) of IT equipment is regulated by national standards or the standards of individual countries (emission standards)



**Figure II.1 - Comparison of Reference Emission Values (CISPR22 and NEBS GR1089)**

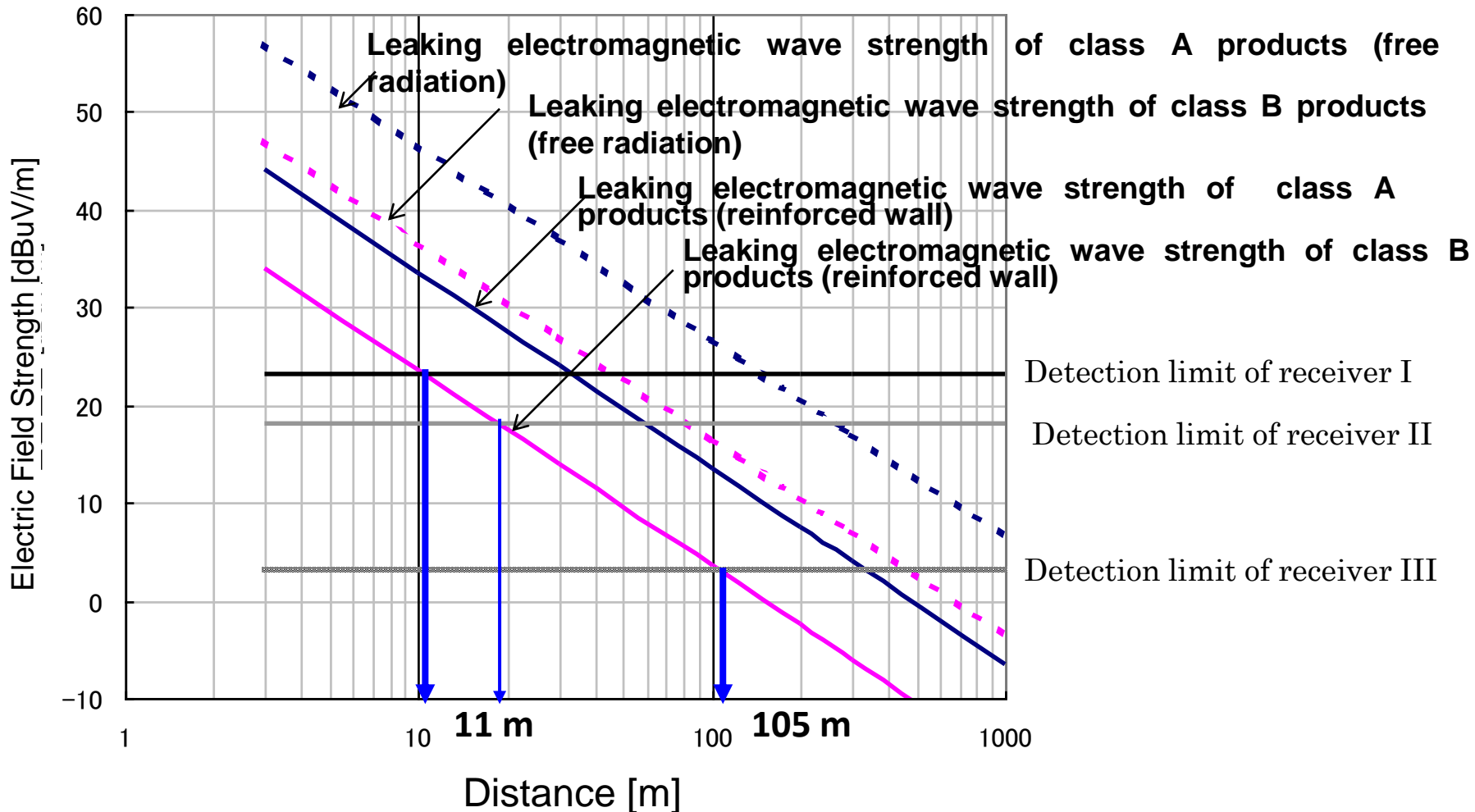


Figure I.2 - Relationship between Possible Electric Field Strength (Strength of Leaking Information) and Distance for EMSEC

**Table 5.1-1 - Examples of Threats Related to Information Leakage**

Types of Threats	Examples of Receiver	Possible distance for EMSEC		Threat Level			Threat Number
		Confidentiality Level Class A	Confidentiality Level Class B	on Attack Side	Portability	Availability	
EMSEC	Special receiver	330 m *)	105 m *)	Zone 0	PIII	AIV	K4-1
	Special receiver	330 m *)	105 m *)	Zone 1	PIII	AIV	K4-2
	General-purpose EMC receiver	59 m *) 263 m	19 m *) 83 m	Zone 1	PII	AIII	K4-3
	General-purpose EMC receiver	59 m *) 263 m	19 m *) 83 m	Zone 2	PII	AIII	K4-4
	Amateur receiver	33 m *) 148 m	11 m *) 47 m	Zone 1	PII	AII	K4-5
	Amateur receiver	33 m *) 148 m	11 m *) 47 m	Zone 2	PII	AII	K4-6
	Amateur receiver	33 m *) 148 m	11 m *) 47 m	Zone 3	PII	AII	K4-7

\*) Assumed to have reinforced concrete walls as 13dB attenuation.

# Why the Electromagnetic Security standards needs?

Security management, Related standards, ITU-T Recommendation K.78, K.81, K.87

# Electromagnetic security issues related to X.1051 Security management.

## 9 Physical and environmental security

### 9.2 Equipment security

#### 9.2.1 Equipment siting and protection

Implementation guidance

The following guidelines should be considered to protect equipment

- d) controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;

## Annex A Telecommunications Extended Control Set

### A.9 Physical and environmental security

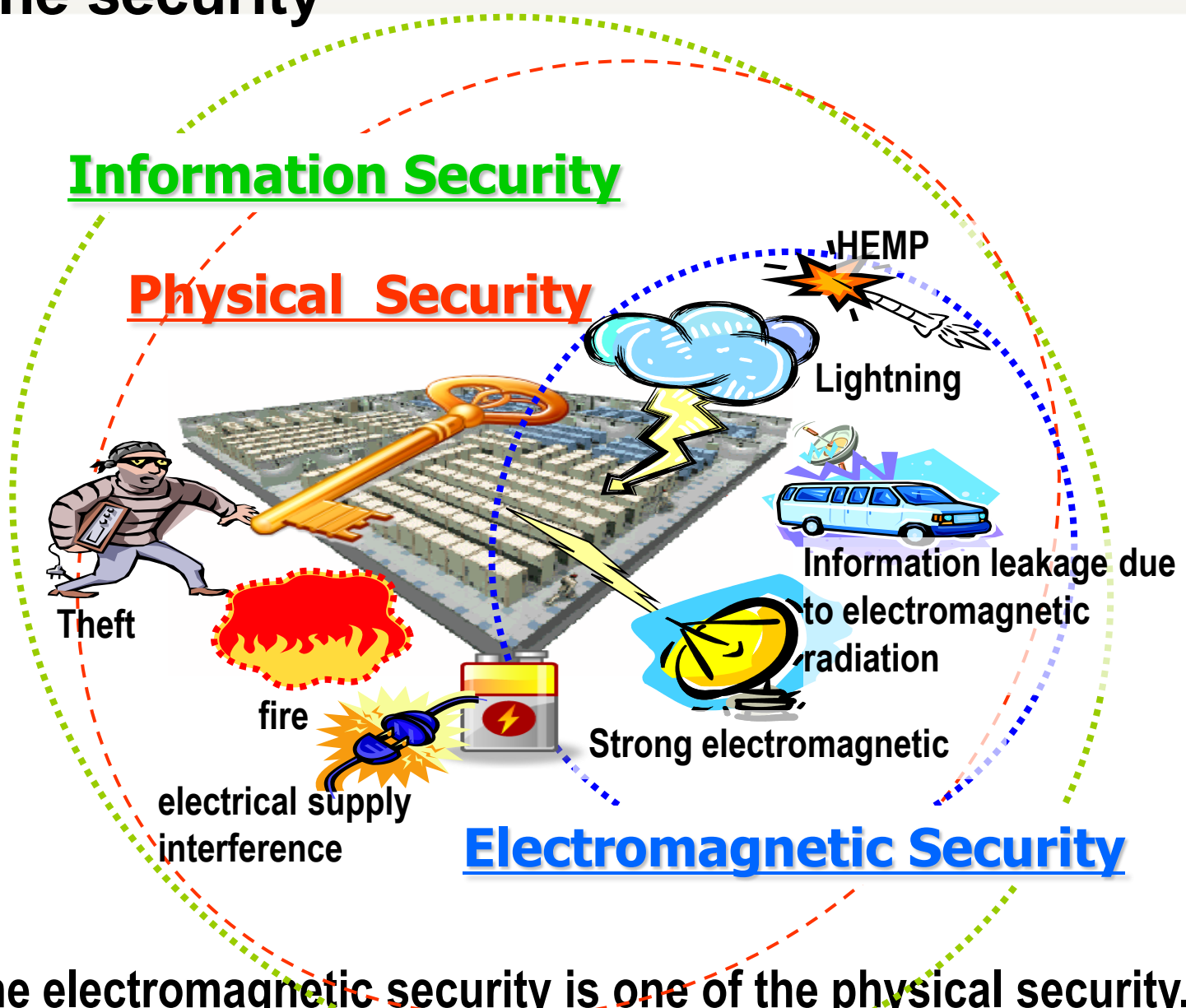
- c) a site whose environment is least susceptible to damage from strong electromagnetic field should be selected for communication centers; where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect telecommunications equipment rooms with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

#### A.9.1.8 Securing telecommunications equipment room

- d) the telecommunications equipment room should be located where it is least susceptible to damage from strong electromagnetic fields; if the room needs to be located where it is susceptible to strong electromagnetic fields, it should be protected by electromagnetic shields or some other measures; especially, if power supply facilities are installed within the telecommunications equipment room, measures should be appropriately taken to prevent interference from electromagnetic field;
- j) if necessary, measures should be taken to protect the data storage room and data safe from electromagnetic interference;



# Telecommunication and data center and the security



The electromagnetic security is one of the physical security.

- What is “electromagnetic radiation” related to security?
- What is “strong electromagnetic field”?
- How to do the risk assessment?

# IEC SC 77C Publications

61000-1-  
(General)

-3 HEMP EFFECTS ON SYSTEMS

-5 HPEM EFFECTS ON SYSTEMS

61000-2-  
(EM  
Environment)

-9 HEMP  
RADIATED  
ENVIRONMENT

-10 HEMP  
CONDUCTED  
ENVIRONMENT

-11 CLASSIFICATION  
OF HEMP  
ENVIRONMENTS

-13 HPEM  
ENVIRONMENTS

61000-4-  
(Testing and  
Measuring  
Techniques)

-23  
TEST  
METHODS  
RADIATED

-24  
TEST  
METHODS  
CONDUCTED

-25  
HEMP  
IMMUNITY  
TESTS

-32  
HEMP  
SIMULATOR  
COMPENDIUM

-33 HPEM  
MEASUREMENT  
METHODS

-35 HPEM  
Simulator Compendium

61000-5-  
(Installation  
and Mitigation  
Guidelines)

-3 HEMP  
PROTECTION  
CONCEPTS

-4 SPECIFICATIONS  
FOR RADIATED  
PROTECTION

-5 SPECIFICATIONS  
FOR CONDUCTED  
PROTECTION

-6 MITIGATION  
OF  
EXTERNAL EM  
INFLUENCES

-7 EM CODE

-8 HEMP protection  
methods for the  
distributed civil  
infrastructure

-9 System-level  
susceptibility  
assessments for  
HEMP and HPEM

61000-6-  
(Generic  
Standards)

-6 GENERIC  
STANDARD FOR HEMP  
IMMUNITY

Completed in 2009

## Information Security

## Physical Security

**X.1051**  
**Security management**

## Electromagnetic Security

Resistibility

**K.Sec (K.87)**

**K.20**

**K.48**

...

**K.78(HEMP)**

**K.81(HPEM)**

**K.84 (Leakage)**

**K.Secmiti**

- **Natural made threats** → existing recommendations
  - Lightning, ESD, EMC (**K.20**, **K.48** and so on)
- **Malicious Man made threats** → work items
  - High power electromagnetic
    - HEMP (High altitude Electromagnetic pulse)
    - HPEM (High Power Electromagnetic)
    - IEMI (Intentional Electromagnetic Interference)
  - Information leakage by unintentional emission
    - EMSEC (Electromagnetic emanation Security) << TEMPEST

The recommendations must be the bridge between the security people and EMC people.

# K-series recommendations related to Electromagnetic security

- **K.78**: High altitude electromagnetic pulse immunity guide for telecommunication centres
- **K.81**: High-power electromagnetic immunity guide for telecommunication systems
- **K.84**: Test methods and guide against information leaks through unintentional electromagnetic emissions
- **K.87 (K.sec)**: Guide for the application of electromagnetic security requirements - Basic Recommendation
- **K.secmiti**: Mitigation methods

Our recommendations can be downloaded by  
ITU-T Home Page

- [http://www.itu.int/ITU-T/recommendations/index\\_sg.aspx?sg=5](http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=5)
- <http://www.itu.int/rec/T-REC-K.78-200906-I>
- <http://www.itu.int/rec/T-REC-K.81-200911-I>
- <http://www.itu.int/rec/T-REC-K.84-201101-P>

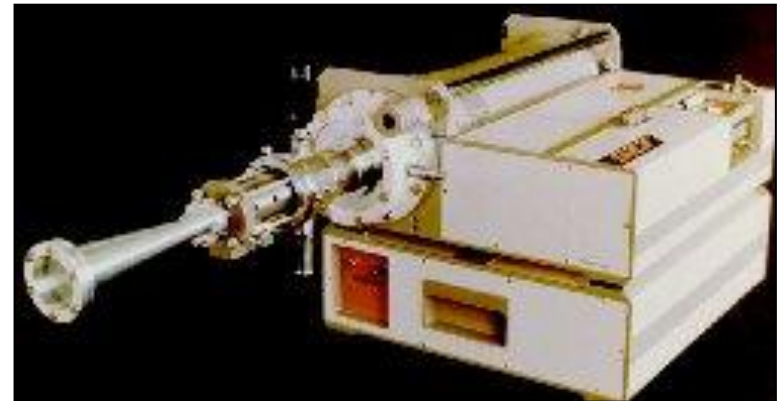
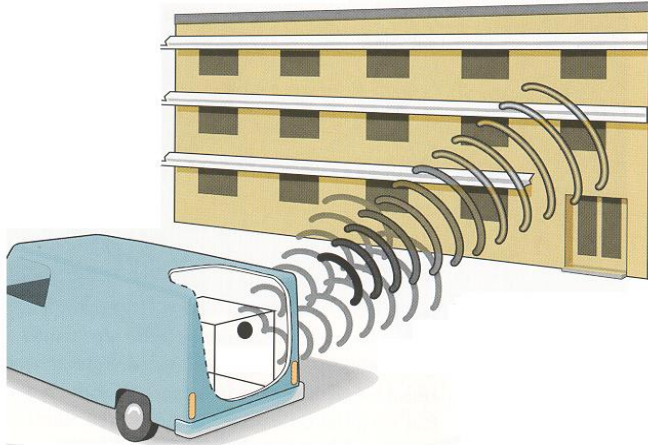
1. SCOPE
2. REFERENCES
3. DEFINITIONS
4. ABBREVIATIONS AND ACRONYMS
5. **CLASSIFICATIONS OF THREAT**
  - 5.1. DEFINITION OF THE PORTABILITY LEVEL
  - 5.2. DEFINITION OF THE INTRUSION AREA
  - 5.3. DEFINITION OF AVAILABILITY LEVELS
  - 5.4. EXAMPLE OF THREAT
6. **VULNERABILITY OF DEVICES TO BE PROTECTED**
  - 6.1. DEFINITION OF VULNERABILITY CLASSIFICATIONS
  - 6.2. EXAMPLE OF VULNERABILITY OF EQUIPMENT TO BE PROTECTED
7. **EM MITIGATION LEVELS**
  - 7.1. GENERAL ITEMS FOR DETERMINING THE EM MITIGATION LEVEL

Appendix A HPEM THREAT AND VULNERABILITY

Appendix B EXAMPLES OF EM MITIGATION LEVELS

**The main body is for risk assessment methods  
Appendix A is the threat database.**

# Electromagnetic attacks (HPEM/IEMI)





# The definitions of Intrusion Area and Portability levels

**Table 5.2-1/ K.81 Intrusion Area and portability levels**

Intrusion Area	Portability levels	
Zone 0	Public Space	The threat is 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 thru the physical Site Security. So, threats of portability levels PI & PII can be located here. The existence of PIII & PIV depends upon physical security protocols for the site.
Zone 2	Building	The threat is located within the same building as the equipment to be protected and hence has passed thru physical Building Security. So, threats of portability levels PI & PII can be located here; only human-portable threats 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 PI & PII can be located here - depending upon physical security protocols within the building.

# Examples of the HPEM/IEMI threat

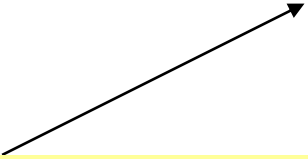
**Table 5.4-1 / K.81 Example of Threat Related to High-Power Electromagnetic Waves**

Threat Type	Example of Attack Device	Intrusion Range on Attack Side	Strength	Frequency Range	Portability	Availability	Threat Number
Electromagnetic Wave Attack -- radiated	JOLT	Zone 0	500kV/m@100m	300MHz-10GHz	PIV	AIV	K1-0
	IRA (Hi-tech)	Zone 0	12.8 kV/m@100m	300MHz-10GHz	PIV	AIV	K1-1
	Commercial radar (Mid-tech)	Zone 0	60 kV/m@100m	1GHz-10GHz (1.285GHz)	PIV	AIV	K1-2
	Navigation radar	Zone 0	385 V/m@100 m	1GHz-10GHz (9.41 GHz)	PIII	AIII	K1-3
	Magnetron generator	Zone 1	475 V/m@10 m	1GHz-3GHz	PIII	AII	K1-4
	Amateur wireless device	Zone 2	286 V/m@1 m	100MHz-3GHz	PII	AII	K1-5
	Amateur wireless device	Zone 3	169 V/m@10 cm	100MHz-3GHz	PI	AI	K1-6
	Illegal CB radio	Zone2	573 V/m@10m	27MHz	PII	AI	K1-7
Electrostatic discharge Attack	Stun gun	Zone 3	500 kV	100MHz-3GHz	PI	AI	K2-1
Electromagnetic Wave Attack – Conducted	Lightning-surge generator	Zone 0	50 kV (charging voltage)	1.2/50 10/700	PIV	AIV	K3-1
	Compact lightning-surge generator	Zone 0-3	10 kV (charging voltage)	1.2/50 10/700	PII	AII	K3-2
	CW generator	Zone 0-3	100V~240V/4kV	1Hz-10MHz	PII	AII	K3-3
	Commercial power supply	Zone 0-3	100V~240V	50/60Hz	PI	AI	K3-4


- The Risk is evaluated by EM mitigation level

**EM mitigation level (dB) = Level of Threat – Vulnerability of equipment**

Select the threat from  
Appendix A Threat database



Confirm the vulnerability level from  
Immunity and Resistibility levels of  
equipment



# Example of Calculated EM mitigation Level and Frequency

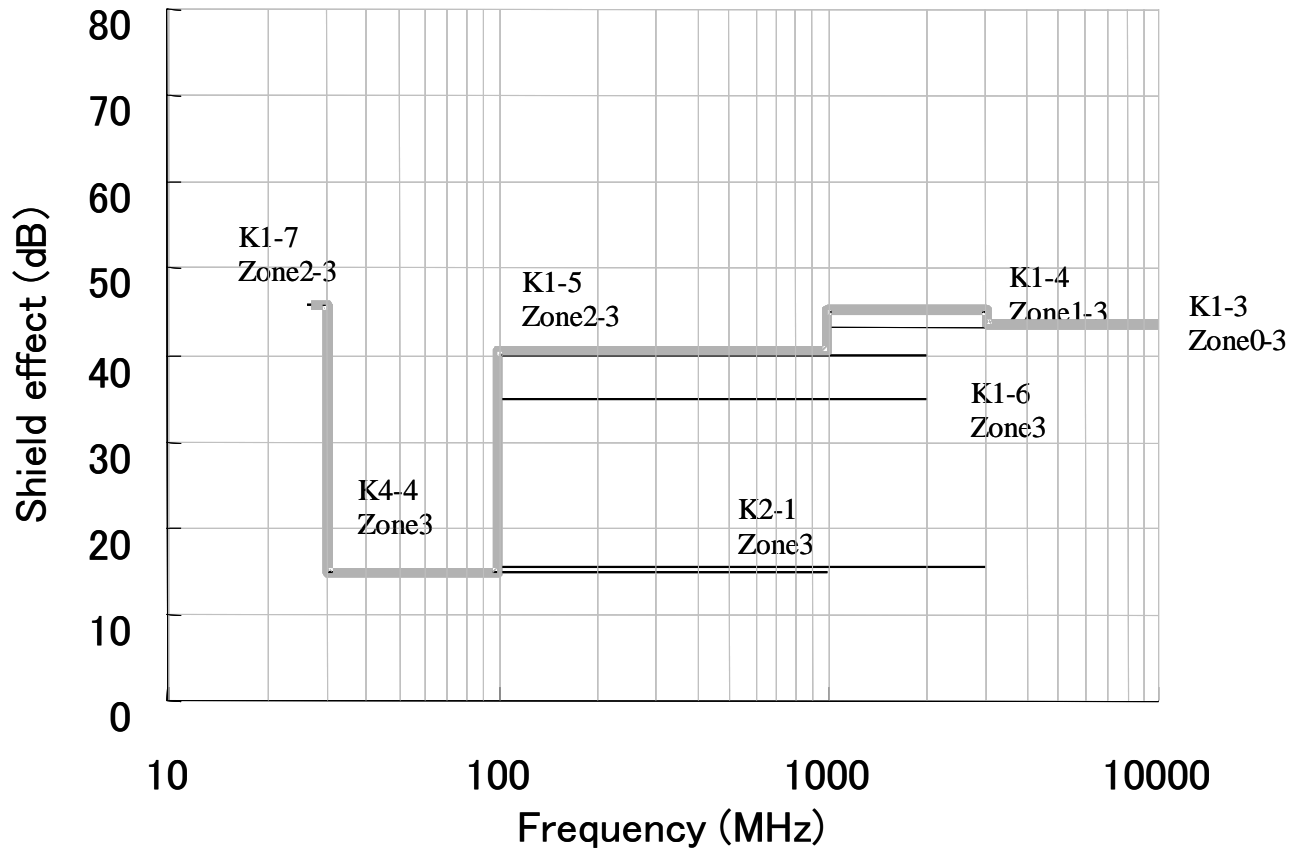


Figure 8.1-2/K.81 Example of Calculating the Relationship between the EM mitigation Level and Frequency

## APPENDIX A HPEM THREAT AND VULNERABILITY

### 1. **CALCULATING HPEM THREAT**

- 1.1. IMPULSE RADIATING ANTENNA (IRA) AND JOLT
- 1.2. COMMERCIAL RADAR
- 1.3. NAVIGATION RADAR
- 1.4. MAGNETRON GENERATOR
- 1.5. ILLEGAL CB RADIO
- 1.6. AMATEUR RADIO
- 1.7. STUN GUN
- 1.8. LIGHTNING-SURGE GENERATOR
- 1.9. CW GENERATOR
- 1.10. COMMERCIAL POWER SUPPLY

### 2. **VULNERABILITY OF IT EQUIPMENT**

- 2.1. VULNERABILITY TO ELECTROMAGNETIC WAVE ATTACK
- 2.2. VULNERABILITY EVALUATION OF A SAMPLE DEVICE
  - 2.2.1. Vulnerability to a Radiated Electromagnetic Field
- 2.3. VULNERABILITY TO ELECTROSTATIC DISCHARGE

## ➤ JOLT system

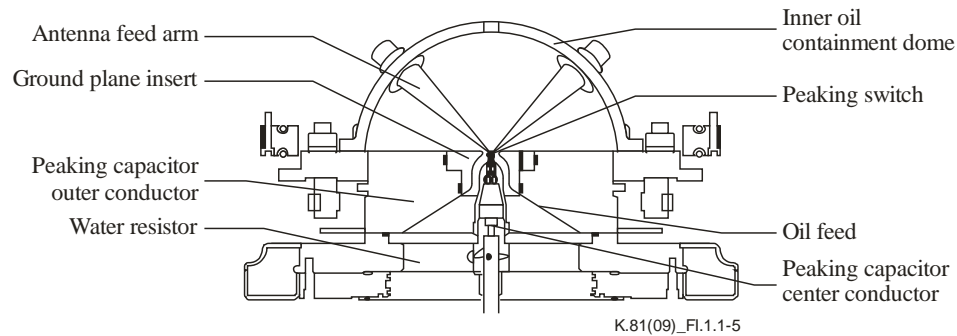
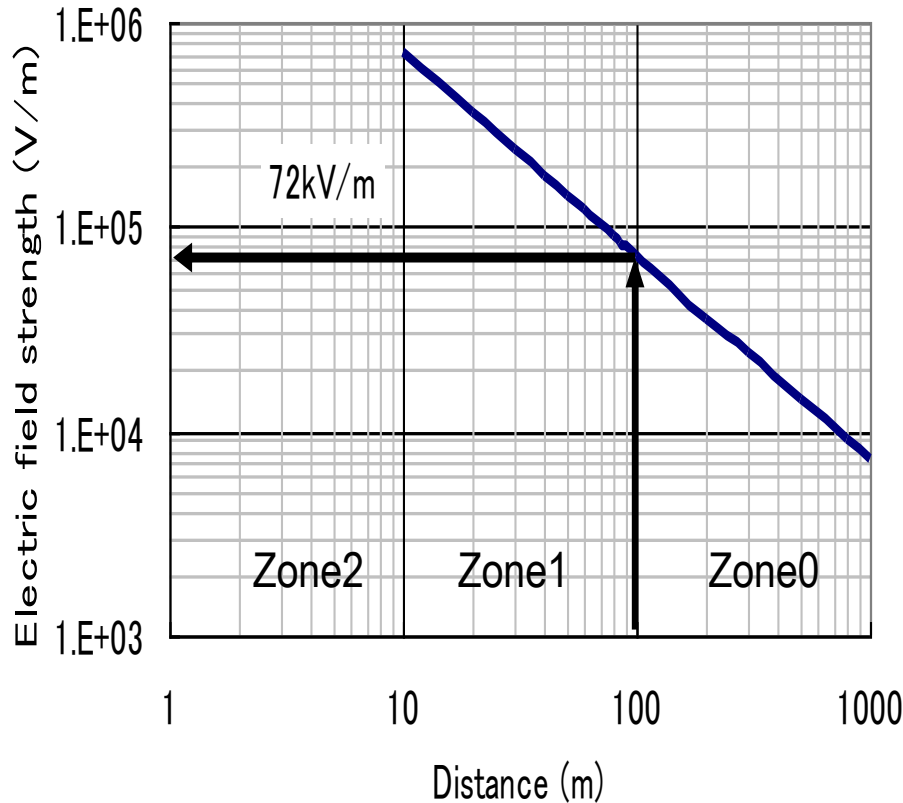


Figure I.1.1-5 – Overview of the JOLT system

Figure 2.2-2/K.81 Relationship Between the JOLT Peak Electric Field Strength and the Protection Distance (Case #5 in Table 2.1-1, Reflector diameter: 3.048 m)

## ➤ Magnetron Generator

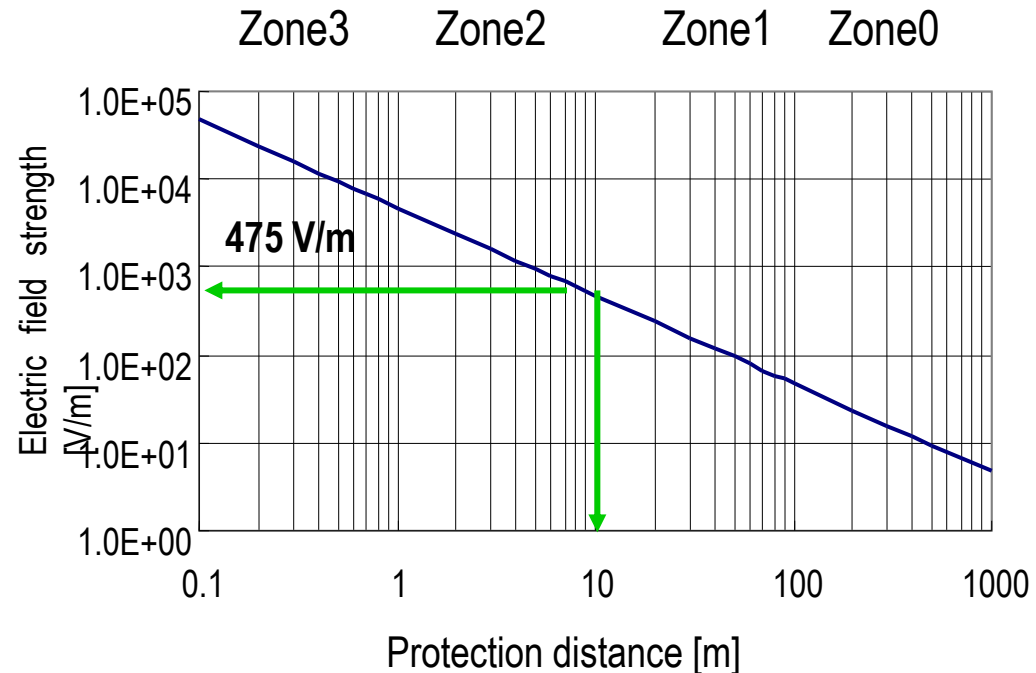
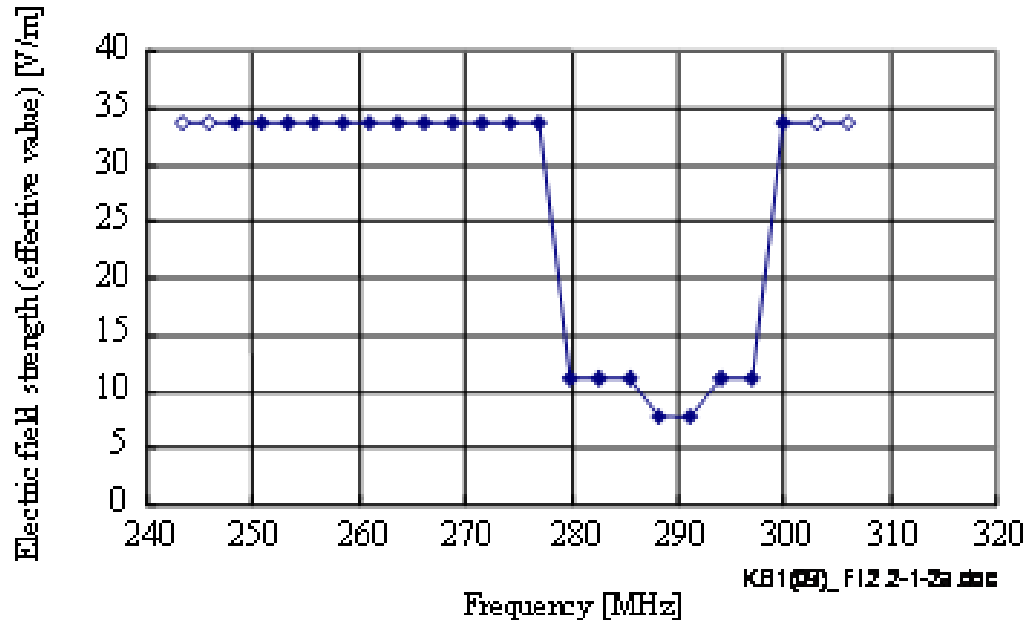


Figure 2.7/ K.81 (K.Hemp) - Relationship between the Peak Electric Field Strength of a Magnetron Generator and Protection Distance (Frequency: 2.46 GHz, Peak transmission output: 1.8 kW, Antenna gain: 24 dBi, Transmission efficiency: 100%)

## ➤ Examined some equipments



(a) Evaluation results for PC1

Figure I.2.2.1-2 – Evaluation results for vulnerability to radiated electromagnetic waves



## ➤ Example

**Table I.2.2.1-1 – Lowest resistances and frequencies**

<b>Device</b>	<b>Lowest resistance value</b>	<b>Frequency</b>	<b>Remarks</b>
PC1	7.8 V/m	291.2 MHz	About 3 × the system clock (99.75 MHz)
PC2	20.2 V/m	535.1 MHz	About 8 × the system clock (66.0 MHz)
Router	11.2 V/m	214.24 MHz	–

## Examples of shield level

APPENDIX B EXAMPLES OF EM MITIGATION LEVELS

EXAMPLE OF EM MITIGATION LEVELS FOR AN IP NETWORK SERVICE

2.4. DATA CENTER (EC SITE)

2.5. DATA CENTER (STORAGE)

2.6. ROUTERS AND SWITCHES (MSP)

2.7. DATA CENTRE OF A LOCAL GOVERNMENT UNIT OR GOVERNMENT ORGANIZATION

2.8. EXAMPLES OF EM MITIGATION LEVELS OF AN IP COMPANY NETWORK

2.8.1. PC, Etc.

2.8.2. Mail Server

2.8.3. ERP Server, Storage, Customer DB Server, Etc.

APPENDIX C REFERENCES

APPENDIX D IEC STANDARDS RELATED TO HPEM

- **IEC SC77C** :Generic : HEMP, HPEM, IEMI
  - [http://www.iec.ch/dyn/www/f?p=102:17:0::::LANG,FSP\\_SEARCH\\_TC:EN,77C](http://www.iec.ch/dyn/www/f?p=102:17:0::::LANG,FSP_SEARCH_TC:EN,77C)
  
- **CIGRE WG C4.206** : Power systems: IEMI
  - [http://www.cigre-c4.org/Site/WG/pa\\_wl.asp?IDWG=643](http://www.cigre-c4.org/Site/WG/pa_wl.asp?IDWG=643)
  
- **ITU-T SG5 Q15** : Telecom: HEMP, HPEM, IEMI,  
**Information leakage**
  - <http://www.itu.int/ITU-T/studygroups/com05/sg5-q15.html>
  
- **IEEE EMC TC5**: High Power Electromagnetic  
IEEE P1642:Public Accessible Computer Systems IEMI  
IEEE EMC TC5 SC2 : **Information leakages**
  - <http://www.emcs.org/committees/tc05/tc05-reports.html>

## ➤ IEEE P1642

- Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI

## ➤ Cigré C4.206 WG

- Protection of the high voltage power network control electronics against intentional electromagnetic interference (IEMI)

## ➤ NIST Smart Grid Activity

- HPEM aspects are being considered in the EMCII WG

## Future work

*We need study further on issues involving  
other kinds of leaked signals.*

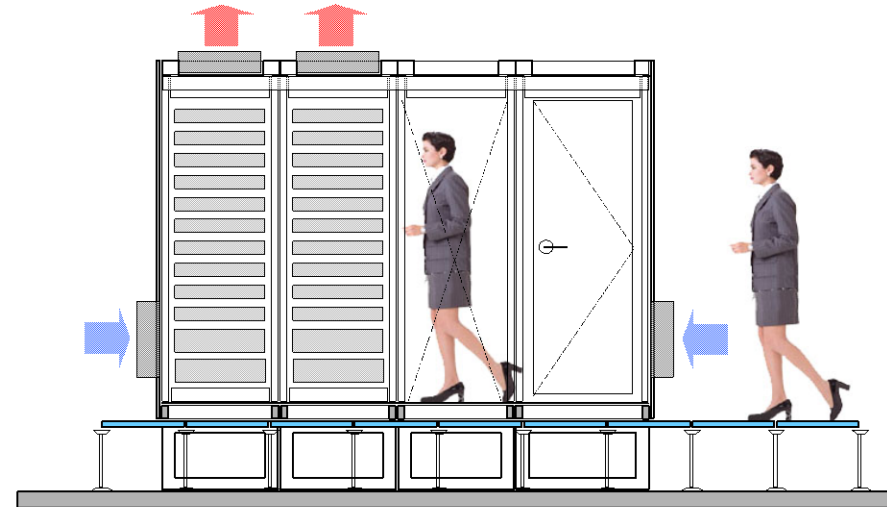
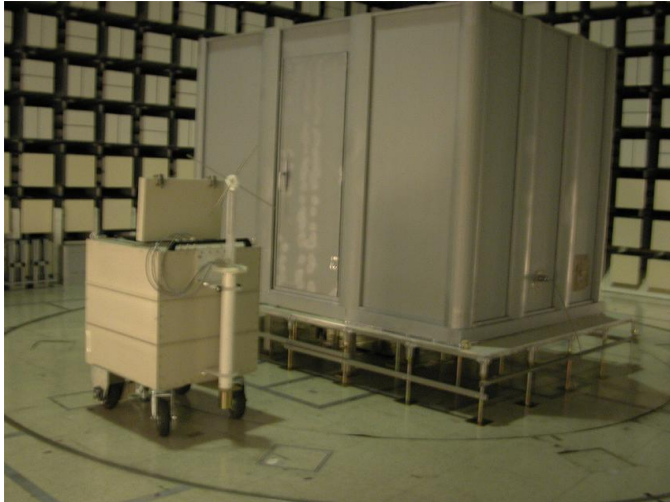
*Evaluate methods for Cryptographics*

- Application guidance for electromagnetic security recommendations;
- Technical requirement for preventing **information leaks by unexpected radio emission** from equipment and protection of telecommunication centres from **attacks using high power radio waves** (HEMP, HPEM/IEMI);
- Mitigation methods such as electromagnetic shielding;
- Methodology for evaluating the protective measures.

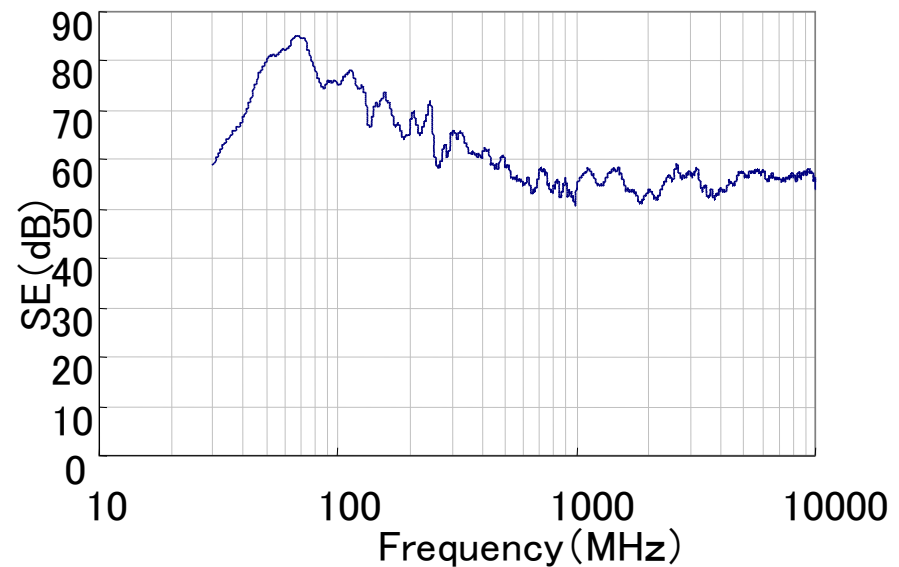
## Table Work Program of Question 15/5

Recommendation	Title of the Recommendation	Priority	Timing	
K.87	Guide for the application of electromagnetic security requirements.- Basic Recommendation	---	2011	
K.78	HEMP immunity guide for telecommunication centres	---	No Action Needed	
K.81	HPEM immunity guide for telecommunication systems	---	No Action Needed 2009-11-29	➔ Revise
K.84	Test methods and guide against information leak through unintentional EM emission	---	No Action Needed 2011-01-13	➔ Revise
K.secmiti	Mitigation methods against EM security threats	H	2013	New

# Mitigation <Pre-Fabric Shielding Cabinet>

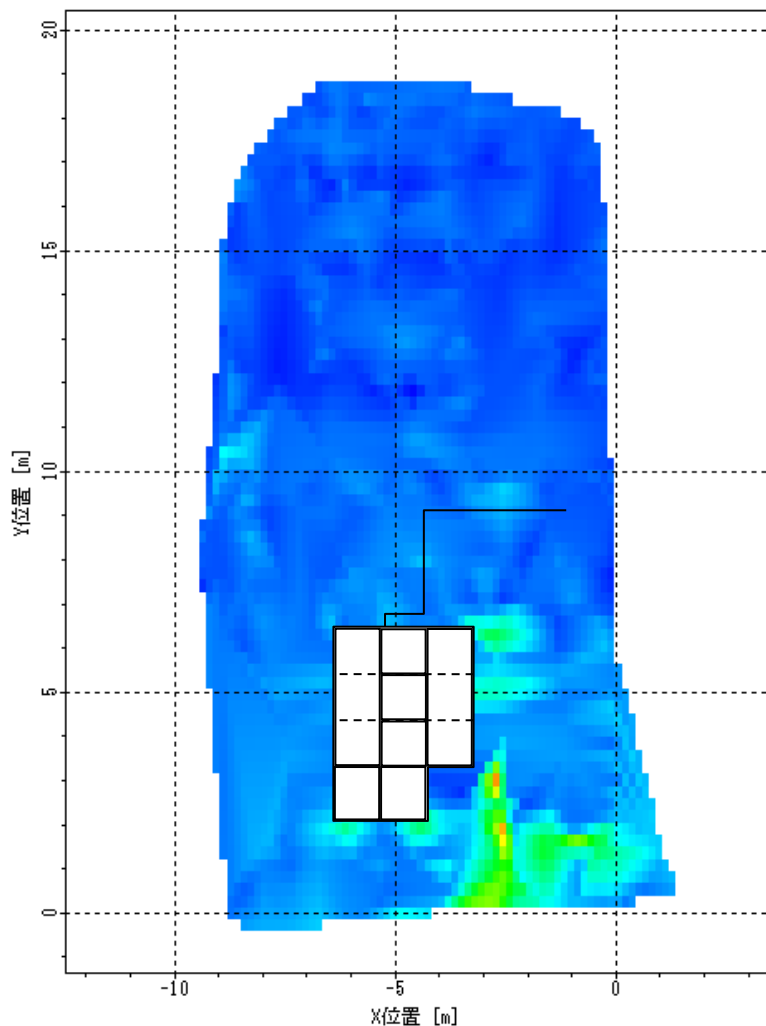
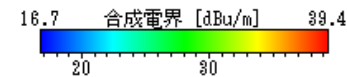
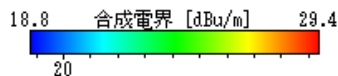


- Shielding Effectiveness
  - 60dB (30MHz ~ 200MHz)
  - 50dB (200MHz ~ 10GHz)
- AC Filter /DC filter spec.
  - 80dB (1M~10GHz)

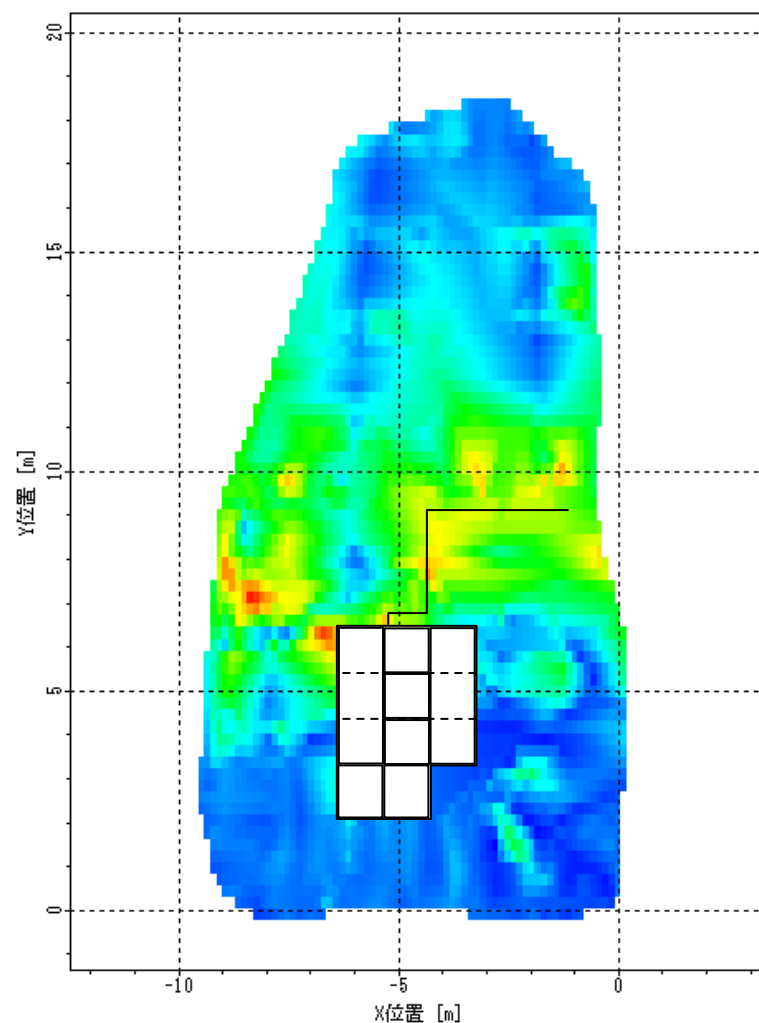


# Mitigation <AC filter and electromagnetic strength distribution>

Maintenance is very important for keep the shield level



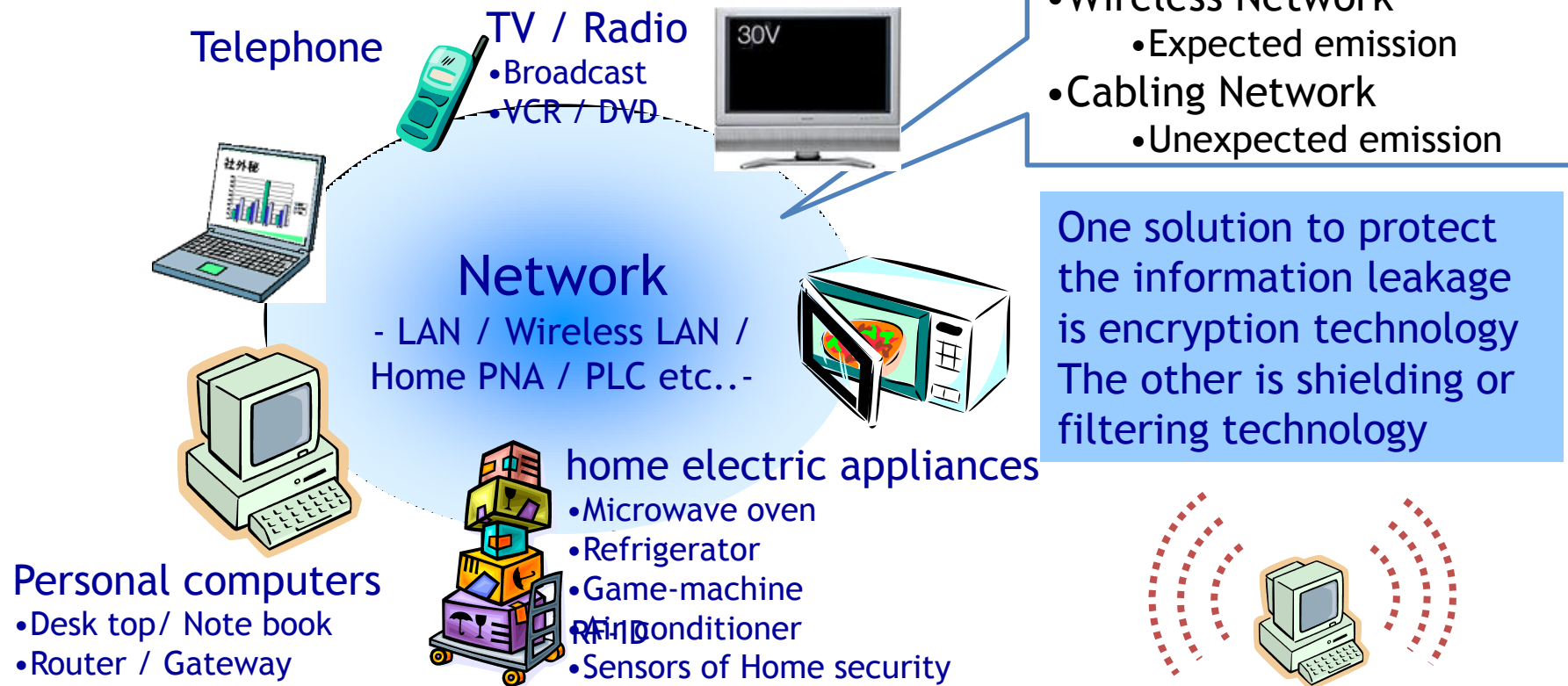
**With AC filter**



**Without AC filter**

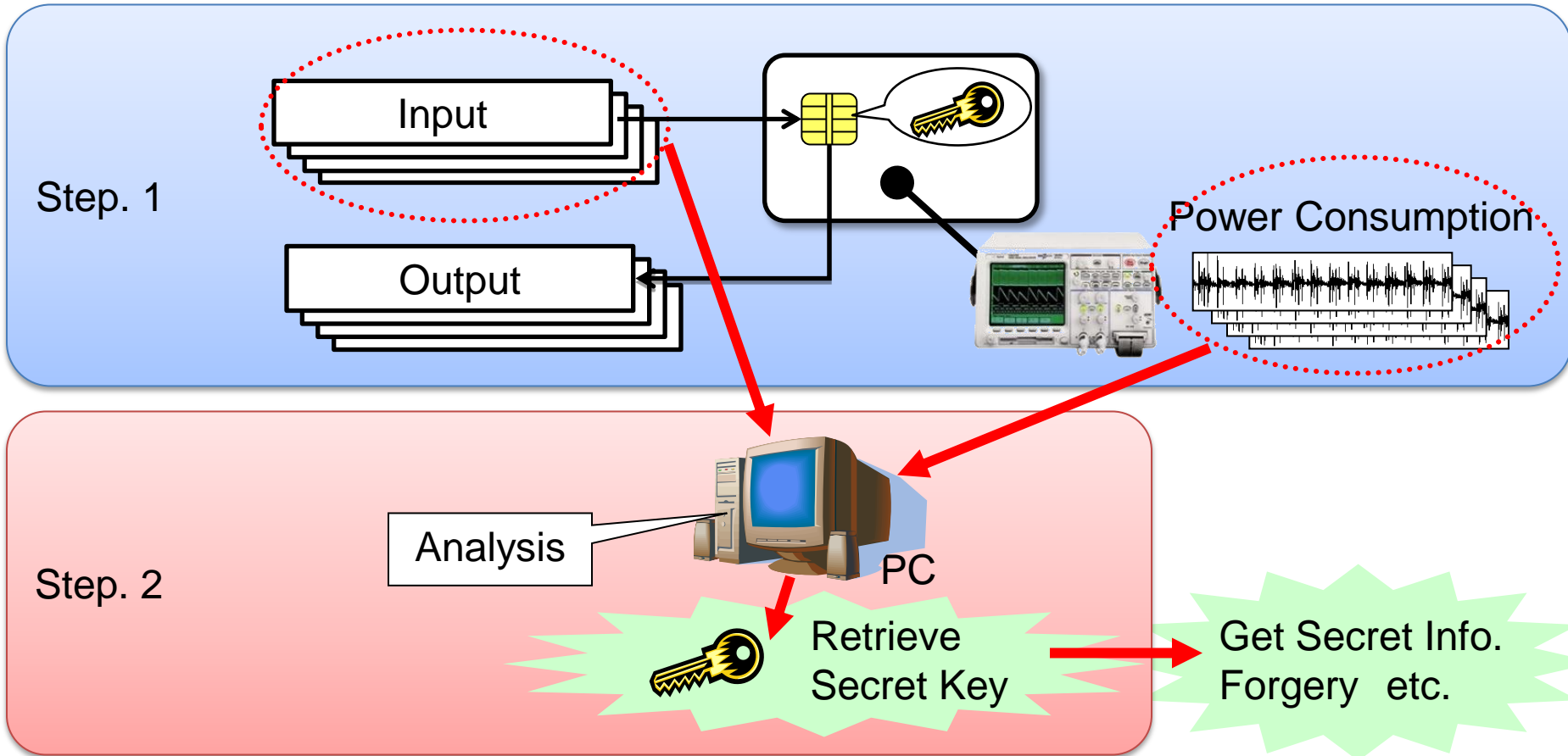


- A lot of appliances are connected with Home Network / Smart Grid
- A lot of Servers in Data centers



Smart – ( ) Safety and Security

Definitions are needed, for understanding each other EMC researcher and Cryptographic researcher



Differential Power Analysis ?

- Increasing to use of ICT for controlling such as Smart Grid, Smart community and so on.
- We have to keep safety and secure communication.
- The exact knowledge is required for adequate countermeasure or mitigation
- The exact knowledge; Definition of Threat, Mechanism, Evaluation Method, Mitigation Methods.
- We are welcome to your contributions.

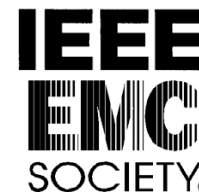
***Study Group 5  
Question 15***



***Technical Committee 77  
Sub Committee 77C***



***Technical Committee 5  
Sub Committee 2***



**Thank you**