Impact of Intentional EMI (IEMI) on the Critical Infrastructures

Dr. William Radasky, Ph.D., P.E.
Metatech Corporation
Goleta, CA
wradasky@aol.com

29 October 2015

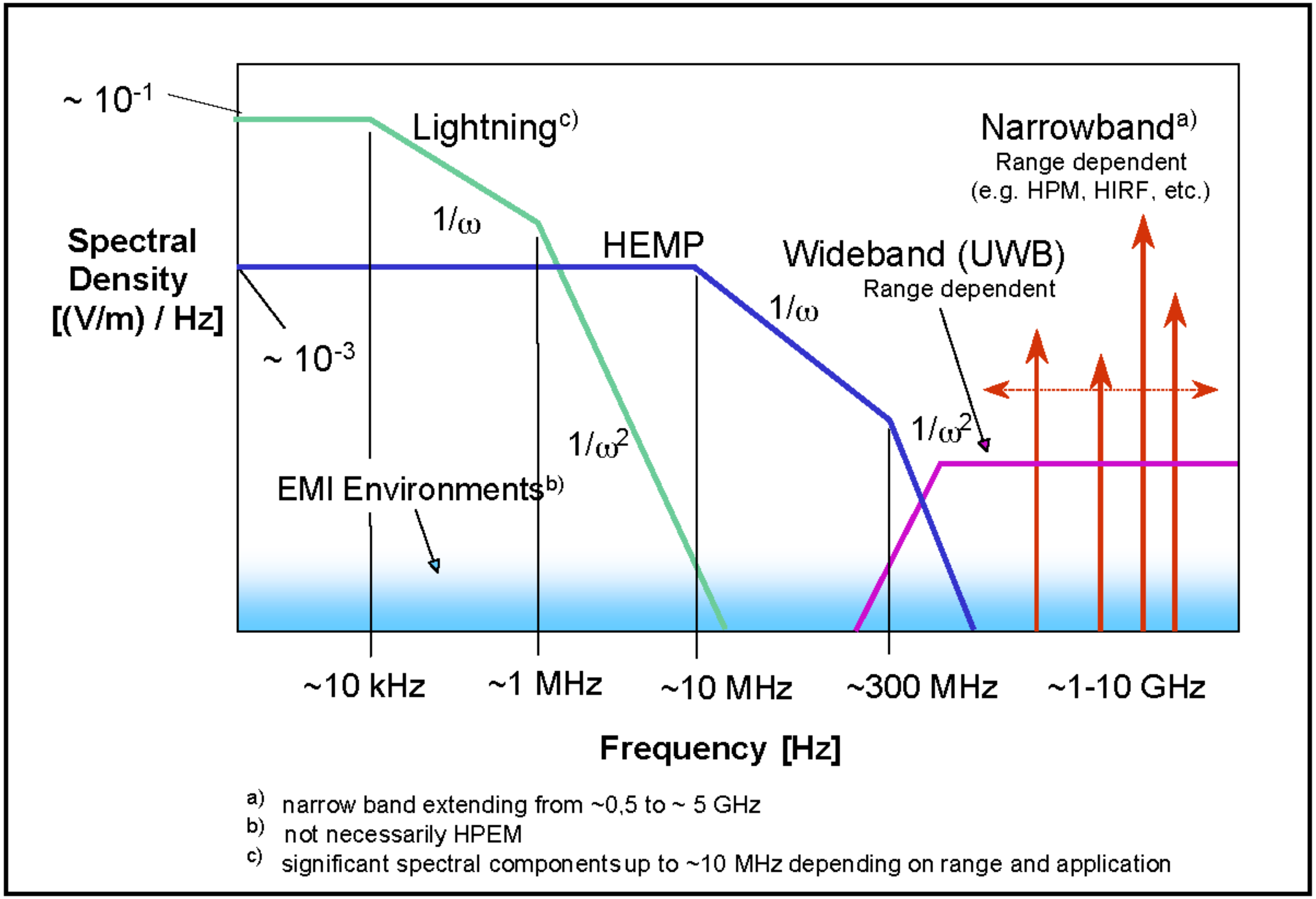
Metatech

Outline of Talk

- The IEMI Environment
- Impacts of IEMI on Electronics
- Impacts of IEMI on the Critical Infrastructures
- Assessment Methods and Protection
- Standards

The IEMI Environment

Comparison of Several EM Environments



Ref: IEC Standard 61000-2-13

What Exactly is Intentional EMI (IEMI)?

Definition:

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 purposes

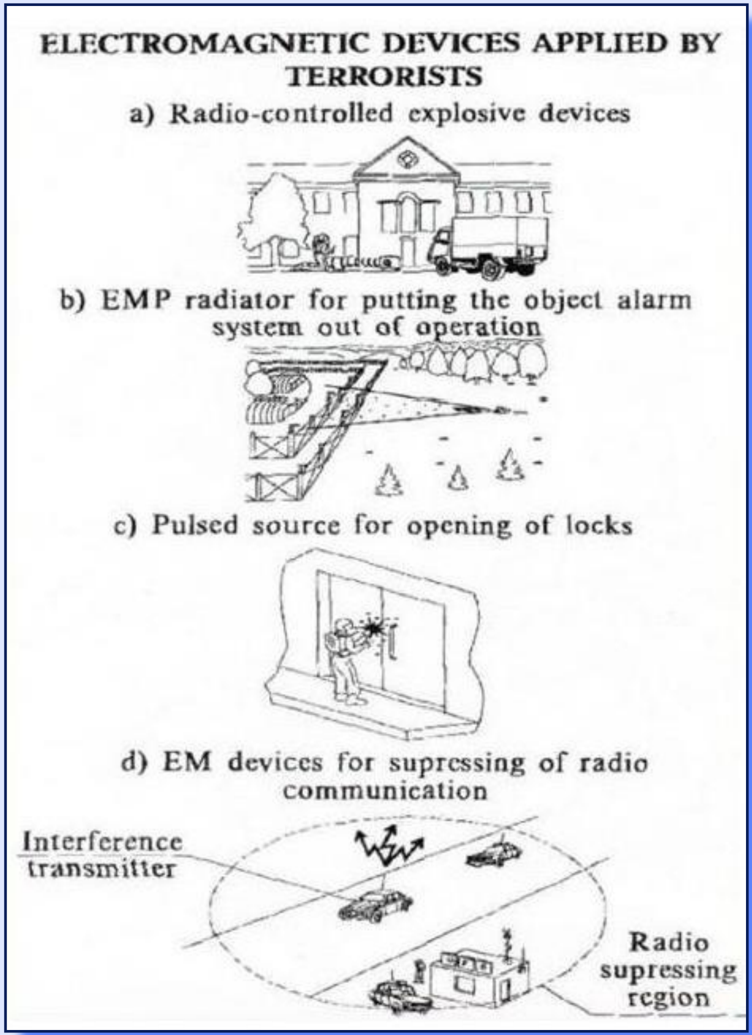
(Zurich EMC Symposium, February 1999;
Also IEC 61000-2-13:2005)

Why the IEMI Threat is of Concern

- Terrorist and criminal threats are increasingly of concern world-wide
- Intentional EMI is a new threat dimension
- Attractiveness of covert operations outside of physical barriers
- Technological advances in higher energy RF sources and antennas
- Increasing proliferation of IEMI sources and knowledge world-wide
- Increasing dependence on information and on automated mission-critical and safety-critical electronic systems
- Increasing EM susceptibility for new high density IT electronics working at higher frequencies and lower voltages

Metatech

IEMI Attacks in Russia



Reported by General Loborev at AMEREM in 1996

Blackmail

DIEU ET MON DROIT

THE SUNDAY TIMES

No 8,962 — 2 JUNE 1996 — Price £1

STYLE — Is this beauty? — ... NOT ACCORDING TO SCIENCE

1000 — FREE TODAY, PART 1 OF A SUPERB NEW SERIES PLUS 20-PAGE EURO 96 SUPPLEMENT

NEWS REVIEW — Lawson's deflation — SECRETS OF NIGEL LAWSON'S DIET

City surrenders to £400m gangs

INSIGHT

CITY of London financial institutions have paid huge sums to international gangs of sophisticated "cyber terrorists" who have amassed up to £400m worldwide by threatening to wipe out computer systems.

Banks, broking firms and investment houses in America have also secretly paid ransom to prevent costly computer meltdown and a collapse in confidence among their customers, according to sources in Whitehall and Washington.

An Insight investigation has established that British and American agencies are examining more than 40 "attacks" on financial institutions in London and New York since 1993.

Victims have paid up to £13m a time after the blackmailers demonstrated their ability to bring trading to a halt using advanced "information warfare" techniques learnt from the military.

According to the American National Security Agency (NSA), they have penetrated computer systems using "logic bombs" (coded devices that can be remotely detonated), electromagnetic pulses and "high emission radio frequency guns", which blow a devastating electronic "wind" through a computer system.

They have also left encrypted threats at the highest security levels, reading: "Now do you believe we can destroy your computers?"

The authorities have been unable to stem the attacks, which are thought to originate from the United States. In most cases, victim banks have failed to notify the police. "They have given in to blackmail rather than risk a collapse in confidence in their security systems," said a security director at one blue-chip merchant bank in the City.

A senior detective in the City of London police said: "We are aware of the extortion methods, but the banking community has ways of dealing with it and rarely reports to the police."

European and American police forces have set up special units to tackle the cyber criminals, who, Ministry of Defence sources believe, have netted between £200m and £400m globally over the past three years. But law enforcement agencies complain that senior financiers have closed ranks and are hindering inquiries.

Experts in the field of information warfare met in Brussels last month to discuss defensive measures. Representatives included Captain Patrick Tyrrell, assistant director of computer information strategy at the Ministry of Defence; General James McCarthy, professor of national security at the US Air Force Academy; General Jean Pichot-Duclos, director of the economic intelligence department of the French Defence Council, and senior figures from the civilian computer industries.

A separate closed meeting involving representatives from Whitehall and the intelligence community was held to analyse the 40 attacks on British and American financial centres since 1993. A further secret seminar took place in Washington this weekend.

Kroll Associates, the international investigating firm, confirmed last week that it had acted for financial institutions that have been blackmailed. "One of the problems we face is that the potential embarrassment from loss of face is very serious," said a spokesman in New York. Kroll had evidence that firms in London and New York had been targeted. "The problem for law enforcement is that the crime is carried out globally, but law enforcement stops at the frontier," he said.

Yesterday a Bank of England spokesman acknowleged the threat from the extortionists: "We are aware of this. It does exist. It is extortion and fraud." But the spokesman also insisted: "It is not the biggest issue in the banking market."

Scotland Yard is now taking part in a Europe-wide initiative to catch the cyber criminals and has appointed a senior detective from its computer crime unit to take part in an operation codenamed Lathe Gambit. Such is the secrecy that few details about the inquiry have emerged.

In America, the FBI has set up three separate units to investigate computer extortion.

The NSA believes there are four cyber gangs and has evidence that at least one is based in Russia. The agency is now examining four examples of blackmail said to have occurred in London:

- January 6, 1993: Trading halted at a broking house after blackmail threat and computer crash. Ransom of £10m paid to account in Zurich.
- January 14, 1993: a blue-chip bank paid £12.5m after blackmail threats.
- January 29, 1993: a broking house paid £10m in ransom after similar threats.
- March 17, 1995: a defence firm paid £10m in ransom.

In all four incidents, the gangs made threats to senior directors and demonstrated that they had the capacity to crash a computer system. Each victim conceded to the blackmailers' demands within hours and tranferred the money to offshore bank accounts, from which it was removed by the gangs within minutes.

The techniques have varied. In London, criminals posing as marketing firms have gained detailed knowledge of a target's system by interviewing the heads of information technology departments. In some cases, they have even issued questionnaires to unsuspecting

continued on back page

Prince Michael in new 'royal for rent' deal with PR firm

Five more CJD victims identified

Alleged blackmailing of banks in UK and US using "logic bombs, EM pulses and radio-frequency guns".

London Newspaper dated 2 June 2006

Background for the IEMI Threat

- Electromagnetic (EM) weapons possess an energy source (e.g. battery, capacitors) and an antenna
- They are designed to produce and propagate a high power EM field to a significant distance from the weapon
- These types of weapons have mainly been designed for military purposes
- The basic technology is not difficult to apply for a qualified engineer
- Commercial electronics equipment is not protected against these types of threats
- A new term has been used over the past 16 years to describe this threat and its effects on commercial equipment -- IEMI (Intentional Electromagnetic Interference)

Worldwide Scientific Activity in Protecting Commercial Systems Against IEMI

- URSI published a resolution in 1999 dealing with the criminal activities of EM “tools” and the need to protect against the emerging threat
- The International Electrotechnical Commission (IEC) SC77C (EMC: High Power Transient Phenomena) began writing standards to deal with this problem in 1999
- The IEEE EMC Transactions published a special issue on IEMI in August 2004
- Many EMC conferences are dealing with the subject of IEMI
- Private companies have developed methods of IEMI threat assessments and protection methods

Narrowband Waveforms

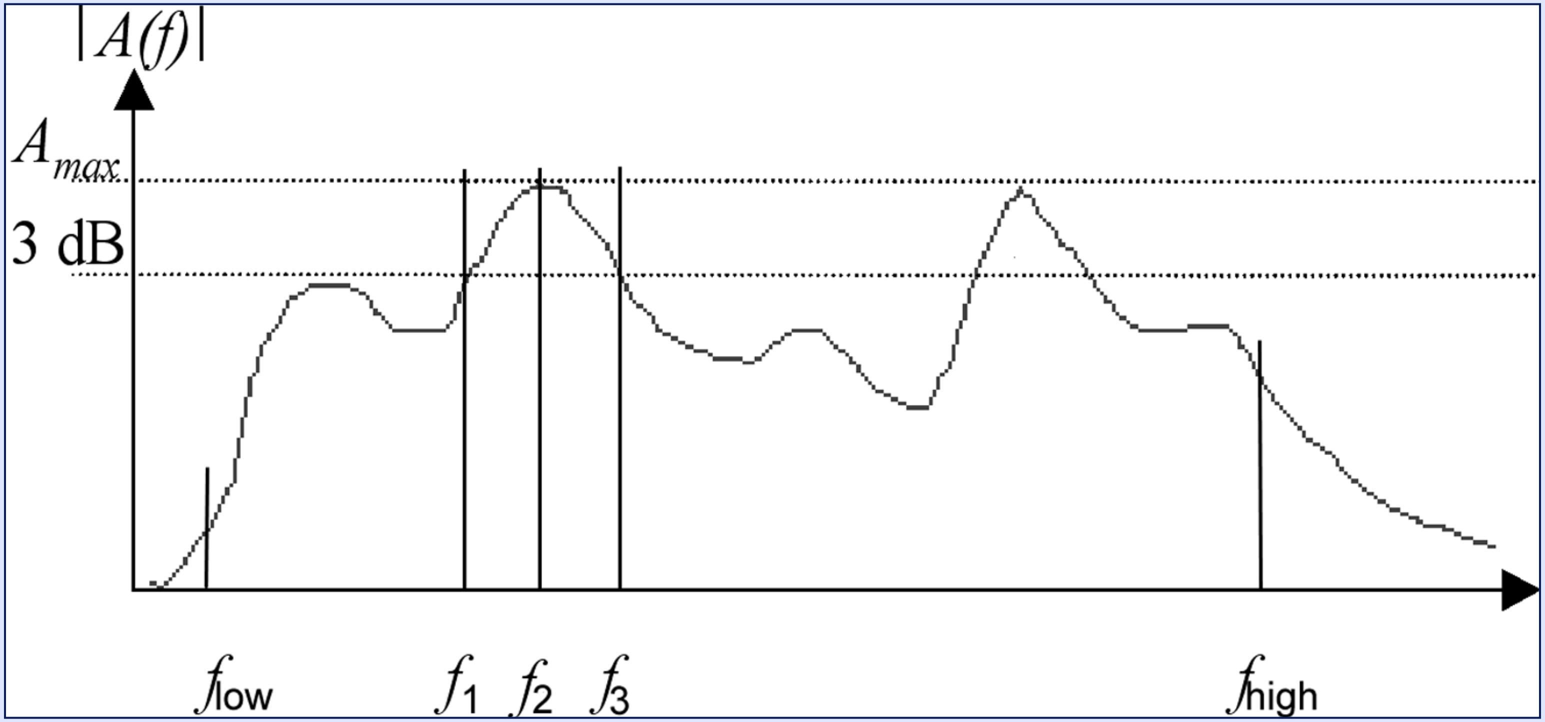
- Nearly single frequency (Percent BW < 1%) high power and energy signal in a pulse with duration up to microseconds and usually radiated within the band 0.3 – 3 GHz
- Pulses can be repetitive, and frequency can vary with time and/or be modulated
- Maximum coupling occurs if tuned to a significant resonance in system transfer function
- May cause permanent damage when system communication frequencies are matched
- Many systems have significant resonance susceptibilities at only particular frequencies, thereby limiting the threat from a single frequency generator
- Note: These threats should not be referred to as HPM as the term is not well-defined and also not all threats are in the microwave range

Metatech

Wideband Waveforms

- A single pulse produces frequency and energy content over a wide range of frequencies. The pulse may be repeated.
- Main frequency content and power is spread over a very broad spectrum usually within 0.3 – 3 GHz. Bandratio (90% of energy) is used instead of percent bandwidth
- Multiple system resonances can be stimulated simultaneously
- Energy produced in a single pulse is spread over many frequencies
- More likely to cause interference than permanent damage as coupling is through unintentional (and indirect) coupling paths
- Note: These should not be called UWB waveforms as this description has no clear technical meaning.

Spectrum Evaluation of Bandratio (IEC 61000-2-13)



Note: 3 dB bandwidth does not represent the range of frequencies over which 90% of the waveform energy is found.

Bandwidth Definitions (IEC 61000-2-13)

	Percentage Bandwidth	Bandratio
hypoband or narrowband	$< 1\%$	< 1.01
mesoband	$1\% < \text{pbw} \leq 100\%$	$1.01 < \text{br} \leq 3$
sub-hyperband	$100\% < \text{pbw} < 163.4\%$	$3 < \text{br} \leq 10$
hyperband	$163.4\% < \text{pbw} < 200\%$	$\text{br} \geq 10$

$$\text{band ratio} = \text{br} = \frac{f_h}{f_l}$$

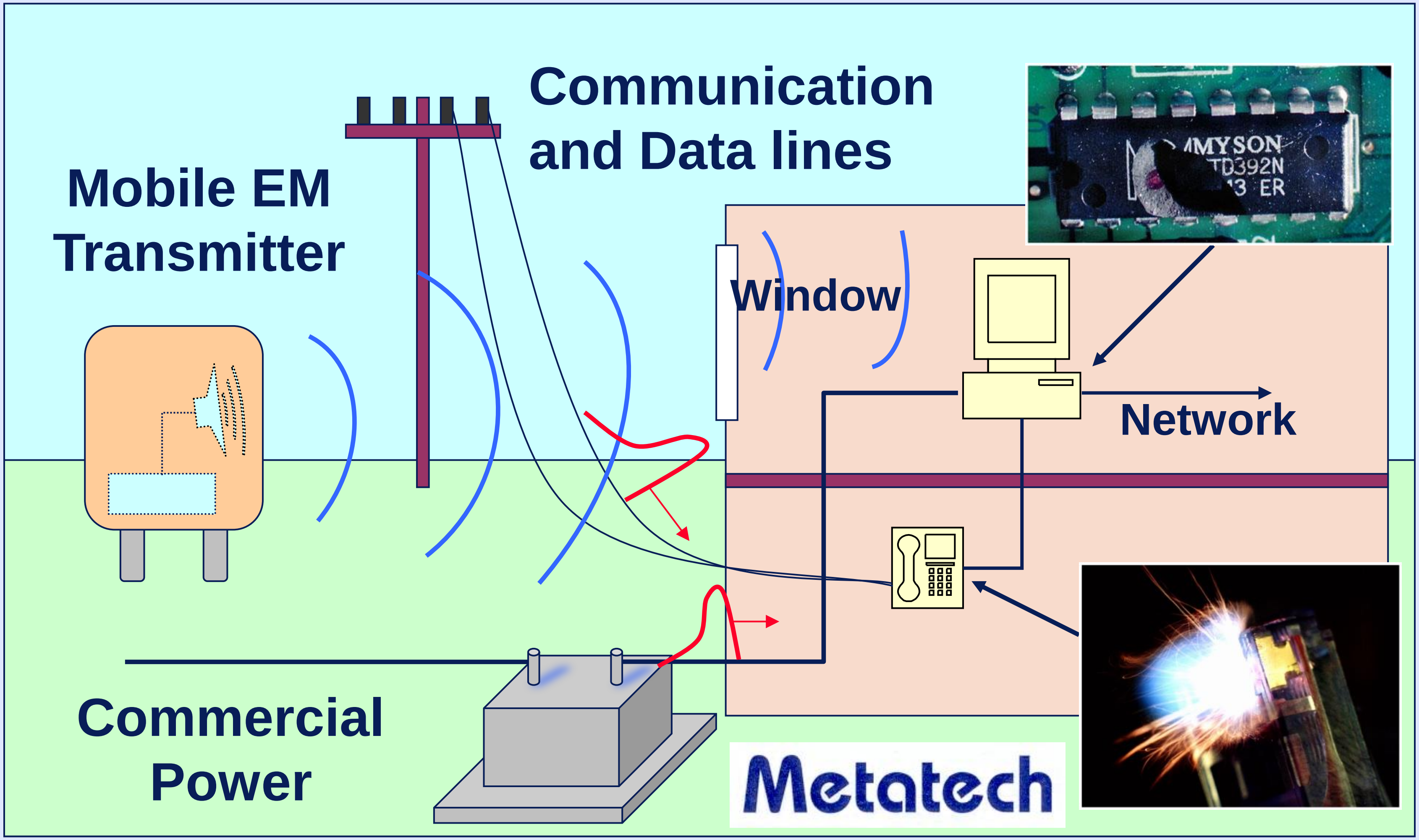
$$\text{band ratio decades} = \text{brd} = \log_{10}(\text{br})$$

$$\text{pbw} = 200\frac{(br-1)}{(br+1)}$$

$$\text{br} = \frac{[1+\frac{pbw}{200}]}{[1-\frac{pbw}{200}]}$$

Metatech

Coupling Paths for Radiated IEMI Fields



Diehl EM Emitter

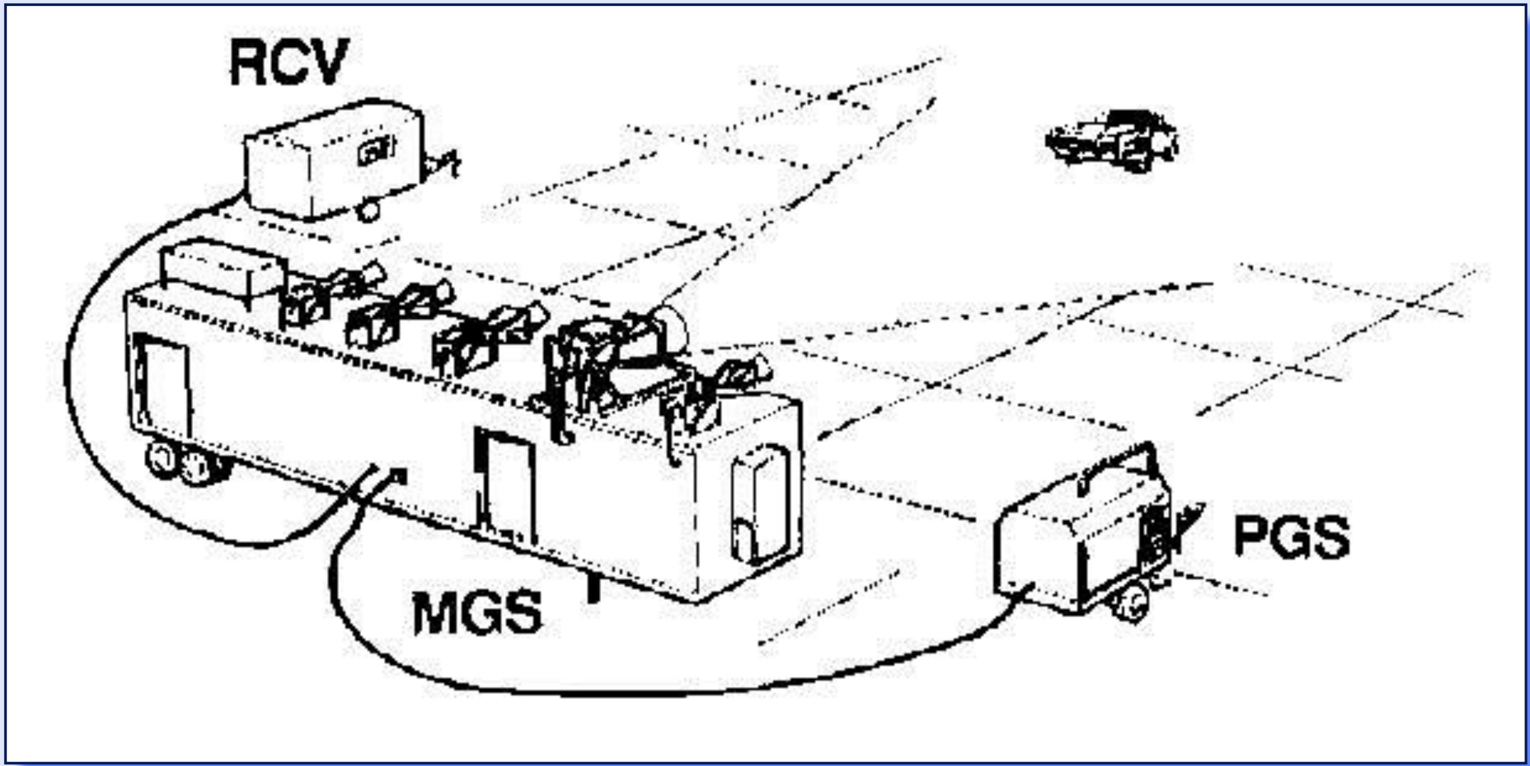
- Diehl Munitions Systeme has developed a small interference source (including an antenna)
  - 350 MHz damped sine field
  - 120 kV/m at 1 meter (omni-directional antenna)
  - 30 minute continuous operation (5 pulses per second) or 3 hours in bursts
  - 20 x 16 x 8 inches and 62 pounds
- Demonstration in Summer 2004 at EUROEM
- Improved versions of this source have been developed since then

JOLT IRA Hyperband Generator

- AFRL has developed an extremely powerful IRA system that produces hyperband pulses
  - E*r = 5.3 MV
  - pulse width ~1 ns

Impacts of IEMI on Electronics

Automobile Testing (Narrowband Radiated Fields)



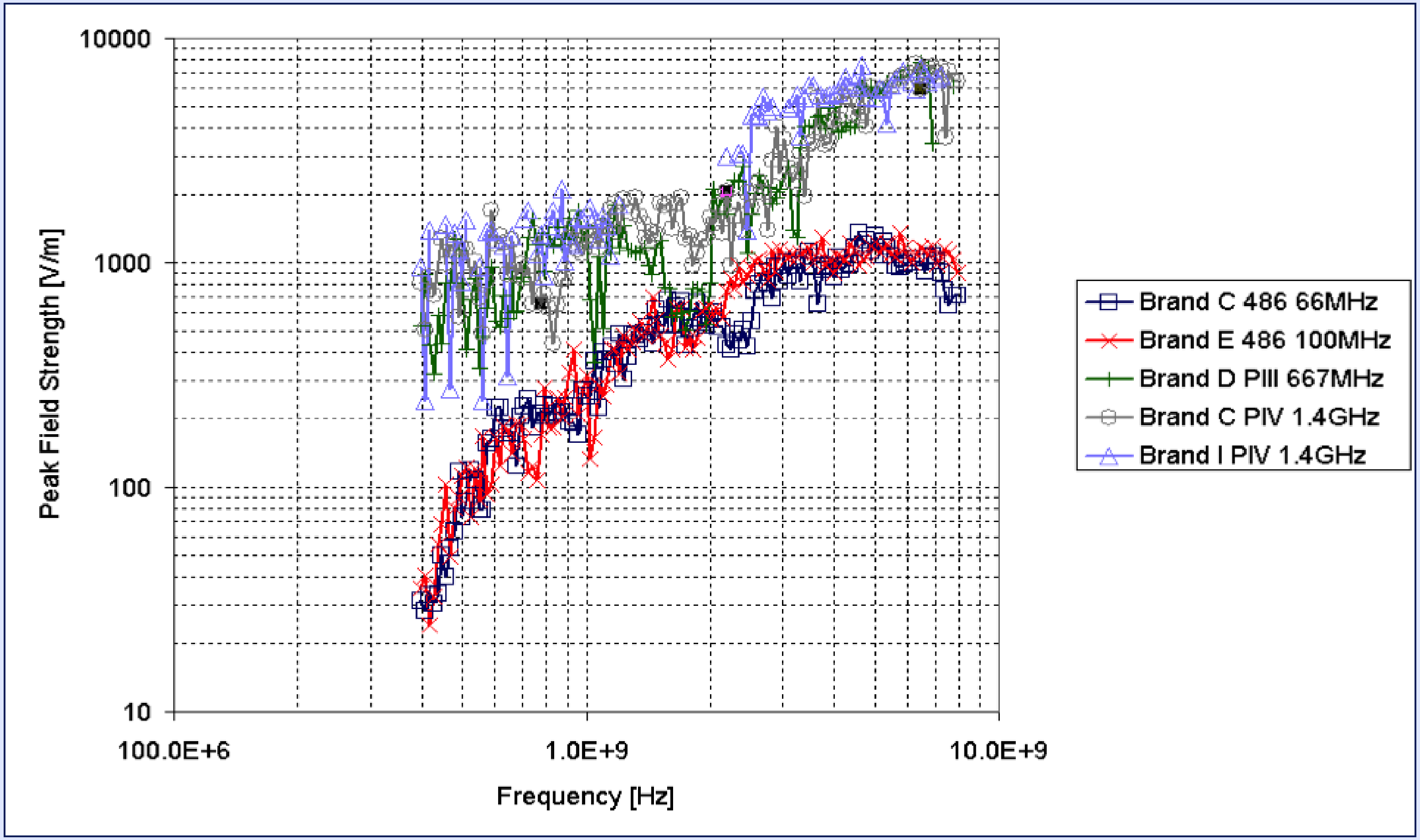
Source: Dr. Mats Bäckström, Zürich EMC Conference 1999

Susceptibility of Automobiles to Narrowband Radiated Fields

- Fixed frequencies between 1.3 – 15 GHz were tested
- Most prominent effects at the lower test frequencies, also when the car was not operating. Types of damage observed included: engine control units, relays, speedometer, revolution counter, burglar alarm, and a video camera.
- Upset (engine stop): 500 V/m
- Permanent damage: 15 kV/m at 1.3 GHz
24 kV/m at 2.86 GHz
- Note: This testing was for automobiles built in the middle 1990s – not for today's automobiles

Source: Dr. Mats Bäckström, Zürich EMC Conference 1999

Narrowband Testing of PCs

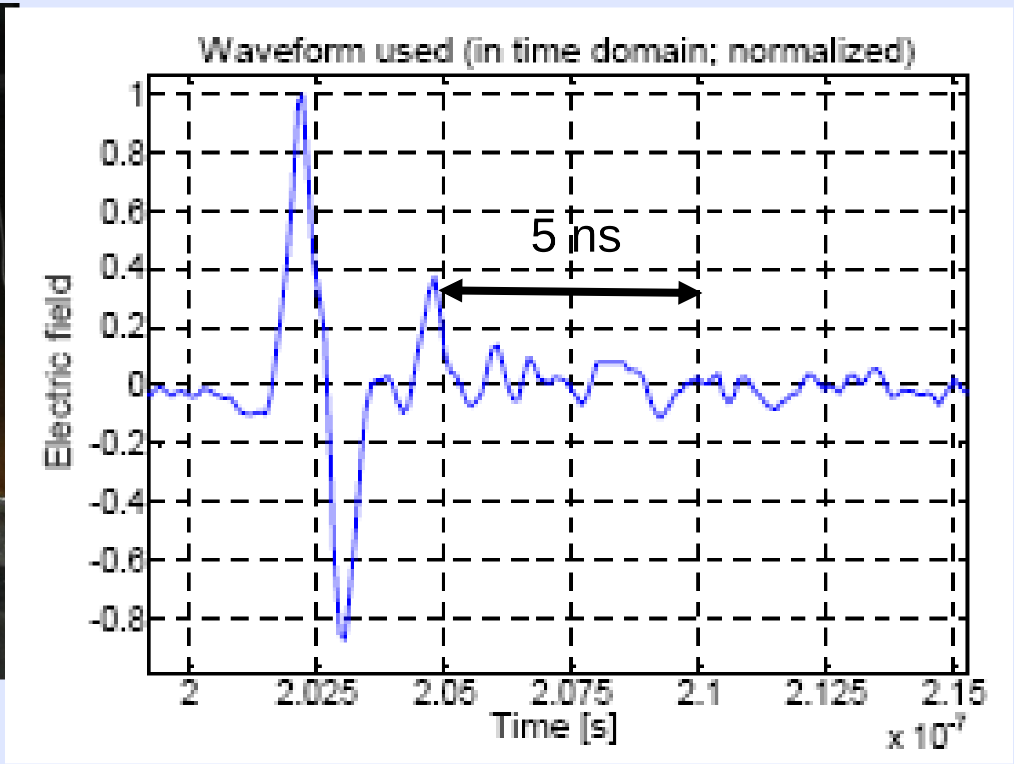


Hoad, R., Carter, N., Herke, D. and Watkins, S., "Trends in EM Susceptibility of IT Equipment," IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, August 2004.

Metatech

Radan 303B (Hyperband) GPS Testing

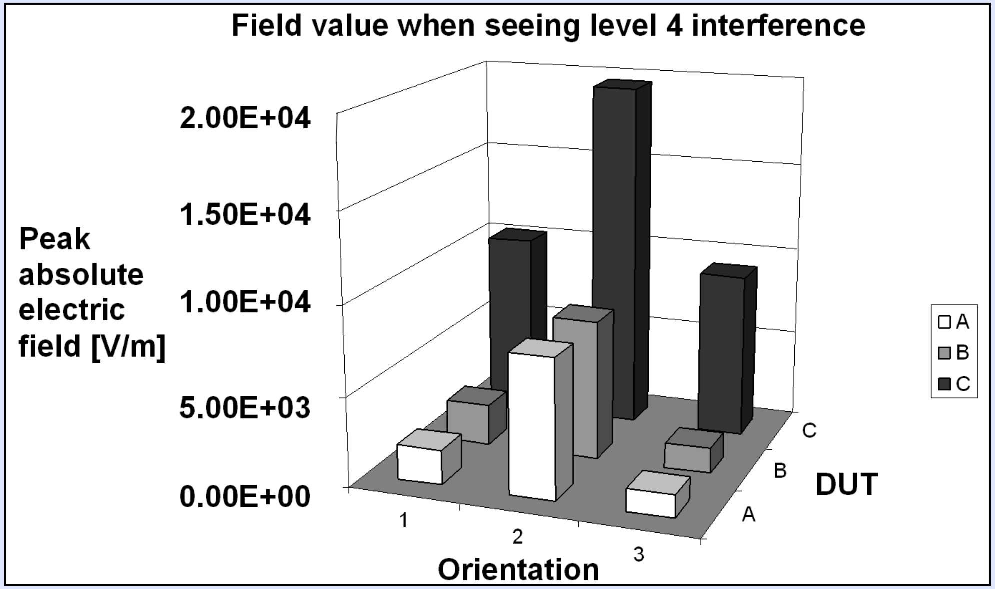
Tests performed by Nillson and Månsson



Radan Time Waveform

GPS Test Results

Orientation 1 – as in figure
Orientation 2 – lying down on the back the top towards the RADAN
Orientation 3 – as Orientation 1 but turned 90˚ sideways



Failure level 4 (Crash, Operator intervention) for GPS receivers for different orientations. Mono pulse. Peak electric field.

Månsson, D., Thottappillil, R., Nilsson, T., Lundén, O. and Bäckström, M., “Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation,” IEEE Transactions on Electromagnetic Compatibility, Vol. 50, No. 2, pp. 434-437, May 2008.

Susceptibility of Electronic Cash Machines (ECM) to Wideband Radiated Fields (Hyperband)

Upset levels

ECM type	Sample 1	Sample 2
Critical level of peak field, kV/m	2.3 – 2.5	2.2 – 2.4

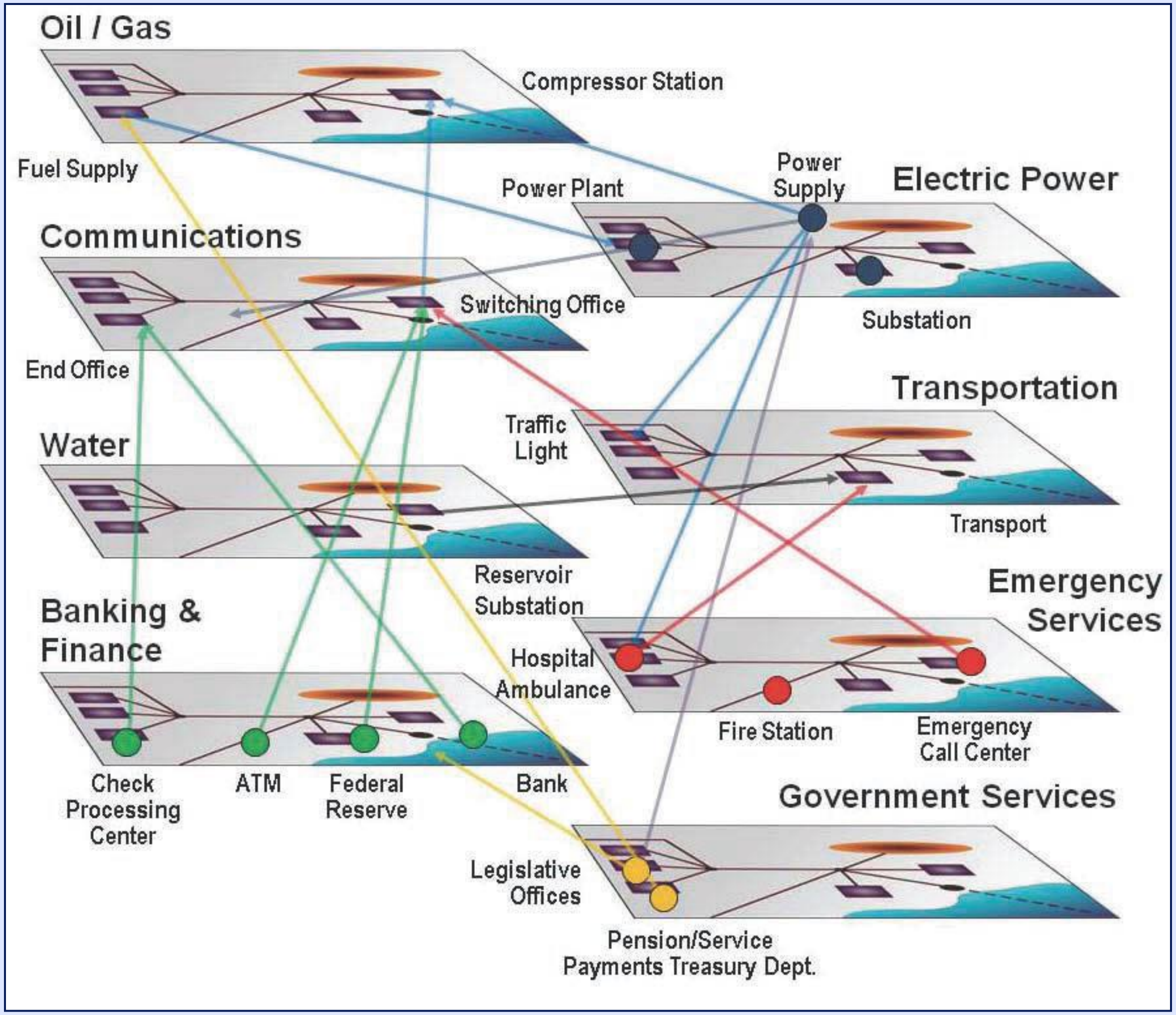
Levels of damage

Level of peak field, kV/m	2.5	3.1	3.9	4.4	4.8	5.1
Result	Upset	Upset	Upset	Upset	Upset	Damage

Source: Dr. Yuri Parfenov, IHED, Russia, Presented at EUROEM 2004

Impacts of IEMI on the Critical Infrastructures

Interdependencies of the Critical Infrastructures



Ref: "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," EMP Commission, April 2008/

Impacts of IEMI on Power System

- The IEMI electromagnetic fields are in a similar (but higher) frequency band as the E1 HEMP
- The impacts on the power grid will be similar to those from E1 HEMP
  - Substation control electronics can be affected by nearby EM weapons
  - Control center computer operations could be affected
  - Power generation controls are also at risk
- Major difference is that the IEMI is a local threat and therefore does not approach the same exposure area level as E1 HEMP, unless a coordinated attack is performed
- Protection methods for the electronics will be similar for IEMI and E1 HEMP
  - In addition security measures such as physical separation of attack locations can be used for IEMI

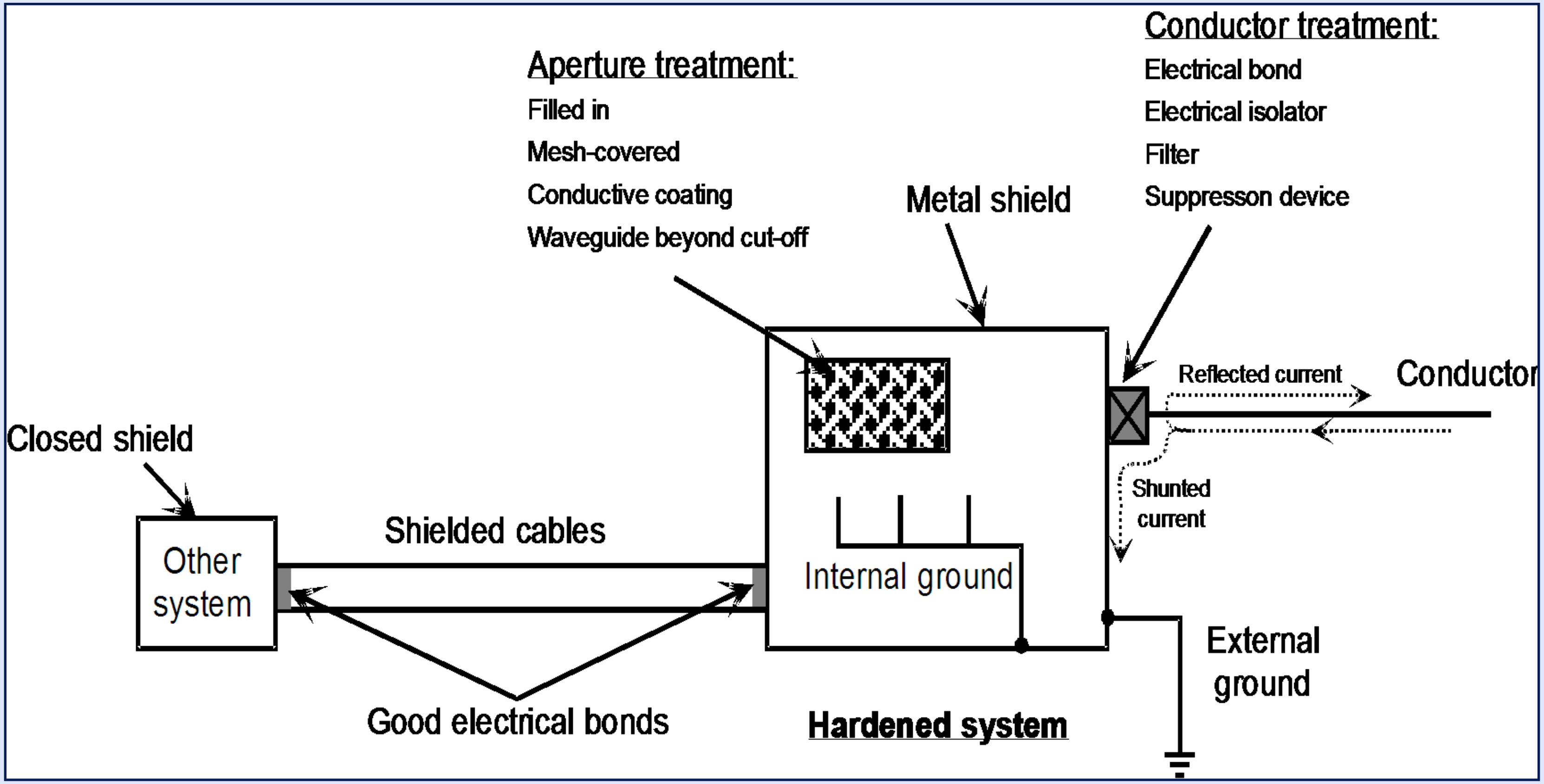
Shielding Effectiveness Measurements of Power System Buildings

Shielding Measurements		
Nominal Shielding, dB	Room	Shielding, dB
0	All wooden bldg	2
5	Room under wood roof	4
	Wood bldg-room 1	4
	Concrete – no rebar	5
	Wood bldg-room 2	6
10	Conc.+rebar-room 1	7
	Conc.+rebar-room 2	11
	Conc.+rebar-room 3	11
20	Conc.+rebar-room 4	18
30	Metal bldg	26
	Conc.+rebar-well prot. room	29

Metatech

Assessments Methods and Protection

EM Protection Approach for New Buildings



Ref: IEC 61000-1-5

IEMI Assessment Steps for Existing Buildings

- Building shielding effectiveness
  - — Measure building EM attenuation
- External EM
  - — IEMI: Select IEMI weapon parameters, determine closest stand-off distance, and calculate EM levels at the building
- Internal EM field levels
  - — Apply building attenuation to external EM levels
- Cable coupled voltages
  - — Identify cable lengths
  - — Apply statistical coupling approach, using EM levels and cable lengths
- Equipment vulnerability voltages
  - — Determine dominant internal equipment and estimate typical upset and damage voltage levels
- Protection deficit
  - — Protection needed: compare induced voltages and vulnerability levels
- Protection measures
  - — Review options for lowering coupled voltage or strengthening equipment

IEMI Protection Options

- Improve the building/room shielding effectiveness
  - External metal sheeting
  - Internal metallic walls
  - New metallic building
  - Shield rooms or racks
- Improve shielding of internal cabling
- Replace metallic with fiber optic cables
- Apply cable ferrites on metallic cables
- Add filters and/or surge arresters at metallic cable connections
- Improve security measures for IEMI (distance, monitoring, etc.)

Standards

Use of IEC Publications for HEMP and IEMI Mitigation

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; -36 IEMI Immunity Test Methods
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; -10 Application Guide
61000-6- (Generic Standards)	-6 Generic Standard For HEMP Immunity

Outline for IEC 61000-5-10, "Guide to the Application of IEC SC 77C HEMP and IEMI Publications"

1 Scope
2 Normative References
3 Terms and Definitions
4 General Introduction
5 Development of the Environment Levels
  5.1 High-altitude Electromagnetic Pulse (HEMP)
  5.2 Intentional Electromagnetic Interference (IEMI)
6 Protection and Testing Approach for New Facilities
  6.1 HEMP Protection for New Facilities
  6.2 IEMI Protection for New Facilities
  6.3 HEMP and IEMI Protection for New Facilities
7 Protection and Testing Approach for Existing Facilities
  7.1 HEMP Protection for Existing Facilities
  7.2 IEMI Protection for Existing Facilities
  7.3 HEMP and IEMI Protection for Existing Facilities
8 Bibliography

Metatech

More Information on IEMI Standardization

- Most of the basic standardization of IEMI fields, test methods and protection methods have been published by IEC SC 77C
- Other organizations have used the IEC basic standards to develop application standards
  - ITU-T K.81, “High-power electromagnetic immunity guide for telecommunication systems,” November 2009.
  - Cigré WG C4.206, “Protection Of The High Voltage Power Network Control Electronics Against Intentional Electromagnetic Interference (IEMI),” Technical Brochure 600, November 2014.
  - IEEE 1642, “Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI,” January 2015.
- As mentioned in this presentation, the IEC will produce its own applications standard (IEC 61000-5-10) for both IEMI and HEMP

Thank you for your attention!