UPPSALA
UNIVERSITET

Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 549

Intentional Electromagnetic Interference (IEMI)

Susceptibility investigations and classification of civilian systems and equipment

DANIEL MÅNSSON

ACTA
UNIVERSITATIS
UPSALIENSIS
UPPSALA
2008

ISSN 1651-6214
ISBN 978-91-554-7272-6
urn:nbn:se:uu:diva-9264

Dissertation presented at Uppsala University to be publicly examined in Häggsalen, Ångströmslaboratoriet, Lägerhyddsvägen 1, Uppsala, Friday, October 3, 2008 at 13:00 for the degree of Doctor of Philosophy. The examination will be conducted in English.

Abstract
Månsson, D. 2008. Intentional electromagnetic interference (IEMI). Susceptibility investigations and classification of civilian systems and equipment. Acta Universitatis Upsaliensis. *Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology* 549. 127 pp. Uppsala. ISBN 978-91-554-7272-6.

This PhD thesis addresses the threat posed to society by sources that can produce high power electromagnetic pulses (HEPM) and be used maliciously to disturb or damage electronic equipment. The vulnerability from intentional electromagnetic interference (IEMI) has increased in the recent decades due to the widespread dependence of the civil society on sensitive electronic systems and proliferation of radiation sources.

As the characteristics of the disturbances associated with IEMI often have very high frequency content, the existing mitigation measures and protection components may not be adequate. It was seen that for ultra wideband (UWB) transients low voltage protection components may not work as intended, due to parasitic components that arises from the packaging of the device.

The large spatial distribution of many civilian facilities and critical infra-structures (e.g., power generation, communications, train system, etc.) presents many unexpected ports for an attacker as the majority of the parts of these systems are not protected or secure.

As the new European Rail Traffic Management System (ERTMS) will utilize wireless communication for communication and control of the trains the vulnerability from different radiating HPEM sources was investigated. Angles of incidence and frequencies that are a threat in a given situation are identified.

Due to the possibility of unexpected ports, the propagation of differential mode ultra wideband transients in low voltage power networks, when injected into a power socket of a facility, was studied. The effects on the transient propagation from cable bends, switches and junctions were studied, both in a laboratory setup and in the network of a facility.

Also, as modern electronic equipment and systems may not be tested for waveforms and disturbances other than standardized EMC tests, experiments on some common commercial-off-the-shelf (COTS) equipment were performed with non-standard test situation. It was seen that these could easily be disturbed or even permanently damaged.

In addition, due to the inherent difficulties with IEMI, a new method for classifying facilities from IEMI is suggested. It is based on available terminology of accessibility (A), susceptibility (S) and consequence (C), but expands these and forms the so called IEMI/ASC-cube.

Keywords: Electromagnetic compatibility, Intentional electromagnetic interference, High power electromagnetic

Daniel Månsson, Department of Engineering Sciences, Box 534, Uppsala University, SE-75121 Uppsala, Sweden

ISSN 1651-6214
ISBN 978-91-554-7272-6
urn:nbn:se:uu:diva-9264 (http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-9264)

“Shall I refuse my dinner because I do not fully understand the process of digestion?”

Oliver Heaviside (1850-1925)

DON’T PANIC

Till min familj och alla mina vänner, nära och kära.
Tack för all er hjälp och ert tålamod.

List of papers

I **Månsson, D** and Thottappillil R, "*Comments on "Linear and Nonlinear Filters Suppressing UWB Pulses*" ", IEEE Transactions Electromagnetic Compatibility, Vol. 47, No. 3, 671-672, August 2005.

II **Månsson**, **D.**; Nilsson, T.; Thottappillil, R.; Bäckström, M., "*Propagation of UWB Transients in Low-Voltage Installation Power Cables*", IEEE Transactions on Electromagnetic Compatibility, Vol. 49, Issue: 3, pp. 585-592, Aug. 2007

III **Månsson, D.**; Thottappillil, R.; Bäckström, M. "*Propagation of UWB transients in low-voltage power installation networks*", IEEE Transactions on Electromagnetic Compatibility, Vol. 50, NO. 3, pp. 619-629, Aug. 2008.

IV **Månsson, D.**; Thottappillil, R.; Bäckström, M.; Lundén, O., "*Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI*", IEEE Transactions on Electromagnetic Compatibility, Vol. 50, NO. 1, pp. 101-109, Feb. 2008.

V **Månsson, D**.; Thottappillil, R.; Nilsson, T.; Lundén, O.; Bäckström, M., "*Susceptibility of Civilian GPS Receivers to electromagnetic radiation*", IEEE Transactions on Electromagnetic Compatibility, Vol. 50, NO. 2, pp. 434-437, May 2008.

VI **Månsson, D**.; Thottappillil, R.; Bäckström, M., "*Methodology for Classifying Facilities with respect to Intentional EMI*", Submitted to IEEE transactions on Electromagnetic Compatibility (April 2008)

VII **Daniel Månsso**n, Tony Nilsson, Rajeev Thottappillil and Mats Bäckström, "*Susceptibility of GPS Receivers and Wireless Cameras to a single Radiated UWB Pulse*", Proceedings of EMC Europe, Barcelona, Spain (2006)

VIII **D. Månsson**, J. Ericsson, R. Thottappillil, "*Effect of conducted EFT type pulses on the point of entry of electrical systems in buildings*", RadioVetenskap och Kommunikation (RVK05), Linköping, June-14-16, 2005.

Examples of other contributions of the author, not included in this thesis

- **D. Månsson** and R. Thottappillil, "*The Threat of Conducted High Power Electromagnetic Pulses in Civilian Facilities*", Proceeding's of the E3 2007 (EMC, ESD och Elsäkerhet) conference, 17- 18 April, 2007, Gothenburg, Sweden
- R. Thottappillil , **Daniel Månsson**, Nelson Theethayi, Mats Bäckström, Tony Nilsson, Göran Undén, Barbro Nordström, Per Bohlin, Per Anders Lindeberg, Ulf Hellström, Peter Lindeberg, Georg Bohlin, Mihael Zitnik, Lise Ekenberg, "*Response of Civilian Facilities to Intentional Electromagnetic Interference (IEMI), with Emphasis on the Swedish Railway Network*", EMC Europe Workshop, Rome , Sept. 19-21, 2005.
- T. Nilsson, **D. Månsson**, M. Bäckström,"*HPM and UWB Susceptibility of GPS Receivers*", AmerEM06, July 2006, Albuquerque, USA
- **Daniel Månsson**, Rajeev Thottappillil, Mats Bäckström, "*Propagation Ability of UWB Transients through Junctions of Low-voltage Power Installation Cable*", Paper 96,19th International Zurich Symposium on Electromagnetic Compatibility, Singapore, May 19 - 22, 2008
- Raul Montaño, Mats Bäckström, **Daniel Månsson**, Rajeev Thottappillil, "*On the Response and Immunity of Critical Infrastructures Against IEMI – Current Swedish Research Initiatives*", Paper 245, 19th International Zurich Symposium on Electromagnetic Compatibility, Singapore, May 19 - 22, 2008
- Rajeev Thottappillil, **Daniel Månsson**, Mats Bäckström, "*Susceptibility of Electrified Railway Facilities to Intentional Electromagnetic Interference*", RVK08, Växjö, June 9-11, 2008
- Rajeev Thottappillil, **Daniel Månsson**, Mats Bäckström, "*Response of Electrified Railway Facilities to Intentional Electromagnetic Interference: Review of Research at Uppsala University*", Paper 105, 19th International Zurich Symposium on Electromagnetic Compatibility, Singapore, May 19 - 22, 2008
- **Daniel Månsson**, Olof Lundén, Rajeev Thottappillil and Mats Bäckström, "*The scenario of intentionally radiated electromagnetic interference to railway systems*", Proceeding of the EMC Europe Workshop 2007, June 14 - 16, 2007, Paris

Contents

Abbreviations

COTS	Commercial off the shelf
DC	Direct current
DS	Damped sinusoidal
EFT	Electrically fast transients
EM	Electromagnetic
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EMP	Electromagnetic pulse
ERTMS	European rail traffic management system
ESD	Electrostatic discharge
FDTD	Finite-difference time-domain
FWHM	Full width at half maximum
GDT	Gas discharge tube
GPS	Global positioning system
GSM-R	Global system for mobile communications - railway
HEMP	High altitude electromagnetic pulse
HERF	High energy radio frequency
HPEM	High power electromagnetic
HPI	High power impulse
HPM	High power microwave
IEMI	Intentional electromagnetic interference
IRFI	Intentional radio-frequency interference
LEMP	Lightning electromagnetic pulse
MOV	Metal oxide varistor
MTL	Multiconductor transmission line
POE	Point of entry
SPD	Surge protective device
TE	Transverse electric
TEM	Transverse electromagnetic
TL	Transmission line
TM	Transverse magnetic
UWB	Ultra wideband

1 Introduction

In Chapter 1, we will acquaint ourselves with the method of scientific investigation in general and how the procedure of acquiring knowledge through science works. A (very brief) history lesson surrounding electromagnetism will be given which will be followed by the basic equations for electromagnetism. A general introduction to the applied fields of electromagnetic compatibility, as well as that of the new areas (compared to electromagnetism) of high power electromagnetic and intentional electromagnetic interference, also known as electromagnetic terrorism, will be given.

1.1 Scientific investigation

The content of this subchapter is based on [1]. What is science? What distinguish science from that of other belief systems? The definition of science from Webster's online dictionary is:

> "Knowledge or a system of knowledge covering general truths or the operation of general laws especially as obtained and tested through scientific method [and] knowledge concerned with the physical world and its phenomena".

However a more thorough definition would be:

> "Science is the systematic procedure through which reproducible knowledge of the surrounding physical world is obtained and tested for reliability and correlation with past observed events as well as prediction of future outcome, through the use of scientific methods".

Compared to knowledge and ideas "obtained" by pseudo-sciences or different religions, scientific theorems and laws are never claimed to be complete or finished (see fig. 1). A constant clarification and validation of the "truths" presented by different branches of science are made. The battles between different researchers and theories are encouraged since this will, as with the natural selection in nature, remove the theories and hypothesizes that are wrong. No theory deduce by the scientific methods stands unchallenged in the face of improvement or correction. The best example is the law of gravitation as described by Sir Isaac Newton, which can for many situations accu-

rately describe the motion of moving bodies. However it was proven faulty for speeds approaching that of light or in the vicinity of a very large mass. This is a case where the validity of the scientific laws were improved to extend, and more accurately described, more situations. In the case of the shape of the earth (flat versus spherical) and alchemy, the theories where proven wrong and discarded for better theories.

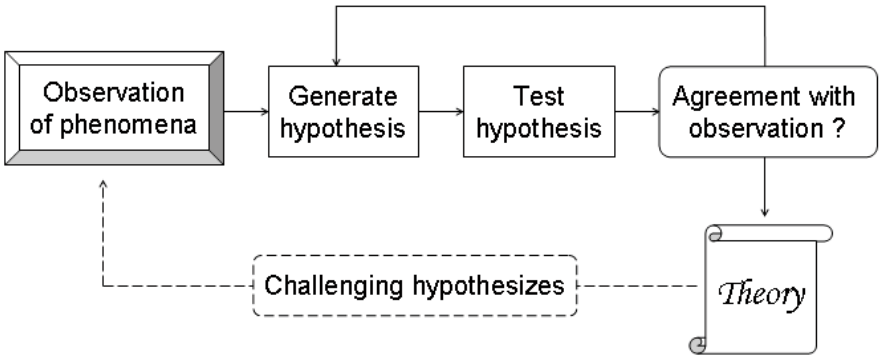

Figure 1. The formation of a theory should be a constant process to improve it.

Therefore, scientific work should, hopefully, follow a standard that allows the work to be judged, improved upon or corrected if erroneous, by that particular scientific community. To maximize the value and accuracy of the work several philosophical schools have proposed methods for conducting scientific work that could be followed. Also, by following these methods the scientific community is given a more precise picture of exactly what have been done, how the conclusions from the work were drawn, and can more easily see any flaws in the reasoning.

There are three basic methods that a vast majority of researchers within all subjects uses, often without knowing it (a more extensive description is given in [1]). If experiments are performed on several occasions and the circumstances are changed, save one variable, then this variable can be the cause of or be an integral part of a particular effect seen (see table 1). This method is often called *Dun Scotus's method of Agreement*.

Table 1. *Dun Scotus's method of Agreement illustrated for 4 different circumstances and demonstrate the correlation between the variable (or condition) "A" and the effect seen, "e"*

Instance	Circumstances	Effect
1	ABCD	e
2	ACE	e
3	ABEF	e
4	ADF	e

An equally well used method is the *Ockham's method of Difference* illustrated in table 2. If several tests are performed and a particular effect is seen only for a particular circumstance and not for any else, then the there exist a condition or variable in that circumstance that can be the cause of, or be an integral part of, the effect seen.

Table 2. *Ockham's method of Difference illustrated for 4 different circumstances.*

Instance	Circumstances	Effect
1	ABC	e
2	BCD	---
3	DEF	---
4	BDF	---

The *Grosseteste's method of Falsification* is another well used method for scientific discovery, which follows the form given below:

$$\begin{array}{l} \text{If H then C} \\ \underline{\text{not C}} \\ \therefore \text{not H} \end{array}$$

For instance, if an universal and invisible ether exists that electromagnetic wave travels in (if H), then differences would be seen in the velocity of the electromagnetic waves traveling in different directions (then C). Since no differences can be seen in the velocity of the electromagnetic waves for different directions (Not C), we can conclude ether doesn't exist and electromagnetic waves do not need it to propagate (Not H). It is important that the assumptions are correct otherwise the conclusion will be faulty even if the reasoning is right.

Observe that there often exist variables or conditions unknown to the researcher (so called "confounders") that correlates both to the independent variable or condition ("x"), and the effect seen (dependent variable, f(x)). Thus, this gives the illusion that it is the independent variable alone that causes the effect. Erroneous conclusion about a singular condition and the

effect seen can also be drawn when two or more conditions act in synergy to cause the effect. Thus there is a possibility of assuming that one condition alone is the cause for the effect.

1.2 Electromagnetism

1.2.1 A very brief history of electromagnetic research and researchers

A start, perhaps not "The" start, but yet a start, was made when Count Alessandro Giuseppe Antonio Anastasio Volta (1745 – 1827) in the year 1800 invented the modern battery, also known as the "Voltaic pile". This was sparked by his work of improving the electrophorus[1] (a capacitive generator) in 1775, and it gave scientists a (almost) stable and reliable source of electric charge. After this came other researchers such as (adopted from [2] and [3]):

- Charles-Augustin de Coulomb (1736 - 1806), who studied the attraction between differently charged objects (even though he initially drew the wrong conclusion and contributing the effect to different kinds of fluids). Coulomb is the SI unit of charge.
- Hans Christian Ørsted (1777 - 1851), Danish physicist and chemist who discovered the connection between electricity and magnetism, through his famous experiment where a current is passed through a conductor, and thus affects a nearby compass needle. Ørsted was one of the discoverers of aluminum.
- André-Marie Ampère (1775 - 1836), french mathematician who along side[2] H.C Ørsted is generally credited to have discovered electromagnetism and finding relationships between the, at that time, different areas of electricity and magnetism (creating electromagnetism or electrodynamics). Ampére is famuos for his experiment with parallel conductors attracting or repelling each other when currents of different polarities (signs) are run through them.
- Michael Faraday (1791 - 1867), a very good experimentalist who laid the foundation for the electromagnetic rotary device (electromotor). Also invented the "Faradays cage", which is the mostly widely used mitigation method for electromagnetic disturbances. He was also a devoted environmentalist and chemist, received an honorary doctoral degree of Civil Law, and rejected a Knighthood and twice the position of president of the

[1] The Electrophorus works by induction and the triboelectric effect and was invented by the Swedish professor Johan Carl Wilcke (who enrolled as a student in Uppsala university in 1749 at the young age of 17) in the year 1764.

[2] It was upon hearing of Ørsted's experiment that Ampére performed his own experiments, just months after. However it was Ampére that formulated the mathematical expressions.

royal society of London. However he accepted the gift of a free mansion, without complaints.

- James Clerk Maxwell (1831 - 1879), Scottish theoretician who combined previous results and conclusions to a set of equations and a consistent theory which demonstrated that electricity, magnetism and light are all due to the same phenomena, the electromagnetic field. He also introduced the displacement current associated with fast changing electric fields. There, however, are various quarrels about the name to the equations; however, it has stuck over the years. He is also famous for not putting his equations in the now known form (which was made by Oliver Heaviside).
- Nikola Tesla (1856 -1943), an electrical engineer who fought strongly for the method of delivering power by the use of alternating currents in the "War of Currents". Also invented the famous Tesla Coil generator and managed to cause a black-out in the town of Colorado Springs in the summer of 1899, when the power company's generator overloaded from using a gigantic version of the Tesla Coil, thus personifying the image of the "mad scientist". Tesla died poor and alone at the age of 86, but his name is today used for the SI unit of magnetic flux density.
- Heinrich Rudolf Hertz (1857 - 1894), the young and nervous experimentalist who discovered the existence, and prove of, Maxwell's theory that electromagnetic waves can travel through free-space (see fig. 2). A young Italian boy named Marconi, later read about Hertz' experiment and went on to become famous for inventing the modern radio (however in a patent dispute with Tesla). Hertz died at the age of 36 due to a disease contracted as a consequence of living in an old refurbished hospital. Gave his name to the SI unit of number of oscillations per second.

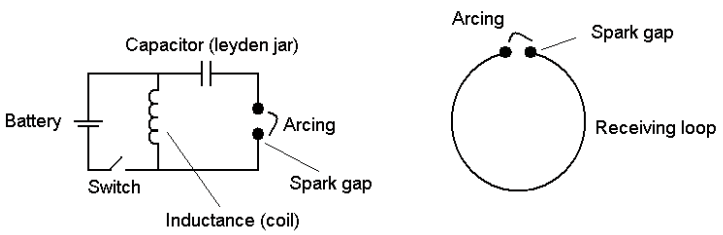

Figure 2. Conceptual schematics of the experiment performed by Hertz, proving the propagation of electromagnetic waves.

1.2.2 Maxwell's equation

This section is intended as a quick overview of the equations that govern the laws of electromagnetism and from where they originate. It is adopted from

[4]. First, Coulomb's law (which is based on empirical evidence) describes the forces between charge particles q_1 and q_2 separated in free space by distance r. If we assume two charged particular, in a stationary situation, we can write the force between them as:

$$F_{q_1 \to q_2} = \frac{q_1}{4\pi\varepsilon_0 r^2} q_2 \equiv E_{q_1} q_2 \tag{1.1}$$

Thus, we defined the electric field, E, from an electric charge. Coulomb's law can be rewritten to cope with several point charges or distributed charges (e.g., surface charges). Second, Ampére's law, which is based on the experimental work, first by Ørsted and then Ampére himself, describes the force between two circuits, carrying currents:

$$\overline{F}_{I_1 \to I_2} = \oint_{C_2} \overline{I}_2 d\overline{s} \times \left(\frac{\mu_0}{4\pi} \oint_{C_1} \frac{\overline{I}_1 d\overline{s} \times \hat{R}}{R^2} \right) \equiv \oint_{C_2} \overline{I}_2 d\overline{s} \times \overline{B}(\overline{r}) \tag{1.2}$$

From this we define the magnetic flux density, B, from one circuit carrying a current. Finally, by rewriting and adding the contribution of these two we get the force on a charged particle moving (with a speed v) and under the influence of an electric and magnetic field:

$$\overline{F} = q(\overline{E} + \overline{v} \times \overline{B}) \tag{1.3}$$

One of the fundamental equations describes the conservation of charge, that is, in an enclosed volume, the sum of the time variation of the charge and the divergence of the current, must equal to zero:

$$\nabla \bullet \overline{J} + \frac{\partial \rho}{\delta t} = 0 \tag{1.4}$$

Thus, a decrease or increase in the charge must be balanced by a current flow. For simplicity, we assume that our propagation medium is linear isotropic and electrically homogenous, and Maxwell's equations can be summarized as.

$$\begin{aligned} \nabla \bullet \overline{D} &= \rho_{free} & \nabla \bullet \overline{B} &= 0 \\ \nabla \times \overline{E} &= -\frac{\partial \overline{B}}{\delta t} & \nabla \times \overline{H} &= \overline{J}_{free} + \frac{\partial \overline{D}}{\delta t} \end{aligned} \tag{1.5}$$

E = Electric field [Volt/meter]
H = Magnetic field [ampere/meter]
B = Magnetic flux density [weber/meter^2], [Tesla]
D = Electric displacement [Coulumb/meter^2]

The relations governing the different fields can be written as (assuming linear isotropic medium):

$$D = \varepsilon E$$
$$B = \mu H \qquad (1.6)$$

We can thus rewrite the more general from of Maxwell's equation considering linear isotropic medium:

$$\nabla \bullet \overline{E} = \rho_{free} / \varepsilon \qquad \nabla \bullet \overline{H} = 0$$
$$\nabla \times \overline{E} = -\mu \frac{\partial \overline{H}}{\delta t} \qquad \nabla \times \overline{H} = \sigma \overline{E} + \overline{J'}_{free} + \varepsilon \frac{\partial \overline{E}}{\delta t} \qquad (1.7)$$

Where $\sigma E = J_{free}$ (in 1.5) and J'_{free} (in 1.7) are source of free current densities arising from other source than the conductivity (σE).

We should remind ourselves of the physical content behind these equations (1.5). The first equation (also known as Gauss' law), $\text{div}(\mathbf{D}) = \rho_{free}$, summarizes coulomb's law together with the electrical effects of matter. It describes that the flux of the electric field out of a closed surface is equal to the charge that is enclosed by that surface. The second equation, $\text{curl}(\mathbf{E}) = -\delta\mathbf{B}/\delta t$, describes Faraday's law of induction, the induced electric field due to a time-varying magnetic flux density. Notice that, without a time-varying **B**-field source, $\text{curl}(\mathbf{E}) = 0$. The physical meaning of $\text{grad}(\mathbf{B}) = 0$ is that magnetic monopoles can not exist. The last equation, $\text{curl}(\mathbf{H}) = \mathbf{J}_{free} + \delta\mathbf{D}/\delta t$, arises from Ampére's law, the conservation of charge and the magnetic effects of matter. Notice the time-varying **D**-field term is the *displacement current* (also known as $\mathbf{J}_D$), which was the big contribution, to these four equations, from Maxwell himself.

1.3 Electromagnetic compatibility, EMC

Electromagnetic compatibility or EMC is defined [5] as:

> "the ability of a device, unit of equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances[3] to anything in that environment".

This means that a device that is electromagnetic compatible will not disturb the function of a nearby device, nor be disturbed by its own function or the function of a nearby device. Everyday examples of EMC, that most people have experienced includes noise from radio speakers when a cellular phone is ringing, "humming" sound in telephone due to coupling from the local power network, a computer monitor placed too close to a microwave oven flickering when the microwave oven is turned on, lightning strikes to power lines causing power failures and more. For example one could be so bold as to say, without the past EMC research, modern systems such as computers would not function reliably. This is because the very fast clock frequency of the processors used today creates high frequency interference that without proper shielding of the processor, minimization of conductor loop area and other EMC design procedures on the chip level would make it impossible for the computer to function normally. This is an example where a device interferes with its own function however with out the proper EMC precautions the computer would also disturb other systems in close proximity. This, and the example with a mobile phone disturbing a radio or a microwave oven creating flicker on the monitor are examples where devices or systems disturbs the normal operation of other equipment. As can be seen from the examples above there are more than scientific curiosity to fuel the research of EMC.

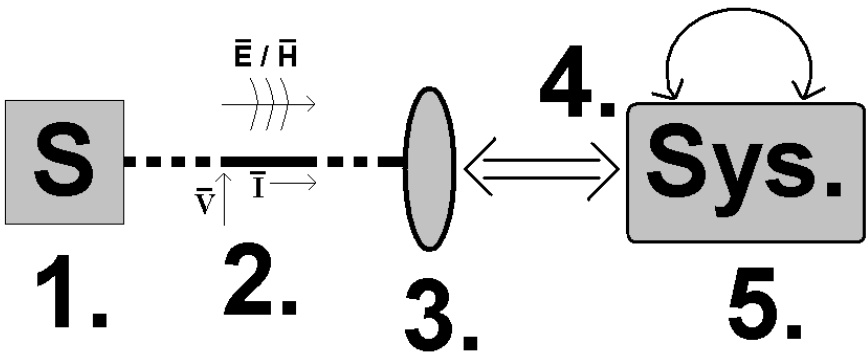

Figure 3. Shown is a schematic decomposition of an EMC problem.

[3] Generally, disturbances can be conducted or radiated in origin, and the latter can be divided into near-field (inductive or capacitive in nature) or far-field

A basic decomposition of an EMC problem can be described as the schematic sketch shown above (fig. 3). A source (1.) is creating a electromagnetic field or a voltage/current transient which propagates along the coupling path (2.) which can either be of galvanic contact (as in the case of voltage and current propagating in a conductor such as a cable) or through a medium like air, dielectric material or metal mesh (as in the case of electric and magnetic fields). At the system exterior (3.) it will couple to the system interior (4.) and finally interact with the system producing a system response (5.). By using the approach described above a problem can more easily be investigated and a solution to an EMC problem can more easily be found.

Reducing the coupling from the source to the affected system, in terms of EMC is done by minimizing the transfer function between the source and the receiver, that is (2.) to (4.) for the given excitation characteristics (frequency or time domain waveform). Practically, this is often done by improving the shielding or installing filter at the exterior boundary of the affected system (3.), but also by e.g. installing or improving shielded cables, minimizing conductor loop areas to decrease field coupling or installing ferrites to decrease common mode transients (2.). If possible, the source emission (1.) is reduced. The function, called A_{tot}, for the response of the system due to a source (see fig. 3. above) can be given as an equation (adopted from [6]).

$$A_{tot}\left(\zeta_j\right) = \prod_{i=2}^{4} A_i\left(\zeta_j\right) \quad \forall \zeta_j \in \Lambda \tag{1.8}$$

where i is the index of the components giving the coupling from source to system response (see fig. 3 above). For instance the contribution from the coupling path (radiated or conducted) to the transfer function is A_2. Let Λ be a subset of variables (of the set of all possible variables) which affects the transfer function. It will include such quantities as the excitation frequency or frequency spectrum[4] of the source, angle of field incidence, polarization of field, peak amplitudes, loss factors and more. In other words, all the things that affect the coupling of the energy from the source to the system response should be taken into account. These quantities are denoted ζ_j. Practically it is enough to consider the frequency and peak amplitude to obtain an approximate value of the system response. The product of all these functions of all the elements from the source to the system response, considering all the quantities of Λ gives the total system response.

EMC can, however, not be reduced to shielding, filtering and SPDs even though these may be the only options available for an engineer dealing with commercial-off-the-shelf (COTS) equipment. Overall economy of the solu-

[4] Instead of a frequency description the rise-time and FWHM-time could be given.

tion is important (see fig. 4 below). An intelligent and well planed design of systems and equipment to make it less susceptible to electromagnetic interference (EMI) and to make it emit less interference are important activities in acquiring electromagnetic compatibility.

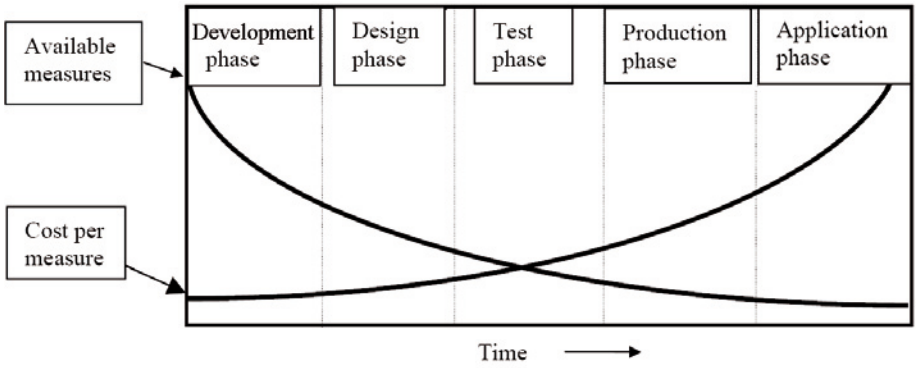

Figure 4. As time progresses in a project the available measures to tackle any EMC issues drops and the cost per measure increases

1.3.1 Electromagnetic topology and zoning concept

A vital philosophy is the concept of "electromagnetic topology" or "electromagnetic zoning". It is today the far most established method for obtaining electromagnetic compatibility between and within individual pieces of equipment or distributed systems. Electromagnetic topology is defined as (adopted from [7] and [8], respectively):

> "This concept involves the definition of principal surfaces and principal volumes which divide up the space occupied by the system. These surfaces and volumes are further divided corresponding to various features of the system design and analysis."

> "In electromagnetic topology, the topological surfaces represent boundaries separating different electromagnetic environments in different zones."

The purpose with zoning is to divide the system or piece of equipment, e.g., an airplane, computer or a facility, into zones that are classified after the electromagnetic environment that can be tolerated in each zone. These zones should be electromagnetically separated (shielded) from each other if the sub-system or components "installed" inside are sensitive or critical for the operation of the original system, or if the emission from these components is unacceptably large.

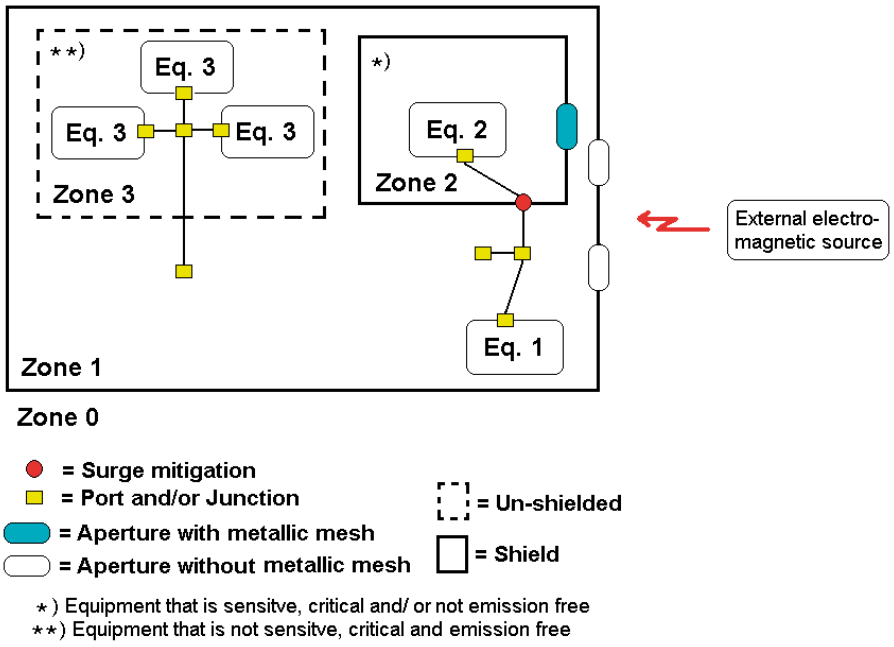

Figure 5. The zoning principle conceptualized via, electromagnetically, separating the different zones after classification of equipment inside and the electromagnetic environment that is allowed inside.

Components or sub-systems that aren't sensitive or critical for the operation of the original system, and don't radiate or otherwise introduce electromagnetic energy (disturbances) in the rest of the system, do not need to be put in a shielded zone (e.g., Zone 1 or 3). The interface at the zone boundaries are controlled either through, e.g., filters or surge protective devices for conductors, or metallic meshes for, e.g., apertures or windows. Traversing the zone boundaries of the system or facility from the outside to the inside, more sensitive, critical or noisy components or sub-systems is placed in deeper lying zones (e.g., Zone 2). The outermost zone is often called "zone 0" and is equal to the external electromagnetic environment. The division of the system into zones, as well as the placement of all the components or subsystems within these zones, is made after a careful examination and classification of the sub-systems regarding threshold levels for upset events, importance to the operation of the system and level of emission. Also, the likely electromagnetic environments that can be present outside the system (exterior electromagnetic environment) have to be taken into account when designing the system.

Normally the shielding and division of the different zones is handled with metallic structures (e.g., plates or meshes) but the distinction between zones could also be made due to other factors giving attenuation, e.g., distance

between source and receiver of the electromagnetic energy. This concept is called “generalized shielding” [8].

If done properly, the philosophy and concept of electromagnetic zoning have proven that even very noisy or susceptible equipment can be shielded or protected from most electromagnetic environments. However, as will be seen in this thesis, the electromagnetic and physical boundaries may not always, unfortunately, coincide, which will create problems when a human intent exists behind a disturbance.

1.3.2 Front-door and back-door coupling

Traditionally the coupling of electromagnetic fields into an electromagnetic zone is defined as front-door or back-door coupling, defined as (Paper IV):

> “Front door coupling; the electromagnetic disturbance uses available ports and coupling paths intended for the propagation of electromagnetic energy, radiated or conducted, and communication with the external environment, e.g., antennas or power sockets.”

> “Back-door coupling; the electromagnetic disturbance uses ports and coupling paths generally not intended for communication with the external environment (through walls or small apertures [in an electromagnetic shield], or coupled onto cables).”

In addition, the coupling of electromagnetic energy into a system can be described how the penetrations in the electromagnetic shield are made. Deliberate- and inadvertent penetrations are respectively defined as [9]:

> “Deliberate penetration; an intentional opening made in an electromagnetic (“EM”) shield that provides a path for the transmission of intended signals into or out of the shielded region. It can also be a consciously made opening for passing power, water, mechanical forces, or even personnel from the outside to the interior, or vice versa.”

> “Inadvertent [EM] penetration; an opening, not deliberately made, that may provide a path for electromagnetic (“EM”) energy through the EM shield. Most often inadvertent penetration is undesired. Typically, leakage through imperfectly conducting material is considered as an inadvertent penetration.”

There is a small, but distinct, difference between the two sets of definitions of the coupling. The first set of definitions (from Paper IV) solely focuses on whether or not the coupling ports or paths are intended for passing electromagnetic energy. The other set of definitions (accordingly to [9]) focuses on whether or not a possible coupling path were deliberately installed (e.g., power cables or water pipes) or appeared by chance or accident (e.g., tear in

metal shield). Also, these definitions focus on a penetration into a zone with shield boundary, whereas the first set of definitions accepts any zone boundary. If combining these definitions, and also interpreting "intended coupling path" as a suitable or very good coupling path in the first set of definitions, one could have one of the following four situations:

1. *Deliberate-front-door coupling*: purposely installed coupling path suitable for passing EM energy (e.g., antenna).
2. *Deliberate-back-door coupling*: purposely installed coupling path not-suitable for passing EM energy (e.g., water pipe).
3. *Inadvertent-front-door coupling*: accidentally installed coupling path suitable for passing EM energy (e.g., an erroneously installed and easily assessable power socket).
4. *Inadvertent-back-door coupling*: accidentally installed coupling path not-suitable for passing EM energy (e.g., a small aperture [compared to wavelength] in a metal shield).

Classification of coupling paths is essential for the investigation of a system and where and what possible mitigation procedure can be taken, however a fundamental complexity when constructing methods of classifying different characteristics for systems is the definition of system itself. The IEC definition [9] of a "system" is:

> "System;
> (1) collection of subsystems, assemblies and/or components that function together in a coherent way to accomplish a basic mission;
>
> (2) collection of equipment, subsystems, skilled personnel, and techniques capable of performing or supporting a defined operational role. A complete system includes related facilities, equipment, subsystems, materials, services, and personnel required for its operation to the degree that it can be considered self sufficient within its operational or support environment.

The second part of the definition leaves ample room for extending the boundaries of a system to a great extent. If considering a computer or an airplane it is quite intuitive of what the system extent is, but how much should be included for an, e.g., large facility or system such as railway network. According to the definition above one could include everything that make up a facility or system, which would include supporting subsystems for water, personal, waste, electricity and more ad absurdum. However this would eventually have to include almost everything due to the interdependencies of the civilian infrastructure and is not helpful to us. It comes down to what level of detail should be considered in conjunction to the threat estimate and also how far the consequences would spread, thus the actual definition of "system". For example, for an airplane it is quite simple to define

front-door coupling (if using that set of definitions) as available antennas and similarly back-door coupling be, e.g., through an aperture (e.g., cockpit window). On the other hand examining a facility it is not so easy to draw distinct lines between the system and the external world (since it is not an isolated entity as, e.g., an airplane). That is, many times the physical and electromagnetic boundaries may not coincide.

In addition to front- and back-door coupling a disturbance can be in-band as well as out-of-band with respect to the receiving system. For a real situation the back-door coupled energy is more likely to be out-of-band with the system. This is since the propagation through the ports and paths not intended for coupling of electromagnetic energy is often an unfavorable path, and thus attenuates the power or spreads it through several paths.

It is very difficult to protect a system from an in-band front-door coupled disturbance. This is since filter equipment can not be applied, as also the intended frequency of operation of the system would be attenuated or stopped. Also, for civilian systems and equipment, the frequency of operations and thus the in-band frequencies are publicly known. Therefore it is very easy for an eventual attacker to tune their electromagnetic source to that/those particular frequency band(s).

1.4 High-altitude electromagnetic pulse (HEMP), or Nuclear electromagnetic pulse, NEMP

It was first noted during the era of nuclear device testing in the atmosphere that unusual electronic effects could take place at distance where the direct effect of the shockwave was not effective. Especially Enrico Fermi is credited for predicting this and the first observations of effects on electronic systems were not planned experiments, but were mainly the result of malfunctions with civilian equipment reported and later analyzed. Particularly the *Starfish Prime* nuclear device [10] having a yield of 1 Megaton of methyl-1,3,5-trinitrobenzene (TNT) detonated 400 km over the Johnston atoll on the night of 8 July 1962 provided some interesting data. Not only did it produce a number of atmospheric phenomena producing e.g. aurora lights seen over, e.g., New Zeeland 6500 km from the Johnston atoll, but also numerous electromagnetic effects were witnessed. In Hawaii, separated by 1400 km from the Johnston atoll radio communication was not possible for 30 min due to the disruptions in the ionosphere, street lights were destroyed, car alarms and air sirens were triggered at the time of the explosion, fuses were reported to be blown out all over the island and isolation transformers were damaged. The test from the Soviet Union in 1962 over Kazakhstan produced similar results with reports of failure of diesel generators, damaged insulators on

power lines, affected antenna systems, failure of communications lines and even an affected communications lines buried over 600 km away [10].

HEMP is generated by several complex processes in the atmosphere at approximately an altitude of about 40 to 400 km [11] but can shortly be said to occur as an effect of the matter and radiation created from the nuclear explosion interacting with matter in the atmosphere and the magnetic field of the earth. The area coverage will be dependant on the actual height of the nuclear explosion in the atmosphere, but will not be a linear function of the height[5].

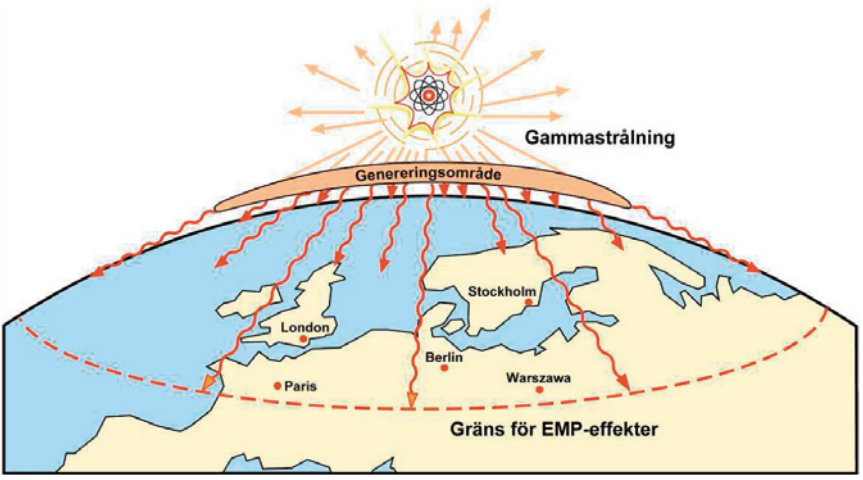

Figure 6. A nuclear explosion at an altitude of 30 km or more will affect all of northern Europe (adopted from [12])

Even though standards [13] give the HEMP waveform as 2.5/25 ns and 50 kV/m amplitude (often used for immunity testing) this only describes the "early time" component of the HEMP electric field (E1). The complete, non-classified waveform of HEMP consists of:

1. early time (E1) , (last about 1 μs) ≈ 50 kV/m peak
2. intermediated (E2) (1 μs to 1 ms) ≈ 100 V/m peak
3. late time pulse (E3) (also know as the magnetohydrodynamic pulse (which can last up to several minutes) (≈ 40 mV/m peak).

Observe that the electric field values are dependent on the polarization and also that the actual waveforms from an HEMP is not publicly available. All of these three components affect electronic systems differently as the wave-

[5] In part due to the curvature of the earth but also due to the different physical processes when creating the HEMP.

lengths associated with them couples differently to objects of different sizes (and general direction compared to the polarization of the electric and magnetic field). For instance, the E1 component can propagate through apertures (due to small wavelength) and, due to the high electric field strength, create breakdown inside systems and the E3 component, even though very weak in strength, can cause problems since it will couple to long power cables and induce currents that may, e.g., saturate transformers. However, it is the synergy between the different components that is the biggest concern. Damage caused by earlier components will increase the effects of next, e.g., E1 may trigger or cause a breakdown of surge arresters, which will leave systems unprotected from the energy of the E2 and/or E3 component.

The physical processes that create the HEMP will, however, not be discussed further; nonetheless the historical role and influence that HEMP has had on EMC research cannot be stressed enough.

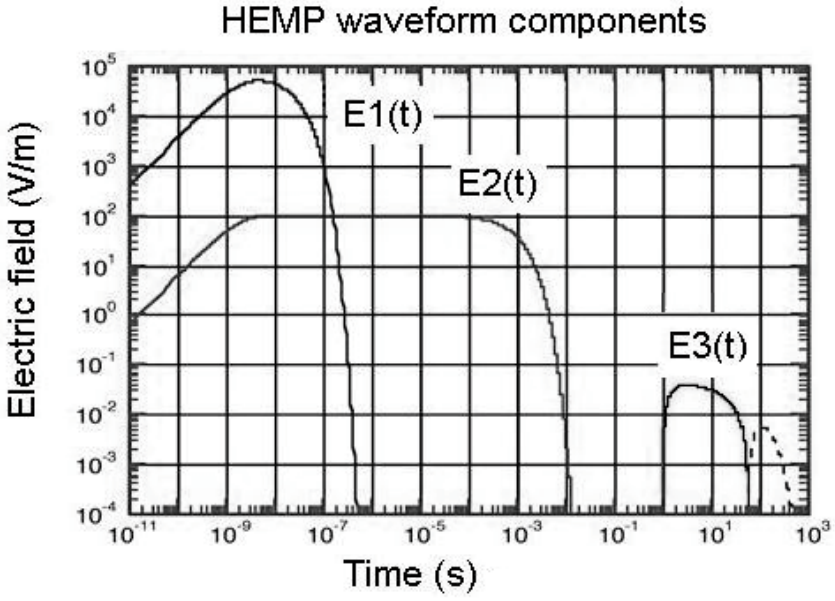

Figure 7. The different components of the HEMP electric field waveform shown in time domain. Note that the timescale stretches over 10^14 powers and that the electric field stretches of 10^9 powers.

Note that the time scale of the E1 component is similar to an electrostatic discharge (ESD), E2 is similar to a lightning electromagnetic pulse (LEMP) and the E3 component is similar to the ground induced currents (GIC) caused by geomagnetic storms [11]. Thus, susceptibility of equipment from HEMP can be tested, or deduced, from results from the above mentioned phenomena.

1.5 High power electromagnetic, HPEM

High power electromagnetic (HPEM) pulses is a new threat that has arisen in the last decades due to the development of improved pulsed power sources (of which many are commercial) and the proliferation of components that can be put together to form crude HPEM weapons. HPEM is a high power environment which can be both conductor bound transients with voltage levels typically exceeding 100 V [9] and radiated with fields typically exceeding 100 V/m [14] (high compared to normal EMC peak field values which are in the range of a few tens of V/m).

Figure 8. The HPEM source "JOLT" [15] (© 2004 IEEE).

The main difference between HEMP and HPEM is the area coverage produced by the source That is, the area illuminated by a HEMP is much larger than from any known HPEM source. Where the amplitude of the HEMP is not very affected by change in small distances on the surface of the earth, the typical HPEM environment is very sensitive to difference in distance between source and point of measurement. According to [14] HPEM environments can be:

1. Radiated or conducted in nature, which means that they can either be propagating along conductors or radiated in a medium.
2. A single pulse envelope with many cycles of a single frequency (an intense narrowband signal that may have some frequency agility). This is also often called high power microwave (HPM).
3. A burst containing many pulses, with each pulse envelope containing many cycles of a single frequency.
4. An ultrawideband (UWB) transient (spectrum content from 10s of MHz to several GHz). This is sometimes called high power impulses (HPI).
5. A burst of many UWB transient pulses.

The two main frequency characteristics considered in HPEM are the narrowband HPM, with a single frequency typically in the range of 1-10 GHz and the broadband UWB transient with a rise-time of usually 0.1 ns and a pulse width of 1 ns (see fig. 9). Since a UWB source spreads the electromagnetic energy generated across a wide spectrum, compared to a narrowband HPM source which concentrates the energy at a (approximately) single frequency, this source is more likely to be used for disturbance purposes, as each frequency component contains only a small part of the total available energy, but covers a larger spectrum. Thus, there is no need to "tune" the source to the victim system. HPM sources are more likely used for destruction purposes since the energy is located in a single band, which however have to be tuned to the victim's vulnerable frequencies (operating frequencies and/or the resonance frequencies).

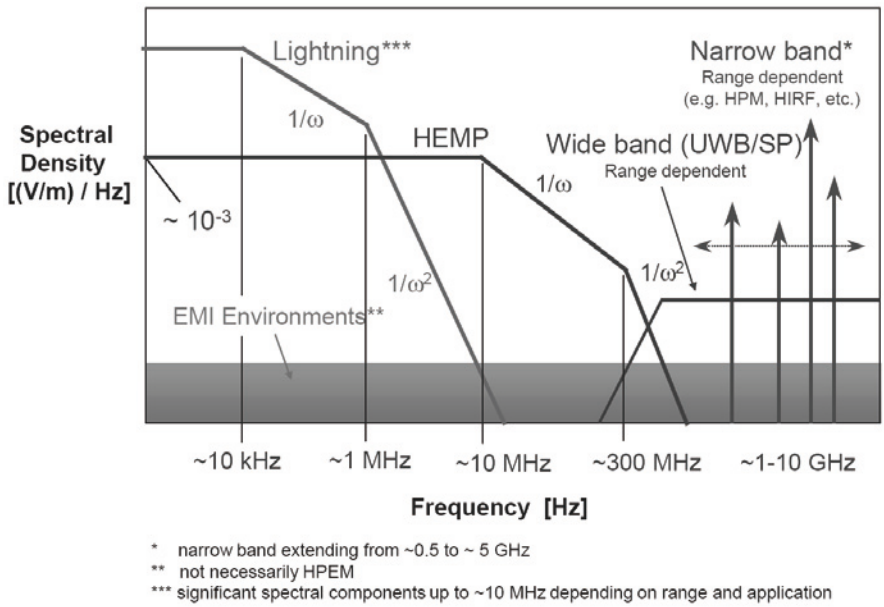

Figure 9. Different electromagnetic environments together with HPEM (adopted from [16]).

Several severe incidents of interference by HPEM have happened and been documented in open literature ([9] and [17]) and at international conferences (e.g. *EuroEM 2004* and *AmerEM 2006*) from which a short review of some cases are given below.

- In 1967 a US Navy jet fighter landed on the aircraft carrier USS Forrestal and due to degraded shield termination of a radio frequency cable the radar energy coupled into the system and inter-

fered with the weapons system. A fully tanked jet fighter was hit by a discharged weapon and exploded, killing 134 people.

- During the early years of antilock braking system (ABS) many cars experienced problems along a certain stretch of the German Autobahn due to the close proximity of a radio transmitter.
- Several fighter planes and army helicopters have been known to be susceptible to EMI when flying too close to radio transmitters. Several cases of crashes due to this are known. E.g., in 1990 an airship lost all power in both its engines due to flying too close to a radio tower. The airship crashed into trees and sustained damage. Power loss was due to high frequency signal coupling into the electronic ignition system.
- 1999 the San Diego County Water Authority and the San Diego Gas and Electric companies were unable to remotely activate critical valve systems in the Supervisory Control and Data Acquisition (SCADA) system. Technicians were sent to manually open and close water and gas valves. The cause was US Navy exercises of the Sand Diego coast broadcasting radar signals in the commercial spectrum of wireless networks.
- In 1992 a US naval ship entered the Panama Canal without turning off its radar systems. The Canal Zone computer systems were damaged due to the illumination of the radar and had to be replaced.
- Sensitive medical equipment have been known to be interfered with due to the radio transmitter on the roof of ambulance, resulting in one case a patient's (on life support equipment) death.

As can be seen from the examples above although some of these systems are designed to be protected against lightning surges and interference traditionally considered in normal EMC hardening investigations, they can however still be vulnerable to HPEM pulses, due to the high power, different characteristics of the pulses and coupling paths and entry points not considered. Unintentional illuminations by high power radars and radio transmitter beams in close proximity of civilian systems have clearly proved the dangers of HPEM.

1.6 Intentional electromagnetic interference, IEMI

In august 1999 the international Union of Radio Science (L'Union radio-scientifique internationale - URSI) adopted a resolution [18] at the Toronto General Assembly in which "criminal activities using electromagnetic tools" are mentioned. It states, among other things, that:

> "This kind of action can be defined as an 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."

The keywords here are "intentional malicious generation", or more simply "intentional", thus a human motive exists behind the interference. In this thesis it will become apparent that it is this human motivation and intent that is the foremost obstacle behind mitigating disturbances created by intentional EMI (IEMI). The URSI adopted resolution also states that:

> "This resolution is intended to make people aware of: … the fact that criminal activities using electromagnetic tools can be undertaken covertly and anonymously and that physical boundaries such as fences and walls can be penetrated by electromagnetic fields."

Observe the words "covertly and anonymously", thus, there may be rouge elements in society that do not wish to draw attention to them by, e.g., exploding a bomb in a public place. Rather, an IEMI attack on a critical infrastructure component of civilian society could be made without the "victim" realizing that the upset occurring is intentionally caused. The scenario of a disturbance source positioned inside a van with dielectric wall and radiating a disturbance is often described in literature. The conceivable targets for an IEMI attack could be telecom, radio/TV networks, power system networks, air traffic control, railway networks, banking and government administrative networks etc. Several reports and rumors [19], [20] of IEMI incidents have circulated in open literature and at international conferences and seminars

- In 1998 two members of the Japanese criminal organization Yakuza were allegedly arrested for manipulating a "pachinko machine" (a gambling machine) with a high energy radio frequency (HERF) generator. The HERF generator was hidden on the waist and the criminal was holding the antenna in the hand.
- A Russian criminal was alleged sentenced in 1996 for disabling the alarm system of a Jewel store by the use of a home made COTS RF generator. Also Chechen commander Salman Radueyev supposedly used jammers during a raid on the city of Kizlyar to disable police radio communications.
- A large area of Moscow lost the telephone network as a result of an IEMI effect [19].

Note that the difference between an IEMI attack and an accident involving a HPEM source (e.g., radar) is only the human intent. Therefore, whether these rumored IEMI incidents are accurate or not, should not diminish the conceived threat from IEMI.

A number of reasons can be given for why the threat from IEMI to the society of today has increased:

1. The overall use of sophisticated and sensitive electronics in society has increased. This explosion of the use of electronics has had the effect of COTS equipment being used even for applications and in installations where before many times specialized and more hardened systems were used. For instance, today one can see commercial PCs supervising and controlling critical infrastructure components (e.g., electrical-, communications-, and transportation networks).
2. This absolute explosion of the use of electronic systems has driven the evolution of these systems forward. From the Intel 4004 chip (1971) that used 10 μm process technology to today (2008) where process technologies have reached the 45 nm resolution for manufacturing electronic circuitry, the miniaturization have leaped almost a factor of 1000. Along with this decrease in chip size and increase in packaging density the inherent susceptibility of electronics have increased (see fig. 43 for some examples). One reason for this is that the signal levels used in electronics have decreased, thus, the field levels that is needed to create false signals in the order of, or above, the operational signal levels has decreased. However, observe that at the same time some systems may be less susceptible as the shielding may have increased. This is a consequence of the system working at higher clock frequencies, creating more emissions which must, thus, be handled in accordance with the EMC regulations This use of shielding to limit the emissions, will also protect the system from outside disturbances.
3. This evolution of our modern society to be highly reliant on technology has increased our use of the EM spectrum. This has brought us such things as mobile phones, wireless computer networks (WLAN), handheld GPS receivers, wireless security cameras etc., which all have increased the EM background field for a wide range of spectra but also the number of open ports that can be disturbed (increased threat of front-door coupled disturbances).
4. In the wake of the cold war research, technology evolved and HPEM sources is utilized for a variety of applications, from sterilizing fluids to non-lethal weapons that can render electrical equipment useless. Thus, the amount of commercial EM sources that can act as weapons have increased. Also, do not forget the existence of large amounts of other commercial sources used for a variety of EMC testing, which also can be used for IEMI.
5. The available amounts of different components that can be assembled to homemade sources (e.g., switches, capacitors, magnetrons etc.) have increased. Also, a number of schematics for construction and assembling these kinds of sources can easily be found on the Internet (see fig. 13).

However the quality of the plans and explanations given are of very varied nature which can lead to injury or death due to high voltages or exposure to microwave radiation

6. Certain groups in society may find it more suitable to carry out IEMI attacks rather that traditional terrorist acts, as IEMI attacks can be attractive as they can be performed anonymously and covertly, as well as the fact that physical boundaries may not apply (e.g., radiation through weakly shielding walls or direct injection into power network through a power socket).

The points 1) – 3) are created and affected by the properties and characteristics of the victim systems whereas 4) – 6) are connected to the source or attacker.

While threats posed by IEMI and HPEM weapons in possession of enemy states had been recognized by the military long time back, sufficient attention was not paid on its possible use against civilian targets by non-state entities until recently. Unlike many modern military systems, civilian systems are generally not hardened against HPEM. Moreover, the weapon carrier can come very close to the intended target in civilian systems and facilities, enhancing the potential for serious damage. For example, according to a study conducted [21], a HPEM source mounted on a van can permanently damage a typical civilian system at a distance of 15 m by radiating them, however it can cause system upset (or function failure) at a distance as far as 500 m (a factor of 20 – 30 dB larger). A small HPEM weapon hidden in a suitcase in close proximity to the target and radiating the system can do considerable damage to electronics and if placed at a distance of 50 m cause disturbances. See Chapter 6 for more on system assessment.

As will be discussed in the sections ahead an attacker can enter a facility and thus circumvent the outer shield and zoning concept. The source can be directly connected to a power or lamp socket and the injected transient can spread in the local power net. Also the abundant existence of antennas that work in the GHz range, which acts as very good coupling paths (front-door coupling) into unprotected sensitive low-voltage systems, present a very good entry for terrorists into a shielded environment or system. Below are some pictures on different source that can easily be found and bought from the Internet (fig. 10 – 12), and also plans and instruction to build an electromagnetic source from commercial components (fig. 13).

Figure 10. Examples of some simple commercial sources from the Internet

Figure 11. The plans for a “microwave canon” can be bought on the Internet.

Figure 12. (left) Two self tuning GPS and GSM jammers for which the schematics can be found on the Internet; (right) a commercial GSM/Umts/GPS/3G jammer.

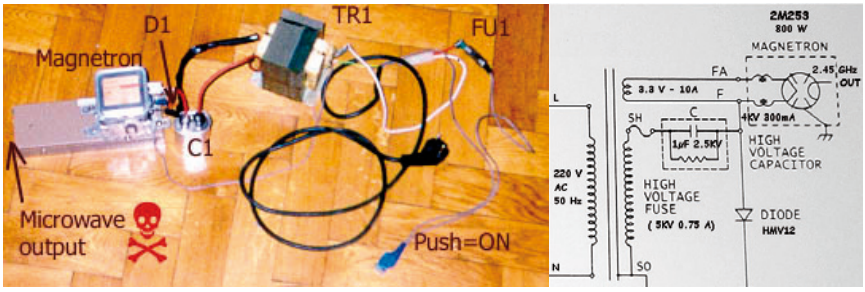

Figure 13. Showing a picture and circuit diagram, found on the Internet, of a crude homemade electromagnetic source.

In addition, it must be noted that IEMI is not confined to specific waveforms spectra and amplitudes; these should rather be used as a guide and a common ground for discussions, but not to limit the concept of IEMI. As the URSI resolution also states, indirectly, any electromagnetic energy introduced into an electronic system with malicious intent, shall be considered IEMI, thus even a household battery or the power supply itself can act as a source of IEMI. However, these are rarely considered as being "electromagnetic weapons". The probability of occurrence of a particular electromagnetic environment generally decreases as the pulse energy of the disturbance increases since, at the same time, the complexity of the source technology, as well as the difficulty of generating that particular disturbance, increases. It is more likely that a system (under an IEMI attack) is subjected to, e.g., a RF jammer than a HPM disturbance. HEMP is the most unlikely to occur due to obvious reasons.

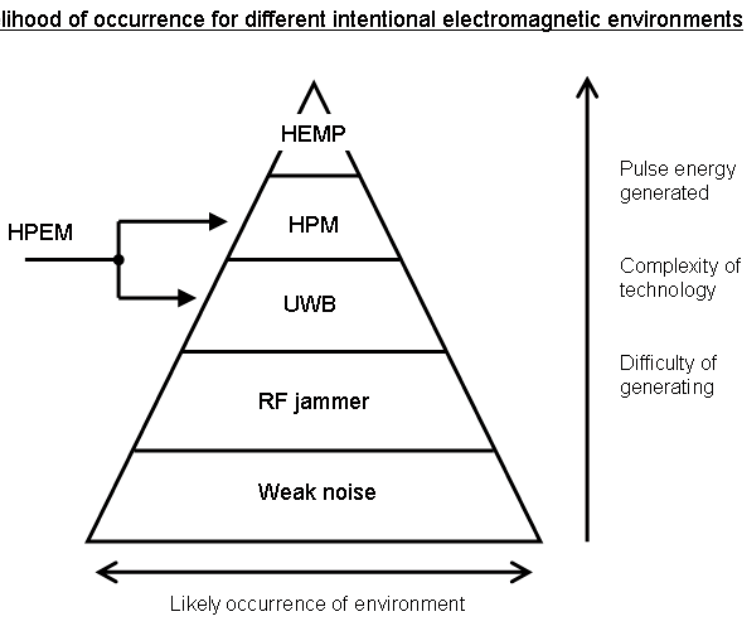

Figure 14. The probability of different intentional electromagnetic environments occurring decreases as the pulse energy, complexity of technology and the difficulty of generating the disturbance increases.

The legal issues of owning a potential IEMI weapon (the use of any electromagnetic source is regulated by ownership of particular frequency spectra and the maximum power transmitted in these) is something that has to be addressed in the future, but will not be discussed in this thesis. The lack of knowledge regarding the response and susceptibility of civilian systems and facilities to HPEM and the potential threat of IEMI is addressed in this thesis.

1.7 Outline of thesis

This Ph.D. thesis will treat the phenomena of IEMI and the threat to society from the various electromagnetic sources that can be used adversely. It is based on the papers, reports and results produced by the author and the outline will follow a "system level assessment" approach (compare fig. 3):

- First, in Chapter 2 we will acquaint ourselves with the different waveforms that are often discussed together with IEMI and HPEM. Different potential IEMI sources have already been introduced here (Chapter 1).

- After this, in Chapter 3, we will go on to study the coupling paths that the electromagnetic energy may take (**Paper II, III**).
- Mitigation of the disturbances will be described in Chapter 4 (**Paper I, VIII**).
- Chapter 5 will discuss the system response and its susceptibility, as well as the difficulty with correlating results (from, e.g., standards) to experiments (**Paper V, VII**).
- In Chapter 6 a method for performing a system level assessment will be put forward (**Paper IV**).
- Chapter 7 will deal with the problems and possibilities of measuring of HPEM signals.
- Finally, Chapter 8 will discuss the problem of, and suggest a method for, classifying facilities (or large distributed systems) from an IEMI perspective (**Paper VI**).

Each chapter will contain subchapters that serve as background or introductive paragraphs that leads up to the subchapters discussing the Papers.

2 Source waveforms

In Chapter 2 the most common waveforms discussed for HPEM and IEMI research will be given. The majorities of the other waveforms are similar to these or can be formed from them. Observe, however, that a threat analyzes should never be limited by such things as fixed waveforms.

2.1 Introduction to IEMI source waveforms

This thesis does not dwell into the subject of sources that produce electromagnetic energy. Many papers have been published on the subject of "pulsed power", "High power electromagnetic pulses", "Ultra wideband sources", etc. However, to be able to protect against and understand IEMI (and HPEM) effects on civilian systems and facilities, a review of different waveforms and their varied characteristics will be made. As will be clear from the sections ahead, EM sources display a great variation in their characteristics; however when regarding possible IEMI sources any device that can produce electromagnetic energy (fields or voltages/currents) can be used to create intentional electromagnetic interferences, theoretically, even a small 9 Volt battery. It is the motivation and knowledge of the attacker about the susceptibility characteristics of the victim that sets the source parameters.

Adopted from [14] we define two quantities to aid us in the division between narrow- and wideband sources:

$$\text{bandratio, br} = \frac{f_h}{f_l} \tag{2.1}$$

$$\text{percent bandwidth} = 200\frac{(br-1)}{(br+1)} \tag{2.2}$$

where the terms f_h and f_l are the upper and lower 3dB point, respectively, for the signal. The maximum possible value for the "*percent bandwidth"* (pbw) is 200%. In addition the "*bandratio"* (br) is defined because many of the HPEM sources created today already have a pbw of > 190%. Some time the waveform has a large DC component or multiple peaks, than bandwidth can

be calculated by taking the limits where 90 % of the energy is contained. Over the years the meaning of "wideband" has changed in accordance to the development of technology and one distinction used today is given in Table 3.

Table 3. *The different definitions for bandwidth classification (according to [14]).*

Band type	**pbw**	**br**
Hypoband	≤ 1 %	≤ 1.01
Mesoband	1 % < pbw ≤ 100 %	1.01 < br ≤ 3
Sub-hyperband	100 % <pbw ≤ 163.4 %	3 < br ≤ 10
Hyperband	163.4 % <pwb ≤ 200 %	br > 10

However, as stated above, the waveform of an IEMI disturbance can take almost any form, DC, AC, narrowband, wide band, etc., but to limit ourselves in the pages here, the three most common, and probable, classes of waveforms will be discussed.

2.2 Narrowband waveforms

Electromagnetic sources that produce waveforms with a pbw of < 1% or a br of < 1.01 are called narrowband or hypoband sources. That is, they produce and deliver their power in a very narrow frequency band (see fig. 15 below).

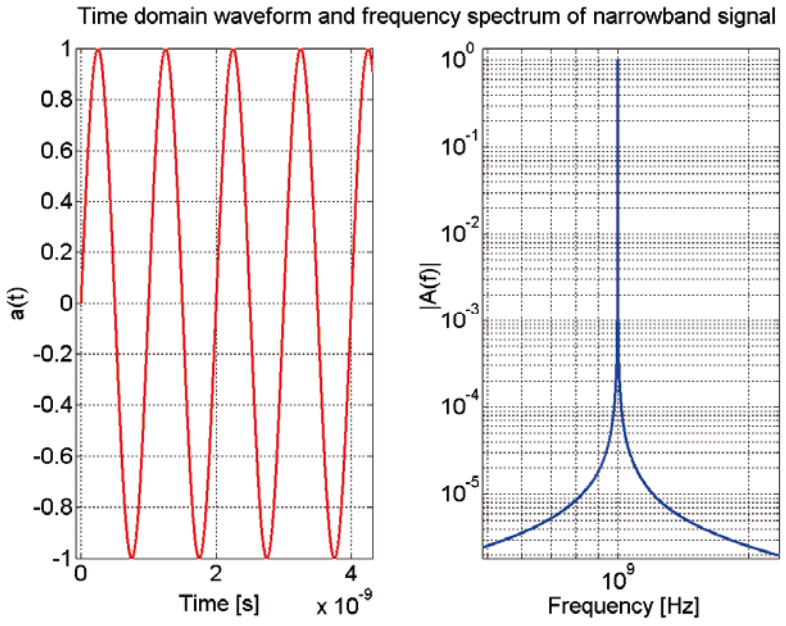

Figure 15. Normalized time domain waveform and frequency domain spectrum from a narrowband source.

The time and frequency equation for the narrowband sinusoidal is given below [12].

$$\begin{cases} a(t) = A_0 \sin(\omega_0 t) \cdot u(t) \\ |A(f)| = A_0 j\pi(\delta(\omega + \omega_0) - \delta(\omega - \omega_0)) \end{cases} \tag{2.3}$$

where A_0 is the peak value, $\omega_0 = 2\pi f_0$ and f_0 is the centre frequency. The term u(t) is to ensure $a(t) \equiv 0;\ t<0$ and is the "Heaviside step function".

Narrowband waveforms have, as can be seen from the figure above, the majority of their power in a very small frequency region. As discussed above, imagine a system or device that is vulnerable in a certain frequency band due to inadequate design of mitigation measures. This then means that a narrowband pulse which does not have a centre frequency in this vulnerable band causes no, or very little, interference. However, as also stated above, if a narrowband source is "tuned" to the systems resonance frequency the power delivered to, and the response of, the system is maximized. The *magnetron* and v*ircator* are example of narrowband sources. A simple narrowband HPM weapon can be built (as shown in the previous chapter) by only utilizing easily available commercial components, e.g., parts from a microwave oven. Such a source can deliver 25 kV/m in the waveguide [14],

yielding, e.g., an approximate distance normalized peak electric field (rE_{peak}) of 4.7 kV when using a reflector antenna of 2.5 m^2.

Table 4. *Distance normalized peak electric field values from a simple narrowband source assembled from a commercial microwave oven (1.1 kW rms power) with different antenna types (data adopted from [14]).*

Microwave magnetron with waveguide (WR-340) peak E-field = 25 kV/m	
Antenna type	**rE_peak**
Open ended WR-340	540 V
Pyramidal Horn	2200 V
Reflector antenna (2.5 m^2)	4680 V

2.3 Ultra wideband waveforms

In the other end of the classification of the spectra of electromagnetic sources is the ultra wideband (UWB) source. These are sources that produce a very fast time domain transient, typically with a rise-time of 0.1 ns and a FWHM-time of 1 ns. This gives a very broadband signal. The figure below (fig. 16) shows a UWB double exponential waveform and the frequency response of it.

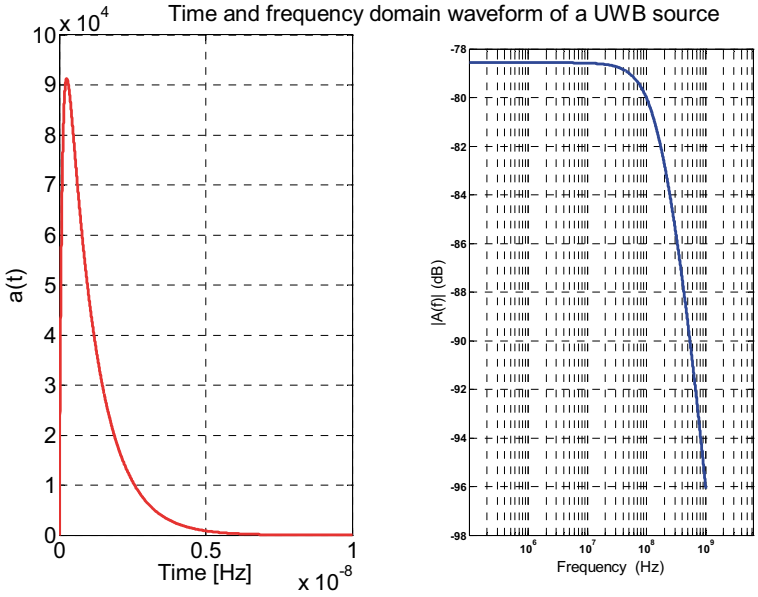

Figure 16. Time domain waveform and frequency domain spectrum from a UWB source with approximate rise-time of 0.1 ns and FWHM-time of 1 ns.

The time and frequency equation for the double exponential waveform is given below [14].

$$\begin{cases} a(t) = A_0\left(e^{-\alpha t} - e^{-\beta t}\right)\cdot u(t) \\ |A(f)| = \left|\dfrac{A_0(\beta-\alpha)}{(\alpha+j\omega)(\beta+j\omega)}\right| \end{cases} \tag{2.4}$$

where α and β relate to the FWHM and rise-time respectively and A_0 is the peak value (observe that $A_0 = A_0(\alpha, \beta)$). The term u(t) is to ensure *a(t) ≡ 0; t<0*, the "Heaviside step function".

Opposite to a narrowband source, (where the power is concentrated around a single frequency) an UWB source spreads the power across a large frequency band. It has a very short duration in the time domain meaning that the energy of the pulse is small. Due to this it is more difficult to create permanent damage to a system by using a UWB source. However, as it is almost certain to cover the resonance(s) and other vulnerable frequencies (operational bands) of the system, it may still create interference (see Chapter 5). The figure below (fig. 17) shows the basic circuit diagram for a simple pulse generator. First a charging unit charges the energy storage unit (1.), which can, e.g., be of capacitive (here) or inductive nature, to a high voltage. A switching section (2.), where a spark gap is often used delivers the stored energy to the pulse shaping network (3.) where the impedance networks (Z1 and Z2) shapes the pulse to the desired waveform. Finally the transient is delivered to the load (4.) which may be an antenna, a system or a batch of milk in case of sterilization measures.

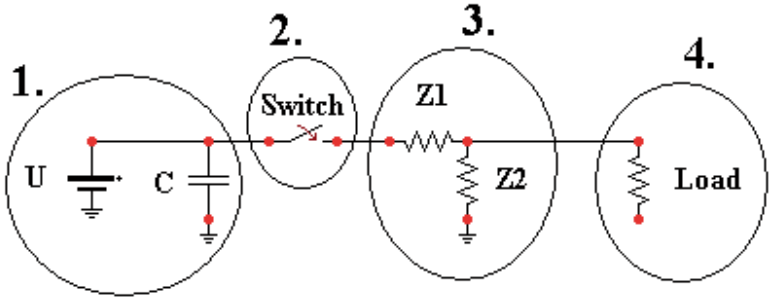

Figure 17. A simple circuit diagram of an impulse generator.

The table below shows some UWB systems used for HPEM research, also observe the high distance normalized peak electric field values.

Table 5. *Modern UWB systems [14].*

Name	Waveform	Reflector area [m^2]	Far-field [kV/m]	rE [kV]	bandratio
IRA1, USA	60 kV; 100 ps/20 ns	10.5	4.2 @ 301m	1280	100
IRA2, USA	75 kV; 85 ps/20 ns	2.6	27.6 @ 25 m	690	50
IRA, Switzerland	2.8 kV; 100 ps /4 ns	2.5	0.22 @ 41 m	10	50
IRA, Netherlands	9 kV; 100 ps/4 ns	0.6	No information	34	25
IRA, Germany	9 kV; 100 ps/4 ns	0.6	No information	34	25

2.4 Damped sinusoidal waveforms

Damped sinusoidal sources combine the short rise-time of an UWB source with the centre frequency and higher energy content (than the UWB source) of a sinusoidal waveform. It is considered to be a very good compromise with a very broad bandwidth, thus, most likely covering most resonance frequencies of a system and still carry a great deal of electromagnetic energy around the centre frequency.

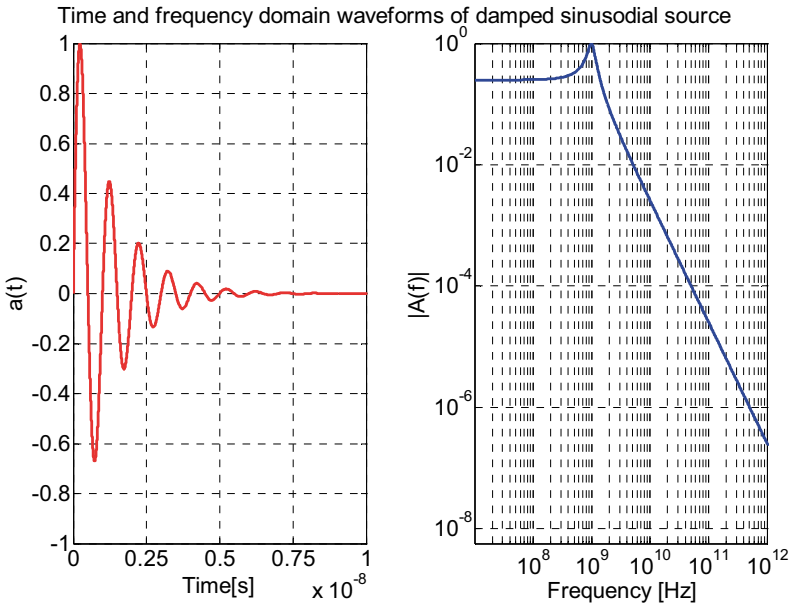

Figure 18. Normalized time domain waveform and frequency domain spectrum from a damped sinusoidal source with 1 GHz oscillatory frequency.

The time and frequency equation for the damped sinusoidal is given below [14].

$$\begin{cases} a(t) = A_0 e^{-\alpha t} \sin(\omega_0 t) \cdot u(t) \\ |A(f)| = \dfrac{\omega_0 A_0}{\sqrt{\left(\alpha^2 + {\omega_0}^2 - \omega^2\right)^2 + 4\alpha^2\omega^2}} \end{cases} \tag{2.5}$$

where A_0 is the peak amplitude, $\omega_0 = 2\pi f_0$, f_0 is the centre frequency and α the dampening factor of the oscillation. The term u(t) is to ensure $a(t) \equiv 0;\ t<0$ and is the "Heaviside step function". Figure 19 below shows the electric field produced by the RADAN 303B, a HPEM generator used in this thesis for Paper V and VII, which produces a damped sinusoidal waveform with ultrawideband frequency response.

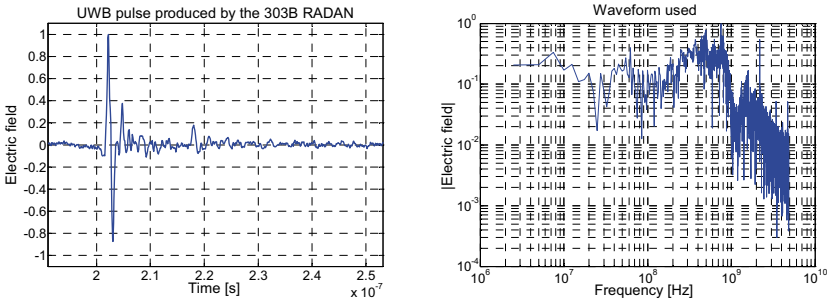

Figure 19. Normalized time domain waveform and frequency domain spectrum of the electric field generated by the RADAN 303B UWB source used by the author (adopted from Paper VII).

2.5 Summary

In Chapter 2 we saw how very different the waveforms, that need to be considered for IEMI, can be. Most other waveforms are similar to, or can be formed from, the narrowband, ultra wideband or damped sinusoidal waveforms. Also, we defined different classes based on the bandwidth of the signal to be able to group different sources together. However, observe that limiting oneself to a few sources or waveforms when performing an IEMI analyses is to greatly hindered oneself. IEMI is not of any particular waveform.

3 Coupling path

In Chapter 3, the different coupling paths for the electromagnetic energy from source to receiver will be discussed. Especially, conducted coupling paths will be investigated and the threat from transients directly injected into a network (power, computer, telephone, etc.) will be investigated with some disturbing possibilities as a result.

3.1 Introduction

As stated previously, the two possible classifications of coupling paths are radiated and conducted. The transfer function from the source to the receiver (victim system) can be written using equation (3.1), taking into account the different coupling factors, e.g., through external shield. It should be noted that for a given situation, from the source to receiver, electromagnetic energy can change back-and-forth between the two coupling paths. For example, an electromagnetic disturbance may originate as radiated free field energy but later couple to a conductor. Propagating along this conductor it could, for some reason, re-radiate again, and finally couple to a, e.g., the leads of a system.

It can, however, be argued that the two coupling paths are merely different expressions of the same phenomena; electromagnetic fields propagating in some medium and also possibly constrained by some boundaries or structures. In this light, conducted transients can either be propagating in the cable insulation and guided by the metal conductors, as in the case of differential mode (DM) transients, or mostly propagating in the medium around the conductor structure, as in the case of common mode transients.

The results and conclusions presented in this chapter are not only for use in an IEMI investigation, but can also be used in other scientific areas, e.g., PLC (power line communication) studies the technique of relaying information in a power network, to attain an internet connection through the use of existing cable routings. Propagation characteristics of transients in low-voltage power installation cables presented here can also be relevant for PLC studies.

3.2 Radiated coupling

Looking back at previous EMP research, the majority has focused on system vulnerability to radiated threats, which may be due to the military legacy (from HEMP). Research have however been done on the coupling of fields to conductors, e.g., power lines. The coupling from a source to a port of the victim system can described with (same as equation (1.8) in Chapter 1 but in different form):

$$P_i = P_s \cdot T_a \cdot T_p \cdot T_o \cdot T_i, \qquad (3.1)$$

where the power measured at the port of interest (P_i) is a function of the source power (P_s) and the transfer functions for the antenna (or launch "vehicle"[6]) (T_a), propagation along the coupling path (T_p) (free-space, medium or conductor bound), coupling through the system exterior (T_e) and interior coupling of the system (T_i). This is of course dependent on, e.g., the frequency, polarization and angle of incident field, as well as parameters of the system itself. For instance, a system with large apertures has, generally (as this depends on the shape of the aperture and the structure of the system inside the aperture), a large transfer function but for a system with small apertures this is smaller. These transfer functions can also include conducted disturbances (on cables and other metallic conductors entering the system) and thus also give an estimate on the degree of filtering or surge protection installed.

Even though irradiated back-door coupled disturbances with smaller wavelength may penetrate apertures more easily, it may well be these disturbances with frequencies above a few GHz may rarely affect systems. This can be explained by the following; the wavelength, λ, decreases and, thus, decreases shielding effectiveness of the system (e.g., increase effective area of apertures). This facilitates access through slots, apertures and other openings. The electromagnetic field will, when entering a complex system (e.g., a computer) reflect and re-radiate from the metallic structures inside and it has been seen [22] - [24] that the directivity of cables inside a complex system can, statistically, be seen to be approximately random and, thus, isotropic (D = 1). Assume now that the wires inside are matched to their connected components, thus no reflection due to impedance mismatches. The effective antenna area of wires inside the system decreases with decreasing wavelength (as the directivity is $\approx$1 in the frequency band considered), which decreases the field to wire coupling[7]. For frequencies above a few GHz the dominant

[6] In the case of a directly injected disturbance into a network a "cross connector" is often needed to connect the source output to the network input.

[7] $A_{eff} = (\lambda^2/(4\pi))*D_0*p*q= \lambda^2/(8\pi)$, where A_{eff} is the effective antenna are, D_0 is the directivity of an isotropic antenna (source) (D_0=1), p is the polarization mismatch factor (p=1/2 for random radiation pattern) and q is the impedance mismatch factor (we assume q=1).

part of these two opposite phenomena (coupling through apertures versus onto wire structures) may be the antenna area and coupling onto wire structures which decreases coupled power to the system. The exception to this statement is front-door coupling (systems having antennas that work in the GHz region (see Paper IV and Chapter 6) and also for conducted transients directly injected into power and/or communication ports of a system (see sections below).

It should be noted that radiated coupling to conductor systems entering a facility or equipment will appear as conducted disturbance at various equipment ports.

3.3 Conducted disturbances

Investigating the civilian infrastructures vulnerability, a DM conducted disturbance may be a serious threat due to several reasons:

1. Easily accessible and unprotected ports (e.g., power-, lamp-, computer sockets, etc.) available in almost all facilities.
2. The connecting network, power or information, link a large number of systems together, that all have the potential to be reached by a directly injected transient.
3. If a facility has surge mitigation installed in, it is most probably only intended for lightning protection, thus positioned on the roof (outer shield) or on incoming power lines, and not within the network.
4. As opposed to a situation where a system is irradiated by a source, no antenna is needed to deliver the power to the port of injection.
5. Also, connecting a source, hidden in an inconspicuous casing, to a power socket may draw less attention, than using a large antenna.

Due to these reasons, investigations on the propagation of DM UWB transients in low-voltage power cables used in most facilities, and the networks formed by these have been performed.

3.4 Transmission line theory

To investigate pulse propagation along conductors using Transmission Line (TL) theory is a good approach to bridge the gap between simple circuit analysis and the complex full wave solution of Maxwell equations. However the TL method (for lossless conductors in a homogenous medium which may be lossy itself through dielectric losses) assumes a TEM (Transverse Electromagnetic Mode) as the main mode of propagation. If the TL requirement is fulfilled, that is, if conductor structure is electrically long, i.e.. much

longer than the wavelength λ considered, and the structure's cross sectional dimensions, e.g.. conductor separation, is electrically small compared to the wavelength λ, then TEM can be assumed to be the main mode of propagation. If not, in addition to the TEM modes higher order of TE and TM modes may start to dominate. For the wire separation, some ambiguity exist concerning the actual distance needed to achieve higher order modes and it has been claimed (see [25]) that for a uniform two conductor structure a wire separation of as small as λ/40 will cause the TEM mode to start collapsing into additional TE and TM modes. However this is a subject under debate. If the conductors are not perfectly conducting (lossy), but otherwise the assumptions above are met, TEM mode is still assumed (so called *quasi-TEM*). A description of how characteristics such as the impedance, but also voltages and currents, can be calculated for a transmission line can be found in Appendix I.

3.5 Comment on Paper II "Propagation of UWB Transients in Low-voltage Installation Cables"

As explained above the TL method is only valid for TEM or quasi-TEM mode. It can not accurately incorporate higher order TE and TM modes. i.e.. it cannot describe radiation losses from these. If going back to physics, radiation is considered to be associated with a time-varying current or charge acceleration (or deceleration). A system experiences radiation losses if the time average Poynting vector is directed away from the system indicating net energy loss. This means that a TL might perhaps be expected to radiate if the conductor structure (in addition to having a time-varying current) is bent, truncated, non-uniform or terminated. Looking at a TL carrying a single time-domain pulse this means that some power of the pulse may be lost if it radiates as a consequence of a change in charge velocity, e.g., at a bend. Some questions must however be asked

- What are the conditions for, e.g., a bend to radiate (conductor structure and waveform)?
- If radiating, how much is radiated for different types of bends?
- If radiating, is the power lost through radiation enough to create a "natural protection"?
- Can the behavior be simulated using numerical code?

These questions need to be answered to determine the threat from directly injected transients in civilian facilities. Paper II addresses these issues and tries to determine if the TEM mode launched from the source (the DM UWB transient) is preserved in the cables tested, straight or bent.

Figure 20. A readily available power socket found on the outside wall of a critical civilian infrastructure facility.

3.5.1 Experimental challenges with UWB transients

The challenges to be addressed in measuring conducted UWB transients (for IEMI investigations) are several.

- Both large voltages and short time durations can be expected, which causes need for both sensitive and robust measuring devices, something which is hard to achieve with conventional voltage/current and/or field probes.
- The measuring system needs to have sufficient bandwidth, sampling rate and memory depth since it can be desirable to measure at several places simultaneously to correlate any eventual effects.
- UWB sources often have coaxial outputs (of different type), which, for a conductor bound test, have to be matched to the port used for injection or measurement. This is done with cross-connectors (see fig. 21 or 31) which may be frequency dependent.

To get a measuring device (probe) with sufficient bandwidth, the cable was directly connected (through a cross-connector and an combined attenuator and balun) to a fast oscilloscope acting as the 50 Ω load. The frequency dependence of the cross-connectors are handled in the following way; a suitable reference measurement (this has to be designed for each experiment) is made first with the setup, after which the investigation starts. The obtained data is later compared to the reference measurement, thus, if the cross-connectors aren't changed the effect of these cancels out. For example, in the experiment described in Paper II, the voltage received when the DM UWB transients has only propagated in a 1 m long cable is used as a reference case, to which the other cases are compared (to see the effect of longer cables) and not with the source waveform (which is distorted by the cross-connectors at the cable ends, but it is assumed that for each cable length the frequency dependence of the cross-connectors is unchanged).

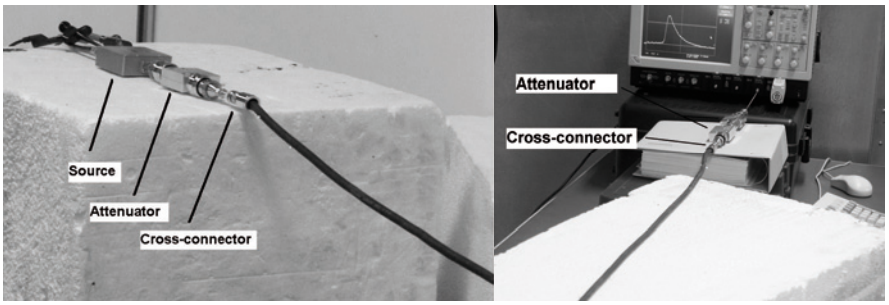

Figure 21. The setup of test for the low- voltage installation cable at the source end and load end.

3.5.2 Results and conclusions

3.5.2.1 Attenuation in straight cable

The average attenuation of the received peak voltage at the load, for the cable lengths studied, were, approximately, between 1 and 1.5 dBV/m when DM UWB transients were injected (see fig. 22).

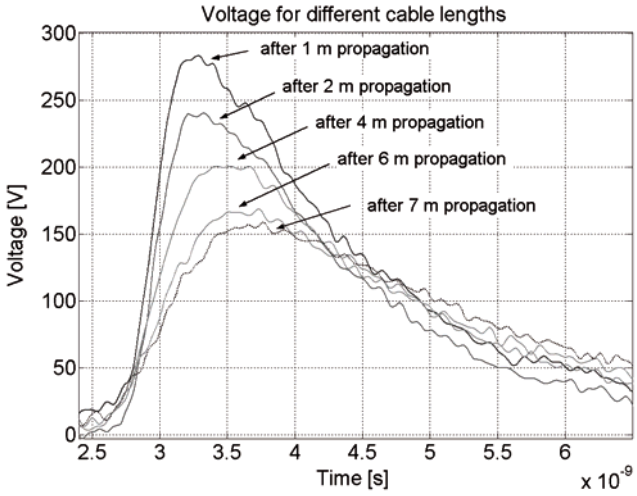

Figure 22. Experimental results of the received voltage. Notice the approximate 1 to 1.5 dBV/m attenuation in peak voltage

For common mode injection into a seven meter cable the attenuation was much higher, approximately an additional 20 dBV more. However, this was seen to be much below the reduction in received voltage as a consequence of the mismatch between source-cable and cable-load. As can be expected the

change in rise-time and pulse width per meter propagated cable was a linearly increasing function which is shown in fig. 23.

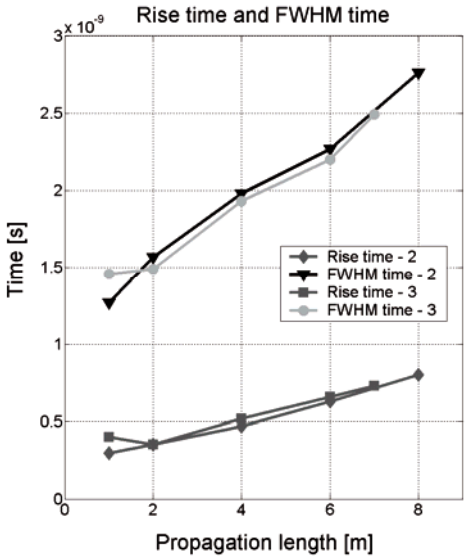

Figure 23. The change in rise-time and pulse width, for the cable types and lengths studied, is a linear function of the cable length (adopted from Paper II compare the linear behavior with fig. 6 in Paper III)).

The change in rise-time and FWHM-time per propagated meter of cable is shown in fig. 23 above and the approximate linear relationship is shown. The change in rise-time is approximately 65 ps/m and the change in FWHM-time is approximately 200 ps/m.

3.5.2.2 Attenuation due to bend

To investigate if a bend on the cables studied radiates substantially for the DM transients injected the *Grosseteste's method of Falsification* is applied. That is:

$$\frac{\begin{array}{l}\text{If H then C}\\ \text{not C}\end{array}}{\therefore \text{not H}},$$

where:

H = "a bend, on the cables tested, significantly radiates power for the transients injected"

C = "less power (voltage) will be received at the oscilloscope".

Different types of bends where studied and no measurable difference in the received voltage (see fig. 24) could be detected which leads to the conclusion that the radiation-loss from the bends is negligible for the low-voltage power installation cable and for pulses with rise-time in the sub-nanosecond region. This conclusion is made as the measured voltage (V), over the resistance (R) of 50 Ω (oscilloscope input impedance) is related to the power (P) through, $P = V^2 / R$ and even a small change in measured voltage would mean a large change in received power. A constant and ideal resistance of the oscilloscope is assumed, however this can be assumed since the oscilloscope input impedance (acting as load) is specified for shorter rise-times and bandwidths exceeding the transient used in Paper II and should thus be constant for the transients used here. Also, a D-dot probe was used to measure any field from the bend and none could be measured. It is thus concluded that the TEM field structure is, beyond our measuring capability, preserved through the bend, which might be due to the electrically small conductor separation of the cable.

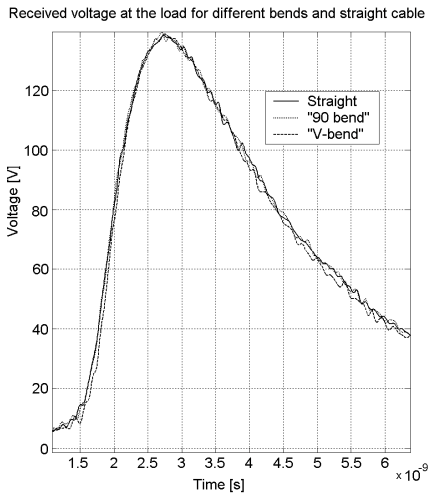

Figure 24. No measurable effect in received power could be seen for different types of bends in a low-voltage power installation cable.

Also, as the TEM field is the dominant propagation mode, the pulse propagation can be modeled either by MTL-FDTD (multiconductor finite-difference time-domain) code or using the exact solution for pulse propagation between two conductors (see the equation in the Appendix of Paper II).The following conclusions could be drawn from the investigation performed in paper II:

1. A differential mode injected transient can propagate large distances in a low-voltage installation power cable with little attenuation per meter propagated cable.
2. The majority of the received power is lost due to the impedance mismatches between source, cable and load. While propagating in the cable, the losses are mainly ohmic in nature and not radiation losses.
3. No measurable power is lost in bends when injecting in differential mode in a low-voltage installation power cable.
4. The main mode of propagation of the differential mode transient is quasi-TEM.

3.6 Junctions and cable branching

In the previous section it was suggested that for DM UWB transient directly injected (even with very fast rise-times, thus, high frequency content) in a straight low-voltage power installation cable TEM is the dominant mode of propagation (disregarding any eventual extra higher order modes, as well as any CM currents and voltages, created at the injection point due to mismatches between source and port). Also, unfortunately from a protection view-point, it was seen that any eventual bends on the cable, will not effect the propagation of this transient to any measurable degree (no power loss, due to radiation from the bend, could be measured) and act as an inherent form of protection. However, in a real facility (or distributed system) there are components, other than cables, that are frequency dependent and can influence the electromagnetic field modes of the propagating transient:

Junctions:
- for branching cables
- between different types of cables

Grounding points
Loads and terminations
Non-linear components:
- surge protective devices
- filters
- transformers
- diodes

Accidental elements:
- arcing
- short-circuits
- broken cables or separated conductors

These components will affect how transients spread in the network and how much of the quantity of interest (e.g., power, voltage, etc.) is received at any

given port. The most frequent component in a power network are different types of junctions for branching cables and will therefore greatly affect the way transients propagate and spread. Investigation of different types of junctions (for branching cables) was investigated in Paper III, as well as a real installation network in a civilian facility.

Generally, if a transient, $V_1(f)$, is injected into a network it will attenuate by a certain factor, $k_1(f)$, as it propagates along a cable section. If it propagates through some component this will transmit a fraction, $T(f)$, of the amplitude through and a transient, $V_2(f)$, will reach the a load or system after propagating another cable section and, thus, also attenuate by a factor $k_2(f)$.

$$V_2(f) = V_1(f) \cdot k_1(f) \cdot T(f) \cdot k_2(f) \tag{3.2}$$

This approach also holds true for junctions. As stated before (Paper II), the attenuation when injecting DM UWB transients in low-voltage power cables is not very significant for shorter distances therefore the transmission coefficient through the component maybe more of interest.

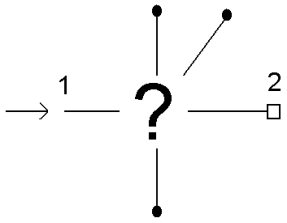

Figure 25. The behavior of junctions is of great concern for the vulnerability estimate of a network.

Provided that the original assumption, i.e., that TEM is the main mode of propagation, the transmission coefficient through a junction can be calculated using known techniques. Referring to fig. 26 and assuming that the TL requirements are fulfilled for all the cable sections, and also having similar characteristic impedance, Z_0, the reflection coefficient, Γ_T, and transmission coefficient, T_T, of a junction containing three separate cable sections (so called "T-junction", e.g., (A) in fig. 26), can be described by:

$$\Gamma_T = \frac{Z_0 // Z_0 - Z_0}{Z_0 // Z_0 + Z_0} = \frac{Z_0 / 2 - Z_0}{Z_0 / 2 + Z_0} = -\frac{1}{3} \quad , \tag{3.3}$$

$$T_T = 1 + \Gamma_T = \frac{2}{3} . \tag{3.4}$$

Since the branches are connected in parallel, the voltage transmitted through the junction will propagate along both branches and if the cable sections have the same characteristics (as assumed here), the current will be equally divided between them. If the junction is a so called "star-junction" with a total of N+1 number of branches [e.g., (C) or (D) in fig. 26 having N+1=4 or N+1=5] that have the same characteristics, the voltage reflection (Γ_*) and transmission coefficients (T_*) are give by:

$$\Gamma_* = \frac{Z_0/N - Z_0}{Z_0/N + Z_0} = -\frac{(N-1)}{(N+1)}, \tag{3.5}$$

$$T_* = 1 + \Gamma_* = \frac{2}{N+1}. \tag{3.6}$$

The T-junction is a special case of a star-junction, which is seen by setting N+1 = 3 [(3.3) and (3.5) becomes identical to (3.4) and (3.6)]. Accounting for the propagation constant and assuming that the cable sections are identical (same cable length, L, and characteristics), the voltage received at a port "down-stream" from a single T-junction [(A) in fig. 26] is:

$$V_2 = V_1 \cdot e^{-\gamma L} \cdot T_T \cdot e^{-\gamma L}, \tag{3.7}$$

where V_0 is the applied differential voltage at one end of a branch, without considering source and cable reflections (forward traveling wave), γ is the propagation constant of the cable type used, and T_T is the transmission coefficient for the T-junction. This expression can of course be modified to handle cables of different types and lengths or to include the term for reflection between source and cable.

If we make the assumption that TEM is the dominant mode of propagation, even through the different types of junction present in a low-voltage power network, then we can use TL theory to describe the propagation through the junction. Also, since it is much more likely that DM transients will deliver the more power than CM, thus, being a larger threat, only DM will be examined. Both simple junctions using low-voltage power cables in a laboratory setup and the power network of a facility were investigated.

3.7 Comment on Paper III "Propagation of UWB Transients in Low-voltage Power Installation Networks"

3.7.1 Transients injected into simple junctions

The junctions in the laboratory setup will not exactly correspond to the junctions made by an electrician in a real low-voltage power network, but the behavior of them will greatly contribute to the knowledge of the propagation of UWB transients and the dominate mode while propagating through these. The different types of junctions investigated in the laboratory setup are given below in fig. 26.

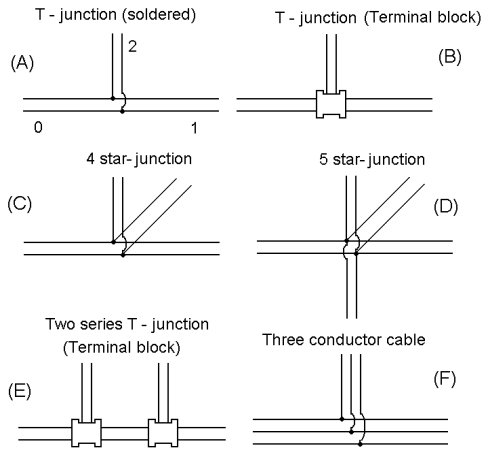

Figure 26. The different types of junctions investigated for propagation of DM UWB transients.

The junctions were made, either by directly soldering the conductors together or terminal blocks designed for the purpose. First it was seen that no discernable difference could be measured between soldering the junction or using block connectors (see fig. 28) and also the difference between keeping the conductors used for injection close to each other and separating them (increasingly violating the TL requirements of small conductors separation) was very small (see fig. 27 below).

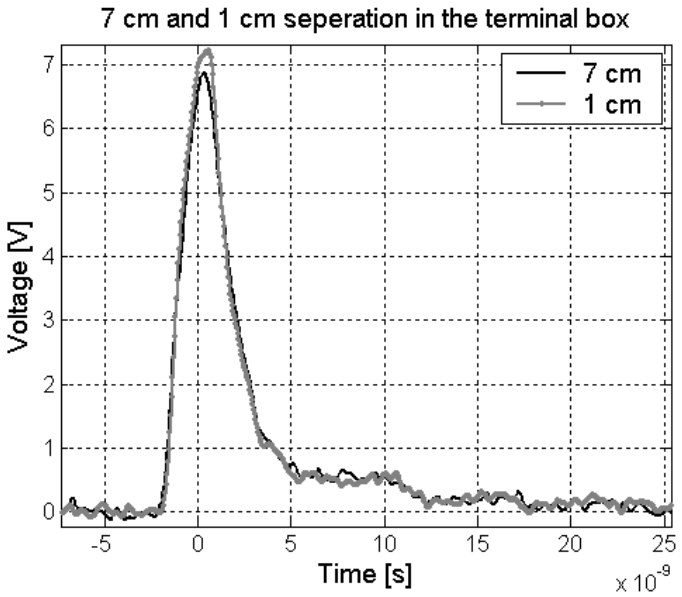

Figure 27. The difference in conductor separation when using a block connector to create the branching junction, when the used DM UWB transient was injected.

Just as in paper II described above, it is necessary to use cross-connectors to connect the source to the cable and the cable to the load (oscilloscope). These have unknown frequency dependence and, thus, instead of using the source waveform as a reference the voltage received at the oscilloscope for a straight cable without a junction is used as reference. If a junction with a third cable branch is added in the middle of the original cable, the voltage received at the oscilloscope is compared to the reference (straight cable without junction). Thus, the frequency dependent factor that arises from the cross-connectors cancels out and the effect of the junction on the transient propagation can be examined.

Fig. 28 shows the cases of injecting a DM UWB transient (from the 004A RADAN source [26]) into a straight cable (used as reference) and also with a T-junction in the middle. Comparing these two voltages allows us to calculate the transmission coefficient through the T-junction. Theoretically this is 2/3 (3.4) and the experimental result gives a transmission coefficient very close to this, supporting the hypothesis of TEM being the dominate mode of propagation for these simple T-junctions.

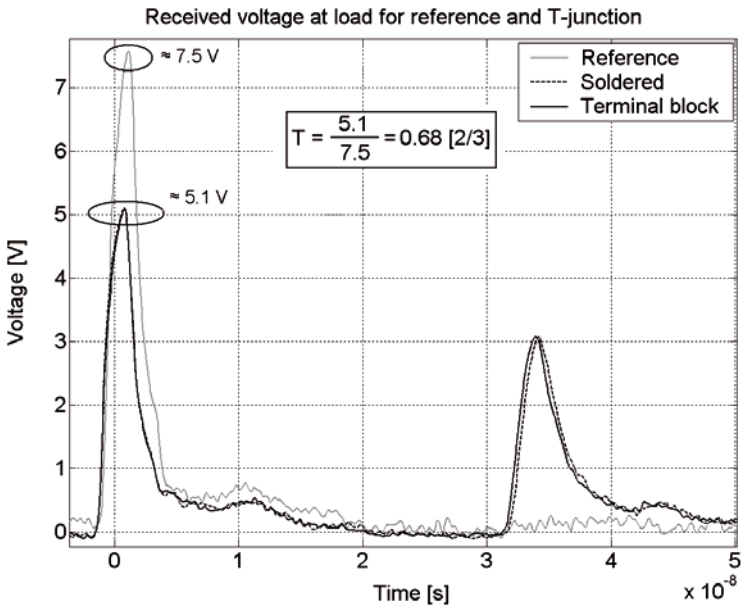

Figure 28. Comparing the reference voltage (6 m straight two conductor cable alone) and a T-junction added either through direct soldering or use of a terminal block. The first reflection is also shown.

By scaling the received voltage through a T-junction with the theoretical transmission coefficient [=2/3 from (3.4)] and over-lapping this waveform with the reference, it can be seen that almost no discernable difference between the two waveforms exists (see fig.29). A radiation loss at the T-junction would, for some frequencies in the spectrum of the transient, diminish the amplitude. This would show up in the time-domain as a change in the waveform, compared to the reference case.

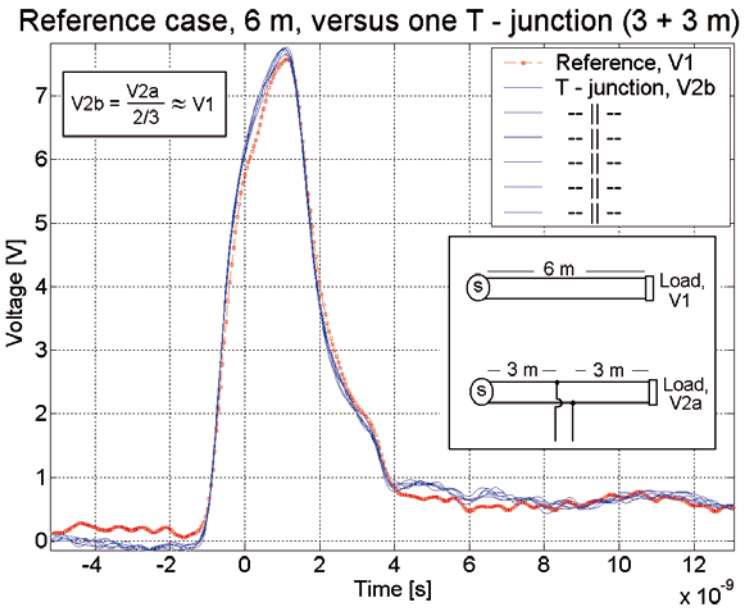

Figure 29. Voltage waveforms for the reference case and the voltage received through the T-junction scaled with the theoretical transmission coefficient.

To some extent, the original assumption that TEM is the main mode of propagation for DM UWB transients through junctions has been established. Still, it may be argued that the symmetry in the electromagnetic field structure will be disrupted if more branches are added at the junction. Severely disrupted field symmetry means that other field modes, TE and TM, may dominate and thus power may be lost, through radiation, from the TEM wave propagating towards the load (reference point). If that is the case, less power reaches the systems attached, compared to if no power is lost through radiation at the junction.

According to TL theory, the theoretical transmission coefficient of a 4-star and 5-star-junction (total number of branches, N+1) is 1/2 and 2/5. A very good correspondence between this theoretical value and experimental results was found (see fig. 30, theoretical value given in brackets). The difference is approximately only 1% for a 4-star-junction but 6% for a 5-star-junction. This suggests yet again that TEM is the dominant field mode and that this symmetry is largely preserved through the junctions examined here. Therefore, no significant power seems to be lost in the junction, through radiation, when the tested DM UWB transient propagates through these junctions.

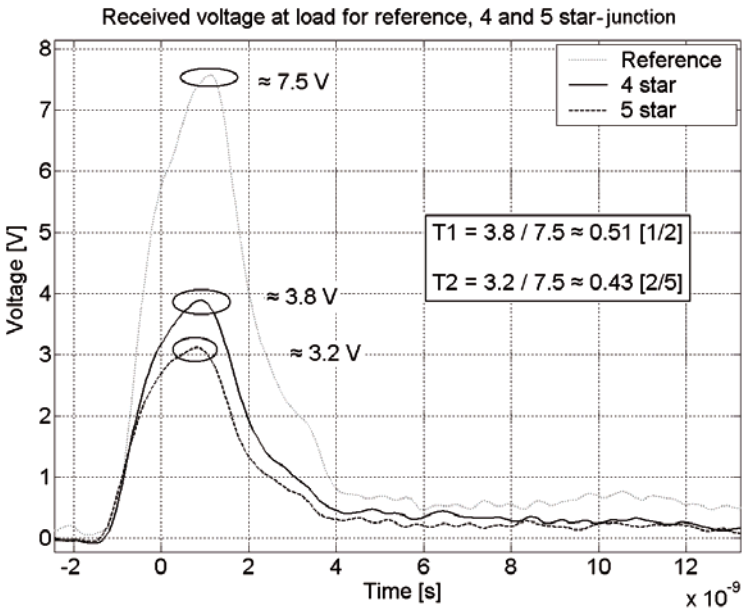

Figure 30. The voltages received through a 4-star and 5-star-junctions and also the reference case (cable without any junction). As can be seen the transmission coefficients for the 4-star and 5-star-junctions (T1 and T2, respectively) is very close to the theoretical values (in brackets), which supports the hypothesis of TEM also being the dominant propagation mode through these junctions.

Thus, for a low-voltage power network, which can be described by junctions and cables with the same characteristics as the ones tested above, our hypotheses that TEM is the dominant mode of propagation) is confirmed. Therefore the propagation through these junctions can be described by transmission coefficients obtained through TL theory. Thus, a DM UWB transient injected into a power socket will not suffer any significant loss in power, due to the junctions, since only a re-distribution between the different ports in the system takes place. Thus, the TEM field being launched from the source is preserved. The reason for this, as also concluded in paper II, is the preservation of the field structure due to the close proximity of the conductors in the cables and junction, compared to the wavelengths of the transient.

3.7.2 Transients injected into civilian facility

It was seen that for some junctions, having electrically small conductor separation, TEM is the dominant wave propagation mode. However, in a real civilian facility this property may not be fully true for the entire network. Some sections may fulfill the transmission line requirements, thus the method above could be used, and some may not. Consequently, other fac-

tors, than the reflection due to the mismatch between cable and junction, can give rise to a decrease in the received voltage at a port.

Previous tests with injecting transients (reported in [14] and [27]), of different frequency characteristics, into the secondary side of the externally positioned feeding transformer of the power network of a facility reports a large attenuation for frequencies above a few MHz. However, the nature of the decrease in received voltage was not clear (e.g., skin-effect or reflection). Also, in an IEMI situation an attacker may acquire access to possible injection ports much deeper into the power network. For example, power or lamp sockets installed in lobby of a facility are easily accessible points that can be vulnerable. Since it was previously seen that 1) a DM UWB transient can propagate, with TEM as the dominant mode of propagation, in a low-voltage cable and 2) for electrically small junctions, TEM is the dominant mode of propagation and 3) injection points can be found deep in a low-voltage network, tests on a real civilian facility was justified and performed.

DM UWB transients (from the 004A RADAN source [26]), with rise-time and FWHM-time of 0.7 and 2 ns, respectively, was injected from an externally positioned and easily available power socket, into the low-voltage network of a civilian facility. The voltage was measured at the power sockets positioned on the inside. The transient was injected and measured by using cross-connectors (fig. 31) between power socket and source and oscilloscope, respectively.

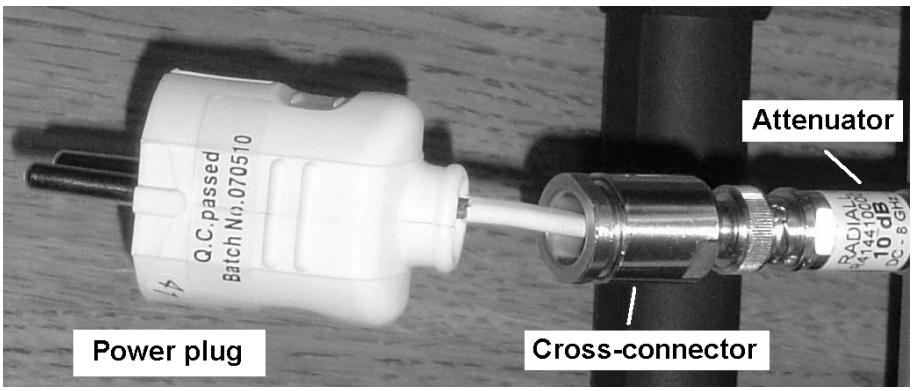

Figure 31. Shown is the assembly used for measuring the received voltages in the low-voltage network consisting of power-plug, cross-connector and attenuator.

As explained previously the cross-connector assemblies have unknown frequency responses which changes the waveform of the source when measured with the oscilloscope. For that reason a reference measurement was made in which a transient was injected into one of two outlets of the same power

socket, and measured in the other of the two. Thus, the measured voltage will, approximately, only depend on the cross-connectors. If comparing the voltages measured at the internal power sockets (when injecting into the external power socket) with this reference voltage it will be possible to exclude the effect of the cross-connectors.

It was seen that the state of the single-pole switches (ON or OFF), in the section studied, affected the voltage received at the various ports (see fig. 32).

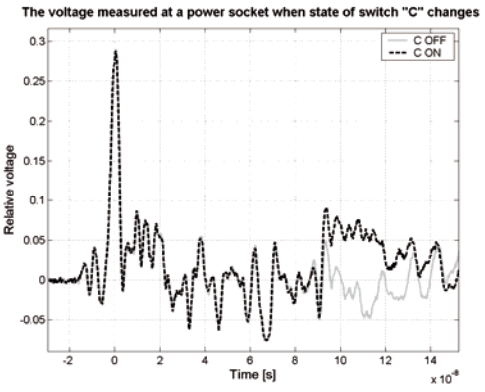

Figure 32. Voltage measured at one of the power sockets inside the facility, when injecting at the outside power socket, notice the difference for switch position.

Since there are several measuring points in the system, several switches, and unknown loads (e.g., lamps), an overall assessment of the result is best reached by the use of probabilistic representation of the data to present the results. Since many times the position, identity, and severity of the most susceptible system in the power network is largely unknown, a completely random placement of this system (that is measuring point) can be made.

The *probability distribution function* (PDF) can be found by examining the occurrence of transients with certain amplitude in relation to the total number of transients. From the PDF the *cumulative distribution function* (CDF) [28] is formed. This describes the probability that a stochastic variable (X) is less than or equal to a number (x), that is CDF = $P(X \leq x)$. The inverse of the CDF is the *complementary cumulative distribution function* (CCDF), that is CCDF = 1 – CDF = $P(X > x)$, which is of great use. The CCDF describes the probability that a stochastic quantity with amplitude X is larger than a certain value x. In fig. 33 the CCDF for the facility test is shown and also showing the distinction between the switch states of “On” and “Off”. Assuming that the voltage is injected into the outside power socket at point 3 (see fig. 15 in Paper III) and the voltage is measured at a

completely random power socket inside the section investigated) the switch state does not have a neglectable effect.

According to fig. 33 the probability of inflicting a voltage (compared to the reference voltage) of 10 % or above is, depending on switch state, approximately between 0.35 and 0.5. If transients with amplitude of 100 kV is injected, this would then give us, with 0.35 or 0.50 probability (depending on the state of the switch), a voltage of 10 kV or more (accordingly to fig. 33). Also, the probability of measuring a voltage in a certain interval (a:b]={x | a < x ≤ b}, at completely random power socket (within the section examined), that is P(a < X ≤ b), is given by:

$$\begin{aligned} &P(a < X \le b) = CDF(b) - CDF(a) = \\ &(1 - CCDF(b)) - (1 - CCDF(a)) = \\ &CCDF(a) - CCDF(b) \end{aligned} \tag{3.8}$$

Thus, the probability of measuring a relative voltage larger than 5% and less than or equal to 25% voltage is, according to fig. 33, approximately 0.5 [CCDF(5)-CCDF(25) = 0.7-0.2 = 0.5]. Thus, there is a 50% chance (0.5) of measuring a voltage between 5 and 25 kV anywhere in the network if 100 kV is injected at the external power socket.

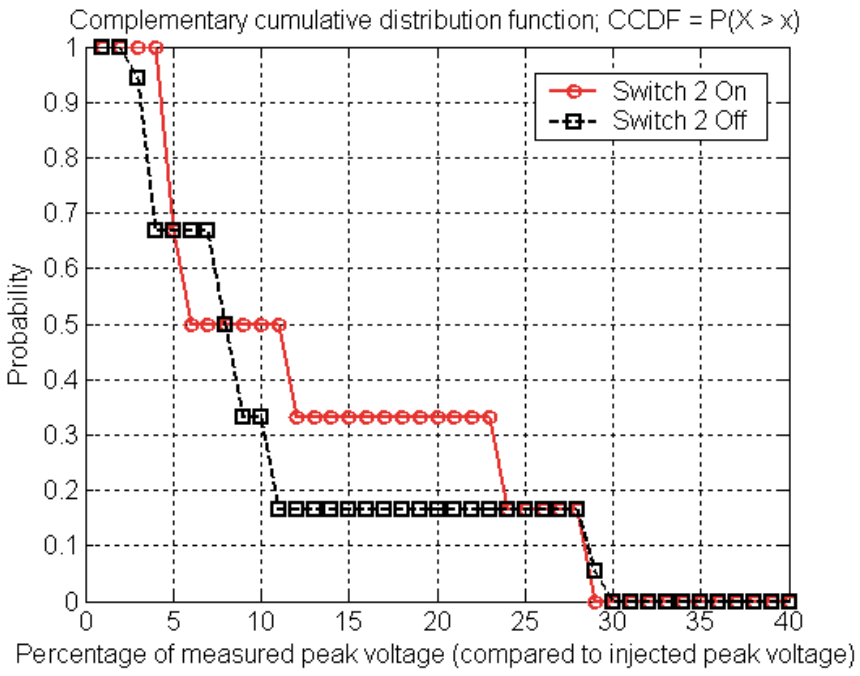

Figure 33. The CCDFs for the two different states of a switch in the network. It is clearly seen that the probability of receiving a large voltage somewhere in the network is larger if the single-pole switch is set to “On”.

One interesting observation was that if the conductor used for injection (the high-voltage lead) was disconnected at the injection point by a switch, no voltage could be measured at the internal power sockets. However if the return conductor of the power socket (i.e., neutral) was disconnected, voltages could still be measured at the internal power sockets. Thus, using a two-pole switch to separate the conductors connecting an external power socket with a low-voltage network could significantly mitigate the DM UWB transients. Also, the voltages received at the different ports could not be explained by transmission line theory, compared to previous junction examined, which is due to the complexity of the network that disrupts the propagating transient. TEM seems to not be the dominant wave propagation mode.

3.8 Summary

In Chapter 3 we saw that electromagnetic energy can follow two coupling paths, conducted along a conducting structure or radiated through a non-conducting medium, and that it is possible for the energy to go back and forth between the two coupling paths.

We discussed the use of the transmission line method along with its limitations and requirements and in Paper II we saw that for DM UWB transients directly injected into a low-voltage power cable, TEM is the dominant wave propagation mode. Also, we saw that a bend on that cable do not significantly radiate any power from the DM transient, thus, not effecting the received power at the load on the other end. As the propagation is mostly TEM it can be easily be simulated by several methods, where FDTD is one possibility.

As Paper II was limited to a single low-voltage power cable, in Paper III the effects of junctions and the behavior of an actual power network of a facility were studied. We saw that for an isolated junction, between low-voltage power cables, the transmission through this can be described by traditional means (using the characteristic impedances of the cable sections and forming the transmission coefficient). Different junction types were tested and it seems that the TEM wave propagation mode is preserved through these junctions even if the junction is made up out of five cable sections (5-star-junction).

In Paper II the power network of facility was also studied. It was seen that from an outside power socket (used for injection of the DM UWB transient) to an internal power socket, the TEM mode was not preserved. This was not unexpected, as the network is very complex with individual conductors not always following the other conductors in the cable bundles. However using statistical methods (complementary cumulative distribution function), the network could still be investigated and the effect of changes to the network (switch states) be studied and judged from an IEMI threat analysis perspec-

tive. Mitigation measures were also suggested, by using a two-pole switch on outside sockets.

4 Mitigation

In Chapter 4 we will talk about the point of entry for conducted systems and a description of some common methods and components used for mitigation of disturbances. Some concerns will also be raised in the use of these against some disturbances, along with the reason for this.

4.1 Point of Entry

The point (or points) in a facility or system where electromagnetic energy, irrespective of the spectrum, can enter and where normally all the power and communications cables crosses the boundary between the exterior and interior environment is called the Point of Entry (PoE). It is defined in [9] as:

> "Physical location (point) on an electromagnetic barrier, where EM energy may enter or exit a topological volume, unless an adequate PoE protective device is provided. A PoE is not limited to a geometrical point. PoEs are classified as aperture PoEs or conductive PoEs according to the type of penetration. They are also classified as architectural, mechanical, structural or electrical PoEs according to the functions they serve."

The protection in an electrical PoE is often realized by having, e.g., breakers, fuses, earth leakage relays, surge protectors, etc., in a shielded box. If the system or facility is shielded with, e.g., a metal mesh then at the PoE the shields of all the shielded cables entering the enclosure is connected to the system shield, thus, creating, for the designed excitation frequencies, a good Faradays cage. Existing surge protective devices (SPDs) are installed at the PoE on the exterior of the shield. It is important that any SPDs are positioned on the exterior of the shielded enclosure so as not to bring any high voltages or currents into the shielded environment (in accordance with normal EMC praxis).

4.2 Comments on Paper VIII "Effect of Conducted EFT Type pulses on the Point of Entry of Electrical Systems in Buildings"

To investigate the threat from conducted IEMI to a civilian system or facility a study of a PoE, constructed accordingly to electrical installation praxis, is essential to determine the response to conducted transients. The components of the PoE are normally only designed and tested for power distribution conditions or for lightning type surges. The response of the components for much higher frequencies is normally not investigated. Also, a PoE may only follow standardized power installation procedures and not EMC regulations and praxis, thus, problems can arise. It is therefore important to construct a realistic PoE following power installation praxis. As was seen in Chapter 3, Paper II and III, transients with great amplitude can easily be injected and deliver a substantional amount of power to an unprotected load. Paper VIII describes an experimental investigation of a realized electrical PoE system (see fig. 34 and 35 below).

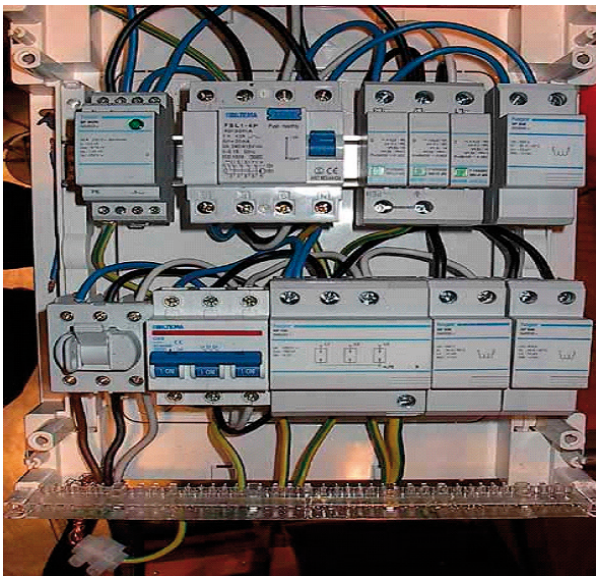

Figure 34. PoE system built and tested

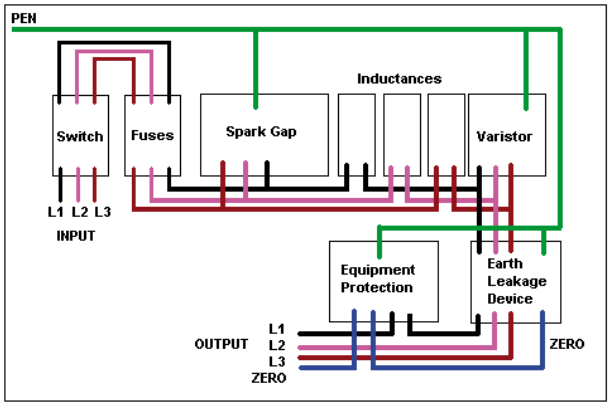

Figure 35. Circuit diagram of tested PoE system (adopted from Paper VIII).

The realized electrical protection PoE system is a three stage protection with spark-gaps (stage I), varistors (stage II) and a combination of the two ("equipment protection", stage III). Also present were earth leakage relays, switches, fuses and inductances separating the stage I and stage II protection, accordingly to normal power installation procedures. The system was stressed with nanosecond rise-time pulses with amplitudes in the kV range. The PoE system was studied for abnormalities in protection ability, e.g., due to increased clamping voltage over the nominal rating and for cross-coupling to conductors not used for voltage injection. It was found that

- The protection ability on the whole of the installed SPDs were as expected from datasheet and reference impulse test (1.2/50 μs) (see, e.g., fig. 7 in Paper VIII).
- The components not normally considered to be SPDs (e.g., fuses or earth leakage relay) was found to not affect the mitigation level at all for the transients injected.
- It was also seen that the setup could couple large voltages to conductors of the PoE not used for injecting the transient and that this voltage increased with decreasing rise-time (see e.g. fig. 9a in Paper VIII).

The observation regarding coupling to unused conductors is important as the area affected by the IEMI attack increases as more phases of the power network is affected, as the transient propagates through the power system.

4.3 Surge protective devices

Surge protective devices (SPDs) are non-linear resistance variable components that shunt away the current, or limit the voltage, of the transient across its terminal. The most common SPDs used are:

- gas discharge tubes (GDT),
- metal oxide varistors (MOV),
- diodes of different types.

Frequency selective filters are often also used as a mitigation measure and, thus, worth mentioning, even though they are not mentioned as SPDs. SPDs are tested for and mainly intended for use against lightning electromagnetic pulses and the behavior when subjected to transients with high frequency content is of great concern. Short descriptions of some common SPDs are for background given below (see [29] for more information). SPDs of different categories can be combined with or without linear (ideal) components to form more complete filters.

4.3.1 Gas discharge tubes

Spark gaps or GDTs are the simplest and earliest form of SPDs. They protect the system by shunting the current to the safety ground. An electrical discharge between two electrodes (three conductors are often used to facilitate breakdown or to include both common mode and differential mode protection in one component) of selected configuration is created and contained in a designed atmosphere which is often a mixture of noble gases (e.g., neon, argon). GDTs are especially used for protection of communications systems, e.g., telephone switches due to the very low parasitic capacitance (typical between 0.5 to 2 pF) giving good performance even for frequencies in excess of 50 MHZ [29]. The GDT can conduct large currents (several kA depending on design) but the drawback of the device is the relatively slow turn on time, the relatively large voltages (> 100 V) needed to conduct and the low arc sustaining voltage which keeps the GDT conducting even if the voltage has fallen below the turn on voltage.

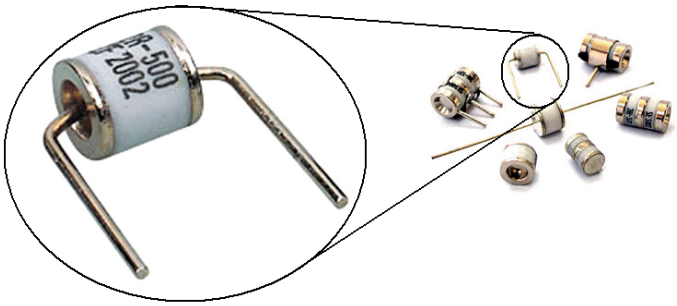

Figure 36. A selection of gas discharge tubes

4.3.2 Metal oxide varistors

The metal oxide varistor (MOV) is the most commonly used type of SPD due to its fast turn on time, relatively large energy absorption ability (though less than for the GDT) and low cost. The disadvantage is the often large parasitic capacitance of the device (1 to 10 nF). The metal oxide material (often ZnO or SiC) has a non-linear V-I characteristics that clamp the voltage across its terminals to a certain level.

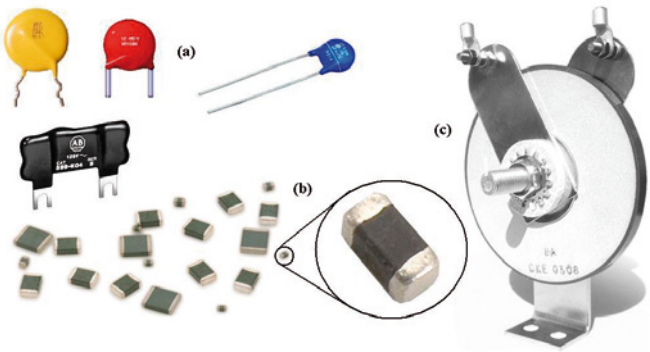

Figure 37. Different types of varistors (not to scale) showing the diverse design from small circuit-board mounted varistors (b) to large power system arresters (c) and low voltage varistors (a)

An important issue (which also is discussed in Paper I below but on different circumstances) is the varistor packaging. If the leads of the varistor are long they could act as a loop antenna and the voltage across the varistor terminals could increase due to coupled field (of course depending on the frequency). Good practice is to have as short leads as possible. See fig. 38 below for a comparison of the response of a low voltage varistor having long leads (approximately couple of cm) and short leads (approximately couple of mm),

otherwise identical, when subjected to a transient with a rise-time and FWHM time of 5 and 100 ns, respectively. This increased voltage will be explained in Paper I.

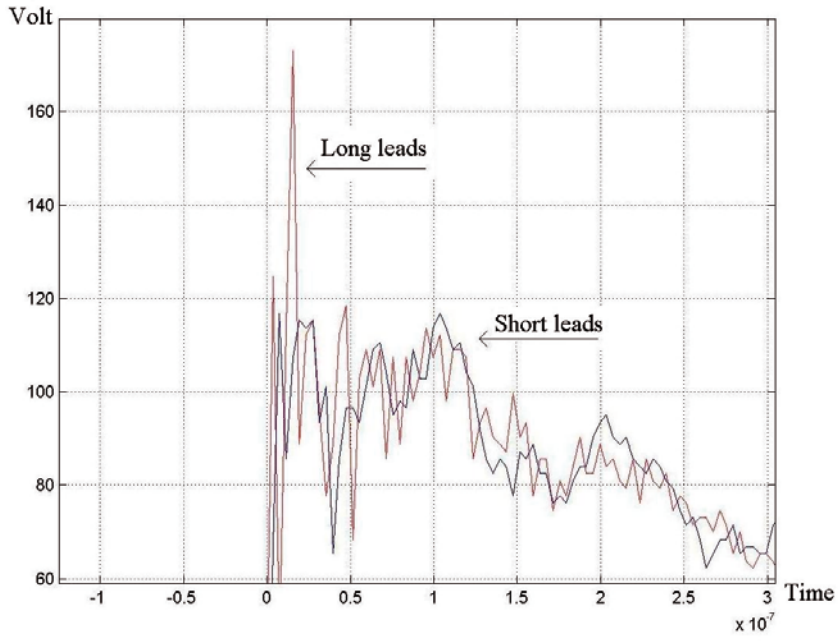

Figure 38. Voltage across the varistor terminals for different lengths of the leads.

4.3.3 Opto-isolation

Even though opto-electronic components are not normally considered when discussing surge protective devices, we'll make an exception here, as they can provide protection from surges. As suggested in Paper IV, to isolate a port (e.g., an antenna) that is connected to sensitive equipment, optocouplers can be used. Of course, these have limits on the isolation ability and break-down strength. Other opto-electronic components could be used to convert the voltage signals to optical signals and carry this with fiber cables to another converter that is connected to the sensitive equipment. The equipment is now galvanically isolated from this port, and from any disturbances this is subjected to. A temporary loss of, e.g., communications, if the first opto-electric converter is destroyed, may be acceptable as such devices are easily replaceable.

4.4 Comment on Paper I "Comments on "Linear and Nonlinear Filters Suppressing UWB Pulses""

One of the most important questions for mitigation of UWB transients with SPDs, is the question of the response time of the nonlinear "elements" (e.g., the response time of ZnO or SF6, etc.) and their ability to switch to their conducting state. It has been reported that COTS ZnO varistors are not useful for these fast transients [30] since the nonlinear clamping effect was not seen (see fig. 41). However it was concluded and shown in Paper I that this is an erroneous statement. The effect seen (or rather the nonlinear effect not seen) limiting the use of the ZnO varistor can be found to originate from parasitic inductances of the varistor leads. Due to the high frequency content of the UWB transient, the transient experiences a high impedance path through the leads. This results in a large voltage drop over the varistor leads and for frequencies between 1 to 10 GHz more than 99% of the voltage was dropped across the inductance of the leads. As a result the ZnO material was not subjected to a voltage exceeding its clamping value. Approximately 2 - 4 V/(grain boundary) is needed across the intergranular grains to elicit the nonlinear behavior of ZnO [31].

It was also observed that the data reported for the varistor components in [30] had the same high frequency behavior as a capacitance, and in Paper I it is shown that they could be modeled very precisely by a simple non-ideal capacitance (see fig. 39 - 41). The capacitance and inductance of the varistor were found from the varistor specification and from a frequency analysis of the varistor component performed in [30]. Also, it was suggested that a feed-through capacitor be used for protection instead of the varistor, the response shown could also be simulated with a simple capacitance model and data from [30] (see fig. 42).

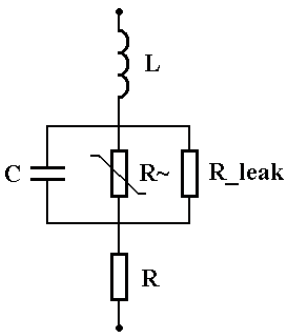

Figure 39. Simple physical model of the ZnO varistor with lead inductance (L) and resistance (R), disc capacitance (C), leakage resistance through the ZnO oxide (R_leak) and the nonlinear resistance of the ZnO (R~)

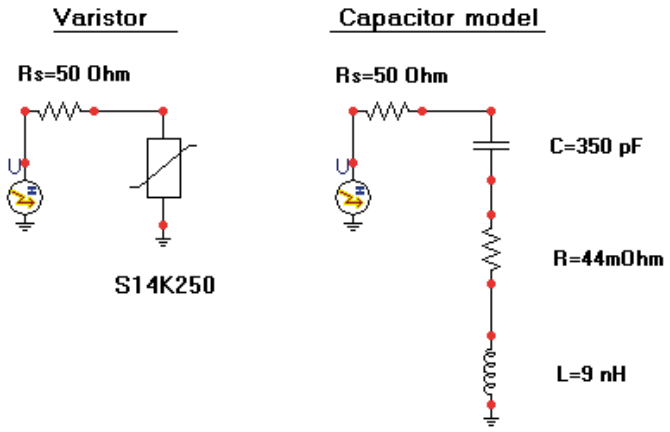

Figure 40. The varistor can be modeled by a non-ideal capacitance and for high frequencies most of the amplitude of the transient is lost over the lead inductance.

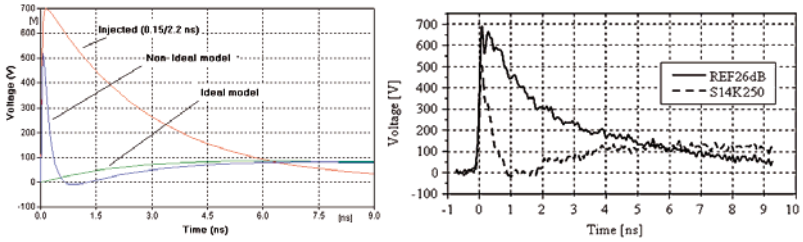

Figure 41. The ideal and non-ideal response of a capacitance to a UWB transient (150 pico-second rise-time), using data on the varistors from [30] (left) and the ZnO varistor response reported in [30] and the UWB transient used (right).

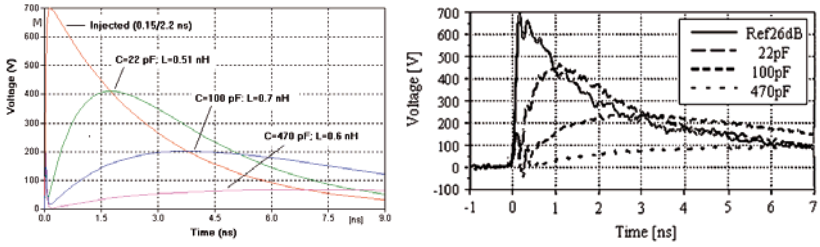

Figure 42. The ideal and non-ideal response of a capacitance to a UWB transient (150 pico-second rise-time), using data on the feed-through capacitances tested in [30] (left) and some feed-through capacitors also tested in [30] (right).

It is clearly shown that for transients with picosecond rise-time the high frequency content generates, if leads are present, large impedances through the inductances of the leads, and that the dominant frequency behavior of the

varistor component then arises from the packaging. The response time of the ZnO material is still an open question and some manufacturers claims response times in the order of 200 ps.

4.5 Summary

In Chapter 4 we discussed the point of entry of a facility (or system) and how the penetration of cables into a shielded enclosure should be handled. Some protection components, SPDs, were described along with the procedure of how they should be combined to achieve the best mitigation. In Paper VIII the response of the PoE protection was investigated when subjected to electrically fast transients (tens of nanosecond rise-times). It was seen that, on the whole, the protection ability of the SPDs was as stated (that is against lightning type pulses, LEMP), but it was also seen that large amounts of the voltage coupled to the conductors ("phases") of the PoE not being used for injection.

In Paper I, it was, explained that a previously reported limitation of ZnO varistors when subjected to UWB transients was a result of the parasitic effects of the packaging. The leads of the varistor create, due to the high frequency content of the signal, a very high impedance path. This impedance decreases the voltage that the ZnO element is subjected to, and to such a degree that the non-linear phenomena does not occur. Thus, the varistor response becomes that of a capacitor and therefore the packaging and installation of the SPDs becomes very critical for protection against UWB signals.

5 Susceptibility

In Chapter 5 we will discuss the susceptibility of a device or system when subjected to different disturbances. We will also see that the EMC requirement set forth may sometimes not be enough for IEMI, or even followed.

5.1 Issues regarding susceptibility of devices

According to [14] electromagnetic susceptibility is defined as[8]:

> "inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance".

Numerous scientific works have been published in journal papers and in conference proceedings dealing with the susceptibility and response of systems when subjected to adverse electromagnetic environments. It is a subject that researchers from many different areas are contributing to. Unfortunately, it is very difficult to make statements about the response and susceptibility of individual pieces of equipment. However, tests performed on different types or generations of components have reveled that, perhaps not unexpectedly, smaller and more complex components are generally more easily destroyed (see fig. 43). However, remember that for some components and systems, the opposite is true (see Chapter 1) due to shielding as a consequence of emissions limits.

Component	Threshold destruction energy
UHF diodes	0.1 - 1 µJ
CMOS IC	1 - 10 µJ
Low power transistors	1 - 100 µJ
Switching diodes	10 - 100 µJ
Relays	1 - 100 mJ
Carbon resistors (0.25W)	10 mJ

Figure 43. Shown are approximate ranges for threshold destruction energies for different technologies, when the components are subjected to pulses of duration less than or equal to 1 µs (data adopted from [32]).

[8] See paper VI for an alternative definition of susceptibility.

5.1.1 Norms used for testing

When a system, or individual component, is subjected to a disturbance there are several phenomena and effects that can take place and cause interference or damage. Some of them are:

1. The amplitude of the transient can directly be sufficient to cause an electric breakdown.
2. The energy in the pulse can directly be sufficient to cause permanent damage.
3. If heat (energy) is not dissipated sufficiently fast from the victim between transients or during the duration of the disturbance, this will build up until the system (component) is damaged.
4. Similarly, charge can also be accumulated and built up.

Therefore, a vital matter is the norm considered when testing (e.g., amplitude versus time integral of the amplitude), as these different norms provoke different responses from the system. Table 6 below (adopted from [6]) gives some important norms and the situations for which they may be applied

Table 6. *Different stress norm factors can be used to explain different failure conditions [6].*

Norm	Description
1. Time domain peak; $\sup \lvert x(t) \rvert, \ \forall\ 0 < t < \infty$	For resistive load termination ($V \propto I$), dielectric breakdown and arc-over effects
2. Total signal energy; $\int_0^\infty \lvert x(t) \rvert^2 \, dt$	For resistive load termination ($V \propto I$), heating effects (burnouts)
3. Peak signal power; $\sup \lvert x(t) \rvert^2, \ \forall\ 0 < t < \infty$	For resistive load termination ($V \propto I$), secondary thermal breakdown
4. Peak time rate of change; $\sup \lvert \frac{d}{dt} x(t) \rvert, \ \forall\ 0 < t < \infty$	For inductive load termination ($V \propto j\omega \cdot I$), dielectric breakdown and arc-over effects
5. Peak time integral of pulse; $\sup \int_0^t x(t)dt, \ \forall\ 0 < t < \infty$	For capacitive load termination ($V \propto \frac{I}{j\omega}$); dielectric breakdown and arc-over effects

Also, for susceptibility tests it is important to have a common scale to compare interference effects from other data sets. The different upset events that can be seen for electronic equipment and systems can be classified according

to a five level scale (Level 0 is often used for devices not tested) (adapted from [33]).

Level 1 – No observed effect
Level 2 – Interference while radiated
Level 3 – Strong interference / crash, self-recovery.
Level 4 – Loss of function / crash, operator-intervention
Level 5 – Physical damage, repair or replace.

5.1.2 Narrowband versus wideband disturbances

Let us assume that a system is only vulnerable in its in-band spectrum (operational frequencies) and a few out-of-band frequencies[9] (see fig. 44). Generally speaking, a narrow band source is more destructive than a wide band source since, approximately, all energy is delivered in a single frequency band. However, this is assuming that the operational frequencies or resonance frequencies are matched to the source. The power is then very efficiently coupled into the system and the response is very significant. Thus, the source has to be tuned to the system and the attacker has to have knowledge of the system[10]. If this is not so, it could be easier, from a source design perspective, to interfere with a system using a wideband source. The vulnerable frequencies are most likely covered by the wideband waveform (see fig. 44). Thus, there is no need to tune the source frequency to match the system resonances or operational band(s). However, the power delivered to individual frequencies is small; thus, the field strengths needed to cause upsets are approximately equal to the narrowband cases (or slightly more, compare fig. 53 and 54).

In the situation in fig. 44 the first narrowband source (NB_1) is radiating in the operational band of the system (in-band interference), which is difficult to protect against (see Chapter 6). The second narrowband source (NB_2) is radiating in the same frequency band as one of the system resonances, however, it doesn't radiate in the frequency band of the most vulnerable frequency. The ultra wideband source (UWB) covers a portion of the operational frequency band of the system, as well as both resonances, even though the power delivered in these individual bands are relatively small.

[9] However, in a real system, apertures and complex interior makes the system vulnerable in more frequency bands, as resonances are numerous, but also due to the possibility of breakdown inside they system (due to high field strengths) and heating effects in material (due to the high energy in pulses with high energy).
[10] Unfortunately, for most civilian systems, the operational frequencies (in-band spectrum) is open literature and well-known.

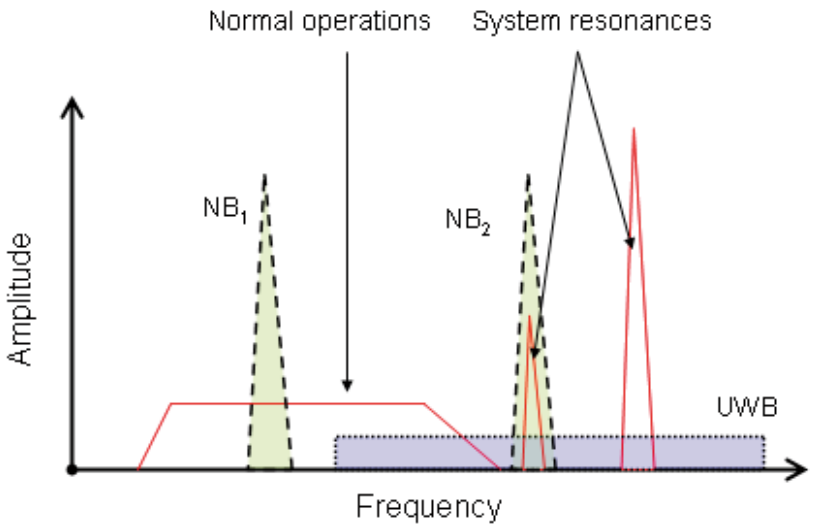

Figure 44. Narrowband versus wideband disturbances in relation to the frequency response of a system.

For a given piece of equipment or system and for sources of electromagnetic disturbances, it is much more likely that equipment is subjected to the weaker forms of upset events than permanent damage (see fig. 45).

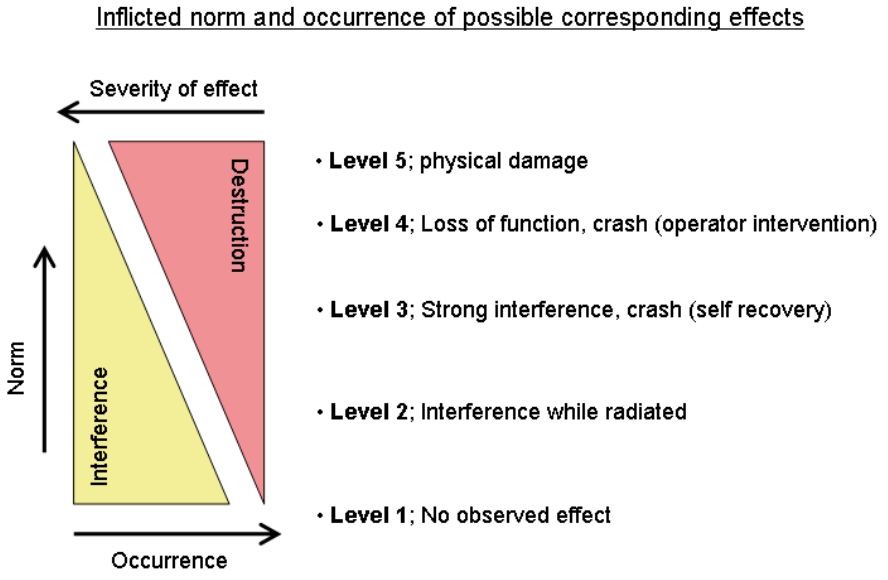

Figure 45. For any given system, and most disturbance sources, it is more likely to see weaker upset events than, e.g., permanent damage.

5.2 Wunsch-Bell

PC systems are today among the most tested complex systems as they often control and monitor a large extent of the civilian infrastructure. It is good to remember when doing susceptibility tests on systems with PC processors that PC systems of more modern design are often less vulnerable [34] (in relative terms) to disturbances than older computers (even though this is not an absolute truth). The explanation given is; the newer models work at a higher clock frequency and have a higher emission of electromagnetic fields. Due to this they are forced to have better EMC shielding so the emissions do not disturb nearby system. This helps to protect against both internal and external fields. However, as was stated previously, without this mitigation, as a consequence of the EMC demands, smaller and more delicate devices have a lower breakdown threshold, than more sturdy devices. These two factors compete with each other.

The “cells” of all PC systems are semiconductor devices. Thermal breakdown of semiconductor devices can be described by the *Wunsch-Bell curve* [35] (see fig. 46 below). It describes three different regions for the relationship between the, to a semiconductor device, maximum applicable power versus the pulse length. The three regions are:

1. Adiabatic, where the pulse length is much short than the time to diffuse the heat (which is dependant on component size) and the threshold energy to cause permanent damage is constant (independent of pulse length).
2. Intermediate region.
3. Steady state region, where the pulse length is equal to or longer than the time needed to diffuse heat (approximately above 1 μs) and the power needed to cause permanent damage is constant (independent of pulse length).

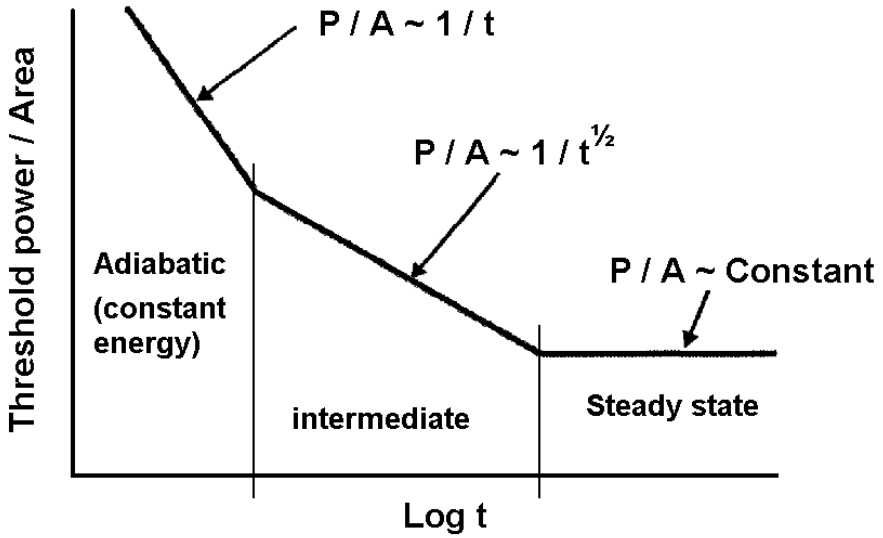

Figure 46. The adiabatic, intermediate and steady state region of the Wunsch-Bell curve.

As discussed above, if the pulse width of the transient is short, heat deposited in the material can still be a problem. The reason is that less energy is needed to destroy the component for a short transient compared to the case when the transient has longer time duration[11] (which is supported, even for UWB transients, in [36]). Also, if the pulse repetitive frequency is high, and the relaxation time between transient is too short to allow heat to dissipate from the material, energy can be built up until the component is destroyed (compare with fig. 49 for charge accumulation).

5.3 Latch-up

Another important phenomenon manifesting itself in semiconductor devices is *Latch-up* in CMOS structures. It arises due to parasitic NPN and PNP bipolar transistor between the VDD and VSS (power supply and ground) on a CMOS IC which forms a thyristor structure (see fig. 47). Normally the withstand voltage of the thyristor structure is higher than the power supply voltage but if the PNPN structure is triggered by, e.g., an external surge to the input or output terminals, the thyristor alters from a high to a low imped-

[11] This can be understood by investigating the Wunsch-Bell curve and noting that only the time scale (x-axis) is in log scale, the power (y-axis) is not, thus the energy ($E = P*\tau$) for each point will increase significantly with longer pulse durations and becomes almost constant for shorter time durations.

ance state. As a consequence the power supply keeps feeding current to the ground until the power supply voltage falls below the turn on voltage of the thyristor or the device burns out (see fig. 48).

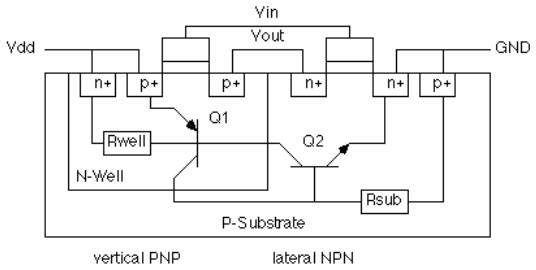

Figure 47. Parasitic thyristor structure in the CMOS device (adopted from [37]).

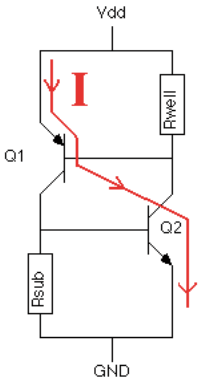

Figure 48. Low impedance path forms between the power supply and ground (adopted from [37])

The transformation of the thyristor to its low impedance state involves charge transfer inside the CMOS structure which will not further be discussed here, however, it is good to know that the critical charge needed to invoke a latch-up is constant and proportional to the amplitude of the trigger pulse and is inversely proportional to the trigger pulse width [38]. That is, as the pulses get longer, the trigger pulse amplitude needed to induce latch-up decreases. Thus, the risk of experiencing a latch-up is higher if the CMOS device is subjected to a lightning electromagnetic pulse than if subjected to pulses with shorter time duration (higher frequency content, e.g., an UWB pulse). Also, if the trigger pulse amplitude is below the critical value but the repetition rate of the trigger pulse is higher than the time it takes the charge to dissipate from the material, a cumulutative effect takes place and after N number of pulses the critical charge amount is reached and latch-up still occurs [38] (see fig. 49).

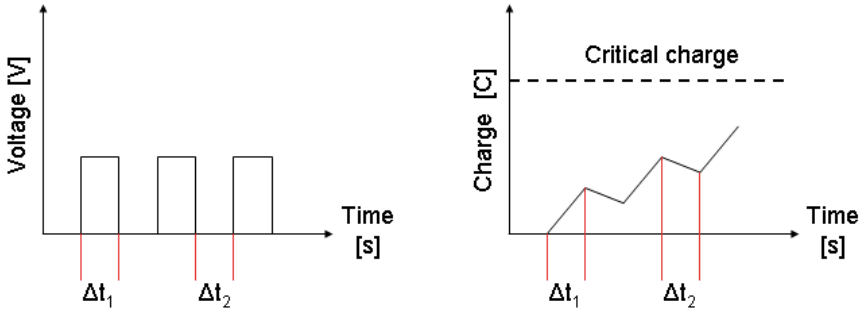

Figure 49. Charge accumulation due to a repetitive pulse where the pulse repetitive frequency is sufficient to increase the charge as the relaxation time is too long as to let charges dissipate between pulses.

5.4 Comment on Paper V "Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation" and Paper VII "Susceptibility of GPS Receivers and Wireless Cameras to a Single Radiated UWB Pulse"

5.4.1 Handheld GPS receivers (Paper V and VII)

As mentioned earlier the systems that control and monitor the sensitive components of civilian infrastructure are changing and are applying more and more sensitive electronics. One such system is the Swedish railway system described in Paper IV. As described in Paper V (and Paper VII) handheld GPS receivers and wireless cameras were tested both against different HPM waveforms and a UWB transient (produced by the RADAN 303B source [26]) to investigate the susceptibility of equipment that will gain more use and trust in coming years. GPS receivers are today, for the majority, used by taxis, for naval navigation, military personal (the use of commercial products may however be limited), in cellular phones and more. It is very probable that in the future the use of GPS receivers will increase further. Other COTS equipment gaining an increase in use is wireless cameras, as they are a low cost approach to monitor an area without the risk of immediate detection. It was found that such sensitive equipment can easily be disturbed by HPEM to an extent that operator intervention was required.

The GPS receivers tested were all CE marked which means they should therefore comply with the existing EMC regulation that is associated with them (see fig. 51). However when comparing the results from the tests with

narrowband disturbances it was seen that the GPS receivers could be disturbed (Level 2) out-of-band by fields several order of magnitude lower than the EMC demands, that they should abide by. In-band, a continues wave (CW) disturbance (several tens of seconds) could affect one of the GPS receivers with electric fields as low as 2 mV/m. Under pulsed conditions (duration of 0.1 μs and PRF of 1 kHz), these threshold levels were more in order of the EMC requirements (see fig. 52).

Figure 50. The three types of handheld receivers tested (from left to right; C, B, A).

Tests were carried out to investigate the threshold for Level 4 and 5 upset events caused by both narrowband and UWB disturbances. It was found that (see fig. 53 and 54), approximately, a few kV/m and tens of kV/m was required, respectively (for both environments). When testing for permanent damage the assumption of out-of-band front-door coupled power was supported, as it appears that it was the communications handling unit that was destroyed and nothing else (loss of satellite connection alone).

Immunity levels - enclosure port			
Frequency	80 - 1000 MHz	1.4 - 2.0 GHz	2.0 - 2.7 GHz
E - field	3 V/m	3 V/m	1 V/m

Figure 51. The EMC constraints according to [39].

	Level 2 threshold field [V/m]					
	GPS model					
	A		**B**		**C**	
Freq.	**Pulsed**	**CW**	**Pulsed**	**CW**	**Pulsed**	**CW**
1.0 GHz	—	0.2	—	0.1	—	1
1.25 GHz	—	0.3	*30*	0.1	—	1
1.575 GHz	*3*	0.02	*1*	0.002	*10*	0.1
1.75 GHz	*9*	0.02	*8*	0.1	*30*	1
2.0 GHz	—	0.1	—	0.1	*10*	1

Figure 52. Threshold levels for the electric field for inducing a Level 2 upset event in the GPS from a narrowband source. Compare with fig. 51.

3 GHz, 1 µs, PRF = 1 KHz			
	GPS model		
	A	B	C
Level 4	4 kV/m	1 kV/m	2 kV/m
Level 5	40 kV/m	30 kV/m	40 kV/m

Figure 53. Threshold levels for the electric field for inducing Level 4 and 5 upset events in the GPS from a HPM source.

Level 4 [kV/m] UWB pulse			
	GPS model		
Orientation	A	B	C
1	2	2	10
2	8	8	20
3	1	2	9

Figure 54. Threshold levels for the electric field for inducing a Level 4 upset event in the GPS from a UWB source. Three different orientations of the GPS receivers were tested.

It was concluded that for handheld GPS receivers:

1. The GPS receivers can be disturbed by CW fields many times lower than the levels stipulated in the EMC regulations.
2. The susceptibility level is dependent on the brand and some variations are observed.
3. The susceptibility of the GPS is highly dependent on the physical orientation of the device with respect to the incoming pulse, thus the polarization of the disturbance compared to the GPS receiver.
4. COTS GPS receivers are easily disturbed but more resilient to permanent damage.

5.4.2 Wireless cameras (Paper VII)

A suggested prevention method for IEMI is the use of small cameras that can monitor an area to add to the security. For this wireless cameras may be good, however they themselves are vulnerable to electromagnetic radiation.

Figure 55. The two types of wireless cameras tested (from left to right; D, A).

The wireless cameras tested, subjected to a single UWB transient from the RADAN 303B source [26], were both powered by batteries and these were included in the test to simulate an accurate representation of the device in a civilian installation. A difference in the response due to the length and position of the battery cable was seen for one of the cameras, however in many realistic situations a longer power cable, than used here, is present, which will couple and transmit more of the impingent field to the cameras. Only one orientation of the wireless cameras was tested.

Table 7. *The range of the electric field needed for inducing a Level 4 upset event*

	Electric field levels [kV/m]
A	2.8 --> 3.9
D	12 --> 20

As can be seen from table 7 the peak electric field values necessary for causing a Level 4 upset differs much for the two types of cameras. Also, the wireless cameras could not be permanently damaged by the UWB source at our disposal (which confirms the statement that UWB sources are more likely to cause an upset than permanent damage, as the power is spread across a wide spectrum).

5.4.3 Discussion

The varying susceptibility test results, both for the narrowband and UWB tests, described here, supports the idea of different mechanisms giving rise to different upset events. Permanent damage is likely to occur due to the sheer amplitude (or energy) of the fields being delivered to the target creating, e.g., a breakdown somewhere within the system. This would explain the decent conformity between the threshold levels for permanent damage seen both for HPM and UWB tests (tens of kV/m) for the GPS receivers. A “softer” interference, such as Level 2, is more likely due to noise or bit errors being created in the circuitry. Thus, more errors are likely created for longer durations

of the disturbance, such as with CW. Note that the very low levels need to disturb the GPS receivers, are in part due to the very low power used to communicate with the satellites (-135 dBm at ground level).

Also, note that if using the upset threshold levels for out-of-band CW disturbances obtained here (from fig. 52, $E \approx 0.1$ V/m) and using (assuming far-field conditions) $E = \sqrt{(30PG)}/R$ [12], where P, G and R are the transmitted power, transmitter antenna gain and distance, respectively, a weak isotropic CW source ($G = 1$ and $P \approx 1$ kW) could disturb the GPS receivers from a distance in the order of km's. Note that, since the source is isotropic, this is a radius, within, which the GPS receivers are disturbed.

5.5 Summary

In Chapter 5, it was seen that newer technology has lower upset threshold levels than older. However, newer system may themselves be less vulnerable to disturbances. Different physical phenomena, that can create upset events, were also discussed. The threshold levels for different upset events of some COTS equipment when subjected to different disturbances were investigated and compared to EMC requirements. It was seen that the CE mark is no guaranty for having electromagnetic compatibility. The tested devices could all be disturbed or destroyed by available sources.

6 System assessment

In Chapter 6 we will discuss how to make use of our knowledge obtained so far. Using data on sources, coupling paths, mitigation measures at system ports (and/or attenuation due to shielding) and susceptibility (threshold values) we can make an estimate of the system performance for a particular disturbance.

6.1 Introduction

Similar to the identification of distinctive shapes and colors on puzzle pieces, we now have some knowledge of the individual processes that are involved in an IEMI attack scenario. Using this information we can finish the puzzle and make a statement of what may happen in a certain scenario. However, in an actual system, every single variable can not be accounted for, still, we can, at the very least, make some approximations on realistic boundaries for the best- and worst-case scenarios. This may not sound as much but knowing the, e.g., electric field levels for best- and worst case scenarios allows system designers to take appropriate mitigation measures within the operation requirements, as well as economical budget, of the system. Therefore, an over- or under-protected system might be avoided.

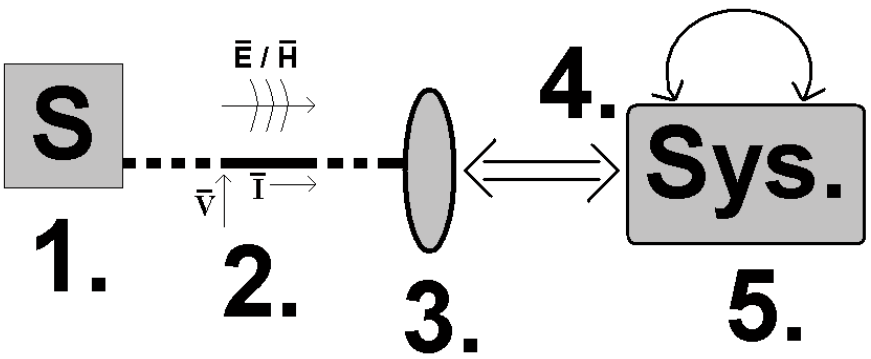

Figure 56. The decomposition of an EMC problem into source (1), coupling path to system (2), system exterior (3), coupling into system interior (4) and response of the system or component of interest (5).

Going back to fig. 3 (also shown here as fig. 56) we already have identified the components that contribute to a general EMC problem and, as was stated, the same division can be used for an IEMI scenario. However, the previous argument made regarding the possible collapse of the EM-topology due to the human intent behind an IEMI attack must be taken into account when doing this assessment. For instance, it has to be considered whether the zone boundaries can, or will, be circumvented (e.g., outer shield penetrated) or if the coupling path regarded is the worst-case scenario (e.g., front-door coupling through power sockets).

6.2 Simple example of assessment

A reflector antenna with a 1 m radius is fed by a pulsed source (see fig. 57) giving a peak power of P_t available to the antenna to radiate (ignoring the internal heat losses due to the internal impedance of the generator[12]) and an excitation frequency of 1 GHz produces a pulse with 100 ns duration. A dipole antenna of 15 cm (half wavelength) is in the boresight of the source and illuminated from a distance of R_0 m. What is the approximate power received at the receiving dipole antenna? The approximate physical area (A) of the reflector antenna is 3.14 m^2, the aperture efficiency, η, which can be defined as the quota of the maximum effective area (for the excitation wavelength) and physical area is set to 0.5. This is usually a good estimate of the nominal value for parabolic reflectors [6]. The directivity of the antenna is given as (not yet including any mismatch terms):

$$D_t = \frac{4\pi}{\lambda^2}\eta \cdot A. \qquad (6.1)$$

[12] The maximum power delivered from the source to the antenna occurs when so called "conjugate matching" is achieved (see e.g. [40]), and then half of the power is given to be radiated by the antenna, the rest unavoidably lost as heat in the internal impedance of the generator.

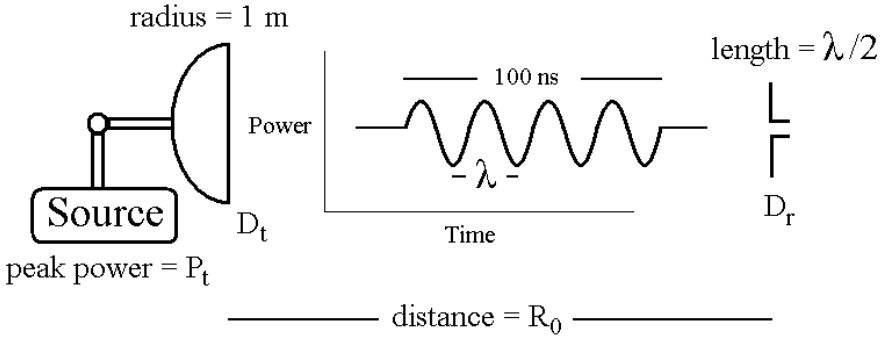

Figure 57. A parabolic antenna with narrowband HPEM (HPM) source is illuminating a dipole antenna.

The maximum directivity of the half wavelength dipole antenna (D_r) is 1.643 [40] and the maximum power received is given by the *Friis Transmission Equation* [40]:

$$\begin{cases} P_r = P_t\left(\dfrac{\lambda}{4\pi R_0}\right)^2 D_t D_r e \\ e = \left|\overline{\rho}_r \bullet \overline{\rho}_t\right|^2 \left(1-\left|\Gamma_t\right|^2\right)\left(1-\left|\Gamma_r\right|^2\right)\varepsilon_{cd,t}\varepsilon_{cd,r} X \end{cases} \tag{6.2}$$

where:

- $|\boldsymbol{\rho}_r \bullet \boldsymbol{\rho}_t|^2$ is the polarization mismatch loss factor between the antennas ($\boldsymbol{\rho}_i$ are the polarization vectors for the antennas)
- $(1-|\Gamma_t|^2)$ and $(1-|\Gamma_r|^2)$ are the impedance mismatch losses for the respective antennas[13]
- $e_{cd,t}{\cdot}e_{cd,r}$ are the antennas efficiencies relating to losses due to dielectric and conductive losses in the antennas

Observe that here X represents various other losses due to, e.g., fringing of the fields around the antenna edges, due to atmospheric attenuation, due to ground reflection, etc. The energy delivered in one burst with 100 ns (τ) duration is approximately:

$$E_r = P_r \cdot \tau\,. \tag{6.3}$$

[13] Depending on the resolution of the measurements and setup, the reflection coefficient can include additional things. Most times, the reflection coefficient includes all reflections that arise from the reflection between free-space and antenna, antenna and connecting cable and cable and source (networks analyzer), respectively. That is, reflection coefficient measured with a network analyzer is built up of these three (or more) terms. However, theoretically all these contributing impedance mismatches could be resolved.

Using eq. (6.1) - (6.2), and setting the loss term $e = 1$, and using a peak power (radiated by the antenna) of {100 kW, 10 MW, 1 GW} at a distance of {10 m, 100 m, 10 km} and a frequency of 1 GHz, we get the following values for received maximum energy in the dipole:

$$E_r = \begin{bmatrix} 21\mu J & 0.21\mu J & 21pJ \\ 2.1mJ & 21\mu J & 2.1nJ \\ 0.21J & 2.1mJ & 0.21\mu J \end{bmatrix},$$

where the terms along one row are increasing distance and down one column are increasing radiated peak power (starting with 100 kW and 10 m at position (1, 1) and ending at 1 GW at 10 km at position (3,3)). To give an example, a moderate source of 10 MW peak power, equipped with a reflector antenna of 1 m radius may couple 21 μJ of energy at a distance of 100 m, destroying many low power electrical components (see fig. 43). The received energy values above can be compared to the values given in fig. 43. These show the threshold destruction energy levels for some common COTS components when subjected to pulses of duration of 1 μs or less. For example, a CMOS IC is permanently damaged if a pulse with energy in the range of 1 – 10 μJ is injected into it. The distances needed to disturb a device, or system, is approximately 20 – 30 dB larger [21]. However, observe that this is a general trend seen and not an absolute rule. It is clear that a HPEM source can, at a large distance, with a relatively small reflector antenna destroy or disturb sensitive electronics.

6.3 Comment to Paper IV "Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI"

6.3.1 Background

During the first decades of this century the railways in Europe will implement the European Rail Traffic Management System (ERTMS) which consists of the ETCS (European Train Control System) and the GSM-R (GSM communications standard for railway usage) [41]. ERTMS (see fig. 58) will be implemented on most high speed railway lines in Europe. This system, will greatly increase the capacity and safety of the European railways, but will rely heavily on wireless communication for train communication and control.

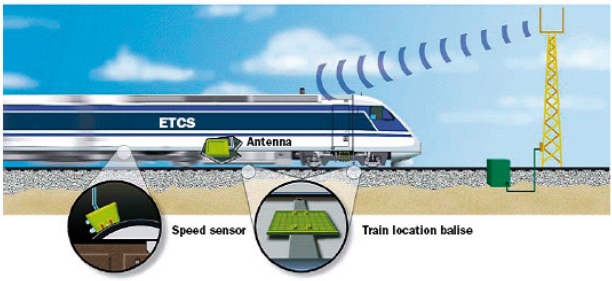

Figure 58. ERTMS relies on GSM-R communication protocol and the Euro balise system to handle control and communicate with the trains (adopted from [42]).

Due to the utilization of antennas that are distributed along the tracks and on the trains, assessment of susceptibility from radiated HPEM sources is important. Trackside antennas are normally positioned on masts 30 to 40 m high and connected to a communication system (i.e., base station) at the bottom of the mast. A low noise amplifier (LNA) is normally positioned at the input port of the communication system and will be a critical component of the system. For the rolling stock, the antenna is normally positioned on the front of the engine and connected through a cable to a cab-radio, with a LNA at the input port.

6.3.2 Assessment

The situation assessed here (shown in fig. 59) is the threat to an ERTMS system that is illuminated by an HPEM source. The communication antenna is either positioned on the engine of the train or at the trackside mast. The HPEM source is hidden in a van (dielectric walls) positioned at some distance from the tracks or mast. The sub-systems that are involved in the assessment ranges from the HPEM source to the connected communication system with a LNA as a critical component. Observe that only permanent damage to the system is considered, the distances for interference are as said above much larger than the distances for inducing permanent damage to a system, which is, the distances that are later presented in fig. 60.

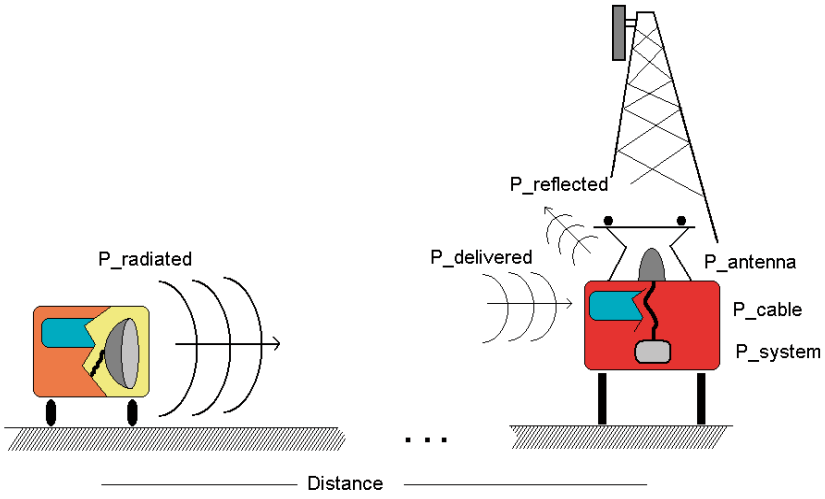

Figure 59. The situation under interest, a HPEM source hidden in a van with dielectric walls, radiating a train or communications mats.

An in-band front-door attack on the GSM-R antennas at trackside or on the engine of the train is considered more likely to cause interference and permanent damage than illumination of the communication system itself inside the building or engine (back-door). With in-band front-door disturbance the specified gain of the targeted antenna will, besides the intended signals, increase the power of any disturbance (in the specified band). Thus, even weak sources can be a problem. Observe that we here assume that the threat from back-door coupling, including any eventual resonance in the e.g. body of the train engine or housing of the bas-station, will not be as severe as the front-door coupling. This is argued on the basis that:

- These back-door resonances, through e.g. apertures, are rather narrow in the frequency domain. Therefore it requires a fine tuned narrowband source to excite it (an UWB source can be used, but the power this delivers is spread over a large frequency band and thus the power at each frequency is very low).
- If the attacker doesn't have a very high insight to the system, these resonances are virtually unknown, due to the complexity of the systems.
- In order to increase the probability of causing a failure both the polarization and angle of incidence should be optimized. However, this requires a very profound knowledge of the system

On the other hand the front-door in-band frequencies are easily known for almost any communication antenna. Also, often the characteristics of civilian antennas are open literature. Therefore an attacker is more likely to tune the

HPEM source to these known frequencies of operations of the system of interest and, thus, this will be the worst-case scenario.

It should be mentioned that a similar assessment approach can also be used for a back-door coupled disturbance or a transient directly injected into a conductor system. The actual variables and characteristics of the sub-system involved would have to be changed accordingly.

The front-door system assessment is divided into:

1. Likely sources used by attacker [1) in fig. 3]).
2. Coupling to system; characteristics and behavior of the antennas [2) and 3) in fig. 3]
3. Propagation; the attenuation in system internal cables [4) in fig. 3] connecting the antennas to communication systems.
4. System response; susceptibility threshold levels of the LNA [5) in fig. 3]

6.3.2.1 Source

A HPEM source [1) of fig. 3] can be categorized according to many characteristics. However the main division is between narrowband (HPM) and wideband (such as UWB or DS) sources. Additionally, other source characteristics such as antenna polarization, or, for conducted transients, mode of injection (DM or CM) must be considered. A correct assessment of the source is vital since the assumed source forms a base for much of the assessment. Referring to fig. 3, point 2) is here the free-space loss [due to the separation distance between the transmitter (attacker) and receiver (victim)].

6.3.2.2 Coupling to system – GSM-R antenna

Since front-door coupling is assumed [3) of fig.3 “system exterior”], the electromagnetic energy is considered to only use the ports intended for receiving and/or delivering electromagnetic energy in some form. This is, here, represented by the, unprotected (no internal protection in the form of, e.g., limiters) GSM-R antennas. Upon investigation of the antennas it became clear that the actual bands of use (frequency and lobe widths) were much wider than specified by the manufacturer. This is of course unfavorable from a susceptibility point-of-view since it opens up for a wider range of sources.

6.3.2.3 Propagation path – Cable

The attenuation in the cables connecting the antennas to the communication systems [4) of fig. 3 “internal coupling”] will decrease the stress on the critical component and thus act to reduce the vulnerability. Assuming that the cables are matched with the antennas (and communication system, thus, disregarding reflections at these points) the attenuation in the signal is due to the electrical properties of the cable. Adding a mismatch factor is not diffi-

cult. The power handling capability (as a function of, e.g., frequency) of the cables in question is also important for the assessment.

6.3.2.4 System response – Susceptibility of low noise amplifier

The LNA [5) of fig. 3 "system response"], which amplifies the weak communication signal captured by the antenna, is a critical component of the communication system. The susceptibility tests performed [43] should match the assumed source waveform [1) of fig. 3] otherwise additional physical processes may give rise to erroneous threshold values. As seen earlier (see Chapter 5), both the time duration and PRF of the disturbance will significantly influence the threshold values.

6.3.2.5 Thresholds for permanent damage to the communication system

Combining the knowledge on HPEM sources, antenna characteristics, cable attenuation and LNA susceptibility thresholds an overall assessment of the ERTMS from front-door interference can be made. A maximum separation distance to induce a permanent damage in the communication systems can be estimated (using the Friis transmission equation):

$$R = \frac{\lambda}{4\pi}\sqrt{\frac{P_{trans}\cdot G_{rec}\cdot G_{trans}\cdot e}{P_{\text{received LNA}}}} \tag{6.4}$$

where G_{rec} is the receiver antenna gain, G_{trans} and P_{tran}) are the assumed transmitter antenna gain and power, $P_{receivedLNA}$ is the susceptibility data from the LNA and e are various attenuation factors (including, e.g., polarization mismatches and cable attenuation). "R" is the approximate maximum distance for achieving different upset events to the communication system (fig. 60). If a wideband source is assumed some Fourier analyses are required.

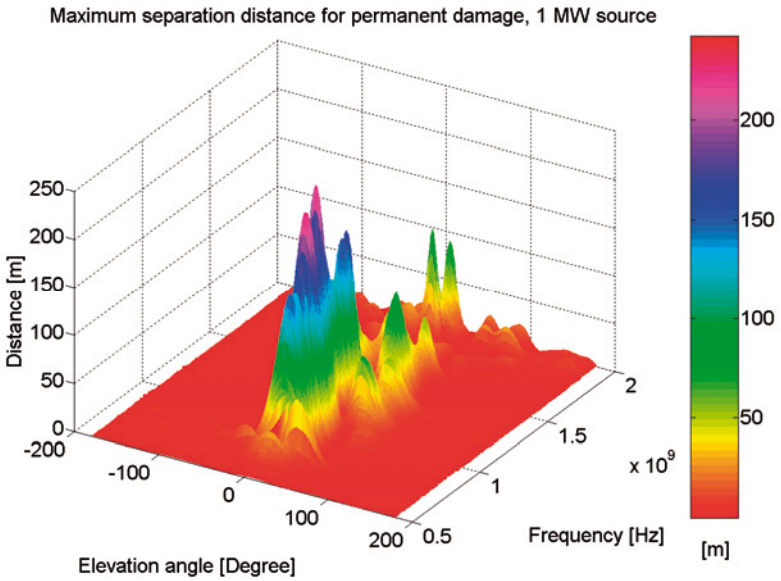

Figure 60. The maximum free-space separation distances between transmitting source and receiving trackside GSM-R antenna to permanently damage the LNA as a function of elevation angle and frequency. Source power is approximately 1 MW. The transmitter is placed aiming at the antenna.

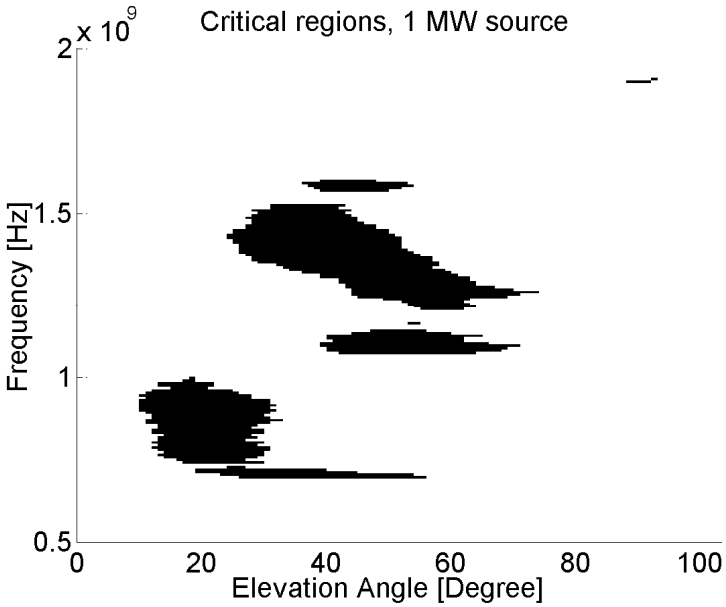

Figure 61. An example of critical regions for permanent damage to a trackside antenna when illuminated by a 1 MW source (see fig. 60). The transmitter is placed on the ground (height approximately 2 m) and the receiver is placed at the top of a tower (30 m). The transmitter is aiming at the GSM-R antenna.

However, not all angles of incidence and frequencies are, for a given situation, a threat. This is due to the fact that for low elevation angles the distance from the HPM generator placed on the ground to the GSM-R receiver grows very large. The critical regions, see fig. 61, are here defined as the regions where the maximum separation distances to induce permanent damage (from fig. 60) minus the physical distances from transmitter to the antenna (on the 30 m tower) are larger than zero ($R_{max\text{-}threshold} - R_{phys} > 0$). This is shown in fig. 61. Observe that the critical regions grow with increased transmitted power (since the maximum free-space separation distance grows).

6.3.3 Conclusions

Even in a worst case scenario, it is highly unlikely that the power radiated from a small HPM source (~ 1 kW) is sufficient to cause permanent damage to the LNA (thus the communication system), even if the pulse duration is in the order of μs. Assuming realistic parameters (e.g., of the HPM source, incident angle and distances, communication system, etc.) the approximate maximum separation distance to cause permanent damage to the LNA is:

- Small source (~ 1 kW) ≈ a few meters
- Medium source (~ 1 MW) ≈ a few hundred meters.
- Large source (~ 1 GW) ≈ several kilometers

However, remember that the distances for causing interference (e.g., a Level 2 upset) are 20 – 30 dB larger. For a UWB pulse it was seen that the maximum separation distance to cause permanent damage is several times smaller than for narrow in-band source and for a damped sinusoidal source it is seen that the maximum separation distance to cause permanent damage is, at best, the same as for narrow in-band source, but often shorter. In addition, it is seen that for a given situation, not all angles of incidences and frequencies are a threat.

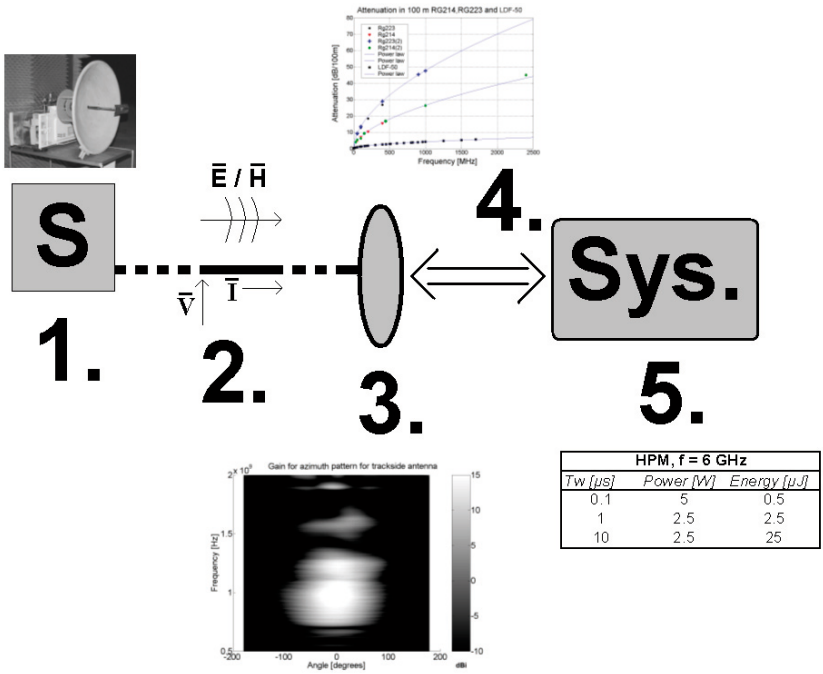

Figure 62. The steps taken in the system assessment; 1) source characterization, 2) coupling path to the system (here free-space propagation), 3) system exterior (here GSM-R antenna), 4) coupling to system interior (here cable properties), 5) system effect and response (here LNA threshold levels).

6.4 Summary

In Chapter 6 and Paper IV, the majority of the knowledge of a situation, from source characteristics to victim susceptibility, is combined in a method for performing a system level assessment. From this the threat level, from different sources, can be estimated (e.g., a lowest power level can be estimated). It was seen that not all situations are a threat, thus, we define the so called “critical regions” where the system is susceptible to permanent damage.

7 Measurement of conducted HPEM pulses

Measuring HPEM signals entails some difficulties, which will be discussed here in Chapter 7. Different means to measure conducted HPEM signals will be described.

7.1 Origin of the difficulties with measuring conducted HPEM signals

The difficulty with measuring conducted HPEM signals is that they contain both high amplitudes and fast time changes in the signal, thus, an extremely high time derivative (dV/dt or dI/dt). This means that the measuring system must be capable of handling very high voltage and/or current amplitudes, which calls for a bulky device that can withstand the amplitude. At the same time the device must be very sensitive and must have a fast response time to be able to measure the very fast changing time signals, and, thus, resolve the signal over a broad frequency range. Reduction of capacitances and inductances, which otherwise will distort the frequency characteristics of the transient is the most important challenge. In this chapter two methods of measuring conducted HPEM transients will be discussed. Measuring radiated HPEM fields are today easier as commercially available field probes, with sufficiently fast response times, exists.

One method of measuring conducted HPEM signals is the approach of measuring the electromagnetic fields associated with the conducted HPEM signal using an antenna inside a small TEM cell (see fig. 63) [44]. The TEM-cell has a coaxial structure which preserves the electromagnetic field structure, even for high frequency signals. It is then connected to the cable or conductor carrying the transient. A broadband electric or magnetic field probe is placed inside the TEM chamber (box) and the measured field is related to the voltage and current carried by the conductor. This so called "Pico-TEM" cell has a high cutoff frequency (approximate 6 GHz) but is limited by the voltage it can measure at lower frequencies due to the risk of breakdown between the inner and outer conductor of the TEM cell at higher voltages. Using a gas, other than normal air under atmospheric pressure, with higher breakdown strength (e.g., SF_6) the limitation set by the break-

down voltage decreases. Generally, for a given dielectric medium the break-down voltage increases with an increase in applied frequency (narrower pulse width).

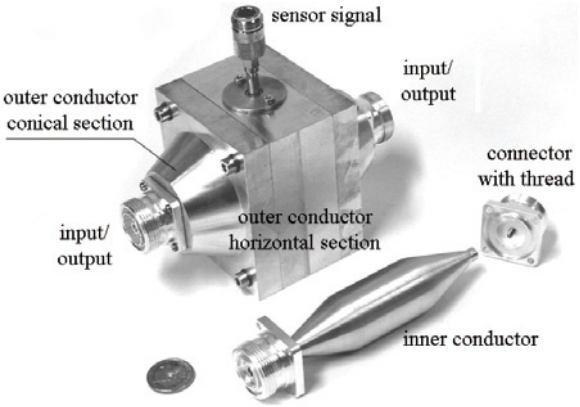

Figure 63. The Pico-TEM cell approach (adopted from [44])

7.2 Characteristics of $CuSO_4*5H_2O$ solution

The Pico-TEM described above is quite complicated, in that it requires some nontrivial calculations (or simulations) in the design phase to accommodate both the wanted frequency response and withstand voltage. Also, the manufacturing of the device is, due to the relatively small dimensions and accuracies needed, non-trivial. There are some alternative techniques, especially when high voltages are to be handled.

It has been reported that $CuSO_4*5H_2O$ (copper sulphate pentahydrate) solutions can handle both relatively high voltages (100s of kV) and fast transients (nanosecond rise-time) [45]-[47]. This means that the resistivity of these solutions themselves is stable under these conditions and, Thus, (approximately) independent of the applied field. The conductivity of a $CuSO_4*5H_2O$ solution as a function of the concentration of $CuSO_4$ in the distilled water (both from experiment performed by the author and from [48]) is given by fig. 64. As can be seen it is desirable to have a concentration above 10 Kg/m^3 (10 gram/liter) as the change in conductivity as a function of concentration is lower in this region. The resistivity of the salt-solutions (ρ) as a function of the concentration of salt (C) can be expressed by a power-law, that is of the shape $\rho=aC^b$. However, for salt concentrations of this order, the conductivity is much more dependant on the temperature of the solution (see fig. 65) than for a lower concentration, for which the solu-

tion is more comparable to pure water (in that the conductivity changes very little with temperature).

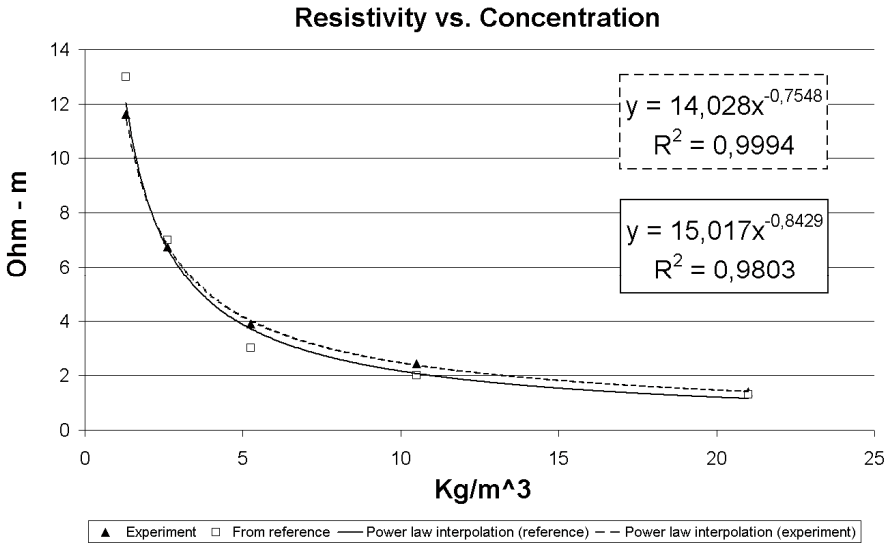

Figure 64. The resistivity of a CuSO4*5H2O solution as a function of concentration from experiments [49] performed as well as from reference [48].

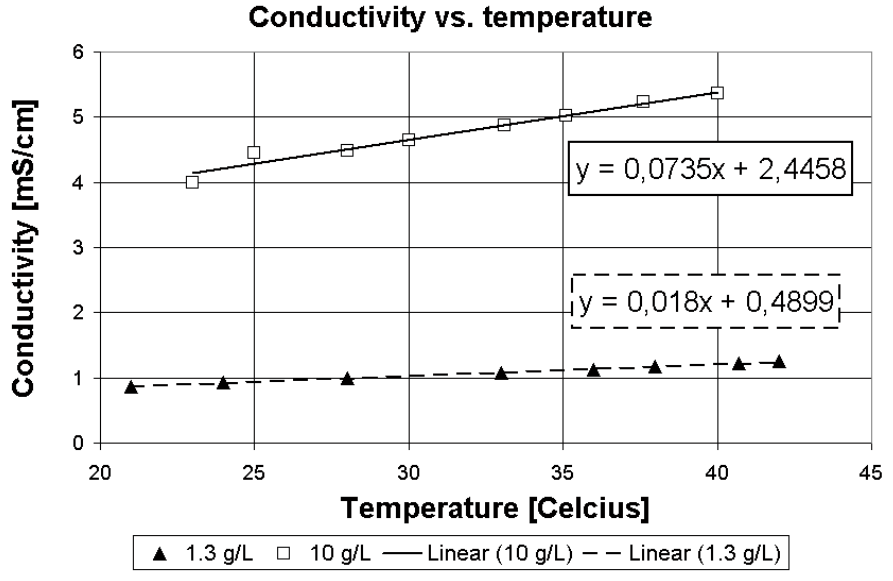

Figure 65. The conductivity of the $CuSO_4$*$5H_2O$ solution, as a function of the temperature, changes drastically with changing concentration. As can be seen here, a

lower concentration of the $CuSO_4$ salt behaves comparable to water (very little change in conductivity with temperature).

7.3 $CuSO_4$ resistive devices for measuring HPEM

To overcome the difficulties described earlier with measuring HPEM signals, a measuring system based on $CuSO_4*5H_2O$ solution in a current shunt configuration (see fig. 66) was built [49] A current probe with a fast response time and high bandwidth is used to measure the current through the shunt. The advantage of this method is that the high voltage is isolated from the sensitive measuring instrument (e.g., an oscilloscope). Thus, even though the setup is simple and robust, the configuration allows measurement of very high voltage or current derivatives. The drawback of the device is the sensitivity based on the conductivity. As seen from fig. 64 and fig. 65 the actual resistance value of the current shunt can differ greatly from specified value if the concentration of the $CuSO_4$ is different from the required, or if the temperature of the solution changes. Still, the simplicity of the device, along with reference measurements on the shunt impedance, makes it a good option.

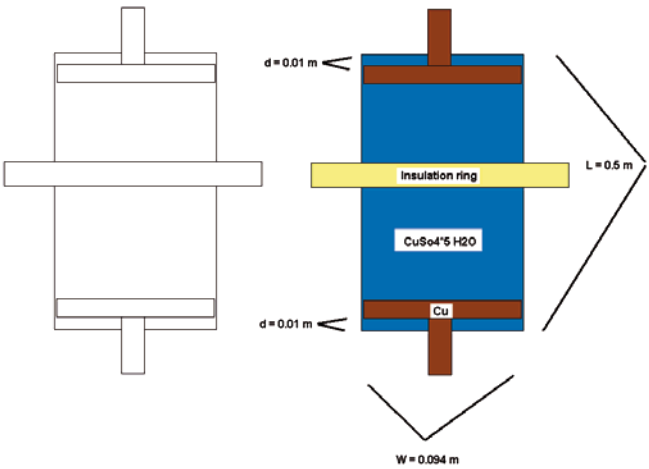

Figure 66. Schematic pictures of the CuSO4 current shunt.

An improvement to the shunt is a device in voltage divider configuration, which is insensitive to small variations of the temperature and salt concentration as both of the resistances formed in the divider are, approximately, af-

fected proportionally. Thus, it is the ratio, and frequency behavior, of the resistances formed that sets the performance of the divider.

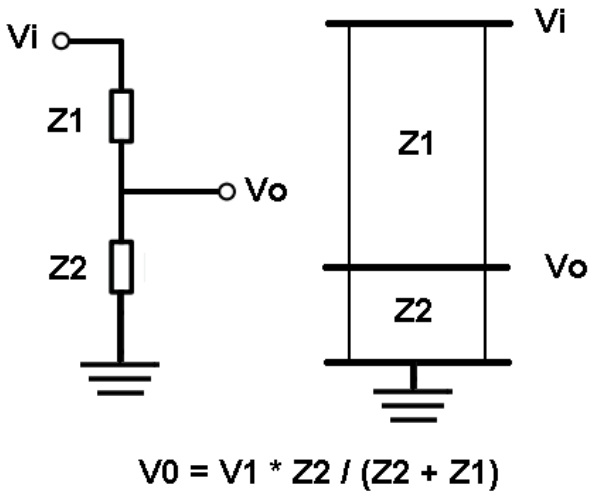

Figure 67. Schematic pictures of the CuSO4 voltage divider (lines do not represent actual conductors for output).

When designing the $CuSO_4$ devices the variables that must be considered, having the specified transients (both amplitude and frequency spectrum) in mind, are:

- Optimizing the concentration so that the rate of change of conductivity as a function of $CuSO_4$ concentration is minimized (practically > 10 Kg/m^3).
- Minimizing parasitic capacitances and inductances to get a good approximation of real resistive values (negligible effects from inductances and/or capacitances).
- Adjusting distances between electrodes to avoid breakdowns.
- Increase breakdown limits, e.g., with insulation rings.

If optimizing these variables it is possible to measure transients with several hundreds of kV amplitude and nanosecond rise-time corresponding to voltage rates of change (dV/dt) of approximately 10^{13} V/s. It is good to remember that the speed of a positive streamer (in air) is approximately 10^5 - 10^6 m/s at approximately 100 kV/m [50], and even less for streamer with negative polarity. It will, e.g., take a positive streamer, with a speed of 10^5 m/s, 5 µs to cross a gap of 0.5 m, and if the full-width-half-maximum time of the transient is much smaller then 5 µs there is little risk of breakdown. The technique and method of measuring conducted HPEM signals by using a $CuSO_4$ shunt has been tested with promising results [49]

7.4 Summary

In Chapter 7, we introduced the problem of measuring HPEM signals, the need for a both very sturdy and tolerant devices (to handle the large power involved), but at the same time very sensitive and fast to be able to correctly reproduce the very rapid signals. A solution to this problem is a probe based on a $CuSO_4$ salt solution that can be designed both in a shunt or divider configuration, respectively. The conductivity of the solution, as a function of both the temperature of the liquid and the concentration of the $CuSO_4$ salt, are easily obtained through experiment or in literature. These types of probes have a good frequency response and can also be designed to withstand high voltages.

8 IEMI classification of facilities

Finally, in Chapter 8 we will explore a possible method for classifying facilities and large distributed systems from IEMI. This will allow us to judge and compare already existing facilities or as a tool for improvement.

8.1 General classification of IEMI

The categorization of IEMI can be done along several diverse lines such as according to source, waveform, technology, coupling path and more. The situation has to be reviewed to determine which method is the most suitable. Strictly speaking IEMI is defined as any intentional electromagnetic interference. This fact leads to the conclusion that IEMI can be of an electromagnetic form; from DC to maximum available frequency (normally several tens of GHz), from few V/m to several 100's kV/m, from a very close range of a few meters to several kilometers distance, from a single narrowband frequency to a bandwidth of several GHz, from conducted to radiated. As long as interference or permanent loss of normal function is achieved intentionally through the use of a source of electromagnetic energy, it should be classified as IEMI.

8.1.1 Classification by transient characteristics

Classifying IEMI after impulse characteristics is the broadest approach and also the most forthcoming regarding analyzes of possible system responses (see Chapter 2 for further explanation of waveform characteristics). Some of the waveforms of interest are:

- A single or several, short transients with a very short rise time and short FWHM-time, i.e., UWB pulses.
- A single or several bursts of one continues frequency, giving rise to a very narrowband spectrum.
- Damped sinusoidal waveform

8.1.2 Classification by technology

The source (and its means to deliver a transient to a system) can be of a varying technological degree [14]:

- *Low technology*: a very simple arrangement which is easy to us, e.g., a rebuilt microwave oven with a horn or reflector antenna. It has been shown that a magnetron from a commercial kitchen microwave is sufficient to interfere, in some degree with the normal operation of some sensitive equipment [51] at a close range. Such a source can be inexpensive and easy to build and a suitcase version can be placed and/or hidden to continuously interfere with the operation of a system both through conducted and radiated power.
- *Medium level*: a source technological equivalent to commercially available radars is considered. Hidden in a van with dielectric walls and equipped with a horn or reflector antenna such a source could cause damage and sever interference and it is not very likely that a hidden mobile source would be quickly found.
- *High technology:* Requires specialized personal to operate and sophisticated equipment, for example, the "JOLT" system ([6] or [15]).

8.1.3 Classification by propagation path

As discussed earlier, two types of propagation paths for the electromagnetic energy are possible:

- Conducted
- Radiated

8.2 Traditional method for classification of systems and facilities

When classifying the electromagnetic compatibility of a system (from radiated disturbances), "shielding attenuation" or "shell protection" is often used. This is the attenuation (often in dB) of the electric and/or magnetic fields from some standardized source outside the exterior barrier of the system to some interior point, according to measuring praxis and standards. The same concept can be extended to conducted transients (attenuation of voltages and currents trough various interfaces (Point of Entries) of the system). Thus, these both describe the decrease in a determined quantity as it passes from the exterior to the interior of the system or facility. It is a measure dependent of polarization, frequency spectrum, etc., of the quality of the electromagnetic shield for a particular disturbance. Also, it should be remem-

bered that the results will be dependent on the position of the internal measuring probe within the facility or system (as a consequence of the variation of the field within this). It should be treated in a statistical sense similar to how results from a reverberation chamber are interpreted.

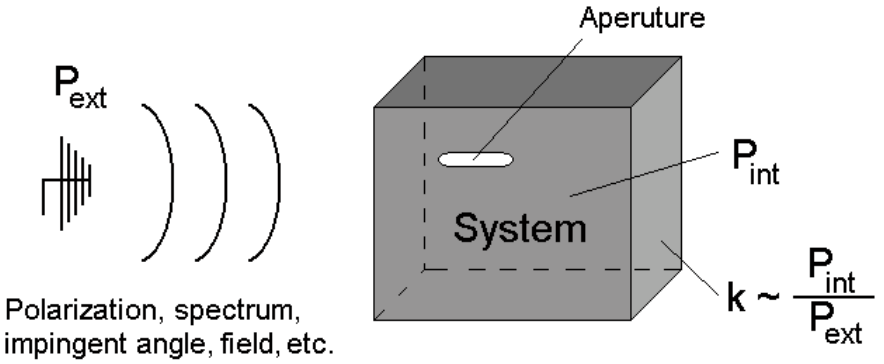

Figure 68. A ratio, between an external quantity (e.g., the electric field) and the same quantity inside a shielded system or facility, can be formed to judge the shielding ability and, thus, classify the system or facility from this. Here the electromagnetic energy couples into the shielded system via an aperture.

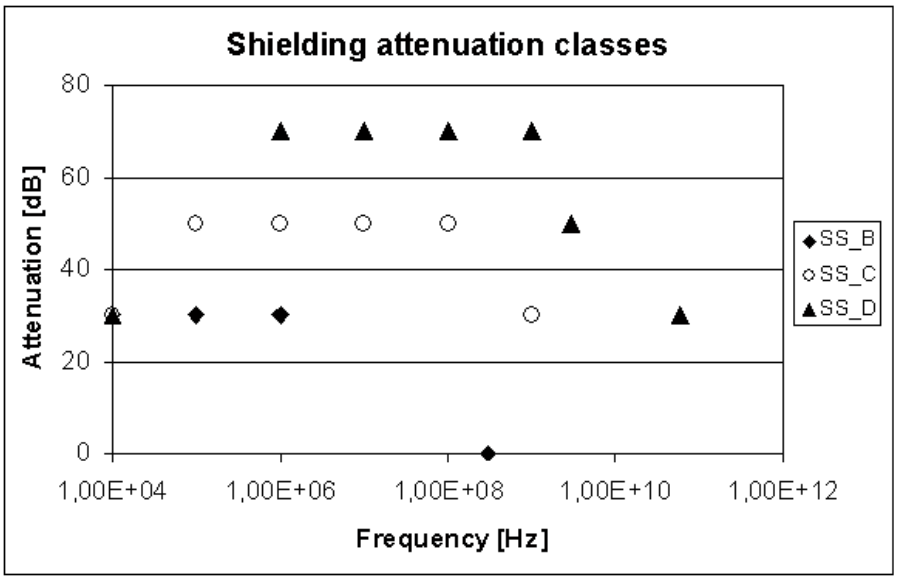

Figure 69. Shielding attenuation for different classes (data adopted from [12]).

Depending on the exterior electromagnetic environment that could be expected, in comparison with the demands placed on the operation of the system, the system under investigation can be placed in different classes. For

instance, for a system that is not very critical or susceptible to electromagnetic interference, a relatively low shielding attenuation factor can be accepted, whereas for a system that is very critical more rigorous demands on the shielding attenuation factor have to be made (see fig. 69). The actual quantification of this factors, thus the classification, is not trivial, as it dependence greatly on the manor of how the measuring procedure is performed Many scientific papers have been produced discussing this topic.

Classifications made according to the shielding attenuation factor is based on the idea that the source is outside the exterior of the system, giving, e.g., an attenuation of 70 dB for a 100 MHz disturbance for a SS_D class system (see fig. 69). However, in the event of an IEMI attack, the perpetrator may enter a facility undetected and locate an unexpected port for injecting electromagnetic energy (such as power- or lamp sockets) or radiate a disturbance in a zone deeper into the facility. In doing so, the first zone boundary and electromagnetic shield is bypassed. The physical boundaries and the zone boundaries need thus not coincide in a civilian facility. Even if a civilian facility was designed and fully built according to the zoning principle, the zoning principle could be violated by a human perpetrator and the disturbance source moved to a zone deeper inside the facility. Thus, much higher norms (e.g., electric fields) than expected may occur in zones containing equipment not designed to comply with these excessive levels. Also, for large distributed systems (e.g., railways or large civilian facilities) it can be difficult to maintain an unbroken physical or electromagnetic zone boundary.

Furthermore, many facilities and distributed systems (like, e.g., the power grid) have many interconnected sub-systems and also connections to other widespread systems. This creates interdependencies within and between systems, and the consequences of an IEMI attack increases due to these connections. There is a possibility that even a relatively weak disturbance creates interference in a sub-system that spreads within a system, causing upsets. This upset could, if the system is strongly connected to other systems continue to spread and affect other distributed systems. For example, hypothetically, a disturbance to a sub-system controlling the power network may cause a loss of electrical power. This will affect systems such as lighting, communications, ventilation, etc., which could cause other effects, such as inability to control, e.g., transportation traffic due to the lack of communication and control.

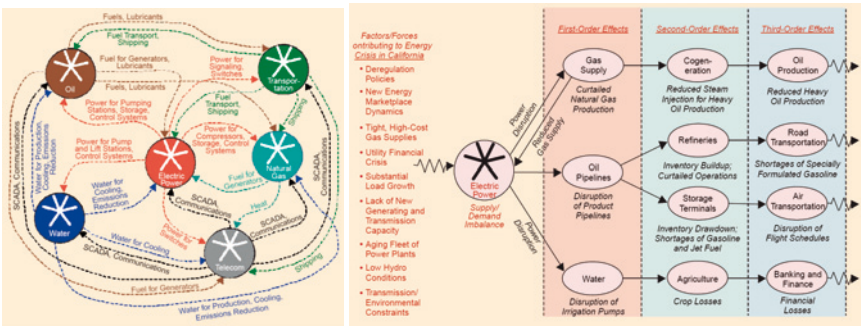

Figure 70. Interconnections and interdependencies between different critical infrastructure components [52] (© 2001 IEEE).

Therefore, a traditional classification using e.g. shielding attenuation factor will not be accurate in a situation as described above. As consequence of these issues raised above, an alternative approach is needed, where the classification of the system or facility is not based on a single number from measured experiments.

8.3 Comment on Paper VI "Methodology for Classifying Facilities with respect to Intentional EMI"

As the reasons given above creates problems for classifying facilities in an IEMI perspective (the perspective of creating electromagnetic compatibility between the facility and all the subsystems inside, and the source of the IEMI), three variables for creating a classification of a facility is defined:

- Accessibility
- Susceptibility
- Consequence

Combing these three variables, the so called ASC-, or IEMI cube (Paper VI), can be formed.

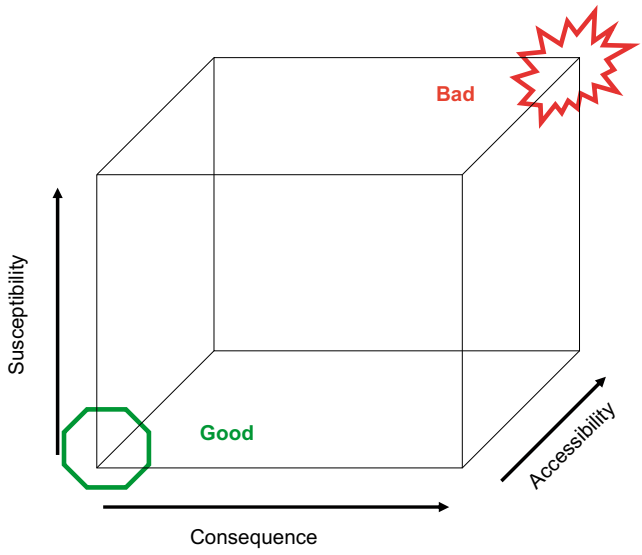

Figure 71. IEMI/ASC-cube with the extreme regions of special interest marked as ‘good’ and ‘bad’.

The quantified ASC is plotted on the axes of the cube, with the origin on the left, bottom, front corner. Systems near the origin have good hardness (less vulnerability) against IEMI and systems near the farthest corner to the origin have least hardness (highly vulnerability) against IEMI. Note that a system should be considered vulnerable even though the consequence of an attack is low but the accessibility and susceptibility factors are high. Therefore, the upper farthest right corner of the ASC-cube describes a system that is denoted critically vulnerable.

8.3.1 Accessibility and consequence

The accessibility of a system, where a low accessibility is desired, describes the ability of gaining access to the different parts of the facility or critical components belonging to it. It relates to the suitability and presence of points and ports that can be used for injection and/or radiating disturbances, but also the extent of the, e.g., surveillance systems, doors or fences, proximity to public roads, etc. An IEMI adapted EMC audit will make it possible to estimate the accessibility factor of a facility.

The consequence of an IEMI attack, where a low consequence is sought, is best determined by the system owner or operator and is, for an outside

engineer, hard to determine without intricate knowledge of the system or facility and its interconnection and interdependencies to other systems.

The scaling of accessibility (as well as “consequence” below) doesn’t necessarily have to be a numbered scale, but should rather follow a form similar to:

1. very limited
2. limited
3. severe
4. very severe
5. catastrophically,

which is the division recommended by the Swedish Emergency Management Agency (sv. Krisberedskapsmyndigheten, KBM) for assessing the consequences of “extra ordinary events” [53]. Of course, the actual meaning of, and differences between, the degrees have to be clarified (which is made in [53] for the consequences of extra ordinary events).

8.3.2 Susceptibility

The susceptibility is defined accordingly to [14] as:

> “inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance”,

and is perhaps the characteristic of a system that is the most often evaluated by an engineer. However, for a large, complex, and distributed system, such as a civilian facility, the meaning of the term susceptibility has to be reviewed. It would, however, be advantageous to keep the above definition, hence avoiding unnecessary confusion in the definition of terms. The susceptibility of a facility should still be based largely on the characteristics and susceptibility of its components (subsystems) in terms of the physical measurable parameters (e.g., fields, induced currents, etc.), but also on the tolerance of the facility against faults (redundancies through, e.g., backup systems) and on the ability to handle, or mitigate, disturbances (e.g., surge protection or shielding). Hence, the concept of susceptibility of a facility includes more than the susceptibility of the individual parts. It can, thus, not be expressed in absolute terms of physical parameters, e.g., V/m. It shall rather be expressed (as is also the case for accessibility and consequence above) in softer terms ranging from, e.g., "very limited" to "catastrophically".

Thus, due to these mentioned differences (between large distributed facilities and “normal” confined systems) the susceptibility term is subdivided into three separate contributing factors:

1. Receptivity, the ability of the facility to mitigate disturbances between and within zones (a description of transfer functions).
2. Sensitivity, the different upset threshold levels of the equipment and sub-systems inside the facility.
3. Redundancy, the availability of backup systems and the ability to "degrade gracefully".

By investigating these three factors and combining them and weighting them against each other, a susceptibility factor, as defined by the IEC above, can be deduced for the facility, in the same "softer" terms given for accessibility and consequence. The factors receptivity, sensitivity, and redundancy are explained further below.

8.3.2.1 Sensitivity

The sensitivity describes how easily the equipment inside the facility can be disturbed for various disturbances, and can be extracted and quantified from immunity tests. The different effects (upset events), that can be seen while, or after, the disturbance is generated, can for example be divided into the Level 1 – 5 scale described in Chapter 5. It is important to make an accurate estimate of the sensitivity, especially since some commercial-off-the-shelf (COTS) equipment may not pass the requirements of the EMC regulations for high frequency and/or wide band disturbances (as seen in Paper V), even if they have passed the regulatory EMC tests.

8.3.2.2 Redundancy

The redundancy term is (like the "consequence" term) estimated from an EMC IEMI audit together with the system owner. It should be based on the extent of backup and/or alternative solutions to performing the facility's primary function. Past experiences, e.g., lightning induced incidents or other faults, may provide insights into the redundancy of the facility. A facility with good redundancy should be able to degrade "gracefully" [54].

8.3.2.3 Receptivity

The receptivity term is defined as to describe a transfer function within and between zones as a gain between two points (simple case being a shielding efficiency factor). It should be dependent on which zone number the disturbance is observed or expected and from which transmission/injection point it originated. It is desirable that the quantity received decreases as the zone number increases (for deeper interior zones).

For practical and economical reasons all possible transfer functions (from and to all ports/points and zones in the system) cannot be examined. Therefore, only the most "critical transfer functions" should be examined. That is, from the most accessible zone/port to zone(s) containing equipment considered especially critical for the operation of the facility's primary function

(denoted “critical zone”) (see fig. 4 in Paper VI). The critical zone could, for example, be from an easily accessible port inside the facility to a room containing sensitive equipment. EMC audits, with IEMI in mind, will determine these zones and/or ports of interest. By correlating the, e.g., voltages, currents or fields within this critical zone from the suggested injection point of the electromagnetic energy, this receptivity of disturbances for the facility can be judged. The receptivity term can be formed for both conducted and radiated disturbances.

8.3.2.3.1 Stochastic approach to transfer function and receptivity

The response of the critical equipment of the facility and the transfer function of the critical zone(s) are often (for a range of waveforms and other parameters) unknown due to complicated equipment response and/or configuration of the facility. Also, we assume that the critical equipment (e.g., computers) in the facility may be located anywhere within this critical zone (position for individual pieces of equipment is stochastic). Furthermore, the transfer function could change with time when (intentional) system changes takes place (e.g., addition of new ports and/or sub-systems), due to deterioration (e.g., corrosion of contacts between metallic plates) or even accidentally (e.g., leaving a door open to shielded compartment). Due to this complexity, a one-to-one determination between a particular disturbance and the outcome (different upset events) is very difficult to attain. A statistical approach to determine the correlation between a particular disturbance and received quantity (that is, the critical transfer function) is instead suggested.

Often the norms/quantities of interest are chosen to be the peak-voltages, -currents, -electric- and/or -magnetic fields, but other norms can be used (see table in Chapter 5)

Given this, the chosen norms can be derived from measurements (low level test as in Paper III), simulations (with, e.g., [55]) or calculations (see, e.g., [7]) for the critical transfer function from which the complementary cumulative distribution function (CCDF) can be formed. The CCDF describes the probability of a norm being larger than a certain value, $P(X > x)$. Also the probability of measuring amplitudes in a certain interval $(a:b] = \{x \mid a < x \leq b\}$ (for the critical zone investigated and data collected), that is $P(a < X \leq b)$, is given by [28] (see eq. 3.8):

$$\begin{aligned} &P(a < X \leq b) = CDF(b) - CDF(a) = \\ &(1 - CCDF(b)) - (1 - CCDF(a)) = \\ &CCDF(a) - CCDF(b). \end{aligned}$$

From this we can derive the probability that the quantity measured is within the tolerated boundaries of the upset threshold levels for the equipment con-

nected to the ports of, or positioned within the critical zone. Thus, from the characteristics of the stochastic functions (the PDF and CDF/CCDF) estimate of the receptivity of the critical zone, of the facility can be made.

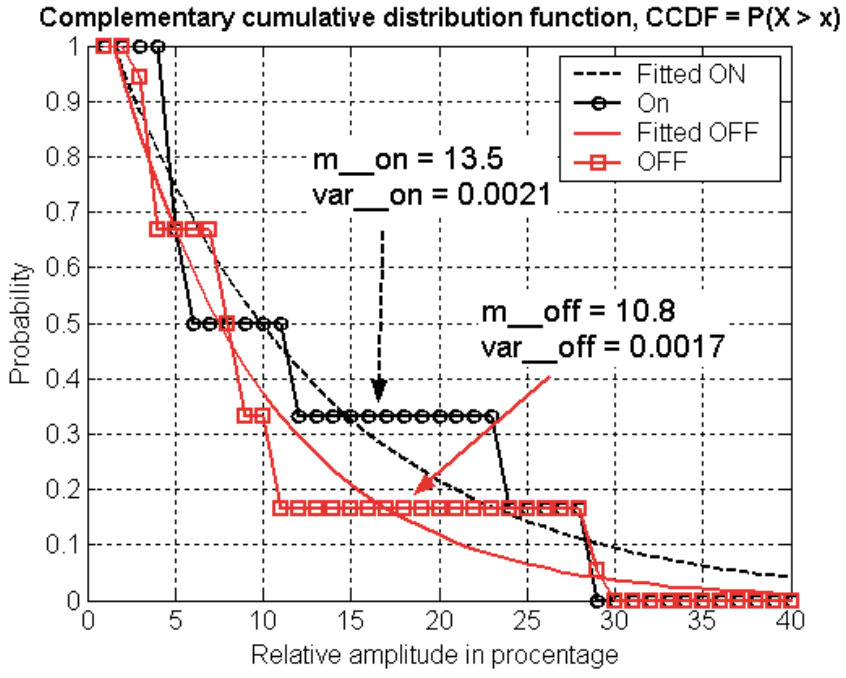

Figure 72. CCDF from Paper VI, describing the probability that the voltage is above a certain value at a random port in the section studied. “ON” and “OFF” represents, respectively, the different states of a switch in the network.

8.3.2.4 Conclusions

First, estimates of the accessibility and consequence together with the susceptibility term (that is formed from the receptivity, redundancy sensitivity terms) are made. Second, by combing these three terms on the axis of the IEMI/ASC-cube a classification of the facility from an IEMI perspective can be made (see fig. 73). Also several facilities can be judged against each other or a mitigation measures installed can be studied, to see the effect on the vulnerability of the facility from IEMI.

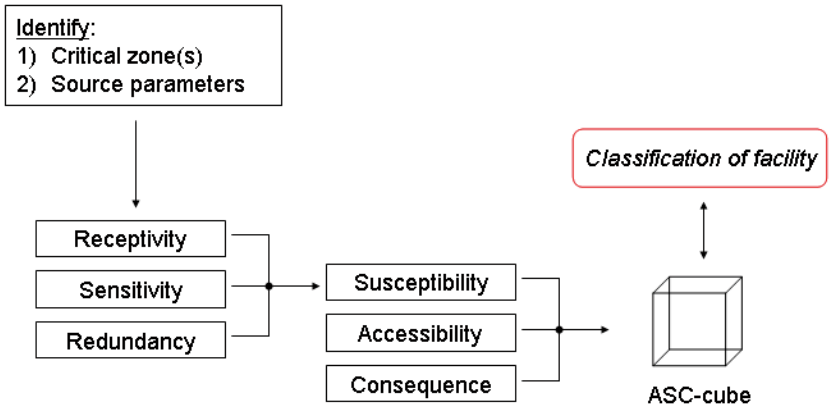

Figure 73. The flowchart for the suggested classification method.

8.4 Summary

In Chapter 8, some of the problems with using a term, such as the shielding effectiveness, to classify systems, were discussed. These difficulties are a result of the large variations of the field within the tested system, when parameters, like internal probe position, change. In addition, in a facility, or large distributed system (e.g., the electrified railway), the physical boundaries may not coincide with the electromagnetic zone boundaries. Therefore a new method was developed (Paper VI) that is based in the terms *accessibility*, *susceptibility* and *consequence*. These terms are in turn defined and estimated on an unnumbered scale. By combining these three factors in the so called ASC-cube the classification of a facility, comparison between several facilities or evaluation of mitigation measures, can be made.

9 Conclusions

It has been seen, in this thesis, that there is a threat posed to civilian society from sources and weapons that can produce high power electromagnetic pulses. These can be used maliciously to disturb or damage electronic equipment and/or system. The main conclusions drawn from this thesis are:

- The military legacy on the research on EMP effects on has focused on radiated disturbances and traditional electromagnetic compatibility (EMC) investigations do not consider very high field strengths or unusual injection means, ports. Thus, the propagation of differential mode (DM) UWB transients in low-voltage power cables, when injected into a power socket of a facility, was studied. The effects on this above said transient, when encountering such objects as bends on the cables, switches and junctions between different cable sections were studied, both in a laboratory setup, but also in the network of a facility. It was seen that for a DM UWB transient that propagates in a low-voltage cable (Paper II), the launched transverse electromagnetic (TEM) propagation mode is the dominant mode, thus, preserved through bends and simple junctions made in the laboratory setup (Paper II and III). Also, the behavior could be simulated (by FDTD code) or predicted by analytical means. For the low-voltage network of an investigated facility it was seen that although the TEM propagation mode of transient was not preserved large voltages could be delivered to loads (systems) connected to the network (Paper III). Using statistical methods, the behavior and characteristics of the network could be investigated.

- As the characteristics of the disturbances associated with IEMI often have very high frequency content, the existing mitigation measures and protection components may not be adequate. Therefore, a realistic point of entry, with normal protection components, were built and tested against transients with nanosecond rise-times (Paper VIII). The response was seen to correspond to specified results from lighting electromagnetic pulses. However, it was seen that for UWB transients (sub-nanosecond rise-time) the protection components may not work as intended, due to parasitic components that arises from the packaging of the device (Paper I).

- The large spatial distribution of many civilian facilities and critical infrastructures (e.g., power generation, communications, train system, etc.) presents many unexpected ports for an attacker as the majority of the parts of these systems are not protected or secure. As the new European Rail Traffic management System (ERTMS) will utilize wireless communication for communication and control of the trains, the vulnerability from different radiating high power electromagnetic (HPEM) sources was investigated (Paper IV). This system level assessment was done by studying the individual parts of the ERTMS. That is, the characteristics of the available attacking source, GSM-R antenna, coaxial cable and communications equipment and from this estimate which sources (in terms of power and waveform) could be a threat to the ERTMS. Also, it was seen, due to geometry, not all angles of incidence and frequencies are a threat in a given situation.

- As modern electronic equipment and systems may not be tested for waveforms and disturbances other than standardized EMC tests, experiments on some very common commercial-off-the-shelf (COTS) equipment were performed. It was seen that these could easily be disturbed or even destroyed by disturbances similar to standardized tests, much below the EMC requirements (Paper V and VII).

- Also, due to the inherent difficulties with IEMI, a new method for classifying facilities from disturbances that are IEMI is made (Paper VI). It is based on available terminology of accessibility (A), susceptibility (S) and consequence (C), but expands these and forms the IEMI/ASC-cube.

10 Future work

1. New mitigation measures and protection methods have to be developed. This is partly, due to the possible unexpected ports of injection of the disturbance, but also due to the high frequency content that is often associated with HPEM and IEMI leading to the necessity of new surge protective devices.
2. With the growing complexity of the networks and systems of today's society, in conjunction with the interconnectedness between the different infrastructure components, the analytical methods and numerical models and code will not be able to accurately predict the voltages that appears between the terminals of a component due to coupled field. Therefore, statistical methods from measurement (as presented and used in, e.g., Paper III and VI) to estimate the, e.g., expected value and standard deviation of the above mentioned voltages due to front- and back-door coupled fields, will be the most viable solution.
3. With the interconnectedness between critical infrastructures and the inherent difficulties of IEMI (unexpected waveforms, points of origin for disturbances, sources, and more) it is important to investigate the response of all the interconnected infrastructures. What is the response of infrastructures if other are disturbed. That is, if a particular disturbance is injected into a port of the SCADA system of the power generating plant, how will this affect the, e.g., water supply or transport sector. In other words, the strengths of the existing connecting links are vital to know. Also, how large is the "attenuation" of the effect of a disturbance from one infrastructure to the next, i.e., how far will it spread from one infrastructure.
4. With the increasing use of complex and sensitive equipment the need for adequate tests methods arise. The standardized EMC test methods of today are not enough to investigate all the possible disturbances (waveforms, polarization, coupling mode, angle of incidence, etc.) that IEMI may require. Thus, statistical methods (again) are needed to find a test procedure that estimates the likely minimum upset threshold levels for the device under test. In addition, more COTS equipment should be tested for various waveforms and coupling methods, to create data bases, which may reveal general trends for the upset threshold levels for the tested systems and equipment.

11 Acknowledgements

The Swedish Emergency Management Agency (KBM), the Swedish Rail Administration (BV), the Swedish Defence Material Administration (FMV) and the Swedish Defence research Agency (FOI) is acknowledged for funding my PhD research.

I would like to thank my supervisor, Professor Rajeev Thottappillil for always taking time to help me with my research, answering my questions and giving supportive comments on my ideas. I could not have found a better mentor anywhere. My co-supervisor, Dr. Mats Bäckström is equally thanked for raising very good questions and points to my research, as well as always answering his phone. Again, I am blessed with the best supervision I could have had.

The help from Dr. Marley Becerra, Dr. Raul Montaño, Dr. Nelson Theethayi has been invaluable for my research, both at the computer with simulations and at the lab with experiments. Also thanked for having the patience of, at one time or another, sharing an office with me. Likewise the discussions with Mr. Surajit Midya and Mr. Ziya Mazloom were appreciated. The discussions and help from Dr. Marcus Berg is something I am very thankful for.

At the Swedish Defence research Agency (FOI) Mr. Tony Nilsson, Mr. Olof Lundén, Mr. Rolf Johansson and Dr. Magnus Höijer has helped me not only with my experiments and research but also encouraged me to think in new ways and along different paths.

Mr. Ulf Ring, master craftsman, is thanked for always making excellent experimental equipment. Without it, it would be impossible to do my PhD research. Mr. Thomas Götschl and Mrs. Gunnerl Ivarsson are acknowledged for always taking time to help and support with my questions.

All the rest at the Division for Electricity is thanked and appreciation for these last years is given to you all and anybody not mentioned here, it is due to woodworm and nothing else.

Daniel

Summary in Swedish

Avsiktliga elektromagnetiska störningar – Känslighets undersökningar och klassificering av civila system och utrustningar

Denna avhandling kommer att behandla det relativt nya området som kallas ”avsiktliga elektromagnetiska störningar” (eng. ”intentional electromagnetic interference”, IEMI), och det hot som källor (vapen) som kan producera elektromagnetiska (EM) pulser utgör mot det civila samhället om de används i illasinnade syften. Intresset för detta hot från s.k. ”EM-terrorism” har ökat de senaste åren i takt med att vårt samhälles beroende av avancerade och känsliga elektroniska system har ökat. Avhandlingen är strukturerad på följande vis: Först behandlas de olika källor och störningar man kan vänta sig. Sedan studeras de kopplingsvägar som störningarna kan ta in i systemen. Efter detta tar avhandlingen upp hur system kan påverkas respektive skyddas från störningar. Allra sist ska vi se hur man kan klassificera byggnader och stora distribuerade system mot dessa avsiktliga elektromagnetiska störningar.

Traditionellt har det oftast studerats, p.g.a. det ”militära arvet” från det kalla kriget, främst hur strålade störningar kan påverka system, inte hur stort hotet från ledningsburna störningar är. Detta, tillsammans med det faktum att traditionella studier inom elektromagnetisk kompatibilitet (EMC, ElectroMagnetic Compatibility) inte behandlar väldigt stora fältstyrkor eller ovanliga kopplingsvägar för hur störningar kan ta sig in i system. Därför är det viktigt att studera hur mycket bredbandiga (stor spridning i frekvens) transienter, injicerade i t.ex. ett eluttag, sprider sig i en byggnads elnät eller datanät. En sådan transient kan lätt injiceras i ett oskyddat uttag och eventuellt sprida sig till flera oskyddade system kopplade till nätverket. För att bedöma riskerna från dessa transienter i ett givet nätverk, är det viktigt att veta hur t.ex. förgreningspunkter mellan flera kablar eller böjar på en kabel eller hur en viss typ av kabel i sig påverkar transienterna. Därför studerades just detta i både laboratorieuppställningar och ett verkligt elnät i en byggnad.

Det sågs att för de studerade transienterna så bevaras den injicerade elektromagnetiska fältmoden (Transversell ElektroMagnetisk, TEM) när transi-

enten utbreder sig i en nätkabel. Därmed kan transienten utan svårigheter simuleras med tillgängliga verktyg. Dessutom sågs det att en böj på kabeln inte påverkar transienten till den grad att det kan mätas i andra änden på kabeln. Det vill säga, transienten tappar ingen mätbar effekt i böjen, något som annars hade kunnat användas som ett skydd. TEM visar sig vara den dominerande utbredningsformen (moden) för de ovannämnda fallen. Det visade sig också att för enklare förgreningspunkter mellan kablar gjorda i laboratoriet så bevarades TEM-moden när den utbreder sig (propagerar) genom dessa förgreningar.

Den spänning som mottas på den andra sidan av förgreningen kunde förutsägas både analytiskt och med numeriska simuleringsverktyg. För elnätet i den studerade byggnaden var den relativa spänning (jämfört med den injicerade) som mättes i de olika eluttagen (nätverkets portar) till största del tillräcklig för att skada eller störa oskyddade system. Däremot kunde inte de mottagna transienterna förklaras med de enkla metoder som användes för uppställningarna i laboratoriet. Detta tros bero på den större komplexiteten som nätverket i byggnaden har. Dock kunde det, med hjälp av statistiska metoder, göras en bedömning av hur transienter injicerade i elnätet skulle fortplanta sig, och därmed hur stor den relativa hotbilden var för system inkopplade i just detta elnät. Vi kommer att återvända till de statistiska metoderna och resultaten för detta elnät senare.

Eftersom de störningar och transienter som normalt förknippas med EM-terrorism (IEMI) ofta har ett frekvensspektrum med väldigt högfrekventa delar är det osäkert om existerande skyddsmetoder och -komponenter är tillräckliga. Därför testades normala skyddskomponenter (varistorer och gasurladdningsrör) i en kopia av en byggnads elcentral, mot transienter med stigtider i nanosekundområdet. Det sågs att skyddskomponenterna generellt sett fungerar mot dessa störningar såsom specificerat (dvs. mot åskliknande transienter). Samtidigt kunde den injicerade transienten koppla till andra ledningar i elcentralen som inte använts för att injicera transienten. Däremot sågs det att skyddskomponenter som utsätts för störningar med stigtider kortare än en nanosekund, inte klarar av dessa. Detta beror på att själva inkapslingen runt den ickelinjära komponenten av skyddet skapar s.k. ”parasitiska impedanser”, som påverkar skyddets förmåga att hantera störningar med väldigt korta stigtider.

På grund av den stora fysiska utspridningen och storleken hos många civila byggnader och system (t.ex. eldistribution, kommunikation, järnvägar, etc.) samt det faktum att stora delar av dessa system inte är skyddade mot störningar eller elsäkerhetsmässigt isolerade, finns det många oväntade ingångar (portar) i vilka elektromagnetisk energi och störningar kan injiceras, antingen ledningsbundet eller strålat. Eftersom det nya europeiska järnvägssignalsystemet (ERTMS) kommer att utnyttja trådlös kommunikation

för detta, kommer det att finnas många avsiktliga antenner där störningar kan ta sig in. Därför studerades hur sårbart detta system kommer att vara mot några typer av elektromagnetiska källor med hög effekt (eng. High Power ElectroMagnetic [source], HPEM) när dessa bestrålar kommunikationsantennerna, som sitter antingen på tågen själva eller i toppen av masterna vid sidan av spåret. Denna undersökning på systemnivå gjordes genom att studera de ingående delarna för kommunikation med tåg i ERTMS, såsom "GSM-R"-antennernas karakteristik utanför det normala användningsområdet och den anslutna kommunikationsutrustningens tålighet mot störningar. Från detta uppskattades i vilka situationer och från vilka källor som systemet kan slås ut. För en given situation sågs det att inte alla infallsvinklar mot GSM-R-antennen är ett hot vid alla frekvenser och att mindre hemma-byggda källor troligast inte kan skada systemet permanent.

Vanlig modern civil elektronisk utrustning är troligen inte testad för tålighet mot störningar som inte är beskrivna i standardiserade EMC-testkrav. Däremot kan sådana störningar definitivt användas avsiktligt. Dessutom används civila elektroniksystem alltmer i applikationer de ursprungligen inte var avsedda för. Av dessa skäl undersöktes tåligheten hos några vanliga trådlösa system. Det visade sig att det är oroväckande lätt att störa, och till och med förstöra, sådana system med väldigt låga fältstyrkor. Även om de genomförda testerna inte tillfullo överensstämmer med standardiserade EMC-tester, så är det intressant att nämna att de testade systemen ibland tålde mindre än de angivna EMC-kraven.

På grund av de problem som nämnts ovan i samband med avsiktliga störningar (ovanliga vågformer och oväntade injiceringspunkter) behövs det en ny metod för att klassificera byggnader och större distribuerade system i ett IEMI-sammanhang. Den föreslagna metoden baseras på att man bestämmer tillgänglighet (eng. accessibility), känslighet (eng. susceptibility) och konsekvens för objektet som undersöks. Sedan sammanfogas de tre värdena i en gemensam punkt i ett kubdiagram. De beskriver då i princip hur lätt det är att få tillträde (access) till vitala system i en byggnad, hur känsliga dessa system är mot störningar samt vilka konsekvenserna blir.

Slutligen undersöktes en metod för hur man ska kunna mäta transienter med både höga effekter och väldigt korta stigtider, genom att använda ett parallellkopplat motstånd (eng. resistive shunt) baserat på en $CuSO_4$-lösning (kopparsulfat), och mäta strömmen genom motståndet med en strömprob med brett frekvensband. Fördelen med detta är att man skiljer högeffektsignalen från den känsliga mätutrustningen, t.ex. oscilloskopet. Metoden har testats med framgång för att mäta HPEM-signaler.

References

1. John Losee, “A Historical Introduction to the Philosophy of Science, 4 ed.”, Oxford university Press, 2001
2. David Bodanis, “Elektricitet: Historien om universums mäktigaste kraft”, Månpocket 2006
3. Nationalencyklopedin, Accessible via www.ne.se, August 2008
4. Roald K. Wangsness; “Electromagnetic fields, 2nd edition”, John Wiley & Sons, 1986
5. IEC Standard, 60050-161, “International Electrotechnical Vocabulary, Chapter 161 on EMC”
6. C. D. Taylor and D. V. Giri; “High-Power Microwave Systems and Effects”, Taylor & Francis, 1994
7. C. E. Baum “Electromagnetic topology: A formal approach to the analysis and design of complex electronic systems”, Interaction Notes 400, Sep. 1980
8. Torbjörn karlsson, “The Topological Concept of Generalized Shield”; Interaction Notes 461, Januari 1988
9. IEC Standard, 61000-1-5, “Electromagnetic compatibility (EMC) - Part 1-5: General - High power electromagnetic (HPEM) effects on civil systems”, 2004
10. IEC Standard, 61000-1-3, “Electromagnetic compatibility (EMC) – Part 1-3: General - The effects of high-altitude EMP (HEMP) on civil equipment and systems”, 2001
11. “Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Volume 1: Executive Report 2004” Accessible via www.empcommission.org, August 2008
12. “Electromagnetic environment handbook; EMMA”, Swedish Material Defence Administration (FMV), 2005
13. IEC Standard, 61000-2-9, “Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance. Basic EMC publication”
14. IEC Standard, 61000-2-13, “Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted”, 2005
15. Baum, C.E.; Baker, W.L.; Prather, W.D.; Lehr, J.M.; O'Loughlin, J.P.; Giri, D.V.; et.al, “JOLT: a highly directive, very intensive, impulse-like radiator”, *Proceedings of the IEEE*, Vol. 92, Issue 7, July 2004 Page(s):1096 - 1109
16. D. V. Giri and F. M. Tesche, “Classification of Intentional Electromagnetic Environments (IEME)”; *IEEE Transactions on Electromagnetic compatibility*, Vol. 46, No. 3, August 2004
17. V. M. Loborev, “The modern research problems,” *presented at the Plenary Lecture, AMEREM’96*, Albuquerque, NM, May 1996.
18. URSI the Toronto General assembly, 1999, Accessible via www.ursi.org/Resolutions/99%20Toronto%20Res%20Eng.doc, August 2008

19. V. Fortov, Y. Parfenov, L. Siniy, L. Zdoukhov, “Russian Research of Intentional Electromagnetic Disturbances Over the Past Ten Years”, *Proceedings of the AMEREM06 conference*, Albuquerque, USA, 2006)
20. D. Sawyer, 20/20 *Segment on Non-Lethal Weapons*. New York: American Broadcasting Company (ABC), Feb. 1999.
21. M. B. Bäckström and K. G. Lövstrand, “Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004
22. Mats Bäckström, Torleif Martin and Jörgen Lorén, ”Analytical Model for Bounding Estimates of Shielding Effectiveness of Complex Resonant Cavities”, *Proceedings of the 2003 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Istanbul, Turkey, May 11-15, 2003.
23. Hill D. A. et al., “Aperture Excitation of Electrically Large, Lossy Cavities”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 36, No. 3, August 1994.
24. Warne L.K. and Lee K.H.S., “Some Remarks on Antenna Response in a Reverberation Chamber”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 43, No. 2, May 2001.
25. C. R. Paul, “Analysis of Multiconductor Transmission Lines”, John Wiley & Sons, 1997
26. K. Madsén, "Performance Tests of the RADAN 303B with Sub-slicer and TEM-antenna", FOI Test Report, FOA-R--99-01140-612--SE, May 1999. Swedish Defence Research Agency (FOI)
27. Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky, and M. Ianoz, “Conducted IEMI Threats for Commercial Buildings”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004
28. G. Blom, Sannolikhetsteori Med Tillämpningar. Lund, Sweden: Studentlitteratur, 1984.
29. R. B. Standler, “Protection of Electronic Circuits from Over-voltages”, John Wiley & Sons, 1989
30. T. Weber, R. Krzikalla and J. L. ter Haseborg, ”Linear and Nonlinear Filters Suppressing UWB Pulses”, *IEEE Transactions on Electromagnetic Compatibil*ity, Vol. 46, No. 3, August 2004
31. P. R. Emtage, “The Physics of Zinc Oxide Varistors”, *Journal of Applied Physics*, Vol. 48, No. 10, October 1977
32. P. Degauque, J. Hamelin, “Electromagnetic Compatibility”, Oxford University Press, 1993
33. IEC Standard 61000-5-9 Ed. 1, “Electromagnetic Compatibility (EMC) -- Part 5-9: Installation and mitigation guidelines -- System level susceptibility assessments for HEMP and HPEM”, 2008
34. Richard Hoad, Nigel J. Carter, David Herke and Stephen P. Watkins, “Trends in EM Susceptibility of IT Equipment”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004
35. D. C. Wunsch and R. R. Bell, “Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors due to Pulse Power Voltages”, *IEEE Trans. Nuc. Sci.*,Vol. NS-17, Dec. 1970.
36. Tony Nilsson and Rolf Johansson “Investigation of HPM Front-door Protection Devices and Component Susceptibility”, FOI-R-1771—SE, ISSN 1650-1942, November 2005. Swedish Defence Research Agency (FOI)
37. http://www.ece.drexel.edu/courses/ECE-E431/latch-up/latch-up.html, August 2008

38. W. Reczek, J. Winnerl and W. Pribyl, “Critical Charge Model for Transient Latch-up in VLSI CMOS Circuits”, *Proceedings IEEE Int. Conference on Microelectronic Test Structures*, Vol. 2, No. 1, March 1989
39. IEC Standard 61000-6-1 Ed. 2, “Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments”, 2005
40. C. A. Balanis, “Antenna Theory; Analysis and Design, 2nd edition”, John Wiley & Sons, 1997
41. European Railway Agency, Accessible via http://www.era.europa.eu/, August 2008
42. www.botniabanan.se, August 2008
43. Tony Nilsson and Rolf Johansson “Implementation of HPM Front-door Protection and Component investigation”, FOI-R-2126—SE, ISSN 1650-1942, December 2006. Swedish Defence Research Agency (FOI)
44. T. Weber and J. L. ter Haseborg, “Measurement Techniques for Conducted HPEM Signals”, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, August 2004
45. Zheng-ying Li, “Improved CuSO4 HV pulse divider”, *Rev. Sci. Instrum.* 59 (7), July 1988
46. B. Rácz and A. Patócs, “Design Note: Fast high-voltage resistive pulse divider”, *Meas. Sci. Technol.* 3 (1992), pages 926 – 928
47. Y. Lee, “Subnanosecond high-voltage two-stage Resistive Divider”, *Rev. Sci. Instrum.* 54 (8), July 1983
48. P. Lubicki, J. D. Cross, S. Jayaram, J. Staron and B. Mazurek, “Effect of water Conductivity on its pulse electric strength”, *Proceedings of IEEE Int. Symp. On Electrical Insulation*, Montreal, Canada, June 1996
49. D. Månsson, “Load for exploding wire experiments”, Internal report at div. for Electricity, UU, December 2005
50. Edited by V. Cooray , “The Lightning Flash”, The Institution of Electrical Engineers, 2003
51. J. Delsing, J. Ekman, J. Johansson, S. Sundberg, M. Bäckström, T. Nilsson, “Susceptibility of Sensor Networks to Intentional Electro-magnetic Interference”, *Proceedings of the 17th International Zurich Symposium*, Page(s):172 – 175, February 2006
52. S.M. Rinaldi, J.P. Peerenboom and T.K. Kelly, “Identifying, Understanding and Analyzing Critical Infrastructure Interdependences”, *IEEE Control Systems Magazine*, Dec. 2001
53. “Risk och sårbarhetsanalyser”, Vägledning för statliga myndigheter, KBM rekommenderar 2006:4, Available at http://www.krisberedskapsmyndigheten.se
54. Rawashdeh, O.A.; Lumpp, J.E., “A technique for specifying dynamically reconfigurable embedded Systems”, in *Proc. IEEE Aerospace Conference*, pp. 1-11, 5-12 March, 2005
55. J. Carlsson, T. Karlsson and G. Undén ”EMEC-an em simulator based on topology”, IEEE Trans. EMC, vol. 46, pp. 353-358, August 2004
56. A. Taflove and S. C. Hagness, “Computational Electrodynamics; the Finite-Difference Time-Domain method”, Artech House Publishers, June 2000

Appendix I

Transmission line calculations

For the transmission line requirement to be fulfilled the following conditions must be true:

1. electrically long, i.e., much longer than the wavelength λ considered,
2. the structures cross sectional dimensions, e.g., conductor separation, is electrically small compared to the wavelength λ,

if these conditions are met TEM mode propagation can be assumed. If the conductors are not perfectly conducting (lossy), but otherwise the assumptions above are met, TEM mode is still assumed (so called *quasi-TEM*). If the conditions above are met (accepting lossy conductors) the transmission line (TL) structure can be divided into segments of length Δz which in turn can be described as lumped circuits (fig. 74) with distributed per length resistance, inductance, capacitance and conductance elements.

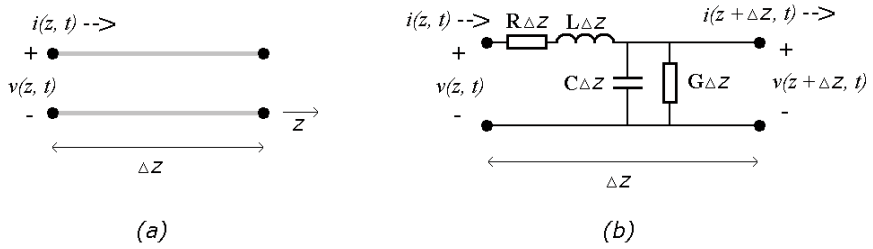

Figure 74. Discrete section of a TL structure. (b) lumped-element equivalent circuit of (a). Here, only two conductors are shown.

Using Kirchhoff's voltage and current laws on the circuit in fig. 74b gives:

$$\begin{cases} v(z,t) - R\Delta z i(z,t) - L\Delta z \dfrac{\partial i(z,t)}{\partial t} - v(z+\Delta z,t) = 0 \\ i(z,t) - G\Delta z v(z+\Delta z,t) - C\Delta z \dfrac{\partial v(z+\Delta z,t)}{\partial t} - i(z+\Delta z,t) = 0 \end{cases} \quad \text{(A.1)}$$

dividing the equations above with Δz and rearranging the terms gives as Δz → 0

$$\begin{cases} \dfrac{\partial v(z,t)}{\partial z} = -Ri(z,t) - L\dfrac{\partial i(z,t)}{\partial t} \\ \dfrac{\partial i(z,t)}{\partial z} = -Gv(z,t) - C\dfrac{\partial v(z,t)}{\partial t} \end{cases} \tag{A.2}$$

which are the time-domain equations for the TL response, also called the *telegraphers equation*. For a steady state sinusoidal condition (A.2) can be written as

$$\begin{cases} \dfrac{\partial V(z)}{\partial z} = -(R + j\omega L)I(z) \\ \dfrac{\partial I(z)}{\partial z} = -(G + j\omega C)V(z) \end{cases} \tag{A.3}$$

The equations (A.3) can be simultaneously solved to give the wave equations for the voltage and current and thus giving the equations for the forward and backwards traveling voltage and current waves with the complex propagation constant along with the characteristic impedance of the TL:

$$\begin{aligned} \gamma &= \alpha + j\beta = \sqrt{(R + j\omega L)(G + j\omega C)} \\ Z_0 &= \sqrt{\frac{R + j\omega L}{G + j\omega C}} \end{aligned} \tag{A.4}$$

However, it is easier to study the pulse propagation using the more complicated time domain equation (A.2), since finite-difference time-domain (FDTD) methods can be used. This is not a study in the numerical sciences and all its complexities, thus, only a brief description of the MTL-FDTD method will be given. The reader is directed to [25] for an extensive source of material. A transmission line is dived into *NDZ* number of space segments each with length Δz and the time span investigated is divided into *NDT* time steps each of duration Δt. The indexes *n* and *k* is used for the time and space domain respectively. Remembering basic numerical sciences, a continuous derivative (around a point *x*) can be written as the difference of function value between point *x*+*h* and *x* normalized by the step length *h* as the step length goes to zero.

$$f'(x) = \frac{\partial f}{\partial x} = \frac{f(x+h) - f(x)}{h} \tag{A.5}$$

using this, the continuous space and time derivatives of (A.2) can be written in discrete form. By rearranging the terms and separating the equations, the voltage and current expressions (V_k^n and I_k^n) for the time step n and in that space point k can be obtained. Equation (A.5) and (A.2) gives after some manipulation the voltage at the source node (k = 1) for the time point n+1.

$$\begin{aligned} V_1^{n+1}\left(\frac{C}{2\Delta t} + \frac{G}{4} + \frac{1}{2\Delta z R_s}\right) = \left(\frac{C}{2\Delta t} - \frac{G}{4} - \frac{1}{2\Delta z R_s}\right) V_1^n \cdots \\ - \frac{1}{\Delta z} I_1^n + \frac{1}{2R_s \Delta z}\left(V_s^{n+1} + V_s^n\right) \end{aligned} \tag{A.6}$$

where V_s^{n+1} is the source voltage at time n+1, R_s is the source internal impedance, G and C are the distributed per length conductance and capacitance, Δz and Δt are the discrete space and time step length. The voltage at the load point ($k = NDZ$+1, observe that the actual load is not considered to be part of the transmission line itself) is given by

$$\begin{aligned} V_{NDZ+1}^{n+1}\left(\frac{C}{2\Delta t} + \frac{G}{4} + \frac{1}{2\Delta z R_L}\right) = \left(\frac{C}{2\Delta t} - \frac{G}{4} - \frac{1}{2\Delta z R_L}\right) V_{NDZ+1}^n \cdots \\ + \frac{1}{\Delta z} I_{NDZ}^n + \frac{1}{2R_L \Delta z}\left(V_L^{n+1} + V_L^n\right) \end{aligned} \tag{A.7}$$

where V_L^{n+1} is the load voltage at time n+1,R_L is the source load. The voltage for all other nodes are given by

$$V_k^{n+1}\left(\frac{C}{\Delta t} + \frac{G}{2}\right) = \left(\frac{C}{\Delta t} - \frac{G}{2}\right) V_k^n - \frac{1}{\Delta z}\left(I_k^n - I_{k-1}^n\right) \tag{A.8}$$

where I_k^n and $I^n{}_{k-1}$ are the currents in the observed point k and the previous point k-1 (which value has to be stored). Finally the current at all the points are given by

$$I_k^{n+1}\left(\frac{L}{\Delta t} + \frac{R}{2}\right) = \left(\frac{L}{\Delta t} - \frac{R}{2}\right) I_k^n - \frac{1}{\Delta z}\left(V_{k+1}^n - V_k^n\right) \tag{A.9}$$

where R and L are the distributed per length resistance and inductance.

Using the initial values ($n = 0$) for the voltages and currents on the TL, load and source and then for each time step k calculating the voltages and currents at all points along the TL the pulse propagation can be obtained.

A short discussion regarding the stability is needed (adopted from [56]. The stability factor (or Courant number) is defined as $S \equiv c\Delta t / \Delta x$, where c is the speed of the wave in the medium. When $S = 1$ the simulated pulse experiences no distortion as it propagates (this is also called "the magic-time-step"), but if $S < 1$ the pulse experiences numerical dispersion which grows as the pulse propagates. If $S > 1$ the solution is unstable and will start to oscillate with ever growing amplitude. In short, our time step is bound by the condition $\Delta t \leq \Delta x / c$ for a stable solution of the propagation of the transient.

Acta Universitatis Upsaliensis

Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 549

Editor: The Dean of the Faculty of Science and Technology

A doctoral dissertation from the Faculty of Science and Technology, Uppsala University, is usually a summary of a number of papers. A few copies of the complete dissertation are kept at major Swedish research libraries, while the summary alone is distributed internationally through the series Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology. (Prior to January, 2005, the series was published under the title "Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology".)

Distribution: publications.uu.se
urn:nbn:se:uu:diva-9264

ACTA
UNIVERSITATIS
UPSALIENSIS
UPPSALA
2008