





SECRET

SECurity of Railways against Electromagnetic aTtacks

Grant Agreement number: 285136
Funding Scheme: Collaborative project
Start date of the contract: 01/08/2012
Project website address: http://www.secret-project.eu

Deliverable D1.3

Model of the waveforms to detect

Submission date: 30/08/2013

Document details

Title	Model of the waveforms to detect
Work package	WP1
Date	30/08/2013
Author(s)	F.Canavero, A.Bonfanti, E.Marchisio
Responsible Partner	POLITO
Document Code	SEC-D1.3-C-0813-Model of the waveforms to detect-POLITO
Version	C
Status	Final

Dissemination level

Project co-funded by the European Commission within the Seventh Framework Programme

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission) Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document history

Revision	Date	Authors	Description
A2	19/08/2013	POLITO	Final Draft

Definitions and acronyms

	Meaning
RF	Radio frequency
EM	Electromagnetic
EMI / IEMI	Electromagnetic Interference / Intentional Electromagnetic Interference
UWB	Ultra wide band
HPEM	High Power Electromagnetic
HEMP	High Altitude Electromagnetic Pulse
FWHM	Full Width at Half Maximum
FFT	Fast Fourier Transform

Table of contents

1. Executive summary ____ *4*

2. Characteristics of the IEMI signals and model of the waveforms ____ *5*

2.1. Model of narrowband waveform ____ **5**

2.1.1. Amplitude modulation ____ 6

2.1.2. Frequency sweep and frequency modulation ____ 8

2.2. Model of ultra wideband waveform ____ **10**

2.3. Model of damped sinusoidal waveform ____ **12**

3. Conclusions ____ *15*

1. Executive summary

In this document the public synthesis of an extensive study performed on signals produced by HPEM and IEMI devices is presented. From this study the various models were extracted.
Interfering signals can be classified as modulated or unmodulated continuous waves, carrierless signals, or pulses. Other waveforms can be formed by combination of basic signals.
Here the most common waveforms are exposed in simplified terms, but modulation schemes can be inter-combined to generate unpredictable waveshapes.

2. Characteristics of the IEMI signals and model of the waveforms

As mentioned in deliverable "D1.2 - Classification of the EM attack signals and characteristics", we have very different types of waveforms we should consider for IEMI. Most of the other waveforms are similar to, or can be formed from, the narrowband, ultra wideband or damped sinusoidal waveforms.
In general, IEMI cannot be exactly identified through a particular waveform: in order to describe mathematically these potential interfering signals, the signal previously mentioned will be taken into account.

2.1. Model of narrowband waveform

The time and frequency domain equations for the narrowband sinusoidal waveform are given by:

$$a(t) = A_0 \cdot \sin(\omega_0 \cdot t) \cdot u(t) \quad \textbf{(eq.1)}$$

$$A(f) = A_0 \cdot j \cdot \pi \cdot [\delta(\omega + \omega_0) - \delta(\omega - \omega_0)] \quad \textbf{(eq.2)}$$

where A_0 is the peak value, $\omega = 2\pi f$, $\omega_0 = 2\pi f_0$ and f_0 is the center frequency. The term $u(t)$ (the so called Heaviside step function) is to ensure $a(t) = 0 \ \forall t < 0$.

In Figure 1 the waveform described in (eq.1) is shown ($A_0 = 1$ for normalization of amplitude).

In Figure 2 the narrowband signal in frequency domain (calculated through the FFT of the time domain signal in Figure 1) is shown.
Please note that, in order to simplify the discussion about the model, the parameters A_0 and f_0 are convenient values chosen to show the model results. For the amplitude value A_0, it is difficult to provide a range of real values, because such values depend on the device characteristics, the distance between the attacking and victim system, the coupling to the victim system, and so on. Therefore, for an analysis of a real case, a more extended investigation must be done, but this goes beyond the purpose of this document.

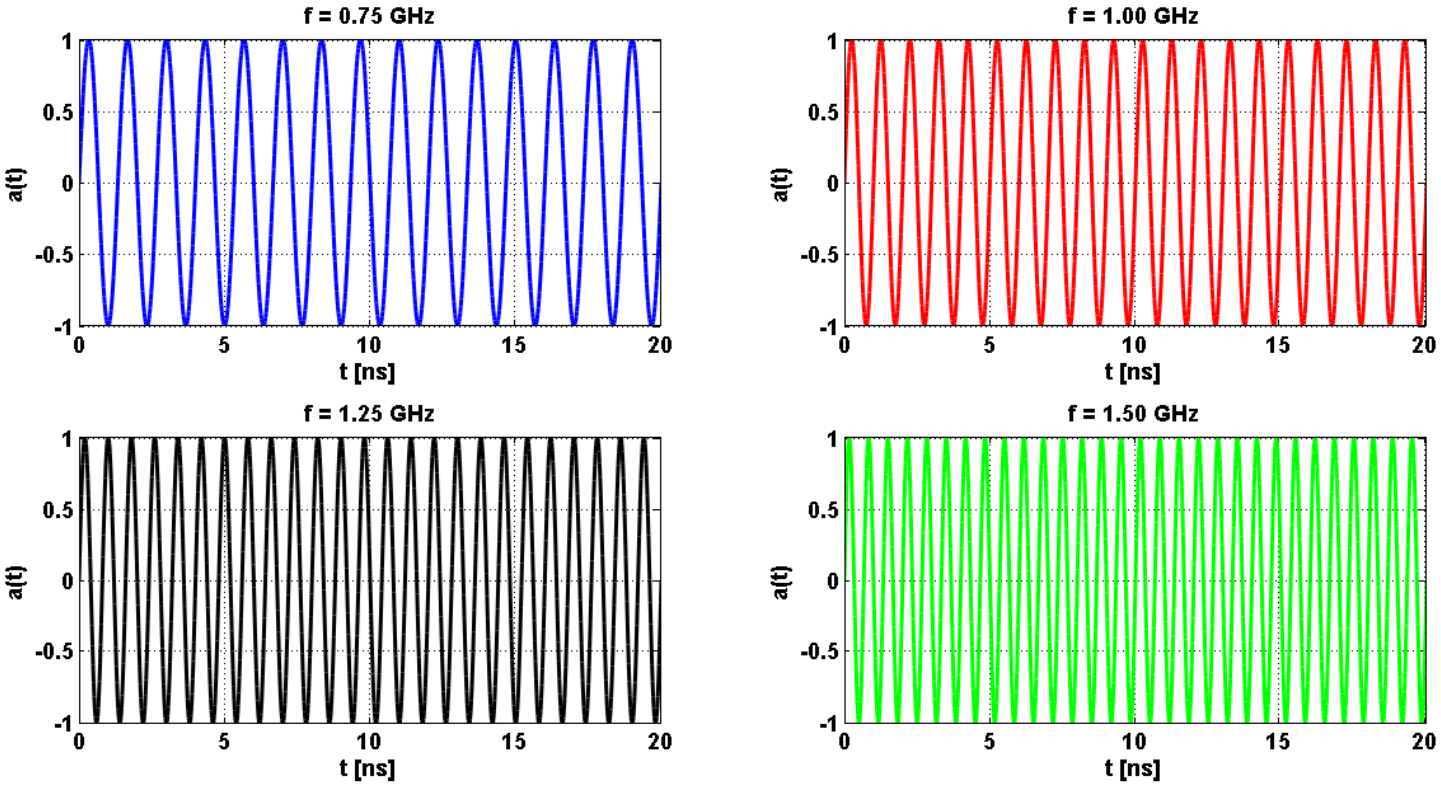


Figure 1 – Narrowband signal in time domain

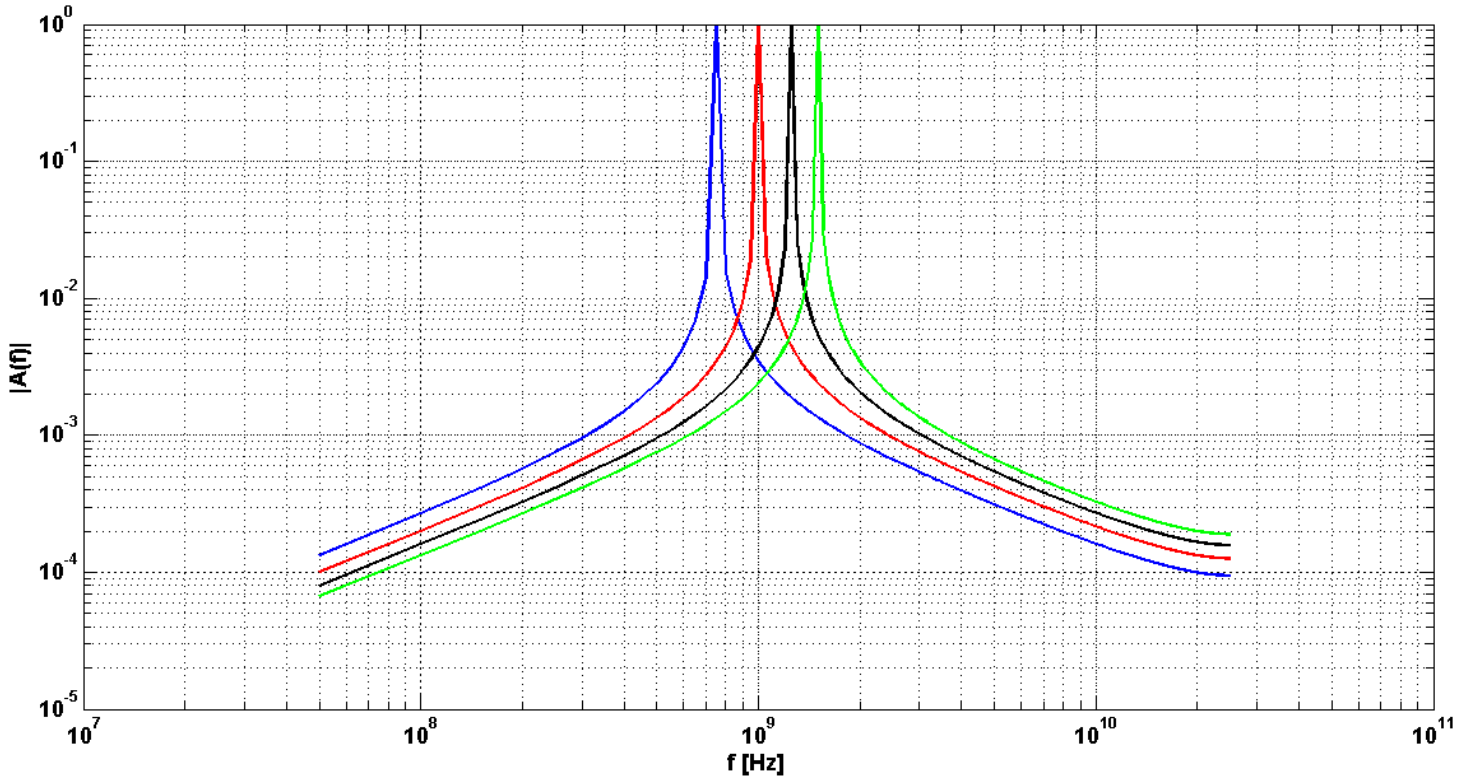


Figure 2 - Narrowband signal in frequency domain (Numerical FFT)

2.1.1. Amplitude modulation

Amplitude modulation (AM) works by varying the strength of the transmitted signal in relation to the information or disturbance being sent. Amplitude modulation is formed by the product of a carrier sine wave and an arbitrary waveform that is the message or disturbance to be transmitted

$$a(t) = A_0[1 + m(t)] \cdot \sin(\omega_0 \cdot t) \cdot u(t) \quad \textbf{(eq.3)}$$

where $m(t)$ represents the modulation and A_0 is the carrier amplitude; ω_0 is the carrier angular frequency. For example, a single tone modulation is described by $m(t) = [M \cos(\omega_m t + \varphi)]$ and M is the message amplitude, i.e. the maximum change in the carrier amplitude, measured from its unmodulated value; ω_m is the modulation angular frequency.
The AM modulation index (also called "modulation depth") is the measure of the amplitude variation surrounding an unmodulated carrier. For AM, it relates to variations in carrier amplitude and is defined as:

$$h = \frac{M}{A_0}$$

So h = 0.5, if the carrier amplitude varies by 50% above (and below) its unmodulated level; and h = 1.0, if it varies by 100%. To avoid distortion, modulation depth must not exceed 100 percent. However, poorly designed AM modulators (as can be the case with disturbing devices) may generate overmodulation. Variations of a modulated signal with percentages of modulation are shown in Fig. 3. In each image, the maximum amplitude is higher than in the previous image (note that the scale changes from one image to the next).

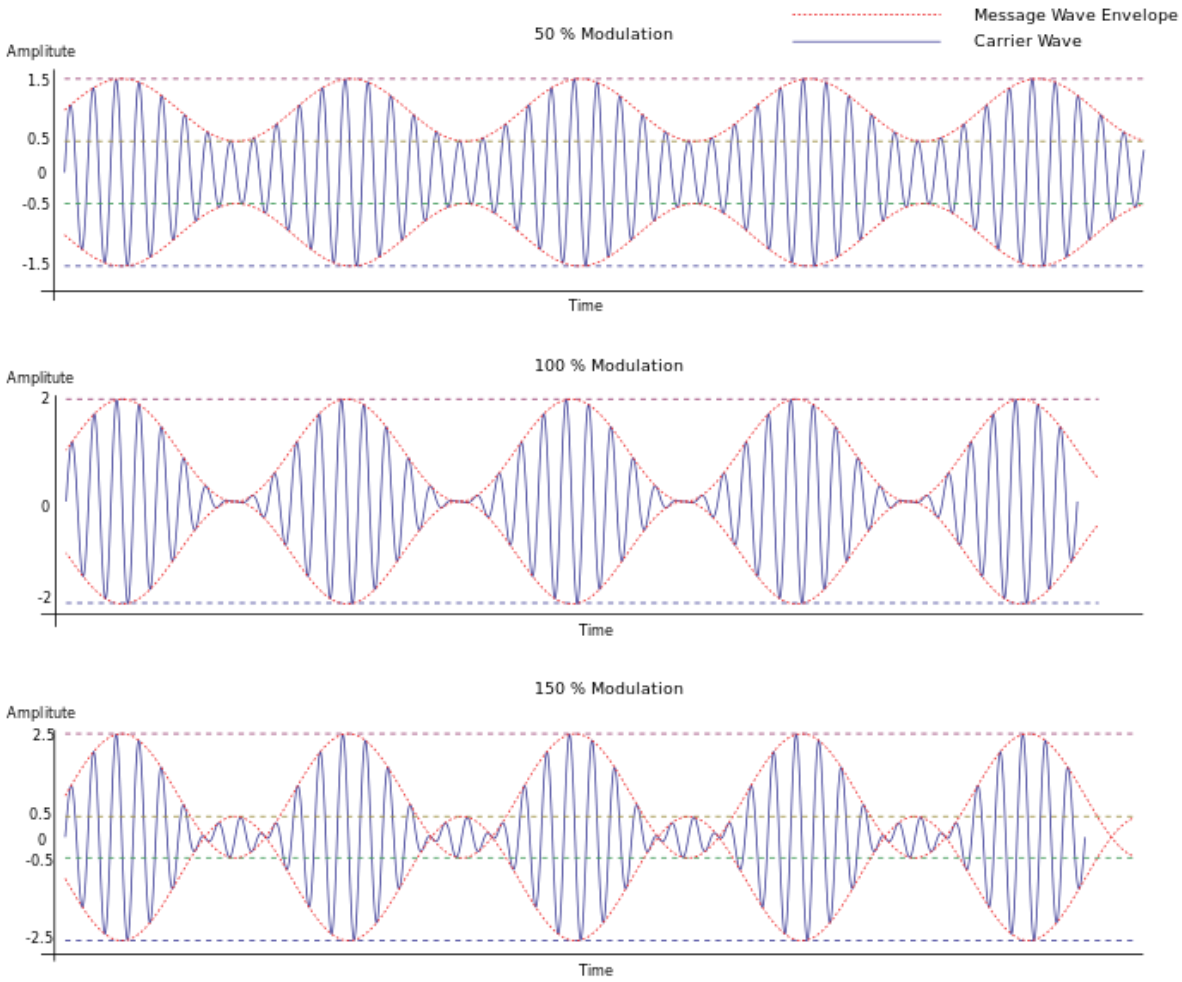


Fig. 3 – AM signal in time domain

The spectrum of AM is a result of computing the Fourier transform of eq. 3 and becomes

$$\mathrm{A}(\mathrm{f}) = \frac{1}{2}\mathrm{A}_0 \cdot \mathrm{j} \cdot \cdot \left[M(\omega + \omega_0) - M(\omega - \omega_0)\right] \quad \textbf{(eq.4)}$$

Where *M*(.) is the Fourier Transform of the modulation quantity *m(t)*. Fig. 4 shows the plot of a general AM-modulation spectrum. The top trace of Figure 4 depicts the frequency of *m*(*t*) the bottom trace depicts the modulated carrier. It has two components: one at a positive frequency centered on $+\omega_c$) and one at a negative frequency (centered on $-\omega_c$). Each component contains the two sidebands and a narrow segment in between, representing energy at the carrier frequency

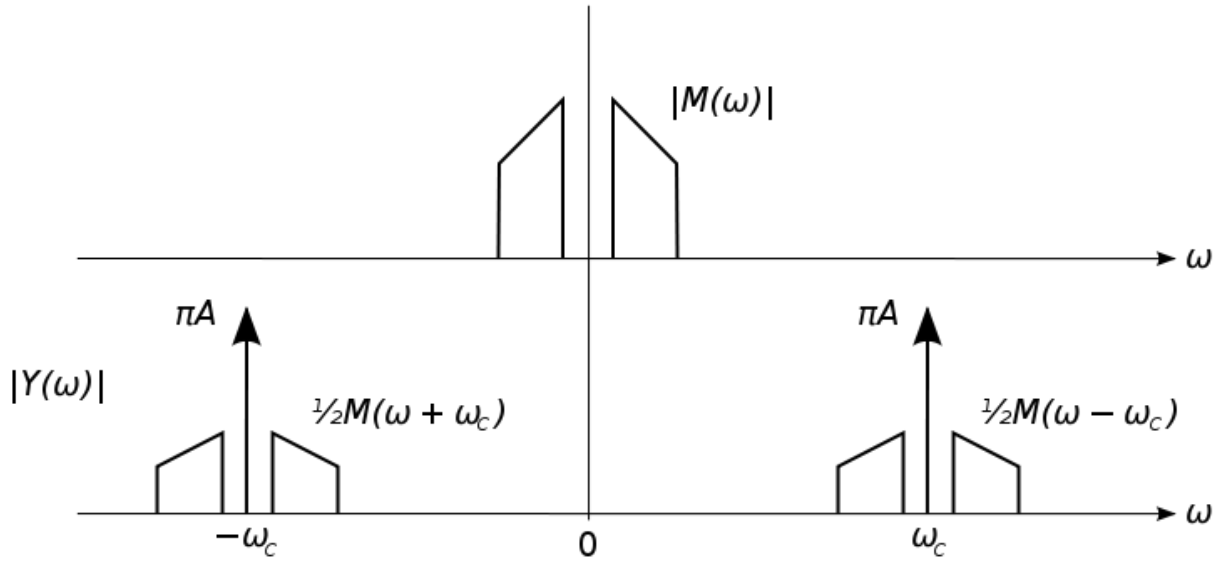


Fig. 4 – Spectrum of a general AM signal

As evidenced by its spectrum, AM is inefficient in power usage; at least two-thirds of the power is concentrated in the carrier signal, and it does not carry the information or the distrubance. For this reason, it is rather unlikely that AM be chosen for a disturbing device.

2.1.2. Frequency sweep and frequency modulation

In order to broaden the spectrum of the sinusoidal signal, a frequency sweep or a frequency modulation can be applied to the original waveform. This can be a way to obtain a larger spectrum and to radiate a large amount of power at the same time.

The notion of frequency sweeping is evident as we can see in Figure 1 and Figure 2.

Concerning the frequency modulation (FM), the mathematical description can be very difficult, and we should avoid overloading the reader with the FM theory.
In order to understand the effect of a frequency modulation, the time domain and frequency domain of the FM signal, respectively, in Figure 5 and Figure 6 are shown.
The time domain equation, which describes the FM signal in Figure 5, is the following:

$$a(t) = A_c \cdot \cos\left[2 \cdot \pi \cdot f_c \cdot t + m \cdot \sin\left(2 \cdot \pi \cdot f_m \cdot t\right)\right] \quad \text{(eq.3)}$$

The parameters used for generating the FM signal are the following:

$$A_c = 1$$
$$f_c = 500\,MHz$$
$$f_m = 10\,MHz$$
$$m = \frac{f_c - f_m}{f_m} = 49$$

where f_c is the carrier frequency, f_m is the modulation frequency and m is the modulation index.

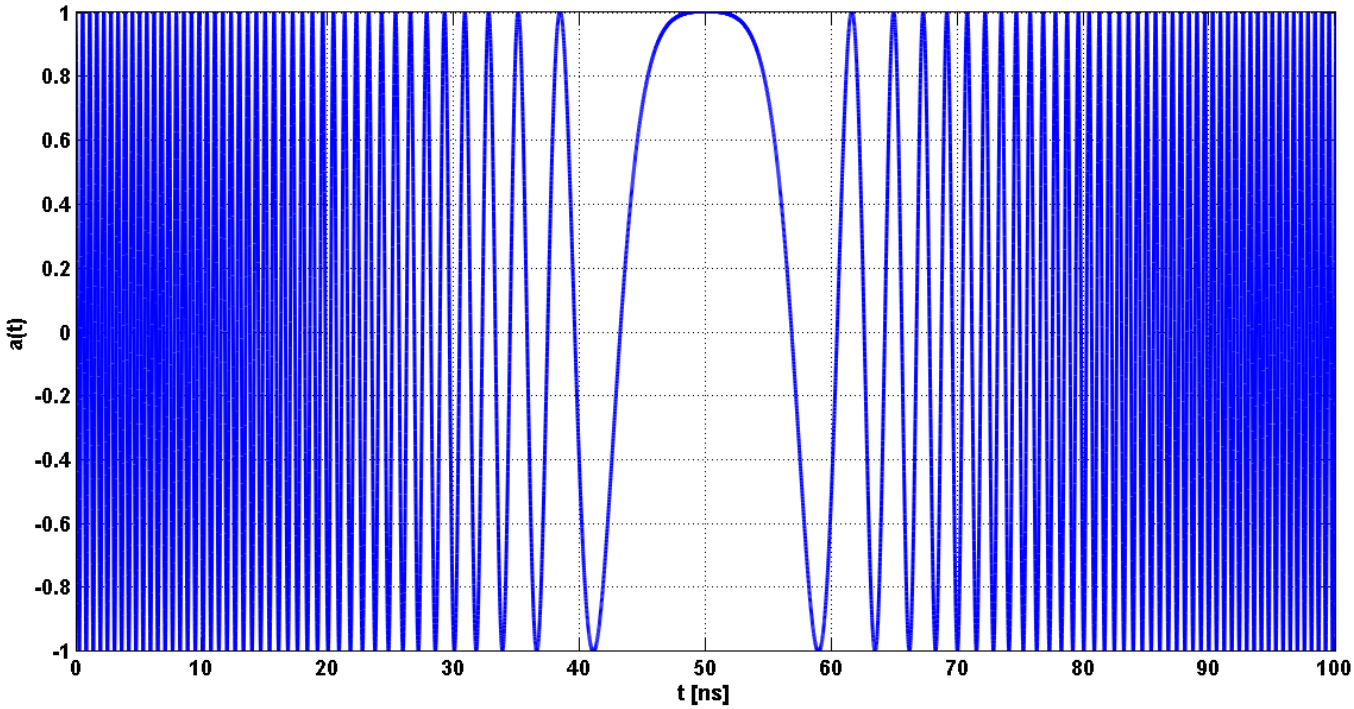


Figure 5 - FM signal in time domain

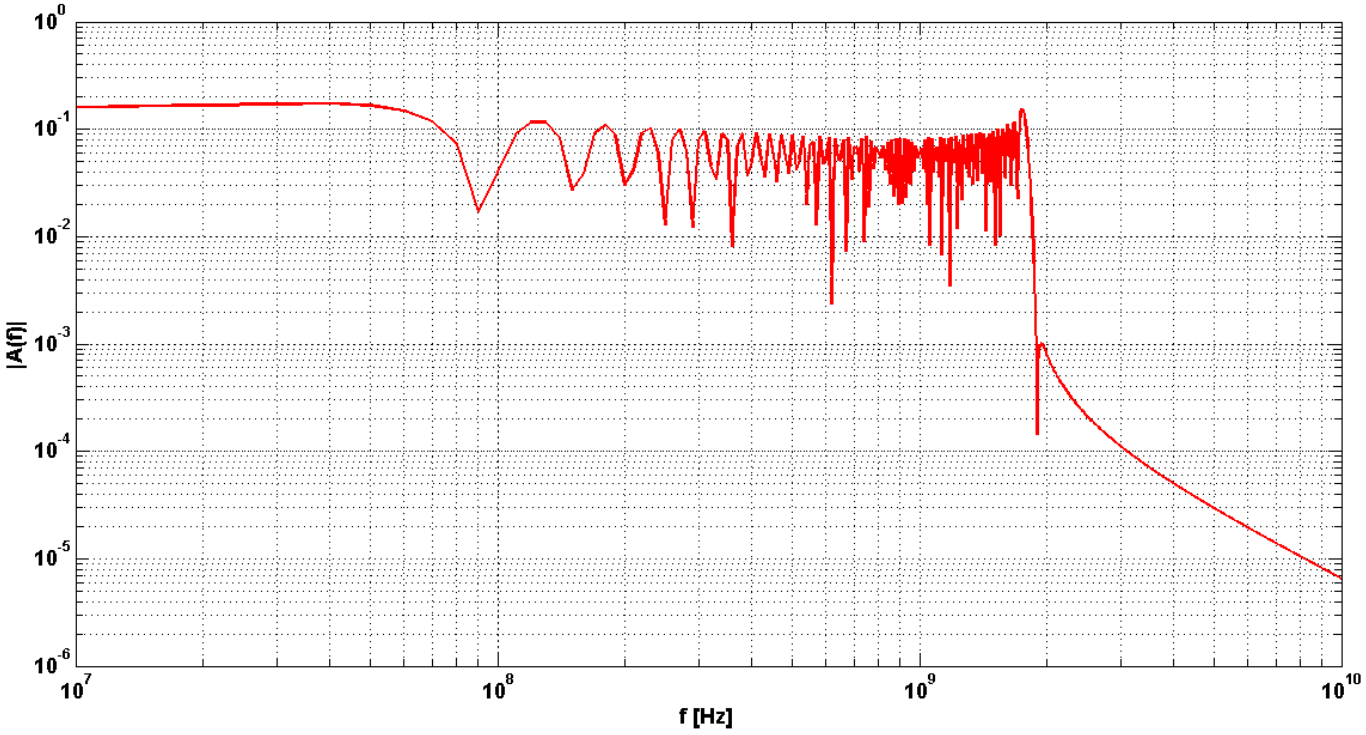


Figure 6 - FM signal in frequency domain (Numerical FFT)

2.2. Model of ultra wideband waveform

The time and frequency domain equations for the double exponential waveform are given by:

$$\mathrm{a}(\mathrm{t}) = A_0 \cdot \left(e^{-\alpha \cdot t} - e^{-\beta \cdot t}\right) \cdot u(t) \quad \textbf{(eq.4)}$$

$$\mathrm{A}(\mathrm{f}) = \frac{A_0 \cdot (\beta - \alpha)}{(\alpha + j\omega) \cdot (\beta + j\omega)} \quad \textbf{(eq.5)}$$

where A_0 is the peak value (note that $\max\{a(t)\} = A_0(\alpha, \beta)$), $\omega = 2\pi f$, α and β relate to the FWHM-time and the rise time respectively. The term $u(t)$ (the so called Heaviside step function) is to ensure $a(t) = 0 \ \forall t < 0$.

$$\alpha = \frac{1}{\mathrm{T}_{\mathrm{FWHM}}}$$

$$\beta = \frac{1}{\mathrm{t}_{\mathrm{rise}}}$$

In Figure 7 the waveform described in (eq.4) is shown ($\mathrm{A}_0 = 1$ for normalization of amplitude).

In Figure 8 the UWB signal in frequency domain (calculated through the FFT of the time domain signal in Figure 7) is shown.

The rise time and FWHM-time depend on the IEMI generator but – according to our study – we may assume that their values broadly fall within the following range:

$$\mathrm{T}_{\mathrm{FWHM}} = 1 \div 10 \ ns$$

$$\mathrm{t}_{\mathrm{rise}} = 0.1 \div 1 \ ns$$

Please note that, in order to simplify the discussion about the model, the parameter A_0 is a convenient value chosen to show the model results. For the amplitude value A_0, it is difficult to provide a range of real values, because such values depend on the device characteristics, the distance between the attacking and victim system, the coupling to the victim system, and so on. Therefore, for an analysis of a real case, a more extended investigation must be done, but this goes beyond the purpose of this document.

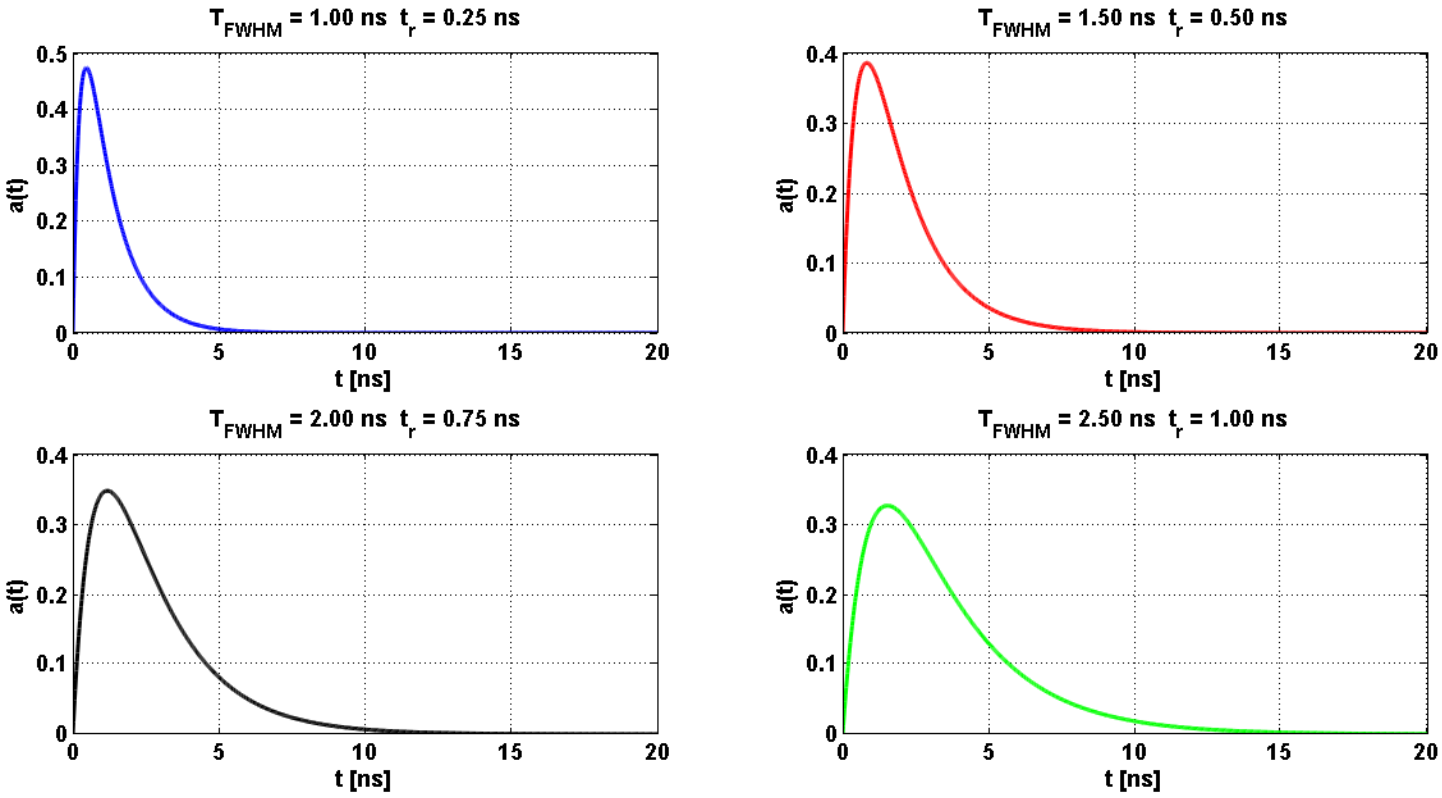


Figure 7 - UWB signal in time domain

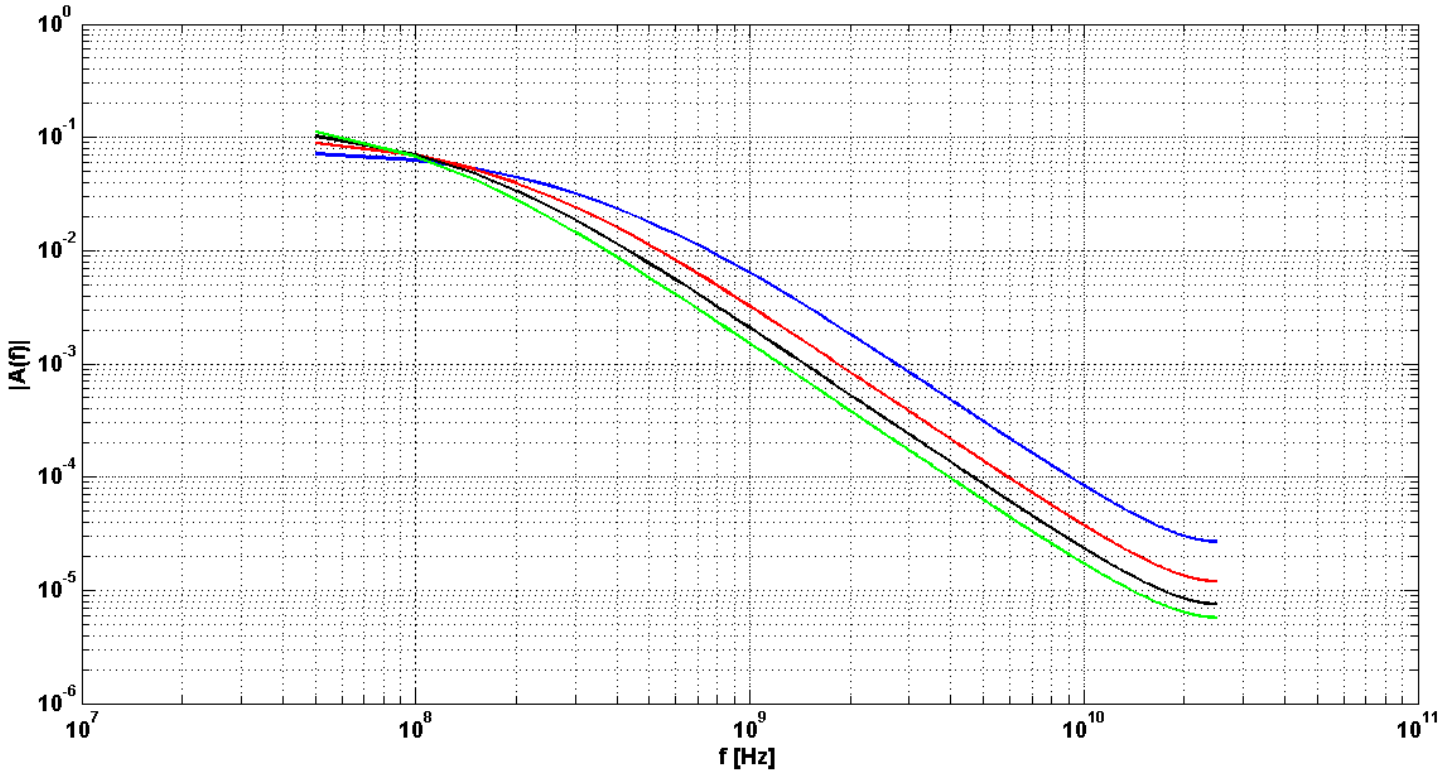


Figure 8 - UWB in frequency domain (Numerical FFT)

2.3. Model of damped sinusoidal waveform

The time and frequency domain equations for the damped sinusoidal waveform are given by:

$$a(t) = A_0 \cdot e^{-\alpha \cdot t} \cdot \sin(\omega_0 \cdot t) \cdot u(t) \quad \textbf{(eq.6)}$$

$$A(f) = \frac{A_0 \cdot \omega_0}{-\omega^2 + 2j\omega\alpha + \omega_0^2 + \alpha^2} \quad \text{(eq.7)}$$

where A_0 is the peak value, $\omega = 2\pi f$, $\omega_0 = 2\pi f_0$, f_0 is the center frequency and α is the damping factor of the oscillation. The term *u(t)* (the so called Heaviside step function) is to ensure $a(t) = 0 \ \forall t < 0$.

$$\alpha = \frac{1}{\tau}$$

In Figure 9 the waveform described in (eq.6) is shown ($A_0 = 1$ for normalization of amplitude).

In Figure 10 the damped signal in frequency domain (calculated through the FFT of the time domain signal in Figure 9) is shown.

The damping factor depends on the IEMI device itself, the antenna system and cabling, but we may assume that it may fall within this range:

$$\tau = 1 \div 10 \ ns$$

Please note that, in order to simplify the discussion about the model, the parameters A_0 and f_0 are convenient values chosen to show the model results. For the amplitude value A_0, it is difficult to provide a range of real values, because such values depend on the device characteristics, the distance between the attacking and victim system, the coupling to the victim system, and so on. Therefore, for an analysis of a real case, a more extended investigation must be done, but this goes beyond the purpose of this document.

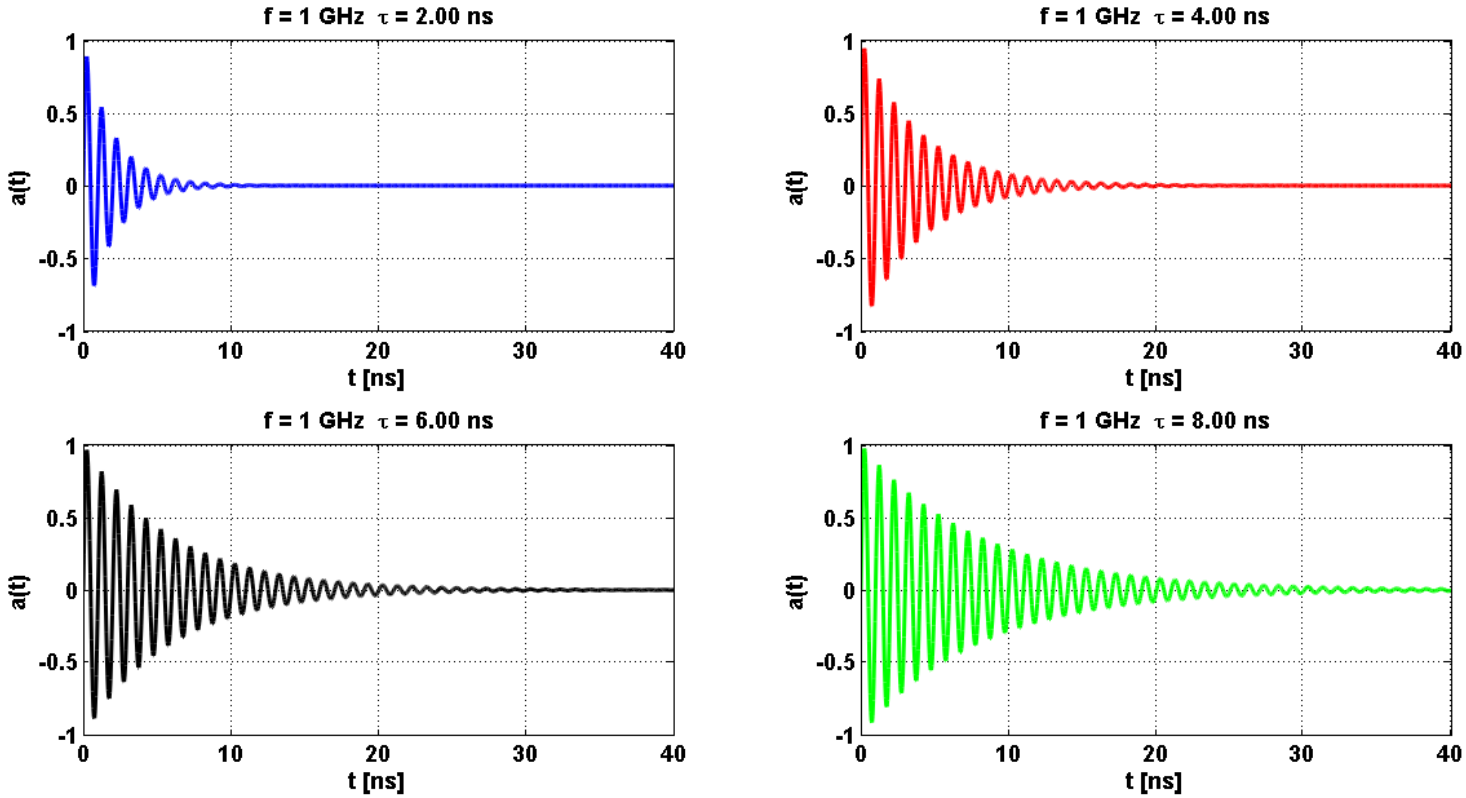


Figure 9 - Damped sinusoidal signal in time domain

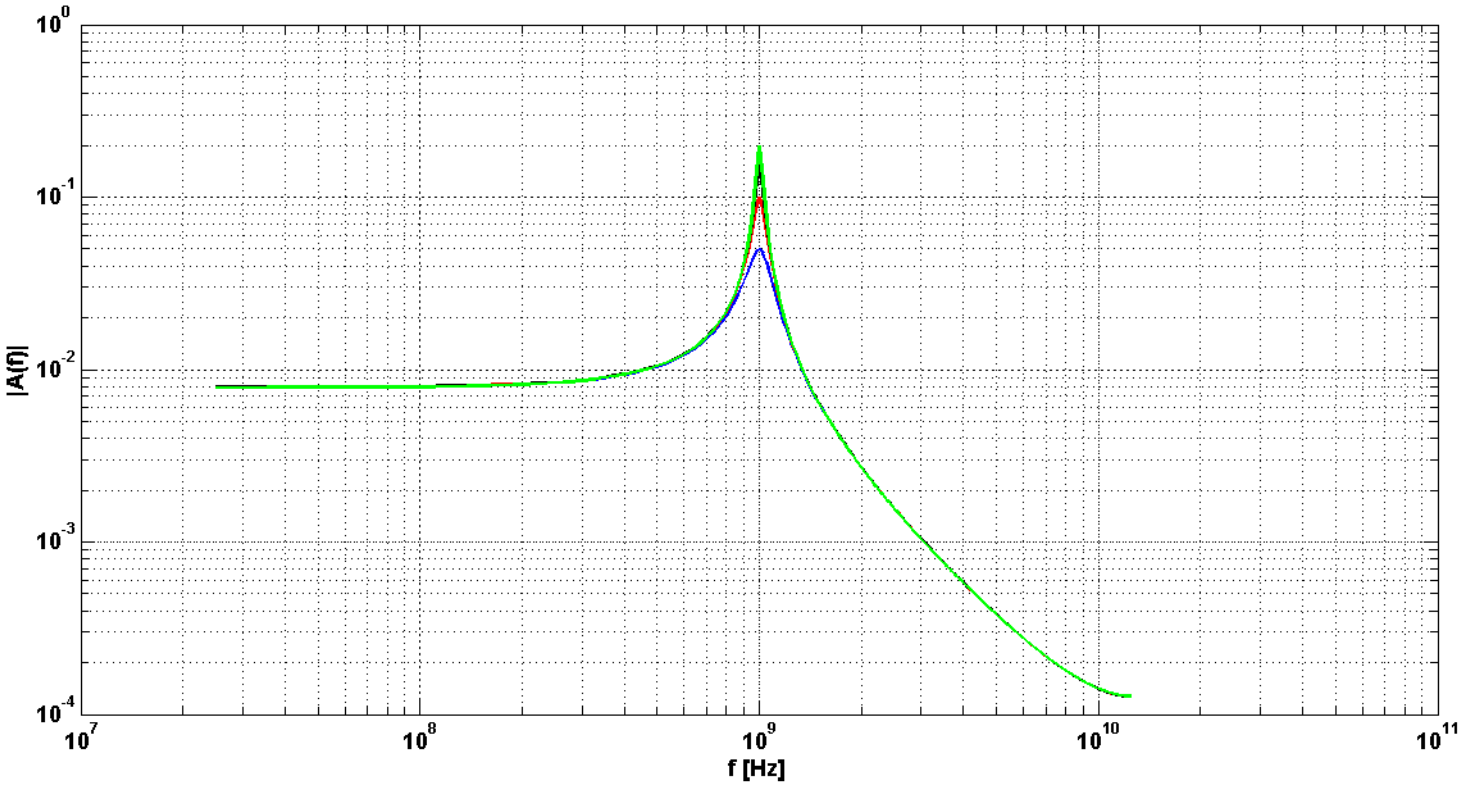


Figure 10 - Damped sinusoidal signal in frequency domain (Numerical FFT)

Table 1 : Main parameters by type of signal

	Signal Type	Parameters	Typical values
Narrow-band	Sinusoidal	Amplitude (A_0) Frequency (f_0)	Normalized Any, from ELF to SHF
	Frequency modulation	Amplitude (A_c) Carrier frequency (f_c) Modulation index (m)	Normalized Any, from HF to SHF 0 to 20
	Amplitude modulation	Amplitude (A_c) Carrier frequency (f_c) Modulation index (m)	Normalized Any, from HF to SHF 0 to 100 %
Wide-band	Double exponential	Peak value (A_0) Rise time ($tr = 1/\beta$)	Normalized $\lesssim$ Ins
	Damped sinusoid	Peak value (A_0) Damping time constant (τ) Center frequency (f_c)	Normalized $\gtrsim$ Ins Any, from HF to SHF

Note : modulation indexes quoted are “standard“ values that can be exceeded.

3. Conclusions

IEMI signals can be grouped under four major cases, but IEMI devices are neither produced according to standards, nor their waveforms are guaranteed.
Analog or digital communications can be disturbed by any in-band Radio frequency signal of greater or comparable amplitude to the incoming signal. Strong out-of-band signals can also disturb.
In principle, any electromagnetic radiation that does not comply with the format expected by the receiver has to be considered an interferer.