Near-Field Measurements for Safety Related Systems and Jamming Attack

Simone Soderi[1, 2, *], Mario Papini[1], Jari Iinatti[2], and Matti Hämäläinen[2]

Abstract—Nowadays new safety related systems design includes electromagnetic analysis (EMA) during their development. Each of these systems is composed by smaller apparatuses that contain electronic components able to emit electromagnetic (EM) waves. On the other hand, the usage of smaller integrated circuit increases their susceptibility to EM interference. Companies often underestimate the importance of emissions lower than standard limits. A method based on near-field (NF) to far-field (FF) transformation is introduced in order to evaluate radiated emission leakage. This study is an important novelty to analyze electromagnetic issues in the case of safety related systems. Moreover, authors present how this method is positioned to current standards. Effectively, NF-FF is proposed for site survey analysis on assembled systems where EM leakages should be mitigated to avoid EM attacks. Tools and measurements presented here can be used to sketch the virtual EM (VEM) interface of device-under-test (DUT) in terms of emissions amplitude, frequency and direction. An opponent could use this information to jam these systems utilizing an attack model based on a circular antenna presented here. The results indicate that it is feasible to use this methodology to analyze EM radiated emissions starting from NF information. Compared with current immunity test levels, the EM attack planned on VEM interface characteristics can be deemed efficiently against safety related systems.

1. INTRODUCTION

One of the main goals of European Union (EU) is to guarantee the free movement of material (e.g., electronic devices) among the Member States. This principle is implemented removing barriers between States and defining specific normative and regulations. Products sold inside the European market must meet essential requirements. Important requirements related to citizen safety and security are stated by European directives. *Safety related* systems are identified as devices, consisting of hardware and software, able to prevent dangerous state by taking appropriate action, i.e., safety function, on detection of a condition which may lead to a hazardous event [1].

With a *directive* the EU makes a legislative act requiring Member States to achieve a particular result without specifying the implementation instructions. In the field of Electromagnetic Compatibility (EMC) and Electromagnetic Immunity (EMI), EU issued the Directive 2004/108/EC [2]. Under this document there are harmonized standards for EMC in different markets, e.g., information technology (IT), industrial, medical and railway. EMC directive and related standards have the declared intention to avoid technical barriers in trade between different countries [3]. On the other hand, these standards do not address specific rules on EM hazards that could occur on safety related systems [4]. EMC requirements refer to immunity and radiated aspects. Each apparatus should be built in order to avoid unintentional emissions over the predefined limits. Moreover, the final product should be immune to both intentional and unintentional electromagnetic (EM) disturbances. Depending on the application, EMC Directive refers to different standards and rules for electronic board design. In most cases, applying these rules to single board design dose not guarantee the compliance with the EM emissions levels.

Received 11 February 2015, Accepted 15 April 2015, Scheduled 21 April 2015

[*] Corresponding author: Simone Soderi (soderi@ieee.org).

[1] GE Transportation Systems, Florence, Italy. [2] Centre for Wireless Communications, University of Oulu, Oulu, Finland.

Typically, the uncertainty is due to the assembly of these boards when building the final product. Furthermore, safety performance could be reduced through EMI.

The European Committee for Electrotechnical Standardization (CENELEC) together with the European Telecommunications Standard Institute (ETSI) is responsible for European standards in the electrical engineering area. The European Committee for Electrotechnical Standardization (CENELEC) produces normative in order to define radiated emissions limits for each application, e.g., CENELEC EN 55011 [5] presents radiated emission limits at a measuring distance of 10 m that varying as reported in Table 1.

Table 1. Radiated emission limits at 10 m.

Frequency range [MHz]	Quasi-Peak Value Limits [dBμV/m]
30 to 230	40
230 to 1000	47

With reference to EMC Directive, tests can be split up into two categories, *full-compliance* and *pre-compliance* tests [6].

- *Full-compliance tests* are performed in accordance with requirements of the standard, harmonized normative and international directive. These tests shall adhere specific methods, limits and test setup;
- *Pre-compliance tests* usually implement full-compliance methods and limits but with some compromise solution on the test setup and instruments. This reduces costs and testing time.

Normally pre-compliance tests are performed prior to formal testing. These tests reduce the risk of failing certification because after a first screening they can focus on the device-under-test (DUT) area that may cause problems. Moreover, using cheaper instruments and faster methods, pre-compliance tests are attractive during product design.

Compared with a full-compliance tests procedure applied to the Notified Body (NoBo) laboratory, the low cost method utilized to define the virtual EM (VEM) interface of DUT [7] is expanded here with the evaluation of real railway system and a jamming attack model. This approach is based on the evaluation of the far-field (FF) pattern measuring the near-field (NF) amplitude. Finally, the outcomes achieved are suggested as the best practice with safety related systems in order to increase the radiated immunity test confidence.

The remainder of the paper is organized as follows. Section 2 introduces the motivations and security aspects. Section 3 formulates the problem and the proposed method. Furthermore, in Section 4 exploiting VEM weaknesses an EM attack is presented. Section 5 continues with the measurement scenario and results from the measurement campaign. Finally, the conclusions are presented in Section 6.

2. BACKGROUND AND MOTIVATION

2.1. Our Contribution

The EMC Directive requires product conformity to essential requirements. The EMC assessment can be carried out in one of the following methods: *detailed technical EMC assessment*, *use of EMC harmonized standards* and *mixed EMC assessment*. The manufacturer is fully responsible for applying the appropriate method and does not have any legal obligation to engage any external laboratory to produce the assessment. The proposed evaluation method measuring the NF is a mixed methodology with a low cost measurement setup.

Studies in literature describe, in detail, EM simulators (e.g., CST [8], ANSYS HFSS [9] and COMSOL RF module [10]) as useful tools during EM design. Some of these software packages include EMC analysis. On the other hand, the difference between EM and EMC models should be clarified. The first considers only interactions between structures and EM fields. The latter also considers functional performance. The increasing system complexity leads to more and more elaborate EM and EMC models where specific skills are required, and quite often the finalization of the numerical results remain difficult in practice [11].

The authors propose a new methodology, as depicted in Figure 1, to measure and evaluate radiated emissions that characterize the VEM interface of assembled safety related systems. The main goal is to highlight possible emission issues of VEM interface. VEM extends classic system's software and hardware interfaces depicting the EM DUT's behavior. An attacker could exploit EM leakage even if these emissions are lower than radiated limits defined by the standard. Nowadays complex safety related systems, such as automotive or railway equipment, are composed by several bricks each of these with its compliance report. From the EM point of view, the system scenario and its VEM interface change when installing additional third party devices. The proposed method could be used in post-installation emissions site surveys.

Finally, when a radiated emission has been described in terms of amplitude, frequency and direction authors present a jamming attack. Utilizing VEM interface characteristics achieved during analysis phase, the attack can improve its effectiveness. To the best of our knowledge, there is no existing solution that incorporates NF to FF transformation into emissions analysis proposing also a system's availability attack based on electromagnetic issues detected.

2.2. Field Regions for the DUT

The EM field generated by a DUT, with maximum dimension D, can be divided by three regions with a gradual transition between those as shown in Figure 2. The reactive NF region is the area closer than

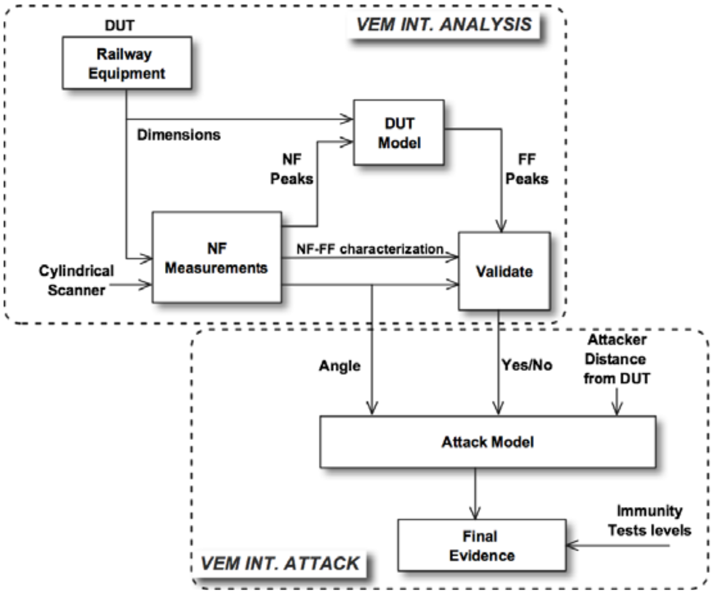

Figure 1. Block diagram of the proposed approach to analyze and attack the VEM interface.

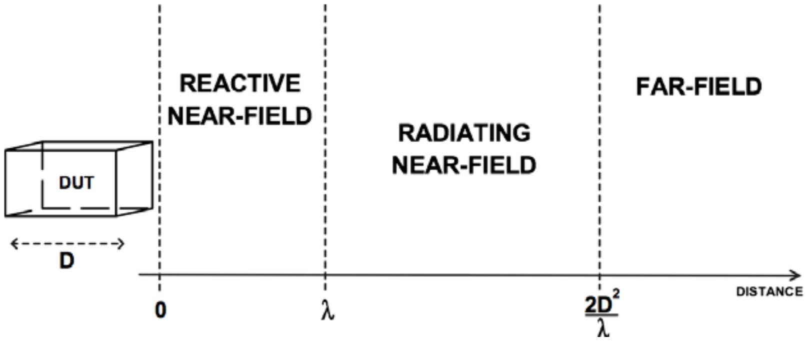

Figure 2. DUT field regions.

one wavelength (λ) to DUT from any radiating surface. The radiating NF region (or Fresnel region) extends from the reactive NF region up to $\frac{2D^2}{\lambda}$. In this area, reactive fields are negligible, but on the other hand energy fluctuations are predominant. Beyond $\frac{2D^2}{\lambda}$ is the FF region (or Fraunhofer region) where the DUT is a source point, and the power level decays according to the inverse square law with distance. NF region definition verifies at least one of the following conditions: $r < \lambda$ or $r < \frac{2D^2}{\lambda}$ [12].

2.3. Radiated Emissions and Security

Measurements of radiated emanations, even if lower than standard's limits, can address interesting investigations in terms of security. Nowadays radiated emissions can be considered as an additional virtual EM interface. An opponent could exploit EM leakage intercepting information carried by EM emanations [13]. Electronic devices emit different EM waves due to current flows within microprocessors, input-output devices and other parts. VEM interface analysis, shown in Figure 1, measures radiated emissions in order to highlight weaknesses.

From EMC point of view, there are two types of EM emissions [14]:

- *Differential mode* radiations generated by small loops, components or printed circuit traces that act as small antennas;
- *Common mode* radiations are the result of undesired voltage difference between two points of the circuits connected to the ground. Any external cable connected to ground acts as antenna.

From an attacker's point of view, EM emanations could be split into two categories [15]:

- *Direct emanations*: these come from active circuits where there are intentional current flows, e.g., short burst of currents;
- *Unintentional emanations*: these are due to high integration of electronic parts, unintentional emanations come from EM coupling of devices in proximity. Typically, these emissions are modulated signals, such as amplitude, frequency or phase modulation.

Security services included in safety related systems are: authentication, confidentiality, integrity and availability. Any attack against availability is classified as a denial-of-service (DoS) where the adversary jams an entire frequency band. The second step shown in Figure 1, i.e., VEM interface attack, describes a jamming model and how it could improve its effectiveness avoiding field strength's rapid fluctuations.

Systematic investigation of these radiated emissions allows an easier exploitation of unintentional emanations because modulated carriers have a better propagation [15]. On the other hand, the probe used to measure the emanation is not able to discern two or more sources. EM field sensors are divided in two categories [16]: *sniffers* and *far-field EM antennas*. The first is the probes to measure near electric and magnetic fields separately. On the other hand, typical examples of the latter are biconical (lower frequencies) and log-periodic (higher frequencies) antennas.

An attacker could exploit EM leakage using a sniffer for NF EM emissions and biconical antenna for FF. Unfortunately EMC requirements defined by current standards do not include EM attack details and their countermeasures. The contribution given in this paper proposes a methodology in order to evaluate EM emissions lower than limits prescribed by standards. These emanations could emphasize emission issues at a given frequency. VEM weaknesses could be exploited by an opponent with intentional interferences.

2.4. Traditional Immunity in Safety Related Applications

Public transportation systems require high level of safety with complex development and testing processes. Specific standards have to be applied to the design of safe systems. The IEC 61508 [1] requires hazards and risks analysis in order to reduce or mitigate issues making the residual risk acceptable. This standard defines four ranks of Safety Integrity Levels (SIL). Each level states the amount of risk reduction in order to guarantee the degree of reliability of the system.

Actually safety related systems consist of many apparatus. These systems have several functions, and each of them has the associated SIL. IEC 61508 describes functional safety in general, and IEC

61000-1-2 [17] has been written to include EMC requirements during the development of safety related systems. This process states the evaluation of EMI on perfect functioning of safety systems [18]. Nowadays, several good EMI practices have been introduced to mitigate and control EM disturbances during safety systems design and also during their entire life-cycle. Most of these techniques are based on safety engineering concepts, i.e., hazards and risks assessments [19]. On the other hand, military EMC applications suggest the usage of a safety margin on the top of immunity level. IEC 61000-6-7 [20] has recently issued new immunity requirements for safety related systems in final draft. In the case that the EM environment is not known, e.g., when a jamming attack occurs, this standard could be used. Basically a safety margin of 6 dB is applied to safety related application such as railway [18, 20]. This margin increases by a factor of 2 when the immunity level is measured in V/m.

The proposed jamming attack model, depicted in Section 4, shows why testing safety related systems with a margin of 6 dB cannot be rated as a robust defense against intentional interferences.

3. DEVICE MODEL AND PROBLEM FORMULATION

The DUT considered here is a rack-mount railway system, sketched as a cube-shaped box in Figure 3. Typically, these systems have metallic flat surfaces and present hardware interfaces, such as cables or connectors, only to the front or rear facing. With this set-up, the DUT model was approximated with only one active surface at the time. In other words, we are interested in the radiated field generated by electric and magnetic currents on that surface-under-test (SUT). This model was validated with the experiment presented in Section 5, where a measurement campaign was carried out using real railway equipment.

The Source Reconstruction Method (SRM) is an integral-equation based method developed for antenna design [21–23]. It is based on the equivalence principle by which actual electric and magnetic sources (i.e., $\overrightarrow{J_1}$, $\overrightarrow{M_1}$) of DUT are replaced by their equivalent sources (i.e., electrical current density $\overrightarrow{J_{eq}}$ and magnetic current density $\overrightarrow{M_{eq}}$) depicted in Figure 3. These current densities are distributed on an imaginary surface (S^1) that encloses the original source to generate the same radiated EM fields into an unbounded space [12]. Both electric and magnetic currents represent the equivalent problem in terms of FF starting from the known radiated NF.

The value of the amplitude of the NF is measured with special probes named *sniffers*. The numerical values of the radiated NF can be calculated by [24]

$$\mathbf{H}(\mathbf{r}) = \frac{jk}{4\pi}(\mathbf{m} \times \mathbf{r})C\mathrm{e}^{-jkr}, \tag{1}$$

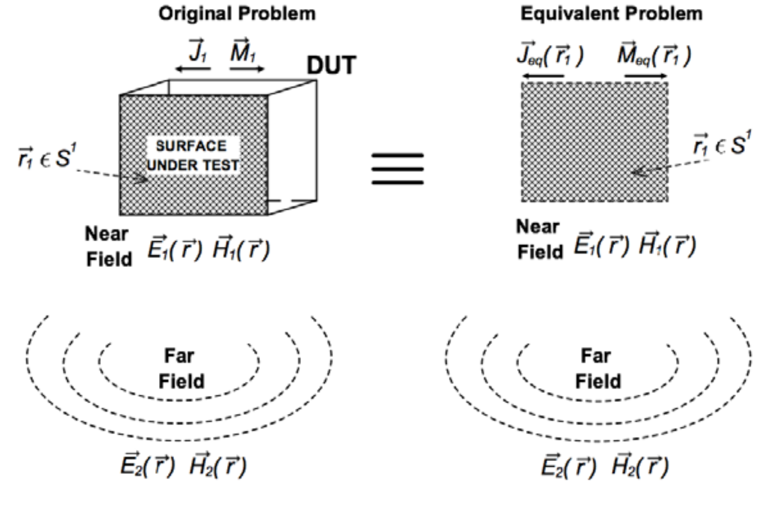
Original Problem
$\vec{J_1}$ $\vec{M_1}$
DUT
SURFACE UNDER TEST
$\vec{r_1} \in S^1$
Near Field $\vec{E_1}(\vec{r})$ $\vec{H_1}(\vec{r})$
Far Field
$\vec{E_2}(\vec{r})$ $\vec{H_2}(\vec{r})$
≡
Equivalent Problem
$\vec{J_{eq}}(\vec{r_1})$ $\vec{M_{eq}}(\vec{r_1})$
$\vec{r_1} \in S^1$
Near Field $\vec{E_1}(\vec{r})$ $\vec{H_1}(\vec{r})$
Far Field
$\vec{E_2}(\vec{r})$ $\vec{H_2}(\vec{r})$

Figure 3. Equivalent problem.

$$\begin{aligned}\mathbf{E}(\mathbf{r}) &= \frac{\eta}{4\pi}\left((\mathbf{M}-\mathbf{m})\left[\frac{jk}{r}+C\right]+2\mathbf{M}C\right)\mathrm{e}^{-jkr},\\ C &= \frac{1}{r^2}\left[1+\frac{1}{jkr}\right], \quad \mathbf{M}=\frac{(\mathbf{r}\cdot\mathbf{m})\,\mathbf{r}}{r^2}\end{aligned} \tag{2}$$

where $r = |\mathbf{r}|$ is the module of observation point $\mathbf{r} = \{x \cdot \mathbf{i_x}, y \cdot \mathbf{i_y}, z \cdot \mathbf{i_z}\}$, $\eta = \sqrt{\frac{\mu}{\epsilon}} = 377\,\Omega$, ϵ the electric permittivity, μ is the magnetic permeability, and $\mathbf{m}$ the dipole moment and $k = \frac{2\pi}{\lambda}$. Knowing the NF measured in N points, this paper proposes a mathematical optimization in order to find the equivalent electric and magnetic currents that best fit the amplitudes of NF values.

3.1. Equivalent Current Representation

In accordance with the equivalent theorem the field radiation by electronic devices can be reproduced from a SUT (i.e., S^1) distribution of electric and magnetic equivalent currents [21].

To solve (1) and (2) the Method of Moments (MoM) is used [24]. MoM is based on Rao-Wilton-Glisson (RWG) edge elements where the surface currents are represented via the so called *dipole model* in Figure 4 [24]. The metallic SUT (S^1), depicted in Figure 3, can be divided into small triangles. Each pair of these triangles creates a dipole ($\mathbf{m}$). In this way, the DUT NF and FF can be expressed as the overall contribution of elementary dipoles shown in Figure 4. In the NF, electric field $\vec{E}$ and magnetic field $\vec{H}$ are independent and can be calculated separately using (1) and (2).

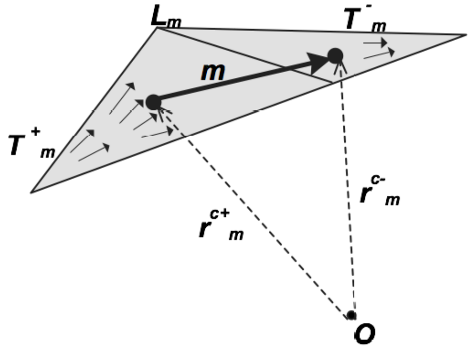

Figure 4. Dipole model interpretation.

On the other hand, at large distances (i.e., FF) from the source, field fronts can be approximated as planar waves. In that point $\vec{E}$ is perpendicular to $\vec{H}$ and both to the direction of propagation [12].

3.2. Proposed Method

The proposed method implements the flowchart represented in Figure 5, and it is a modified version of the SRM. First, the $\vec{E}$ and $\vec{H}$ near-fields' amplitudes are measured with sniffers in both polarizations, i.e., vertical and horizontal. During the cylindrical scan the error due to truncating measurement area was left out because it was compensated extending the cylindrical surface along the y axis. The approximation is acceptable because this methodology provides a rough estimation of the radiated emissions. The number of samples on the extended observation surface that encloses the sources is [25]

$$N \cong \frac{A_\Sigma}{\left(\dfrac{\lambda}{2}\right)^2}, \tag{3}$$

where $A_\Sigma = 2\pi Rh$ is the cylindrical observation curve depicted in the measurement scenario of Section 5, and R and h are its radius and height, respectively. In accordance with the Nyquist sampling rate in

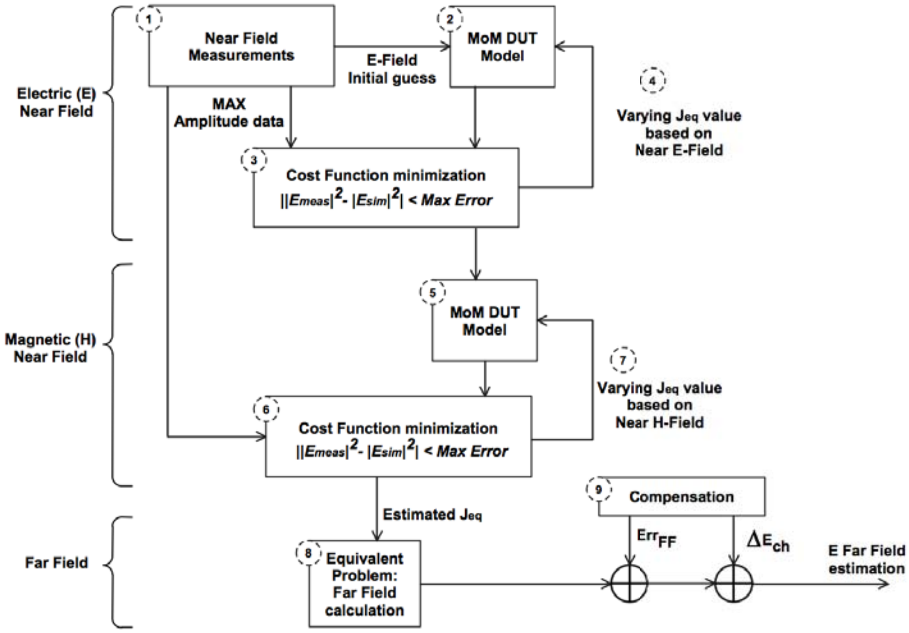
1
Near Field Measurements
E-Field Initial guess
2
MoM DUT Model
Electric (E) Near Field
MAX Amplitude data
4
Varying Jeq value based on Near E-Field
3
Cost Function minimization
||Emeas|2- |Esim|2| < Max Error
5
MoM DUT Model
Magnetic (H) Near Field
7
Varying Jeq value based on Near H-Field
6
Cost Function minimization
||Emeas|2- |Esim|2| < Max Error
9
Compensation
Estimated Jeq
ErrFF
ΔEch
E Far Field estimation
Far Field
8
Equivalent Problem: Far Field calculation

Figure 5. Flowchart for the proposed method.

the NF-FF transformation, the NF measurements are typically performed on a discrete surface with the maximum distance less than $\frac{\lambda}{2}$ at the higher frequency (i.e., 1 GHz in our case). The measurement setup considered in this study oversampled the NF. The number of samples N at the higher frequency was calculated for FF distance using (3) and kept the same in NF. Effectively that choice leads to more precise NF measurements.

Electric field amplitude was selected along the direction of DUT maximum radiated emissions. In fact, the method is not for radiation diagram reconstruction but for radiated emissions detection and analysis. After a complete cylindrical NF scan the direction of maximum E-field emissions is selected. This value could be along vertical or horizontal polarization, and from this time forward, any further calculation is made along this direction.

E_{meas}^{NF} is used to minimize the difference against the E-field simulated (i.e., E_{sim}^{NF}) in NF via MoM varying the electrical surface currents as depicted in Figure 5. The proposed cost function is

$$\left|\left|E_{meas}^{NF}\right|^2 - \left|E_{sim}^{NF}\right|^2\right| < Err_{NF}, \tag{4}$$

where Err_{NF} is the maximum error in NF, and E_{meas}^{NF} and E_{sim}^{NF} represent RMS values. Eq. (4) does not need any information about the phase [22, 26]. Collecting independent amplitude data, the left side of (4) can be minimized achieving the estimation of the electric field. The minimization of (4) utilizes standard algorithm [27] that requires a starting value. The data measured in NF are used as an initial starting point. In order to avoid local minimum error in (4), the initial measured starting value is modified and the process repeated [28].

Assuming that in the NF $\vec{E}$ and $\vec{H}$ are independent, a second block of iterations refines the previous near E-field estimation using near H-field independently measured with a magnetic sniffer. The process ends for NF when the maximum error constraint is verified.

Then, from the $\overrightarrow{J_{eq}}$, estimated using NF information and SUT equivalent model, the FF $\vec{E}$ estimation, i.e., $\tilde{E}^{FF}$, is given by

$$\left|\tilde{E}^{FF}\right| = \left|E_{sim}^{FF}\right| + Err_{FF} + \Delta E_{ch}, \tag{5}$$

where E_{sim}^{FF} represents the simulated E-field, and it is compensated with the sniffer characterization against biconical antenna, i.e., ΔE_{ch}, and with a maximum acceptable error in FF, i.e., Err_{FF}.

ΔE_{ch} describes the difference in decibels between biconical antenna and E-field sniffer based on 0 dBm signal transmitted. The characterization is done for each polarization before getting measurements, and it depends on the sniffers and antenna utilized.

Err_{FF} is the overall error in FF and can be specified, e.g., < 2 dB. Otherwise, it can be calculated following an iterative process where the simulated FF is compared with the one measured with the biconical antenna, and it is given by

$$|\Delta E_{ms} - \Delta E_{ch}| < Err_{FF}, \tag{6}$$

where ΔE_{ms} is the difference in decibels between E^{FF}_{meas} and E^{FF}_{sim} in FF, and ΔE_{ch} is the sniffer characterization.

A limitation of the proposed method could happen when spectrum analyzer (SA) receives an interference signal during NF measurements with sniffers. The SA used for EMI/EMC tests is a calibrated and flexible super-receiver. It measures the power of a given input signal in the frequency domain. In the case of multiple uncorrelated input signals, SA measures the power of each received signal. In the worst case, this interference overlaps the frequencies under investigation (e.g., 30–1000 MHz). In other words, the unwanted interference signal sets the environmental noise floor. In order to keep the measured NF valid in the frequency under investigation, the measured power in NF shall verify the condition

$$P_{Int} < P_{NF}, \tag{7}$$

where P_{Int} and P_{NF} are the powers of measured interference and NF signals, respectively. On the other hand, this limitation defines the additional lower radiated emissions criteria as shown in Figure 6.

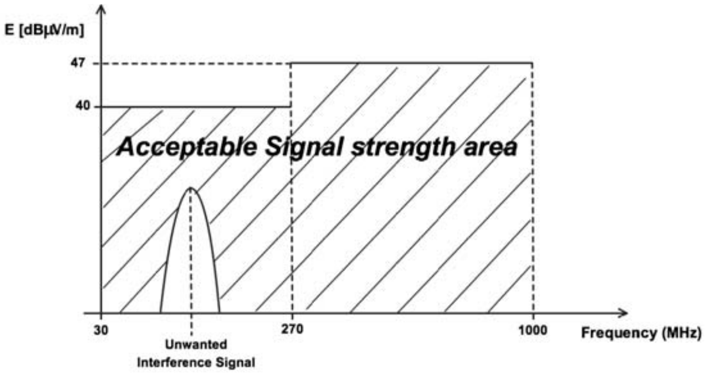

Figure 6. Additional lower radiated emission limits in presence of interference.

4. JAMMING ATTACK MODEL

The jamming attack model is represented in Figure 7, and this section describes how to increase its effectiveness. The adversary's primary goal is to produce a DoS attack utilizing a directional antenna. It is assumed that the attacker knows the direction of maximum emissions. Radiated emissions can be captured with sniffers and antennas around the DUT (i.e., victim device) as previously described in Section 3.

The Fresnel and regions boundaries are defined by the Rayleigh-Sommerfeld diffraction formula [29]

$$\mathbf{E}(\mathbf{r}) = 2\oint_{S'} \mathbf{E}\left(\mathbf{r}'\right)\cos\theta\left(jk + \frac{1}{r}\right)\frac{\mathrm{e}^{-jkr}}{4\pi r}dS', \tag{8}$$

where $\mathbf{E}(\mathbf{r})$ is the electric field in the observation point $\mathbf{r} = \{x\cdot\mathbf{i_x}, y\cdot\mathbf{i_y}, z\cdot\mathbf{i_z}\}$, $\mathbf{r}' = \{x'\cdot\mathbf{i_x}, y'\cdot\mathbf{i_y}, z'\cdot\mathbf{i_z}\}$ the sources coordinates, $\mathbf{E}(\mathbf{r}')$ the field over the aperture, θ the angle between the symmetric axis and $\mathbf{r}$, and r the distance of the observation point. In the case of circular aperture with uniform plane wave illumination and using the Fresnel approximation, the field intensity along the symmetric axis is [30]

$$|\mathbf{E}(0,0,z)| = 2E_0\sin\left(\frac{ka^2}{4z}\right), \tag{9}$$

where z is the distance from the circular antenna having a radius a and E_0 a constant.

The time average Poynting vector (average power density) is given by

$$\mathbf{S}(\mathbf{r}) = \frac{1}{2}\Re\left[\mathbf{E} \times \mathbf{H}^*\right] = \frac{1}{2\eta}|\mathbf{E}|^2 = \frac{1}{\eta}|\mathbf{E}_{rms}|^2, \tag{10}$$

where $\mathbf{S}(\mathbf{r})$ is expressed in $\frac{W}{m^2}$, $\eta = \sqrt{\frac{\mu}{\epsilon}}$; $\mathbf{E}$ and $\mathbf{H}$ represent the peak values; $\mathbf{E}_{rms}$ is the RMS value [12].

On the other hand, in the case of circular aperture antenna, (10) can be written as

$$\mathbf{S}(\mathbf{r}) = \mathbf{S_0} 4 \sin^2\left(\frac{A}{2\lambda r}\right), \tag{11}$$

where $\mathbf{S_0} = \frac{P_{tx}}{A}$ is the average power density provided by the circular antenna, and A is its area. Getting closer to the circular antenna the field strength's rapid fluctuations should be considered as shown in Figure 8. $\mathbf{S}(\mathbf{r})$ is maximum over the distance when

$$\sin^2\left(\frac{A}{2\lambda r}\right) = 1. \tag{12}$$

Due to field strength's fluctuations, it can also be demonstrated that the distance from DUT which causes the maximum error between the normalized version of $\mathbf{S}(\mathbf{r})$, i.e., $\frac{\mathbf{S}(\mathbf{r})}{\mathbf{S_0}}$, and far-field trend, i.e., $\frac{4}{(\frac{\lambda r}{A})^2}$, is

$$r = \frac{\pi}{8}\frac{D^2}{\lambda}, \tag{13}$$

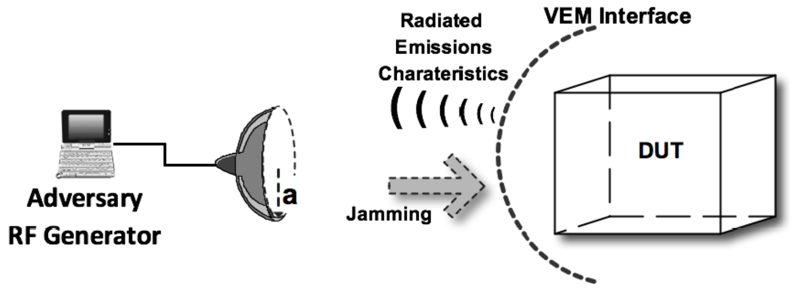

Figure 7. Jamming attack with circular aperture antenna.

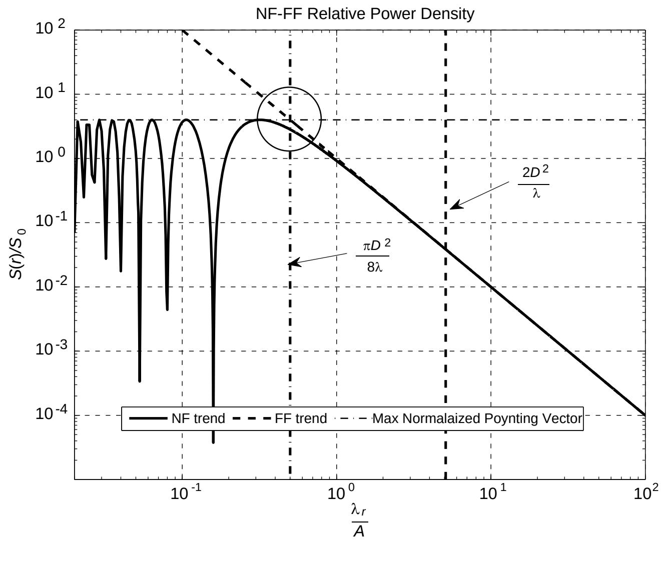

Figure 8. Average DUT power density.

where $D = 2a$ is the circular aperture diameter.

Comparing the lower limit of the FF region, i.e., $r < \frac{2D^2}{\lambda}$, with [13], the attacker can be moved five times closer to the DUT and he still goes on with his antenna in FF. Figure 8 shows the average of DUT power density trend against two distance conditions. In this scenario, a jamming attack at the distance indicated with (13) increases in 13 dB its power (see Appendix A). In other words, this power rising is equivalent to increasing the electric field, measured in V/m, by a factor of 4.5, and it is significantly higher than the level tested with safety margin proposed in IEC 61000-6-7.

5. MEASUREMENTS SCENARIO AND EXPERIMENTAL RESULTS

Using a rotary table and a Y-probe positioner (Figure 9 shows the reference system), a computer acquired only NF and FF amplitude data via a SA at closer and larger distances, respectively. NF was measured with sniffers, instead FF was acquired utilizing a biconical antenna. The SA is a frequency selective voltmeter that displays root mean square (RMS) value of a sine wave scaling its readout by 0.707 (-3 dB). As a result, the notation used throughout this paper refers to RMS values. As laid down

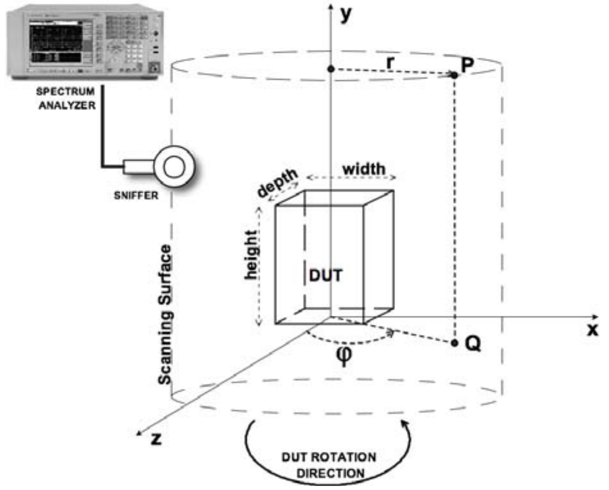

Figure 9. NF measurements on a cylindrical surface.

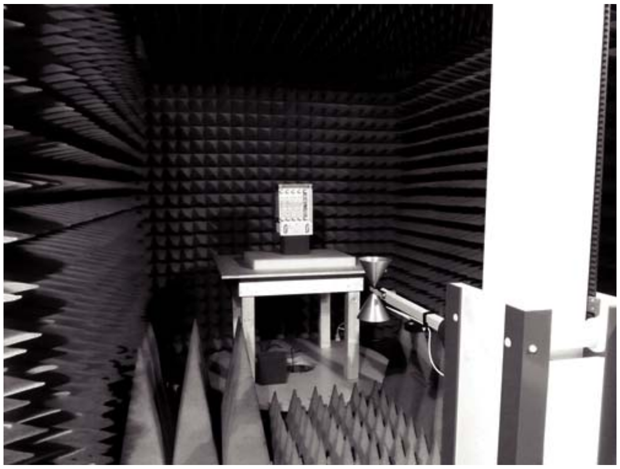

Figure 10. Fully automated measurement setup in semi-anechoic chamber.

Table 2. Measurements scenario parameters.

Parameter	Value
DUT Dimensions $L \times W \times H$ [cm]	$20 \times 20 \times 20$
Frequency range	80 MHz $\div$ 1 GHz
Spectrum analyzer resolution bandwidth	120 kHz[1]
Number of samples (N) at Nyquist rate	196[2]
Near Field max distance from DUT	30 cm
Sniffer Type	E, H field
Far-field antenna type	Biconical
Max dimension of Biconical antenna	20 cm
Distance from DUT	30[3], 140[4] cm
Scanner type	cylindrical
Vertical scan height	50 cm

[1] Defined for EMI/EMC compliance tests in EN55011.
[2] Same N for NF and FF.
[3] Near-field.
[4] Far-field.

in CISPR 16-1-1 [31], the SA utilized has three different detectors for RF emissions measurements: *peak*, *quasi-peak* and *average*. The proposed method utilizes the peak detector. It instantaneously measures the peak value of the signal. This detector is very fast and suitable for the cylindrical scan implemented during the VEM interface qualifying measurements. On the other hand, it could overestimate the levels of pulsed or modulated signals. In order to mitigate this disadvantage, the SA was set to use maximum hold up to 3 seconds for each measurements.

A measurement campaign was carried out inside a semi-anechoic chamber to verify the proposed method. Measurements started with the sniffer characterization wherein its data were compared against biconical antenna's ones. This difference was measured transmitting a 0 dBm reference signal in the frequency range reported in Table 2. The setup utilized the tracking generator included in the Agilent N9342C spectrum analyzer. Both polarizations were tested (i.e., vertical and horizontal) at the same distance. The characterization was needed to measure the gap in decibels between probes in NF and biconical antenna in FF with a 0 dBm known signal.

Afterwards, the measurements were divided into main groups, first with sniffers (electric and magnetic) in NF region and afterwards with biconical antenna in FF. Table 2 presents the parameters used in this experiment. The measurement setup included a signal generator (Agilent E8267D PSG) connected to an omnidirectional dipole (Seibersdorf POD 16), whereas the receiver was composed by a spectrum analyzer (Agilent PXA N9030) connected either to the NF probes (Aaronia PBS2) or to the biconical antenna (Seibersdorf PCD 3100). Measurement setup also included a fully automated cylindrical scanner composed by turn table, mast antenna and dedicated software to acquire field only amplitude data in each point depicted in Figure 10. Furthermore, measurements performed with this scanner were not affected by any tilt phenomena. Finally, the data were post-processed and compared with predicted values achieved by the algorithm described in Section 3.

Table 3. VEM interface characteristics.

Peaks Number	**Frequency [MHz]**	**Antenna**		
		Polarization	**Height [m]**	**Angle [°]**
1st	781	Vertical	1	0
2nd	719			
3rd	680			
4th	800			
Manually Selected	250			

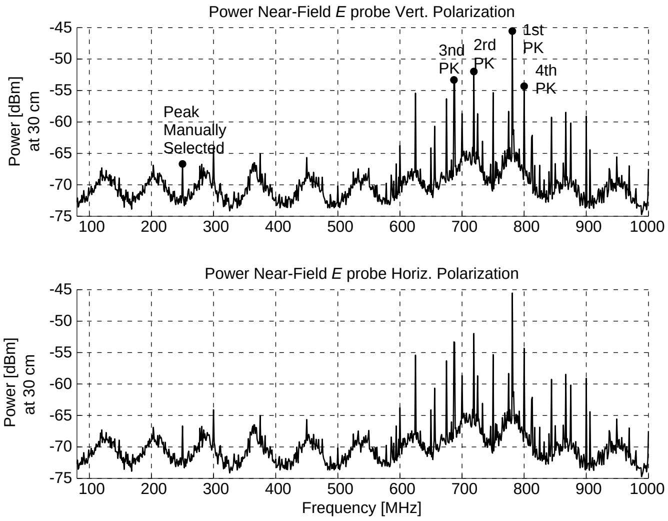

Figure 11. Measured Power in NF with *E*-field probe and peaks selection.

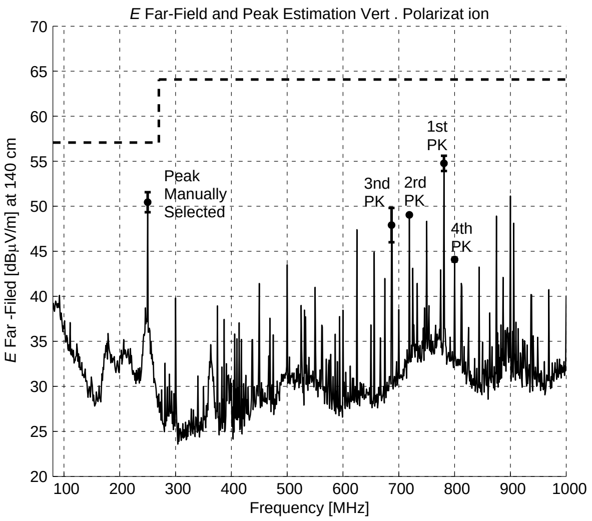

Figure 12. *E* FF peak estimation in vertical polarization.

Table 4. Comparison of predicted and measured $|E|$ in FF.

Number of Triangles	Error [dB]					Average Error [dB]
	1st	2nd	3rd	4th	Manually Selected	
16	0.85	0.1	1.9	0.22	1.11	0.5
32	0.82	0.07	1.9	0.24	0.24	0.33
64	0.84	0.05	1.88	0.21	0.39	0.18

Table 5. Measurements of power attack level.

Frequency [MHz]	Tx Power [dBm]	Distance [m]		Attack power level [dBm]		Power increase [dB]
		R2	R1	Power at R2	Power at R1	
781	0	3.2	0.64	−50.5	−35.2	15.3
2400	0	3.2	0.64	−53	−41.3	11.7
5800	0	3.2	0.64	−66.5	−53.8	12.7

This experiment revealed the maximum NF received power along vertical polarization at 781 MHz as sketched in Figure 11. The simulator was set up to analyze four higher peaks and an additional one manually selected as shown in Figure 11. The algorithm used the NF peak detected information reported in Table 3 minimizing (4) for each peak. When the surface currents distributions that minimize the difference between the $|E_{sim}|$ and $|E_{meas}|$ are achieved, the FF is simulated. Figure 12 shows how the algorithm detects the peaks in FF, and Table 4 reports the average error in decibels for each peak. The direction of the maximum radiated emission measured in Table 3 validated the DUT model with only one active surface because the railway equipment under test had connection on the front facing.

SUT mesh discretization changes do not have any significant impact on the mean error in decibels between the predicted and measured $|E|$ in FF as shown in Table 4. The highest average error was 0.5 dB at 1.4 m in FF region when simulations used a SUT mesh with 16 triangles. The difference decreases only to 0.18 dB using meshes with 64 triangles, but the computational cost significantly increases.

In the end, starting from VEM interface characteristics reported in Table 3, the jamming model proposed in Section 4 was verified. The measurement setup included a signal generator (Agilent E8267D PSG) connected to a rectangular horn antenna (AH Systems), whereas the receiver was composed by a spectrum analyzer (Agilent PXA N9030) connected to the biconical antenna (Seibersdorf PCD 3100). The maximum dimensions for these antennas were 0.24 m and 0.21 m for the horn and biconical, respectively. From a far-field distance of 3.2 m (i.e., R_2) the attacker moved five times close till 0.64 m (i.e., R_1). The transmitted power was always 0 dBm. The results achieved, shown in Table 5, can give only an indication due to the different antennas used for the jamming attack. Unfortunately at the time of the writing, the circular aperture antenna was not available. The measured increment of the jamming attack power is closer to theoretical value at higher frequencies. On the other hand, at lower frequencies such as 781 MHz, the antenna dimensions are comparable with wavelength disturbing the EM field.

6. CONCLUSIONS

This paper discussed the NF to FF transformation as an effective methodology in emissions site survey analysis. Starting from the NF measurements, the proposed algorithm predicts FF at a given distance analyzing peaks along the direction of maximum emissions. In order to increase the performances, the NF probes were characterized against the FF antenna. The behavior of the algorithm was tested in laboratory, but considering the restrictions presented in Section 3.2, expensive semi-anechoic chamber is needed for NF measurements.

The authors proposed an innovative use of NF to FF transformation to highlight possible emission security issues of VEM interface. The methodology analyzed assembled safety related systems and verified results with a measurement campaign carried out using real railway equipment. The algorithm represents also an useful tool during post-installation in order to identify emissions leakage. Characteristics of these emissions, such as frequencies and direction, could be exploited from an opponent to plan a jamming attack. For instance, the evaluation of EM weaknesses could be done on-board train, where the entire system is installed. These measurements would be easier and cheaper than trying to reproduce the scenario in a laboratory. On the other hand, the knowledge of the EM vulnerabilities will drive new processes to improve emission security for safety related apparatus.

Finally, an experiment to verify the proposed jamming model was presented. The model effectiveness was improved utilizing the VEM interface characteristics. It demonstrated how an attacker with limited resources can increase, up to 13 dB, the signal power moving, along the maximum radiated emission direction, five times closer to the victim. The attack can be deemed efficient against safety related systems even if these are tested utilizing a safety margin on the top of radiated immunity levels. On the other hand, the jamming model could be used to test the DUT exploiting the frequencies detected by the algorithm and to improve the system design.

ACKNOWLEDGMENT

The authors would like to acknowledge and thank Prof. Ing. Luigi Millanta for his innovative research as precursor in EMC, electrical and electronic measurements.

APPENDIX A.

When the circular aperture antenna moved closer to the DUT the incident power increase. It can be easily verified that

$$\Delta S = 10\log\left(4\sin^2\left(\frac{A}{2\lambda r}\right)\bigg|_{r1}\right) - 10\log\left(\frac{1}{\left(\frac{\lambda r}{A}\right)^2}\bigg|_{r2}\right) = 12.64 \approx 13\,\text{dB}, \tag{A1}$$

where $r1 = \frac{\pi}{8}\frac{D^2}{\lambda}$, $r2 = \frac{2D^2}{\lambda}$ and ΔS is the power increment in decibels.

REFERENCES

1. "Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC 61508-0, Jan. 2005.
2. Directive 2004/108/EC, Online Available: http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/electromagnetic-compatibility/index_en.htm.
3. Armstrong, K., "Emc and functional safety," *IEE Review*, Vol. 46, No. 6, 34–37, Nov. 2000.
4. Armstrong, K., "New guidance on EMC-related functional safety," *IEEE International Symposium on Electromagnetic Compatibility*, Vol. 2, 774–779, 2001.
5. "CENELEC EN 55011 — Industrial, scientific and medical (ISM) radio-frequency equipment — Electromagnetic disturbance characteristics — Limits and methods of measurement," 2007.
6. Williams, T., *EMC for Product Designers*, 4th Edition, Elsevier, Burlington, MA, 2007.
7. Soderi, S., M. Papini, M. Hamalainen, and J. Iinatti, "NF-FF transformation for emissions and security," *1st IEEE International Conference on Numerical Electromagnetic Modeling and Optimization (NEMO)*, May 2014.
8. Computer Simulation Technology (CST), Online Available: https://www.cst.com.
9. ANSYS HFSS, Online Available: http://www.ansys.com/Products/Simulation+Technology/Electronics/Signal+Integrity/ANSYS+HFSS.
10. COMSOL — RF Module, Online Available: http://www.comsol.com/rf-module.
11. Ruddle, A., "Electromagnetic modelling for emc," *IET 7th International Conference on Computation in Electromagnetics (CEM)*, 170–174, Apr. 2008.

12. Balanis, C. A., *Antenna Theory: Analysis and Design*, Wiley-Interscience, 2005.
13. Anderson, R. J., *Security Engineering — A Guide to Building Dependable Distributed Systems*, 2nd Edition, Wiley, 2008.
14. "Compromising electromagnetic emanations of wired and wireless keyboards," Online Available: https://www.usenix.org/legacy/event/sec09/tech/full_papers/vuagnoux.pdf.
15. Agrawal, D., B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side-channel(s): Attacks and assessment methodologies," Online Available: https://web.cs.jhu.edu/ astubble/600.412/s-c-papers/em.pdf.
16. Li, H., A. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," *Tenth IEEE International High-Level Design Validation and Test Workshop*, 211–218, 2005.
17. "Electromagnetic compatibility (EMC) — Parts 1–2: General — Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena," IEC 61000-1-2, 2010.
18. Ogunsola, A. and A. Mariscotti, *Electromagnetic Compatibility in Railways: Analysis and Management (Lecture Notes in Electrical Engineering)*, Vol. 168, Springer, 2013.
19. Armstrong, K., "EMI and functional safety why traditional immunity testing is inadequate and what should be done instead," *17th International Zurich Symposium on Electromagnetic Compatibility, EMC-Zurich 2006*, 469–472, Feb. 2006.
20. "Electromagnetic compatibility (EMC) — Parts 6–7: Generic standards — Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations," IEC 61000-6-7, 2014.
21. Alvarez, Y., M. Rodríguez, F. Las-Heras, and M. Hernando, "On the use of the source reconstruction method for estimating radiated emi in electronic circuits," *IEEE Transactions on Instrumentation and Measurement*, Vol. 59, No. 12, 3174–3183, 2010.
22. Las-Heras, F. and T. Sarkar, "A direct optimization approach for source reconstruction and NF-FF transformation using amplitude-only data," *IEEE Transactions on Antennas and Propagation*, Vol. 50, No. 4, 500–510, 2002.
23. Sarkar, T., "A super-resolution source reconstruction method using free space green's function," *IEEE International Conference on Wireless Information Technology and Systems (ICWITS)*, 1–4, 2010.
24. Markov, S. N., *Antenna and EM Modeling with MATLAB*, Wiley, 2002.
25. Bucci, O., C. Gennarelli, and C. Savarese, "Representation of electromagnetic fields over arbitrary surfaces by a finite and nonredundant number of samples," *IEEE Transactions on Antennas and Propagation*, Vol. 46, No. 3, 351–359, Mar. 1998.
26. Las-Heras, F. and T. Sarkar, "Planar NF-FF with direct optimization-source reconstruction using amplitude only data," *IEEE Antennas and Propagation Society International Symposium*, Vol. 2, 618–621, 2001.
27. MathWorks — Optimization Toolbox User's Guide, Online Available: http://www.mathworks.com/help/pdf_doc/optim/optim_tb.pdf.
28. Bertocco, M., D. Dainese, and A. Sona, "Evaluation of telecommunication station parameters by means em field measurements," *Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference, IMTC 04*, Vol. 1, 273–277, May 2004.
29. Goodman, J., *Introduction to Fourier Optics*, 2nd Edition, MaGraw-Hill, 1996.
30. Mezouari, S. and A. Harvey, "Validity of Fresnel and Fraunhofer approximations in scalar diffraction," *Journal of Optics A — Pure and Applied Optics*, Vol. 5, No. 4, S86–S91, Jul. 2003.
31. "Specification for radio disturbance and immunity measuring apparatus and methods — Part 1-1: Radio disturbance and immunity measuring apparatus — Measuring apparatus," CISPR 16-1-1, 2010.