HPM DETECTOR SYSTEM WITH FREQUENCY IDENTIFICATION

Ch. Adami[1], Ch. Braun[2], P. Clemens[3], M. Joester[4], M. Suhrke[5], H.U. Schmidt[6], H.J. Taenzer[7]

[1] *christian.adami@int.fraunhofer.de*
[2] *christian.braun@int.fraunhofer.de*
[3] *peter.clemens@int.fraunhofer.de*
[4] *michael.joester@int.fraunhofer.de*
[5] *michael.suhrke@int.fraunhofer.de*
[6] *hans-ulrich.schmidt@int.fraunhofer.de*
[7] *hans-joachim.taenzer@int.fraunhofer.de*

Fraunhofer Institute for Technological Trend Analysis INT, Dept Electromagnetic Effects and Threats, Appelsgarten 2, 53879 Euskirchen (Germany)

Abstract

Warning devices, which simply notify the occurrence of High Power Microwave (HPM) pulses, are not sufficient for HPM threat analysis. Instead, the determination of characteristic parameters like field strength, pulse width, repetition frequency, direction of arrival, and the carrier of the Radio Frequency (RF) allows the analysis and tracking of HPM threat signals (forensics). As part of a comprehensive HPM protection framework it offers both, an alert with some additional information about direction and time for short term fast response, and all RF related information for an attack analysis used for long-term counter measures within a protection concept.

Keywords: HPEM, IEMI, Electromagnetic Threat, RF Sensor, HPM Detection, HPM Protection.

INTRODUCTION

In all areas of our society, information flow, related actions, and reactions are accompanied by complex electronic systems. The risk of malicious disturbance with High Power Electromagnetic (HPEM) rises simultaneously with increasing complexity of these systems.

A possible scenario is the use of HPEM to facilitate criminal or terrorist activities on critical infrastructures, as e. g. airports, data centers, or traffic control centers. The offenders might intent to disrupt or to disable security appliances to enter restricted areas or to hack into computer networks. In particular, an HPEM attack could be used to disable airport security checkpoints, alarm systems, or video surveillance systems, or else to distract guards by repeated false alarms of these systems. Apart from that, temporary or permanent degraded access protection of computer networks by re-booting IT devices could be used by hackers to take over parts of the network.

An HPEM attack is difficult to identify derived from the behavior of the affected electronic devices, especially if it has not been expected. So, the comprehensive detection of HPEM threats can be integrated into a protection concept of critical infrastructures, offering detailed RF parameters for an intensive forensic analysis on top of a simple warning signal for fast response. A detector cannot prevent electronics from being disturbed or destroyed, but it can be a key part of a protection concept.

DETECTOR CONCEPT

The achievements in digital signal processing regarding function integration, size and speed are amazing and might be seductive to be development base of an HPM detector. But there are some arguments against the digital concept.

In general the complexity of electronic circuits within a rough electromagnetic environment shall be as low as possible to keep the risk of malfunctions low as shielding and filtering effectiveness are always limited.

The RF frequency range of interest comprises several GHz, therefore an analog-to-digital (A/D) converter has to be a real-time sampling device and the fastest one available on the market beside a large amount of special memory. Currently available A/D converters for this high sample rate use 8 bits respectively 6 to 7 effective bits for signal quantization, resulting in 36 up to 40 dB dynamic range - assuming an adequate broadband front-end. For a frequency analysis a Fast Fourier Transformation (FFT) has to be performed. The FFT performance is related to the memory size and speed and therefore limited. Ready-to-use devices would be high-end oscilloscopes that are very expensive.

The power consumption of the detector is related to integrated functionality. Target should be a low power consumption in 24/7 activity to fulfill environment safety requirements and a light weight backup battery supply.

Therefore an analog concept is preferable for the HPM detector. One possible way would be a classical spectrum analyzer. It sweeps a frequency window across the RF frequency range of interest. The advantage of this device is the large signal dynamic range. The disadvantage of the sweep concept is, that the device is tuned just a fraction of sweep time on a dedicated RF frequency, the caption probability for short RF pulses is low.

Logarithmic RF amplifiers offer a broad frequency range up to several GHz and a dynamic range up to 60 dB. Detecting the RF envelope amplitude instead of the RF itself, the output signal has a bandwidth of approximately 100 MHz only and a 250 MHz / 1 GS/s oscilloscope to sample these signals is sufficient.

The frequency detection can be realized with a combination of logarithmic amplification and frequency-to-voltage converter, which will be described in detail in the following chapter.

Besides the main function of HPM source identification the instantaneous frequency measurement has the further advantage to offer correction of frequency dependent antenna gains, amplifications, and detector characteristics with pre-measured calibration tables which increases the precision of the field strength measurements. This is a part of the software concept of the detector.

DETECTOR HARDWARE

Fraunhofer INT developed several stages of generic demonstrators with the capability of sector surveillance (spiral antennas with beam width of 90 degrees) and high dynamic amplitude measurement (logarithmic amplifier/detector modules) [1]. A four-channel version with four broadband antennas showed the possibility of 360 degree surveillance and direction finding via comparison of the antenna voltage magnitudes, see Fig. 1.

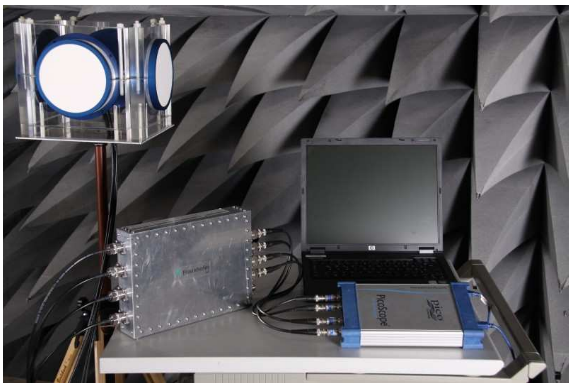

Fig. 1: Fraunhofer INT four-channel amplitude detection demonstrator

Concept of frequency detection

As discussed in the previous chapter, a frequency-to-voltage converter has been chosen for the instantaneous measurement of the HPM pulse carrier frequency. In detail, this can be done with a so-called delay-line frequency discriminator, see Fig. 2.

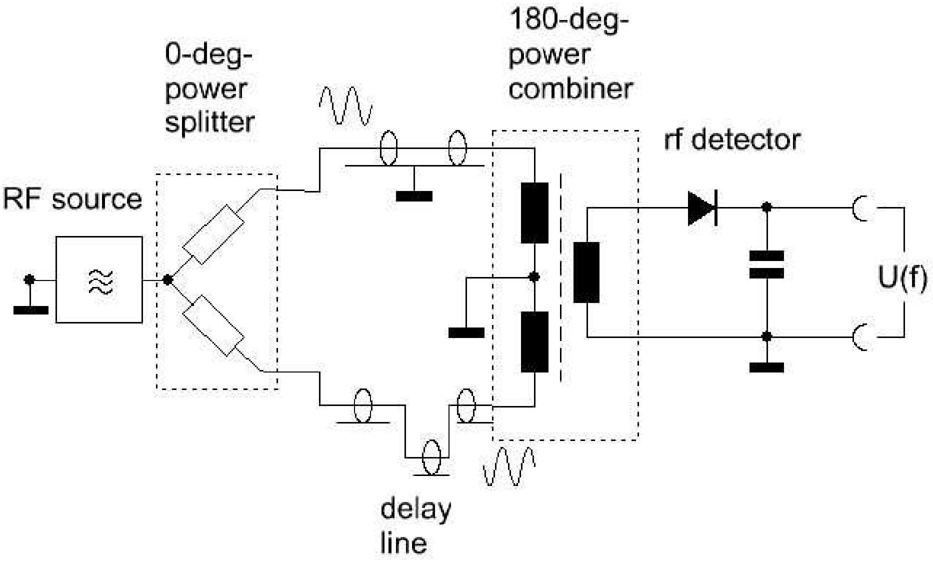

Fig. 2: Simplified diagram of a delay-line frequency discriminator

Basically it consists of a 0-degree power splitter, two coaxial lines with a defined delay time difference, a 180-degree power combiner to merge the branches and a linear RF amplitude detector. Its output amplitude increases linearly with frequency from zero to maximum at the frequency with 180 degree phase shift at the combiner due to the delay time difference. This technique allows detecting not only Continuous Wave (CW) signals, but also pulsed signals.

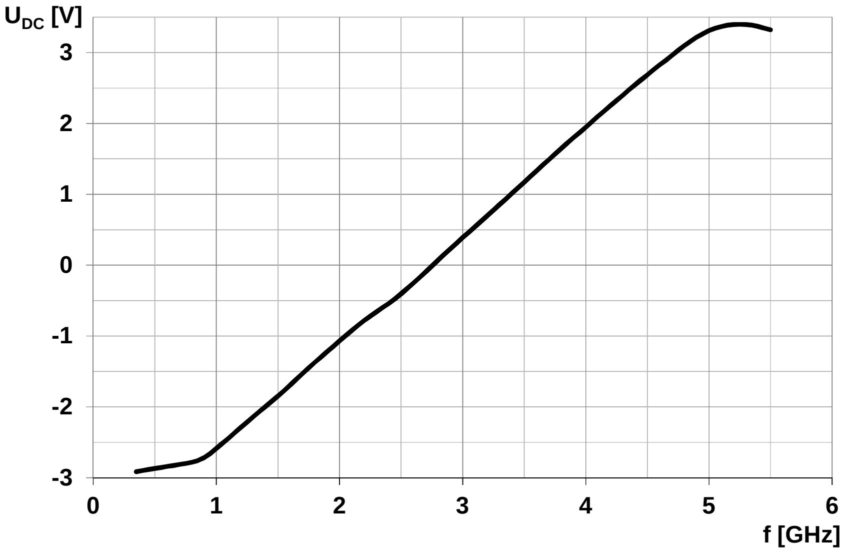

Fig. 3: Frequency vs. voltage characteristic of the integrated frequency discriminator

Precondition for the realization of such a frequency discriminator is an extremely constant input amplitude by a limiter-amplifier at the input, together with extremely good standing wave ratios of all RF components, as a ripple would easily obscure the desired signal, and a very linear and well impedance matched RF detector. An integrated frequency discriminator comprises all needed components with appropriate precision in a microwave-module housing. The discriminator is driven by an integrated broadband amplifier, which provides constant output amplitude with a dynamic range of 60 to 70 dB.

Demonstrator of a single channel HPM detector system with frequency identification

A single channel generic demonstrator detecting the frequency has been realized [2]. Fig. 4 shows the block diagram of the RF unit with one magnitude detection path combined with the described frequency detection path.

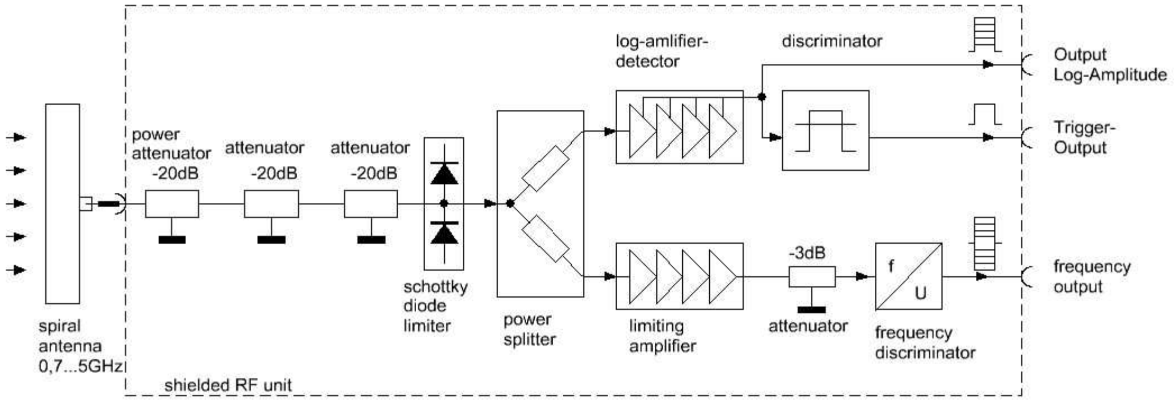

Fig. 4: RF unit block diagram of the HPM detector with frequency detection

These components are placed in a well-shielded box to realize the capability to resist field strengths of 10 kV/m and more, as expected in a surveillance environment. This RF unit is supplied via an RF filter by an external shielded battery or shielded power supply.

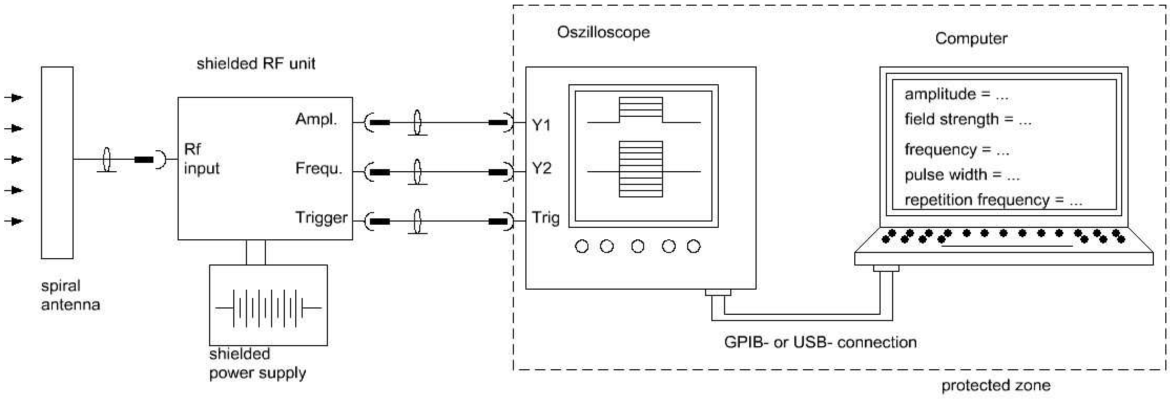

Fig. 5: Block diagram of the detector with frequency detection

The digital oscilloscope for signal acquisition is connected to the RF unit with three shielded coax cables. It has to be operated together with the control computer in a protected zone with adequate shielding effectiveness (Fig. 5Fig. 6). The hardware link between the oscilloscope and the control PC could be GPIB or USB. In case a compact oscilloscope without display is used, it could be combined with the RF unit in a separate shielded housing. Hence only the computer has to be placed in the protected area, connected with a USB-to-fiber-optics converter to the oscilloscope.

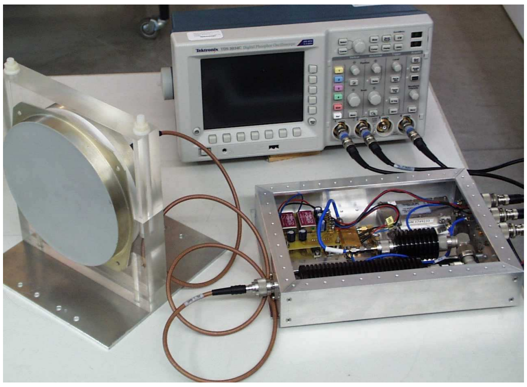

Fig. 6: Generic demonstrator of a single channel frequency detector

DETECTOR SOFTWARE

In the current development step software has been realized for the four-channel detector. The software takes care basically of oscilloscope control, arming the trigger and calculating the amplitude values. A first version of the Graphical User Interface (GUI) shows simplified information about HPM field amplitude with three threshold values and the direction of the threat relative to the antenna positions, as illustrated in Fig. 7.

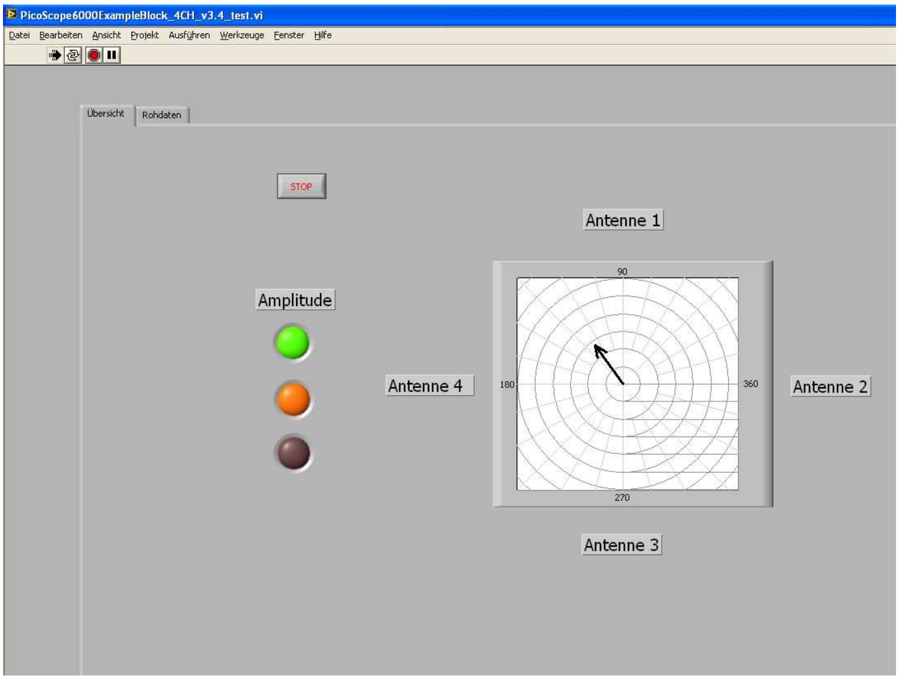
PicoScope6000ExampleBlock_4CH_v3.4_test.vi
Datei Bearbeiten Ansicht Projekt Ausführen Werkzeuge Fenster Hilfe
Übersicht
Rohdaten
STOP
Antenne 1
Amplitude
Antenne 4
90
180
360
270
Antenne 2
Antenne 3

Fig. 7: Screenshot of the four-channel detector software GUI

FUTURE PROSPECTS

Detector Integration into a Protection Concept

In case of an HPM attack, there is the need to react in short time according to defined procedures described in the protection concept. To realize this, the guard of that property needs only an instantaneous ascertainable alert, direction information, and the time stamps of the HPM pulses. There are several reactions which could be defined in the protection concept. They range from simply closing off an area as e. g. a gate of the airport via requiring additional armed guards, as the alarm system in all sectors might be doubtful, through to chasing the offenders, possibly with usage of a mobile HPM detector with direction detection. IT experts might monitor external data access attentively, check peripheral IT network devices and computers, or temporary disconnect networks. There is no deeper knowledge of HPM necessary except a short briefing for the involved people to follow this part of the protection concept.

Mid-term and long-term measures require more detailed RF information. After an attack RF experts can identify the kind of RF source and evaluate the field strengths and RF energies that affected the object. The coupling paths for RF play a key role affecting victim electronics within the protected property. All this information helps to estimate and predict temporary or permanent malfunction of electronics within the protected property. As long-term measures, the forensic investigation results of the attack can lead to a countermeasures plan with dedicated shielding and filtering, using other electronic devices and adapting the protection concept.

Future Development Steps towards a Product

Current investigations deal with the optimization of the broadband antennas for the usage in HPM detectors. One development target is to reduce the antenna size as a trade-off with frequency range and gain as commercial antennas are designed to other development targets. Another target is a directivity of 120° in a wide frequency range. This would reduce the number of magnitude detection channels to three, keeping the 360° direction surveillance.

To get a low power consumption of the detector, an A/D converter has to be developed and programmed instead of using a commercial oscilloscope. The objective is a compact and light-weight detector including supply, battery backup, remote control, and an HPEM hardened interface into the surveillance system.

The detector software will be realized as an application running directly in popular operating systems with the GUI reflecting the protection concept to offer the needed information tailored to the users.

As the detector is only useful as a part of a protection concept, a concept scheme for detector integration has to be worked out as well.

REFERENCES

[1] Chr. Adami, Chr. Braun, P. Clemens, M. Jöster, H.-U. Schmidt, M. Suhrke, and H.-J. Taenzer. *HPM Detector with Extended Detection Features*. Ultra-Wideband, Short-Pulse Electromagnetics 10 Book, to be published.

[2] Chr. Adami, P. Clemens, M. Jöster, H.U. Schmidt, M. Suhrke, and H.J. Taenzer. *Ein HPM-Detektionssystem mit frequenz- und Amplituden-Messung - 1. Prototyp eines einkanaligen Gerätes*. Fraunhofer INT Report 26/2013 (Juni 2013).