UNIVERSITY *of York*

This is a repository copy of *Circuit and Electromagnetic Modelling of a low cost IEMI Sensor*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/82956/

Proceedings Paper:

Dawson, John Frederick orcid.org/0000-0003-4537-9977, Flintoft, Ian David orcid.org/0000-0003-3153-8447, Rebers, Lauritz et al. (3 more authors) (2014) Circuit and Electromagnetic Modelling of a low cost IEMI Sensor. In: Proceedings of EMCUK 2014. .

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Circuit and Electromagnetic Modelling of a Low Cost Intentional Electromagnetic Interference Sensor

J F Dawson, I D Flintoft, and L Dawson, Department of Electronics, University of York
L Rebers, Dept of Electronics and Information Technology, University of Hannover
Michael Camp, Juergen Schmitz, and Markus Jung, Rheinmetall Waffe Munition GmbH

ABSTRACT

The design of a low cost broadband Intentional Electromagnetic Interference (IEMI) detector and antenna to achieve a flat frequency response over a broad range is considered. SPICE simulation of the antenna, detector and low power log-amplifier circuit is used to predict the detector performance. The SPICE Antenna model is derived from numerical electromagnetic simulation. Simulations are compared with measured performance.

INTRODUCTION

The possible use of Intentional Electromagnetic Interference (IEMI) to disrupt critical infrastructure is becoming a significant concern [1]. One aspect of this threat is detecting the cause of a system failure. A failure due to IEMI may be blamed on faulty hardware or software, and much time and money may be wasted on searching for the cause, particularly if the failure is intermittent. It is therefore beneficial to consider how IEMI attacks may be detected. A number of IEMI detector systems have been developed previously such as those in references [2] and [3] which can detect IEMI. Although reference [4] describes a system that can determine the direction to the IEMI source, we have not been able to find references describing practical systems capable of determining the complete location of the source. In this paper, we describe a low cost detection system being developed as part of the STRUCTURES programme [5]. The STRUCTURES programme is one of several EU funded research programmes evaluating the effects of IEMI on critical infrastructure, including protection and detection. A complementary identification and location system is also being designed and a brief description is included in this paper for comparative purposes.

DETECTOR DESIRABLES

The three most important requirements for the detection system are the ability to detect an IEMI attack and generate an alarm, to send the received data for logging and post-processing, and to be cost-efficient. Additional features, such as locating and/or identifying the source of the attack, require designing a significantly more complex system, which is thus likely to be more expensive. Within the STRUCTURES project we are developing both, low-cost and high-performance detectors outlined in this paper.

Detection of threat

Clearly the first desirable property of a detector is that it can successfully detect the presence of an IEMI threat. False alarms should also be minimized. A field detector must have some means of discriminating between IEMI threats and other intentional or accidental sources such as mobile phones and electrostatic discharge. For simple detectors the discrimination between threat and other fields might be largely based on the level, though this can also be aided by ensuring that the detector is located away from expected transmitters such as mobile phones. A more complex system might be able to discriminate on the basis of frequency content and/or the time domain waveform. Similarly, a conducted interference detector must be able to differentiate between "normal" levels of transient and noise on a wire and that introduced by IEMI.

Since most radiated IMEI sources are likely to use high gain antennas with narrow beam widths, it seems advantageous that a number of detectors are placed around any sensitive equipment, sufficiently close together that at least one detector will see the beam of any attack, even if it is slightly mis-directed.

The susceptibility level of equipment used in industrial applications should be greater than 10 V/m and typical failure levels can be considerably higher and tend to increase with frequency [6] & [7]. Therefore, a detector should be sensitive to levels above 10 V/m and if the detector is placed between the source and equipment to be protected, it is likely to have an alarm threshold considerably greater than 10 V/m.

Sources are available at ever increasing frequencies but their complexity increases with frequency. Although the majority of available sources operate below 3 GHz [8], detection at higher frequencies is desirable to allow for future developments.

Communication and logging

In order to allow notification of a threat and subsequent analysis (forensics) of the time, duration and number of attacks, some mechanism is required for the data from a number of sensors to be communicated to a local or remote monitoring and logging system, to send alerts and alarm indications (e.g. to a security office).

Identification of threat

Identification of the type of interfering signal is desirable, partly to discriminate between signals that may not be IEMI, such as a nearby mobile phone, and partly to aid in tracking the source of interference. A simple system is likely to be able to determine simple waveform features such as whether the threat is CW, long or short pulse, but will be unable to observe details of very fast rise time or short pulses. A more sophisticated system may seek to determine frequency, rise-time, Pulse Repetition Frequency (PRF), etc. which can provide a picture of the source type in use.

Location of threat

Location of the source of the threat would enable action to be taken to identify and apprehend the perpetrators of the attack. It is possible that a simple system can give some indication of the location of a threat if a large number of detectors are used, simply by observing which detectors are triggered. A more complex system can use many techniques for direction finding, such as those based on antenna directivity, time difference of arrival, etc.

Cost

Any practical detector system will also have to be affordable. A low cost system may only be able to detect the presence of a possible threat, whereas a system capable of identifying and locating the threat is likely to be more expensive. Within the STRUCTURES project we are developing both low-cost and high performance detectors outlined in this paper.

A MODULAR DETECTOR SYSTEM

Here we propose a concept of a modular IEMI detector system and discuss how one such system can be upgraded to achieve localization and identification of an IEMI source.

Low cost detectors

Figure 1. shows the concept of the low-cost IEMI detection system being developed in the STRUCTURES project. Multiple sensors are coupled to a (protected) computer system for warning, logging and analysis. Optical fibre communications provide robust communications, though wireless or wired links may be desirable in some cases.

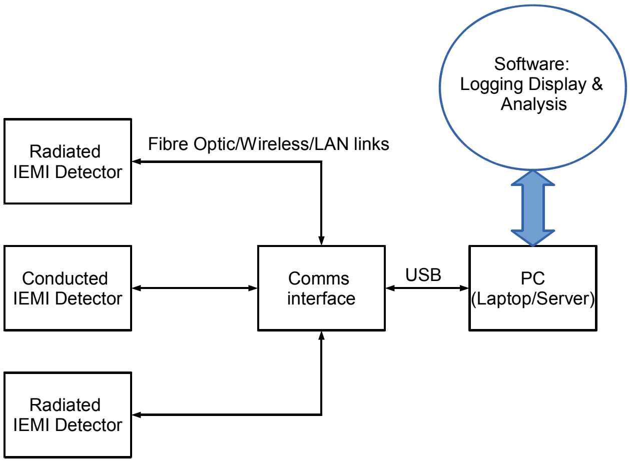

Figure 1. Low cost IEMI detector system concept

The block diagram for individual low-cost detectors is shown in Figure 2. In a low cost system it is desirable that each detector unit operate on battery power for extended periods. Low-power consumption could be achieved with the assistance or solar or other scavenged energy sources.

Low power operation is possible for many microcontrollers, and wireless links such as Zigbee [9]. Optical links can also be operated at very low power consumption levels, making battery operation possible. Wired network connections tend to have much higher power consumption requirements but power over Ethernet is becoming readily available.

For the conducted and radiated IEMI detectors, a wide dynamic range is required and this implies the use of a logarithmic amplifier. Whilst commercial broadband logarithmic detectors with high dynamic range and operating frequencies up to 10 GHz are available, their power consumption is high, around 100 mA, and so they are not suitable for battery powered operation. The design of a low powered radiated IEMI detector with logarithmic amplifier is the subject of the remainder of this paper.

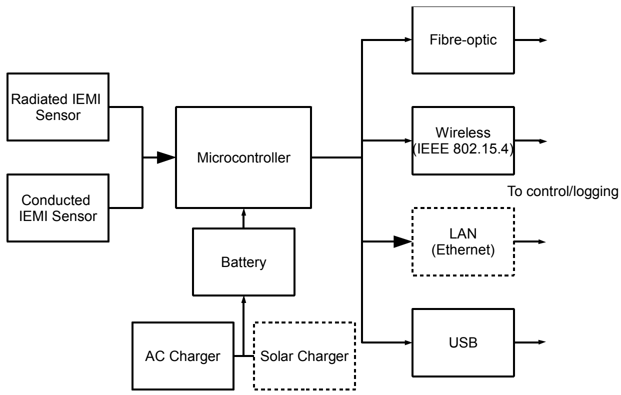

Figure 2. Detector concept

LOG AMPLIFIER AND DETECTOR DESIGN

Design concept

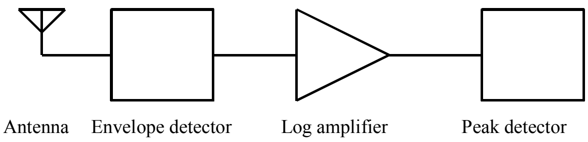

Figure 3. Log amplifier and detector design concept

An initial simulation of the diode detector shows that the limit of sensitivity is about 10mV. It can also be seen that the detector output is temperature sensitive so some means of compensation is required. Measurements showed that the detector was useable down to about -40dBm input (4.47mV).

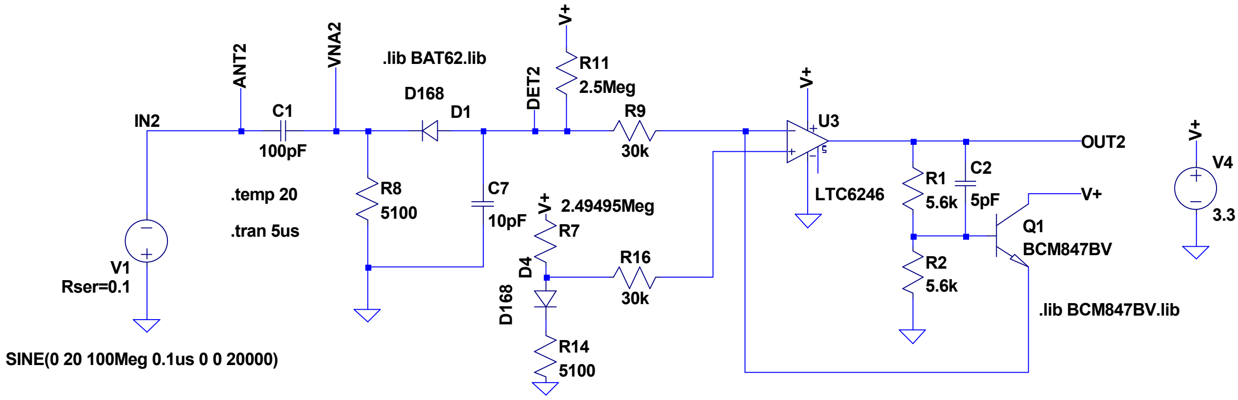

Figure 4. Log amplifier and detector initial design

Log amp design and performance

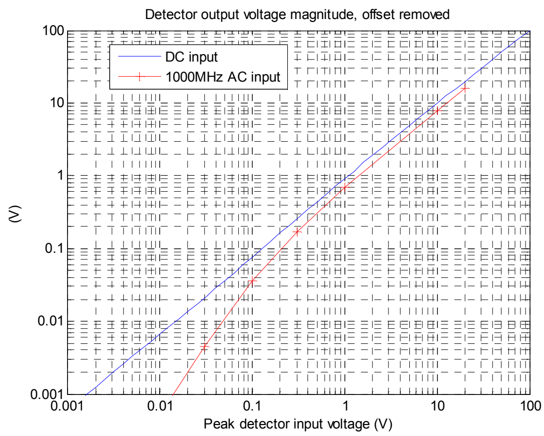

Figure 5. Detector performance models

Figure 5. shows the input v output voltage for the detector, when attached to the log amplifier when driven by a dc source and when capacitively coupled to an ac source. The dc case is easy to simulate but diverges from the ac case for small inputs.

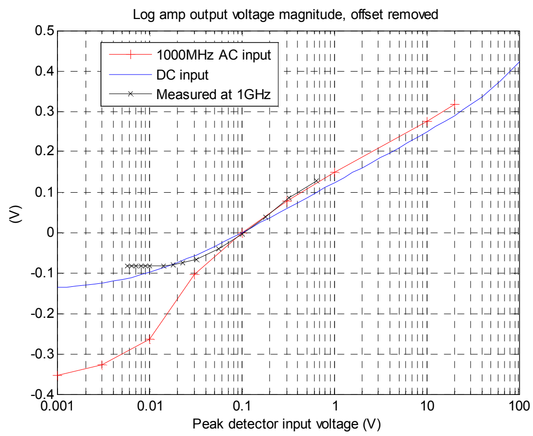

Figure 6. Detector output as a function of ac input at 1GHz

Figure 6. shows the output of the log amplifier with the dec offset removed, when driven by a dc source and when capacitively coupled to an ac source, along with measured data. As the offset voltage varies in each case the offset has been removed by setting the outputs to be equal at 0.1Vpeak input.

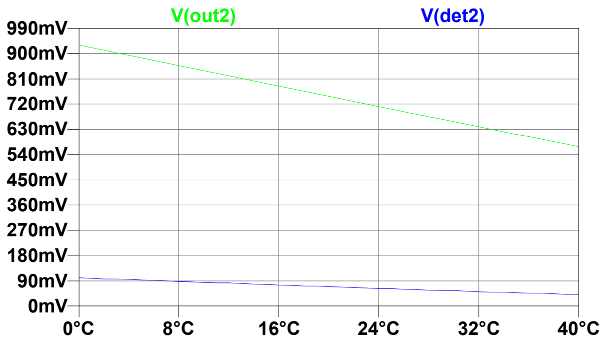

Figure 7. Effect of temperature on log amplifier

Unfortunately both the detector diode and the log-amp transistor junctions suffer a variation of voltage with temperature so is necessary to compensate for this effect.

Figure 8. shows the completed circuit, consisting of two log-amp detector circuits driving a differential amplifier followed by an active peak detector. Also a model of the antenna is included, connected to the detector and connected to a linear equivalent of the detector model. The antenna model is discussed later. The second log-amp detector circuit is necessary to compensate for the temperature drift of the detector and log-amplifier. The output of the second log-amp detector circuit is subtracted from the output of the rf driven detector and log amplifier circuit by a differential amplifier. A peak detector circuit is also added to make measurement of transient peaks easier. In this circuit the model shows no detectable change in output voltage with temperature. There is however a small change in the log-amp gain with temperature that is not compensated.

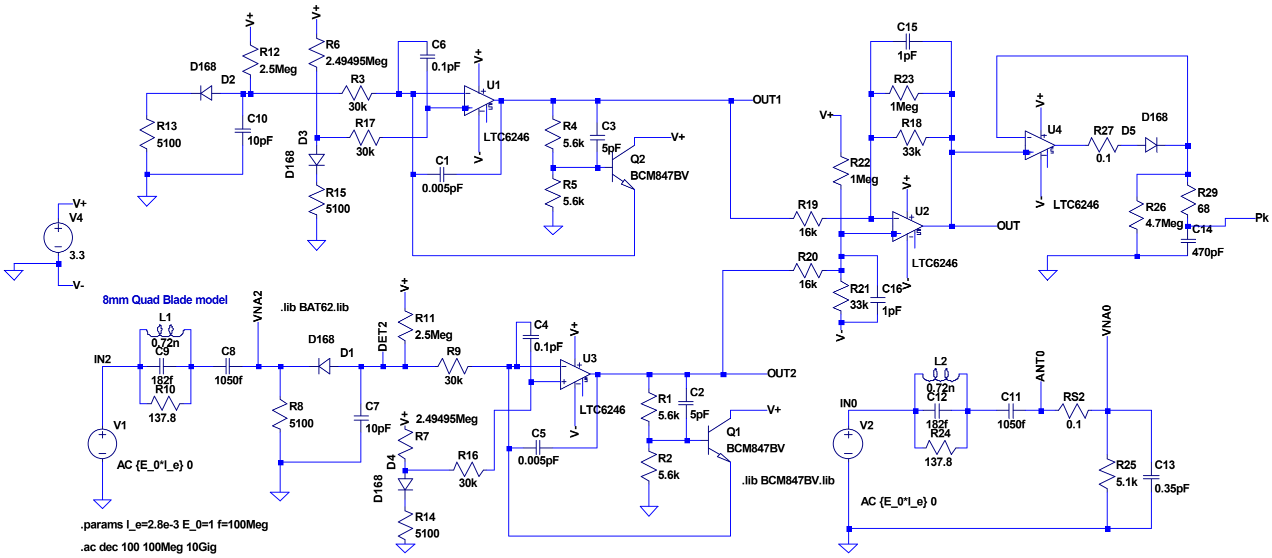

Figure 8. Log amplifier and detector final design including antenna model and linear detector/antenna model

Antenna design and performance

Kanda [10] showed that it is possible to achieve a flat frequency response over a broad bandwidth using a simple dipole antenna directly connected to a detector diode. This is due to the fact that the detector charges its output capacitor which eventually reverse-biases the diode so the antenna sees only the diode capacitance as its load. A dipole like antenna below resonance exhibits a purely capacitive impedance and this acts as a frequency independent potential divider with the diode capacitance.

We would like to achieve a useable operating range towards 10 GHz. An 8 mm monopole has a quarter wave resonant frequency of approximately 9 GHz and Figure 9. shows the frequency response of the monopole driving the capacitive load of the diode simulated using the CONCEPT [11] full-wave numerical electromagnetic simulator. A significant dip in antenna factor can be seen as the antenna passes through resonance.

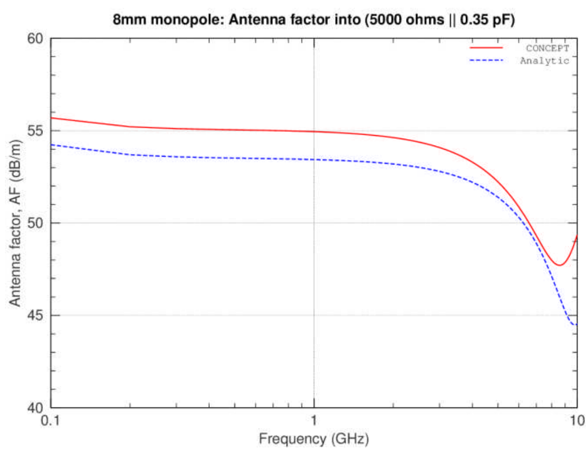

Figure 9. 8mm monopole antenna factor

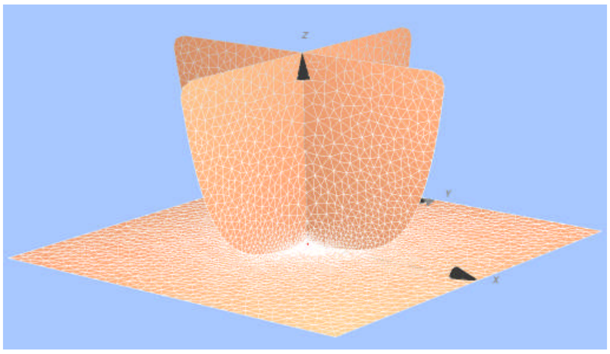

Figure 10. 8mm Quad-blade antenna with increased capacitance

From Figure 6. The measured results indicate that we can detect voltages as low as about 20 mV. For an 8mm dipole with a 57 dB/m antenna factor (SeeFigure 9.), the corresponding minimum detectable field sensitivity is:

$$E_1 = V \cdot AF_1 = 11.2 \text{ V/m}$$

Since the antenna forms a capacitive potential divider with the detector, the antenna factor can be controlled by modifying the antenna capacitance. Figure 10. shows an 8 mm high antenna with increased capacitance. We chose the shape as recent experience in designing a broadband antenna for reverberation chambers [12] shows that the taper at the base radiates well at frequencies above resonance and it suppresses the effect of the monopole resonance(s). It can be seen (Figure 11.) that the increase in capacitance results in a small reduction of antenna factor. The reduced antenna factor of 53.5 dB results in an increased sensitivity of the detector such that the minimum detectable field for a detector sensitive to 20 mV is:

$$E_2 = V \cdot AF_2 = 9.46 \text{ V/m}$$

The change in sensitivity was smaller than expected and the resonance is still present as we were unable to manufacture a small enough feed gap to achieve the same performance as in [12].

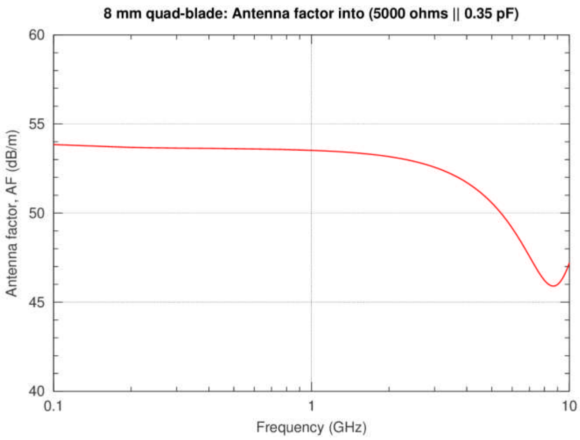

Figure 11. 8mm quad-blade antenna factor

Detector Frequency response

The antenna behaviour can be simulated using a SPICE model of the antenna derived from the monopole model proposed by Tang et al [13]. Figure 12. Shows the antenna factor for a simple linear model of the detector using just the diode capacitance and the SPICE AC simulation result using a more detailed model of the diode.

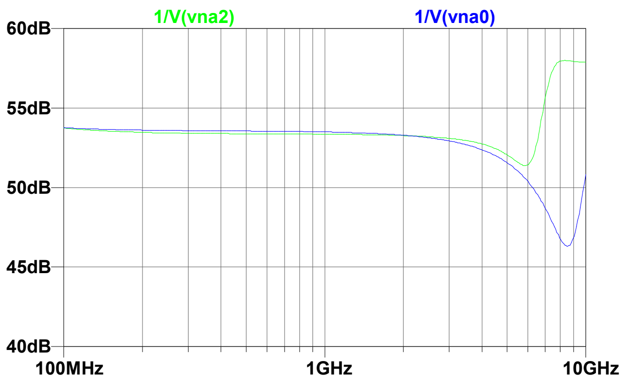

Figure 12. SPICE model of Detector frequency response showing antenna factor of Quad-blade with BAT62 diode for the linearised real circuit (blue) and simple antenna detector model (green).

The SPICE model can also be used to estimate the time response of the detector to pulsed waveforms. Figure 13. Shows the time response to a large sinusoidal input (800 V/m). The rise time of the detector is about 200 ns. Figure 14. Shows the time response to a 10 V/m sinusoidal input. It can be seen that the rise time is much slower and the detector does not fully respond in the 5 µs pulse width. This is due in part to the non-linearity of the diode detector and in part due to the log-amp having a slower rise-time for smaller signals. We therefore had some concern as to whether the detector would respond adequately to some of the short pulses found in IEMI waveforms

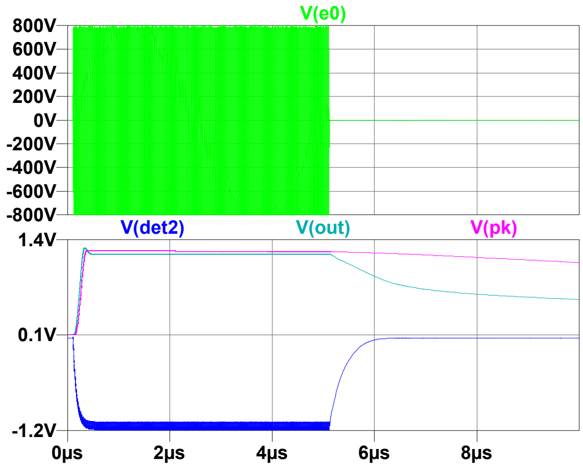

Figure 13. SPICE model of Detector showing time response of the detector to a 100 MHz sinusoidal input. The top trace shows the incident field in V/m and the bottom trace shows the microwave detector output (dark blue), the differential amplifier output (light blue) and the peak detector output (magenta).

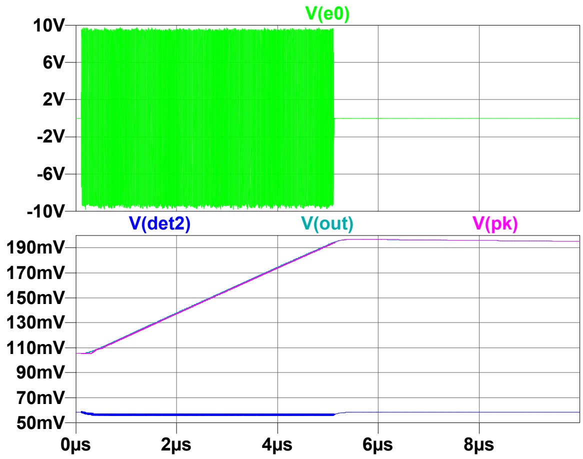

Figure 14. SPICE model of Detector showing time response of the detector to a 100 MHz sinusoidal input. The top trace shows the incident field in V/m and the bottom trace shows the microwave detector output (dark blue), the differential amplifier output (light blue) and the peak detector output (magenta).

Currently measurements are underway to characterise the detector performance and compare it with the model results. The simple model above omits many parasitic elements so exact correspondence is not expected but preliminary data shows the detector has good performance up to about 6 GHz.

IEMI DETECTOR SYSTEM TEST RESULTS

To-date the detector system has undergone some preliminary tests at Rheinmetal up to 1GHz CW and with several pulsed sources.

Figure 15. and Figure 16. Show the experimental setup. Figure 17. shows a detailed view of the antenna and detector realised on a FR$ PCB laminate.

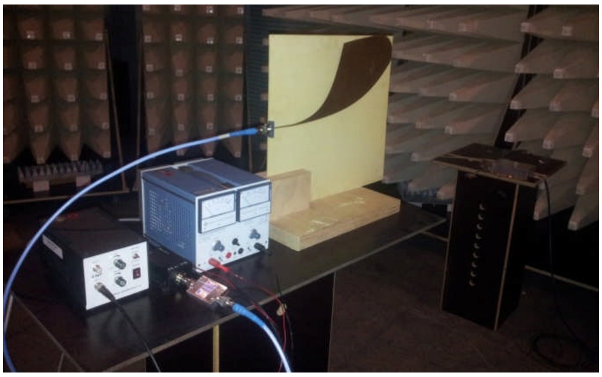

Figure 15. IEMI detector test setup with pulse generator at Rheinmetal's a nechoic chamber

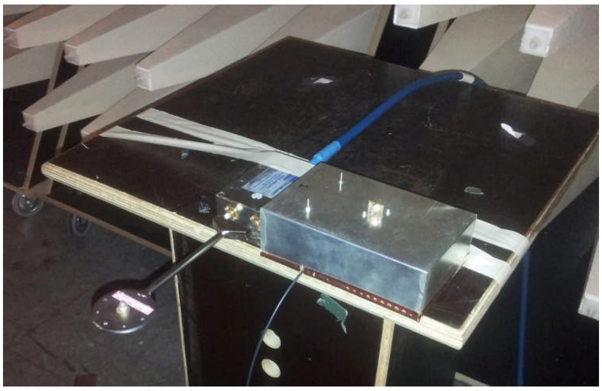

Figure 16. IEMI detector test setup at Rheinmetal's Anechoic chamber

Figure 17. Close up of quad blade antenna

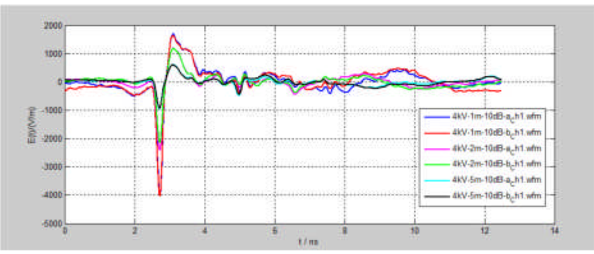

Figure 18. Incident field from pulse generator measured with D-dot sensor

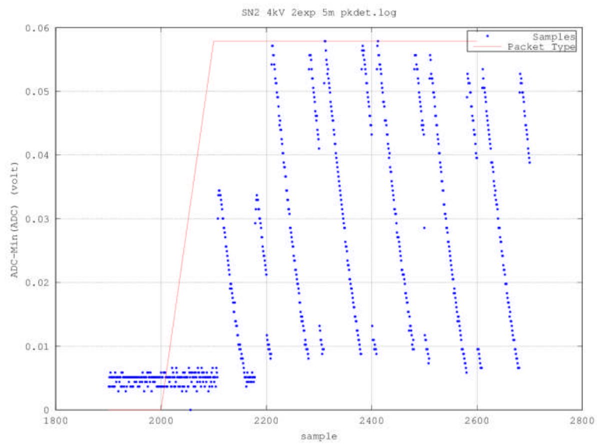

Figure 19. IEMI detector log-amplifier detector output for 800V/m pulse

The incident field was measured using a D-dot sensor [15] and Figure 18. shows the measured field waveform from a 4 kV double exponential pulse generator driving a Vivaldi antenna. This is obtained by integrating the output of the D-dot sensor.

The initial pulse width is less than half a nanosecond wide and is much shorter than the time constant of the detector and amplifier circuits. Figure 19. Shows the output of the Analogue to digital converter connected to the peak detector output for an 800 V/m pulse from the pulse generator. Due to the fact that the pulse is shorter than the time constant of the detector the detector does not record the full pulse amplitude. The first two pulses are shown as a smaller amplitude – this is the power supply of the pulse generator ramping up to full voltage as it is switched on. The red line is the trigger state of the detector: low is not triggered and high is triggered. A number of pre-trigger samples are also shown.

CONCLUSIONS

An outline of the use of SPICE and CONCEPT to predict the performance of an Intentional Electromagnetic Interference Detector has been presented. Currently the performance of the detector is being evaluated and we hope to present further results during the conference.

References

[1] Radasky, W.; Baum, C. & Wik, M. , "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)" , *Electromagnetic Compatibility, IEEE Transactions on* , *vol. 46, no. 3* , 314 - 321 , Aug. 2004.

[2] Adami, C.; Braun, C.; Clemens, P.; Suhrke, M.; Schmidt, H. U. & Taenzer, A. , "HPM detection system for mobile and stationary use" , *EMC Europe 2011 York* , 1-6 2011.

[3] Hoad, R. & Leaver, A. , "The Application Intentional Electromagnetic Interference (IEMI) Detectors for Safety and Security" , *EMC Europe Workshop 2007, Paris, France, 14th - 15th June* 2007.

[4] Adami, C.; Braun, C.; Clemens, P.; Joester, M.; Suhrke, M.; Schmidt, H. & Taenzer, H. , "HPM Detector System With Frequency Identification" , *Proceedings of the 8th Future Security Research Conference 2013 (Berlin)* 2013.

[5] Dawson, J. F. , "The STRUCTURES Project: Strategies for The impRovement of critical infrastrUCTUre Resilience to Electromagnetic attackS" , *IET Seminar on: Extreme Electromagnetics* - The *Triple Threat to Infrastructure* , 14th January 2013. , Available from: http://www.theiet.org/communities/electromagnetics/triple-threat/index.cfm

[6] Zammit, C. & Kerr, B. , "General Electronic Equipment Microwave Susceptibility Trend as a Function of frequency" , *Proc. Institution of Engineering and Technology Pulsed Power Symposium* , 59-61 2006.

[7] Hoad, R.; Carter, N.; Herke, D. & Watkins, S. , "Trends in EM susceptibility of IT equipment" , *Electromagnetic Compatibility, IEEE Transactions on* , *vol. 46, no. 3* , 390 - 395 , aug. 2004.

[8] Giri, D. & Tesche, F. , "Classification of intentional electromagnetic environments (IEME)" , *Electromagnetic Compatibility, IEEE Transactions on* , *vol. 46, no. 3* , 322 - 328 , aug. 2004.

[9] ZigBee Alliance, "ZigBee Specification" , January 2008. , Available from: http://www.zigbee.org/en/index.asp

[10] Kanda, M. & Driver, L. , "An Isotropic Electric-Field Probe with Tapered Resistive Dipoles for Broad-Band Use, 100 kHz to 18 GHz" , *Microwave Theory and Techniques, IEEE Transactions on* , *vol. 35, no. 2* , 124-130 , February 1987.

[11] CONCEPT-II: Advanced Electromagnetic Field Simulation. , Available from: http://www.tet.tuhh.de/downloads/concept/CONCEPT-II-September-2013.pdf

[12] Marvin, A.; Esposito, G.; Dawson, J.; Flintoft, I.; Dawson, L.; Everard, J. & Melia, G. , "A wide-band hybrid antenna for use in reverberation chambers" , *Electromagnetic Compatibility (EMC), 2013 IEEE International Symposium on* , 222-226 , August 2013.

[13] Tang, T. G.; Tieng, Q. M. & Gunn, M. W. , "Equivalent circuit of a dipole antenna using frequency independant lumped elements" , *IEEE Transactions on Antennas and Propagation* , *vol. 41, no. 1* , 100-103 , January 1993.

[14] Stojilovic, M.; Menssen, B.; Flintoft, I.; Garbe, H.; Dawson, J. & Rubinstein, M. , "TDoA-Based Localisation of Radiated IEMI Sources", *EMC Europe* 2014.

[15] Baum, C.; Breen, E.; Giles, J.; O'Nelll, J. & Sower, G. , "Sensors for Electromagnetic Pulse Measurements Both Inside and Away from Nuclear Source Regions" , *Electromagnetic Compatibility, IEEE Transactions on* , *vol. EMC-20, no. 1* , 22-35 , Feb 1978.

Acknowledgement

The research leading to these results has been implemented in the framework of the Project STRUCTURES co-funded by the European Union Seventh Framework Programme under grant agreement n° 285257.