# Preliminary Investigation Into a Methodology for Assessing The Direct RF Susceptibility of Digital Hardware

## Final Report

for

**Radiocommunications Agency**

**Copy 1 of 6**

Document number R/99/042

Project number 0921

Author: .....
Dr I. D. Flintoft, BSc, PhD

Checked: .....
Prof. A. C. Marvin, M.Eng, PhD, CEng, MIEE, MIEEE

Approved: .....
Mr. C.A. Marshman, B.Eng, M. Phil, CEng, MIEE

| Issue | Description | Issue by | Date |
|---|---|---|---|
| **A** | **First Issue** | **CAM** | **12 May 1999** |

# ABBREVIATIONS

| | |
|---|---|
| AEG | Applied Electromagnetics Group |
| AM | Amplitude Modulation |
| CMP | Cross Modulation Product |
| EMI | Electromagnetic Interference |
| EMC | Electromagnetic Compatibility |
| EUT | Equipment Under Test |
| IP | Intermodulation Product |
| PMR | Private Mobile Radio |
| RAM | Radio Absorbing Material |
| RFI | Radio Frequency Interference |
| RMS | Root Mean Square |
| YES | York EMC Services |

# CONTENTS

# 1.0 INTRODUCTION

The immunity of digital hardware to radio frequency interference (RFI) is not always adequately assessed by current EMC immunity test methods. This report presents the findings of a feasibility study into alternative methods of assessing the RF susceptibility of digital equipment.

## 1.1 Objectives

The study had three main objectives:

1 Proposing techniques for ***quantifying*** the direct RF ***susceptibility*** of digital hardware independently of the software, error correction and other effects not related to the actual hardware itself.

2 Proposing new types of ***threat field*** for immunity testing of digital equipment which are more representative of today's complex electromagnetic environments and which can be used in conjunction with the techniques proposed in 1.

3 Showing how the proposed techniques and threat fields can be developed into a practical EMC immunity test method.

These objectives are in essence answers to three important questions which arise when considering the problems of assessing the immunity of digital equipment in complex electromagnetic environments:

1. **How do we measure failure?** Is the perceived malfunction of a piece of equipment by human observation the only way to define failure in an immunity test? Perceived assessment of immunity is unable to determine the effects of software error correction on the actual performance of digital systems in the presence of EMI and provides little indication of the risk of failure in different types of environment. Other observations which are able to quantify the immunity may provide more information on the effect of EMI on the operation of digital systems.

2. **What are appropriate threat fields for digital systems in current and future EM environments?** As indicated in [1] narrow band threat fields with simple modulations are no longer necessarily representative of the EMI which causes the failure in digital systems. We must therefore look at more broad-band test signals, impulsive signals and also statistical signals which are representative of ensembles of EMI from multiple sources. The question of how the different modes of operation which may be present in a digital system affect the immunity of the system to such threats must also be addressed.

3. **What is the best way of delivering the threat field to the EUT?** Any techniques proposed for testing digital hardware must be practical, using the current testing infrastructure of EMC test houses. This means either a chamber measurement or some type of test cell.

## 1.2 Approach

A search for any existing techniques and relevant theoretical and experimental information was undertaken jointly by the Applied Electromagnetics Group (AEG) and York EMC

Services Ltd (YES). This search encompassed relevant standards organisations, the INSPEC database and the AEG's specialist knowledge of the EMC literature. The information obtained from the standards bodies and literature search are summarised in Section 2.0.

The survey of standards bodies and other organisations produced no indication of directly relevant work being undertaken elsewhere with the exception of possible work by the military. The details of this work were not available to us.

The literature survey produced no evidence of work being carried out which was directly applicable to the first of our objectives, except for the research conducted by the University of York on modulated and non-linear scattering from digital equipment [2,3]. The study therefore concentrated on investigating measurement arrangements based on variations of this technique. A review of the theoretical basis of the technique, in the context of immunity testing, is given in Section 3.0.

It was apparent that many of the issues related to the practicality of the non-linear scattering method could be informed by a short experimental test programme with focused objectives. The limited resources available to this feasibility study precluded the use of the YES commercial testing facilities. The measurements were therefore undertaken in the research laboratories of the Applied Electromagnetics Group. This caused significant limitations in what could be achieved, but at the same time, the success of the experiments within these limitations demonstrate that the technique is feasible with current test equipment. The series of experiments was performed between 16/1/99 and 12/3/99 and the results are presented in Section 4.0 of this report.

Based on the theoretical analysis and the testing programme a series of test methods are proposed in Section 5.0. Section 5.1 discusses the general features common to all the proposed methods. Sections 5.2 and 5.3 give specific implementations of the modulated scattering technique with carrier wave threats using chamber and cell based configurations respectively.

The literature survey did show that research was being carried out on the extension of the threat fields used in immunity tests beyond carriers with simple AM modulation. Some of these ideas, together with some of our own, are discussed in the context of the modulated scattering method in Section 5.4.

# 2.0 INFORMATION SEARCH

The information search was performed using web search and literature review techniques by YES and the Applied Electromagnetics Group. In addition, other avenues were pursued by contacting individuals within organisations that may have performed work in the area of interest. These contacts were found from personal knowledge, recommendations from colleagues and other contacts, and from speculative enquiries to general contact addresses found whilst performing the web and literature reviews. This work was carried out between 16/12/98 and 25/1/99.

## 2.1 Standards Organisation

Relevant information from the following principal organisations was investigated. This involved locating and searching the associated web sites and also contacting individuals where possible.

1. Radiocommunications Agency (RA)
2. International Telecommunication Union (ITU)
3. ETSI
4. British Standards Institution (BSI)
5. DAVIC
6. CISPR
7. CENELEC
8. Military EMC

Details of the responses can be found in Appendix A. With the exception of the military no indication was found of relevant work being carried out by any of these organisations. A number of contacts suggested that work had been done by the military in this area but that the information was sensitive.

## 2.2 Literature Search

A comprehensive search was undertaken of the INSPEC database for years 1995 to 1998. A selection of search keys designed to catch general references on digital immunity and specific references on the use of re-radiation characteristics of digital equipment were used. The details of the search are provided in Appendix B.

The literature survey provided many general references and indicates that the problems with current EMC standards and digital equipment are starting to be recognised. We found no references on directly applicable generic measurement techniques which are able to quantify immunity (with the exception of [17] which was regarded as limited in scope, impractical and not appropriate to an EMC test standard). There were however many ideas for more broad-band and statistical test signals which may be useful for digital systems and analysis of the statistics and reliability of immunity tests for digital systems. Time domain or impulsive techniques may also offer a more reliable and general immunity testing approach.

# 3 DIGITAL IMMUNITY AND MODULATED SCATTERING

## 3.1 Susceptibility Characteristics Of Digital Equipment

Digital equipment generally has quite different susceptibility characteristics to analogue equipment. The failure of digital hardware in the presence of electromagnetic interference (EMI) is usually quite abrupt and typically requires the system to be reset before normal operation can be continued. This is in contrast to analogue systems which tend to show increasing effects as the EMI is increased and tend to recover spontaneously when the EMI is removed.

Although the nature of digital equipment provides a degree of immunity to EMI, low levels of external interference can still cause problems. Failures of digital hardware are generally classified as static or dynamic:

**Static Failures**: Static failure occurs at high levels of interference when the level of EMI induced in the digital signals is sufficient to cause false switching of gates in the circuit [4]. This occurs when the level of EMI induced on signal bearing conductors becomes comparable to the difference in the switching thresholds of the logic. Static failure is characterised by the noise margin of the component devices in the circuit which defines the maximum amount the output of a device can be perturbed without causing misinterpretation of the signal by a following compatible device.

**Dynamic Failures**: At low levels of interference significant changes in the propagation delay of a device can occur. This can lead to violation of timing constraints such as hold times of flip-flops and hence a failure of the system [5,6,7]. Changes in propagation delay can be the primary cause of failure at low levels of interference. They can be characterised by a parameter called the delay margin of the circuit. The delay margin is the maximum change in the timing of a signal transition for which the circuit continues to operate reliably. Note that delay margin is a property of circuits and not just individual devices like noise margin.

Static failures can occur even in the quiescent state of a digital system and are generally not strongly dependent on the state of the system (once interference reaches a level where false switching can occur the state of system is a secondary factor). Dynamic failures are however much more dependent on the state of the system having a strong impact on the time variability of a systems susceptibility. The relative phase of the EMI and the logic transitions can lead to changes in the failure rate from 0% to 100% on time scales of a few nanoseconds. This type of failure has also been shown to be strongly dependent on the microcontroller architecture and software used by digital systems [8]. This makes it difficult to conduct repeatable immunity measurements on digital hardware, particular hardware with many different time scales in its cycles of operation. Two methods which have been proposed to overcome this difficulty of immunity testing digital equipment with many cycle times are "statistical evaluation of test results" and "testing all time windows". Measurements have shown that synchronising pulsed RFI with the digital signals in an EUT can significantly increase the measured susceptibility [9] of the EUT and maybe provide a worst case estimate of the susceptibility. However, this requires the use of a synchronisation unit connected to the EUT and is not practical for bulk EMC testing.

Dynamic failure may become more of a problem with the current trend to higher clock speeds which will make timing errors more likely. The trend towards lower power logic will also

increase the risk of EMI related failures in digital hardware - both static and dynamic - unless more care is taken in the EMC design of the equipment.

Software error correction techniques are able to correct for low frequency errors caused by either type of failure and can therefore mask an inherently susceptible piece of equipment during standard immunity tests. This may give a false impression of the immunity of a piece equipment which then has EMC problems in real environments.

The non-linearity of digital systems also poses a problem for current testing methods. The measurement of the immunity of a non-linear system at two different carrier frequencies does not allow the observer to infer an immunity level against a threat composed of both frequencies simultaneously if the system can fail in a non-linear way [1]. Discrete frequency testing is therefore inadequate for non-linear systems and more complex threat fields may need to be considered which are related to the operating environment of the equipment.

## 3.2 Modulated Scattering Of RF Fields From Digital Equipment

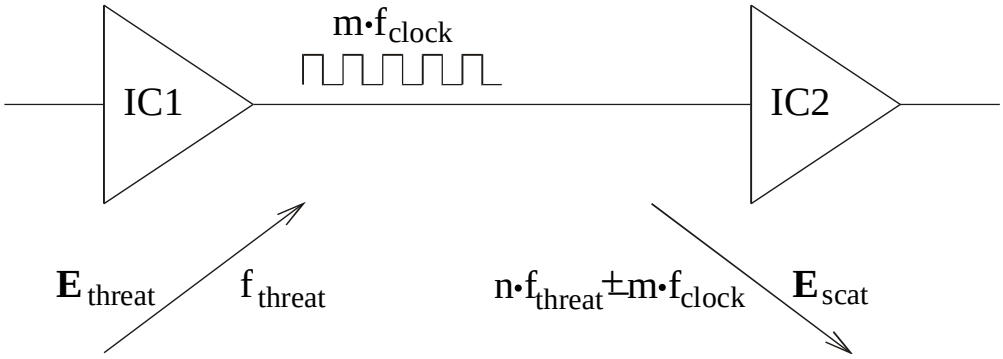


**Figure 1: Basic theory of scattering from digital hardware.**

In the presence of radio frequency interference (RFI) the internal signals of a piece of digital equipment are modified in a systematic way (

Figure 1). This causes changes in the spectra of the internal signals associated with the incident RF threat energy which indicate that the interference has reached a particular sub-system in the equipment. The original work proposed four regimes corresponding to increasing levels of threat RFI [2]:

1 At low energy levels the threat RFI does not induce non-linear behaviour in the active devices of the system. The functional behaviour of the equipment is not affected unless part of the threat signal spectrum falls within a sensitive part of the system passband. The operation of digital sub-systems is not disrupted, however, the spectrum of the threat energy is modified by the system. In a particular system state the threat energy propagates within the system. As the system changes state the incremental impedances of the active devices also change thus altering the amplitude and phase of the threat energy in the system. The spectrum of the energy within the system, and hence the radiated energy spectrum, is modified. This modification of the energy spectrum may be used to quantify the effect of the RFI on the operation of the equipment

2 As the threat energy level is increased non-linear interactions with the active devices begin to occur, even though the energy is still insufficient to change device states and thus cause the interference to be apparent in the functional state of the system. The non-linearities cause harmonics of the threat energy to be produced which are dependent on

the device states. The system now exhibits enhanced modification to its spectrum, typically manifested as inter-modulation products of the threat and clock harmonic frequencies.

3 As the threat energy is further increased disruption occurs to the digital subsystems, though initially at a level and rate low enough to be masked by software correction techniques. This regime may be detectable in the re-radiated spectrum of the equipment.

4 Eventually the threat energy reaches a level where it causes a repeatable system malfunction. It is then detectable by standard EMC test procedures.

In the first two regimes only dynamic failures occur. As we move into regime three dynamic failures are starting to become likely and in regime four the RFI is at a high enough level for reproducible static failures.

In the first regime the threat RFI is cross-modulated by the digital waveform in the system where the interaction takes place. This will result in the generation of cross-modulation products (CMPs) in the spectrum of the re-radiated field around the frequency of the threat RFI. Thus for an ideal square wave clock signal with period $T_{clock} = 1/f_{clock}$ the re-radiated spectrum will contain CMPs at frequencies given by:

$$f_{threat} \pm m \cdot f_{clock}$$

where $f_{threat}$ is the frequency of the threat RFI and m is an integer. The spectrum of the clock signal will be strongly correlated with the low frequency emission spectrum of the circuit (it will be modified by the transfer function of the coupling path taken by the radiation out of the equipment - an antenna factor). The theory therefore predicts that the cross-modulation of the clock signal and RFI will cause the re-radiated spectrum to have a copy of the low frequency emission spectrum around the threat frequency (see Figure 2). The theory in [2] shows how to predict the magnitude of these CMPs around the threat for a simple circuit. This correlation of the shifted pure emission spectrum and re-radiated spectrum shows that the RFI has penetrated into the clock circuit.

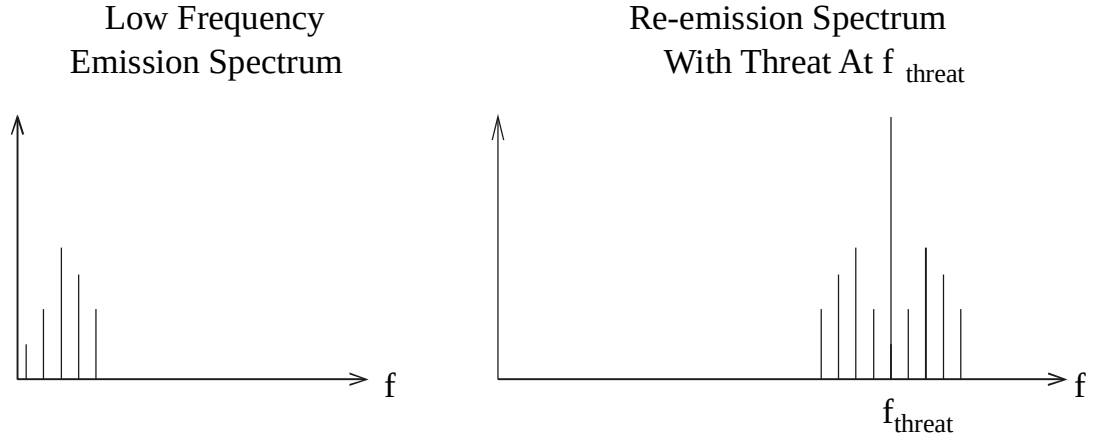


**Figure 2: Correlation of the re-radiated spectrum from a digital circuit subject to RFI with low the frequency emission spectrum.**

In the second regime, with higher levels of RFI, the non-linearities in the devices terminating the transmission lines will start to have an effect. In particular harmonics of the interfering signal may be generated. These harmonics will propagate within the system and also become cross-modulated by the digital waveform on the transmission lines in the same way as the first regime. The non-linearities may also directly generate inter-modulation products (IPs) of the threat RFI and digital signal which will coincide with the CMPs generated by the cross-modulation. This will result in the appearance of CMPs/IPs in the re-radiated spectrum at frequencies:

$$n \cdot f_{threat} \pm m \cdot f_{clock}$$

Note that if $n \cdot f_{threat} = m \cdot f_{clock}$ for some m and n (i.e. the threat and clock frequencies are commensurate) then CMPs associated with $n \cdot f_{threat}$ will coincide with harmonics of the clock signal. In broad terms this will result in the reproduction of the low frequency pure emission spectrum of the digital equipment around harmonics of the threat frequency.

The level of these CMPs depends not only on the high and low impedances of the gates driving the affected subsystem, but also on the non-linear properties of these devices. The prediction of the level CMPs therefore requires non-linear macromodels of the devices in the circuit which are valid for RF signals [3]. Determination of the parameters for these models is generally very difficult.

## 3.3 Correlation Of The Re-emission Spectrum And Equipment Immunity

The theory reviewed in Section 3.2 suggests that the penetration of EMI into digital equipment can manifest itself in the spectrum of the radiation re-emitted from the equipment - that is the re-emission spectrum. The strength of the CMPs in the re-emission spectrum are related to the levels of EMI which has reached the particular subsystem in the equipment concerned. This suggests that the level of CMPs may correlate with the susceptibility of equipment to both static and dynamic failures. The presence of CMPs indicates that a digital subsystem with a spectrum correlated to the CMPs has been reached by the EMI and is therefore susceptible to failure.

This theory has the potential of being the basis of a measurement method which provides a susceptibility profile of a piece of digital equipment. Unlike conventional immunity tests which assess the effect of EMI on equipment under test (EUT) by the observed functional behaviour of the EUT this technique would provided many benefits:

1 It may be possible to measure a full susceptibility profile of the EUT;

2 Even if the EUT does not fail (as determined by conventional measures) an indication of how close it was to failure for a given level of threat field may be given;

3 Software error correction would not mask the fact that EMI is already at a sufficient level to cause interaction with the digital signals in the EUT;

4 The susceptibility profile may also indicate which subsystems in the EUT are susceptible to given threat environments;

5 The technique may also be the basis of an EMC diagnostic tool.

Various indicators of equipment susceptibility may be extracted by comparison of the re-emission, $S_{re}(f)$, spectrum with the pure emission spectrum, $S_{em}(f)$. For example, we can postulate that the following may correlate with equipment susceptibility:

1 The level of CMPs about the threat frequency.

2 The level of CMPs about harmonics of the threat frequency.

3 The total energy in the CMPs,

$$\int |S_{re}(f)|^2 - |S_{em}(f)|^2 \, df.$$

4 The cross-correlation function, $R(f_1,f_2)=<S_{em}(f_1)\, S_{re}(f_2)>$, of the pure emission and re-emission spectrum. As discussed in Section 3.2 this should show peaks when $f_1-f_2=n \cdot f_{threat}$ if the threat EMI has penetrated into the EUT.

Much research and development is needed in this area to confirm that these predictions are valid for the wide variety of digital equipment on the market.

# 4.0 EXPERIMENTS WITH A SIMPLE TEST BOARD

A preliminary test programme was conducted to demonstrate the feasibility of immunity testing methods based on the modulated scattering of RFI from digital equipment. With the limited resources available to this study it was necessary to limit the goals of this testing programme to objectives which could be achieved in a few days of experimental work. The measurement programme therefore set out to accomplish the following:

1 Measurement of the emission and re-emission spectrum from a simple test board.

2 Verification of the theory of the behaviour of the re-emissions spectrum as a function of threat field strength.

3 Demonstration of the measurement of the re-emission spectrum of the test board in a realistic chamber configuration using current EMC test equipment.

The tests were conducted in the Applied Electromagnetic Group's screened room at the University of York. As far as possible the equipment used for the measurements was restricted to standard EMC test equipment available to any EMC testing facility. The only exception to this was the use of two tuneable bandpass filters for suppressing harmonics from the power amplifier and rejecting the directly coupled threat field in the receiver circuit where necessary.

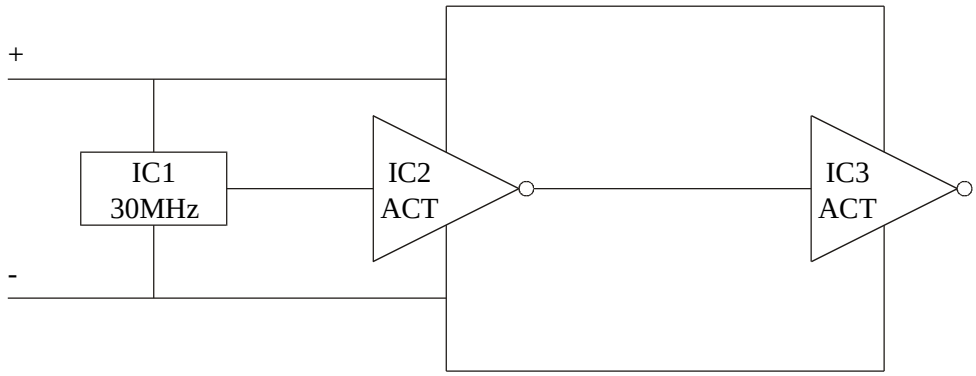


**Figure 3: Circuit diagram of the test board.**

## 4.1 The Test Board

As an initial verification of the technique a simple test board was used with a clean emission spectrum. The circuit, shown in Figure 3, consists of a 30 MHz oscillator module driving a clock signal between a pair of 74ACT CMOS inverters. All the integrated circuits are decoupled with 100 nF ceramic capacitors. The fast edge rates of the ACT CMOS (rise and fall time of 1.1 ns) result in a very board spectral content to the digital signals between the inverters.

The PCB layout is shown in Figure 4. The layout was designed with the oscillator module as close as possible to the first inverter and a large loop between the inverters to minimise the radiation directly from the clock and maximise that from the digital signal between the inverters. A photograph of the board is given in Figure 5.

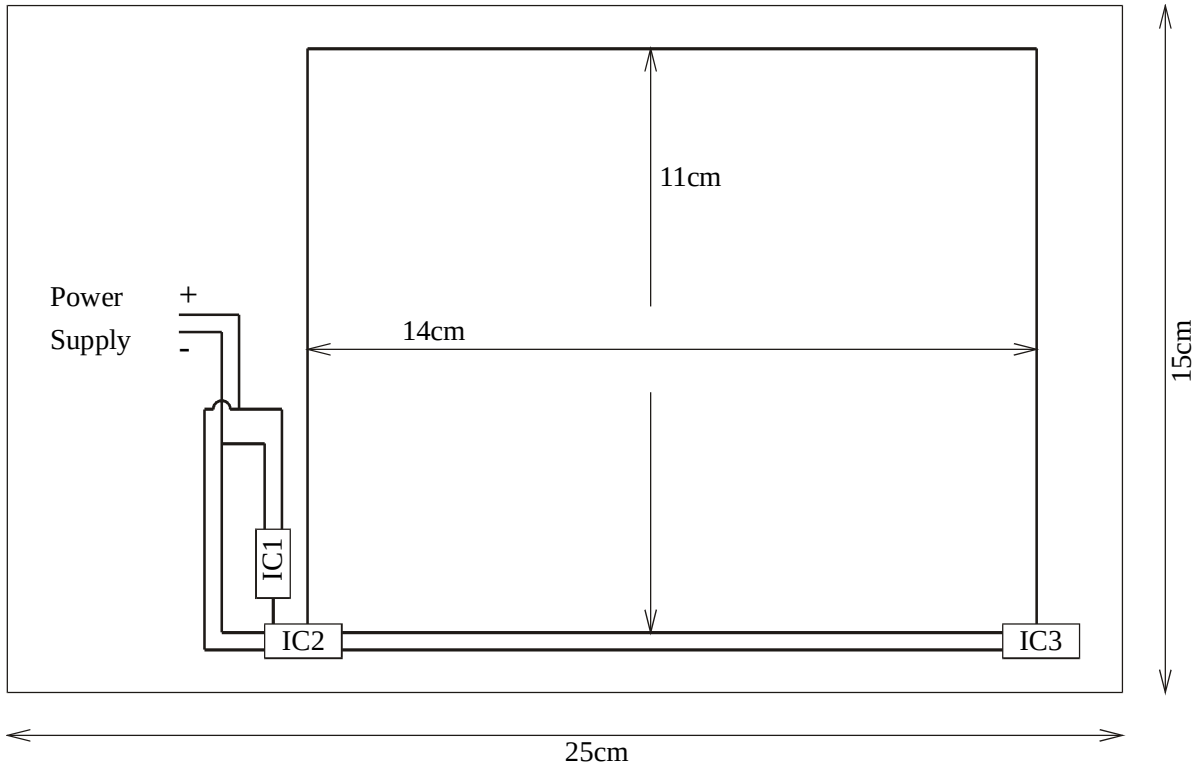


**Figure 4: PCB layout of the 30 MHz test board.**

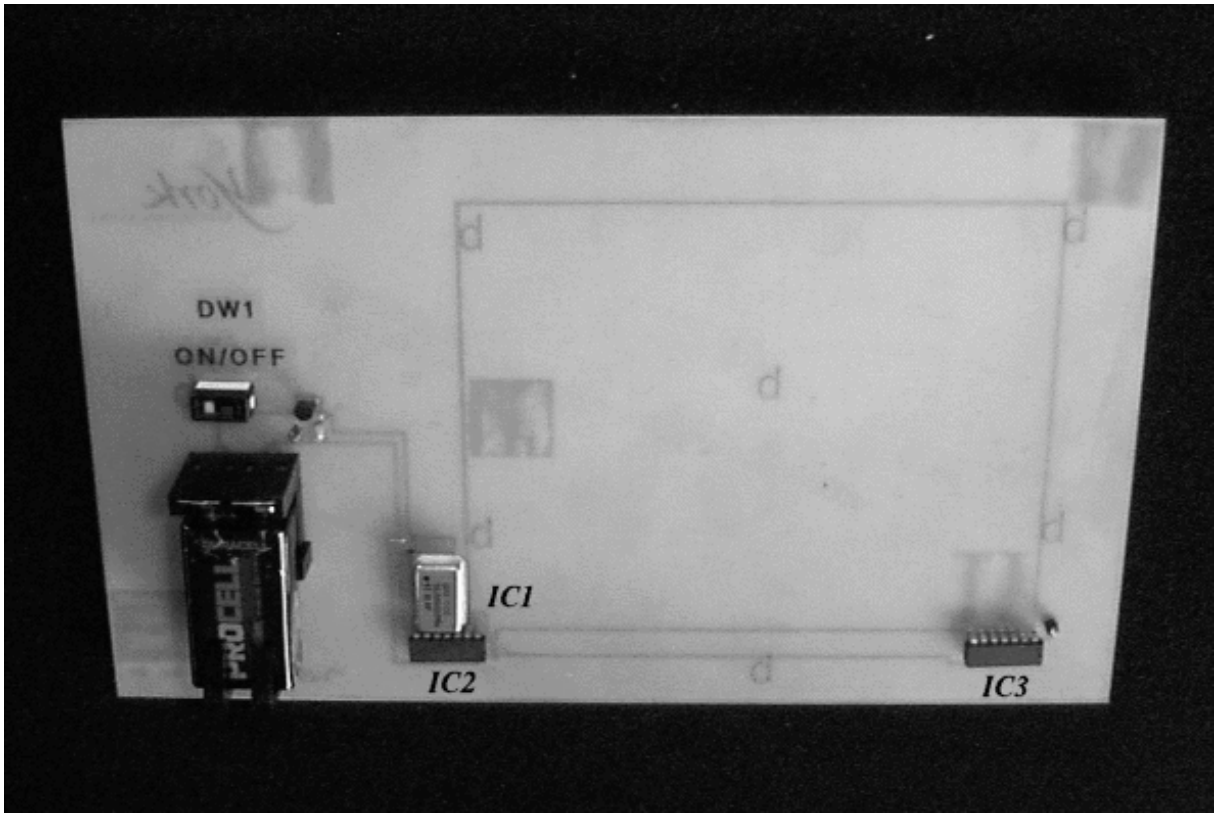


**Figure 5: Photograph of the 30 MHz test board.**

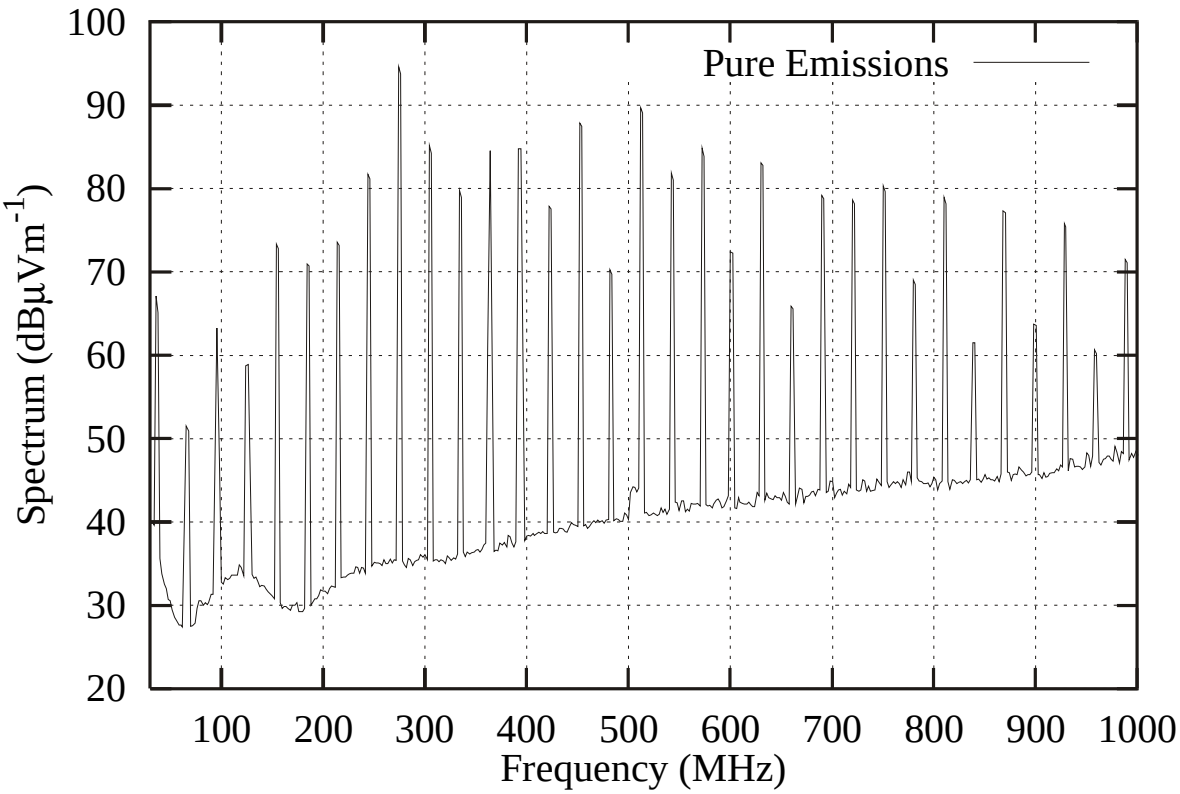


**Figure 6: Pure emission spectrum from the test board.**

This board is a relatively efficient antenna over a wide frequency range. The pure emission spectrum, measured in the screened room with a BiLog antenna is shown in Figure 6. It has strong emissions at harmonics of the 30 MHz clock up to and beyond 1 GHz.

## 4.2 Near Field Measurements

The first series of tests were performed using two small loop antennas placed 3 cm from the board inside the screened room. One antenna was connected to a spectrum analyser and the other was driven from a signal generator with 10 dBm of power. The threat carrier frequency was varied from 400 MHz to 500 MHz.

Figure 7 shows the spectrum radiated from the board when it is subjected to a sinusoidal threat field at 405 MHz, 407 MHz and 410 MHz compared to the pure emission spectrum. The spectra on the left show the CMPs generated around the threat frequency and those on the right the spectra around twice the threat frequency. These spectra are uncalibrated and should be treated in relative terms.

The pure emission spectrum around 400 MHz shows harmonics of the 30 MHz clock at ..., 330, 360, 390, 420, 450, 580,... MHz. With a threat field at 405 MHz CMPs are generated around this frequency at ..., 345, 375, 435, 465, 495,... MHz. Since in this case twice the threat frequency is a harmonic of the board clock all the CMPs around 810 MHz coincide with harmonics of the clock and are not easily seen: the CMPs seen around 810 MHz are from 405 ±€n ·€30 MHz and not CMPs related to 810 MHz.

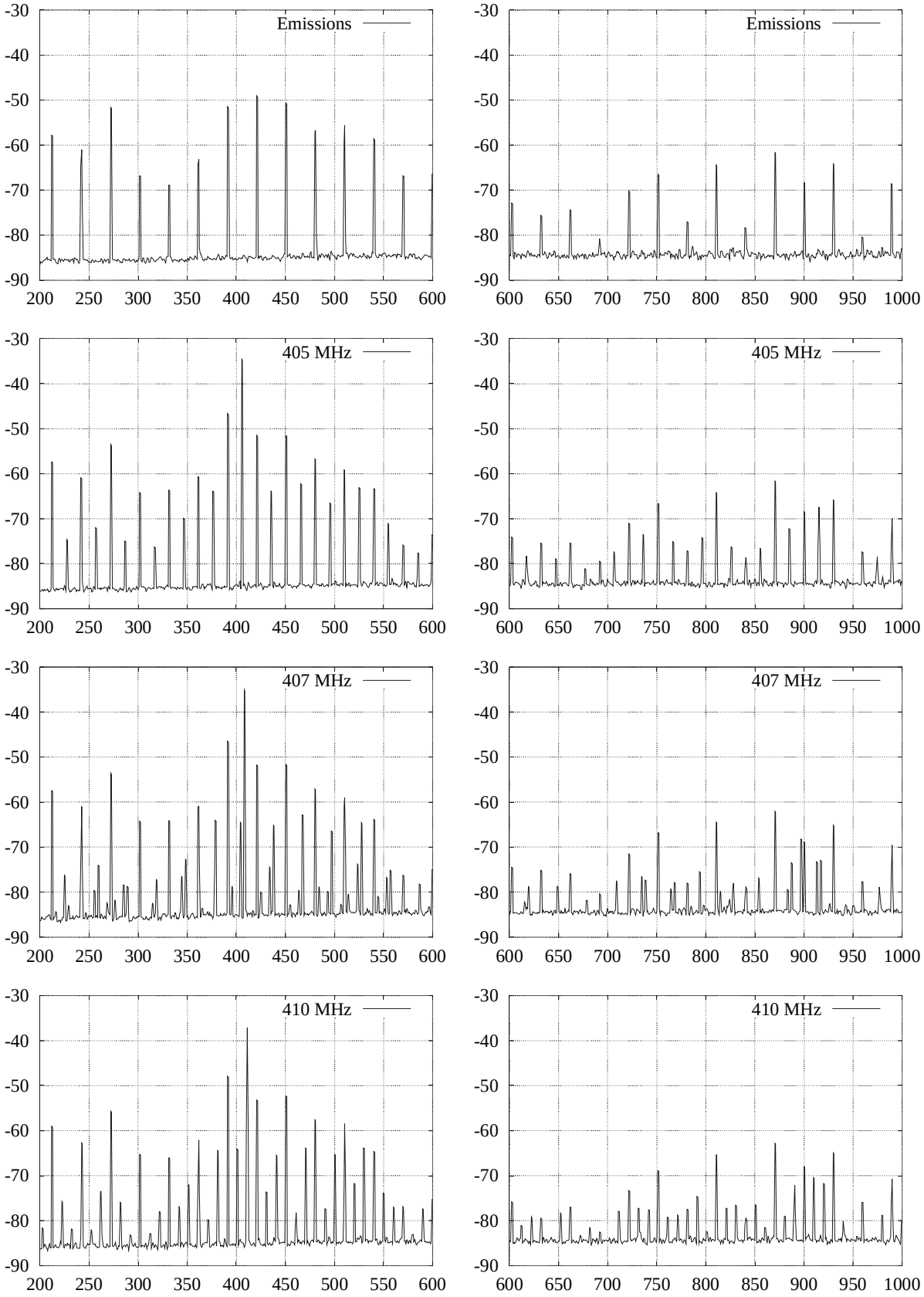


**Figure 7: Cross-modulation products generated by the test board for various threat carrier frequencies. Each plot shows a spectrum in dBm (uncalibrated) against frequency in MHz with the threat frequency given on the graph.**

Shifting the threat frequency to 407 MHz many more CMPs become visible at all frequencies. The CMPs from multiples of the carrier frequency, i.e. $m \cdot 407 \pm n \cdot 30$ MHz, no longer coincide with the clock harmonics and make themselves visible. Similarly with the threat at 410 MHz many high order CMPs are visible. The level of the CMPs increases with increasing threat field strength.

These results confirm the basic theory of the modulated and non-linear scattering technique presented in Section 3.2.

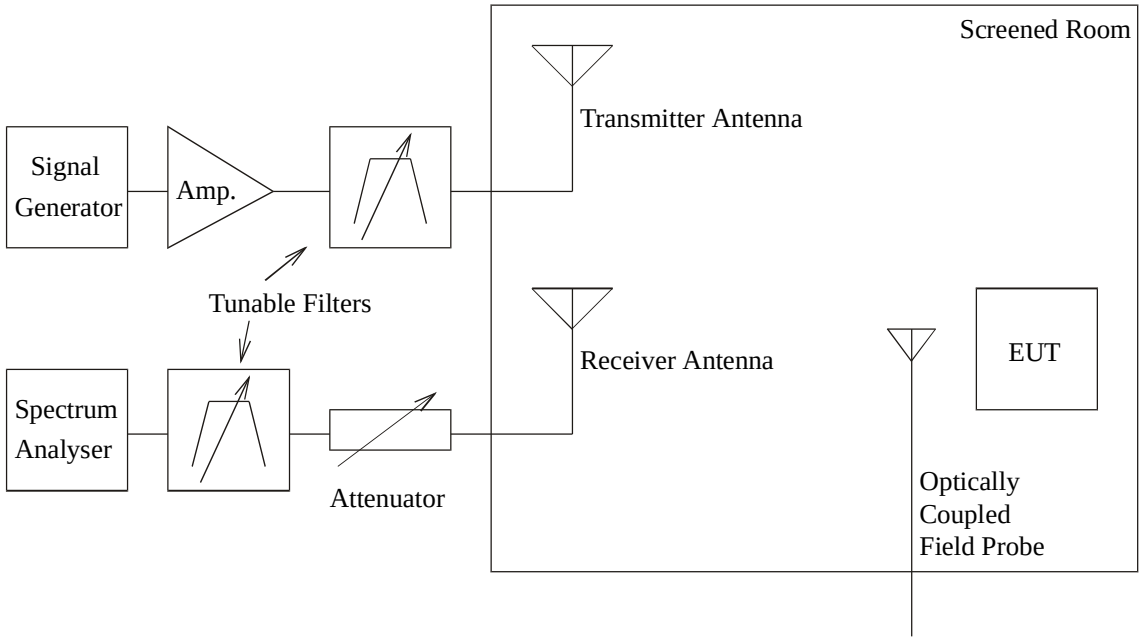


**Figure 8: Screened room test set-up.**

## 4.3 Chamber Measurements

The next stage of the testing program was to verify that the same results could be obtained from the test board in the screened room using a practical test configuration. A second series of experiments were therefore conducted with the arrangement illustrated in Figure 8. The EUT was placed on a wooden table 1m above the floor of the screened room and surrounded by Radio Absorbing Material (RAM) to damp the resonances of the screened room (which was not anechoic). The field strength next to the EUT was monitored with an optically coupled field probe.

Carrier wave threat fields were used, generated by a Marconi signal generator and a 20 W Wessex power amplifier fed via a tuneable bandpass filter with a bandwidth of 20 MHz (adjusted to match the carrier frequency of the signal generator) to a Chase log-periodic antenna in the chamber. The transmitter antenna was placed at distance of 1m from the EUT. The scattered field was detected using a Chase BiLog antenna connected to another tuneable bandpass filter, variable attenuator and spectrum analyser. The receiving antenna was placed at a range of 0.5 m from the EUT and polarised in the same direction as the transmitting antenna. The test equipment in operation is shown in Figure 9.

For some of the measurements the filter in the receiver circuit was left out to allow measurement of the entire re-emission spectrum. This could only be done with low powers of

the threat field to prevent damage to the spectrum analyser. Cross polarising the transmitting and receiving antenna also provides some isolation between the antennas at the threat carrier frequency. (Note that the scattered spectrum from the EUT is generally randomised in polarisation and therefore not significantly reduced by cross-polarising the antennas.)

The board was initially illuminated with a carrier wave field at 505 MHz and cross-modulation products were sought around this frequency, i.e. at $500 \pm n \cdot 30$ MHz = ..., 415 , 445, 475, 535, 565, 595,... MHz. (The bandpass filters available limited us to threat frequencies in the range 500 MHz to 1 GHz for the chamber based method).

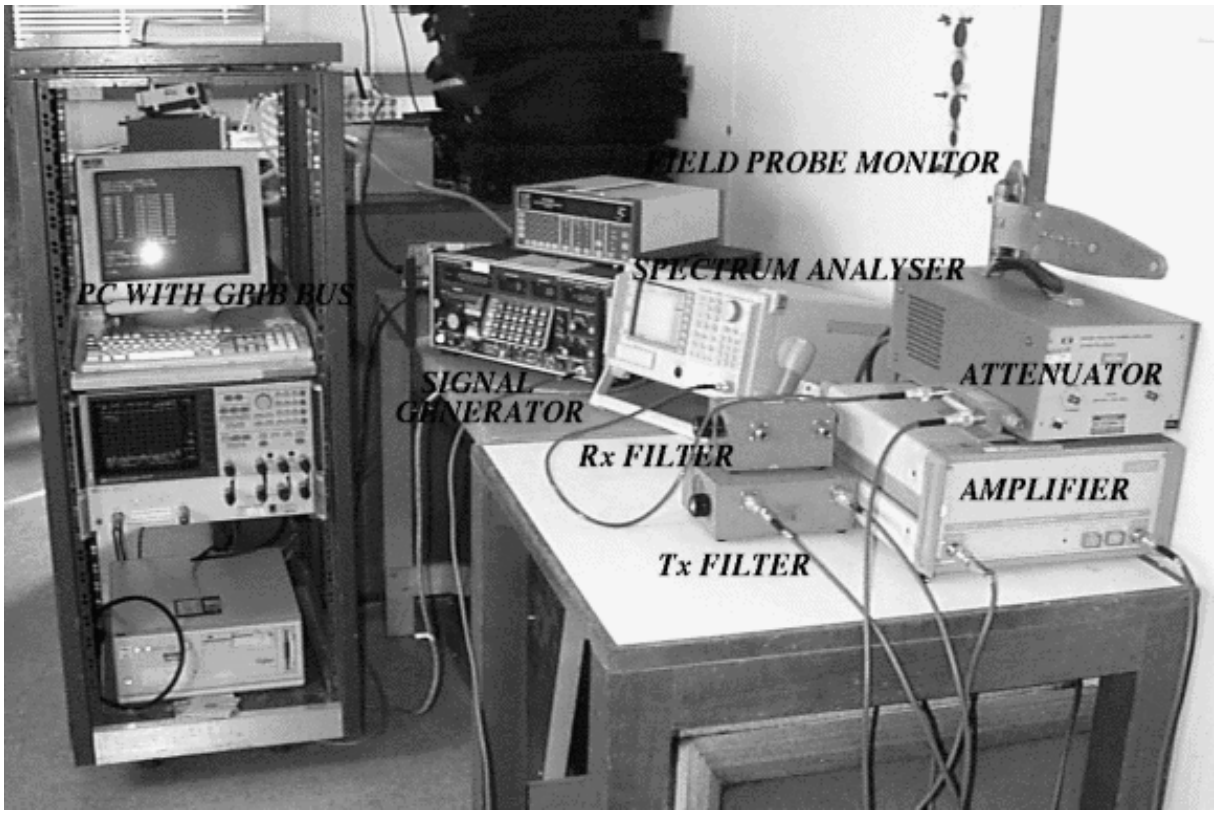


**Figure 9: Test equipment outside screened room.**

Figure 10 shows the pure emission spectrum of the test board from 500 MHz to 600 MHz compared to the re-emission spectrum with a threat field level of 1 $Vm^{-1}$ and 10 $Vm^{-1}$ respectively. The spectrum clearly shows CMPs at the predicted frequencies at 1 $Vm^{-1}$ (and some higher order CMPs). At a field strength of 10 $Vm^{-1}$ many high order CMPs from multiples of the threat frequency are generated.

This demonstrates that the technique works with a relatively simple EUT which has high susceptibility to RF radiation. The trend of increasing CMP level with threat field is also validated. In particular the CMPs around multiples of the threat frequency become significant a higher field strengths. Note that the broad low level spectrum immediately either side of the threat frequency is noise from the amplifier which passes through the 20 MHz bandpass filter. (The 20 W amplifier used in our experiments was of low quality and very noisy. This will not be a problem with the standard high power amplifiers used EMC test houses).

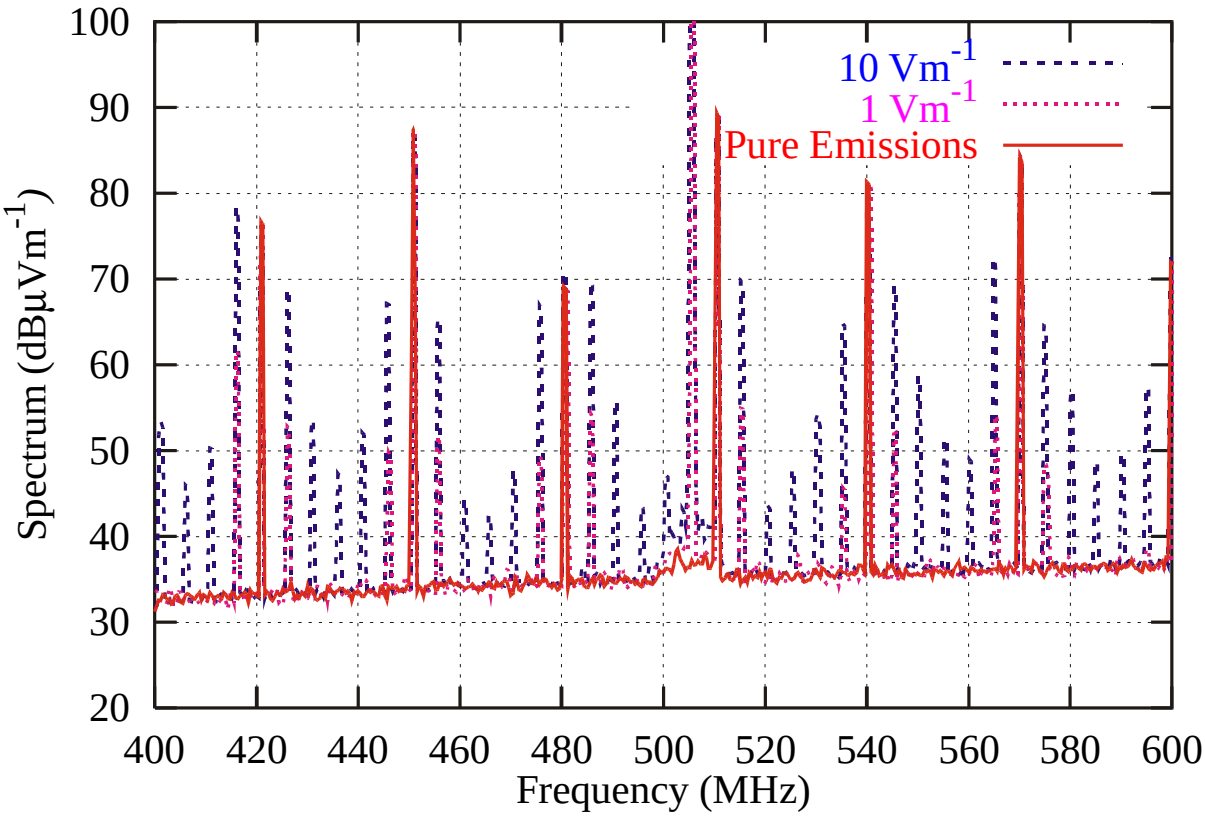


**Figure 10: Scattered spectrum from test board in chamber with 505 MHz threat at 10 $Vm^{-1}$ and 1 $Vm^{-1}$.**

# 5.0 TEST METHODS

The theory in Section 3.0 and measurement program in Section 4.0 have demonstrated that an immunity test for digital equipment based on the scattered radiation spectrum is feasible. There are a number of ways to utilise this technique as part of a test procedure. In this section we explore the different methods which may be employed and discuss their practicality, limitations and what work is needed to develop them into an immunity test. Section 5.1 provides an analysis of the aspects which are common to all of the test methods based on this technique. The technique is applicable to both chamber and cell based measurements; specific test configurations and methodologies for these two approaches are given in Section 5.2 and 5.3 respectively. Section 5.4 looks at the scattered radiation technique in the context of non-sinusoidal threat fields which are necessary to measure equipment susceptibility in complex electromagnetic environments such as those generated by a dense usage of mobile telecommunication systems.

## 5.1 Common Features

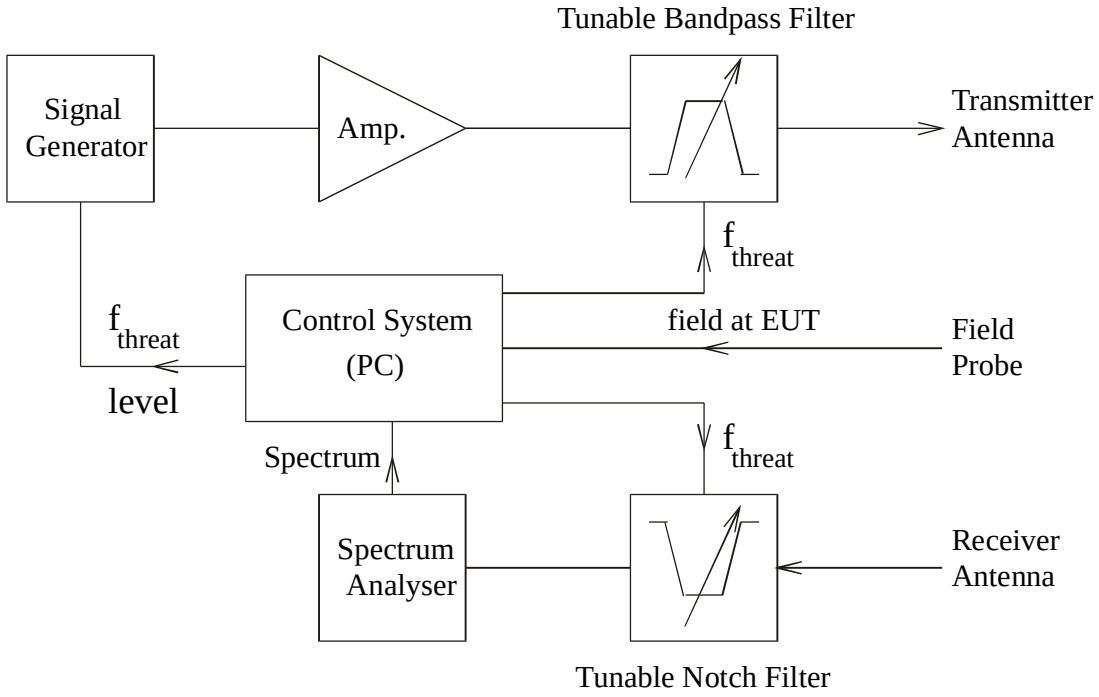


**Figure 11: Block diagram of transmission and reception systems.**

The proposed test methodologies are all based on the same measurement technique: simultaneous irradiation of the EUT with a known threat field and measurement of the resultant spectrum. The transmission and reception circuits for a measurement system based on sinusoidal threats are shown in Figure 11. The same basic system can be used with all the specific chamber and cell based methods in the following section.

The transmission system consists of signal generator driving a power amplifier to generate the threat field. Unless expensive power amplifiers with very low harmonics are used it will be necessary to use a tuneable bandpass filter after the amplifier to suppress any harmonics generated by the amplifier. The technique depends on the determination of cross-modulation products which could be compromised if harmonics of the threat frequency are transmitted at

significant level from the amplifier. In a practical system the tuning of the filter will need to be automatically controlled via a stepping motor. The threat field is monitored by some method so that the electric field strength incident on the EUT can be determined relative to the output level of the signal generator.

The reception circuit consists of another automatically tuneable filter, in this case a notch filter, to attenuate the frequency of the threat field coupled directly into the receiver antenna and a spectrum analyser. The whole system is controlled centrally, for example using a PC and IEEE-488 bus. If it is necessary to monitor cross-modulation products around harmonics of the threat the frequency range of the reception circuit may need to be twice that of the transmission circuit. For immunity testing up to 1 GHz this will require the receiver circuit to operate up to 2 GHz.

The bandwidth of the filter in the transmission circuit can be relatively broad, say 20 MHz, but must have high attenuation at the harmonics of the passband. Making the bandwidth relatively large also relaxes the tolerances required from the automation system. The bandwidth of the notch filter is more critical. It determines the minimum separation in frequency between any CMPs and the threat frequency in the re-emission spectrum below which the CMPs can not be measured. This places a lower limit on the fundamental frequencies of digital signals in the EUT which may be detected. However, harmonics of low frequency digital signals may still lie outside the bandwidth of the notch filter.

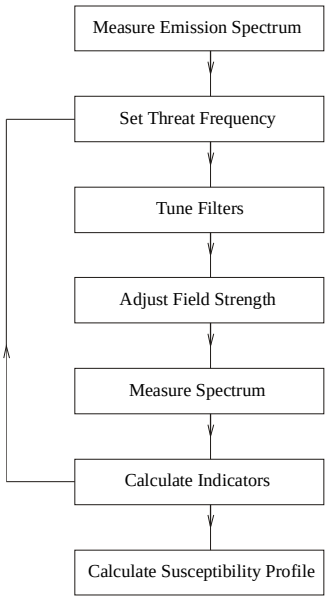


**Figure 12: Measurement methodology.**

The methodology is summarised by the flow chart in Figure 12. The first stage is to measure the pure emission spectrum of the EUT. This is required by the EMC standards anyway, though the parameters of the emissions measurement need to be the same as those used in the immunity measurements to allow comparison of the spectra. The EUT is then irradiated by a sinusoidal threat field at a series of frequencies. At each frequency the signal generator and filters are tuned to the threat frequency and the field strength incident on the EUT is set. The spectrum is then measured by the spectrum analyser and compared by the control system (PC) to the pure emission spectrum. Various susceptibility indicators at the current threat frequency

are then calculated before moving on to the next frequency. The EUT will need to be monitored for an actual failure during the testing so it may be reset if necessary. If the development of the technique is a success the control system may be able to identify characteristics in the re-emission spectrum indicative of a failure and raise an alarm.

The frequency stepping rate can be chosen to match current test techniques though a finer stepping may provide more informative results. The sweep rate (and therefore dwell time) can also be chosen to match current standards though for digital systems with long cycles this may be decreased. At the end of the measurement a complete susceptibility profile of the EUT is available. In fact the technique has the potential for adaptive testing based on the susceptibility indicators measured during the frequency iteration.

Much research is required to develop the technique into a practical EMC immunity test. This work falls broadly in two areas:

1 Establishing the correlation between equipment susceptibility and modulated scattering;

2 Determination of the specifications required by the reception circuit and post processing system.

The second task is dependent on the outcome of the first. At this stage the experimental results are promising but there are many issues to be resolved. The following tasks need to be undertaken to address the first item above:

1 Developing the basic theory of modulated and non-linear scattering at the device level to provide theoretical models of the dependence of the re-emission spectrum on the strength of the threat field and the non-linear profiles of different types of device. This may include development of non-linear RF macromodels for devices.

2 Theoretically correlating the failure of digital equipment (both static and dynamic) with the predicted characteristics of the re-emission spectrum.

3 Correlating the immunity of equipment perceived from its functional behaviour in threat RF fields and the properties of the re-emission spectrum.

4 A comprehensive testing program using both simple, controlled test circuits to validate the theory and equipment of increasing degrees of complexity. This will provide empirical correlation between immunity and the re-emission spectrum.

5 Identifying which properties of the re-emission spectrum are the best indicators of equipment susceptibility based on both the theoretical and experimental results. Set limits for these indicators.

Given the success of these tasks the issue is then one of practicality. This is strongly influenced by the specifications of the reception circuit which follow from the results of the above work. The circuit will need to be sensitive to the minimum level of features in the re-emission spectrum which are shown to be correlated with equipment failure. At this stage of the feasibility study we cannot say what this level is. Determination of this level is one of the primary goals of any further work on this technique. It is therefore difficult to be specific about the type of antenna arrangement needed in the receiver circuit: the proposed techniques in the following sections allow for a number of options.

The worst case outcome could require a number of receiver antennas and a RF switch to give the required sensitivity over the bandwidth of the immunity test [10]. Such an arrangement could use a mixture of current probes, low and high frequency broad-band antennas, and near

field probes placed in various locations relative to the EUT (see Figure 13). This complexity of apparatus should only be considered if absolutely necessary.

Other issues related to the practicality of the method include:

1 Determination of the optimum test parameters (for example, frequency stepping increment, sweep rate) for testing digital equipment.

2 Applicability to low power devices. Equipment which has low emissions due to the low power of signals in the digital circuits and not because of an inherently low coupling to the environment may be particularly difficult to assess. This is again related to the sensitivity of the receiver circuit in the test set-up.

3 Non-digital failures due to analogue subsystems in an EUT. Failures due solely to an analogue subsystem may not be detected. Consideration may need to be given to how the technique would fit into a combined analogue/digital test methodology.

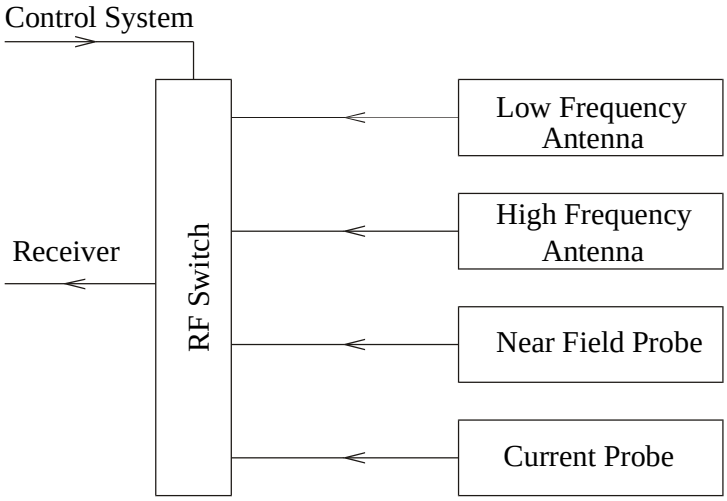


**Figure 13: Using a RF switch in the receiver system to provide a diversity of antennas for the re-emission spectrum.**

## 5.2 Chamber Based Methods

Two implementations of the technique based on chamber measurements are shown schematically in Figure 14. The first, shown in Figure 14(a) is based directly on the methodology employed successfully in our testing programme. The transmission and reception circuits are provided by two standard EMC antennas and the field strength at the EUT is monitored by a field probe. The transmission antenna is placed at 1 m or 3 m as in current immunity tests. The receiving antenna can be placed closer to the EUT.

The second method, shown in Figure 14(b), allows for the possibility of detecting features at much lower levels in the re-emission spectrum by placing the reception antenna directly next to the EUT (see the discussion on the receiver circuit sensitivity in Section 5.1). All the equipment required within the chamber is currently available to EMC test laboratories.

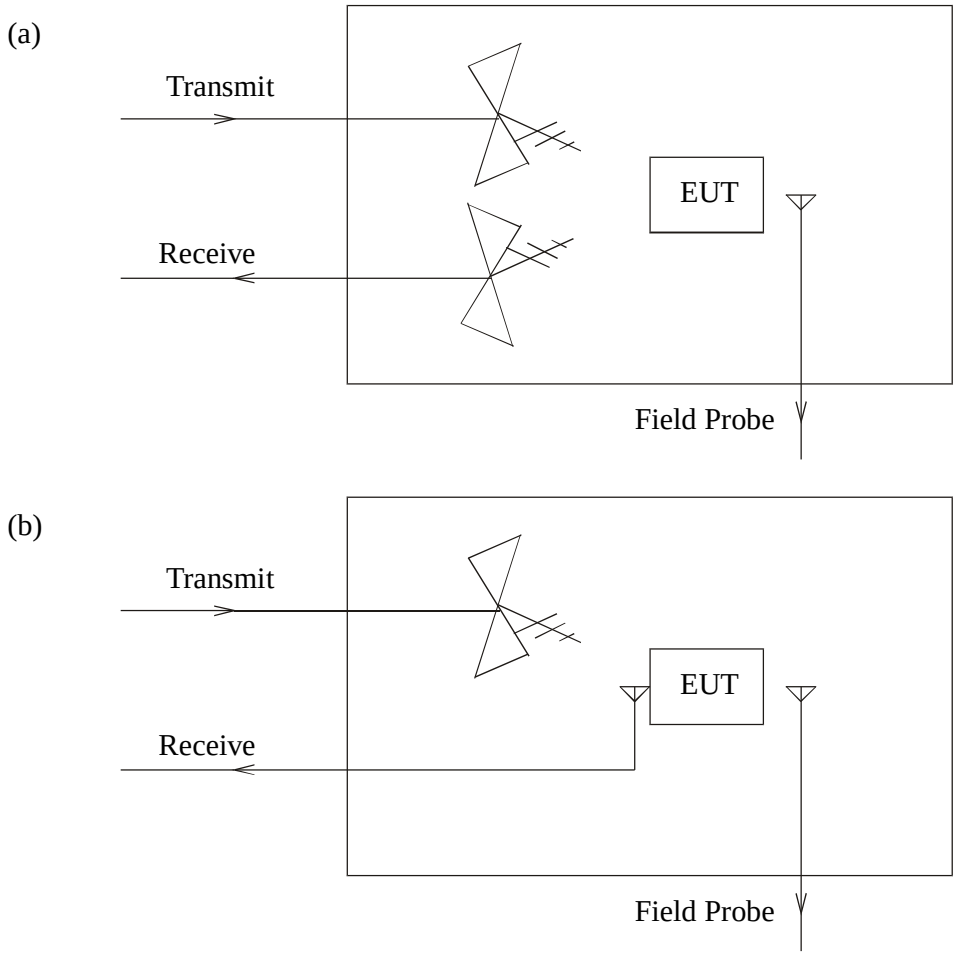


**Figure 14: Chamber based test methods: (a) using a receiving antenna at a distance of one to three metres and (b) using a receiving antenna directly next to the EUT.**

## 5.3 Cell Based Methods

There are a number of different types of TEM test cell available on the market for use in EMC test houses and precompliance testing by manufacturers. One of the most popular is the GTEM cell which can be used for both emissions and immunity testing of EUTs with dimensions up to $1m^3$. Two configurations for implementing the re-emission technique with a GTEM are shown in Figure 15. The field incident on the EUT in such cells in generally inferred from the input power using a calibration so no field probe is required.

The first method, shown in Figure 15(a) uses a directional coupler connected to the drive point of the GTEM to simultaneously transmit and receive RF power. The attenuation from the coupler in the receiver circuit (a minimum of around 10 dB) will reduce the sensitivity of the measurement system. The second method shown in Figure 15(b) in which the reception circuit uses an antenna inside the cell next to the EUT may therefore be preferable.

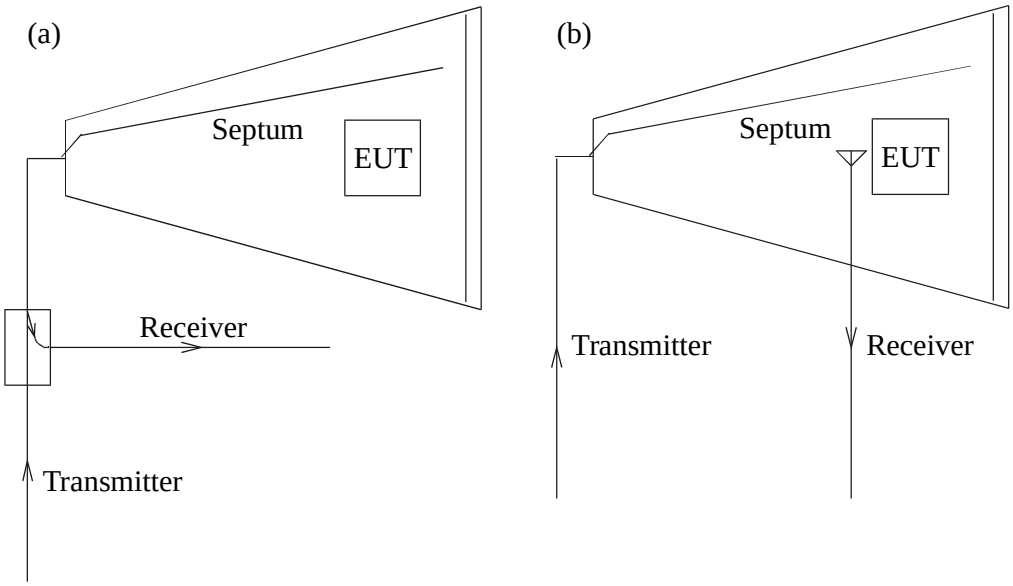


**Figure 15: GTEM test configurations using a directional coupler (a) and a receiving antenna placed inside the cell next to the EUT (b).**

Another approach would utilise a cell with multiple septa such as the EUROTEM developed by Hansen [11]. The Model 2 EUROTEM, shown schematically in Figure 16, uses two pairs of septa, excited with a phase shift of 180$^{o}$ to generate either vertically or horizontally polarised fields . This cell has lower power requirements and is more compact than the GTEM and so may be more attractive for these reasons alone. However, greater utility to the current application is the availability of an eight septa version (the Model 4 shown in Figure 17) which can also generate diagonally polarised fields [12]. The cell may be adapted to use four of the septa for transmission and four for reception with a polarisation angle of 45$^{o}$ between them. This would also provided some isolation between the transmission and reception circuits.

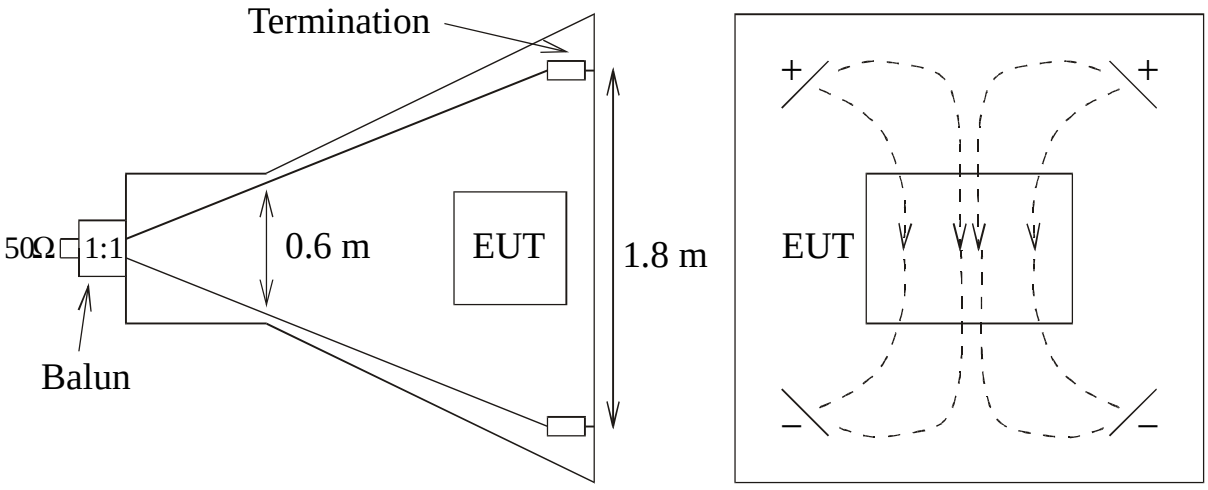


**Figure 16: Schematic of the EUROTEM Model 2 (side view left and cross-section right).**

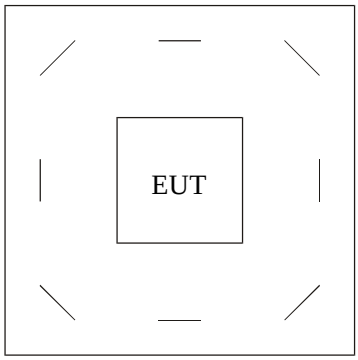


**Figure 17: Cross-section of the EUROTEM Model 4.**

## 5.4 Non-Sinusoidal Test Signals

The test methods discussed so far have implicitly assumed that the threat field being applied to the EUT is sinusoidal. In this section the proposed modulated scattering technique in quantifying equipment susceptibility to more complex threat fields is explored.

The first thing to note is that even with a sinusoidal threat field the modulated scattering approach potentially provides much more information than measuring a yes/no immunity figure at each frequency (though if the EUT is observed during the test this is done as well a The EUT susceptibility profile is determined for discrete frequency fields across the whole spectrum. Even if the equipment does not malfunction, a strong indication of coupling of RF into the equipment across a band of frequencies may indicate a potential immunity problem with certain threat environments.

For example, if some piece of equipment showed strong cross-modulation products in its re-emission spectrum with incident fields over the 380-420 MHz frequency band it is potentially at risk from TETRA PMR systems which operate in this band. Some equipment is particularly sensitive to the low frequency pulse modulation on mobile radio systems such as TETRA which use Time Division Multiple Access (TDMA) technology. Current EMC standards do not require testing equipment with this type of modulation so equipment may pass the EMC tests and still be susceptible to relatively low fields strengths from this type of system. The test techniques proposed here however offer the possibility of detecting that RF energy in the 400 MHz range has entered the digital systems of the equipment and quantifying the degree of this ingress.

One application of the technique would therefore be as a guide for more selective testing against particular threats in the measured susceptibility bands of the EUT. The susceptibility profile would identify the frequency windows in which the EUT interacts with RFI allowing more specific threats to be applied within these frequency bands. For example, the LINK Personal Communication Programme EMC Project will propose a test for environments consisting of multiple narrow band TDMA sources (such as TETRA, GSM, PCN and DECT) using a two level swept pulse modulation scheme [13]. A low frequency pulse modulation is used to simulate the TDMA and a high frequency pulse modulation is used to represent the short duration "spikes" in the ensemble field caused by multiple sources coming instantaneously into phase. The parameters for this high frequency pulse modulation are based on the statistics of ensemble fields determined by the project. A number of severity levels based on the number of transmitters have also been defined.

The technique can also be applied directly to non-sinusoidal threats, however the correlation techniques required to determine the degree of interaction with the EUT are then more complex. For example band limited Gaussian noise up-converted by double side band modulation has been proposed as a threat field for immunity testing [14]. The transmission circuit for this type of test is shown in Figure 18.

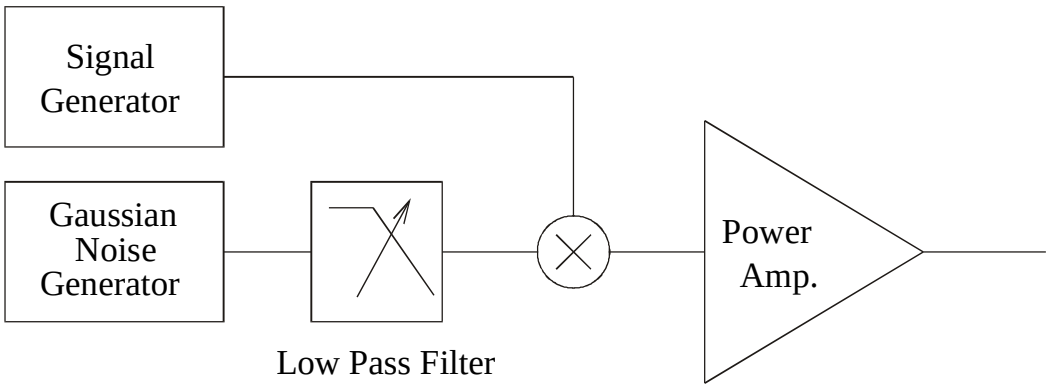


**Figure 18: Band limited Gaussian noise threat field generation.**

This generates a noise like spectrum, with a bandwidth twice that of the low pass filter, around the frequency of the signal generator. More complex noise sources with programmable amplitude probability distributions have also been considered [15].

An alternative method of generating a threat field with a noise like polarisation and amplitude based on an extension of a field rotating method [16] is proposed here. The method is illustrated in Figure 19. Two orthogonal antennas are fed with quadrature carriers which have been modulated by two identical noise sources $n_1(t)$ and $n_2(t)$. The x and y components of the resultant electric field are given by:

$$E_X(t) = a \cdot n_1(t) \cdot \cos(\omega_0.t)$$

$$E_Y(t) = a \cdot n_2(t) \cdot \sin(\omega_0.t) = a \cdot n_2(t) \cdot \cos(\omega_0 t - \pi/2)$$

where $\omega_0$ is the carrier frequency and a is the amplitude of the signal generator. This generates a field with a random amplitude and polarisation given by:

$$|E(t)|^2 = a^2 \cdot [\, n_1^2(t) \cdot \cos^2(\omega_0 t) + n_2^2(t) \cdot \sin^2(\omega_0 t) \,]$$

$$\tan \theta(t) = n_2(t) \cdot \tan(\omega_0 t) / n_1(t)$$

The statistics of this field are determined by the properties of the noise sources. If the noise sources are bounded by $0 \le n_{1,2}(t) \le n_0$ the magnitude of the electric field is bounded by $0 \le |E(t)| \le a \cdot n_0$ and has a RMS value of $E_{rms} = a \cdot n_{rms}$. In fact any direction perpendicular to the direction of propagation of the electromagnetic field will see a randomly varying electric field with the same statistics. The EUT will therefore be irradiated with a field which exhibits a random field amplitude in all directions.

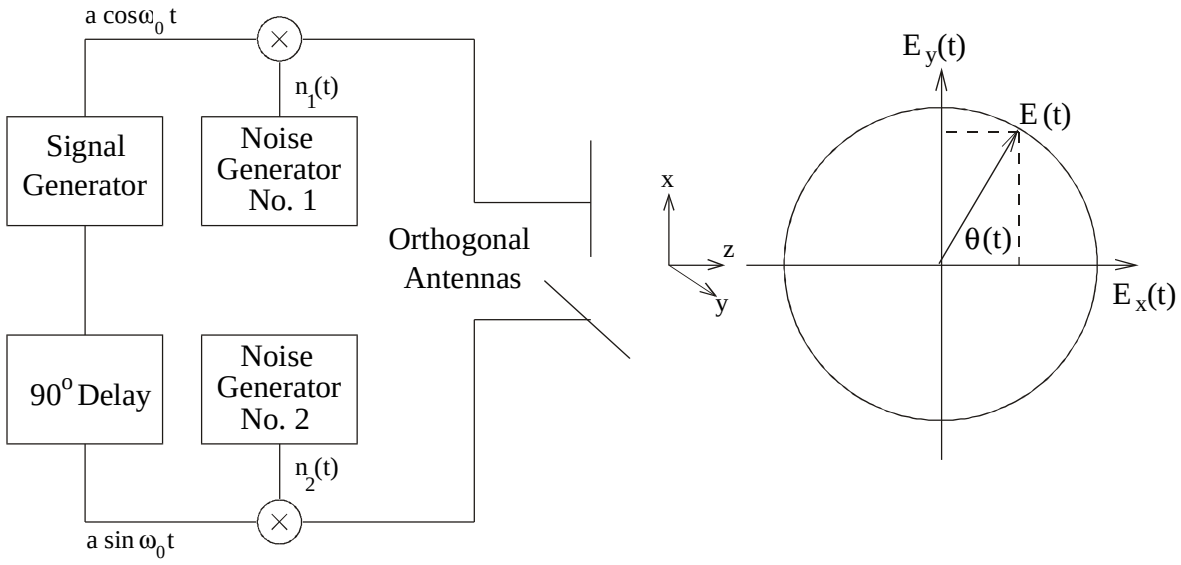


**Figure 19: Field rotation method using orthogonal antennas and noise sources.**

This type of threat field could be implemented by appropriate phasing of the four septa in a Model 2 EUROTEM or similar cell (see Section 5.3). In fact using the Model 4 EUROTEM with eight septa it may be possible to apply this randomly polarised threat field to an EUT using four of the septa and use the remaining septa to measure the re-emission spectrum. This would provide a compact and convenient way to use the modulated scattering technique in conjunction with a probabilistic threat field.

The re-emission spectrum from an EUT subject to complex threats can be measured but the determination of the degree of interaction with the EUT will require complex real time cross-correlation techniques. Relating the results to the immunity of an EUT will also be much more difficult than with sinusoidal fields. As such the method proposed above must be considered conjecture until the modulated scattering technique is proven with simple threat fields.

# 6.0 CONCLUSIONS

The re-emission spectrum of digital hardware under the influence of RFI provides a great deal of information about the coupling of the RFI to the equipment. This modulated scattering of RFI from digital equipment is potentially the basis of a powerful immunity testing technique.

The theory of modulated and non-linear scattering has been reviewed in the context of equipment susceptibility and shown how the re-emission spectrum from digital equipment may correlate with equipment immunity. The feasibility of the modulated scattering technique has been successfully demonstrated, experimentally for quantifying the susceptibility of digital equipment. Specifically it has been shown that:

1. The re-emission spectrum of a simple test board can be measured in a realistic chamber based test environment using current EMC test facilities;
2. The behaviour of the re-emission spectrum of the test board agrees with theory;

The technique potentially has many benefits including:

1. quantification of equipment immunity;
2. indication of how close to failure an EUT is for a given level of threat;
3. generation of a susceptibility profile for the EUT;
4. independence from software error correction;
5. provision of useful diagnostic information;
6. potential to aid the statistical estimation of EUT immunity in different types of threat environment;

At this stage it is not clear if the correlation between the re-emission spectrum and actual failure of digital systems is itself rigorous enough to be used as the sole criterion for a immunity test outcome. However it has been shown how the technique may be used to identify the frequency bands in which RFI couples to digital circuits. This information could then be used for more specific tests appropriate to each susceptibility window. This could be of great benefit in targeting immunity tests, especially as the upper frequency of immunity tests is increased, possibly to 18 GHz.

The areas for further research identified by the study include:

1. extension of the theory of modulated scattering to account for the type of logic used in the system. This will help quantify and bound any EUT dependent effects;
2. modelling of simple circuits to provide information on the correlation between the re-emission spectrum and static and dynamic failures of the circuits;
3. experimental measurements of the correlation between the re-emission spectrum and device failure using specialised test boards in which the digital waveforms can be monitored;
4. an empirical test programme applying the technique to real equipment, particularly equipment which is difficult to assess using current methods;
5. determination of the most reliable susceptibility indicators which can be extracted from the re-emission spectrum;

6. determination of the minimum level of feature in the re-emission spectrum which is correlated with EUT failure at a given level of threat. This defines the sensitivity of the receiver system required in an immunity test.

A number of test methodologies, both chamber and cell based, have been proposed based on this technique. We have also investigated how the technique may be used to assess the susceptibility of equipment to more complex threat fields such as those generated by mobile telecommunication systems.

# 7.0 REFERENCES


[1] D A Townsend, T J F Pavasek and B N Segal, "Breaking All the Rules: Challenging the Engineering and Regulatory Precepts of Electromagnetic Compatibility", IEEE 1995, Int. Symp. Electromag. Compat., Atlanta, 1995, pp. 194-199.

[2] T Konefal and A C Marvin "Prediction and Measurement of EMC Radiated Immunity Problems in Interconnected Digital Systems", IEE Proc. Sci. Meas. Technol., Vol. 141, No. 6, 1994, pp. 464-470.

[3] T Konefal and A C Marvin, "UHF Inter-modulation Product Prediction in Digital Systems Using SPICE: The Need for Non-linear Macromodels", IEE Proc. Sci. Meas. Technol., Vol. 143, No. 5, 1996, pp. 313-318.

[4] D J Kenneally, D S Koellen and S Epshtein, "RF Upset Susceptibility Of CMOS And Low Power Schottky D-Type Flip-Flops", Int. Electromag. Compat. Symp. Rec., Denver, CO, May 1989, pp. 190-195.

[5] J F Chappel and S Zaky, "EMI Effects and Timing Design for Increased Reliability in Digital Systems", IEEE Trans. Circuits and Systems I, Vol. 44, No. 2, pp. 130-142, 1992.

[6] M P Robinson, T M Bension *et. al.*, "Effect of component choice on the immunity of digital circuits", EMC '96 ROMA, Int. Symp. Electromag. Compat., Rome, 1996, pp233-236.

[7] J-J Laurin and S G Zaky, "On the Prediction of Digital Circuit Susceptibility to Radiated EMI", IEEE Trans. Electromag. Compat., Vol. 37, No. 4, 1995, pp. 528-535.

[8] R Vick and E Habiger, "The Dependence of the Immunity of Digital Equipment on the Hardware and Software Structure", 1997 Int. Symp. Electromag. Compat. Proc., IEEE, New York, 1997, pp. 383-386.

[9] S Wendsche and E Habiger, "Using Reinforcement Learning Methods For Effective EMC Immunity Testing Of Computerised Equipment", EMC'96 Roma, Int. Symp. Electromag. Compat., Rome 1996, pp. 221-226.

[10] S. Sebastiani, "Characterisation to a TEMPEST testing laboratory and methodology for control to compromising emanations", IEEE 1998, Int. Symp. Electromag. Compat. Denver, 1998, pp. 165-170.

[11] D. Hansen, J Funck, D. Ristau and S. Moessler, "Comparing the Field Quality of the New EUROTEM to GTEM and Fully Absorber Lined Chambers", IEEE 1998, Int. Symp. Electromag. Compat. , Denver, 1998, pp. 132-136.

[12] EES Web Pages, URL http://www.euro-emc-service.de/rd.htm.

[13] LINK PCP EMC Project, Draft Final Report.

[14] D R Kempf, "A Comparison of the Isotropic Broadband Susceptibility Test Method and an RS103 Test on an ARC-182 Radio", IEEE 1994, Int. Symp. Electromag. Compat., Chicago, 1994, pp. 54-57.

[15] M Tanaka, K Sasajima and H Inoue, "Programmable Composite Noise Generator (P-CNG)

and Its Application to the Opinion Test on TV Picture Degradation", IEEE 1998, Int. Symp. Electromag. Compat. , Denver, 1998, pp. 270-275.

[16] K Murano and Y Kami, "New Radiated Immunity Test Method Using Fields of Low Speed Rotation", IEEE 1998, Int. Symp. Electromag. Compat. , Denver, 1998, pp. 731-733.

[17] S R Wendsche, “Improved statistical and self-adaptive method for EMC-immunity testing of computerized equipment”, 1995 IEEE International Conference on Systems, Man and Cybernetics, IEEE, New York, 1995, Vol. 4, pp.3368-73.