

Innovative Magnetic-Field Array Probe for TRUST Integrated Circuits

Yoann Tagro¹, Jonmei J. Yan¹, Donald F. Kimball¹, Houman Ghajari¹ and Daniel Sievenpiper²

¹MaXentric Technologies LLC, San Diego, CA
²University of California, San Diego, La Jolla, CA

Abstract: Over the past decade counterfeiting of electronics technologies have become an important issue. Despite all actions and concerns, this problem continues to escalate due to offshore fabrication of the integrated circuits ICs [1]. In order to satisfy this growing security demand, we have designed a magnetic field probe array that has potential to create a system capable of identifying the functionality of component elements of ICs, identifying malicious circuitry (Trojan), physical and electrical faults in ICs, compare ICs to known good circuits for the purpose of quality control. Measurement results with the designed EM probe demonstrated an operating frequency range from DC to 5GHz, an isolation between each loop of about 40dB, a dynamic range of 25 dB between the ON and OFF state of the probe, and the capability to map in real-time an IC device. This non-invasive solution is cost effective, with a small form factor.

Keywords: Electromagnetic radiation; Near-Field; H-field; Probe Array; Counterfeit Detection; IC Trust.

Introduction

Counterfeiting is a huge flail that still continues to serve in the electronics industry despite industry's good will and best efforts to eliminate it.

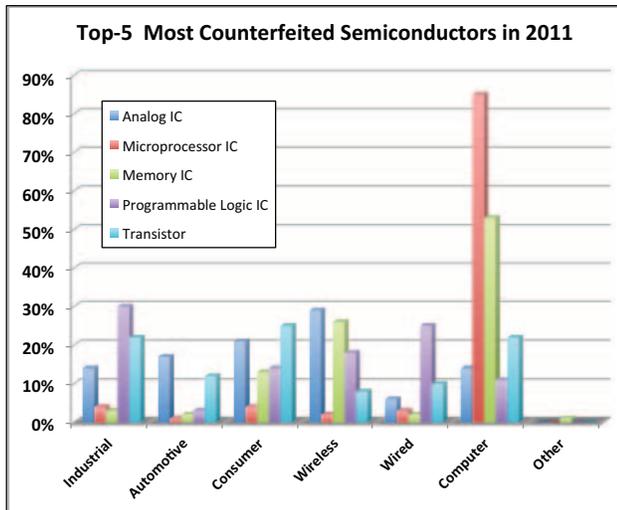


Figure 1. Percentage of market revenue for most commonly counterfeited products by application market.

According to [2] and figure 1, the top 5 counterfeited semiconductor parts that have widespread commercial and military represent upmost \$150 billion in potential annual

risk for the global semiconductor market. 2011 was a record year for counterfeit reporting, and incidents of counterfeit parts have tripled during the past two years. However, it becomes paramount to help industry to overcome this problem. The main challenge for this solicitation was to design, develop and fabricate a low cost electromagnetic probe array for ICs counterfeit. The probe array should operate in the near field domain with a high sensitivity, high resolution and should have a potential to create a system to identify functionality of component elements of ICs.

Measurement of electric and magnetic fields provides an avenue for the mapping of the fields in an operational device. The field maps illustrate the physical behavior of the ICs and demonstrate how signals and waves propagate inside the device. The field mapping can be used in the diagnosis and fault isolation in ICs, as well as the characterization of the functionality of ICs including malicious circuitry. Integrated circuits emit both electric and magnetic fields although usually one field dominates. The H-Field can be captured with a probe in a loop while the E-Field is captured with a monopole probe.

In this study, we present a description of the overall system used. Next, the test bench setup is described along with the characterization of a 50-Ohm transmission line is used to validate the performance of our new system. Finally, a real-time characterization of an active device (MaXE1.0™) is presented.

System Description

Figure 2 shows the top-down block diagram of the cost-effective EM scanner probe.

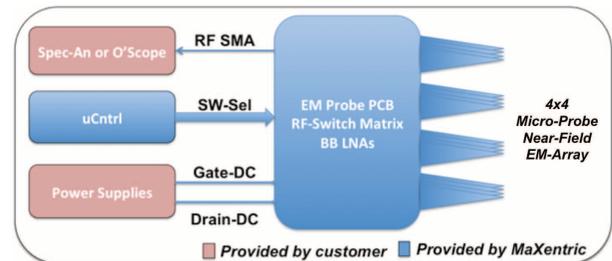


Figure 2. Block Diagram of MaXentric's EMPA Probe

The base tile is a 4x4 micro-probe near-field EM-array mounted on a Rogers material 20mil thick dielectric substrate with 2 metal layers on the outside. The PCB also

contains the RF-switch matrix and broad-band (BB) low noise amplifiers (LNAs). Our overall effort was focus on modeling, designing, fabricating, and utilizing novel electromagnetic probes for the analysis, characterization, and exploitation of EM signals and waveforms. The output is a single coaxial RF connector (e.g. SMA) with an output switch matrix, allowing each loop of the probe to be serially addressable one at a time for fine resolution probing, and raster scanning. The single output RF coaxial connector interfaces with a spectrum analyzer, vector signal analyzer, and/or an oscilloscope for scanning purpose. The switch selection is currently accomplished through an external microcontroller (from measurement computing) that allows the array to be scanned digitally in a variety of patterns to facilitate post-digital signal processing. A power supply provides separate gate and drain DC biases for the RF switches and LNAs.

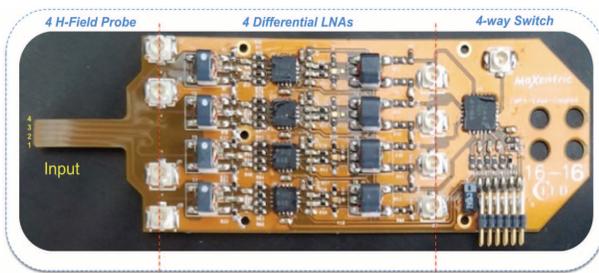


Figure 3. Picture of the fabricated 4x1 array probe

Figure 3 shows the fabricated 4x1 H-Field array probe. The probe array can be used to evaluate semiconductor technologies for failure analysis, root cause investigations, and supply chain monitoring among other applications.

When selecting a probe for near field-testing, the sensitivity, the resolution, and the frequency response are important factors to consider. Inasmuch as the sensitivity of close field probe is not an absolute value, one needs to evaluate the sensitivity of the spectrum analyzer and probe together as a system. The entire system should be able to detect small and any change of emissions before and after hardware modifications. Resolution is a probe’s key to locating emission sources. Trade-off between sensitivity and resolution is mostly observed for a single probe. The larger the size of the H-field probe is, the better is the sensitivity, and the less is the resolution (making it difficult to isolate a precise source of emission). Finally, the frequency response is an important factor, but commonly overlooked.

Test Bench Set-up and Probe Evaluation

Figure 4 shows the test bench used to characterize the fabricated probe. Using a passive element as the device under test (DUT), the injected signal from the signal generator drives the 50 Ω microstrip transmission line terminated with a 50 Ω BB load. The current flows in the direction of the transmission line generating a magnetic

field in the zy-plane, which is approximately constant along the x-direction. The EM probes capture the magnetic field with the probe tip placed as close as possible to the trace ($H \sim 0$ mm). This is possible due to the robustness of the flexible loops used at the probe tips. The spectrum analyzer receives the output signal from the probe. Operating the probe loops parallel or perpendicular to the current flow will result in a maximum and minimum capture of the H-field, respectively. Thus, the difference between these two measurements can be used to evaluate the suppression capability of unwanted field components of the probes. The EM probe operates from few kHz up to 5GHz.

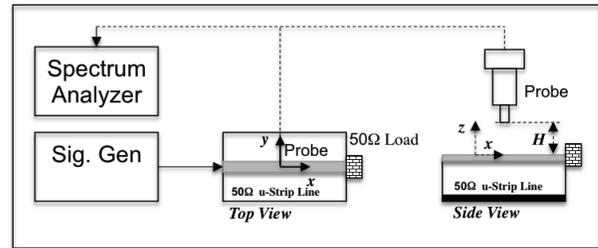


Figure 4. Frequency Domain test bench – Probe evaluation over a 50 Ohm microstrip transmission line

Figure 5 shows the coupling factor of each loop of the 4x1 H-Field probe array. This measurement has been performed using the same test bench described in Figure 4. However, a two ports vector network analyzer (VNA) is used in place of the spectrum analyzer and the signal generator.

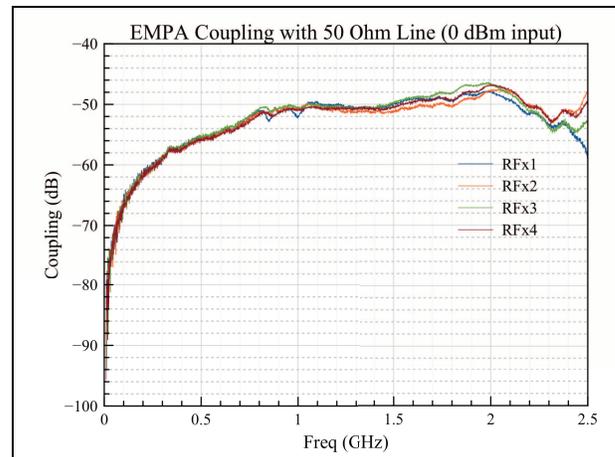


Figure 5. Characterization of the probe coupling versus frequency

The input port (port 1) of the VNA is connected to the 50-Ohm transmission line terminated with a 50-Ohm BB-load. The second port of the VNA (port 2) is connected to the probe array, and the transmission line is then excited with 0dBm input signal. The probe in quasi-contact with the transmission line is oriented in a manner to capture the maximum amount of magnetic field. The transmission coefficient “coupling-factor” (S21) is then measured. Each

curve in Figure 5 represents the S21 of each loop of the 4x1 probe-array. RFx1 for the first loop up to RFx4 for the fourth loop. The measured coupling is about -50dBm between 0.8 GHz and 2.5 GHz and a variation is observed from -70dBm to -50dBm between 0.1GHz and 0.8GHz.

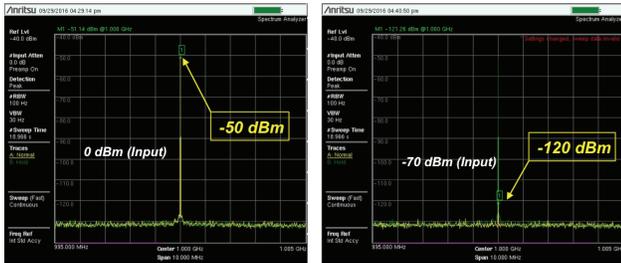


Figure 6. Probe coupling and minimum detectable signal performed at 1GHz

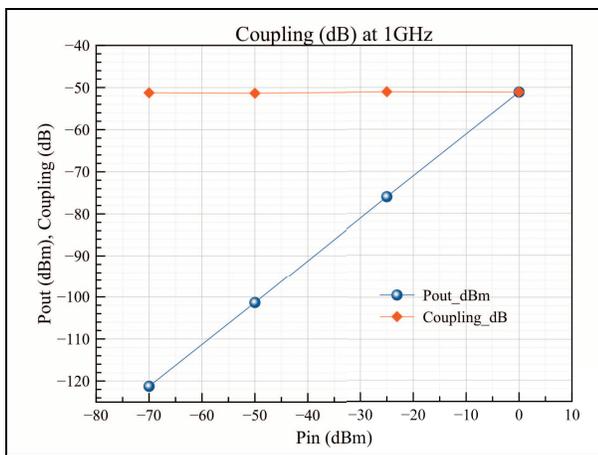


Figure 7. Probe coupling and minimum detectable signal performed at 1GHz

We have then evaluated the sensitivity of our probe array at 1GHz using the test bench (Figure 4) described above. The terminated 50-Ohm transmission line is connected to a signal generator and the probe array is connected to a spectrum analyzer. We vary the injected input signal from 0dBm to -70dBm and observe the captured response on the spectrum analyzer. As explained above, the sensitivity test of a probe has to be taken in consideration using the probe and the spectrum analyzer as a system. The spectrum analyzer is then set-up at its best condition to be able to observe a signal as low as possible. Figure 6 and 7 present respectively the spectrum response for an injected signal of 0dBm and -70dBm, and gathered response from -70dBm to 0dBm. An output power of -120dBm (10dB higher than the noise floor ~ -130 dBm) is observed for -70dBm input signal. As a result, we can observe that the minimum detectable signal strongly correlated to the probe coupling and the noise floor of the spectrum analyzer.

These tests serve as validation towards the feasibility and functionality of our probe array.

Measurement of a magnetic field distribution over a real ICs (MaXEA1.0™)

For the active DUT test, the MaXentric MaXEA1.0™ (5x5mm QFN) was used. It is an integrated envelope modulator designed in a high voltage silicon process [3]. MaXEA1.0™ is part of the MaXentric Technologies GreenAmp™-Lite Envelope Tracking (ET) product line, and provides a wideband high efficiency RF power amplifier solution. The following input signal (700KHz sine wave, with a 1.4V peak-to-peak, and a 1.2V DC offset) is used for the measurement.

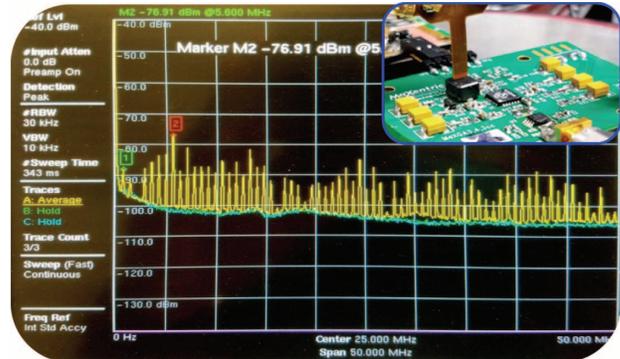


Figure 8. Probe over the magnetic inductance

Using the test-bench in Figure 4 the real-time scan of the entire evaluation board (MaXEA1.0™) was performed with an emphasis on the QFN IC. In Figure 8 (inset) only the encapsulated magnetic inductor was probed, and the flexible probe tips were not in contact with the DUT. The encapsulated inductor consists of a coil of wire loop. A constant electric current running through an inductor produces a magnetic field. This magnetic field is proportional to the number of wire loops and to the amount of current. The experiment was performed at 700KHz; however, the frequency response of the scan shows expected results from DC to 50MHz.



Figure 9. MaXEA1.0™ scanned with the fabricated probe

In Figure 9 the flexible probes tips were placed just above contact with the MaXEA1.0™ and the scan is performed along the entire surface of the IC. The width of MaXEA1.0™ is about two times the total width of the

array probe. In order to avoid redundancy of the measurement only one loop of the array has been used for the test. Figure 10 shows a comparison of the frequency response of the IC from DC to 50MHz using the first loop (far right - yellow) and the 4th loop (far left - green) of the 4x1 array probe. Both loops are separated from each other of 1.4 mm, and the frequency response shows 10 dB differences at high frequency. As a result of the differences, it is possible to identify which area of the IC is in presence of a high magnetic field, allowing for fine accurate locating of the readings.

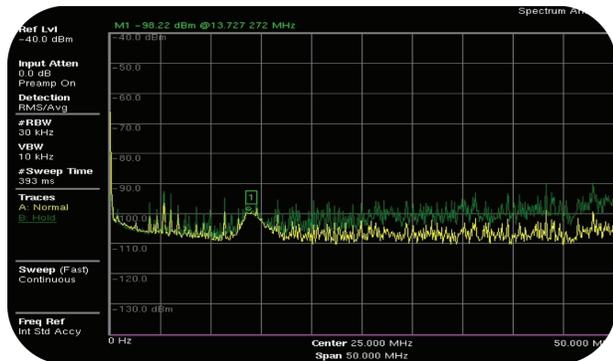


Figure 10. Frequency response (probe 1"yellow" and probe 4 "green") of the scan of **MaXEA1.0TM**

EM mapping of the captured field from the scan of **MaXEA1.0TM** has been performed at 700KHz. Figure 11 summarized the mapping results, and allow an easy identification of the source of the generated magnetic field. The blue and the purple color locate respectively the area of low and high magnetic field. As a matter of fact, the mapping shows the source of magnetic field. These results match expectations since the IC has a high current activity at that location.

Acknowledgements

This project has been funded by the U.S.A. Government (AFRL, Wright-Patterson Air Force Base), under the EMPA project, contract number **FA8650-15-D-1954 0001**.

References

1. Dean R. Collins, "TRUST in Integrated Circuits", GoMacTech 2008.

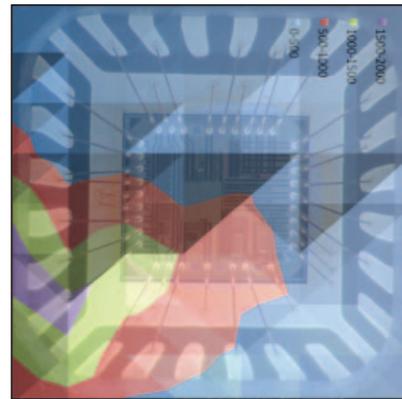


Figure 11. EM mapping of **MaXEA1.0TM** at 700KHz

Conclusion

Novel Flexible Electromagnetic Array (4x1) Probe has been fabricated, tested and used for IC's TRUST. Measurement setup has been proposed for system validation and of IC scanning surface. Validation test of the system has been conducted through coupling factor measurement using a 50-Ohm transmission line. The EMPA offer a coupling of -50dB from 0.8GHz up to 2.5GHz, a high sensitivity (-70dB input signal in a 50 Ohm transmission line), a high dynamic range, and a high resolution (detection of 100um wide transmission line). Real-time EM mapping has been performed using **MaXEA1.0TM** (integrated envelope modulator) as a DUT, and allows us to identify the area of high current activity of the IC. The study shows that the probe can be use for ICs failure detection and components counterfeit estimation.

2. Top 5 most counterfeited semiconductor parts. <http://chipsecurity.org/2012/04/top-5-most-counterfeited-semiconductor-parts/>
3. Paul T. Theilmann, Cuong Vu, Jonmei J. Yan and D. Kimball, "High Efficiency Wideband Envelope Amplifier for Handheld and Manpack Power Amplifiers", GoMacTech 2013.