

Test & Measurement

Immunity and Emissions Scanning for EMC

Logic Threshold Voltages

TTL	2 to 5V (rarely used today)
CMOS	1.8 volts and less
GTL	<1V

Figure 1: Logic Threshold Voltages

As we all know, to comply with current industry standard virtually all electronic and electronically controlled products are tested for immunity to Electrostatic Discharges (ESD), transients on power and signal lines and their susceptibility to Radiated Frequencies (RF). In addition, products are tested in insure they don't produce undesirable emissions that could interfere with other electronic products. All of this can be time consuming and expensive, especially when a product fails a test and requires extensive investigation to determine the cause and develop a fix. Scanning reduces test and evaluation time significantly and significantly reduces the likelihood of failing subsequent compliance test.

Using scanning techniques to identify product sensitivities and RF emissions levels prior to compliance testing the engineer can quickly make the necessary decisions that will save his company both time and money. A Standard Practice addressing ESD scanning has been published by the EOS/ESD Association as ANSI/ESD SP14.5-2015, which describes scanning techniques and provides useful information about the necessary probes and field coupling to a product being tested.

ESD and Magnetic Fields

To simulate the effect of an ESD event using Immunity scanning, a magnetic loop probe is used to couple a pulse onto a circuit trace at a specific point, which then may couple

into other traces or an active device directly. Before we get into the scanning techniques, it's important to understand why injecting a magnetic field into a circuit to simulate an ESD or other transient makes sense. ESD events can cause currents of more than 50 A to flow directly into a port or via a cable, along a chassis or onto a PCB via secondary discharges. As these currents travel through various available paths, magnetic fields are generated which in turn develop voltages along the way. Large currents developing large voltages can cause hard failures – device damage - from which recovery isn't possible but the fault is easy to find (smoke?!); lower currents produce lower voltages that cause upset but no damage. In this case the system can typically be reset, rebooted, or may even have selfrecovery routines to bring the system back on-line. For many products this upset, sometimes called a "soft" failure, is in fact, a failure. Think of what upset occurring in critical control circuits might cause – avionics, medical procedures, and self-driving cars, to name a few.

As an example of the direct effect of ESD currents flowing into or on a product, one needs to remember:

$$V = L(di/dt)$$

Where

V = the voltage developed

L = Inductance of the path and

di/dt = rate of change in the amplitude of the current.

ESD events have very fast rising currents that are in the picosecond to nanosecond range, so it doesn't take much inductance to develop a significant voltage. An example of $V=L(di/dt)$ effects can be made as follows: Assume a poor connection between a USB cable shield and chassis, say a 2 nH connection inductance. If we also assume a 5 kV ESD event having a current rising to about 20 A in 1 ns:

$$V = L(di/dt) = 40 \text{ V!}$$

(IEC values are: 1.2 ns risetimes at 3.75 A/kV; therefore a 5 kV discharge would provide a current of 18.75 A.)

The 40 V spike will appear inside the enclosure and drive a current into a circuit board.

Fig. 1 shows some typical logic threshold voltages, and actual levels today can be 0.3 V or less. One can see it wouldn't take much of an ESD event to produce enough voltage to re-set a device if the voltage appeared in the right place.

ESD/EMC Immunity Scanning

The basic technology isn't new: Engineers have been using probes to inject fields into a circuit to locate trouble spots for some time. Historically, these have been large probes with fields covering a wide area which allows determining a general area of a board that is sensitive but difficult to pinpoint the problem device or circuit. Today's crowded circuit boards and physically small components significantly reduce the usefulness of this method.

To get around the size problem, ESD/EMI scanning uses very small probes, less than 1 mm in diameter that allows precise positioning and iterative scanning to provide a 3 dimensional plot. An engineer can not only

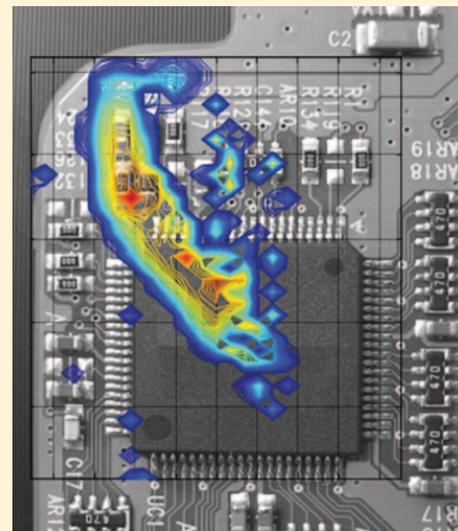


Figure 2: Scan of a sensitive device, colors indicate sensitivity levels, with red being most sensitive and blue the least sensitive (Courtesy of Amber Precision Instruments)

Michael Hopkins
Amber Precision
AR
www.arworld.us

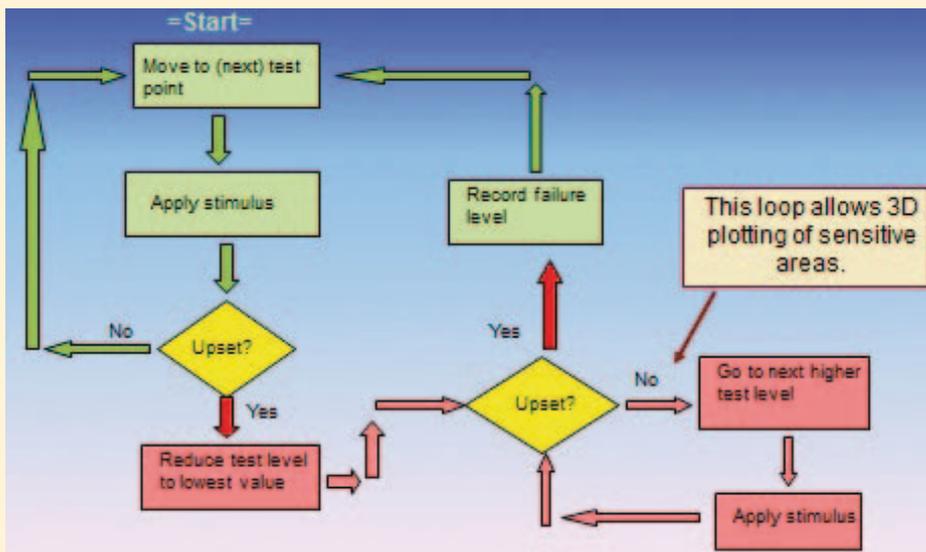


Figure 3: Algorithm for an automated scanner

identify a sensitive component, but also can determine its relative level of sensitivity and the pins and associated components involved. Fig. 2 below is an example of a scan done on a sensitive circuit.

In Fig. 2, the source of the disturbance is a pulse induced via a small H-Field loop close to the surface of the board. The resulting voltages and currents developed are responsible for the device upset. This is, in fact, the mechanism for most ESD caused upsets.

ESD/EMC scanning is done by stimulating a location on a board and looking for upset, taking care to NOT cause circuit damage. This allows an iterative process of increasing and decreasing stimulus levels to determine a relative level of susceptibility at a specific point.

A flow diagram for an automated system for ESD/EMC Scanning is shown in Fig. 3 and an example of an automated scanning system is shown in Fig 4.

In Fig. 3 the test begins at the block “Apply Stimulus”. Following the arrows to “Upset?” if no upset is detected, the probe is moved to the next location and the test repeated. If an upset is detected, the stimulus is reduced to a lower level. If upset still occurs, the stimulus is again reduced until no upset is detected or the lowest test level is reached. Once the upset level at one point is recorded, the probe is moved to the next point and the iteration repeated. At the end of the test, a display such as that shown in Fig. 2 is produced.

Upset is detected by monitoring key functions of the system under test. Optical monitors are used to detect changes in a display, V/I monitors for reset lines, audio detectors for some circuits, data streams, etc...

almost any key function can be monitored automatically for testing. System re-set is also a requirement for automated scanning. When a failure is detected, the system being tested needs to be brought back to a known operating state before testing can continue. This can easily be done for most products using external switching to re-set and/or reboot a system. More complicated systems may require more complex monitoring, such as re-boot, send an instruction to the system to set it in a known condition and then exercise the system to make sure it's functional again.

There are situations where Electric Field scanning might be preferred and this can easily be accomplished using E-Field probes in place of H-field probes. For example, LCD display touch screens and associated distributed circuitry is often sensitive to fast changing E-Fields and might not respond to magnetic field scanning, but may respond dramatically to a changing E-field.

RF Immunity Scanning

RF Immunity scanning is done to locate specific nodes in a circuit that are susceptible to some frequency or range of frequencies. This is basically a sub-set of the EMC immunity scanning described in the previous section. The fully automated scanning system shown in Figure 4 is easily adapted to RF immunity scanning; however, there are some additional hardware requirements. An RF immunity scan requires an RF Sweep generator capable of covering the frequency range of interest plus RF amplifiers to drive the probes. Levels need to be automatically adjusted to compensate for the frequency response of the probes. This isn't difficult and is being done all the time with antennas

in used for RF immunity compliance testing. Numerous software programs and calibration procedures exist and can easily be modified for use with RF Immunity scanning. All the RF instrumentation and software required for this test is readily available.

RF Emissions Scanning

The basic scanning system for ESD/EMI Immunity can be used to locate and quantify radiation coming from a circuit. Near-field (NF) EMI scanning is a technique used by several manufacturers to evaluate boards for radiation. It's a useful tool for locating the source of RF radiation and its relative amplitude, but correlation to a far-field (FF) test, necessary for determining standards compliance, is difficult. Most EMI scanners provide only NF results and some scanners use algorithms to estimate the far field but to do this properly requires the phase information associated with the radiated field. With appropriate probes, instrumentation, and software, RF Emissions scanning to 40 GHz and correlation to far-field is possible.

Maxwell's equations tell us that knowledge of the near field in magnitude and phase is sufficient to reconstruct a model of the source and obtain the far field emissions. This information significantly improves modeling for RFI analysis and can be used to predict RFI coupling within a system and in turn, be used to qualify ICs and modules to reduce the chance of RFI problems later in product design.

Resonance Scanning

Resonance scanning can help determine the likelihood of an RF problem. This is



Figure 4: Fully Automated ESD/EMC Scanner

done by first doing a resonance scan with an unpowered system to determine the location, frequency and Q of a resonant circuits (The amount of coupling enhancement due to resonance depends on the Q of the circuit.). Since one cannot reasonably test every point at every frequency for sensitivity, it's reasonable to test only the identified locations and frequencies which will significantly reduce test time.

When the engineer can determine what resonances exist in a design – location, frequency and Q – steps can be taken to minimize the potential for RF Immunity problems.

Once the RF immunity scan at resonant locations is complete, the engineer will have a complete set of information: location, frequency, Q and the relative sensitivity at each location and therefore the likelihood that any resonant location will be a problem.

Scanning and Shield Effectiveness Evaluation

Using an automated scanning system with field measurement software and specialized probes can provide very accurate shielding effectiveness measurements to 18 GHz. With the correct probes, some as small as .025 mm or even 0.1 mm, it's possible to achieve enough spatial resolution to accurately measure the shielding effectiveness of small DUTs and IC's. Software can provide full test reports to minimize the engineers time evaluating the results.

Current Spreading

Current Spreading is a method of using an EMC Scanner to visually re-constructing the current flow on a board caused by a transient event.

Using a well-controlled current sources and specially designed probes, it is possible to make measurements over an entire DUT and produce a video that shows how the injected currents flow with a resolution of better than 100 ps. This can be extremely useful to determine the performance of protection components and aide in determining where protective devices may need to be located.

In the example of Fig. 5, the bulk of the current is diverted through a primary pro-

tection device located at the input to a DUT but residual current can be seen traveling toward a semiconductor device that probably has an internal protector. In addition, currents may be observed moving in unexpected directions providing an invaluable tool to the engineers.

Summary

Scanning Technologies for EMC can provide significant advantages to design, compliance and test engineers by providing information not previously available: precise location of ESD and RF sensitive circuits and components, emissions data including phase measurements for far field characteristics, the location of resonant structures on a PCB and last but not least, the ability to produce an actual video of transient current flow into a board. The data provided from these new technologies will allow more accurate modeling for the design engineer and the ability to locate and correct problems found in the field and in compliance testing.

Acknowledgments:

Dr. David David Pommerenke
Missouri University of S&T
EMC – Laboratory

Jin Min
President
Amber Precision Instruments

Giorgi Muchaidze
System Integration Manager
Amber Precision Instruments

References:

ANSI SP14.5-2015 EOS/ESD Association
Standard Practice for Electrostatic Discharge
Sensitivity Testing – Near Field Immunity
Scanning

Charvaka, D., Gossner H., (2015) System
Level ESD Co-Design, Wiley, IEEE Press

Standard Practice in EMI Measurement on
Shielding Effectiveness (SE) Evaluation Test
(2016) Amber Precision Instruments 2016
www.amberpi.com ◀

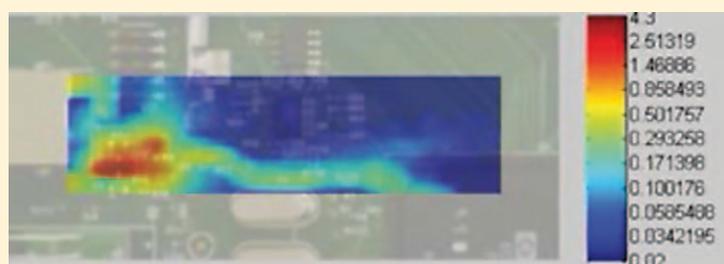


Figure 5:
Snapshot of injected current through a TVS device and towards a protected IC