

Susceptibility testing of Boards and Semiconductor Devices

Bridging the gap between device and system level immunity testing

Michael Hopkins Amber Precision Instruments

Overview

There appears to be a disconnect in the EMC world between system manufacturers testing for **upset** and device manufacturers testing devices for **failure**. To be fair, the device manufacturers really aren't trying to perform EMC tests, but the manufacturers of a broad range of products are now asking semiconductor device manufacturers to test devices using system level EMC



Background

We all understand that faster and smaller is the key to success with modern electronic circuits, but the price is often increased susceptibility to the threats provided by the environment: Static, noise, radiation and transient electrical events of all sorts threaten stable operation of circuits -- and in the worst case, cause damage.

The problem is **not** that engineers don't understand these events: individual IC's are hardened against potential damage during the handling process and whole industries exist to provide power line and data line protection at the system level. These efforts successfully protect hardware from most damaging EMC events, but they often fail to prevent system level upset or malfunction.

The problem is that upset and malfunction are generally caused by fast, low level events radiated into a circuit bypassing protective devices, or conducted into a circuit at levels below the operating voltage of a protective device.¹ An integrated circuit that can withstand a few thousand volts of ESD without damage during handling can often be upset -- or reset -- with only a few volts!

Pinpointing circuits and devices that are sensitive to low level events is practically impossible using standard EMC test methods, but new methods of susceptibility testing are being used by a few leading edge companies to identify sensitive devices and circuits – saving time and money and most importantly, providing the consumer with a more reliable product.





¹ "Tze Wee Chen, Timothy J. Maloney, Bruce Chou, "Detecting E and H Fields with Microstrip Transmission Lines" *IEEE International Symposium on Electromagnetic Compatibility, Detroit, MI, August 18-22, 2008*



Device Testing -- for Immunity?

Devices are not really tested for immunity to EMC events -- they're tested for failure during handling, and it's a critical difference. Immunity implies the ability to keep functioning in the face of electrical disturbances - ESD, transients, RF but individual devices are typically only tested to determine the voltage level beyond which the device will be damaged². Several ESDA (Electrostatic Discharge Association) and JEDEC (Joint Electron Devices Engineering Council) standards exist to qualify devices for their ability to withstand ESD during the handling process, but none exist that deal

System Testing for Immunity

with susceptibility.³

Systems, i.e. finished products, really are tested for immunity. Hardware damage, loss of data and unsafe operation resulting from a test are never allowed.

Mandatory compliance testing for the CE marking as well as most other industry and corporate standards include failure criteria similar to that in IEC standards. The Performance criterion from the IEC Generic Standard for residential, commercial and light industrial environments is as follows:

a) Performance criterion A: The apparatus shall continue to operate as intended during and after the test. No degradation of performance or loss of function is allowed below a performance level specified by the manufacturer, when the apparatus is used as intended. The performance level may be replaced by a permissible loss of performance. If the minimum performance level or the permissible performance loss is not specified by the manufacturer, either of these may be derived from the product description and documentation and what the user may reasonably expect from the apparatus if used as intended.

b) Performance criterion B: The apparatus shall continue to operate as intended after the test. No degradation of performance or loss of function is allowed below a performance level specified by the manufacturer, when the apparatus is used as intended. The performance level may be replaced by a permissible loss of performance. During the test, degradation of performance is however allowed. No change of actual operating state or stored data is allowed. If the minimum performance level or the permissible performance loss is not specified by the manufacturer, either of these may be derived from the product description and documentation and what the user may reasonably expect from the apparatus if used as intended.

c) Performance criterion C: Temporary loss of function is allowed, provided the function is selfrecoverable or can be restored by the operation of the controls.

Reboot!



² Methods do exist for testing ICs for **RF** Immunity in TEM cells. The device is mounted on one side of a circuit board with exposed circuitry on the other side. The board is then mounted in the wall of a TEM cell with the device exposed inside and power applied from the outside.

Although software routines and error correction protocols exist to prevent corruption of data transmissions, these won't prevent malfunction of the device itself due to ESD or other transients.







The Disconnect

The disconnect between system testing and device testing can be summarized as follows:

- The system manufacturer believes that by requiring the device manufacturers to test to system level standards -- IEC 61000-4-2 waveforms for example -- the system will likely pass compliance tests.
- The device manufacturer believes he's doing what the system level manufacturer requires. After all, he did a test at several thousand volts⁴ and the device still functioned afterwards.

Of course, both are mistaken. The device may be able to handle a 4kV ESD event during handling, but because a few volts appears at a reset pin during compliance level testing, the system is considered to have failed – and the finger pointing begins!

Testing to bridge the gap

How do we provide a solution to bridge the gap between these two worlds? The answer:



A susceptibility test that can be done by both the system manufacturer and the device manufacturer.

- It's a test that can be done by both the system and device manufacturer and the results are meaningful to both.
- As a preventive measure during design or device selection, it provides the engineer with a tool to see potential problems before a product is put into production.
- For resolving EMC susceptibility problems in a sub-assembly or finished product, it
 provides a method to quickly see those areas likely to be the root cause of upset or
 malfunction.
- For the device manufacturer it's an invaluable tool for determining the sensitive of a device something rarely done in industry today.

Susceptibility testing doesn't replace system level testing to compliance standards or device level testing for voltage withstand during handling. What it *will* do is provide a tool that can be used by both the system level manufacturer and the semiconductor manufacturer to identify susceptibility problems at every level – device, board, sub-assembly and system.

In addition to identifying a sensitive component or circuit, testing must be able to quantify susceptibility levels and ideally correlate these results with the system level test results. Simply doing a system level test on a device is useless unless susceptibility levels can be determined and quantified.

⁴ The ESD Association Working Group 5.6 is currently working on a Standard Practice that will give device manufacturers some guidance about how to accomplish this testing in the lab.



What is Susceptibility Scanning?

Susceptibility scanning is essentially a method of stimulating a circuit or device either directly at a pin or trace, or via a small electrical field probes. In order to localize the sensitive area, the probe needs to be quite small and the stimulus level kept low. A 0.5mm H Field probe has been found to be adequate for most boards and many devices.⁵



H Field, E Field and direct injection probes used for susceptibility scanning Courtesy of Amber Precision Instruments

Scanning can be done either manually or with an automated system. An automated system has the advantage of being able to precisely locate the probes, increase and decrease stimulus levels, plot relative sensitivities and perform analysis. The manual method can be used to quickly locate a sensitive area but it is more cumbersome when it comes to doing analysis. Scanning itself isn't new: there are commercial EMI (Electromagnetic Interference) scanners for detecting near field radiation analyzing the radiation from a board or system, and manual EMC immunity scanning has been done for some time to localize sensitive circuits⁶ but what *is* new is the ability to do susceptibility scanning in a controlled, quantifiable and repeatable way at both the system and device level.



Photo Courtesy of Amber Precision Instruments

⁵ Giorgi Muchaidze, Jayong Koo, Quing Cai, Tun Li, Lijun Han, Andrew Martwick, Kai Wang, Jin Min, James L. Drewniak, David Pommerenke, "Susceptibility Scanning as a Failure analysis Tool for System-Level Electrostatic Discharge (ESD) Problems, *IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY, VOL 50, NO.2 MAY 2008*

⁶ Doug Smith (2007), "Using Current Probes to Inject Pulses for Troubleshooting (Current Probes, More Useful Than You Think – Part 2) " Technical Tidbits, High Frequency Measurements Web Page, <u>www.emcesd.org</u>



Susceptibility scanning not only identifies sensitive areas of a circuit or device but with the proper software can also plot the relative sensitivities in 3 dimensions. In the example above the most sensitive areas of a device and its associated circuitry are easily identified. Replacing the device in this example with an identical device from a different manufacturer lot will quickly show if there is a difference in susceptibility.



An example of an automated EMC Immunity Scanner showing the necessary components is shown above. In this case, a TLP (Transmission Line Pulser) is used as the stimulus source to an H-Field probe (hidden below the robotic cross-arms). Other sources, such as an Electrical Fast Transient or IEC ESD Waveform generator could be used but experience has show the H-Field generated by a TLP tester works extremely well. Data collection units monitor the EUT looking for expected upset or malfunction.

Several key factors need to be understood for successful susceptibility scanning:

- A board or system being scanned needs to be monitored in order to determine that a circuit has been upset, and this can be done in several ways including:
 - Voltage probing suspect nodes or traces
 - Monitoring of data streams looking for errors
 - Optical monitoring of status indicators
- Testing a device requires specific input circuitry and careful monitoring of the outputs
 - Testing of a complex device is typically done in a known system or sub-system where the device can be properly exercised and it's effect on the system monitored.
 - Generic device testing of a complex IC is a practical nightmare. It will typically require considerable circuitry to get it into a known state, exercise its functions and monitor its outputs.
- Selection of the noise source can be critical to determining a circuits' response. There are many possible noise sources, including:
 - A fast, ESD like pulse
 - A square wave with defined rise and fall times
 - o Controlled noise bursts, such as the Electrical Fast Transient commonly used for system level testing
 - RF, but then what frequencies should be used
- The test level needs to be carefully selected. It would be desirable to select a level to be the equivalent of
 what would result from a system level test or that results from field failures, but determining that level can



be extremely complex. It is imperative, however that the level selected not cause circuit damage. Unlike other testing done to determine ESD withstand levels of devices, susceptibility scanning is by definition, non-destructive.

Putting everything together

Device manufacturers already do considerable testing to insure that devices can withstand relatively high ESD voltages and remain operational – no damage – but the levels at which upset or malfunction might occur are unknown. Even the additional testing of devices to system level standards (IEC 61000-4-2 for example) still doesn't provide any information about sensitivity to upset. EMC Susceptibility scanning on devices operating on a test board or in a known circuit configuration solves this problem – devices *can* be qualified in a way that helps a manufacturer insure passing system level compliance tests and provides useful, *and previously unavailable*, information to the device manufacturer regarding the device performance.

For the system level manufacturer currently doing EMC Compliance testing an ESD event causes upset but there's no information about what happened and hence the guess work begins – what circuits are involved, let's try some ferrites, let's see if a different case material will help, etc. EMC scanning at the system level will quickly pin down the sensitive area(s) in a design telling the engineer where to focus his attention saving both time and money. Now the system level manufacturer can go to the device people with a test that makes sense and not just another of looking at the voltage withstand levels.



Hence, the new EMC testing dynamic:

Copyright Amber Precision Instruments, reproduced with permission



Just a word about ESD Events

Why should one believe that by finding the sensitive areas of a board or circuit will insure passing system level tests and improve field reliability? Nothing's 100%, but it's certainly clear that by knowing what parts of a circuit are sensitive to transient events makes it possible to take steps to protect or improve that susceptibility. It's also clear that if during a system level test upset does occur, it's pretty likely that some remnant energy got to a sensitive area of the design.

Think about how transients get into a system – an ESD event, electrical fast transient or surge comes in from the outside world. Primary and secondary protective devices operate to get rid of the bulk of the energy coming in on the mains or into an I/O port. Even at the device level, protective structures exist to divert any higher than normal voltages preventing hardware damage. What's left to cause upset are E and H fields that are either radiated into the system or developed as a result of secondary effects. Susceptibility of systems and devices has been shown to be more related to these radiated effects than to the voltage levels of external ESD.

Any remnant voltage that does get to a device and causes upset or an unwanted reset doesn't look anything like the event coming in from the outside world unless it's directly connected to the outside world. Even then, it's likely to be considerably modified by surrounding circuit elements and parasitic effects. Anything that gets to a sensitive area deep inside a product is much more likely to be the result of E and H fields that result from the initial transient.

Conclusions

Although the gap between system level testing and testing done by device manufactures does exist, there is a way to bridge this gap. EMC Susceptibility can and is being done to identify sensitive circuits and devices – to the point of identifying the areas within an individual IC that are sensitive. Using different probes, determination can be made as to whether the sensitivity is to an E Field or to an H field and therefore what kind of steps need to be taken to reduce susceptibility levels.