Spring 2021

Investigating the effect of operating condition on ESD-induced soft-failures

Omid Hoseini Izadi

Department: Electrical and Computer Engineering

INVESTIGATING THE EFFECT OF OPERATING CONDITION ON ESD-INDUCED SOFT-FAILURES

by

OMID HOSEINI IZADI

A DISSERTATION

Presented to the Graduate Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

2021

Approved by:

Dr. Chulsoon Hwang, Advisor
Dr. Daryl Beetner
Dr. Jun Fan
Dr. DongHyun Kim
Dr. Victor Khilkevich
Dr. Daniel Fischer

PUBLICATION DISSERTATION OPTION

This dissertation consists of the following four articles, formatted in the style used by the Missouri University of Science and Technology:

Paper I, found on pages 5–25, "Systematic Analysis Of ESD-induced Soft-failures As a Function of Operating Conditions," has been published in the IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), in Singapore, in May 2018.

Paper II, found on pages 26–44, "Analysis of Software Loading Effect on ESD Susceptibility," has been published in the IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), in Reno, NV, in July 2020.

Paper III, found on pages 45–69, "Automated ESD-induced Soft Failure Detection and Characterization Using Image- and Audio-based Methods," been published in the IEEE Transactions on Electromagnetic Compatibility.

Paper IV, found on pages 70–81, "Investigation of Electrostatic Discharge-Induced Soft-Failure Using 3D Robotic Scanning," has been published in the IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+SIPI), in New Orleans, LA, in July 2019.

ABSTRACT

Conflicting observations have been found in the literature regarding the effect of operating conditions on ESD (electrostatic discharge) susceptibility. While some studies have suggested a strong correlation between the two, others observed little to no correlation. In this work, a systematic study has been carried out suggesting the existence of a strong correlation between the ESD susceptibility and operating conditions. It is found that the root cause of this conflict is random ESD noise injection. A measurement approach is proposed to synchronize the noise injection with the system activity such as high/low CPU load. In this approach, the current consumption or the EMI (electromagnetic interference) of the device under test is monitored and used to synchronize the injections.

To improve the poor repeatability of the ESD tests, the proposed approach is incorporated into a robotic scanner to create an automated ESD tester. Soft failure detection algorithms are added to the tester, giving it the ability to detect (and characterize) a soft failure in a similar way as a human – through sight and hearing. This is the first time that image processing algorithms are used for characterizing soft failures. Using the tester, a 2-D color-coded susceptibility map is obtained for each soft failure. These failure-specific maps can be used to identify/pinpoint the sensitive locations of the device knowing the soft failure type, reducing the tedious and time-consuming process of soft failure investigations.

ACKNOWLEDGMENTS

I would like to express my special thanks to my former advisor, Dr. David Pommerenke, for his friendship, support, patience, and guidance. My sincere thanks also go to my current advisor, Dr. Chulsoon Hwang, for his support and guidance.

I would also like to thank Dr. Daryl Beetner, Dr. James Drewniak, Dr. Victor Khilkevich, Dr. Jun Fan, Dr. DongHyun (Bill) Kim, and the rest of the EMCLAB family for their continuous support in my academic career. It was a great privilege and honor to be part of this supportive family.

I am very thankful to my parents for their love, and unconditional support every step of the way. Without their support, I could not have been where I am today.

Lastly, I would like to express my very special thanks and gratitude to my beloved wife, a wonderful person who postponed her success to support mine, who gave up her time to buy me time, and who supported me through her patience, kindness, and love. I hope I can support her the way she supported me. I am forever in her debt.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

PAPER II

PAPER III

PAPER IV

LIST OF TABLES

SECTION

1. INTRODUCTION

1.1. BACKGROUND

An electrostatic discharge (ESD) can disturb the sensitive circuitry of an electronic device. Such an event can upset electronic components and lead to a *hard failure*, a *soft failure*, or a *latch up*. Hard failures are irreversible damages. Simply, the damaged component stops working. Soft failures on the other hand can be recovered from. A power-cycle, reboot, or even simple time-lapse can clear the soft failure. Latch ups can lead to increased current consumption, excessive heat, faster battery discharge, and even permanent damage through overheating.

1.2. RELEVANT STANDARDS AND THEIR SCOPE

ESD susceptibility testing can be done at the component level or the system level. The former scenario is called component-level testing and is covered by the JEDEC and the ESDA. These standards only focus on hard failures. System-level testing on the other hand is established by IEC and focuses on both hard and soft failures. Table 1.1 compares important aspects of these standards with each other. An important aspect of system-level testing as shown in the table is that it is application-specific, as opposed to the JEDEC, and ESDA standards that are standardized. Also, as shown in Figure 1.1, the IEC current waveform (system-level testing) has higher energy. In other words, the system design has to meet more stringent requirements than component-level design. Another important difference observed in Table 1.1 is that the system is tested under both powered and

unpowered conditions in system-level testing, as opposed to only unpowered testing in component-level testing. Due to these differences, even if robust components were used in a system, there would be no guarantee that the system would pass system-level testing criteria (a common misconception). Therefore, it is important to perform system-level testing and meet the requirements.

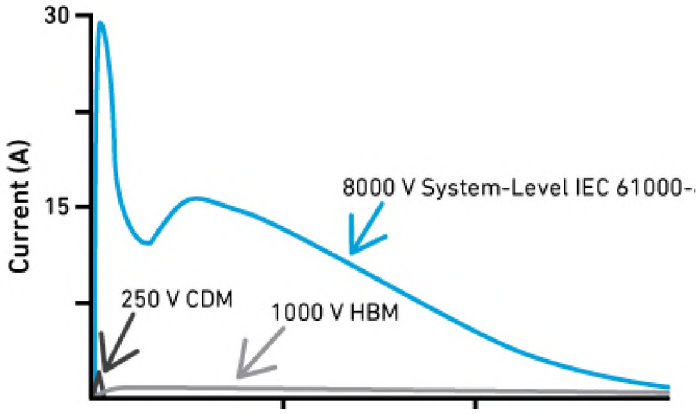


Figure 1.1. Current levels of Human Body Model (HBM) at 1 kV, Charged Device Model (CDM) at 250 V, and System level IEC 61000-4-2 at 8 kV. Adopted from [1].

1.3. OBJECTIVE AND CONTRIBUTION

This dissertation is focused on ESD-induced soft failures, which is part of the system-level testing and is covered by the IEC 61000-4-2, "Testing and measurement techniques – Electrostatic discharge immunity test." This standard only represents a scenario where a charged human body discharges to a point on a system through a metal object. No information is given on what the system operating conditions should be, or whether there is a correlation between the system ESD susceptibility and the operating conditions. Searching the literature for an answer, we found conflicting studies. While references [2, 3] reported a correlation between the ESD susceptibility and operating

conditions, other studies such as [4] did not observe any correlation as shown in Figure 1.2.

Table 1.1. System-Level vs. Component Level ESD. Adopted from [1].

	Component level ESD	**System-level ESD**
Standard	JEDEC, ESDA	IEC
Environment	Factory assembly	End used normal operation
Test setup	Standardized	Application dependent
EUT applications	IC	System (PC, cell phone, etc.)
EUT operation	Unpowered	Powered and unpowered
Discharge R-C network	100 pF/ 1500 Ω	150 pF/ 330 Ω
Typical test voltage	1-2 kV	2-8 kV
Peak current	0.7 A/kV	3.75 A/kV
Rise time	2 to 10 ns	0.6 to 1 ns
Pulse width	150 ns	50 ns
Test application	IC pins	Enclosure, pins
Testing pin groups	Different pin combinations	Few special pins
Tested properties	IC protection circuits and concept	System design
Failure	Hard	Hard and soft

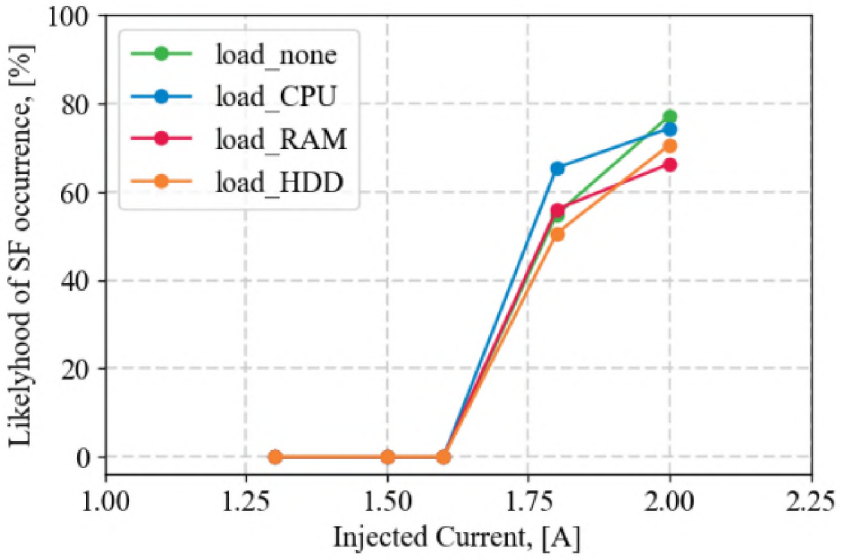


Figure 1.2. No correlation was reported. Adopted from [4].

The goal of this dissertation is to determine the root cause of the confliction in the literature and find out whether there is a correlation between the ESD-induced soft failures and the operating conditions. Further goals of this dissertation are to develop proper measurement techniques and setups to enable the observation and investigation of this (potential) correlation.

This dissertation is composed of four papers. Paper I systematically analyzes soft failures as a function of various operating conditions. Paper II proposes the required measurement setups and techniques to observe the "operating condition-ESD susceptibility" correlation. Paper III, for the first time, introduces image and audio processing algorithms for soft failure detection and characterization. Paper IV performs automated soft failure investigations by equipping a humanoid robotic arm with the algorithms developed in Paper III.

PAPER

I. SYSTEMATIC ANALYSIS OF ESD-INDUCED SOFT-FAILURES AS A FUNCTION OF OPERATING CONDITIONS

Omid Hoseini Izadi
Department of Electrical Engineering
Missouri University of Science and Technology, Rolla, MO, 65409
E-mail: ohp63@mst.edu

ABSTRACT

Electrostatic discharges (ESD) to parts of a system can lead to system-level soft-failures. These failures can depend on the activity of the system at the moment of discharge. This paper investigates ESD susceptibility as a function of different operating conditions such as software loading, clock frequency, and VDD voltage. Due to the large number of possible conditions, a commercial automated ESD scanner is modified and used to obtain ESD susceptibility maps for each operating condition. The core processor of a single-board computer is selected as the device under test. It is observed that the processor becomes more sensitive to ESD events as its software loading increases. The effect of VDD voltage and clock frequency on the sensitivity of the processor is also discussed. Moreover, the effect of increasing the power distribution network impedance and noise is investigated, partially leading to counterintuitive results.

1. INTRODUCTION

Electrostatic discharges (ESD) can couple into an integrated circuit (IC) via its pins and cause different types of system-level failures. ESD energy can also directly couple to the bond wires and cause a failure. Typical examples are loss of data, data corruption, program termination, system hang, system reset, latch-up, etc. These type of failures are known as soft-failures as the system recovers by power-cycling. Soft-failures can be grouped into two categories with respect to software loading conditions: those that are not affected by the core processor loading and those that have an increased likelihood to occur if the processor is highly active [1]. For instance, coupling to the reset circuitry or system clock will most likely lead to a system reset or hang up, independent of the loading condition. However, memory access disturbance will only lead to visible effects if the memory was active at the moment of the disturbance.

In [2, 3], via many measurements on single-board computers, it has been shown that occurrence of a specific soft-failure might depend on the program, running on the system. The authors have shown the core processing IC of a smartphone became more sensitive to ESD events when a computationally intensive application was running compared to the case where the device was in standby mode [4]. These studies focused on the relationship between the system loadings and susceptibility, but no work was done on systematic analysis of the susceptibility concerning operating conditions of the system.

The susceptibility of a device under test (DUT) as a function of different operating conditions such as software loading, clock frequency, power distribution

network (PDN) noise and impedance, and VDD voltage is investigated for 5 different platforms. However, only one DUT is thoroughly analyzed in this paper. To better understand the effect of each condition on the susceptibility, the conditions are analyzed by obtaining ESD susceptibility maps for each condition. A susceptibility map shows the TLP voltage required to cause a soft-failure at various locations on the DUT. Such maps can be obtained by coupling noise to the DUT (through a magnetic field probe) while monitoring the system behavior. Magnetic probe is preferred to reduce chances of permanent damages to the DUT. If a soft-failure occurs, the TLP voltage and location are recorded for plotting. Figure 1 shows a typical susceptibility map. The small red dots indicate the probe position, and the color bar shows the voltage required to cause failure at each location. Due to the large number of positions required to obtain each map and the large number of possible conditions, manually obtaining the complete set of susceptibility maps could be very time-consuming and cumbersome.

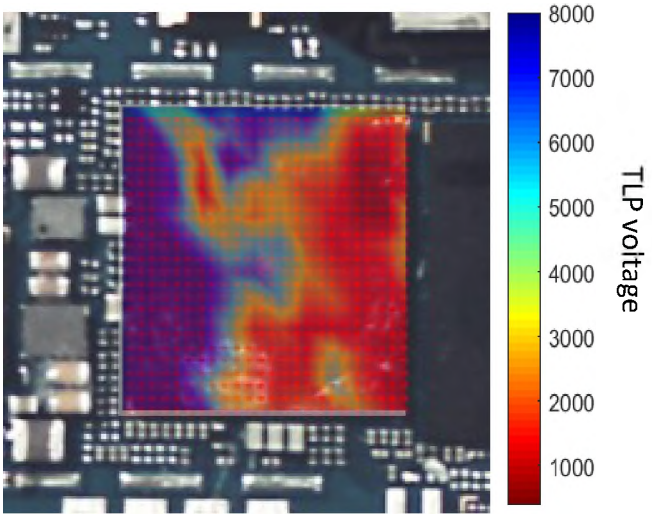


Figure 1. A typical susceptibility map.

For instance, obtaining one susceptibility map for a 15×15 mm IC can take up to 14 hours. In [5], an automated scanner is developed and used for obtaining ESD susceptibility maps. In [6], a commercial version of the robot scanner is used for analyzing root causes of system-level immunity sensitivities. This product is modified accordingly and then used to obtain the ESD susceptibility maps as a function of different operating conditions as discussed in Section 2 and 3, respectively.

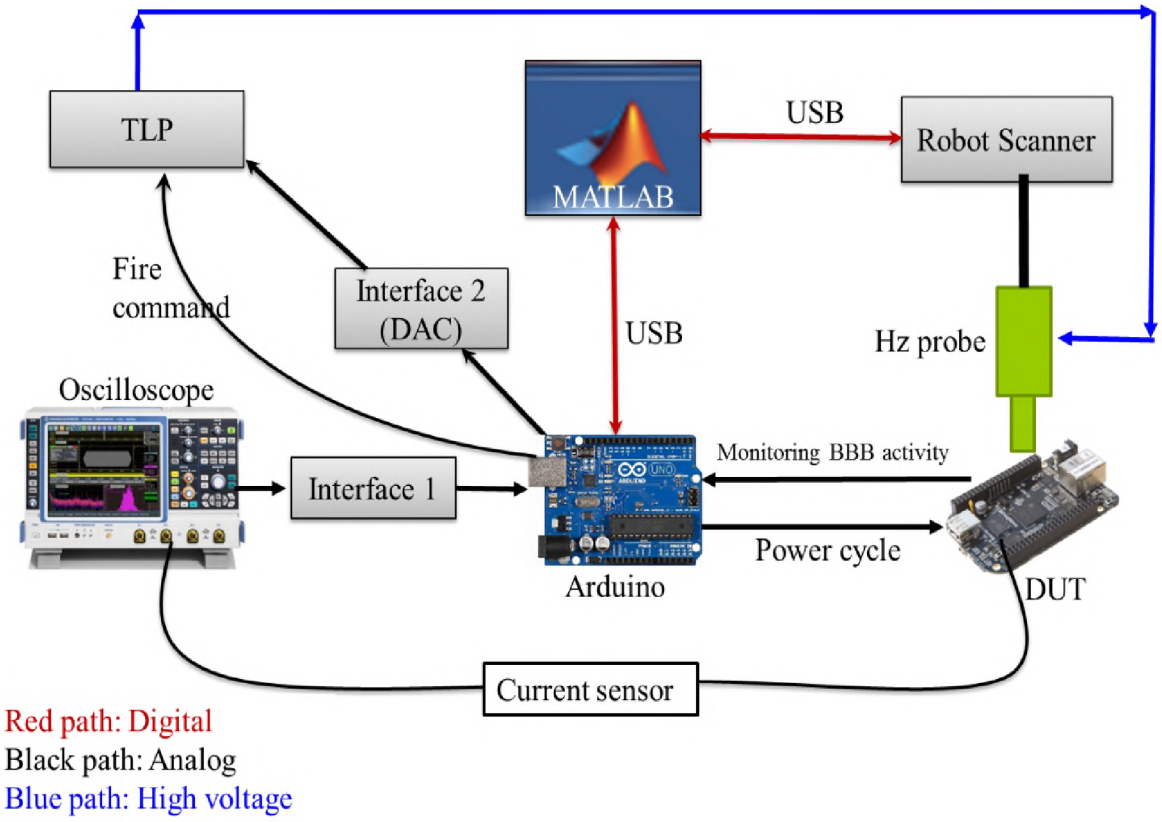


Figure 2. Block diagram of the automated scanner built around an API robot scanner, MATLAB, TLP, Arduino UNO and a couple of interfaces.

2. MODIFICATION OF THE ROBOT SCANNER

A fully automated ESD scanner requires many features such as automatization, failure detection, power-cycling and rebooting the DUT, verifying a successful reboot, detecting the DUT operating phases by monitoring its current consumption, software-activity-based injection of ESD noise, performing synchronous or asynchronous injections, changing TLP source voltage, changing injection location, and recording the injection voltage and robot arm coordinate. These requirements can be satisfied by the proposed block diagram and flowchart.

2.1. BLOCK DIAGRAM

Figure 2 shows the block diagram of an automated ESD scanner built around an API robot scanner [7], a transmission line pulse generator (TLP) with a rise time of about 300 ps, and an oscilloscope. The injecting probe is a Hz probe consisting of a small loop with a diameter of 2 mm. The probe can produce both Hx and Hy fields at the same time. Hence, there is no need to scan the IC using probes of Hx and Hy orientation. Full-wave simulations showed the maximum generated magnetic field at 1 mm distance under the Hz probe when the probe loop is driven by 1 A of current, is about 114 A/m. This field strength can induce about 10 mA of current in a 1×0.5 mm loop placed at 1 mm below the probe and 1 mm to the side as shown in Figure 3. These two loops are placed orthogonally to mimic the orientation of the probe relative to possible coupling structures inside an IC (DUT). The exact dimensions and the induced current will depend on the details of the IC structures and the package. The current going to the probe loop and the

resulting field strength is set by the TLP source voltage. For instance, 1000 V charge voltage will lead to 20 A of current inside the probe loop as the loop forms a short. The selected DUT for our investigation is the CPU of a BeagleBone Black (BBB). This single-board computer has a Linux-based operating system with root access allowing us to control the CPU parameters from within the code.

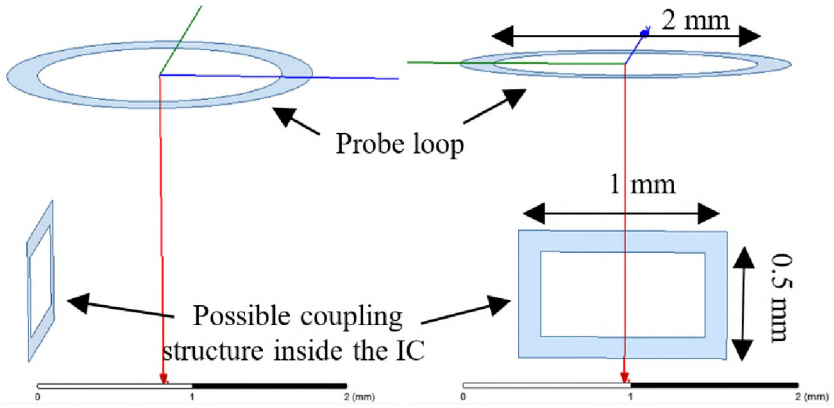


Figure 3. The orientation of the Hz probe loop relative to possible coupling structures inside the IC at two different views.

As shown in Figure 2, the BBB current consumption is monitored using a current sensor and an oscilloscope. The oscilloscope is configured to generate a trigger pulse when it detects a certain current level. The number of generated pulses per second depends on the running application on the BBB. About 3 to 8 pulses can be generated every second. The generated pulses are too narrow for the Arduino to detect (~10 µs); thus, Interface 1 is placed between the oscilloscope and the Arduino to increase the pulse width. Upon detection of the pulse, the Arduino sends an injection command to the TLP. The TLP source voltage also is controlled by the Arduino by using a digital to analog converter (Interface 2). As the main controller of the automated scanner, the Arduino

continuously reports the scanner status to MATLAB. This information helps MATLAB to control the robot arm accordingly. The functionality of the system is explained in more details in the next section using the system flowchart.

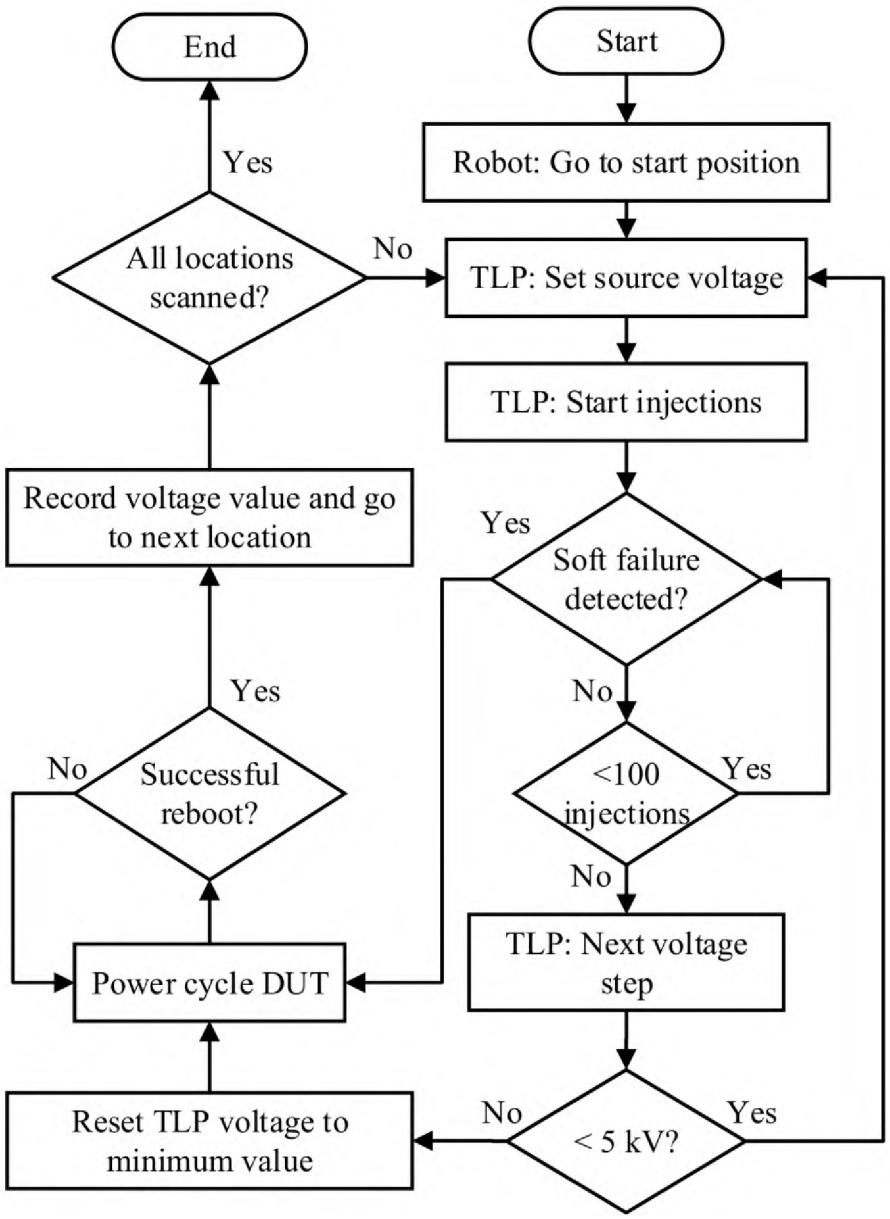


Figure 4. Automated ESD scanner functionality flowchart.

2.2. SYSTEM FLOWCHART

Figure 4 shows the flowchart of the automated ESD scanner. Turning on the system causes the robot arm to move to the start position and power up the BBB. The voltage of the TLP source is set to a preset value (defined by the user). Once a successful boot is confirmed, the system starts injecting ESD noise on the BBB via the Hz probe. The Arduino increases the TLP voltage to the next step if no failure detected and more than 100 injections performed. The voltage steps are logarithmically spaced to minimize the total number of voltage steps for covering the whole voltage range of the TLP source (0 V to 5 kV). In this paper, 15 voltage steps were used. Once the final voltage step is reached, the robot arm moves to the next location, the source voltage goes to the default value, and injection starts again. If the BBB fails during any of the mentioned stages, the source voltage, which caused the failure, and the probe coordinates are recorded. The system then power-cycles the BBB. On the other hand, if no failure is detected and the maximum TLP voltage (5 kV) is reached, the Arduino power-cycles the BBB and requests MATLAB to move the probe to the next location. These processes continue until the entire IC (i.e., all 120 locations) is scanned.

For the BBB, the most common failures are CPU hang, and reduction of the clock frequency to 300 MHz or 500 MHz. The CPU hang is detected by comparing the blinking rate of the onboard LED against a timer (in Arduino). When the LED stops blinking (i.e., a failure occurred), the timer overflows, and a failure flag is set. The other common failure, (i.e., reduction in the clock frequency) can be detected by monitoring the current consumption waveform of the BBB. Once the clock frequency reduces, the current

consumption decreases resulting in no more trigger generation and; hence, raising a failure flag.

3. EFFECT OF CPU CONDITIONS ON ESD SUSCEPTIBILITY

3.1. CPU LOADING

Three different CPU loadings are <5%, ~50%, and ~100%. The lowest load (<5%) is created by putting the system in standby mode; i.e., no additional code is running. The 50% load is generated by using a freely available code named "CPU-load-generator." This code can generate an arbitrary CPU load from 1% to 99% using a pulse width modulation (PWM) technique. The highest load (100%) is created using a code developed by the authors. The code fully loads the CPU by running intensive mathematical calculations (multiplication, division, and addition) in a loop. The effect of CPU loads on the susceptibility of the IC is then investigated using the automated ESD scanner.

Figure 5 shows the ESD susceptibility map of the BBB CPU for various software loadings at 1 GHz clock frequency. The ESD susceptibility maps depict the sensitive regions of the IC to ESD noise and the corresponding TLP source voltage at each location. For this study, knowing the TLP source voltage is sufficient as the maps are compared together. The blue regions in the maps indicate the locations where the IC did not fail at all while the dark red regions show the most sensitive locations of the IC. The largeness of the orange/red regions (i.e., area), and/or the redness of the regions (i.e.,

color) indicate the increased sensitivity. In some cases, only one of the two factors can indicate the increased sensitivity as will be shown later.

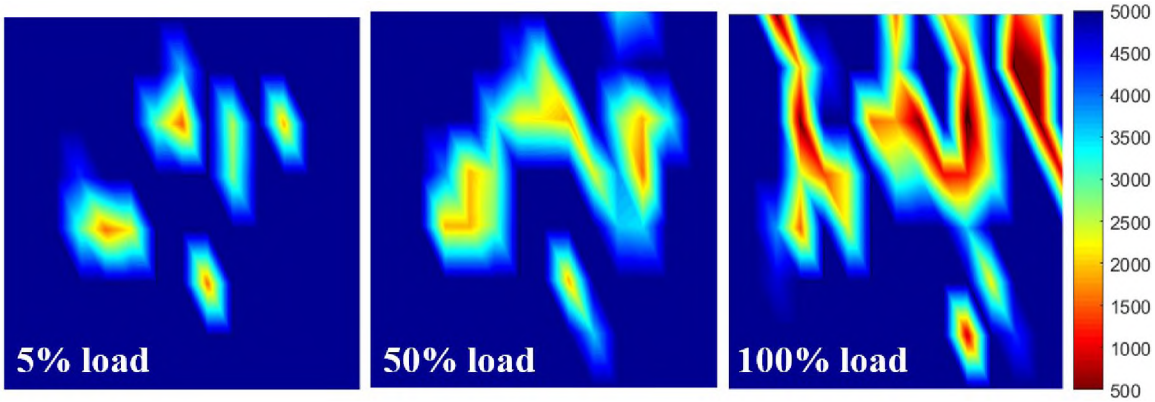


Figure 5. ESD susceptibility map of the BeagleBone Black CPU for various software loadings at 1 GHz.

3.2. CLOCK FREQUENCY AND VDD VOLTAGE

Besides the CPU loading, CPU clock frequency may also affect the sensitivity of the CPU. The underlying thought is that the upper limit of the clock frequency is often given by signal integrity inside the IC. As the signal integrity of the IC diminishes with increasing the clock frequency, it is plausible to expect increased sensitivity for the IC. Investigation of the effect of the clock frequency requires full control over the CPU frequency. In other words, the operating system must be unable to control the clock frequency once it is set by the user. Such level of control, over the system, calls for administrative control (or root access) which may not be granted by default. Once this access is acquired, the automated scanner can be used to obtain ESD sensitivity maps as a function of CPU clock frequency. Figure 6 shows the ESD susceptibility map of the BBB CPU obtained for various clock frequencies at 50% loading. Contrary to one's

expectation, the CPU became more robust as the clock frequency increased. This observation can be explained as follows:

On the BBB board, there is a power management IC (PMIC) which provides and manages different VDD voltages for different parts of the board. Once a higher CPU clock speed is requested, the CPU communicates with the PMIC through an I2C bus requesting a higher voltage on CPU VDD_Core pin. According to the CPU datasheet [8], the VDD_Core voltage can vary between 1.056 V and 1.144 V. A higher VDD_Core voltage makes the IC more robust because a larger ESD event is required to cause a failure. As a measure for quantifying and comparing the IC robustness, the number of locations in Figure 6 with a TLP voltage of less than 700 V and less than 3 kV is counted and shown in Table 1. As indicated by this figure and Table 1, the IC becomes less susceptible, as the VDD_Core increases.

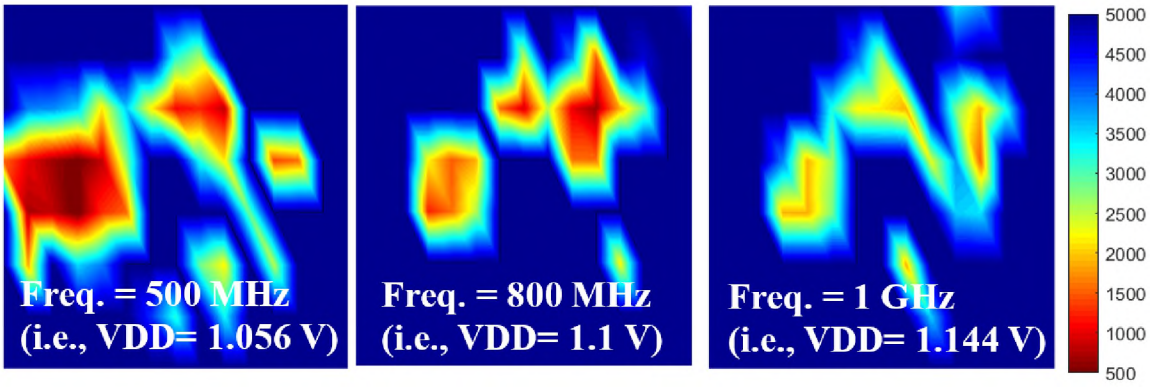


Figure 6. ESD susceptibility map of the BeagleBone Black CPU for various clock frequencies (/VDD_Core voltages) at 50% load.

Another measure for quantifying the IC robustness could be the minimum TLP voltage needed to upset the IC at each clock frequency. As shown in Figure 7, the

minimum TLP voltage increases by 275%; i.e., from ~400 V to ~1500 V as the VDD_Core voltage increases by ~8%; i.e., from 1.056 V to 1.144 V. One may argue that the IC robustness should increase accordingly (~8%); however, it increased by 275%. Due to lack of deep understanding of this IC and its failure mechanisms, this argument could not be addressed fully. A plausible explanation, however, could be given by considering the available voltage margins for the ESD event at each VDD_Core (/clock frequency) voltage.

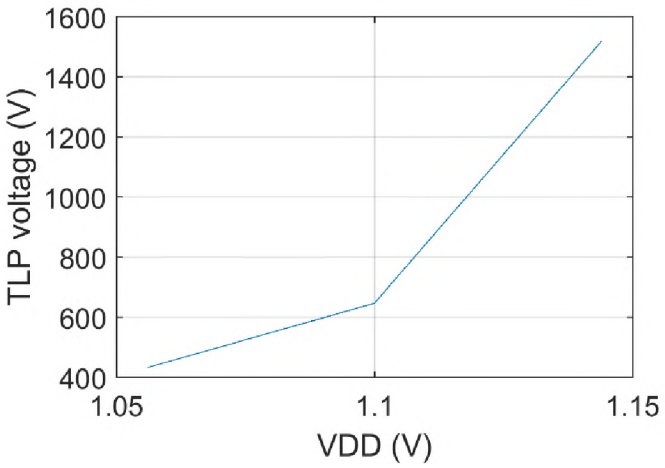


Figure 7. Minimum TLP voltage at each clock frequency (/VDD_Core voltage).

As shown in Figure 8, the VDD_Core voltage can swing between 1.056 V to 1.144 V. Assuming the lowest VDD_Core voltage at which the IC can function properly is 1 V, there is a 56 mV margin for the ESD event to cause a failure when the VDD_Core voltage is at 1.056 V, whereas the margin is 144 mV when the VDD_Core voltage is at 1.144 V. Therefore, the available margin for the ESD noise increases by 256% which is

close to the observed increase of 275%. This point of view can explain the observed increase of the TLP voltage in Figure 7.

Table 1. Number of locations (out of 120) with a TLP voltage less than 700 V and 3 kV at various VDD_Core voltages (/clock frequencies).

	1.056 V	**1.1 V**	**1.144 V**
<700 V	3	1	0
<3 kV	25	18	14

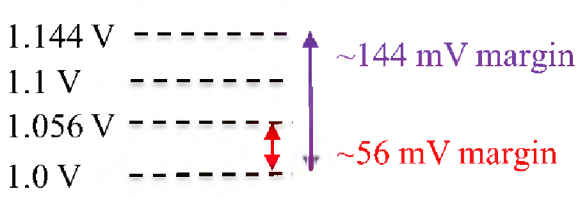


Figure 8. Available voltage margin for the ESD noise.

3.3. PDN NOISE AND IMPEDANCE

Increasing the PDN impedance, and consequently, the PDN noise of the BBB may cause the CPU to become more susceptible to ESD events. This investigation requires removal of all decoupling capacitors (decaps) connected to the VDD_Core voltage rail. Since the capacitor in the LC filter of the PMIC DC-DC converter can also act as a decoupling capacitor, it must be removed too. However, removal of this capacitor prevents the DC-DC converter from operating. A workaround is to add a low pass filter consisting of a ferrite bead paralleled with a low value (2 Ω) resistor between the capacitor and the rest of the circuit. Therefore, the capacitor cannot act as a decap and the DC-DC converter is not disturbed anymore.

Figure 9 compares the PDN impedance for the case where all decaps are removed (green trace) to the case where no decaps are removed (blue trace). The bump at ~2 MHz in the green trace is caused by the 2 Ω resistor. At higher frequencies, the 2 Ω resistor is dominated by the impedance of the PDN inductance (~3 nH). For the case where no decaps are removed, 12 dB/dec slope of the blue trace at higher frequencies suggests that the impedance is not purely inductive. Figure 9 clearly shows that the PDN impedance increases when all the decaps are removed.

Removing the decaps also affects the PDN noise. Figure 10 and Figure 11 show the PDN noise as a function of removed decaps at 50% and 100% loading, respectively. The peak to peak noise voltage increased from ~6 mV to ~80 mV for both load conditions. In Figure 11, the voltage spikes are present regardless of the presence of the decaps; removing the decaps only increased the magnitude of the spikes. Figure 12 and Figure 13 illustrate the effect of removing decaps in the frequency domain for 50% and 100% loading, respectively. As observed, the broadband noise level increased by ~10 dB whereas the magnitude of the harmonics increased by ~10 to 35 dB. Moreover, comparing Figure 12 (a) with Figure 13 (a), and Figure 12 (b) with Figure 13 (b) suggest no additional harmonic is generated when the CPU load increases from 50% to 100%. Only the amplitude of the spikes increases.

By intuition, one may expect the CPU sensitivity to increase when the decaps are removed. This hypothesis is tested by obtaining the susceptibility map for various CPU loadings, and clock frequencies before and after the decaps are removed. Figure 14 shows the ESD susceptibility map of the CPU for 50% and 100% loading when the CPU clock

frequency is set at 1 GHz. For both loadings, the CPU becomes more sensitive when the decaps are removed. However, this is not the case at all clock frequencies.

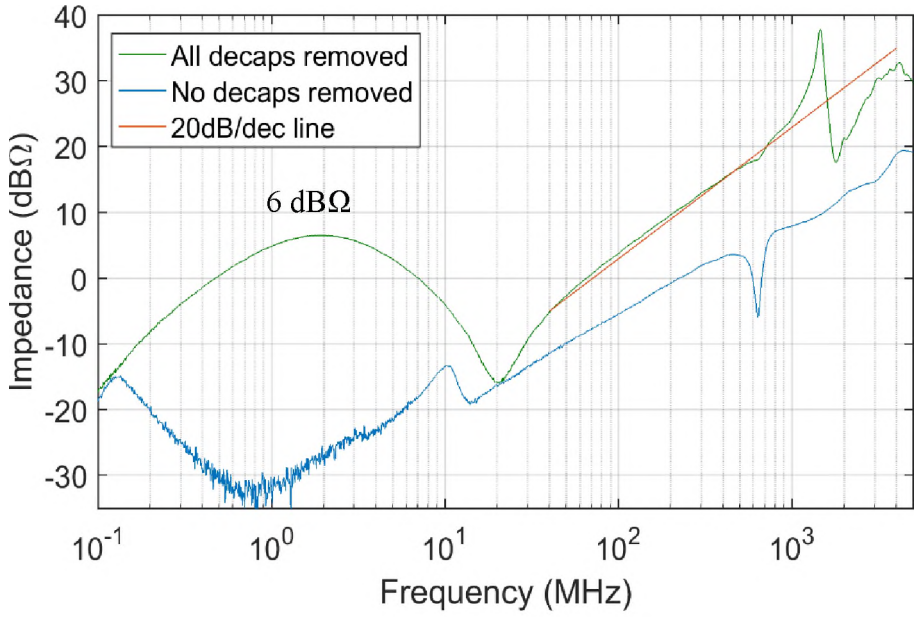
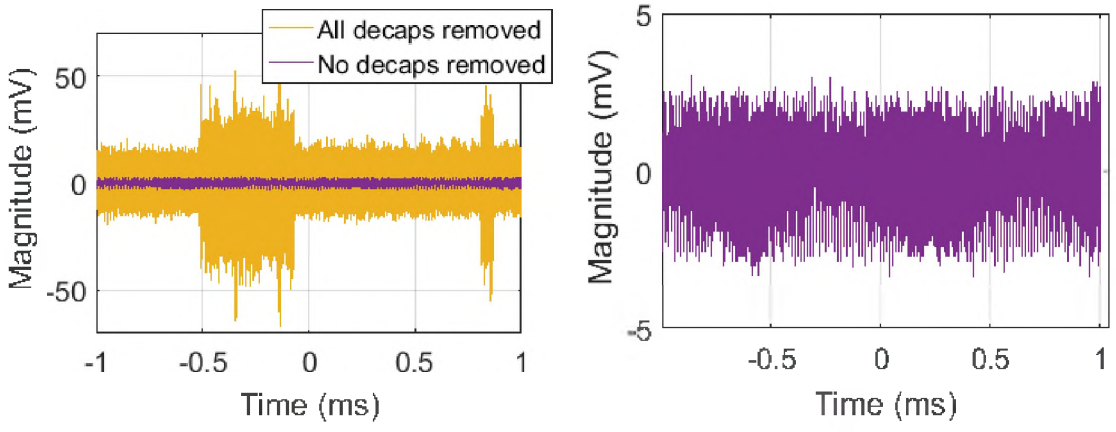
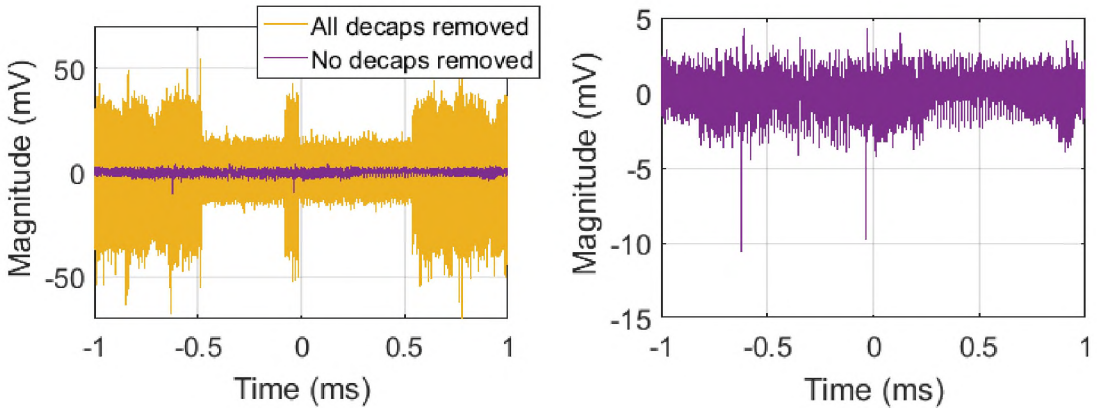


Figure 9. Effect of low pass filter on the PDN impedance of the BBB.



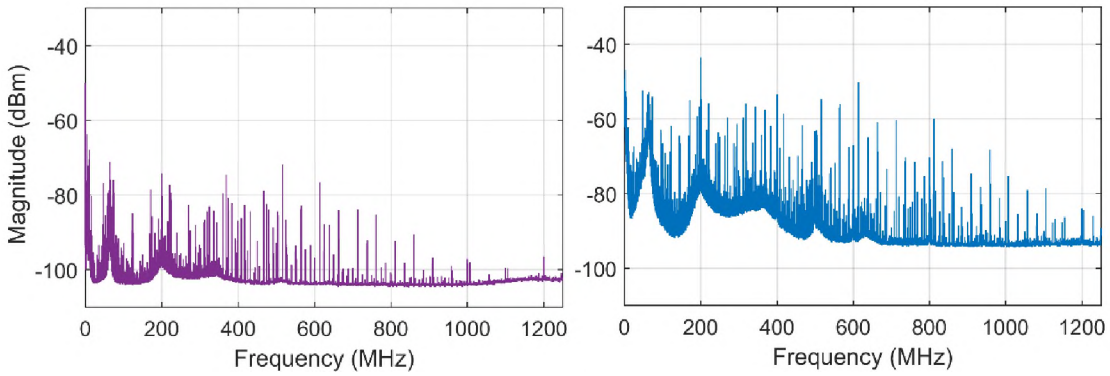
a b

Figure 10. PDN noise as a function of removed decaps at 50% CPU load. a) Noise before and after removing decaps. b) Close up view of the noise before removing decaps.



a b

Figure 11. PDN noise as a function of removed decaps at 100% CPU load. a) Noise before and after removing decaps. b) Close up view of the noise before removing decaps.



a b

Figure 12. PDN noise in frequency domain for the 50% CPU load. a) No decap removed. b) All decaps removed.

Figure 15 illustrates the effect of removing the decaps at various clock frequencies. As shown, the IC becomes more sensitive after removing the decaps when the clock frequency is 500 MHz and 1 GHz. Due to the visual similarity of the plots, the sensitivity is quantified by counting the number of locations with a TLP voltage of less than 700 V and less than 3 kV. Table 2 and Table 3 show the number of locations that

require <3 kV to fail increased by 32% and 107% at 500 MHz and 1000 MHz, respectively when the decaps are removed. Despite Figure 15 (a) and (c) which suggest the IC becomes more sensitive after removing decaps, Figure 15 (b) suggests the IC becomes more robust when the decaps are removed. The core reason for this behavior is not clear to the authors; however, this discrepancy can be diminished by taking into account the minimum TLP voltage, before and after removing the decaps as follows.

In Figure 15 (b), the minimum TLP voltage for the with-decaps case is 650 V; whereas, it is 340 V for the decaps removed case. This reduction in the TLP voltage indicates the IC becomes more sensitive after removing the decaps. However, the increased sensitivity is only reflected in the form of reduced minimum TLP voltage and not enlarged (non-blue) area as was the case in Figure 15 (a) and (b). Although the root cause of these observations is not clear to the authors, this result suggests that the behavior of complicated ICs can be deeply investigated using high-resolution susceptibility maps obtained by the ESD scanner.

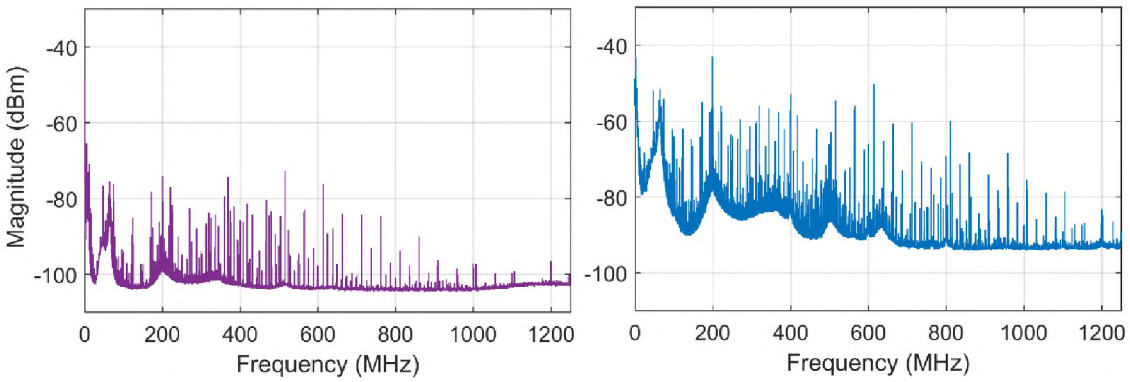
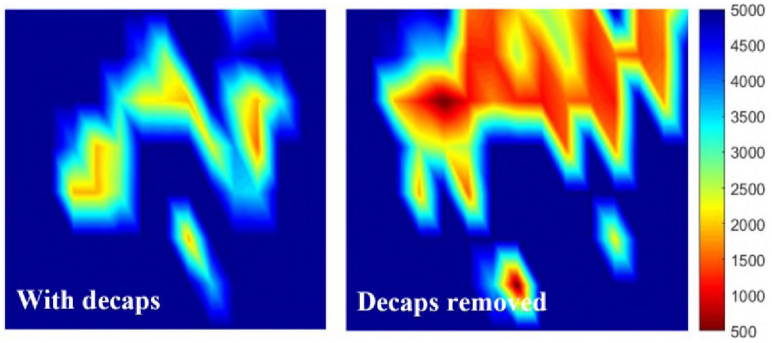
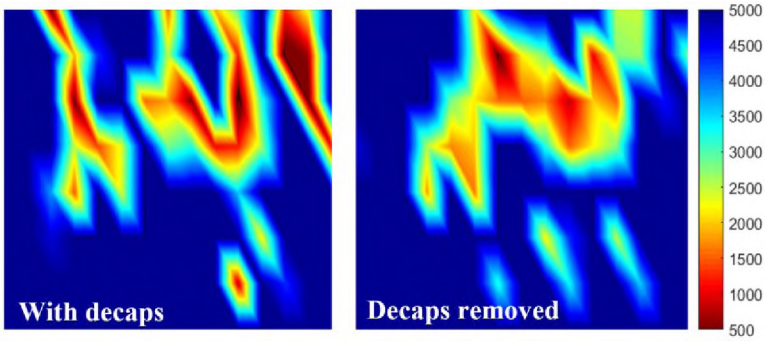


Figure 13. PDN noise in frequency domain for the 100% CPU load. a) No decap removed. b) All decaps removed.



a



b

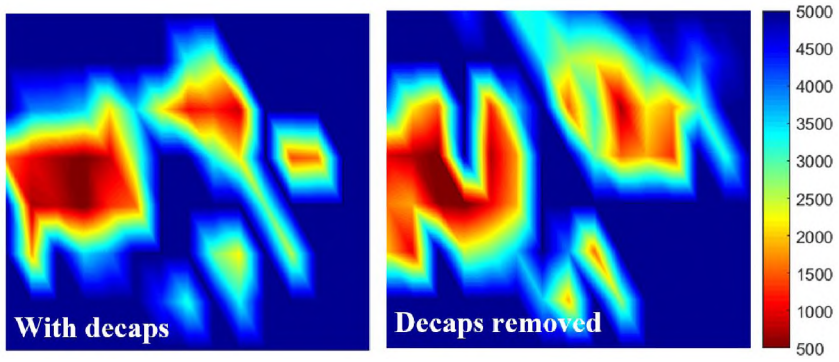
Figure 14. Effect removing decaps on CPU susceptibility. a) 50% CPU load. b) 100% CPU load.

Table 2. Number of locations (out of 120) with a TLP voltage less than 700 V and or less than 3 kV at the clock frequency of 500 MHz.

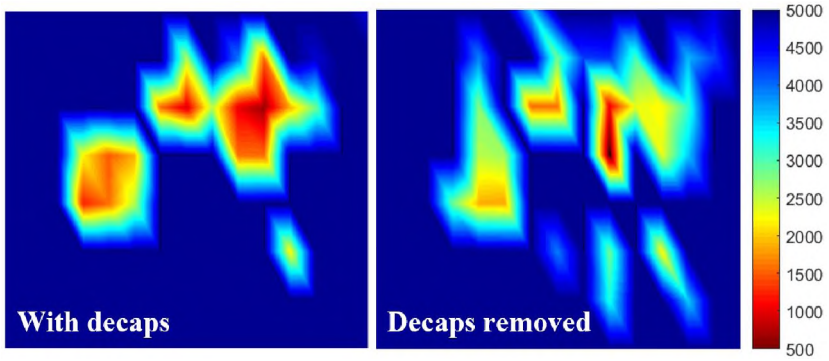
	With decaps	**Decaps removed**
<700 V	3	4
<3 kV	25	33

Table 3. Number of locations (out of 120) with a TLP voltage less than 700 V and or less than 3 kV at the clock frequency of 1000 MHz.

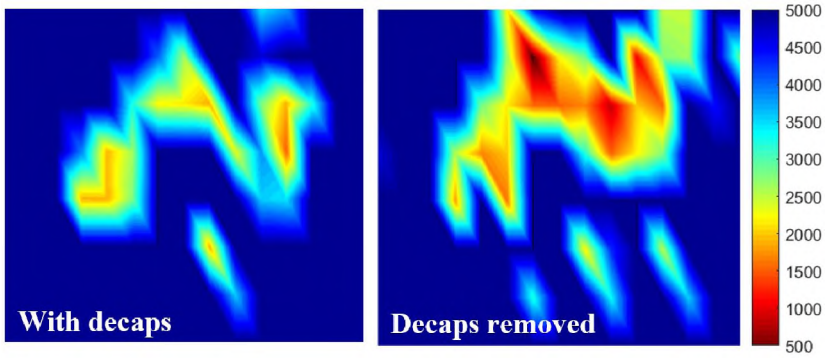
	With decaps	**Decaps removed**
<700 V	0	1
<3 kV	14	29



a



b



c

Figure 15. Effect of removing decaps on CPU susceptibility for various clock frequencies. a) 500 MHz. b) 800 MHz. c) 1000 MHz.

4. SUMMARY AND CONCLUSION

The effect of several operating conditions on the susceptibility of the BeagleBone Black CPU was systematically explored. Due to the large number of required tests for this investigation, an automated scanner was developed. Our investigations showed the IC became more sensitive as its load increased. However, contrary to our expectations, increasing the clock frequency caused the IC to become more robust. The reason for this observation was attributed to an increase of the VDD core voltage of the CPU. Furthermore, the effect of removing decaps on the sensitivity of the CPU was investigated. Although the PDN noise and PDN impedance increased when the decaps were removed, the CPU sensitivity did not always increase.

If the goal is to make a system sensitive to ESD without any modifications to the hardware, one should select a high load for the core processor and a low VDD voltage. Removing decaps will further increase the sensitivity. Motivated by the results obtained from this work, more DUTs will be tested to acquire a broader picture of the behavior of the core processors as a function of different operating conditions.

REFERENCES

[1] K. Mohanram, N. A. Touba, "Cost-effective approach for reducing soft error failure rate in logic circuits," in Test Conference, 2003. Proceedings. ITC 2003. International, pp. 893 - 901, 2003.

[2] S. Vora, R. Jiang, S. Vasudevan, and E. Rosenbaum, "Application level investigation of system-level ESD-induced soft failures," presented at the 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), IEEE, pp. 1-10, 2016.

[3] N. A. Thomson, Y. Xiu, and E. Rosenbaum, "Soft-Failures Induced by System-Level ESD," IEEE Transactions on Device and Materials Reliability, vol. 17, no. 1, pp. 90-98, 2017.

[4] A. Hosseinbeig, O. H. Izadi, S. Shinde, D. Pommerenke, H. Shumiya, J. Maeshima, and K. Araki, "A Study on Correlation Between Near-Field EMI Scan and ESD Susceptibility of ICs," presented at the 2017 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), Washington DC, pp. 169-174, 2017.

[5] K. Wang, D. Pommerenke, Zhang, J. Min, and R. Chundru, "The PCB level ESD immunity study by using 3 dimension ESD scan system," in Electromagnetic Compatibility, 2004 International Symposium on, pp. 343-348, 2004.

[6] G. Muchaidze, J. Koo, Q. Cai, T. Li, L. Han, A. Martwick, K. Wang, J. Min, J. Drewniak, and D. Pommerenke, "Susceptibility scanning as a failure analysis tool for system-level electrostatic discharge (ESD) problems," IEEE Transactions on Electromagnetic Compatibility, vol. 50, pp. 268-276, 2008.

[7] Amber Precision Instruments, "www.amberpi.com."

[8] Texas Instruments, "AM335x Sitara™ Processors," Oct. 2011 [Revised April 2016].

.

II. ANALYSIS OF CPU LOADING EFFECT ON ESD SUSCEPTIBILITY

Omid Hoseini Izadi
Department of Electrical Engineering
Missouri University of Science and Technology, Rolla, MO, 65409
E-mail: ohp63@mst.edu

ABSTRACT

Two complementary approaches are presented to help to understand how CPU loading affects the sensitivity of an electronic device to ESD (electrostatic discharge) stress. Both approaches rely on synchronized noise injection while the software is running at the desired load. One of the approaches monitors the device's current consumption while the other monitors the device's electromagnetic field to synchronize noise injections. These approaches revealed that as the CPU loading increases, the device becomes more active and hence more susceptible to ESD stress. Moreover, it was observed that, in each loading condition, the device randomly became susceptible. These complementary approaches enable the capturing of high/low active intervals as well as the injection of noise voltage to the desired activity, thus, allowing for the analysis of the effect of CPU loading on ESD susceptibility.

1. INTRODUCTION

Soft failure investigations are necessary for evaluating the ESD (electrostatic discharge) susceptibility of an electronic device. Soft failure is a temporary upset,

disturbing the normal operation of the devices. Soft failures are resolved either automatically after a short time (a few seconds) or by power-cycling the device [1, 2]. Latch-ups and permanent damages (hard failures) could also happen as a result of ESD events [3]; however, they are out of the scope of this paper.

For soft failure investigation, the operating condition of the device under test (DUT) should be considered, as the DUT's susceptibility can change when the operating condition changes [4]. Reference [5] has shown that the DUT became more sensitive to ESD when the system loading increased. It also reported that increasing or decreasing the CPU frequency can affect sensitivity. In [6], the authors observed that, while a file compression program was running, other soft failure types occurred other than those related to the display. These studies suggest that higher system loading leads to higher sensitivity.

On the contrary, other studies did not observe a similar trend. Reference [7] reported no correlation between DUT sensitivity and system loading.

In the mentioned works, the ESD noise voltage was injected randomly; i.e., the injections were not associated with any particular activity of the DUT. As will be discussed in the following sections, random injection is not a suitable approach for evaluating the effect of system loading on device susceptibility. A better approach is to correlate ESD injections with the DUT activity; in other words, the injections should be synchronized to a particular activity, to understand the effect of system loading on the device susceptibility.

In this paper, two complementary approaches are presented for synchronizing the noise injection to the device activity. The first approach performs injections synchronous

to the current consumption waveform, whereas, the second approach uses electromagnetic interference (EMI). Finally, using a smartphone as our DUT, the approaches are put to the test and compared.

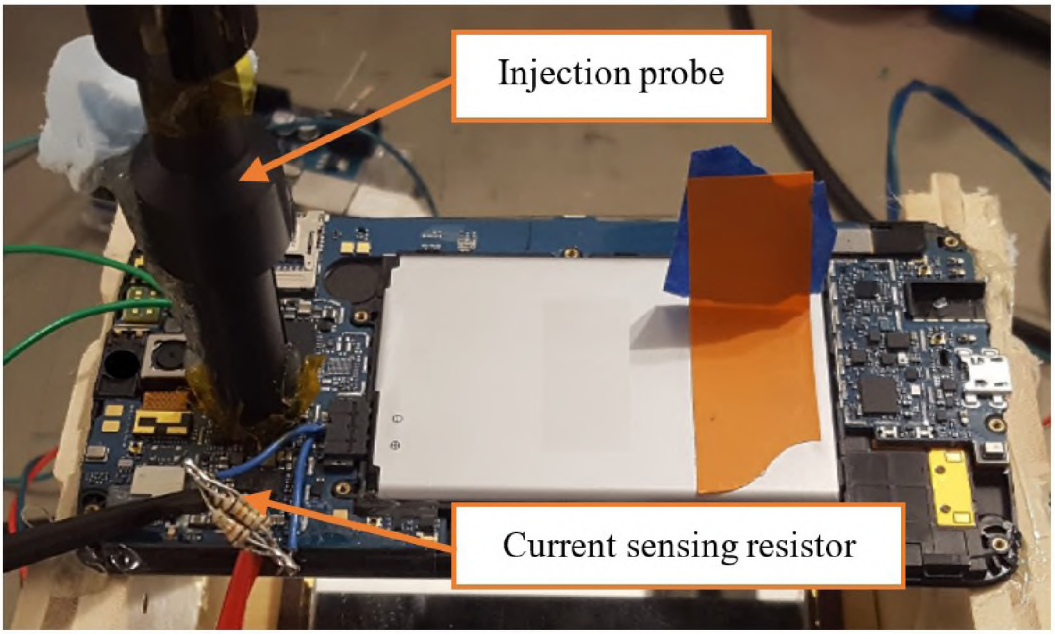
2. CURRENT CONSUMPTION-BASED SYNCHRONIZATION METHOD

2.1. MEASUREMENT SETUP

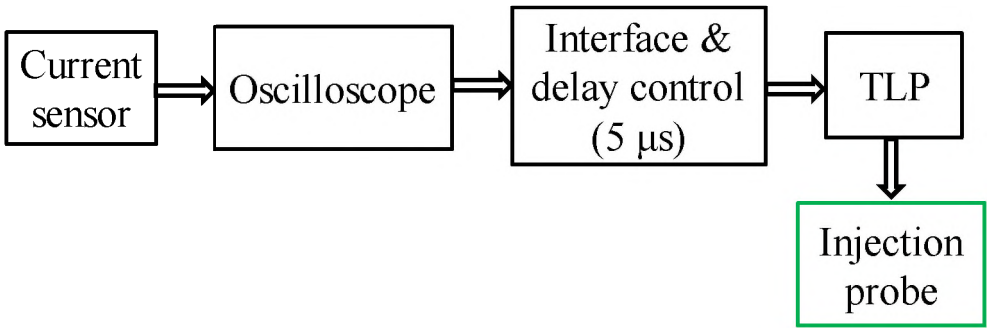
Figure 1 shows the block diagram and the measurement setup. The current sensor is a resistor placed in series with the entire PCB of the device and is used to monitor the instantaneous current consumption of the device. The voltage drop across this resistor is monitored by an oscilloscope. The oscilloscope is set to generate a trigger signal to the TLP (transmission line pulse) generator whenever the current waveform exceeds a user-defined level, which will be henceforth referred to as the trigger level. Because the trigger level depends on the CPU loading and CPU frequency of the DUT, it should be set at the peak of the current waveform in order to trigger on high activity intervals, as shown by the horizontal dashed lines in Figure 2. Similarly, the trigger level is set at the valley points for targeting low activity intervals. With these settings, the oscilloscope is triggered whenever the current consumption crosses the trigger level (dashed line). The generated trigger passes through the delay-control block, gets delayed, and then is fed to the TLP. The delay block compensates for the delay added by the other blocks.

An 8-mm magnetic field probe is used to inject noise into the DUT. When driven by 1 A of current, this probe can couple about 10 mA of current into a 1×0.5 mm loop

placed 1 mm below the probe. A detailed explanation is provided about the injection probe in [5].



a



b

Figure 1. Current consumption-based synchronization measurement setup. a) Injection probe and DUT. b) Block diagram of entire setup. The delay control circuitry has ~5 µs delay, which is negligible compared to the 3.4 ms delay of the TLP generator.

2.2. SYNCHRONIZATION REQUIREMENTS

For a successful synchronization, the following requirements should be satisfied.

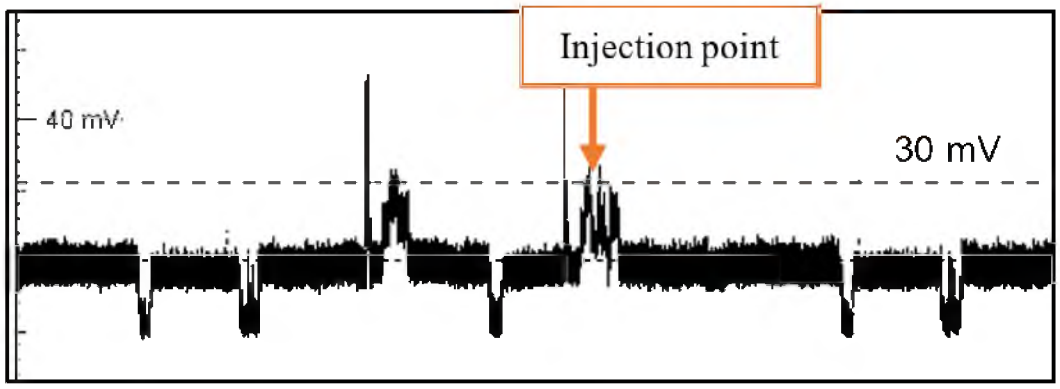
- Steady clock frequency: If the DUT clock frequency can be controlled through software, the user should fix the clock frequency. This can reduce the variations of the current consumption waveform caused by CPU frequency hops. We set the CPU frequency of our DUT at 1 GHz.
- Known delay: The delay between the moment that the oscilloscope is triggered and when the actual pulse appears at the TLP output should be known with sub-millisecond uncertainty. Most of this delay comes from the TLP relay. A mercury relay can reduce the uncertainty to less than 1 ms. The delay caused by the TLP is 3.4 ms ± 1 ms. The delay caused by the other blocks is in the range of a few micro-seconds and thus is neglected.
- An additional delay should often be added to the total delay such that the injection occurs at the next active interval. For instance, in Figure 2c, the valley point repeats every ~6 ms, thus, an additional delay of 6-3.4 = 2.6 ms should be added so that the injection happens at the next active interval. Although the current consumption waveform is not periodic in general, especially at low CPU loadings and low clock frequencies, the waveform starts to show a semi-periodic behavior as the CPU loading and the clock frequency increase, as observed in Figure 2a, 2b, and 2c.

To generate different CPU loadings, it is recommended to employ a software designed for this purpose. A simple infinite loop with arithmetic calculation can intensely

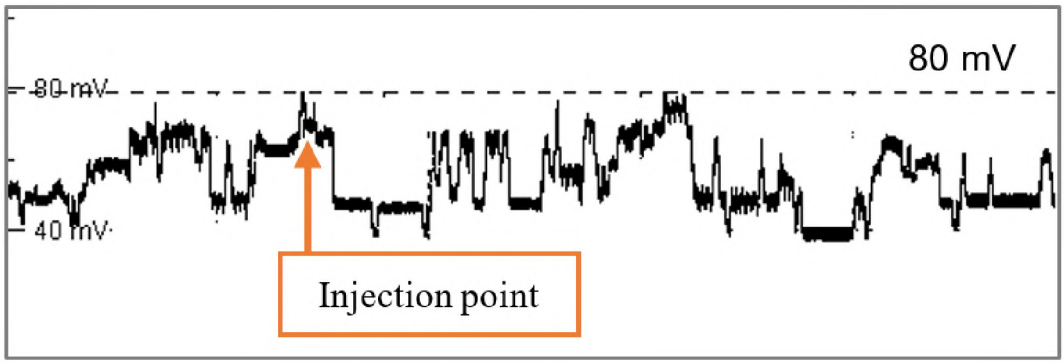
load the CPU; however, other parts of the system (RAM, graphic IC, etc.) may not be involved as much as the CPU. Moreover, in case of the loop, the CPU loading intensity cannot be changed – The load would always be close to 100%. In this study, a low load condition (below 10%) was created by leaving the DUT in standby without running any additional software except for the already running system-related tasks. For creating medium load (~50%), a video recording app was used, which could load the graphic IC, RAM, and CPU to some extent. Since this app had not been designed for generating a well-defined load, the activity of the CPU does not have a specific pattern (see Figure 2b). This lack of pattern adds uncertainty to the trigger timing. For high load (above 90%), an app called StressCPU ([8]) was used. This app could create a steady load for the CPU and RAM, as shown in Figure 2c.

2.3. PERFORMING SYNCHRONIZED INJECTION AND ANALYSIS

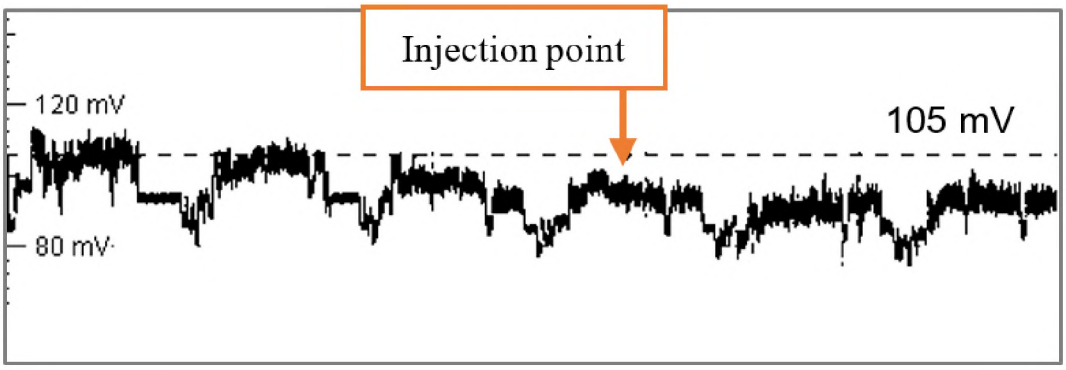
A smartphone is used as our device under test (DUT). Its CPU frequency can hop between 300, 500, 800, 1000, and 1200 MHz, which can be controlled by software. Due to the lack of proper heat transfer between the CPU and the environment, we limited the frequency to 1000 MHz. This limitation is imposed because the injection probe directly lands on top of the CPU, which reduces the heat transfer rate. For frequencies below 500 MHz, the current consumption waveform changes irregularly and smoothly, therefore, it was difficult to achieve synchronization, hence the 1000 MHz frequency. To prevent the overheat protection circuitry from kicking in and reducing the CPU frequency by hardware (forcefully), an external fan cools down the CPU.



a



b



c

Figure 2. Current consumption of the device under test under different CPU loading. a) *Low load* (<10%). b) *Medium load* (~50%). c) *High load* (>90%). The CPU frequency was fixed at 1 GHz. The noise was injected during the marked low and high activity periods.

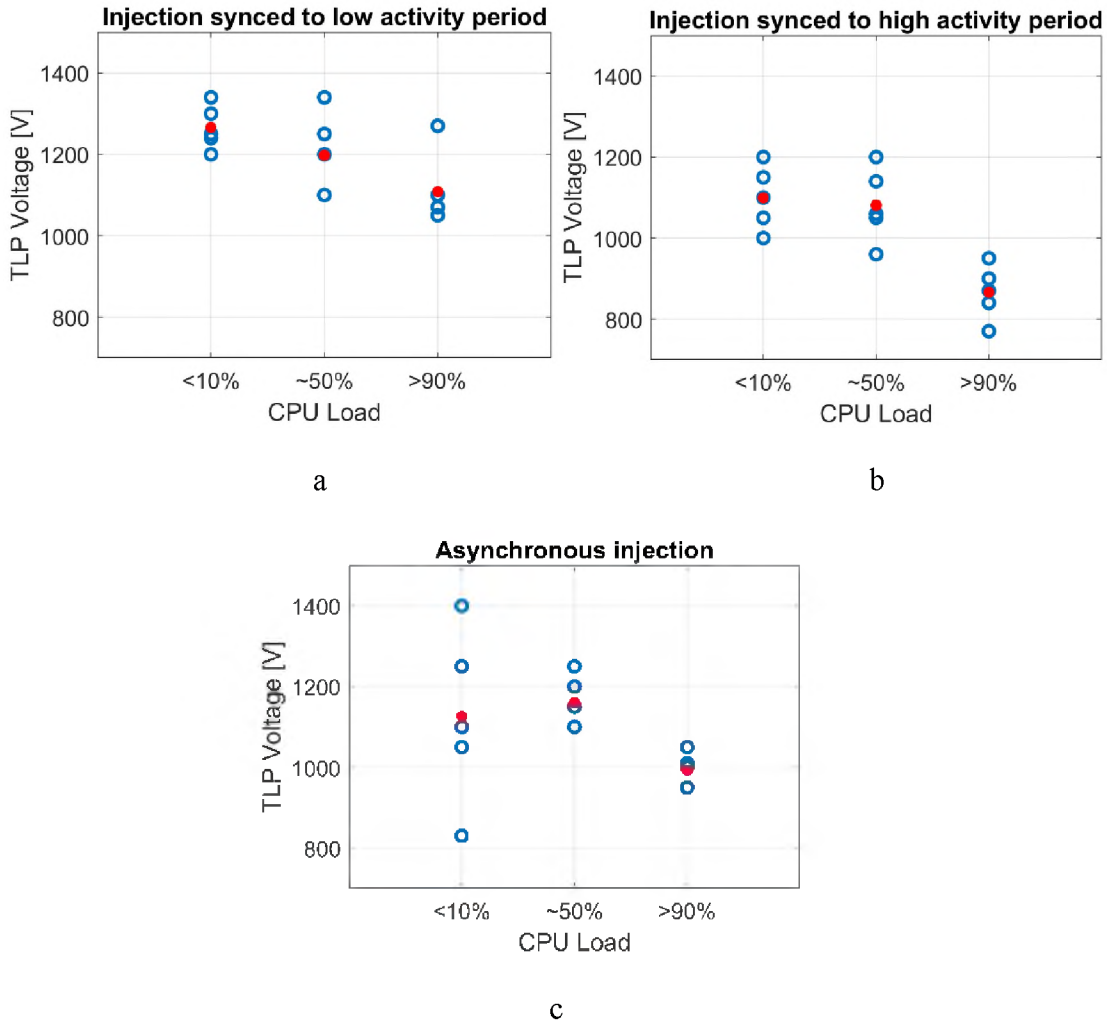


Figure 3. TLP voltage causing a soft failure vs. CPU load. a) Synchronized to low activity. b) Synchronized to high activity. c) Random injection.

The TLP source voltage is increased from 0 to 5 kV until a soft failure was observed. The voltage that caused this soft failure is recorded, and the DUT is power cycled to return the DUT to its condition before the soft failure occurrence. Repeating these steps for low load, medium load, and high load conditions gives us the TLP voltage at which the DUT soft-failed vs. CPU load, as shown in Figure 3. Figure 3a, 3b, and 3c are obtained by synchronizing the injections to the low activity period of the CPU

(corresponding to Figure 2a), synchronizing to high activity period (corresponding to Figure 2c), and injecting randomly (asynchronously), respectively. The red asterisk illustrates the average value (of the five repetitions). The following observation can be made from Figure 3:

For synchronized injection (Figure 3a and 3b), as the CPU load increases the CPU becomes more sensitive, i.e., lower TLP voltages cause a soft failure. Ideally, the CPU sensitivity should not be affected, as the CPU was stressed during a particular activity period (in low or high corresponding to Figure 3a and 3b). However, this ideal case is not achievable because: (1) The CPU loading momentarily fluctuates due to system-related apps, housekeeping, or other system activities that are not under the user control; (2) during high load condition (see Figure 2c), the valley point of the current consumption waveform does not revert to the low value of low load condition (see Figure 2a); in other words, the CPU loading baseline value increases as the load increases.

Figure 3b is obtained by synchronizing the injections to high activity periods. As expected, the CPU becomes more susceptible when it is highly active. One may also expect that the CPU sensitivity should remain steady and high, regardless of the loading condition, since the injections are synchronized to high activity periods. This contradiction can be explained using the irregular behavior of the system mentioned above.

Moreover, it is observed that the average value (red asterisk) in each loading condition in Figure 3a is higher than the corresponding loading condition in the asynchronous scenario (Figure 3c). This observation suggests the CPU is more robust when it is stressed during its low activity intervals.

Finally, Figure 3c shows the results for asynchronous injection. Since the injections are performed randomly for this plot, it is expected to have a poor repeatability or in other words a large distribution, especially at lower loads. As the load increases, the idle intervals reduce and become less frequent, drastically reducing the chance of hitting a valley point. This trend can be observed in the current consumption waveforms shown in Figure 2.

Although the current-based synchronization approach can improve repeatability and reduce the uncertainty of the results, its major downside is its requirement for monitoring the current consumption of the target IC. For a device with one CPU IC, this requirement can be met; however, if more than one CPU IC exists on the device, this approach may fail because the total current consumption of the entire device is not a good indicator of the target IC activity. An alternative approach is to employ the EMI-based synchronization method.

3. EMI-BASED SYNCHRONIZATION METHOD

3.1. MEASUREMENT SETUP

The electromagnetic (EM) field of an IC usually has a broad frequency range. It can consist of both broad and narrow band spectral components. Some of these components may vary as the activity level of the IC changes. These components can be filtered out and used to trigger the TLP.

Figure 4 shows the measurement block diagram. The detection loop picks up the field generated by the IC of interest. The acquired signal is then amplified and fed to a

super-heterodyne bandpass filter, which includes a fixed bandpass filter with 1.575 GHz center frequency and 5 MHz bandwidth, two mixers, and one synthesized source. The target frequency is mixed up to fall in the filter bandwidth and then mixed down to the baseband (0-90 MHz). This process allows sweeping through many frequencies without changing the setup. The outputted signal triggers the oscilloscope, and then the TLP after being adjusted by the delay-control block.

The selected frequency to pass through the filter and trigger the TLP should be unique for each loading condition. A frequency that is used for, namely, low load condition should not appear in the spectrum of high load or medium load. Moreover, in each loading condition, the magnitude of the selected frequency should significantly fluctuate with activity – at least 10 dB is suggested. The biggest challenge of this method is finding a frequency that satisfies these requirements. As shown in Figure 5, there are many frequencies to be examined. The selected frequencies in this study are 1.138 GHz, 1.600 GHz, and 1.200 GHz for low load, medium load, and high load conditions, respectively.

Figure 6 compares the current consumption of the device (same smartphone used in the other approach) with the signal picked-up by the loop after the super-heterodyne filter in each loading condition. As clearly observed in Figure 6b and 6c, the current consumption waveform resembles that of the selected frequency, validating the frequency selection for these loads. In low load conditions, the DUT is in standby; thus, the signal picked up by the loop has a relatively constant amplitude, as there is not much change in the DUT's activity in standby; however, as encircled in Figure 6a, a pattern with small

magnitude fluctuation can be observed in the filtered signal. The TLP is triggered based on this pattern.

As for the medium load shown in Figure 6b, as discussed before, a media recording app was employed to generate this load; thus, the CPU activity has an irregular pattern, adding uncertainty to the trigger timing. This lack of pattern can be observed both in the current waveform and the behavior of the selected frequency component.

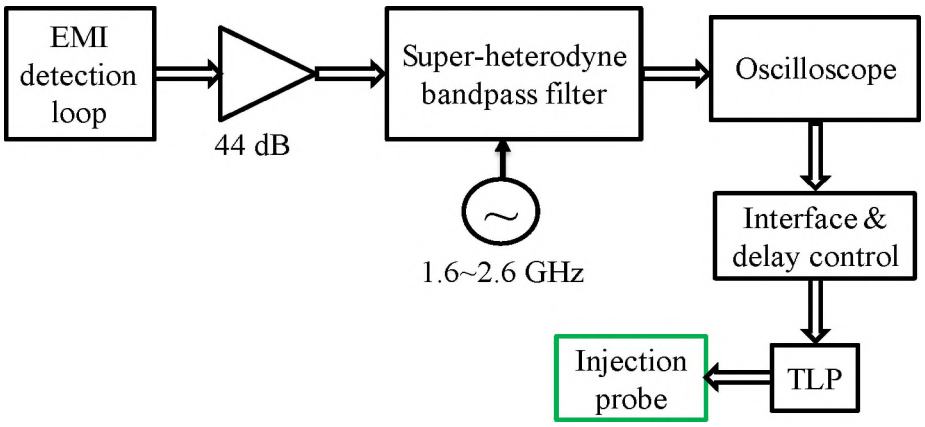


Figure 4. Measurement block diagram for EMI-based synchronization method.

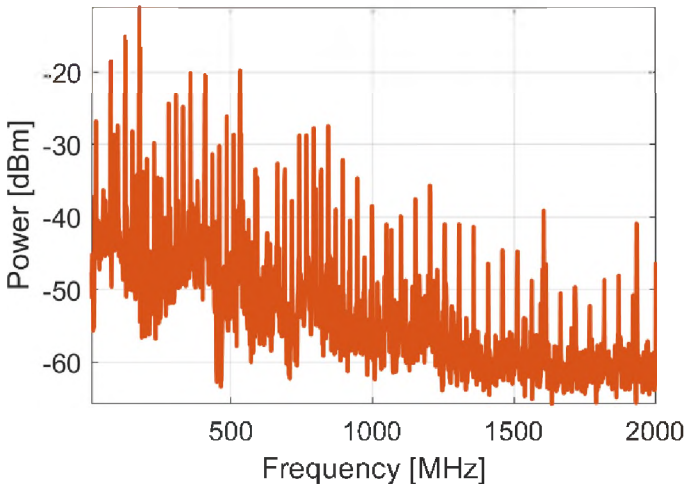
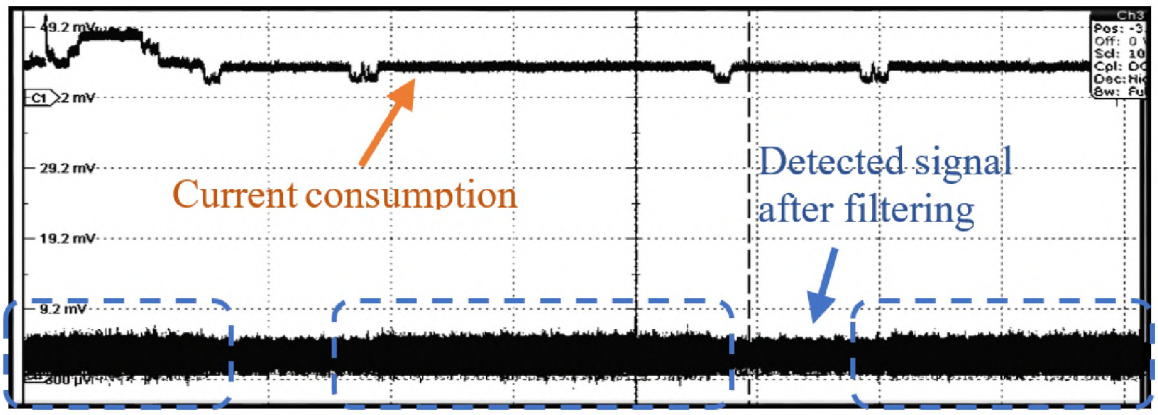
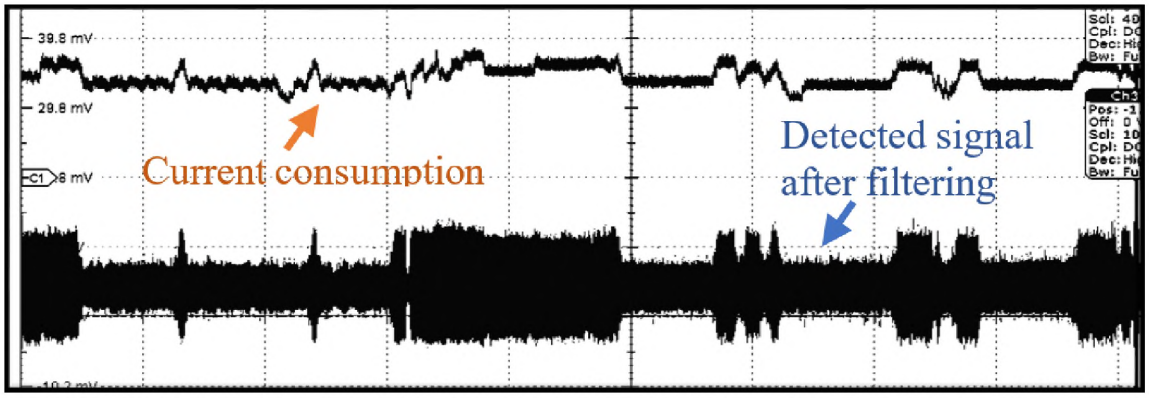


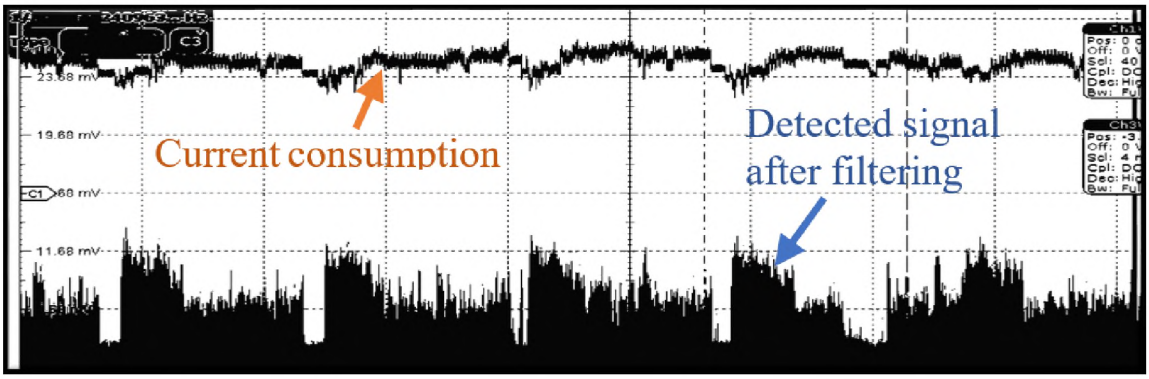
Figure 5. Amplified spectrum of the IC under test picked up by the detection loop.



a



b



c

Figure 6. Current consumption waveform compared to the picked-up signal by the detection loop after the super-heterodyne filter. a) Low load. b) Medium load. c) High load.

As observed in Figure 6c, the filtered signal not only has a semi-periodic feature, but it also has large amplitude variation. Therefore, it is expected that the failure voltages be relatively less spread out, and the IC be more sensitive in high load. This is discussed in the following section.

3.2. PERFORMING SYNCHRONIZED INJECTION AND ANALYSIS

Figure 7 shows the TLP voltage at which the DUT soft-failed vs. CPU load when injections are synchronized to the high activity periods. The decreasing mean value for an increasing CPU load, suggests that the susceptibility of the device increases when the CPU loading increases, i.e., a lower TLP voltage is needed to cause a failure. This behavior is consistent between both synchronization methods. Comparing Figure 7 with Figure 3c (asynchronous injection), one can observe that a much better uncertainly is achieved at low load (<10%). Comparing Figure 7 with its counterpart, Figure 3b, one can observe that (1) the data has a large distribution especially at medium load, and (2) the failure voltages are usually higher.

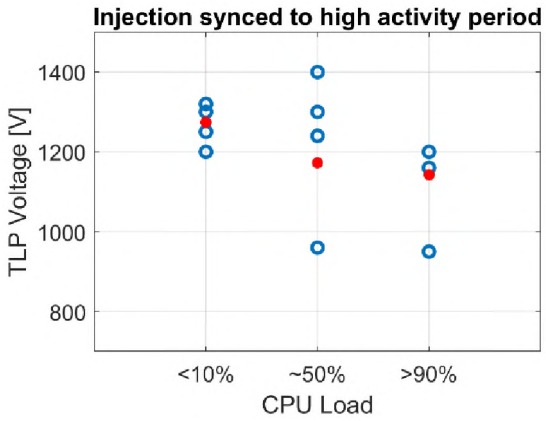


Figure 7. TLP voltage causing a soft failure vs. CPU load.

These observations suggest that the EMI-based method should be used as a complementary approach for the current consumption approach, or where current monitoring is not possible.

4. DISCUSSION

4.1. RELATIONSHIP BETWEEN LEVEL OF CPU ACTIVITY AND ESD SUSCEPTIBILITY

The proposed test methods enable us to analyze the level of CPU activity with respect to ESD susceptibility. Some possible physical explanation behind the proportional relationship between the level of CPU activity and ESD susceptibility are:

- When the system is highly active, the system draws more power from the power distribution network (PDN), leading to increased PDN noise. As pointed out in [5], higher PDN noise can lead to higher ESD sensitivity. Higher CPU frequencies exacerbate the situation, as expressed by Equation (1):

$$V(f) = I(f).Z(f), \tag{1}$$

where V is the voltage drop across the impedance of the power distribution network (Z), and I is the current drawn by the CPU.

- During high CPU activity intervals, more subsystems are turned on, compared to those of the low CPU activity intervals. If one or more subsystems that are only ON during high CPU activity intervals are more sensitive to ESD than others and get disturbed by ESD, the resulting soft

failure can propagate throughout the system and be observed by the user. However, if the subsystem is OFF its failure may remain hidden.

4.2. MULTI-CORE CPU

The CPU of the smartphone under test shown in Figure 1 is a Quad-core CPU, which consists of four ARM Cortex A7 CPUs as well as embedded peripherals such as USB, Bluetooth and Wi-Fi, Cellular Modem, GPU and Display modules. It is assumed that most of the current is consumed by the processors, not the peripherals; therefore, the active low and high intervals in the current waveform are caused by the processor activity.

Due to the multi-core architecture of such CPUs, in general, it is not clear how, namely, a 50% load is distributed between the cores. However, for the CPU tested here, a 100% load completely loads all 4 cores of the CPU. This was verified using a system monitoring app. For a 50% load, since the camera app is being used to generate this load, the load distribution is not uniform between the cores. Which is to say that the loading of the cores fluctuates. These fluctuations can be limited by preventing the CPU frequency to hop (which was done here) and/or use an app to generate a 50% load. The latter could not be achieved because of the lack of the needed skills for Android programming. In a similar study, however, a code was written in Python to generate the desired load. The DUT was BeagleBone Black with a Linux-based operating system called Debian.

4.3. LEVEL OF SENSITIVITY FOR CPU AND RAM

In a different study, where a BeagleBone Black is used as the DUT, the EMI-based synchronization method was performed on the RAM IC. It is observed that the RAM is not as susceptible as the CPU. This observation may be different for different DUTs.

4.4. ABSOLUTE TLP VOLTAGE LEVEL VS. TREND

The average TLP voltage obtained from the current-based approach is slightly lower than the EMI-based approach under the same loading condition. This difference is rooted in different test setups. The authors have observed that a 0.2-mm change in the injection probe height can change failure TLP voltage. Therefore, absolute TLP voltage levels can vary (and should not be compared), while the trend is comparable.

5. SUMMARY AND CONCLUSION

Motivated by the observed contradiction between different studies regarding the effect of CPU loading on ESD susceptibility, we presented two approaches to synchronize noise injection with CPU activity and take into account the effect of CPU loading. Using the current consumption-based synchronization method, we observed that the IC became more sensitive as its load increased. Also, we noticed that regardless of the loading condition, the IC susceptibility increased during high activity intervals. While the former shows how the IC behaves as a function of loading condition, the latter shows how the IC behaves in millisecond windows during each loading condition. Due to these

millisecond active intervals, the asynchronized (random) injection approach could not show how sensitive the IC became under ESD stress. The main drawback of the current-based approach was the need to access and monitor the current consumed by the target IC, which could be impractical in certain devices, such as multi-layered PCBs, or if only one of the many CPU ICs is to be tested. Alternatively, the EMI-based synchronization approach was presented, which monitored the near field of the target IC, instead of its current consumption. Using the EMI-based method, we observed that the target IC became more sensitive as its load increased, a trend consistent with that of the current-based method. The most prominent advantage of the EMI-based method was at low loads (<10%) because there was less variability in the results (compare Figure 7 with Figure 3b). Therefore, the two methods should not be used interchangeably, but complementarily. If the load cannot generate a pattern in the current consumption waveform, the EMI-based method should be used instead.

REFERENCES

[1] Nicholas A Thomson, Yang Xiu, and Elyse Rosenbaum, "Soft-Failures Induced by System-Level ESD," IEEE Transactions on Device and Materials Reliability, vol. 17, pp. 90-98, 2017.

[2] Omid Hoseini Izadi, David Pommerenke, Hideki Shumiya, and Kenji Araki, "Investigation of Electrostatic Discharge-Induced Soft-Failure Using 3d Robotic Scanning," in 2019 IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+ SIPI), 2019, pp. 173-177.

[3] Ki Hyuk Kim, Jeong-Hoi Koo, Bong-Gyu Kang, Soon Jae Kwon, Yongsup Kim, and Joongho Jeong, "Systematic Design Technique for Improvements of Mobile Phone's Immunity to Electrostatic Discharge Soft Failures," in 2010 IEEE International Symposium on Electromagnetic Compatibility, 2010, pp. 348-353.

[4] Ahmad Hosseinbeig, Omid Hoseini Izadi, Satyajeet Shinde, David Pommerenke, Hideki Shumiya, Junji Maeshima, and Kenji Araki, "A Study on Correlation between near-Field Emi Scan and ESD Susceptibility of Ics," in 2017 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), 2017, pp. 169-174.

[5] Omid Hoseini Izadi, Ahmad Hosseinbeig, David Pommerenke, Hideki Shumiya, Junji Maeshima, and Kenji Araki, "Systematic Analysis of ESD-Induced Soft-Failures as a Function of Operating Conditions," in 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018, pp. 286-291.

[6] Sandeep Vora, Rui Jiang, Shobha Vasudevan, and Elyse Rosenbaum, "Application Level Investigation of System-Level ESD-Induced Soft Failures," in 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), 2016, pp. 1-10.

[7] Giorgi Maghlakelidze, Pengyu Wei, Wei Huang, Harald Gossner, and David Pommerenke, "Pin Specific ESD Soft Failure Characterization Using a Fully Automated Set-Up," in 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), 2018, pp. 1-9.

[8] Frank Sabath, Daniel Nitsch, Markus Jung, and Thomas HGG Weise, "Design and Setup of a Short Pulse Simulator for Susceptibility Investigations," IEEE Transactions on Plasma Science, vol. 30, pp. 1722-1727, 2002.

III. AUTOMATED DETECTION AND CHARACTERIZATION OF ESD-INDUCED SOFT FAILURES USING IMAGE- AND AUDIO-BASED METHODS

Omid Hoseini Izadi
Department of Electrical Engineering
Missouri University of Science and Technology, Rolla, MO, 65409
E-mail: ohp63@mst.edu

ABSTRACT

Audio- and image-based soft failure detection methods are developed, which can detect both severe failures (such as system hang) and subtle ones (such as glitch or a momentary disturbance on display). Incorporating the developed detection methods with a robotic ESD (electrostatic discharge) tester, we developed a fully automated soft failure investigation tool. Using this fully automated tool, we obtained failure-specific susceptibility maps for a camera (our target device). These susceptibility maps not only illustrated the sensitive locations of the device, they also showed what type of soft failure is correlated with which locations.

1. INTRODUCTION

When an electrostatic discharge (ESD) occurs, the victim device may experience a latch-up event, permanent hardware damage (hard failure), or a temporary upset (soft failure). Soft failures are temporary and can be solved by power-cycling the device. For soft failure immunity testing, one can manually perform a few tests to quickly and approximately locate the sensitive locations of the target device; however, for a

systematic investigation, manual testing is not the correct approach. For a systematic investigation, it is strongly advised to employ automatization, as manual testing has poor repeatability and is time-consuming. Additionally, the likelihood of soft failure occurrence can depend on the operating conditions, as investigated in [1], which means even more tests might be required. Under these conditions, automatization is the best approach.

Automatization can improve repeatability, reduce human mistakes, and in general, can produce reliable results; however, it calls for (1) an automated tester for moving the injection probe, injecting ESD noise, controlling noise source voltage, etc., and (2) soft failure detection and decision making. The focus of this paper is the second requirement – soft failure detection and decision making – as the first requirement is rather well established in the literature. For instance, [2] used a planar scanner to move an injection probe on the target device and obtain susceptibility maps for the CPU (central processing unit) of the device under test (DUT). Reference [1] used a planar scanner to systematically investigate the relationship between soft failures and operating conditions by studying the susceptibility maps of the DUT. Both these studies monitored the DUT's DC current consumption in order to detect a soft failure; whenever the current consumption exceeded a defined value, a failure flag was raised.

Soft failures can be detected by other methods besides DC current consumption. [3-5] investigated several other methods and elaborated on their effectiveness in detecting a failure. These methods are listed in Table 1. Among these methods, Down-mixing, Short Term Fourier Transform (STFT), Kernel calls, and Wavelet Transformation require adaptive post-processing; i.e., an operator must adaptively tweak the methods'

parameters in order to find the irregularity caused by the soft failure(s) in the recorded data. Thermal imaging works best for failures that lead to a temperature change (usually a temperature rise), which is commonly associated with latch-ups. DC current consumption method is simple and effective, however, cannot detect failures that do not cause an abnormal change in the current consumption, such as multi-colored stripes on the display or a glitch on the display. These are considered failures to the human eye and should not be missed. For the Spectral method to detect a failure, the spectral variations caused by the failure should be abnormally larger than what it is in normal operation. According to [4], this method is effective only 31% of the time. Table 1 compares these methods in terms of their requirements.

Many of the presented methods lack the ability to detect soft failure independent of an operator; they also have lengthy post-processing times [1, 2]. On the other hand, simple methods such as DC current consumption and Spectral method are not reliable for soft failure detection as they miss failures that do not cause abnormal current consumption or abnormal spectral content.

This paper is an extension to our previous paper ([6]); it presents a new, different approach that allows for the detection of soft failures in a similar manner that humans do – through hearing and sight. Thus, it is effective for the class of devices with a display or a speaker. A few examples of this class are phones, professional and cinematic cameras, amateur cameras, sound systems, music players, smart speakers, etc. Any failure that can be detected by the user can also be detected by this approach. The biggest challenge is the detection of both severe failures such as a system hang or restart, as well as the subtle ones such as a momentary display malfunction, defocus, etc.

Table 1. Soft failure detection methods.

Method	Post-processing?	Specific requirement?
Short Term Fourier Transform (STFT)	Yes	Parameter tweak by a human
DC current consumption	No	No
Thermal imaging	No	- Infra-red camera - line-of-sight between the DUT components and the camera
Wavelet Transformation	Yes	Parameter tweak by a human
Down-mixing (to audio band)	Yes	Parameter tweak by a human
Spectral method	No	No
Kernel calls	Yes	- Parameter tweak by a human - Dedicated serial port on DUT

In the following sections, we will elaborate on our soft failure detection approach. Using a camera and a music player as our target DUT, we develop image-based and audio-based detection and characterization methods; then we combine these methods with a 6-axis robot to achieve automatization. Finally, the combined system is used to demonstrate automated soft failure testing for a different DUT.

2. AUTOMATED ESD TESTING

2.1. SYSTEM BLOCK DIAGRAM

Figure 1 shows the system block diagram of the automated ESD tester. An industrial Mitsubishi 6-axis robot is used to move the injection probe on the DUT. The 6-

axis robot can approach the DUT from any direction and at any angle allowing us to test complex 3-D objects [6].

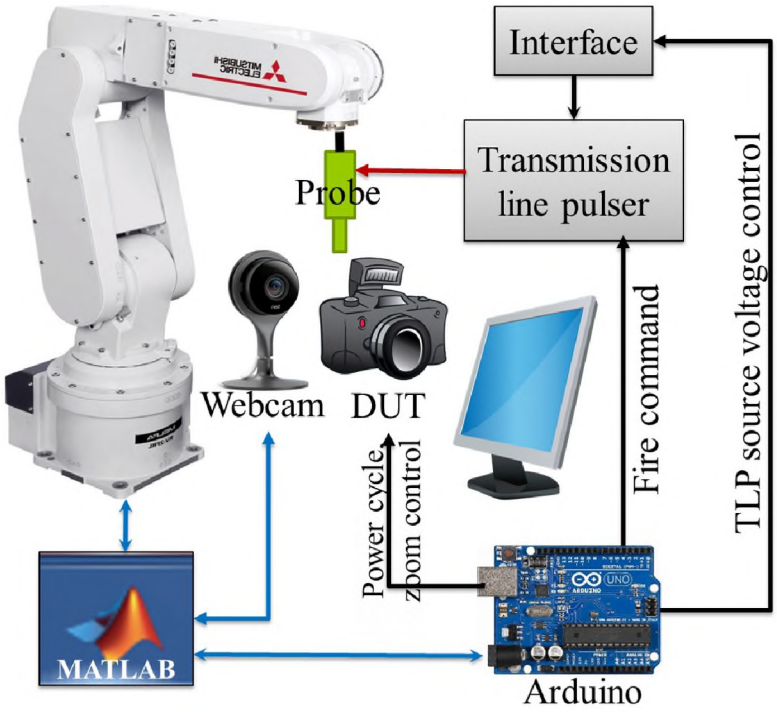


Figure 1. Block diagram of the automated ESD tester when a camera is used as the DUT. For the case of a music player as the DUT, the webcam is replaced with a mic, and the monitor is removed.

The DUT (camera) is set to look at the monitor while the monitor is playing a video. A webcam, which is connected to MATLAB, is focused on the DUT display. The webcam image resolution is set to 400×300 pixels – higher resolution is not necessary. With this image size, about five images can be processed per second. The procedure is simple: once the captured image is processed, another image is taken by the webcam, transferred to MATLAB to be processed. A higher rate was not needed because the DUT reaction to a failure was relatively slow (in the range of couple of seconds).

Figure 2 shows the system flowchart of the automated ESD tester. The flowchart is self-explanatory and is already explained in detail in [1] and [6]; however, the necessary blocks are explained here. The algorithms used to decide if the DUT failed ("DUT failed?" block in Figure 2) are the core part of this paper and will be discussed in detail in the following sections.

2.2. IMAGE-BASED SOFT FAILURE DETECTION

Figure 3 shows the soft failure types observed during more than 50 susceptibility tests performed on the DUT (camera). For these tests, an 8 mm magnetic field probe and a transmission line pulse generator with ~7 ns pulse width was used to inject a noise voltage into the DUT. (See [1] for more detail about the probe structure). All flex cables, processors, integrated circuits (IC), etc. were subject to noise injection.

Figure 3a shows the *defocus* failure. It was observed that the injected noise disturbed the control circuitry of the lens, resulting in a defocused image. This failure has an occurrence rate of ~15% (out of 50 preliminary tests) and is considered a severe failure. It can be solved by either re-focusing or power cycling the camera.

Figure 3b illustrates the *vertical strips* failure. It has an occurrence rate of more than 55% and can only be solved by power cycling. Figure 3c illustrates the *vertical gray regions* failure. This failure requires power cycling to be solved and has a small occurrence rate of 5%. Figure 3e is the *frozen-image* failure. With less than 5% occurrence rate, this failure is considered severe too. It needs a power cycle to be solved, as it causes a system hang. Figure 3f shows the *horizontal colored regions* failure. This failure cannot be considered as a severe one, as the colored regions appear and disappear

momentarily, without negative impacts on the normal operation of the DUT. With 5% occurrence rate, it might not be of great concern for a consumer camera but could be of great importance for a professional cinematic camera. Therefore, it is important to detect this failure too. The last failure type is a direct *restart* and is shown in Figure 3d. It has an occurrence rate of more than 15%. In summary, the *vertical strips* failure, *vertical gray regions* failure, *restart* failure, and *frozen-image* failure are considered severe, as they all lead to system hang and/or require a power cycle to be solved. The *horizontal colored regions* failure, however, is considered a subtle failure as it shortly appears and then disappears.

2.2.1. Feature Extraction of Failures. Figure 3a shows the *defocus* failure. Using focus evaluation algorithms, one can evaluate the focus quality of the image. For this evaluation, it is important that both the camera (DUT) and the webcam are focused. Focus quality can be assessed using algorithms such as Absolute Central Moment (ACM), Image Curvature, Brenner's, Thresholded gradient, Helmli's mean method, Histogram entropy, Gaussian derivative, Gray level variance, Energy of gradient, and many more [7]. In this study, the absolute central moment is used as it can distinguish a defocused image from a low contrast one [8]. Equation (1) can be used to calculate the focus measure (FM) using absolute central moment. Figure 4 illustrates how much a low contrast and a defocused image can look alike.

$$f = \sum_{i=0}^{N-1} |i - \mu| p(i), \tag{1}$$

where p is the image histogram, μ is the image mean value, and f is the calculated focus measure.

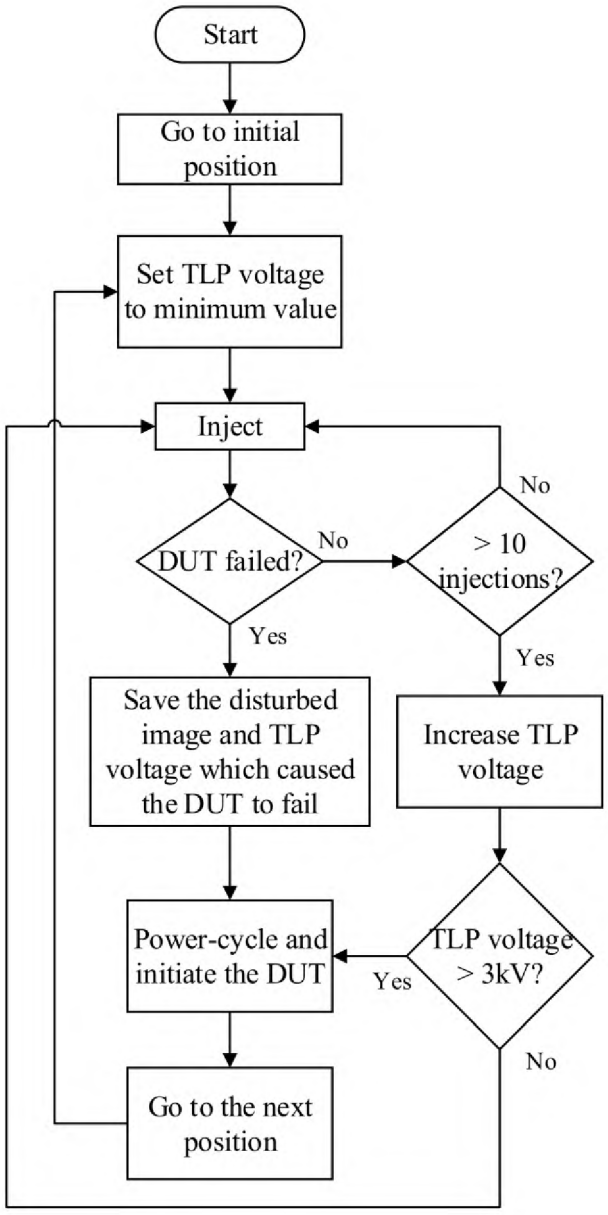
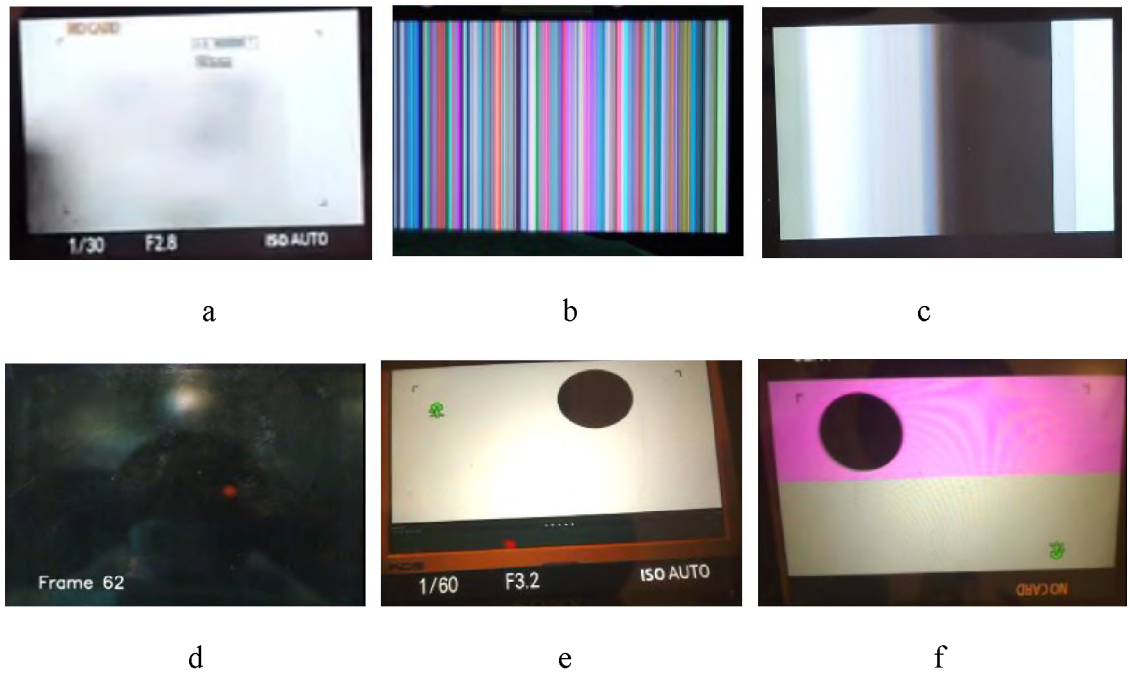


Figure 2. Flowchart of automated ESD tester. The corresponding block diagram is shown in Figure 1.

By comparing the focus measure value of one image calculated by the absolute central moment algorithm with preceding images, one can keep track of changes in the focus measure values and detect a *defocus* failure. The image content does not affect the

focus measure value; thus, failures such as *vertical strips, frozen-image, horizontal colored regions,* and *vertical gray regions* do not change the focus measure value, drastically; whereas, a *restart* significantly affects this value. Therefore, the focus measure is used for both detecting a *restart* and *defocus* failure. A large change in the focus measure value (more than 75%) is considered as a result of a *restart* failure, while smaller changes (less than 75%) are considered to be caused by the *defocus* failure.



a b c

d e f

Figure 3. Observed soft failures for the camera under test. a) Defocus. b) Vertical strips. c) Vertical gray regions. d) Restart. e) Frozen image. f) Horizontal colored regions. After each failure occurrence, the camera was power cycled to revert it to a known state for the next test.

The most obvious features of the *vertical strips* (Figure 3b) failure is the presence of vertical lines in the image. The Canny operator [9, 10] can be used to accentuate the edges in the image. This operator uses two thresholds to keep track of the edges, which

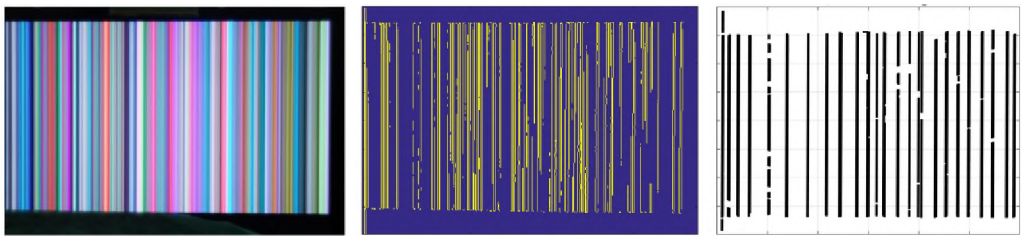
makes it a robust algorithm for edge detection purposes. To quantify the detected edges, a Hough transformation [11, 12] is used after the Canny operator to convert all the edges into line segments. This transformation assigns a value to each line segment, quantifying the line length and population. By comparing the total segment length and count of the current image with previous images, one can keep track of the changes in subsequent images and determine whether a failure occurred or not. Figure 5 illustrates the images resulted after edge detection step and Hough transformation. The total number of lines detected by this approach (Figure 5c) is 228, which is significantly larger than the total lines detected in the image before the failure happened (24 count). In this study, a threshold of 100 lines is used. If the stripes appeared horizontally (or in other directions), the Canny operator and the Hough transformation still can be applied without further changes.

a b c

Figure 4. Comparison between low contrast and defocused image. The similarity can be confusing for an algorithm. a) low contrast image. b) defocused image. c) high contrast image.

The effectiveness of the Canny operator can be improved by applying a line filter such as a Sobel (or Prewitt) operator before applying the Canny operator. The Sobel (or

Prewitt) operator convolves the image with a 3×3 matrix in the vertical and horizontal direction to roughly calculate the gradient of the image intensity in a computationally inexpensive way [13, 14]. The Sobel operator is used in this study, since the lines were vertical. This operator should not be used for tilted lines.



a b c

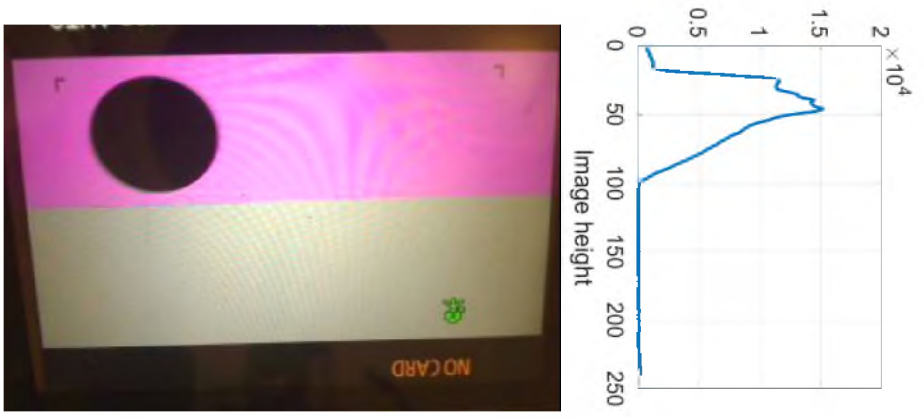
Figure 5. Steps to detect vertical lines in an image. a) Original image. b) Image after edge detection filter. c) Image after Hough transformation. After Hough transformation, the segments' length and count are compared with those of the previous images.

The most prominent feature of the *restart* failure (Figure 3d) is the sudden change of the screen color from mostly white to almost complete black. This sudden change is used for detection of the *restart* failure (in parallel with the focus measure approach). One can simply add up the pixels color data and compare the sum value with that of the baseline image and/or the preceding images. Because of the plain white background in the baseline image, the sum of the pixel color data does not change more than a few percent, even with the movement of the black ball. If the entire display was completely white, a *restart* failure could turn the display black, creating nearly 100% color change; however, because of the presence of the black ball in the image, the *restart*'s change will be less than 100%. In this study, a change more than 95% relative to the baseline image is considered to be due to the *restart* failure. This approach (which is named Area

Difference (AD) by the authors) is not computationally expensive and is easy to implement.

The *Frozen image* failure (Figure 3e) can also be detected by the Area Difference detector. When this failure occurs, the image on the DUT display will not change; therefore, the Area Difference detector would calculate the same value for two back-to-back images. In this study, a difference less than 5% between two consecutive images indicates a *frozen image* failure occurred.

Figure 3f shows the *colored regions* failure. For the camera used in this study, the region appears horizontally and in purple, but it can be of any color and shape. To detect *colored regions* failure, the data of all the pixels in each row is added together, which results in one value for each row. By comparing these values with other rows in the same image, one can determine the occurrence of the *colored regions* failure, as shown in Figure 6. Using Figure 6b, we set the threshold at 0.5e4; a value more than 0.5e4 indicates the *colored regions* failure occurred.



a b

Figure 6. Detection of the colored regions failure. a) Snapshot of the failure. b) Identified rows with a large change in the color data.

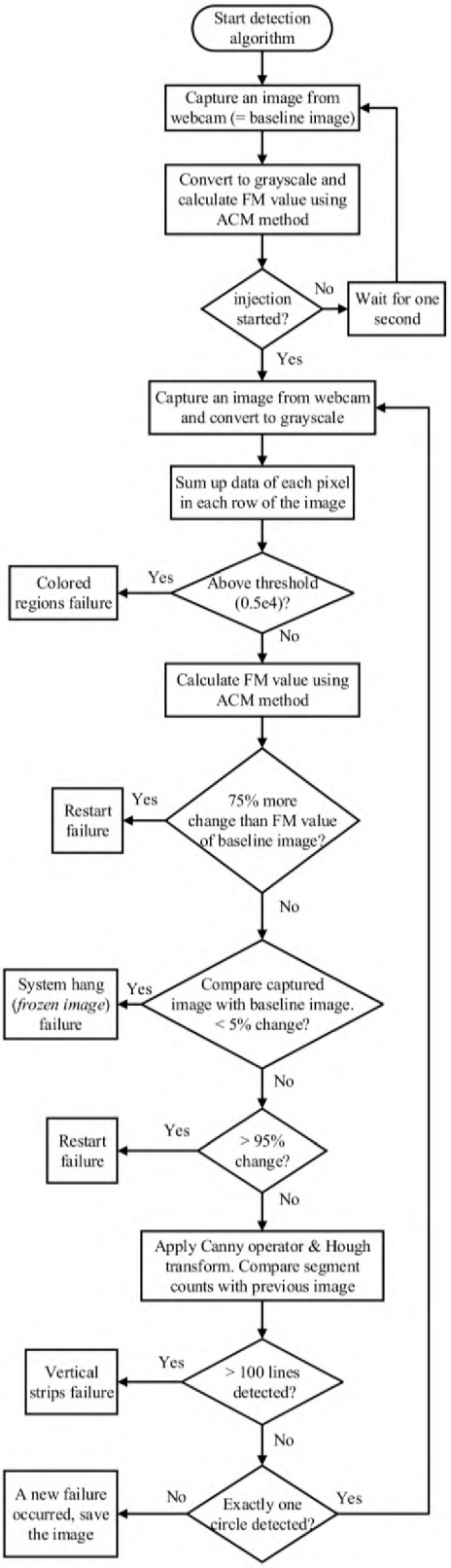


Figure 7. Image-based detection and characterization algorithm flowchart.

This same procedure is performed in vertical direction (for each column), evaluating the presence of a vertical color change in the image. In this way, the *vertical gray regions* (Figure 3c) can also be detected. As for the computational cost, this approach is not expensive as the main mathematical operation is a simple summation. Figure 7 shows the complete flowchart of the image-based soft failure detection algorithm.

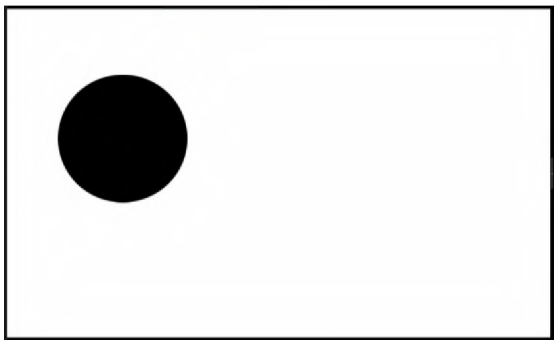


Figure 8. Snapshot of the test video clip, shown on the monitor to the DUT (camera) during the ESD tests.

2.2.1. Test Video. For easier failure detection, a test video has been created to be displayed to the DUT (camera). This test video consists of a white background and a moving black ball. Figure 8 illustrates a snapshot of this test video. Its notable features are plain, white background, black ball, and movement. The white background helps to detect a failure that disturbs color data in the image (such as vertical strips, vertical gray regions, horizontal colored regions, and restart failures shown in Figure 3), the black ball helps to detect defocus failure, and its movement helps to detect the frozen image failure.

2.3. AUDIO-BASED SOFT FAILURE DETECTION

In this section, audio-based soft failure detection algorithm is presented. This algorithm can detect soft failures that cause a change in the audio signal played by the DUT (music player). Similar to the previous section, first we identify the soft failures through a preliminary study, then the distinctive features of the soft failures are determined, and finally suitable algorithms to extract these features are developed.

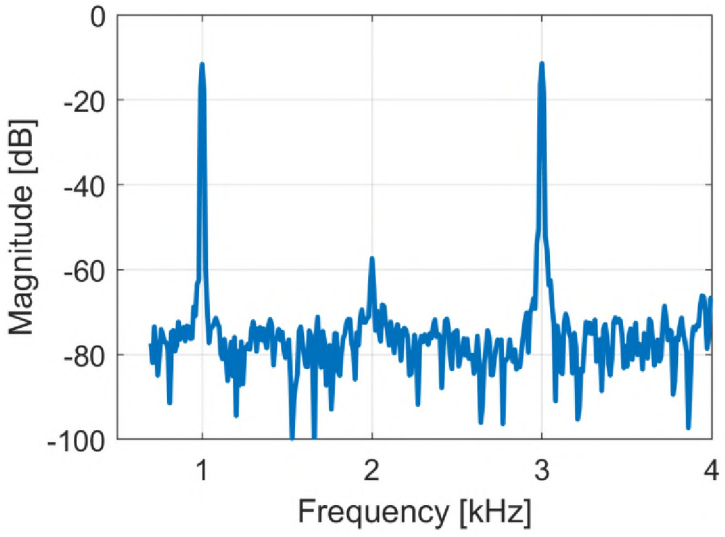


Figure 9. Spectral contents of the test audio in normal operation (no failure). This serves as the baseline audio. The frequency contents below 700 Hz and above 4 kHz are ignored to remove any artifacts around DC, and limit the bandwidth to 4 kHz, respectively.

2.3.1. Test Audio. The test audio track is composed of two single tones at 1 and 3 kHz. This selection allows the detection algorithm to look for certain properties: absolute frequency (two single tones at 1 and 3 kHz), relative frequency distance (2 kHz), and relative magnitude with respect to the noise floor. Figure 9 shows the measured spectral content of the test audio track in normal operation (without any ESD stress). The

second tone was selected to be the 3rd harmonic of the first tone to avoid the appearance of other harmonics as a result of calculating the Fourier Transform in a short period of time (1 second).

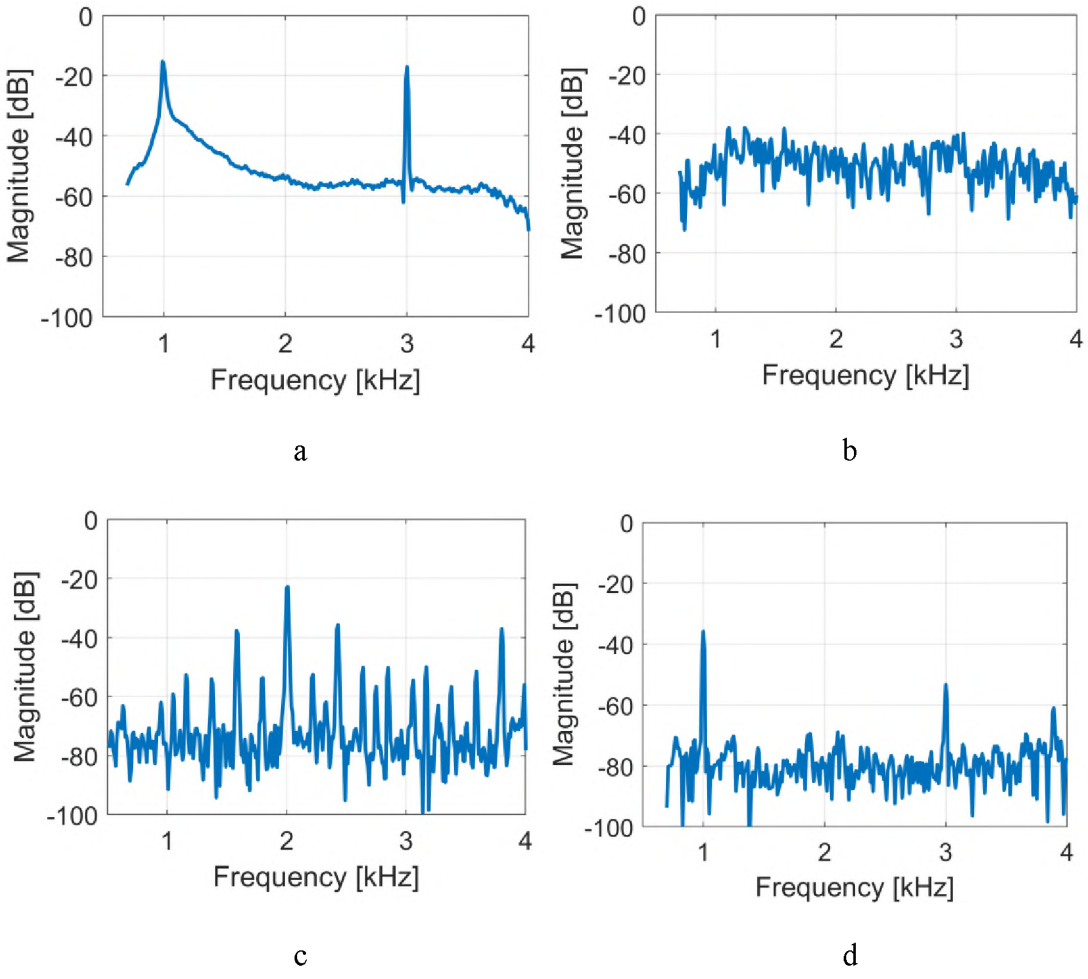


Figure 10. Different variations in spectral contents of the test audio. a) Increased noise floor. b) Absence of expected tones (1 and 3 kHz) plus increased noise floor. c) Multiple tones. d) Difference between the magnitudes of expected tones.

2.3.2. Feature Extraction of Failures. Figure 10 shows how the spectral content of the test audio can change due to a soft failure in this DUT. A different DUT may react

differently under ESD stress. However, it may generate either a complete silence (i.e., no tones), or a combination of humming sound (i.e., increased noise floor), buzzing sound (i.e., addition of other tones), or reduced magnitude of one or both tones. The reduced magnitude failure may not be easily detected by a human and may not be critical for consumer products, but it is important for professional sound systems.

The most prominent feature of Figure 10a is the increased noise floor (by more than 30 dB) relative to the baseline sound (compare to Figure 9). This failure produces a humming sound as if the tones were recorded in a noisy environment. By comparing the average noise floor of the recorded sample with that of the baseline audio, one can determine if this failure has occurred. In this study, an increase more than 10 dB is considered as a failure. The only time-consuming part of this process is the FFT calculation, which considering the sampling rate of the audio file (8 kSa/sec) and the short record length (1 sec), it does not take more than a few milliseconds on a laptop. After FFT calculation, the frequency contents below 700 Hz and above 4 kHz are ignored to remove any artifacts around DC, and limit the bandwidth to 4 kHz, respectively. This choice leaves the frequency range of 700 Hz to 4 kHz intact, where the human hearing is most sensitive [15, 16].

In Figure 10b, there are two distinct features: increased noise floor, and lack of the 1 and 3 kHz tones. This failure can be identified by comparing the magnitude of the tones against the average noise floor, or by comparing the average noise floor with the average noise floor of the baseline audio. The latter approach was used to detect this failure, since the code was already developed; in other words, this failure type is not considered different from Figure 10a.

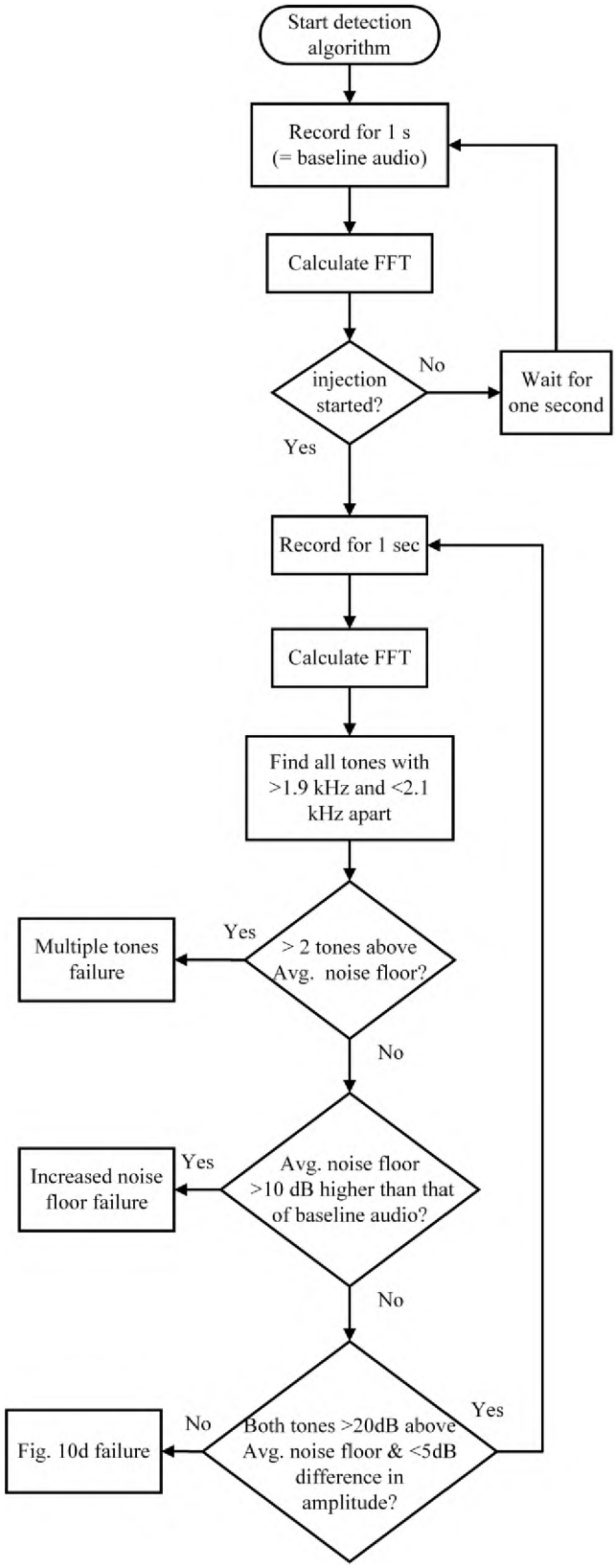


Figure 11. Audio-based detection and characterization algorithm flowchart.

The most obvious feature of Figure 10c is the presence of other tones. In general, these tones might be close to the expected tones (1 and 3 kHz), which makes the detection of this failure more difficult. The algorithm calculates the distance between any two random tones; if this distance is more than 1.9 kHz and less than 2.1 kHz, the two tones are kept for further processing, and the rest are discarded. If more than two tones satisfy the distance criterion, a soft failure has occurred.

The hardest failure to detect is the one shown in Figure 10d because the only difference between this one and the baseline audio is reduced magnitudes of the tones, one tone more than the other. This failure may not be easy to detect for the human ear, as the user might think the volume is low, or the sound was recorded at a low volume. To detect this failure, we used two thresholds. Threshold 1, which is set to 20 dB, enforces that the tones must be at least 20 dB stronger than the average noise floor. Threshold 2, which is set to 5 dB, imposes that the tones must have a magnitude difference of less than 5 dB. The tones are supposed to have the same magnitude. If any of these criteria are met, a failure flag is raised. Figure 11 illustrates the developed audio-based detection algorithm.

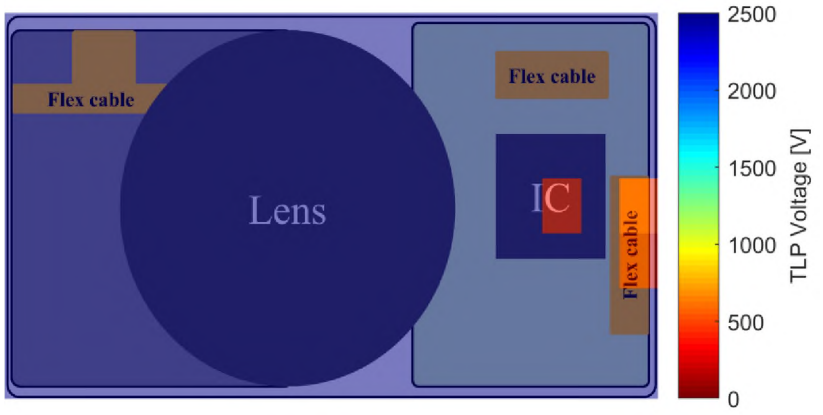
3. FAILURE-SPECIFIC SUSCEPTIBILITY MAP

Using the developed image-based soft failure detection algorithm in conjunction with the automated ESD tester shown in Figure 1, we performed automated soft failure testing on a (different) camera. For this test, an 8 mm magnetic field probe was used to inject noise voltage to the camera circuitry. The probe was moved by the robot while

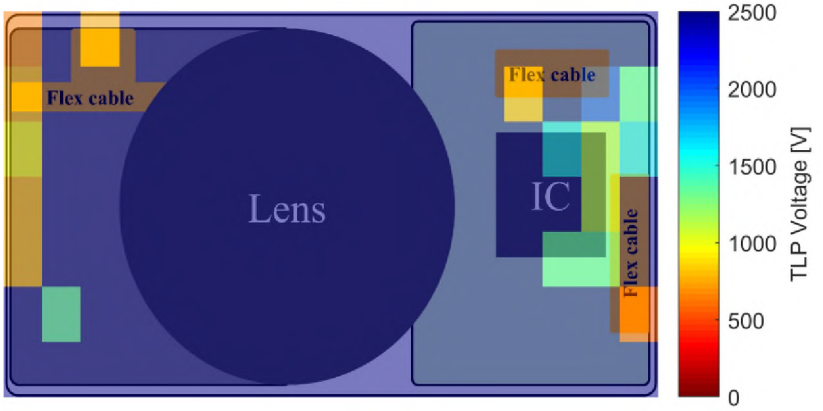
injecting a noise voltage into the DUT. Once a soft failure is detected, the robot position and the TLP voltage that caused this failure are recorded by MATLAB. With this information, a color-coded 2D susceptibility map can be generated for each soft failure. These maps not only show the sensitive locations of the device, but they also show which location(s) are associated with what failure type(s). Figure 12 shows the susceptibility maps obtained from the backside of the camera under test. The camera is replaced with a drawing to preserve confidentiality. The warm colors in the map show the more sensitive regions where a lower noise voltage (see color bar values) was needed to cause a failure. The colder colors show more robust areas.

For this camera, only two types of soft failures occurred: *vertical strips* failure, and *restart* failure. The *restart* failure occurred when the locations shown in Figure 12b were disturbed, while the *vertical strips* failure occurred when the center of the main IC and the middle region of the flex cable were stressed (Figure 12a). This flex cable connects the main IC to the display IC located on the backside of the display (not shown here). One can conclude the main IC is more sensitive than the display IC because disturbing the flex cable resulted in the same failure type as it did when the main IC was stressed (*vertical strips* failure). In other words, this observation suggests the same circuitry was disturbed in both scenarios.

On the left and top side of the DUT, there exists other circuitry for changing focus, controlling the lens, and other settings. Disturbing these circuitries or the flex cable connected to them leads to the *restart* failure. Figure 12b shows the sensitive regions associated with this failure.



a



b

Figure 12. Susceptibility maps separated by failure type. a) *Vertical strips* failure. b) *Direct restart* failure. A drawing is used instead of a photo to preserve confidentiality.

4. DISCUSSION

If the camera under test is changed to a different one, new soft failures might be observed. It is likely that the algorithm cannot characterize the new failures; however, the algorithm can still determine the occurrence of the failures, as explained below.

In general, a soft failure can distort the image by adding extra lines to the image, changing the color of the pixels, warping the image, etc. As a result of this distortion, the

lowest block in Figure 7, which looks for circles in the image using a Circular Hough Transform-based algorithm [17, 18], does not detect exactly one circle in the image. If more or less than one circle is found, provided that the algorithm has not characterized the type of the failure yet, a failure flag is raised, and the image is saved for manual processing. As such, a new soft failure can be detected without a priori knowledge of the failure's feature(s). In order to characterize a new soft failure automatically, a new characterization algorithm must be developed. In the service of this aim, the authors have attempted to elaborate on both the development process and logic that went into the presented algorithms so that the reader can develop their own as needed when called for by the situation.

While thresholds are employed for decision making in the algorithms presented, in order to ensure their accuracy for making correct decisions they should be adjusted to every DUT. One image (or audio track) that includes the failure of interest is sufficient to adjust the threshold(s) associated with that failure. While this is not time-consuming, creating the failure of interest might be difficult and time-consuming as soft failures could be difficult to reproduce.

Finally, the presented algorithms can be considered a platform for automatized soft failure testing, as there is room for improvement. For instance, the algorithms can be enhanced by incorporating supervised or unsupervised machine learning algorithms. Instead of having a human inspect the new soft failures, extract their features, and set thresholds, an algorithm can "learn" to perform these tasks. One of the biggest potential downsides of this approach could be the time needed to train the supervised algorithm, which could be more than the time required to perform the investigations normally,

especially considering that thousands of soft failure types might be needed to train the algorithm. Unsupervised learning algorithms, on the other hand, do not have a training phase. These algorithms try to classify the new soft failures based on the similarities and differences between the features of the new failures and those in the dataset. The use of machine learning algorithms is only one of many possibilities to improve the presented platform.

5. SUMMARY AND CONCLUSION

Automatized soft failure testing can improve the repeatability of the tests and allows for systematic, automated investigations. Automatization requires (1) an automated tester, and (2) soft failure detection and characterization algorithms. The challenge is to detect and characterize both severe and subtle soft failures. In this paper, we developed audio- and image-based algorithms to detect both severe and subtle failures and determine their types. This approach differs from previous approaches (shown in Table 1) in that it detects soft failures in a similar manner the user does – through sight and hearing. These algorithms were then incorporated with a 6-axis industrial Mitsubishi robotic arm to perform automated ESD immunity testing on the target device (camera). Failure-specific susceptibility maps were obtained for this device; only two types of soft failure were observed for this DUT – *vertical strips* failure and *restart* failure. It was found that the main IC was more sensitive than the display IC. Moreover, thanks to the failure-specific susceptibility maps, we found which sensitive location corresponds to what soft failure type.

Having a failure-specific susceptibility map can help to address an ESD immunity issue easier and more efficiently. For instance, a dataset for soft failures and their corresponding regions can be generated. In the case of a reoccurring soft failure, the sensitive parts/circuitry of the product that is responsible for that particular failure can be efficiently identified using the dataset.

REFERENCES

[1] O. H. Izadi, A. Hosseinbeig, D. Pommerenke, H. Shumiya, J. Maeshima, and K. Araki, "Systematic analysis of ESD-induced soft-failures as a function of operating conditions," in 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018, pp. 286-291.

[2] A. Hosseinbeig, O. H. Izadi, S. Shinde, D. Pommerenke, H. Shumiya, J. Maeshima, et al., "A study on correlation between near-field EMI scan and ESD susceptibility of ICs," in 2017 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), 2017, pp. 169-174.

[3] X. Liu, O. H. Izadi, G. Maghlakelidze, M. Pommerenke, and D. Pommerenke, "A Preliminary Study of ESD Effects on the Process Calls Tree of a Wireless Router," in 2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity (EMC, SI & PI), 2018, pp. 408-413.

[4] J. Zhou, Y. Guo, S. Shinde, A. Hosseinbeig, A. Patnaik, O. H. Izadi, et al., "Measurement Techniques to Identify Soft Failure Sensitivity to ESD," IEEE Transactions on Electromagnetic Compatibility, 2019.

[5] X. Liu, G. Maghlakelidze, J. Zhou, O. H. Izadi, L. Shen, M. Pommerenke, et al., "Detection of ESD-induced Soft Failures by Analyzing Linux Kernel Function Calls," IEEE Transactions on Device and Materials Reliability, 2020.

[6] O. H. Izadi, D. Pommerenke, H. Shumiya, and K. Araki, "Investigation of Electrostatic Discharge-Induced Soft-Failure Using 3D Robotic Scanning," in 2019 IEEE International Symposium on Electromagnetic Compatibility, Signal & Power Integrity (EMC+ SIPI), 2019, pp. 173-177.

[7] S. Pertuz, D. Puig, and M. A. Garcia, "Analysis of focus measure operators for shape-from-focus," Pattern Recognition, vol. 46, pp. 1415-1432, 2013.

[8] M. V. Shirvaikar, "An optimal measure for camera focus and exposure," in Thirty-Sixth Southeastern Symposium on System Theory, 2004. Proceedings of the, 2004, pp. 472-475.

[9] J. Canny, "A computational approach to edge detection," IEEE Transactions on pattern analysis and machine intelligence, pp. 679-698, 1986.

[10] C. Gonzalez and E. Woods, "Digital Image Processing, Addison-Wesley Publishing Company," 1991.

[11] P. V. Hough, "Method and means for recognizing complex patterns," ed: Google Patents, 1962.

[12] L. Shapiro and C. George, "Stockman g: computer vision," in Prentice Hall, ed, 2002.

[13] J. R. Parker, Algorithms for image processing and computer vision: John Wiley & Sons, 2010.

[14] D. Adlakha, D. Adlakha, and R. Tanwar, "Analytical comparison between Sobel and Prewitt edge detection techniques," International Journal of Scientific & Engineering Research, vol. 7, p. 4, 2016.

[15] M. Russ, Sound synthesis and sampling: Routledge, 2012.

[16] U. Zölzer, DAFX: digital audio effects: John Wiley & Sons, 2011.

[17] T. Atherton and D. Kerbyson, "Size Invariant Circle Detection Image and Vision Computing," I, vol. 999, p. 7.

[18] E. R. Davies, Machine vision: theory, algorithms, practicalities: Elsevier, 2004.

IV. INVESTIGATION OF ELECTROSTATIC DISCHARGE-INDUCED SOFT-FAILURE USING 3D ROBOTIC SCANNING

Omid Hoseini Izadi
Department of Electrical Engineering
Missouri University of Science and Technology, Rolla, MO, 65409
E-mail: ohp63@mst.edu

ABSTRACT

A robotic ESD scanning system is presented for scanning complex 3D objects. It provides pseudo-2D plots that illustrate the sensitive locations of the device under test on a relative scale. Using this system, we could determine the susceptible regions of the device. It was observed that disturbing different sensitive regions lead to different soft-failure types. Determining the sensitive locations of a complex-shaped DUT helps to identify the disturbed circuitry and verify the effect of countermeasures in a repeatable way.

1. INTRODUCTION

The energy coupled to sensitive circuitry of an electronic device as a result of electro-static discharge (ESD) can cause hard-failure, soft-failure (temporary disturbance) [1, 2], or latch-up [3, 4]. Hard-failures are associated with permanent damage, while soft-failures can be cured by simply power cycling the system. Latch-ups, on the other hand, can lead to a hard-failure, a soft-failure, or an increased current consumption, which can drain the battery quickly.

The root cause of soft-failure can be identified by susceptibility scanning [5]. During a susceptibility scan, noise voltages or currents are induced via electric or magnetic field probes to the device under test (DUT). These probes are moved over the DUT (printed circuit board (PCB), integrated circuit (IC), etc.) while the behavior of the object is monitored. The level of injected noise is varied, starting at a low value and increasing until a soft-failure is observed, or the user-defined maximum level is reached. This is repeated at each test point (location) to obtain a susceptibility map of the DUT. In many cases, transmission line pulsers (TLP) serve as the noise source to inject noise in the form of nano-second pulses. The induced noise at a given probe location is proportional to the TLP charge voltage; thus, the relative sensitivity is often expressed in TLP charge voltage [5].

While hand-held probing often guides the engineer during debugging, it is not reliable for soft-failure characterization because the probe position is not well-defined. A robot can help to increase the chance of obtaining repeatable results and avoid human mistakes.

In [6], the authors incorporated a robot to assist them in obtaining a 2D ESD map for various operating conditions of a device under test. In [7], a robot was used to determine the ESD current propagation throughout a PCB. The authors of [8] employed a robot to identify resonances on a PCB. In [9], a robot was used to scan a flat plane to localize the radiating sources located on a PCB. These robots can only scan a planar DUT with small height variations (a few millimeters). However, geometrically complex DUTs have multiple facets that need to be scanned. The robots mentioned above cannot satisfy this need.

To address this need, we have used a Mitsubishi industrial 6-axis robot to develop an ESD scanning system. 6-axis robots are commonly used for near-field scanning ([10-12]), due to their ability to reach the object from any direction and at any angle. In the following sections, the ESD scanning system block diagram and the corresponding flowchart are presented. This system is then used for investigating the sensitivity of a camera (DUT). As a result, a sensitivity map is obtained for each facet of the DUT. The sensitive regions of the device are identified using these maps.

2. SCANNING SYSTEM TEST SETUP

2.1. BLOCK DIAGRAM AND SYSTEM FLOWCHART

Figure 1 shows the block diagram of the ESD scanning system. The device under test is a camera focused on the monitor. The monitor plays a pre-defined moving image to the camera during the measurements. A webcam connected to MATLAB continuously monitors the DUT's screen. Any distortion in the image is an indication of a soft-failure; therefore, it is essential that the camera and the webcam both be focused. This approach was selected because the operator can see the video being played both on the monitor and the DUT screen. The operator can validate the system functionality and the image quality by comparing the captured image (by the webcam) with the image shown on the monitor.

The Arduino in this diagram acts as the interface between MATLAB, the TLP, and the DUT. Upon MATLAB's command, the Arduino power cycles the DUT, restarts, or changes the zoom settings of the camera (to avoid blurry image). The Arduino can also change the TLP source voltage via the interface block using a pulse width modulation

(PWM) technique. The interface block acts as a low-pass filter by converting the PWM waveform to an analog voltage and hence changing the TLP source voltage. The internal circuitry of the interface block and the Arduino code logic are out of the scope of this paper.

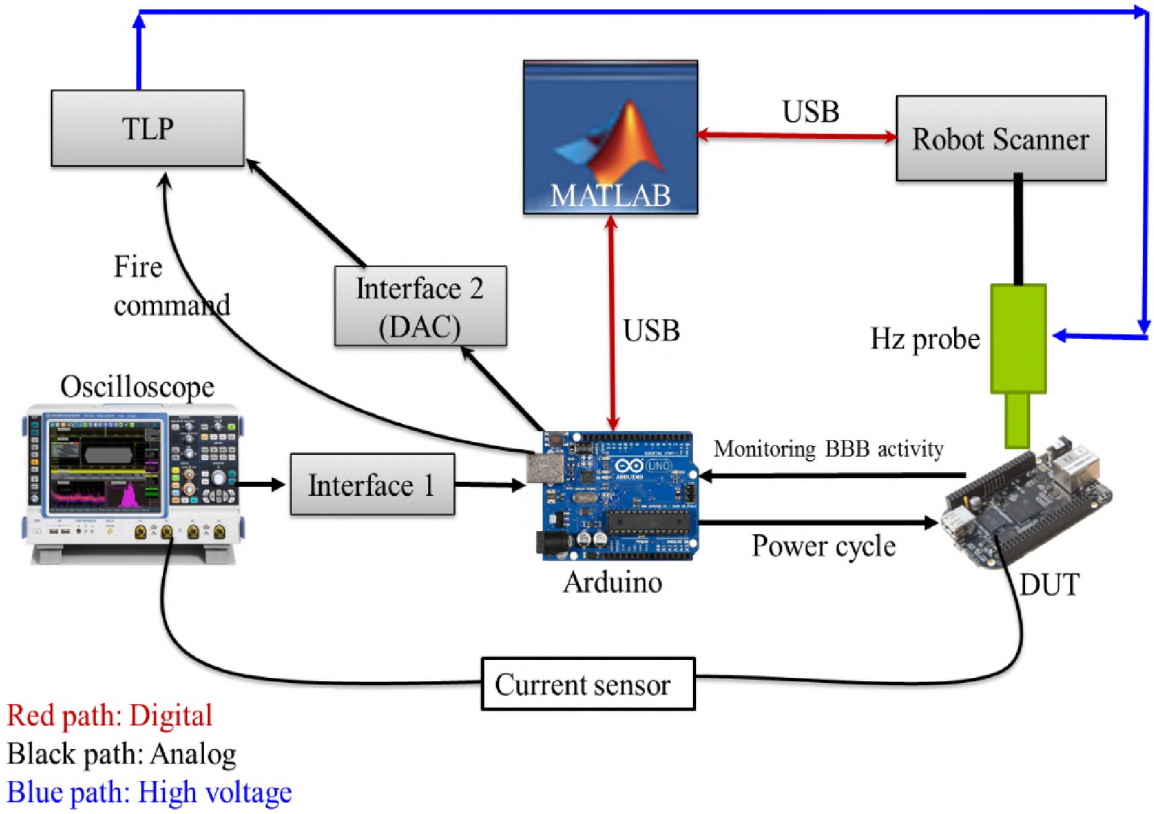
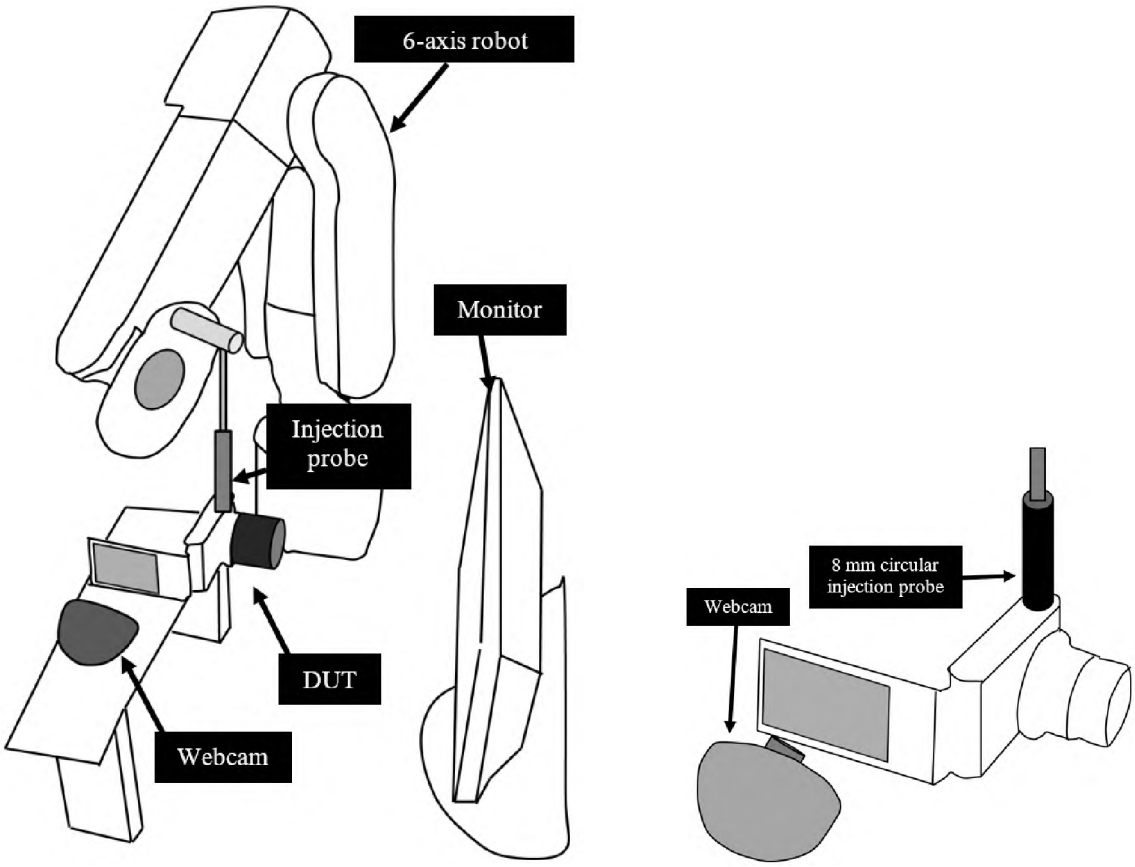


Figure 1. Block diagram of the proposed ESD scanning system.

A 6-axis robot allows us to reach the DUT from many angles and to perform a 3D scan of the object. This robot has a motion uncertainty of less than 100 µm. However, accuracy is only important in case of using a smaller injection probe or a direct injection probe, as the probe must touch a pin or a thin trace on the DUT. Figure 2 and Figure 3 show the measurement setup and the corresponding flowchart, respectively.



a b

Figure 2. a) Measurement setup. b) Close-up view of the device under test and the injection probe. The probe is located on the top of the DUT in this figure. The TLP and the interface blocks are not shown here. A drawing is used instead of a photo to preserve confidentiality.

The injection is done with a magnetic field probe, comprised of a circular loop with 8 mm diameter. More details about the probe geometry are given in [5]. When the probe is driven with 1 A of current, it can produce a magnetic field strength of 114 A/m and induce ~10 mA of current to a 1×0.5 mm loop located ~1 mm beneath the probe loop. The rise time of the pulse is about 350 ps.

As shown in Figure 3, when the test starts the robot is moved to the initial position, MATLAB then sets the TLP voltage to the minimum value set by the user and

initializes the DUT. The initialization process includes power cycling, zooming to the target monitor, and verifying a focused image. A vivid image is critical for correct detection of soft-failures. Once the image quality is verified by using the absolute central moment algorithm, the test starts. Unlike other commonly used algorithms, absolute central moment algorithm does not confuse an out-of-focus image with a low contrast image [13]. This capability helps to avoid false failure detection. After every injection, the MATLAB code evaluates the image obtained by the webcam for a disturbance. If no failure is detected after ten injections, the TLP voltage is increased, and a new image is taken for evaluation. If the TLP voltage reaches 3 kV, the robot is moved to the next location, the DUT is power cycled, and the TLP voltage is reduced to the minimum value. However, if a disturbance is found, the disturbed image and the TLP voltage that caused the failure are recorded. Then the DUT is power cycled and initialized again, prepared for the next round of tests.

2.2. COMMON SOFT-FAILURE TYPES

The MATLAB code is designed to not only detect the occurrence of failure but also to determine the type of failure. The type of soft-failure depends on the DUT (firmware and hardware). For the camera under test, the most common failure types are *black screen*, *direct restart*, *hang*, and *vertical stripes*. A *black screen* error simply turns the camera screen black. It may or may not lead to a restart or a hang afterward. A *hang* failure makes the camera freeze; a power cycle is needed to recover the camera from this failure. The DUT may also directly restart due to the injections, hence the name *direct restart* failure. A *vertical stripes* error is the last commonly observed failure for this

DUT. Given enough time (tens of seconds), this failure will eventually elevate to a restart. When a failure is detected by the code, the code power cycles the DUT within a few seconds after the failure occurrence to prevent possible hardware damage due to latch-up.

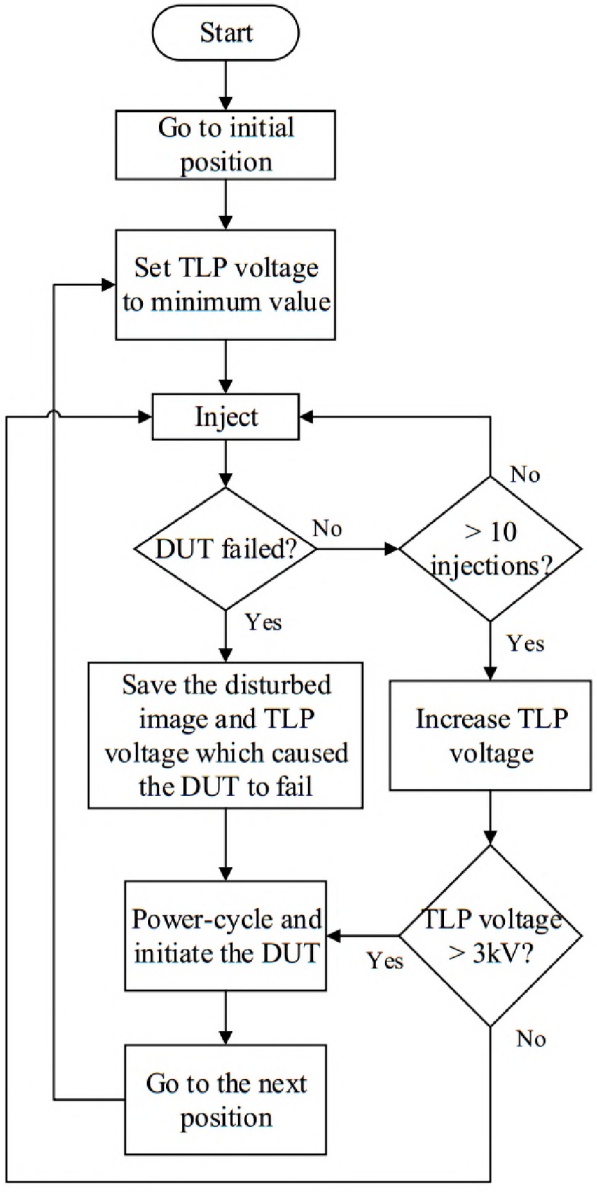


Figure 3. Flowchart of ESD scanning logic.

Besides the MATLAB and Arduino codes, the Smartzap software is also needed to communicate with the robot and control the robot actions. More information on this software is available in [14].

3. SCANNING RESULTS

3.1. SUSCEPTIBILITY MAPS

A susceptibility map shows the sensitive locations of the DUT and the corresponding TLP source voltage that caused a failure. The blue color indicates the DUT has not failed even at the maximum TLP source voltage (3 kV).

Three sides of the DUT have been scanned: left, top, and back. The front side (where the lens is located) and the right side (where the webcam is located) could not be scanned (see Figure 2b), because the robot arm should not cover the webcam-to-screen or the lens-to-monitor line-of-sight. The bottom side could not be scanned either, because the camera is mounted on a stand.

Figure 4 shows the obtained susceptibility maps for the back, the top, and the left side of the camera. Analyzing the data shown in Figure 4a reveals that the area near the IC and the flex cables are the most sensitive regions. This observation is expected, as the flex cables often do not confine the fields well, leading to susceptibility problems. Figure 4b suggests there are some sensitive regions on the top side of the camera, which lead to failure at TLP source voltages as low as 400 V. Opening the camera at this region reveals the presence of some circuitry that is directly connected to the IC through flex cables. A similar observation holds for Figure 4c.

Each colored rectangular in Figure 4 is about 5×5 mm. With this step size, the back side scan takes about 1 hour. A finer resolution is also possible with a smaller probe and step size.

3.2. FAILURE-SPECIFIC SUSCEPTIBILITY MAP

During the susceptibility scan, if the device fails, the failure type will also be recorded. This information allows us to display a susceptibility map for each failure type, as shown in Figure 5. Figure 5a shows three locations on the back side of the camera which led the *vertical stripes* failure when disturbed. Other sensitive locations on the back caused a *direct restart* failure under stress. As observed, a *vertical stripes* failure is triggered at lower TLP source voltages (~400–600 V), than the *direct restart* failure.

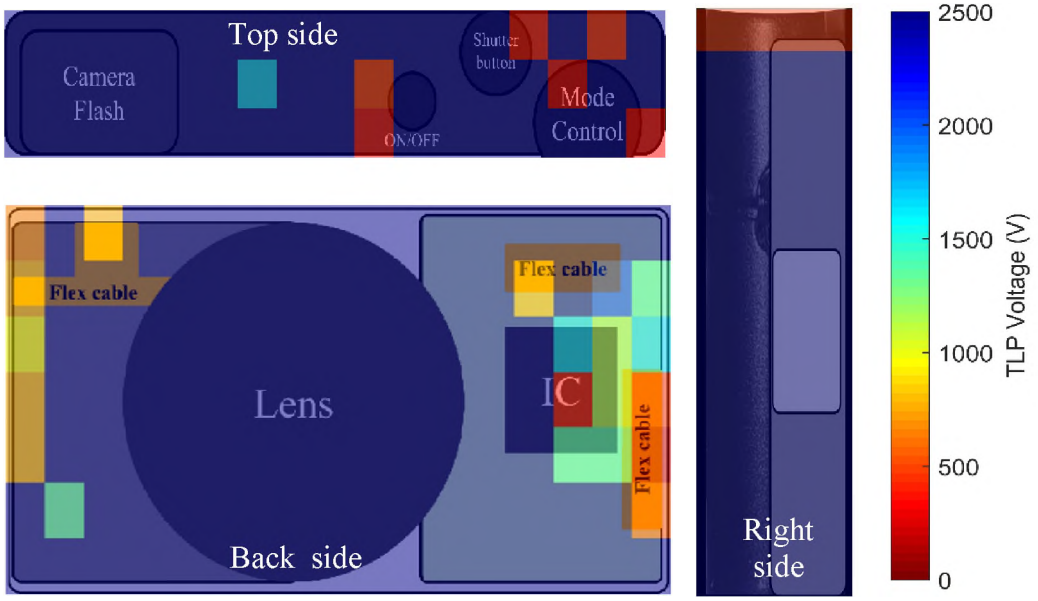
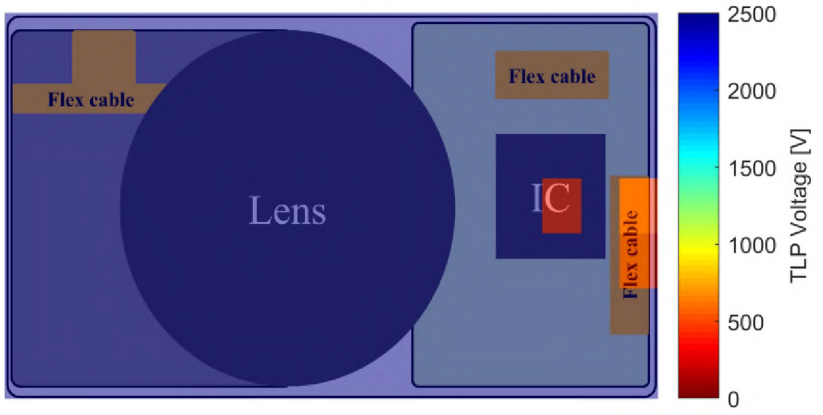
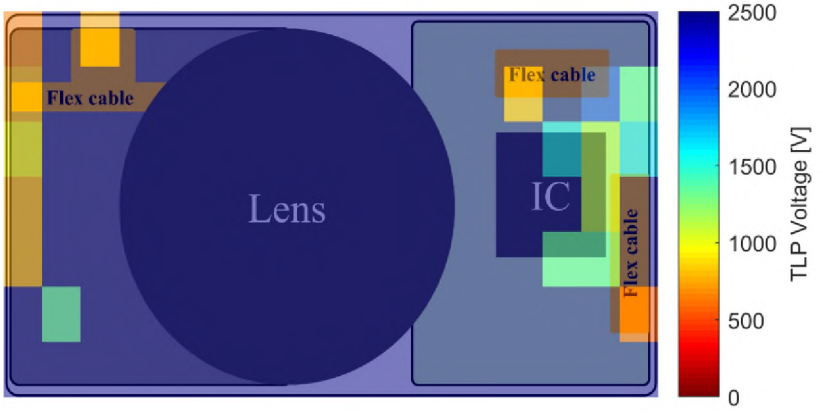


Figure 4. Relative susceptibility maps for back side, top side, and left side of the camera. The color bar represents the TLP source voltage and is the same for all three maps.



a



b

Figure 5. Susceptibility maps separated by failure type. a) *Vertical strips* failure. b) *Direct restart* failure. A drawing is used instead of a photo to preserve confidentiality.

For the top and left side of the camera, only one type of failure was observed: *black screen* failure followed by a system hang. This failure was never observed while scanning the back side.

A failure specific susceptibility map can simplify the root cause analysis of soft-failure as it can help identify which IC (or which part of the device) is disturbed. For instance, if a device fails, one could create a failure specific susceptibility map, narrow down or pinpoint the responsible ICs (or parts), and apply relevant ESD countermeasures.

4. SUMMARY AND CONCLUSION

While hand-held scanning can aid in root cause analysis of ESD-induced soft-failure in DUTs with complex geometry, it does not allow for repeatable testing due to the difficulty for a human to reproduce (and keep track of) the location under stress. The robots used previously for ESD susceptibility scanning could only scan in a 2D plane and were limited to flat surfaces or relatively flat PCBs. In this paper, a 6-axis robot was employed to scan complex 3D surfaces. A block diagram was presented, depicting different parts of the scanner. Three facets of a camera have been scanned, which resulted in three susceptibility maps. Furthermore, for each failure type, an individual susceptibility map was obtained showing the utility of the 6-axis ESD scanning system.

REFERENCES

[1] IEC 61000-4-2: Electromagnetic Compatibility (EMC) – Part 4-2: “Testing and Measurement Techniques – Electrostatic Discharge Immunity Test," Edition 2, Dec. 2008.

[2] N. A. Thomson, Y. Xiu, and E. Rosenbaum, "Soft-failures induced by system-level ESD," IEEE Transactions on Device and Materials Reliability, vol. 17, pp. 90-98, 2017.

[3] T. Brodbeck, W. Stadler, C. Baumann, K. Esmark, and K. Domanski, "Triggering of transient latch-up by system-level ESD," IEEE Transactions on Device and Materials Reliability, vol. 11, pp. 509-515, 2011.

[4] C. Duvvury and H. Gossner, System level ESD co-design: John Wiley & Sons, 2015.

[5] O. H. Izadi, A. Hosseinbeig, D. Pommerenke, H. Shumiya, J. Maeshima, and K. Araki, "Systematic analysis of ESD-induced soft-failures as a function of operating conditions," in 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018, pp. 286-291.

[6] A. Hosseinbeig, O. H. Izadi, S. Shinde, D. Pommerenke, H. Shumiya, J. Maeshima, et al., "A study on correlation between near-field EMI scan and ESD susceptibility of ICs," in Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), 2017 IEEE International Symposium on, 2017, pp. 169-174.

[7] W. Huang, D. Pommerenke, J. Xiao, D. Liu, J. Min, G. Muchaidze, et al., "A measurement technique for ESD current spreading on a PCB using near field scanning," in Electromagnetic Compatibility, 2009. EMC 2009. IEEE International Symposium on, 2009, pp. 18-23.

[8] G. Muchaidze, H. Wei, J. Min, S. Peng, J. Drewniak, and D. Pommerenke, "Automated near-field scanning to identify resonances," in Electromagnetic Compatibility-EMC Europe, 2008 International Symposium on, 2008, pp. 1-5.

[9] P. Maheshwari, H. Kajbaf, V. V. Khilkevich, and D. Pommerenke, "Emission source microscopy technique for EMI source localization," IEEE Transactions on Electromagnetic Compatibility, vol. 58, pp. 729-737, 2016.

[10] J. A. Gordon, D. R. Novotny, M. H. Francis, R. C. Wittmann, M. L. Butler, A. E. Curtin, et al., "Millimeter-wave near-field measurements using coordinated robotics," IEEE Transactions on Antennas and Propagation, vol. 63, pp. 5351-5362, 2015.

[11] R. M. Lebrón, J. L. Salazar, C. Fulton, S. Duthoit, D. Schmidt, and R. Palmer, "A novel near-field robotic scanner for surface, RF and thermal characterization of millimeter-wave active phased array antenna," in Phased Array Systems and Technology (PAST), 2016 IEEE International Symposium on, 2016, pp. 1-6.

[12] R. Li, Z. Huang, E. Kurniawan, and C. K. Ho, "AuRoSS: an autonomous robotic shelf scanning system," in Intelligent Robots and Systems (IROS), 2015 IEEE/RSJ International Conference on, 2015, pp. 6100-6105.

[13] M. V. Shirvaikar, "An optimal measure for camera focus and exposure," in System Theory, 2004. Proceedings of the Thirty-Sixth Southeastern Symposium on, 2004, pp. 472-475.

[14] Internet: http://www.amberpi.com/

.

SECTION

2. CONCLUSIONS AND RECOMMENDATIONS

2.1. SUMMARY AND CONCLUSION

The poor repeatability of ESD (electrostatic discharge) immunity tests combined with a lack of standardized measurement setup/technique for soft failure investigations has led to conflicting observations in the literature regarding the effect of operating conditions on ESD susceptibility. In this dissertation, a synchronized injection approach was proposed to address this conflict, which was rooted in asynchronous injection. In this approach, the system's current consumption and the DUT's EMI were monitored to synchronize injection and detect soft failures. The repeatability of the tests was improved by using a robot scanner. An automated ESD tester was developed by incorporating the synchronized injection setups with a robot scanner, which helped us conclude that:

- The operating conditions did affect the ESD susceptibility of an electronic device.
- The system load instantaneously increases (decreases) even in a manipulated constant load condition.
- The ESD susceptibility of the system is tied to its loading condition and instantaneously increases (decreases) with the system load.

Finally, the capabilities of the automated ESD tester were improved by replacing the XYZ robot with a 6-axis robot and equipping the tester with soft failure characterization algorithms. For the latter, image and audio processing algorithms were

developed and used to detect a soft failure in the same way a human would do – through sight and hearing. This was the first time that signal-processing algorithms were developed and used for soft failure detection and characterization.

Using this upgraded tester, both subtle and severe soft failures were detected and characterized – subtle being a glitch on the display or an audible noise from the speaker; and severe being a restart or a system hang. Soft failure-specific susceptibility maps were obtained, thanks to this approach; i.e., those locations on the device that lead to this specific failure when stressed are found. Such a map facilitates soft failure investigations.

2.2. RECOMMENDATIONS

The detection algorithms developed in this dissertation rely on thresholds to detect, determine, and characterize a soft failure. As already mentioned, these thresholds need to be set beforehand by the operator, which means a newly occurring soft failure cannot be characterized; it can only be detected.

One remedy to this problem is to create a large data set indexing all the possible soft failures associated with the device under test (DUT). This is approach is time-consuming and given that a DUT might get damaged during the data collection process, it is impractical. A better approach would be gathering only part of these data and instead use machine learning to characterize the newly occurred soft failures.

BIBLIOGRAPHY

[1] J. Yousaf, H. Lee, and W. Nah. "System Level ESD Analysis: A Comprehensive Review II on ESD Coupling Analysis Techniques." Journal of Electrical Engineering & Technology 13, no. 5, 2018, pp. 2033-2044.

[2] S. Vora, et al., "Application level investigation of system-level ESD-induced soft failures," in 2016 38th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), 2016, pp. 1-10.

[3] O. H. Izadi, et al. "Systematic analysis of ESD-induced soft-failures as a function of operating conditions." 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), IEEE, 2018.

[4] G. Maghlakelidze, et al., "Pin specific ESD soft failure characterization using a fully automated set-up," in 2018 40th Electrical Overstress/Electrostatic Discharge Symposium (EOS/ESD), 2018, pp. 1-9.

VITA

Omid Hoseini Izadi was born in Esfahan, Iran. He received the B.S. degree and the M.S. degree in Electrical Engineering in 2008 and 2011, respectively. He worked as a research assistant at the Isfahan University of Technology from 2010-2015. He taught various undergraduate courses in 2011 and 2014.

In August 2015, he joined the EMCLAB at the Missouri University of Science and Technology to pursue his Ph.D. degree. His research interests included electromagnetic compatibility (EMC), electromagnetic interference (EMI), ESD-induced soft-failure, and system-efficient ESD design (SEED) modeling. He was the recipient of the IEEE EMC Best Student Design Award and the winner of the IEEE EMC+SIPI Student Hardware Design Contest in 2016 and 2020, respectively. In May 2021, he received his Ph.D. degree in Electrical Engineering from the Missouri University of Science and Technology.

Omid Hoseini Izadi joined Apple Inc. as an EMC System Design Engineer shortly after completion of his Ph.D. program.